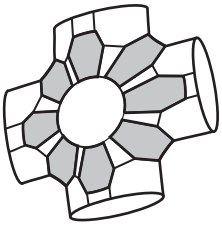


ARS MATHEMATICA CONTEMPORANEA

Volume 24, Number 2, Spring/Summer 2024, Pages 155–383

Covered by:
Mathematical Reviews
zbMATH (formerly Zentralblatt MATH)
COBISS
SCOPUS
Science Citation Index-Expanded (SCIE)
Web of Science
ISI Alerting Service
Current Contents/Physical, Chemical & Earth Sciences (CC/PC & ES)
dblp computer science bibliography

The University of Primorska

The Society of Mathematicians, Physicists and Astronomers of Slovenia
The Institute of Mathematics, Physics and Mechanics
The Slovenian Discrete and Applied Mathematics Society

The publication is partially supported by the Slovenian Research Agency from the Call for co-financing of scientific periodical publications.

Contents

Volume 24, Number 2, Spring/Summer 2024, Pages 155–383

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 24 (2024) #P2.01 / 155–186
https://doi.org/10.26493/1855-3974.2749.b64
(Also available at http://amc-journal.eu)

On local operations that preserve symmetries and on preserving polyhedrality of maps

Gunnar Brinkmann, Heidi Van den Camp *
Ghent University, Krijgslaan 281 S9, Ghent, Belgium

Received 1 December 2021, accepted 8 July 2023, published online 4 September 2023

Abstract

We prove that local operations that preserve all symmetries, as e.g. dual, truncation, medial, or join, as well as local operations that are only guaranteed to preserve all orientation-preserving symmetries, as e.g. gyro or snub, preserve the polyhedrality of simple maps. This generalizes a result by Mohar proving this for the operation dual. We give the proof based on an abstract characterization of these operations, prove that the operations are well defined, and also demonstrate the close connection between these operations and Delaney-Dress symbols.

Keywords: Embedded graph, map, polyhedral embedding, operation, symmetry, tiling.

Math. Subj. Class. (2020): 05C76, 05C10, 05C40, 52B05

1 Introduction

Symmetry-preserving operations on polyhedra have been studied for a very long time. They were first applied in ancient Greece. Some of the Archimedean solids can be obtained from Platonic solids by applying the operation which was later called truncation by Kepler. Over the centuries, polyhedra and specific operations on them have been studied extensively [3, 11, 12, 18, 22]. However, a general definition of the concept *local symmetry-preserving operation* and a systematic way of describing such operations was only presented in 2017 [2]. This description covers a large class of operations on maps, including all well-known symmetry-preserving operations such as truncation, dual, or those operations known as achiral Goldberg-Coxeter operations [4, 5]. Goldberg-Coxeter operations were in fact introduced by Caspar and Klug [4] and can be used to construct all fullerenes or certain viruses with icosahedral symmetry.

*Corresponding author.
E-mail addresses: Gunnar.Brinkmann@ugent.be (Gunnar Brinkmann), heidi.vandencamp@gmail.com (Heidi Van den Camp)

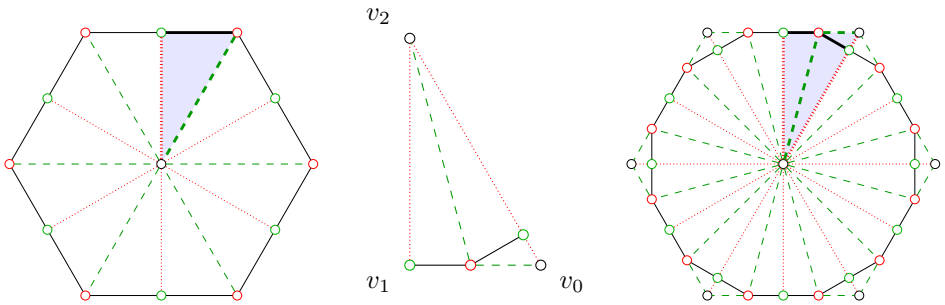


Figure 1: On the left, the barycentric subdivision of a hexagonal face is shown. In the middle, the lsp-operation truncation is given and on the right the barycentric subdivision of the result of applying the operation. The blue shaded area shows one chamber of the original hexagon.

In addition to these local symmetry-preserving operations (lsp-operations), which preserve all the symmetries of a map, there are also operations that are only guaranteed to preserve the orientation-preserving symmetries. Well-known examples of such operations are snub and gyro [23], or the chiral Goldberg-Coxeter operations. In [2], a general description of such *local orientation-preserving symmetry-preserving operations* (lopsp-operations) was also presented. The very general way of describing lsp- and lopsp-operations in [2] allows to tackle various problems from a more abstract perspective, and also allows to prove general theorems about the whole class of operations instead of considering each operation separately. In this paper we will use the new description to prove that all those operations (e.g. dual, medial, truncation, snub, ...) preserve polyhedrality of maps i.e., if an lsp- or lopsp-operation is applied to a simple 3-connected map of face-width at least 3, then the result is also simple and 3-connected and it has face-width at least 3.

As the description in [2] was aimed at a broader audience than just mathematicians, the approach was described in a more intuitive way. In that article an operation is defined as a triangle 'cut' out of a simple periodic 3-connected tiling, and it is applied by gluing copies of that triangle into the barycentric subdivision of a map. Another way of looking at it is that the faces of the barycentric subdivision, which are triangles, are further subdivided into smaller triangles. This is done in a way that the subdivisions of the faces of the barycentric subdivision are identical or mirror images of each other, or – in case only orientation preserving symmetries must be preserved – in a way that each pair of two triangular faces of the subdivision that share the same edge as well as the same face of the map is subdivided in the same way. In the remainder of this text we will give the conditions for these subdivisions that guarantee that the result is the barycentric subdivision of another map – the result of the operation. An example of an lsp-operation and its application is shown in Figure 1. In this article, we will give the more direct definition based on Delaney-Dress symbols that forms the base of this approach and show the connection to the original description. We will also show that for every lsp-operation there is an equivalent lopsp-operation, i.e. a lopsp-operation that has the same result as the lsp-operation when applied to a map.

In [2], it is proved that the result of applying an lsp-operation to a polyhedron – that is: a simple 3-connected map embedded in the plane [17] – is also a polyhedron. In [14] this result is also announced for all lopsp-operations. We will modify some concepts that

are used in that paper, but due to some serious problems in that paper we will not use the results given there.

Originally, lsp- as well as lopsp-operations were only defined for simple plane maps because of their origin in the study of polyhedra. However, there is no mathematical reason why these definitions should not be applied to maps with multiple edges or loops and embeddings of higher genus. The question then arises in how far we can extend the theorem for 3-connected simple plane maps to 3-connected maps of higher genus.

In general, lopsp-operations do not necessarily preserve 3-connectivity for maps that are not plane. This is obvious for maps with faces of size 1 or 2, but it is also true for simple maps in general, even if we require the result to be simple. The most striking example of a local symmetry-preserving operation that can turn 3-connected maps into (even simple) maps with lower connectivity is *dual*. In [1] it is proven that for any $k \geq 1$, there exist embeddings of k-connected simple maps M so that the dual M^* is simple and has a 1-cut.

However, even dual always preserves 3-connectivity in simple maps of face-width at least three, as proven in [20]. In Definition 4.1 and Definition 4.8 we will define $\mathbf{c}k$-maps and $\mathbf{c}k$-operations. A map is $\mathbf{c}k$ if it is k-connected, it has face-width at least k, and all of its faces have size at least k. In this paper we will prove the general Theorem 4.9 from which the following key result is a corollary. The result in [20] for dual is a special case of this result. The map $O(M)$ is the result of applying the operation O to the map M:

Corollary 1.1. *Let $k \in \{1, 2, 3\}$. If M is a $\mathbf{c}k$-map, and O is a $\mathbf{c}k$-lsp- or $\mathbf{c}k$-lopsp-operation, then $O(M)$ is also $\mathbf{c}k$.*

This theorem is most interesting and relevant for $k = 3$. This has two reasons. Firstly, the set of $\mathbf{c}3$-operations contains all well-known and intensely studied operations. Lsp-operations that are not $\mathbf{c}3$-lsp-operations were not even included in the original definition of lsp-operations [2]. Secondly, $\mathbf{c}3$-maps, which are in fact simple embedded 3-connected maps of face-width at least three, have some very interesting properties. These maps are also known as *polyhedral maps* or polyhedral embeddings [20]. They can be defined equivalently as simple maps where every facial walk is a simple cycle and any two faces are either disjoint or their intersection consists of only one vertex or one edge. As the name suggests, polyhedral maps are a generalisation of polyhedra to surfaces of higher genus. It turns out that the key property that these operations preserve is not 3-connectivity but polyhedrality. This property is equivalent to being simple and 3-connected in the plane, but only in the plane. The main result of this article follows immediately from Corollary 1.1: If M is a polyhedral map and O is a $\mathbf{c}3$-lsp- or $\mathbf{c}3$-lopsp-operation, then $O(M)$ is also a polyhedral map (Theorem 4.10).

In Section 2 we give the definitions of the terminology we will use in this text. It starts with some basic concepts and then the definitions of lsp- and lopsp-operations are given. There is some freedom in the way that lopsp-operations are applied. However, in Section 3 we will prove that the result of applying a lopsp-operation is independent of the choices that are made in its application. Section 4 holds the main results of this paper: We prove a general result that implies that all lopsp-operations preserve polyhedrality of maps. To show that the definition of lopsp-operations we give is equivalent to the original definition in [2], we explore the strong connection between lsp- and lopsp-operations and tilings in Section 5.

2 Definitions

There are many different, often equivalent, definitions of a map. A short description is that a *map* is a cellular decomposition of a surface into vertices (0-cells), edges (1-cells), and faces (2-cells). Perhaps more intuitively, a map is an embedding of a topological representation of a graph G onto a surface S. In this text we will only consider 2-cell embeddings, which means that all the connected components of $S \setminus G$ are homeomorphic to 2-dimensional disks. We will only consider *oriented* surfaces. What we will refer to as map is often called an oriented map in texts where more general maps are also studied. Maps are often studied from a topological point of view. To make some technical details easier to describe rigorously, we will use the combinatorial approach that is given below. This definition is equivalent to the topological ones [16, 21]. We will define a map as a graph together with a rotation system, which for every vertex imposes a cyclic rotational order on the edges incident to that vertex.

A *graph* is a tuple (V, E) where V is the set of *vertices* and E is the set of *edges*. Every edge is incident to two vertices that are not necessarily different. If they are the same vertex, then that edge is a *loop*. Though we are mainly interested in graphs without loops or multiple edges, they will occur in a natural way — e.g. as tools or as the result of an operation — so that we will in general assume that the underlying graph of a map may have multiple edges and loops and explicitly restrict the class where necessary.

With every edge of a graph G, we associate two oriented edges, each starting in one vertex of the edge and ending in the other. In the literature these are also called directed edges or darts. If e is one oriented edge, then e^{-1} is the other oriented edge associated with the same edge of G. For every vertex v of G, a cyclic order is assigned to all oriented edges starting at v. This way, every oriented edge e has a 'successor' $\sigma(e)$. A *map* – also known as embedded graph or graph embedding – is a connected graph together with such a successor function σ. In a more general context, our maps could be referred to as oriented maps. As we will not consider unoriented maps we just use the term map. The vertices and edges of a map are the vertices and edges of the underlying graph. When drawing maps, the cyclic order around the vertices induced by σ corresponds to the clockwise order of edges around that vertex in the drawing.

A map is *simple* if it has no loops and no multiple edges that are incident with the same 2 vertices.

A map is *k-connected* if it has at least $k + 1$ vertices and it has no vertex-cut of fewer than k vertices.

Consider three oriented edges e_1, e_2, and e_3 incident with a vertex v. We say that e_2 is *between* e_1 and e_3 if e_1, e_2, e_3 occur in this order in the cyclic order around v, i.e. the cyclic order of edges around v is of the form $(\ldots e_1 \ldots e_2 \ldots e_3 \ldots)$ and not $(\ldots e_3 \ldots e_2 \ldots e_1 \ldots)$.

We say that e and $\sigma(e^{-1})$ form an *angle* in the map. A *face* of a map M is a cyclic sequence of oriented edges such that every two consecutive edges form an angle. We will use the term *facial walk* to refer to the closed walk in M corresponding to this cyclic sequence of oriented edges. This definition of face corresponds to the topological notion of a face.

For a map M, with V_M, E_M, and F_M denoting the sets of vertices, edges, and faces of M respectively, $\chi(M) = |V_M| - |E_M| + |F_M|$ is the *Euler characteristic* of M. The *genus* of M is defined as $gen(M) = \frac{2-\chi(M)}{2}$. If a map has genus 0, it is called *plane*. Note that a plane map is not the same as a planar graph. A planar graph is a graph (not embedded) that

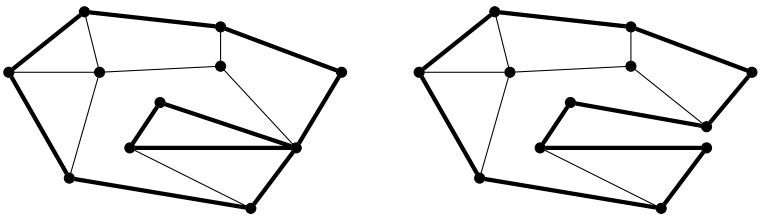


Figure 2: The left figure shows a map and one of its submaps with bold edges.The right figure shows the internal component of the only face of the submap that has bridges.

can be embedded such that it has genus 0. A plane map is one specific genus 0 embedding of a graph.

Let M be a map and G' a subgraph of the underlying graph of M. The map M' which is the graph G' with the embedding induced by that of M is called a *submap* of M.

To formalize when a vertex or edge is 'in' a face of one of its submaps we will now define what a *bridge* for a submap M' of M is. There are two kinds of bridges:

- If $e \in E_M \setminus E_{M'}$ is an edge with endpoints $v, w \in V_{M'}$, then the submap with vertex set $\{v, w\}$ and edge set $\{e\}$ is a bridge.
- Let C be a component of the submap of M induced by the vertices of M that are not in M', and define $E'_C = \{e \in E_M \mid e \cap V_C \neq \emptyset\}$ and $V'_C = \{v \in V_M \mid \exists e \in E'_C : v \in e\}$. Then the submap with vertex set V'_C and edge set E'_C is a bridge.

If a bridge has an edge that is between two edges e and e' so that e^{-1} and e' form an angle in a face of M', then the bridge is *in that face*. All the vertices and edges of the bridge are also said to be *in the face*. The *boundary* ∂f of a face f is the submap of M consisting of all the vertices and edges in the facial walk of f. A vertex or edge of M is in the *interior* of a face of M' if it is in that face and it is not in the boundary.

If a bridge is in more than one face, we say that those faces are *bridged*. A face that is not bridged is called *simple*.

Let f be a simple face of M'. We will define the *internal component* of f as follows. Start with the submap N of M that consists of the boundary of f together with all bridges in f. Intuitively, we cut along the boundary of f in N in such a way that the facial walk becomes a simple cycle. More formally, we replace every vertex v of N that appears $k > 1$ times in the facial walk of f by k pairwise different vertices $v_1, ..., v_k$. If both oriented edges associated with an edge of M' appear in the facial walk, this edge is also split into two different edges between different copies of its vertices. Let (x, v) and (v, y) be the oriented edges that form the angle in M' at the i-th occurrence of v. Then we define the rotational order (and also the neighbours) of v_i to be the same as the rotational order around v in M, but restricted to the edges between (v, x) and (v, y). Of course some vertices may be replaced by their copies. The result of this is the internal component $IC(f)$ of f. An example of an internal component is illustrated in Figure 2. If $IC(f)$ is plane, we call f *internally plane*.

An important concept in the definition of lsp- and lopsp-operations is the barycentric subdivision of a map. It is obtained by subdividing every face into triangular faces, which we will call chambers. We will also use the barycentric subdivision to define contractible cycles and face-width in a combinatorial way.

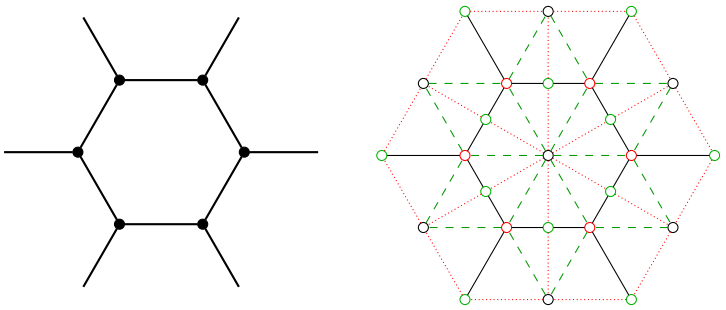


Figure 3: A face in a map M and the corresponding part of B_M. Edges of colour 1 are dashed and edges of colour 2 are dotted.

The *barycentric subdivision* B_M of a map M is a map that has a unique vertex for every vertex, for every edge and for every face of M. We always assume that B_M comes with the natural vertex-colouring that assigns colours 0, 1, and 2 to vertices that correspond to vertices, edges, and faces of M respectively. These colours correspond to their topological dimension. There are edges between vertices of colour 0 and 1 if the corresponding vertex and edge are incident. There are edges between vertices of colour 0 or 1 and colour 2 if the corresponding vertex or edge appears in the boundary of the corresponding face. There are no edges between vertices of the same colour. For $i \in \{0, 1, 2\}$, an edge is *of colour* i if it is not incident with a vertex of colour i. We will also refer to vertices and edges of colour i as i-vertices and i-edges. The rotational order of the edges adjacent to a vertex of colour 2 follows the order of the vertices and edges in the corresponding facial walk of M, and similarly for vertices of colour 0 and 1. This is illustrated in Figure 3. Every face of B_M is a triangle. Note that in every figure in this text, colours are represented by colours in the order rgb, that is: a red is colour 0, green is colour 1, and black is colour 2. The edges of colour 1 are dashed and the edges of colour 2 are dotted, so that when looking at the figures printed in black and white it should still be clear which edges have which colour. With this rotation system, a short calculation of the Euler characteristic shows that $gen(B_M) = gen(M)$. If x is a face, edge or vertex of M, then to keep notation simple we will also write x for the corresponding vertex of B_M.

Every face of B_M is a triangle, with exactly one vertex and one edge of each colour. We call such a triangle a *chamber*. Two chambers are *adjacent* if they share an edge. In the literature, chambers are also called *flags*. The *flag graph* of M is the dual of B_M, i.e. it is the 3-regular graph that has the chambers as its vertices, and there is an edge between two vertices if their corresponding chambers are adjacent. In some papers flags are defined as triples (v, e, f) where v, e, and f are respectively a vertex, an edge, and a face such that v is a vertex of e and v and e are in face f [7, 19]. We cannot use that approach here because with our general definition of a map there is no 1-to-1 correspondence between chambers and triples (v, e, f). For example, an edge can have the same face on both sides so that there are multiple chambers with the same vertices.

Lemma 2.1. *A map M, vertex-coloured with colours 0,1, and 2 is the barycentric subdivision of another map if and only if:*

(i) *Every face of M is a triangle.*

(ii) *There are no edges between vertices of the same colour.*

(iii) *Every vertex of colour* 1 *has degree* 4.

Proof. Let V_G and E_G be the sets of vertices of M with colours 0 and 1 respectively. Conditions (i) and (ii) imply that every face has exactly one vertex of each colour. It now follows from (iii) that a vertex $e \in E_G$ of colour 1 has two neighbours in V_G and two neighbours f and g of colour 2. This induces an incidence relation on the vertex set V_G and the edge set E_G that defines a graph G. The rotation system of M induces a rotation system on G. Let N be the map that consists of G with this rotation system. It is not difficult to check that $M = B_N$. □

The *double chamber map* D_M of a map M is the submap of B_M that only contains the edges of colours 1 and 2. A *double chamber* of a map M is a face in D_M. Every double chamber has length four: two (in case of no loops different) vertices of colour 0, one of colour 1, and one of colour 2. Two double chambers are *adjacent* if they share a 1-edge or two 2-edges.

In [2], lsp- and lopsp-operations are – following Goldberg [15] – defined in a geometric way as triangles 'cut' out of the barycentric subdivision of a 3-connected tiling of the plane, such that in case of lsp-operations the sides of the triangle are on symmetry axes of the tiling. In this article we give purely combinatorial definitions of lsp- and lopsp-operations, similar to [14] and [13]. The definitions given here are equivalent to those in [2] when restricted to what we will later call **c**3-operations. The equivalence can be seen by applying operations as defined here to some special periodic tiling, but readers who want to see the equivalence already before starting on the main results of this paper and who want to have a deeper insight into the relation of operations and periodic tilings encoded by Delaney-Dress symbols, can find a direct proof without applications of the operations in Section 5.

Definition 2.2. Let O be a 2-connected plane map with vertex set V, together with a colouring $c\colon V \to \{0, 1, 2\}$. One of the faces is called the outer face. This face contains three special vertices marked as v_0, v_1, and v_2. We say that a vertex v has *colour* i if $c(v) = i$. This 3-coloured map O is a *local symmetry preserving operation*, lsp-operation for short, if the following properties hold:

(1) Every inner face — i.e. every face that is not the outer face — is a triangle.

(2) There are no edges between vertices of the same colour, i.e. the colouring is proper.

(3) For each vertex that is not in the outer face:

$$c(v) = 1 \Rightarrow deg(v) = 4$$

For each vertex v in the outer face, different from v_0, v_1, and v_2:

$$c(v) = 1 \Rightarrow deg(v) = 3$$

and

$$c(v_0), c(v_2) \neq 1$$

$$c(v_1) = 1 \Rightarrow deg(v_1) = 2$$

An example of an lsp-operation is shown in the middle of Figure 1.

Just like for barycentric subdivisions we say that an edge is of *colour* i if it is not incident to a vertex of colour i. This is well-defined because of the second property.

Every inner face has exactly one vertex and one edge of each colour. We will refer to these triangular faces as *chambers*.

In the original paper [2] only operations that preserve 3-connectivity of polyhedra were discussed, so the result of the operation also had to have only vertices of degree at least 3. In [13] operations were also discussed that produce maps with 1- or 2-cuts, but the restriction that vertices in the result should have degree at least 3 was kept. Our definition of lsp-operations is even more general. With this definition, the result of applying an lsp-operation may have vertices of degree 1 or 2.

Application of an lsp-operation:

Let O be an lsp-operation and let M be a map. The operation is applied to M by first replacing for $i \in \{0, 1, 2\}$ the i-edges of B_M by copies of the part of the boundary of the outer face of O between v_j and v_k with $i \neq j, k$. The copy of v_j is identified with the j-vertex and the copy of v_k with the k-vertex. Then — depending on the orientation — either a copy of O or a copy of the mirror image of O — which has the same underlying graph as O but the rotation system is the inverse of that of O — is glued into every face of the modified B_M. Note that chambers of B_M sharing an edge have different orientations. The boundary vertices are identified with their copies. This results in a 3-coloured triangulation. An example of the gluing — restricted to a single face — is given in Figure 1. With Lemma 2.1 and Definition 2.2 it follows that this triangulation is the barycentric subdivision of a map $O(M)$, the *result* of applying O to M.

As any symmetry group acts on the chamber system, lsp-operations preserve all the symmetries of a map. New symmetries can also occur. However, all known examples of 3-connected maps where lsp-operations can increase symmetry are maps of genus at least 1 or they are self-dual. It is an open question whether lsp-operations can increase symmetry in plane 3-connected maps (polyhedra) that are not self-dual.

There are also interesting operations such as gyro and snub that are only guaranteed to preserve the orientation-preserving symmetries of maps. These cannot be described by lsp-operations. In the supplementary material of [2] and in [14], local orientation-preserving symmetry-preserving operations (lopsp-operations) are defined similarly to lsp-operations. The most important difference is that here the decoration is glued into double chambers instead of chambers. As with lsp-operations, we will give a more explicit definition of lopsp-operations that is not directly based on tilings.

There are some problems that arise in the original definition of lopsp-operations that do not appear for lsp-operations. With the original definition, it is possible to cut different patches out of a tiling that describe the same operation and must be shown to have the same result. That is why we define a lopsp-operation as a plane triangulation, similar to [14], and not as a quadrangle that we can glue directly into double chambers. Although this simplifies the definition of a lopsp-operation, the same problem comes back when it is described how the operation is applied.

Definition 2.3. Let O be a 2-connected plane map with vertex set V, together with a colouring $c\colon V \to \{0, 1, 2\}$ and three special vertices marked as v_0, v_1, and v_2. We say

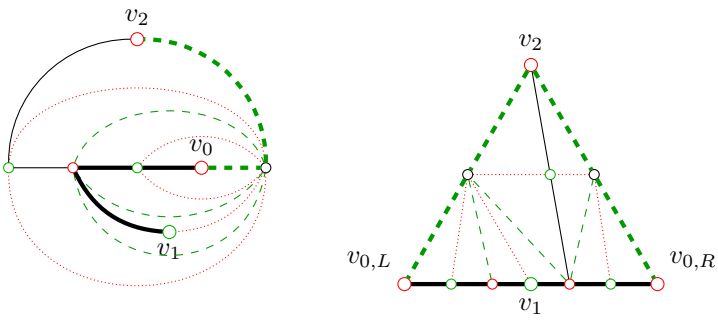


Figure 4: On the left, the lopsp-operation gyro is shown. The thick edges are the edges of the path P. On the right the corresponding double chamber patch O_P is drawn.

that a vertex is of *colour* i if $c(v) = i$. The map O is a *local orientation-preserving symmetry-preserving operation*, lopsp-operation for short, if the following properties hold:

(1) Every face is a triangle.

(2) There are no edges between vertices of the same colour, i.e. the colouring is proper.

(3) For each vertex v different from v_0, v_1, and v_2:

$$c(v) = 1 \Rightarrow deg(v) = 4$$

and

$$c(v_0), c(v_2) \neq 1$$

$$c(v_1) = 1 \Rightarrow deg(v_1) = 2$$

Again we say that an edge has *colour* i if it is not incident to a vertex of colour i and this is well-defined because of the second property. Note that the edges incident with a vertex have two different colours, and as every face is a triangle, these colours appear alternatingly in the cyclic order around the vertex. The requirement that O is 2-connected is mentioned in the beginning, but would in fact also follow from the other conditions. Again every face has exactly one vertex and one edge of each colour and will be referred to as a *chamber*. The dual of O will be referred to as the *flag structure* of O.

Application of a lopsp-operation:

For vertices v, v' in a path P we write $P_{v,v'}$ for the subpath of P from v to v'.

As lopsp-operations are 2-connected, due to Menger's theorem there are two paths, one from v_0 to v_1 and one from v_0 to v_2 that have only v_0 in common. These paths together form a longer path P from v_1 to v_2 through v_0. As a submap of O, P has a single face. In this facial walk only v_1 and v_2 occur once and all other vertices of P occur twice. We say that such a path P is a *cut-path* of O. Consider the internal component of the only face of

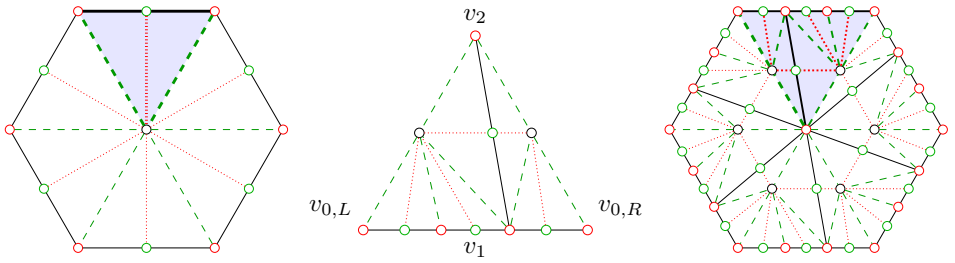


Figure 5: On the left the barycentric subdivision of a hexagonal face is shown. In the middle, a double chamber patch O_P of the operation gyro is drawn, and the right image shows the part of $BO_P(M)$ corresponding to the hexagonal face. The blue shaded area shows one double chamber.

submap P. This is the *double chamber patch* O_P. It can be drawn in the plane, so that the two copies of P form the boundary of the outer face. Figure 4 shows this for the operation gyro. The result of the cutting is a 4-gon with corner vertices v_1, v_2, and two copies of v_0, which we will denote as $v_{0,L}$ and $v_{0,R}$. The *flag structure* of O_P is the flag structure of O where the edges corresponding to edges of P are removed.

The lopsp-operation is now applied by first replacing the edges of a double chamber map D_M to form the map $D_{M,P}$. An edge of colour 2 is replaced by a copy of P_{v_0,v_1} and an edge of colour 1 is replaced by a copy of P_{v_0,v_2} in a way that for $i \in \{0,1,2\}$ a copy of v_i is identified with a vertex of colour i.

Gluing copies of the double chamber patch O_P into the faces of $D_{M,P}$ — identifying corresponding vertices in $D_{M,P}$ and the copies of double chamber patches — gives a coloured map $BO_P(M)$. Note that the orientation inside a double chamber fixes how the different copies of v_0 have to be identified. Unlike with lsp-operations, we do not use mirrored copies of O. Figure 5 gives an example — restricted to one face — of this gluing. A *side* of a double chamber is a path in the boundary of the corresponding face of $D_{M,P}$ that is a copy of the path in O_P between v_2 and $v_{0,L}$, between v_2 and $v_{0,R}$, or between $v_{0,L}$ and $v_{0,R}$. A side is a 1-side if it is between copies of v_0 and v_2 and it is a 2-side if it is between two copies of v_0.

Lemma 2.4. *Let M be a map and let O be a lopsp-operation with a cut-path P. The 3-coloured map $BO_P(M)$ is the barycentric subdivision of a connected map.*

Proof. This follows immediately from Lemma 2.1. □

As lsp-operations preserve all symmetries of a map, they also preserve the orientation-preserving symmetries, so one would expect that for every lsp-operation, there is a lopsp-operation that has the same result when applied to any map. This observation allows to prove some properties of the result of applying lsp- or lopsp-operations only for lopsp-operations. The result for lsp-operations can then be deduced from the corresponding lopsp-operation. Such an equivalent lopsp-operation can be obtained in the following way:

Let O be an lsp-operation, and let c be the boundary of the outer face of O. Let O_{lopsp} be the map obtained by gluing a mirrored copy of the inner face of c into the outer face, identifying the vertices on c with their copies. The vertices v_0, v_1, and v_2 of O are also the vertices v_0, v_1, and v_2 of O_{lopsp}.

Lemma 2.5. *If O is an lsp-operation, then O_{lopsp} is a lopsp-operation, and $O(M) = O_{lopsp}(M)$ for any map M.*

Proof. O_{lopsp} is obviously a triangulation of the disc and there are no edges between vertices with the same colour. As O_{lopsp} consists of two copies of O, glued along the boundary c, we can associate a unique vertex $o(x)$ of O with every vertex x of O_{lopsp}. The degree of x in O_{lopsp} is given by

$$deg(x) = \begin{cases} deg(o(x)) & \text{if } o(x) \text{ is not in } c \\ 2deg(o(x)) - 2 & \text{if } o(x) \text{ is in } c \end{cases}.$$

From the degree restrictions for lsp-operations we can now deduce the degree restrictions in the definition of lopsp-operations for O_{lopsp}. It follows that O_{lopsp} is a lopsp-operation.

Choosing the cut-path in O_{lopsp} that corresponds to the path from v_1 to v_2 through v_0 in c for the application of O_{lopsp} shows immediately that the results of applying O and O_{lopsp} are isomorphic: a double chamber is filled in the same way by O_{lopsp} as two adjacent chambers are filled by O. □

3 The path invariance of lopsp-operations

The cut-path chosen to apply an operation is far from unique, so there are many ways to apply a single lopsp-operation. In this section it is proved that although the ways in which the operation is applied differ, the result of applying a lopsp-operation to a map is independent of the chosen path. An essential tool in proving this are *chamber flips*, which simulate homotopic deformations.

Definition 3.1. Let P be a directed walk in a barycentric subdivision or lopsp-operation. For any two different vertices of a chamber C, there are two different simple paths P_0, P_1 between these vertices in the boundary of C. If for $i \in \{0, 1\}$ path P_i occurs at a certain position in P, then a *chamber flip* of C (at this position) is the operation of replacing P_i by P_{1-i}.

As a first tool we will discuss transformations of one path into another:

Lemma 3.2. *Let P, P' be two directed paths of the form $P = P_sR$, $P' = P_sR'$ from x to y in a lopsp-operation T, so that $R'R^{-1}$ is the facial walk of an internally plane face f in the submap of T consisting of the vertices and edges of P and P'.*

Then there is a sequence of paths $P = P_0, P_1, \ldots, P_k = P'$ so that for $1 \leq i \leq k$ path P_i is obtained from P_{i-1} by a chamber flip and every vertex of P_i is in P_s or in the boundary or the interior of f. As chamber flips can be reversed, the same is true with the role of P and P' interchanged.

Proof. We will prove this by induction on the number $|\mathscr{C}|$ with $\mathscr{C}$ the set of chambers of T inside f. If $|\mathscr{C}| = 1$, then R and R' are the two paths along the boundary of a chamber, so one can be transformed into the other by one chamber flip and we are done. Now assume that $|\mathscr{C}| \geq 2$. We prove that there are at least two chambers in $\mathscr{C}$ that have a connected intersection with ∂f that contains at least one edge: Let $\mathscr{F}_f$ be the dual of T restricted to

$\mathscr{C}$ and without edges that correspond to edges in ∂f. If T is the barycentric subdivision of a map then $\mathscr{F}_f$ is part of the flag graph of that map. There are at least two chambers in $\mathscr{C}$ that contain an edge of ∂f. Assume that there is a chamber C such that $C \cap \partial f$ is disconnected. This chamber C splits the set $\mathscr{C}$ into two parts, i.e. the vertex corresponding to C is a cut-vertex of $\mathscr{F}_f$. In each component of $\mathscr{F}_f \setminus C$ there is at least one chamber that shares an edge with ∂f. Let C_0 be a chamber that contains an edge of ∂f that has the largest distance d_{max} to C along a path in $\mathscr{F}_f$. If this chamber has a disconnected intersection with ∂f, then its corresponding vertex is a cut-vertex of $\mathscr{F}_f$. This implies that there is a chamber that shares an edge with ∂f and has a larger distance to C than d_{max}, which is in contradiction with the maximality of d_{max}. Repeating this argument for the other component of $\mathscr{F}_f \setminus C$, it follows that in each of the two components there is a chamber that has a connected intersection with the facial walk ∂f that contains at least one edge.

Assume that one of these two chambers intersects ∂f in a single edge or in two edges of P or of P'. Then we can do a chamber flip to obtain either a path P_1 or P_{k-1}, so that we can apply induction to P_1, P' or P, P_{k-1} and use that each chamber flip can be undone by a reverse chamber flip.

If the intersection of neither of the two chambers with ∂f is one or two edges of P or P', then both intersections consist of one edge of P and one edge of P'. For one of the chambers, the shared vertex of those edges is the first vertex of R and R'. Applying a chamber flip replacing the edge of P, we get a path P_1 to which we can apply induction. □

Lemma 3.3. *Let Q, Q' be two directed paths from x to y in a lopsp-operation, and z a vertex not contained in either of the paths.*

Then there is a sequence of paths $Q = Q_0, Q_1, \ldots, Q_k = Q'$ from x to y so that for $1 \leq i \leq k$ the path Q_i is obtained from Q_{i-1} by a chamber flip and none of the paths contain z.

Proof. We will prove this by backwards induction on the number n of edges in the beginning of Q that Q and Q' have in common. Remember that for vertices v, v' in a path Q we write $Q_{v,v'}$ for the subpath of Q from v to v'.

If $n = |Q'|$, then $Q = Q'$, so assume that $n < |Q'|$ and that the assumption is true for $n' > n$. Then there is a first vertex a in Q that is incident with an edge that is in Q' but not in Q. Let b be the next vertex after a in Q' that Q' shares with Q. We will show that Q can be transformed to $Q'_{x,a}Q'_{a,b}Q_{b,y}$ in the described way, so that we can apply induction to transform $Q'_{x,a}Q'_{a,b}Q_{b,y}$ into Q'.

Let c be the cycle $Q_{a,b} \cup Q'_{a,b}$. We call the face of c containing z the exterior. Note that neither $Q'_{x,a} = Q_{x,a}$ nor $Q_{b,y}$ intersects c in a vertex other than a or b.

There are four possibilities for the position of $Q_{x,a}$ and $Q_{b,y}$. These are depicted in Figure 6. If $Q_{x,a}$ or $Q_{b,y}$ are in the interior of c, we use them as part of the face boundary when applying Lemma 3.2, otherwise we do not. As Lemma 3.2 already allows to consider paths that start with a common part outside the face, we can choose P, P' from Lemma 3.2 in the following way:

$Q_{b,y}$ outside:	Choose $P = Q_{x,a}Q_{a,b}$, $P' = Q'_{x,a}Q'_{a,b}$.
$Q_{b,y}$ inside:	Choose $P = Q_{x,a}Q_{a,b}Q_{b,y}$, $P' = Q'_{x,a}Q'_{a,b}Q_{b,y}$.

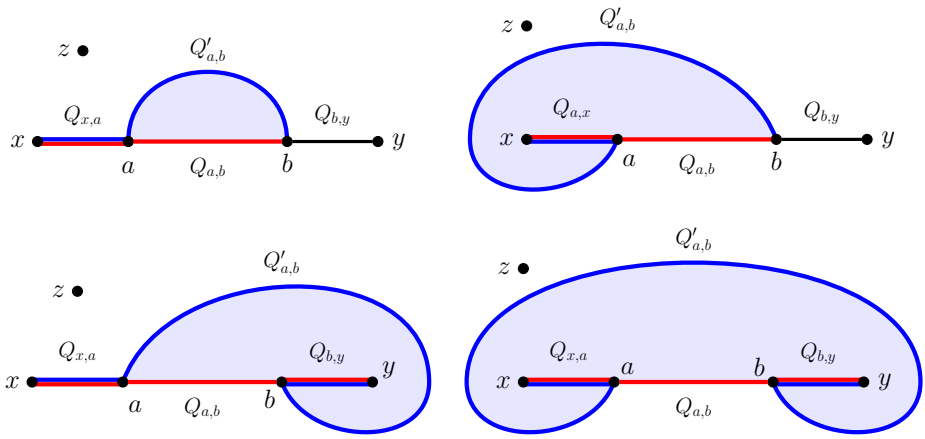


Figure 6: The four different cases in the proof of Lemma 3.3 are shown here. The shaded area represents the interior.

Note that in case $Q_{x,a}$ is outside c it forms the P_s from Lemma 3.2, otherwise P_s consists of a single vertex. In each case Lemma 3.2 can be applied to prove that Q can be transformed to $Q'_{x,a}Q'_{a,b}Q_{b,y}$ in the described way, and as the beginning of $Q'_{x,a}Q'_{a,b}Q_{b,y}$ has more than n edges in common with Q', we can apply reverse induction. □

Let M be a map, O a lopsp-operation with cut-path P and O_P the corresponding double chamber patch. Recall that $BO_P(M)$ is obtained by gluing copies of O_P into D_M. Therefore every vertex v in $BO_P(M)$ is in at least one copy of O_P. If v is in more than one copy, v corresponds to the same vertex of O in each of these copies. Similarly, every edge or face of $BO_P(M)$ also corresponds to exactly one edge or face of O respectively. This allows us to define a surjective mapping π_P, that maps every vertex, edge, and face of $BO_P(M)$ to its corresponding vertex, edge, or face of O.

The mapping π_P is not a bijection, but we can define a kind of inverse function π_P^{-1}. It maps a set X of vertices, edges or faces in O to the set of all the vertices, edges or faces in $BO_P(M)$ whose image under π_P is in X. If we apply π_P^{-1} to a single vertex, edge or face x of O, we will often write $\pi_P^{-1}(x)$ instead of $\pi_P^{-1}(\{x\})$. For submaps M' of O the image $\pi_P^{-1}(M')$ is a subset of vertices and edges of $BO_P(M)$. If these form a connected graph, we interpret it as a map with the embedding induced by $BO_P(M)$.

The definition of $BO_P(M)$ depends on P. We will now prove that the result of an operation is independent of P, so that we can define $O(M)$ for a lopsp-operation O.

Theorem 3.4. *Let O be a lopsp-operation and let P and Q be two cut-paths in O. Let M be a map. Then $BO_P(M) \cong BO_Q(M)$.*

Proof. The idea of this proof is as follows. We define a submap $BO_P(M)|_Q$ of $BO_P(M)$ and prove that the underlying graph of this map is isomorphic as a graph to $D_{M,Q}$. Then we prove that they are also isomorphic as maps, and that the internal component of each face of $BO_P(M)|_Q$ is isomorphic to O_Q. It follows that $BO_P(M)$ is isomorphic to $BO_Q(M)$.

Let e be an edge of D_M, and let j be 1 if e has colour 2 and 2 if e has colour 1. Let P^e be the copy of P_{v_j,v_0} in $BO_P(M)$ that replaced e. By Lemma 3.3 there is a series of paths $P_{v_j,v_0} = P_0, \ldots, P_k = Q_{v_j,v_0}$ from v_j to v_0 in O, so that the path P_{i+1} is obtained from P_i by a chamber flip of a chamber C_i and none of v_0, v_1, v_2 occur as interior points of any of the paths. We define a sequence of paths $P^e = P_0^e, \ldots, P_k^e$ in $BO_P(M)$ with $\pi_P(P_i^e) = P_i$ for $0 \leq i \leq k$. The path P_{i+1}^e will be obtained from P_i^e by applying a chamber flip to a chamber $C \in \pi_P^{-1}(C_i)$. The chamber flips in O on the paths P_i replace subpaths of one or two edges. In case of one edge it is clear that a corresponding chamber flip can be performed on P_i^e in $BO_P(M)$. In case of two edges, we have to prove that the two corresponding edges of P_i^e are also contained in the same chamber. As P_i^e is a path, the two edges share one of their vertices, say v. By definition of the paths P_i we get that $\pi_P(v) \notin \{v_0, v_1, v_2\}$. For such a vertex v it is true that if $e_1, e_2, \ldots, e_k$ is the cyclic order of edges around v, then $\pi_P(e_1), \pi_P(e_2), \ldots, \pi_P(e_k)$ is the cyclic order of the edges around the vertex $\pi_P(v)$. If a chamber flip is applied to the edges $\pi_P(e_j)$ and $\pi_P(e_{j+1})$ to go from P_i to P_{i+1}, then we can apply a chamber flip to the edges e_j and e_{j+1} to go from P_i^e to a new path P_{i+1}^e. Thus our sequence of paths $P^e = P_0^e, \ldots, P_k^e$ in $BO_P(M)$ with $\pi_P(P_i^e) = P_i$ is defined for $0 \leq i \leq k$ and $\pi_P(P_k^e) = Q_{v_j,v_0}$. We denote P_k^e as Q^e. Note that Q^e is isomorphic to Q_{v_j,v_0}, not to Q. Let $BO_P(M)|_Q$ be the map consisting of all the vertices and edges of $BO_P(M)$ contained in Q^e for some edge e. With the rotational orders induced by $BO_P(M)$ we have that $BO_P(M)|_Q$ is a submap of $BO_P(M)$. First we prove that as (non-embedded) graphs, $BO_P(M)|_Q$ and $D_{M,Q}$ are isomorphic.

Two paths Q^e and $Q^{e'}$ can only intersect in their endpoints: Every other vertex v of Q^e and $Q^{e'}$ satisfies $\pi_P(v) \notin \{v_0, v_1, v_2\}$, which implies that v has only two incident edges that are mapped to edges in Q by π_P. It follows that two paths of the form Q^e are either disjoint — except possibly for their endpoints — or identical. We prove by induction that P_i^e and $P_i^{e'}$ are disjoint (except for their endpoints) for all $0 \leq i \leq k$ and edges e and e' in D_M. If e and e' are edges of a different colour this is trivial as at least one of their endpoints is different. Assume that e and e' have the same colour. By our previous argument it suffices to show that their first edge is different. For $i = 0$ this is clear. Assume that it is true for $i-1$. Let ε_i and ε_i' be the first edges of P_i^e and $P_i^{e'}$ respectively. We can assume that they are both incident with the same vertex $x \in \pi_P^{-1}(\{v_0, v_1, v_2\})$. The paths P_i^e and $P_i^{e'}$ are obtained from P_{i-1}^e and $P_{i-1}^{e'}$ by one chamber flip for each path. Either $\varepsilon_i = \varepsilon_{i-1}$ and $\varepsilon_i' = \varepsilon_{i-1}'$, or the chamber flips replace ε_{i-1} and ε_{i-1}' by both their previous edges or both their next edges in the rotational order around x. As ε_{i-1} and ε_{i-1}' are different edges, ε_i and ε_i' are also different edges, which proves our statement.

It follows that $BO_P(M)|_Q$ and $D_{M,Q}$ are isomorphic as graphs. Next we prove that they are also isomorphic as maps.

Let m denote the total number of chamber flips necessary to transform first P_{v_1,v_0} to Q_{v_1,v_0} and then P_{v_2,v_0} to Q_{v_2,v_0}. With every face (that is: double chamber) D of D_M and $0 \leq i \leq m$ we can now associate a closed walk W_i that consists of the four paths $P_i^{e_1}, P_i^{e_2}, P_i^{e_3}, P_i^{e_4}$ in $BO_P(M)$ where $e_1, \ldots, e_4$ are the four edges of D, in the same order as they appear in D.

Claim: $BO_P(M)|_Q$ is a submap of $BO_P(M)$ that is isomorphic as a map to $D_{M,Q}$ and the internal component of each face is isomorphic to O_Q.

Let $\mathscr{C}$ be the set of all chambers in $BO_P(M)$, and let n be the number of chambers in O. We will define functions $\alpha_i \colon \mathscr{C} \to \mathbb{Z}$ $(0 \leq i \leq m)$ with the following properties:

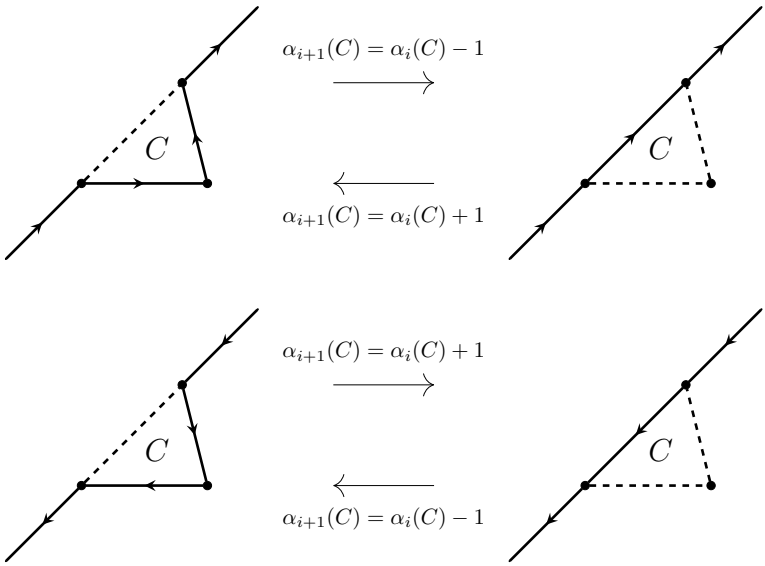


Figure 7: The evolution of α after chamber flips. The bold paths with arrows are W_i and W_{i+1}.

(i) Let C, C' in $BO_P(M)$ be two adjacent chambers sharing the directed edges e and e^{-1}, so that C is on the left of e. For $e' \in \{e, e^{-1}\}$ we define $n_i(e')$ as the number of times e' occurs in the cyclic walk W_i. Then $\alpha_i(C) - \alpha_i(C') = n_i(e) - n_i(e^{-1})$.

(ii) For every chamber C in O: $\sum_{C' \in \pi_P^{-1}(C)} \alpha_i(C') = 1$

As a consequence of (ii) we have $\sum_{C \in \mathscr{C}} \alpha_i(C) = n$.

The walk W_0 is an internally plane facial walk of $D_{M,P}$ with an internal component that is isomorphic to O_P. We define $\alpha_0(C) = 1$ if C is a chamber on the inside of W_0 and $\alpha_0(C) = 0$ if C is on the outside. As W_0 has exactly one copy of each chamber in O inside we get (ii) for α_0. As α_0 only differs for neighbouring chambers if they share an edge of W_0, and then in the way described by (i), we also get (i).

For $i > 0$ we define α_i inductively. Let C be the chamber of O to which a chamber flip is applied when changing W_{i-1} to W_i. These chamber flips occur in two places of W_{i-1}, and in fact in different directions. Two chambers C^-, C^+ with $\pi_P(C^-) = \pi_P(C^+) = C$ are involved, C^- on the left of the cyclic walk and C^+ on the right. We now define $\alpha_i(C^-) = \alpha_{i-1}(C^-) - 1$ and $\alpha_i(C^+) = \alpha_{i-1}(C^+) + 1$. This is illustrated in Figure 7. As we once add one and once subtract one for two chambers with the same image under π_P, (ii) is immediate. Property (i) can be checked easily by looking at α_i for C^-, C^+, and the neighbouring chambers sharing an edge with them.

For $i = 0$, The function α_i describes whether a chamber is inside or outside W_i. For other i this is not always the case. If W_i self-intersects the intuitive meaning of α_i is less obvious.

For $j = 1$ or $j = 2$, the two edges of W_i incident to the j-vertex x of D are always moved in the same direction by the chamber flips. This implies that $\{\alpha_i(C) \mid x \in C\}$ is the same set for every $0 \leq i \leq m$. As $\{\alpha_0(C) \mid x \in C\} \subseteq \{0, 1\}$ — it can be $\{1\}$ if

M has a loop — every chamber that contains x is mapped to 0 or 1 by α_m. The degree in W_m of every vertex that is not in $\pi_P^{-1}(\{v_0, v_1, v_2\})$ is two, so we can follow W_m from v_1 and from v_2 to the copies of v_0 to conclude that for each edge of W_m, the two chambers C and C' containing it have $\alpha_m(C) \in \{0, 1\}$ and $\alpha_m(C') \in \{0, 1\}$. The α_m values of two adjacent chambers can only differ if their shared edge is in W_m, so 0 and 1 are the only values of α_m. Note that this argument only works because every vertex of W_m that is not in $\pi_P^{-1}(\{v_0, v_1, v_2\})$ has degree 2 in W_m. For $0 < i < m$ this is not necessarily the case, and for those values of i the mapping α_i may have values different from 0 and 1.

Consider the submap $\mathscr{F}_m$ of the dual of $BO_P(M)$ — i.e. the flag graph of the map N such that $B_N = BO_P(M)$ — induced by the chambers C with $\alpha_m(C) = 1$, where edges in that map corresponding to edges in W_m are removed. By (ii) it follows that for every chamber C_O in O there is exactly one vertex in $\mathscr{F}_m$. For every edge in the flag structure of O_Q there is exactly one edge in $\mathscr{F}_m$, as by (i) adjacent chambers have the same value under α_m if their shared edge is not in W_m. In fact, these are all the edges of $\mathscr{F}_m$: The maximum degree of a vertex in $\mathscr{F}_m$ is 3, as a chamber is adjacent to three others. Let k be the number of edges in Q. As there are $2k$ edges in W_m, we get $2{\cdot}|E_{\mathscr{F}_m}| = \sum_{v \in \mathscr{F}_m} deg(v) \leq 3n{-}2k$. We also have $2|E_{\mathscr{F}_m}| \geq 2|E_{O_Q}| = 3n - 2k$ and thus $|E_{\mathscr{F}_m}| = |E_{O_Q}|$. It follows that the flag structure of O_Q is isomorphic to $\mathscr{F}_m$. As there are no edges in the flag structure of O_Q that correspond to edges of Q, the walk W_m is the facial walk of a face of $BO_P(M)|_Q$. It follows that $BO_P(M)|_Q$ and $D_{M,Q}$ are isomorphic maps and the internal component of each face of $BO_P(M)|_Q$ is isomorphic to O_Q. □

Definition 3.5. Let O be a lopsp-operation and let M be a map. Choose any cut-path P in O. The *result* $O(M)$ of applying O to M is the map with barycentric subdivision $BO_P(M)$.

By Lemma 2.4 and Theorem 3.4, $O(M)$ is well-defined and independent of the chosen path. We can also define the map $\pi := \pi_P$ as it is independent of the chosen path.

4 The effect of lsp- and lopsp-operations on polyhedrality

Polyhedral maps are simple maps that are 3-connected and have 'face-width' at least three. The face-width (or representativity) of a map is a measure of 'local planarity'. Embeddings of high face-width share certain properties with plane maps. We will define face-width in a combinatorial way, using barycentric subdivisions. It is not difficult to prove that the definition given here is equivalent to the definition in e.g. [20].

A cycle in a map M is *contractible* if – as a submap of M – it has a simple internally plane face. The *face-width* of a map M, denoted $fw(M)$, is the minimal length of a non-contractible cycle in B_M, divided by two. If M has no non-contractible cycles, i.e. M is plane, then we define $fw(M) = \infty$.

Definition 4.1. For $k \geq 1$ we define a map M to be **c**k if:

- M has no cut-sets with fewer than k vertices
- $fw(M) \geq k$
- The size of every face of M is at least k
- The degree of every vertex of M is at least k

The condition that neither cuts with fewer than k vertices nor vertices with degree smaller than k may be present instead of just requiring the map to be k-connected is chosen in order to deal with small boundary cases. For example, a cycle is 2-connected, but its dual is a map with only two vertices so it is not 2-connected. Both a cycle and its dual are $\mathbf{c}2$.

A *polyhedral map* is a simple, 3-connected map that has face-width at least three.

Lemma 4.2. *A map is* $\mathbf{c}3$ *if and only if it is polyhedral.*

Proof. It suffices to prove that every $\mathbf{c}3$-map is simple and has at least four vertices. The rest of the statement is trivial when the definitions are written out. Let M be a $\mathbf{c}3$-map. Facial loops and facial 2-cycles are excluded by the restrictions on face sizes and non-facial loops and non-facial 2-cycles imply either smaller cuts or a smaller face-width. Therefore M is simple. It has at least 4 vertices as it has minimum degree at least 3 and it is simple. □

The reason why the term $\mathbf{c}3$ is used instead of polyhedral in this article is that many results are proven for $\mathbf{c}k$ maps for general $k \in \{1, 2, 3\}$.

The following lemma characterises $\mathbf{c}2$- and $\mathbf{c}3$-maps by a condition based on the chamber system. A 4-cycle in a barycentric subdivision is called *trivial* if it has a face that has no vertex or only a single colour-1 vertex in its interior.

Lemma 4.3. *Let M be a map.*

(i) *M is $\mathbf{c}2$ if and only if B_M has no cycles of length 2.*

(ii) *M is $\mathbf{c}3$ if and only if M is $\mathbf{c}2$, and B_M has no nontrivial cycles of length 4.*

Proof. (i): Let M be a map and assume that M is not $\mathbf{c}2$. There are four possible reasons for not being $\mathbf{c}2$: the existence of a cutvertex, the existence of a facial loop (a face of size 1), the existence of a vertex of degree 1, or the existence of a non-contractible 2-cycle in B_M. The last three immediately imply the existence of a 2-cycle in B_M, so assume that M has a cutvertex v. If there is a loop in M, then there is a 2-cycle in B_M, so assume that M has no loops. Then vertex v has neighbours x and y in different components such that y follows x in the rotational order around v. The facial walk $(x, v), (v, y), (y, w_1), \ldots, (w_k, x)$ of the face f containing this angle must also contain v as one of the w_i as otherwise part of the facial walk would be a path from x to y in $M \setminus \{v\}$. This implies that in the barycentric subdivision there are 2 edges between v and the vertex corresponding to f — a 2-cycle.

Conversely, assume that there is a 2-cycle c in B_M. If there is a 0- or 2-vertex of degree two in B_M then there is a vertex of degree 1 or a face of size 1 in M, so we can assume that every vertex of B_M has degree at least four. We can also assume that every cycle of length 2 in B_M is contractible, as otherwise $fw(M) = 1$ and we are done. This implies that every 2-cycle has two well-defined sides.

Assume w.l.o.g. that c is *innermost*, that is: it contains no 2-cycle in its simple, plane face f_c. Let v and w be the vertices of c. Assume that v has colour 1. Then the two neighbours of v that are not w are on different sides of c. Every face has only three edges and there are no vertices of degree 2, so there are two edges between each of these neighbours of v and w. This is not possible as c is innermost. It follows that the two vertices of c have colours 0 and 2 respectively. There is at least one vertex e_f of colour 1 in the interior of f_c. This vertex e_f has degree 4. If there are no 0-vertices in the interior of f_c then there must

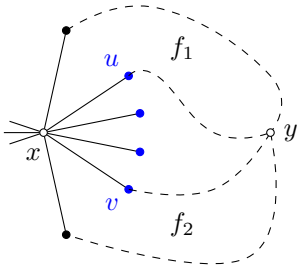


Figure 8: This figure clarifies the proof of (ii) of Lemma 4.3. The blue vertices are all in the same component of $M \setminus \{x, y\}$, and the black vertices are not in that component.

be two edges between e_f and the 0-vertex of c. This is a contradiction with the assumption that c is innermost. It follows that f_c has a 0-vertex in its interior. As every 2-cycle has two well-defined sides, there is an innermost 2-cycle in the other face g_c of c. Using the same arguments as for f_c on that cycle we get that g_c also has a 0-vertex in its interior. Every path in B_M between the 0-vertices in the two faces using only 2-edges must pass through the 0-vertex of c. It follows that this vertex is a cutvertex of M, so that M is not $\mathbf{c}2$.

(ii): Let M be a map and assume that M is not $\mathbf{c}3$. If it is also not $\mathbf{c}2$ we are done, so assume that M is $\mathbf{c}2$. There are four possible reasons for not being $\mathbf{c}3$: the existence of a cutset $\{x, y\}$ of size two, the existence of a face of size two, the existence of a vertex with degree 2, or the existence of a non-contractible 4-cycle in B_M. Again the last three, as well as double edges forming a non-facial 2-cycle in M, immediately give a nontrivial 4-cycle in B_M, so assume that there are no double edges or loops in M, but there is a 2-cut $\{x, y\}$.

Both x and y have neighbours in different components. Let $u \neq y$ be a neighbour of x, so that the previous vertex in the rotational order around x is not in the same component of $M \setminus \{x, y\}$ as u. Let v be the last vertex, as seen from u, in the rotational order around x such that v and all vertices in the rotational order between u and v are in the same component as u, as shown in Figure 8. Note that $u = v$ is possible. If the edges (x, u) and (v, x) would belong to the same face then there would be a colour-1 cycle of length 2 in B_M, so they are in different faces f_1 and f_2 of M. Both f_1 and f_2 must also contain y as otherwise the next, resp. previous neighbour of x would belong to the same component as u and v. The cycle x, f_1, y, f_2 is a nontrivial cycle of length 4 in B_M.

Conversely, assume that M is $\mathbf{c}3$ and that M is not $\mathbf{c}2$ or B_M has a nontrivial cycle of length 4. As M is $\mathbf{c}3$ it is also $\mathbf{c}2$, so B_M has a nontrivial cycle c of length 4. Note that there are no double edges in B_M as M is $\mathbf{c}2$, and M is simple and 3-connected by Lemma 4.2.

The cycle c is contractible because $fw(M) \geq 3$. It therefore has two well-defined sides. Assume first that c has no vertices of colour 0 on one side. Then there must be a 2-vertex on that side, as there cannot only be vertices of colour 1. This 2-vertex can have degree at most 4 as it can be adjacent to at most two 0-vertices in c and there are no double edges in B_M. This implies a facial 2-cycle in M, a contradiction. It follows that there is at least one 0-vertex on each side of c. Every colour-2 path between 0-vertices on different sides passes through c. This implies that the vertices and edges of M corresponding to vertices of c form a cut of M. Ignoring edges if one of their incident vertices is also in c,

this cut consists of 2 vertices, a vertex and an edge or two edges. For each of the edges we can choose one of its incident vertices such that we find a cut-set consisting of 2 vertices, which is a contradiction with the 3-connectivity of M. □

Lemma 4.3 is very useful to determine whether a map is $\mathbf{c}2$ or $\mathbf{c}3$. It will often be used in the following lemmas and theorems. The main theorem of this last section is Theorem 4.9, which shows the equivalence of different definitions of $\mathbf{c}k$-lopsp-operations and states that when applying $\mathbf{c}k$-lopsp-operations with $k \in \{1, 2, 3\}$ to certain maps, the result is $\mathbf{c}k$. The most difficult part of its proof is captured in Theorem 4.5 for $\mathbf{c}2$-maps and Theorem 4.7 for $\mathbf{c}3$-maps.

Lemma 4.4. *Let O be a lopsp-operation with a cut-path P of minimal length.*

(i) *If the vertices of an edge e in O are both in P_{v_0,v_i} for an $i \in \{1, 2\}$, then e or an edge with the same vertices as e is also in P_{v_0,v_i}.*

(ii) *If the vertices of an edge in O_P are in different copies of P_{v_0,v_1}, then there is a nontrivial 4-cycle in two copies of O_P sharing their copies of P_{v_0,v_1}.*

Proof. (i): This follows immediately from the minimality of the length of P.
(ii): If P_{v_0,v_1} is $v_0 = t_1, \ldots, t_k = v_1$ and we denote one copy with $t_1, \ldots, t_k$ and the other with $t'_1, \ldots, t'_k$, then — again due to minimality and as O has no loops — such an edge connects w.l.o.g. t_i with t'_{i+1} for some $1 \leq i < (k-1)$. Considering two copies of O_P sharing the copies of P_{v_0,v_1}, this gives a 4-cycle $c = t_i, t'_{i+1}, t'_i, t_{i+1}$ with v_1 in the interior. If c was trivial, then v_1 would be a 1-vertex adjacent to all 4 vertices on c — also t_i and t'_i — which contradicts the minimality of P. □

Theorem 4.5. *Let M be a $\mathbf{c}2$-map and let O be a lopsp-operation. Then $O(M)$ is $\mathbf{c}2$ if and only if for each cut path P in O we have that there is no 2-cycle in O_P.*

Note that we must consider 2-cycles in O_P and not in O. It is possible that there are 2-cycles in O that do not induce 2-cycles in O_P for any cut-path. For example, the operation gyro, shown in Figure 4*, has several 2-cycles but none in O_P for any cut-path P.*

Proof. If there is a 2-cycle in O_P for a cut-path P then each copy of O_P inserted into $D_{M,P}$ contains a copy of this 2-cycle. Lemma 4.3 now implies that $O(M)$ is not $\mathbf{c}2$.

Conversely, assume that $O(M)$ is not $\mathbf{c}2$. Then there is a 2-cycle c in $B_{O(M)}$. Let x and y be the vertices of c and let e_1 and e_2 be its edges. Let P be a cut-path in O of minimal length. Note that by Lemma 4.3 applied to M, every double chamber has two different 0-vertices and therefore the boundary of each double chamber is simple. It follows that if there exists a double chamber that contains both edges of c in its interior or on its boundary, then c induces a cycle in a copy of O_P and we are done. Assume that e_1 and e_2 are in different double chambers D_1 and D_2 respectively.

Both D_1 and D_2 contain x and y, so those vertices are on the boundary of both double chambers. Assume first that x and y are not both on copies of P_{v_0,v_1} or both on copies of P_{v_0,v_2}. Then D_1 and D_2 share their 1-vertex and their 2-vertex which implies a 2-cycle in B_M, a contradiction. It follows that x and y are both on copies of P_{v_0,v_1} or both on copies of P_{v_0,v_2}. If they are in the same copy of P_{v_0,v_1} or P_{v_0,v_2}, then by Lemma 4.4(i) an edge e_0 with the same vertices is also in that copy of P_{v_0,v_1} or P_{v_0,v_2}, so that O_P contains a 2-cycle.

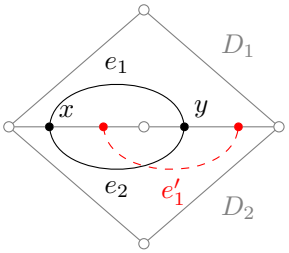


Figure 9: This figure clarifies a step in the proof of Theorem 4.5. It shows that a 2-cycle in $B_{O(M)}$ with its vertices on different copies of the same P_{v_0,v_i} cannot exist. The middle vertex can be the 1- or the 2-vertex of the double chambers. In either case, the left- and rightmost vertices are the 0-vertices.

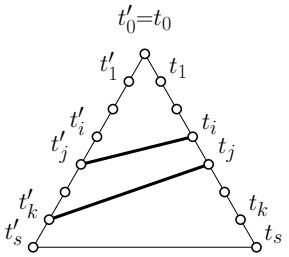


Figure 10: The double chamber patch in the proof of Lemma 4.6. There can be no edge $\{t_l', t_m\}$ with $l < j$ and $m > i$.

The last possibility is that x and y are in different copies of P_{v_0,v_1} or in different copies of P_{v_0,v_2}. As O does not contain loops we have $\pi(x) \neq \pi(y)$. Applying Jordan's curve theorem to c we get that the edge e_1' in D_2 with $\pi(e_1) = \pi(e_1')$ cannot exist — a contradiction (see Figure 9). □

Lemma 4.6. *Let M be a* **c**3*-map and let O be a lopsp-operation with a cut-path P of minimal length. Let f be a 2-vertex of D_M, and consider the submap S_f of $B_{O(M)}$ consisting of all the edges and vertices in the double chambers with 2-vertex f. If there is a nontrivial 4-cycle c in S_f, then there is a 2-cycle in O_P or c is contained in either only one of these double chambers, or in two adjacent double chambers.*

Proof. As M is **c**3, the submap of all vertices and edges of $O(M)$ belonging to one of the double chambers containing f is plane. The map formed by the vertices and edges on the 2-sides of the double chambers in S_f is a simple cycle, that we consider to be the boundary of the outer face of the map S_f. There are at least three double chambers in S_f. If c contains only edges on edges of D_M, then c is the boundary of one double chamber, so assume that c contains at least one edge in the interior of a double chamber.

The boundary ∂D of every double chamber D in S_f is a cycle. As S_f is plane, it follows with the Jordan curve theorem that c must cross ∂D an even number of times. By *cross* we mean that there is a subpath of c whose first and last vertex are on different sides of c, and whose other vertices are all in ∂D. Let D be a double chamber in S_f that contains

an edge of c in its interior. If c crosses ∂D 0 times, then c is contained in one copy of O_P and we are done. If c crosses ∂D 4 times then there must be an edge outside of D that has both its vertices on ∂D. In this case Lemma 4.4 implies that there is a 2-cycle in O_P and we are done. We can therefore assume that c crosses ∂D exactly twice. Note that every crossing is on a 1-side. Assume that the vertices of these crossings are on the same 1-side of D. If there would be only one edge of c in D this again leads to a 2-cycle in O_P with Lemma 4.4. If there is no crossing in f it is clear that a chamber D' adjacent to D also has two crossings with c on the same 1-side. If f is in c that follows from the fact that f is on every 1-side and there must be at least two edges of c in a double chamber that has 2 crossings with c on the same 1-side. It follows that c is completely contained in D and D', i.e. in two adjacent double chambers.

We can now assume that c has two crossings with ∂D that are on different 1-sides and not in f. As c crosses into the double chambers adjacent to D those must also have two crossings on different 1-sides. Repeating this argument we get that every double chamber in S_f has two crossings with c on different 1-sides.

It follows that every double chamber in S_f contains a subpath of c connecting vertices different from f on their two 1-sides. As there are at least three double chambers in S_f and there must be at least one edge of c in each one, there are exactly three or four double chambers in S_f. In each case there are at least two adjacent double chambers that contain only one edge of c. Let e_1 and e_2 be the only edges of c in two adjacent double chambers. As the vertices of e_1 and e_2 are on different 1-sides of O_P the edges e_1 and e_2 are not in P. Therefore the edges $\pi(e_1)$ and $\pi(e_2)$ induce unique edges, that we will also denote with $\pi(e_1)$ and $\pi(e_2)$, in O_P. If the vertices of P_{v_2,v_0} in O are — in this order — $t_0, t_1, \ldots, t_s$, then we will denote the vertices on the different 1-sides of O_P with $t_0, t_1, \ldots, t_s$, resp. $t'_0, t'_1, \ldots, t'_s$. We have $\pi(e_1) = \{t_i, t'_j\}$ and $\pi(e_2) = \{t_j, t'_k\}$ with w.l.o.g. $0 < i < j \leq s$. Note that $i \neq j$ as there are no loops in O. Due to the Jordan curve theorem applied to the cycle $t_0 = t'_0, t'_1, \ldots, t'_j, t_i, t_{i-1}, \ldots, t_0$ there is no edge $\{t_m, t'_l\}$ in O_P with $m > i$ and $l < j$. As $j > i$ and $\pi(e_2) = \{t_j, t'_k\}$ is in O_P, it follows that $k > j$. This situation is shown in Figure 10.

If there are four double chambers in S_f we can repeat this argument on every pair of adjacent double chambers. With x_1, x_2, x_3, x_4 the vertices of c in cyclic order and $\pi(x_a) = t_{i_a}$ we get that $i_a < i_{a+1}$ for all $1 \leq a \leq 3$ and $i_4 < i_1$, so that by transitivity $i_1 < i_1$, a contradiction. If there are only three double chambers in S_f, then there must be two edges e_3 and e_4 of c in the same double chamber. The edges $\pi(e_3)$ and $\pi(e_4)$ form a path from t'_i to t_k. Such a path would have to cross both the edges $\pi(e_1)$ and $\pi(e_2)$, which is only possible if the path has at least three edges — it must contain t_i or t'_j and t_j or t'_k— which is a contradiction. □

Theorem 4.7. *Let M be a* **c**3*-map and let O be a lopsp-operation. Then $O(M)$ is* **c**3 *if and only if it is* **c**2 *and for each cut-path P in O we have that there is no nontrivial 4-cycle in a patch of two adjacent copies of O_P sharing one of their sides.*

Proof. The implication that $O(M)$ is not **c**3 if there is a 2- or nontrivial 4-cycle for some cut-path P is obvious, as corresponding pairs of two adjacent copies of O_P in $B_{O(M)}$ would contain such cycles.

For the other implication we assume that $O(M)$ is not **c**3 but it is **c**2, and that there is no nontrivial 4-cycle in a patch of two adjacent copies of O_P for a cut-path P. We will come to a contradiction by constructing such a 4-cycle. Let P be a cut-path in O of minimal

length. We will refer to the copies of v_2 or v_0 in the double chamber patches as the *corners* of the double chamber patches. By Lemma 4.3 there is a nontrivial 4-cycle c in $B_{O(M)}$. Let X be a set of double chambers in D_M of minimal size, so that the union of all double chamber patches for double chambers in X contains c. For simplicity we will also refer to the set of those double chamber patches as X. The fact that c has four edges implies that $1 \leq |X| \leq 4$. If $|X| = 1$ then c can be thought of as a 4-cycle in O_P, which we assumed does not exist, so $|X| > 1$. We make the following observations:

(i) Every double chamber in X shares at least two of its corners with other elements of X: As $|X| > 1$ the cycle c 'enters' and 'leaves' any double chamber $D \in X$ in two different vertices. Both of these vertices must be in the intersection of D with the other double chambers of X.

(ii) If two double chambers share two corners they also share the side containing those two corners. This follows immediately from the fact that there are no double edges in M and B_M.

(iii) If the intersection of a double chamber $D \in X$ with the other double chambers of X is exactly one side, then there are at least two edges of c in D: Assume that there is only one edge e of c in D, and let D' be the double chamber of X sharing the side with D. Both vertices of e are on the side shared by D and D', but e itself is not, as otherwise D could be removed from X and X would not be minimal. If the vertices of e are on the same edge of D_M, then Lemma 4.4 implies that there is a 2-cycle in O_P, a contradiction with Theorem 4.5. If the vertices of e are on different copies of P_{v_0,v_1} then Lemma 4.4 implies a nontrivial 4-cycle in two adjacent copies of O_P, a contradiction.

It follows from (i) and (ii) that if $|X| = 2$ then c is a 4-cycle in two adjacent copies of O_P, so $|X| > 2$. We will now prove that there is a cycle of length 4 in D_M that contains at least one edge of each double chamber in X. We call such a cycle a *saturating* 4-cycle.

Assume first that every double chamber in X shares the same 2-vertex. With (i), (ii), and (iii), it follows easily that X consists of all the three or four double chambers corresponding to one face of M. Lemma 4.6 now implies that $O(M)$ is not **c**2 or that there is a 4-cycle in two adjacent copies of O_P. Both are contradictions.

Now assume that there is a 2-vertex f of D_M such that there is only one edge e of c in the union of all the double chamber patches of X with 2-vertex f. The edge e has both its vertices on the same 2-side. As at least one of its vertices is not a corner, both double chambers sharing that 2-side are in X. This is a contradiction with (iii).

It follows that there are two 2-vertices f and g in D_M such that the unions X_f and X_g of double chambers patches in X with 2-vertex f and g respectively each contain exactly two edges of c. With (i), (ii), and (iii) it follows that there are 0-vertices v and w of double chambers in X_f and X_g such that v, f, w, g is a saturating 4-cycle.

As M is **c**3, Lemma 4.3 implies that the saturating 4-cycle is the boundary of a double chamber, or two double chambers sharing the 1-vertex.

If e is the 1-vertex in these one or two double chambers, then c is contained in the set N_e consisting of all six double chambers that share a side with a double chamber containing e. We say that the two double chambers with 1-vertex e are the central double chambers, and the four other double chambers in N_e are the extremal double chambers. The three possible configurations of N_e with respect to shared sides are shown in Figure 11. Using the fact

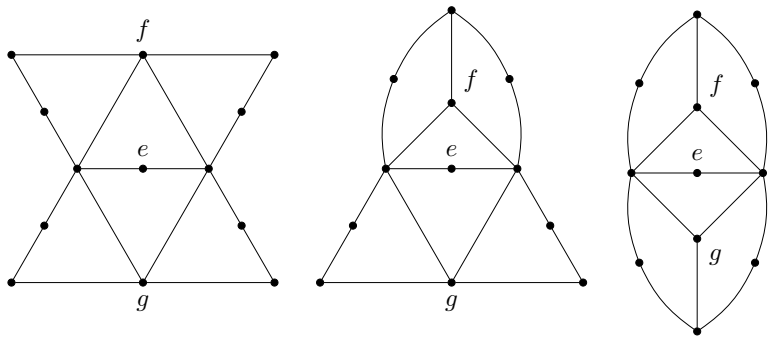


Figure 11: The three possible configurations of the six double chambers in the set N_e are shown here. Different vertices in the drawing represent different vertices of D_M.

that there are no nontrivial 4-cycles in B_M it can easily be verified that no two vertices in Figure 11 represent the same vertex of D_M.

We already proved that $|X| \geq 3$ and that there are two edges of c in X_f and two in X_g. Therefore we can assume w.l.o.g. that X_f consists of two double chambers. It follows from (iii) that these two double chambers are extremal double chambers. The two vertices of the edge e are in c. If the third vertex of c in X_f is f, then with Lemma 4.4 and the fact that there are no 2-cycles in O_P, it follows that the edges of c in X_f are 1-edges of D_M. In that case we can replace the two extremal double chambers in X by the central double chamber so X was not of minimal size, a contradiction. If the third vertex x of c in X_f is not f, then the extremal double chambers share a side and x is on this side. Let e_1 and e_2 be the edges of c in these double chambers. The edge e_1 corresponds to an edge in O_P from w.l.o.g. $v_{0,R}$ to an internal vertex of $P_{(v_{0,L}),v_2}$ and e_2 corresponds to an edge from $v_{0,L}$ to $P_{(v_{0,R}),v_2}$. This would imply crossing edges in the plane map O_P, a contradiction.

It follows that X_f and X_g each consist of only one double chamber, which by (i) must be the central double chamber. Then c is a nontrivial 4-cycle in a patch of two adjacent copies of O_P, a contradiction. □

For a lopsp-operation O, let T_O be the tiling of the Euclidean plane obtained by applying O to the regular hexagonal tiling of the plane. We say T_O is the *associated tiling* of O. With the definition for lopsp-operations from [2] this is the tiling from which O is defined. In Section 5 we will further explore the fundamental connection between lopsp-operations and tilings.

We will use the connectivity of the associated tiling of a lopsp-operation to define when an operation is $\mathbf{c}k$. With Theorem 4.5 and Theorem 4.7 we will then prove an equivalent characterisation in Theorem 4.9 which does not depend on the associated tiling.

Definition 4.8. For $k \in \{1, 2, 3\}$ a lopsp-operation O is $\mathbf{c}k$ if the associated tiling T_O is k-connected and all faces have size at least k. An lsp-operation is $\mathbf{c}k$ if the equivalent lopsp-operation O_{lopsp} is $\mathbf{c}k$.

For a $\mathbf{c}k$-lopsp-operation O and a map M with minimum face size at least k and minimum degree at least k that is not necessarily $\mathbf{c}k$, the map $O(M)$ also has minimum face size at least k and minimum degree at least k. For the vertices of $B_{O(M)}$ of colour 0 or 2

that are not 0-vertices or 2-vertices of D_M, the fact that they have degree at least $2k$ follows from O being a $\mathbf{c}k$-lopsp-operation, as these degrees also occur in the tiling T_O. For the others it follows from the degrees of 0-vertices and 2-vertices in D_M. In case M is also $\mathbf{c}k$, we have a stronger result:

Theorem 4.9. *The following statements are equivalent for $k \in \{1, 2, 3\}$ and a lopsp-operation O:*

(**a**) *O is a $\mathbf{c}k$-lopsp-operation*

(**b**) *For all $\mathbf{c}k$-maps M, $O(M)$ is $\mathbf{c}k$.*

(**c**) *There exists a $\mathbf{c}k$-map M such that $O(M)$ is $\mathbf{c}k$.*

Proof. $\boxed{\textbf{(a)} \Rightarrow \textbf{(b)}}$

For $k = 1$ this is trivial. Assume that there is a $\mathbf{c}2$-map M such that $O(M)$ is not $\mathbf{c}2$. By Theorem 4.5 there is a 2-cycle in O_P for some cut-path P in O. This cycle induces a cycle in B_{T_O}, which implies a 1-cut or a face of size 1 in the tiling T_O. It follows that O is not a $\mathbf{c}2$-operation — a contradiction. Similarly, if there is a $\mathbf{c}3$-map M such that $O(M)$ is not $\mathbf{c}3$, we find a 2-cut in T_O using the cycle from Theorem 4.7.

$\boxed{\textbf{(b)} \Rightarrow \textbf{(a)}}$ For $k = 1$ this is trivial.

The tiling T_O is obtained by inserting copies of O_P (for some P) into the double chamber map of the hexagonal tiling. Let us call the map formed by the subdivided 2-edges of the double chamber map of the hexagonal tiling the hexagonal skeleton.

Assume now that O is not a $\mathbf{c}2$-lopsp operation. Then there is a face f of size 1 or a 1-cut $\{x\}$ in T_O. In case of a 1-cut, at least one of the components of $T_O \setminus \{x\}$, say C_0, is finite. Let C denote a finite submap of the hexagonal skeleton that contains f, resp. C_0 together with the cut vertex x. Using Goldberg-Coxeter operations (see [2] or [4]) with sufficiently large parameters to construct large icosahedral fullerenes, we get a fullerene F, that is $\mathbf{c}3$ and contains an isomorphic copy of C with the paths between the 0-vertices replaced by edges. Applying O to that fullerene, we get a submap S of $O(F)$ that has a face f' of size 1 or that is isomorphic to C_0 and where all vertices corresponding to vertices of C_0 have — except for the vertex x' corresponding to x — only neighbours in S. So f' or the vertex x', which is a cut-vertex of $O(F)$, are contradictions to the assumption.

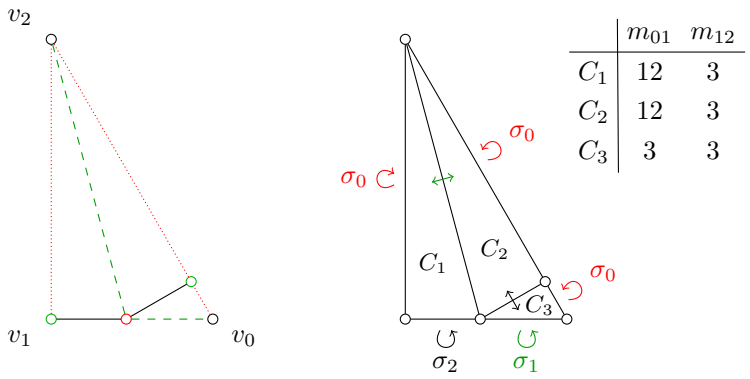
The case $k = 3$ is completely analogous, with also a 2-face and a 2-cut in the argument.

$\boxed{\textbf{(b)} \Rightarrow \textbf{(c)}}$ Trivial.

$\boxed{\textbf{(c)} \Rightarrow \textbf{(b)}}$ Note that the conditions in Theorems 4.5 and 4.7 are — except for M being $\mathbf{c}k$ — independent of M, as O_P and the union of two copies of O_P sharing a side are the same for all these M. This implies that if $O(M)$ is $\mathbf{c}k$ for some $\mathbf{c}k$-map M, then $O(N)$ is $\mathbf{c}k$ for any $\mathbf{c}k$-map N. □

One of the main results of this paper, Theorem 4.10, now follows from Theorem 4.9 and Lemma 2.5.

Theorem 4.10. *If M is a polyhedral map and O is a $\mathbf{c}3$-lsp- or $\mathbf{c}3$-lopsp-operation, then $O(M)$ is also a polyhedral map.*



	m_{01}	m_{12}
C_1	12	3
C_2	12	3
C_3	3	3

Figure 12: The operation truncation and the Delaney-Dress symbol encoding a tiling from which the operation can be obtained when the original definition is applied.

5 Connection to tilings

In a series of papers [8, 9, 10], Andreas Dress (in later papers together with coauthors) developed a finite symbol encoding the topology as well as the symmetry of periodic tilings. He attributed the idea to Matthew Delaney and called these symbols *Delaney symbols*. In later papers by other authors, these symbols are called *Delaney-Dress symbols*. In [6] and [10] Delaney-Dress symbols of periodic tilings of the Euclidean plane and the hyperbolic plane are characterized.

In this section we show that there is a very fundamental connection between l(op)sp-operations and Delaney-Dress symbols and therefore to tilings. Recall that we defined the associated tiling T_O of a lopsp-operation O as the tiling that is the result of applying O to the hexagonal tiling of the plane, i.e. the tiling with Schläfli symbol $\{6,3\}$. We will find the same tiling in a different way using Delaney-Dress symbols, and we will see that from a mathematical point of view the choice of the tiling $\{6,3\}$ is quite arbitrary. The hexagonal tiling was chosen because it was also used in the original definition of lsp-operations in [2], where in turn it was chosen as a tribute to a paper by Goldberg [15]. By proving this connection it follows that our abstract combinatorial definitions are equivalent – in the 3-connected case – to the definitions of lsp- and lopsp-operations in [2].

As a topological definition of tilings falls outside the scope of this article, we will directly start with the combinatorial characterization described in [6, 9, 10]. We will sketch the connection to tilings, but for a detailed description we refer the reader to [6] or [10].

Theorem 5.1 (A.W.M. Dress [9])**.** *Let $\mathscr{D}$ be a set together with an action (from the right) of the Coxeter group $\Sigma = \langle \sigma_0, \sigma_1, \sigma_2 \mid \sigma_i^2 = 1 \rangle$ on $\mathscr{D}$, and for $(i,j) \in \{(0,1),(0,2),(1,2)\}$ let $m_{ij} \colon \mathscr{D} \to \mathbb{N}$ be maps with $m_{02}(C) = 2$ for all $C \in \mathscr{D}$. The tuple $(\mathscr{D}, m_{01}, m_{02}, m_{12})$ is the* Delaney-Dress symbol *of a tiling of the Euclidean plane if and only if the following properties hold:*

(1) *$\mathscr{D}$ has finitely many elements*

(2) *Σ acts transitively on $\mathscr{D}$*

(3) *For $i, j \in \{0, 1, 2\}, i < j$, m_{ij} is constant on $\langle \sigma_i, \sigma_j \rangle$-orbits and $C(\sigma_i\sigma_j)^{m_{ij}(C)} = C$ for all $C \in \mathscr{D}$*

(4) *We have*
$$\mathscr{C}(\mathscr{D}, m_{01}, m_{02}, m_{12}) = \sum_{C \in \mathscr{D}} \left(\frac{1}{m_{01}(C)} + \frac{1}{m_{12}(C)} - \frac{1}{m_{02}(C)} \right) = 0$$

Such Delaney-Dress symbols encode the combinatorial structure of periodic tilings of the Euclidean plane, together with a symmetry group acting on the tiling. If $\mathscr{C}(\mathscr{D}, m_{01}, m_{02}, m_{12}) \neq 0$, the tuple can also be a Delaney-Dress symbol, but then it encodes a periodic tiling of the hyperbolic plane ($\mathscr{C} < 0$) or — in case additional divisibility rules are fulfilled — the sphere ($\mathscr{C} > 0$) [6]. The elements of $\mathscr{D}$ are the orbits of chambers of the tiling under the symmetry group. An element $C \in \mathscr{D}$ with $C\sigma_i = C$ represents an orbit of chambers with mirror symmetries of the tiling stabilizing the edges of colour i. If there are no $C \in \mathscr{D}$ with $C\sigma_i = C$, the symmetry group contains no pure reflections, but maybe sliding reflections. If there are no odd cycles, that is $C\sigma_{i_1} \dots \sigma_{i_k} \neq C$ for odd k, all symmetries are orientation preserving. The maps m_{01} and m_{12} give information about the symmetry group of the tiling. Let $\{i, j, k\} = \{0, 1, 2\}$, $i < j$ and for $C \in \mathscr{D}$ let $r_{ij}(C) = \min\{r \mid C(\sigma_i\sigma_j)^r = C\}$. Note that r_{ij} is constant on $\langle \sigma_i, \sigma_j \rangle$-orbits. If a $\langle \sigma_i, \sigma_j \rangle$-orbit $C^{\langle \sigma_i, \sigma_j \rangle}$ contains no C' with $C'\sigma_i = C'$ or $C'\sigma_j = C'$, then the vertices of colour k of the corresponding chambers in the tiling are centers of an f_r-fold rotation with $f_r = m_{ij}(C)/r_{ij}(C)$. If an orbit $C^{\langle \sigma_i, \sigma_j \rangle}$ contains a C' with $C'\sigma_i = C'$ or $C'\sigma_j = C'$, then with $f_m = 2m_{ij}(C)/r_{ij}(C)$ for $f_m > 1$ the vertices of colour k of the chambers in orbit C are intersections of mirror axes with an angle of $360/f_m$ degrees.

We will now associate a tuple $(\mathscr{D}_O, m_{01}, m_{02}, m_{12})$ with an lsp- or lopsp-operation O and prove that it is a Delaney-Dress symbol. In fact, it will be a Delaney-Dress symbol of the tiling $O(T)$ where T is the tiling with Schläfli symbol $\{6, 3\}$, i.e. the hexagonal tiling of the plane where every vertex has degree 3 and every face has 6 edges. Due to the relation between Delaney-Dress symbols and tilings as described in [6] and [10], this also shows the equivalence of the combinatorial definitions of lsp- and lopsp-operations defined here and the geometric ones given in [2]. There a l(op)sp-operation is described as a 'triangle' cut out of a tiling in such a way that certain conditions on the symmetry are satisfied.

One could replace the values 3 and 6 we will use for defining the mappings m_{ij} by, for example, 4 and 4, and Theorem 5.3 would still be true. It would however be the Delaney-Dress symbol of the tiling that can be obtained by applying O to the square tiling of the plane, which is 4-regular and every face has 4 edges. By using other numbers, other tilings — even spherical or hyperbolic ones — could be used as source tilings. All of those tilings can be used to define l(op)sp-operations in the geometric way that was described in [2] for the hexagonal tiling.

Let O be an lsp-operation and let $\mathscr{D}_O$ be the set of chambers of O. We define the action of Σ on $\mathscr{D}_O$ by letting $C\sigma_i = C'$ if C and C' share their i-edge, and $C\sigma_i = C$ if the i-edge of C is in the outer face of O. For $(i, j) \in \{(0, 1), (0, 2), (1, 2)\}$, let $v^{ij}(C)$ be the vertex of chamber C that is not of colour i or j. We get:

$$r_{ij}(C) = \min\{r \mid C(\sigma_i\sigma_j)^r = C\} = \begin{cases} \frac{\left|C^{\langle\sigma_i,\sigma_j\rangle}\right|}{2} = \frac{deg(v^{ij}(C))}{2} & \text{if } v^{ij}(C) \text{ is not in the outer face} \\ \left|C^{\langle\sigma_i,\sigma_j\rangle}\right| = deg(v^{ij}(C)) - 1 & \text{if } v^{ij}(C) \text{ is in the outer face} \end{cases}$$

To find the Delaney-Dress symbol of the tiling obtained by applying O to $\{6,3\}$ we define $m_{ij}\colon \mathscr{D}_O \to \mathbb{N}$ as follows:

$$m_{ij}(C) = \begin{cases} r_{ij}(C)\cdot 2 & \text{if } v^{ij}(C) = v_1 \\ r_{ij}(C)\cdot 3 & \text{if } v^{ij}(C) = v_0 \\ r_{ij}(C)\cdot 6 & \text{if } v^{ij}(C) = v_2 \\ r_{ij}(C) & \text{if } v^{ij}(C) \notin \{v_0, v_1, v_2\} \end{cases}$$

Note that the requirements for the vertex degrees in an lsp-operation imply that for all $C \in \mathscr{D}_O$, the value $m_{02}(C)$ is 2.

We define $\mathscr{D}(O) = (\mathscr{D}_O, m_{01}, m_{02}, m_{12})$ and call it the Delaney-Dress symbol corresponding to the lsp-operation O. This correspondence is illustrated for the operation truncation in Figure 12. Theorem 5.2 states that it is in fact a Delaney-Dress symbol of a tiling of the Euclidean plane.

By our previous remarks there is a 2-fold rotation around each copy of v_1 in that tiling, a 3-fold rotation around each copy of v_0, and a 6-fold rotation around each copy of v_2. There are also intersections of mirror axes with $90°$, $60°$, and $30°$ angles at v_1, v_0, and v_2 respectively. This is the symmetry we expect when applying an lsp-operation to tiling $\{6,3\}$. This is also the symmetry that is required to define an lsp-operation from a tiling with the geometric definition.

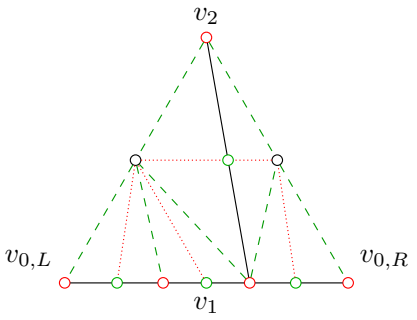
Theorem 5.2. *If O is an lsp-operation, then $\mathscr{D}(O) = (\mathscr{D}_O, m_{01}, m_{02}, m_{12})$ is the* Delaney-Dress symbol *of a tiling of the Euclidean plane.*

Proof. We have to prove the properties in Theorem 5.1. The first two properties are obvious, so we will focus on the other two.

(3): Let $(i,j) \in \{(0,1),(0,2),(1,2)\}$. A $\langle\sigma_i,\sigma_j\rangle$-orbit consists of all the chambers sharing the same vertex $v^{ij}(C)$, so that by definition m_{ij} is constant on $\langle\sigma_i,\sigma_j\rangle$-orbits. It is clear that $C(\sigma_i\sigma_j)^{m_{ij}(C)} = C(\sigma_i\sigma_j)^{r_{ij}(C)\cdot k} = C$

(4): Let $\{i,j,k\} = \{0,1,2\}$. For a vertex v of colour k and $i < j$ we define $\alpha(v) = \sum_{\substack{C\in\mathscr{D}_O \\ v\in C}} \left(\frac{1}{m_{ij}(C)}\right)$.

Counting the number of chambers with a certain vertex and using the definition of m_{ij}, we get that



	m_{01}	m_{12}
C_1	5	6
C_2	5	6
C_3	5	3
C_4	5	3
C_5	5	3
C_6	5	3
C_7	5	3
C_8	5	3
C_9	5	3
C_{10}	5	3

Figure 13: On the left, the double chamber patch of the lopsp-operation gyro is shown and on the right the corresponding Delaney-Dress symbol.

$$\alpha(v) = \begin{cases} 2 & \text{if } v \text{ is an inner vertex} \\ 1 & \text{if } v \text{ is an outer vertex different from } v_i \text{ for } i = 0,1,2 \\ 1/2 & \text{if } v = v_1 \\ 1/3 & \text{if } v = v_0 \\ 1/6 & \text{if } v = v_2 \end{cases}.$$

Let n be the number of vertices (and equivalently edges) in the outer face. As every vertex of O has exactly one colour we get that:

$$\begin{aligned} \mathscr{C}(\mathscr{D}_O, m_{01}, m_{02}, m_{12}) &= \sum_{C \in \mathscr{D}_O} \left(\frac{1}{m_{01}(C)} + \frac{1}{m_{12}(C)} - \frac{1}{m_{02}(C)} \right) \\ &= \sum_{C \in \mathscr{D}_O} \left(\frac{1}{m_{01}(C)} + \frac{1}{m_{12}(C)} + \frac{1}{m_{02}(C)} \right) - \sum_{C \in \mathscr{D}_O} (1) \\ &= \sum_{v \in V_O} \alpha(v) - (|F_O| - 1) \\ &= (|V_O| - n) \cdot 2 + (n-3) \cdot 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - (|F_O| - 1) \\ &= 2|V_O| - |F_O| - n - 1 \end{aligned}$$

By counting the number of directed edges associated with edges in the triangulated disk O in two ways, we get that $2|E_O| = 3(|F_O| - 1) + n$ or equivalently $|F_O| = 2|E_O| - 2|F_O| + 3 - n$. We also know that O is plane, so $|V_O| - |E_O| + |F_O| = 2$. It follows that:

$$\mathscr{C}(\mathscr{D}_O, m_{01}, m_{02}, m_{12}) = 2|V_O| - 2|E_O| + 2|F_O| - 3 + n - n - 1 = 0 \quad \square$$

We will now prove the corresponding result for lopsp-operations. Let O be a lopsp-operation and let $\mathscr{D}_O$ be the set of chambers of O. We define the action of Σ on $\mathscr{D}_O$ by letting $C\sigma_i = C'$ if C and C' share their i-edge. For lopsp-operations there is no outer face, so $r_{ij}(C)$ is always $\frac{deg(v^{ij})}{2}$. We define $m_{01}, m_{02}, m_{12} : \mathscr{D}_O \to \mathbb{N}$ exactly as before:

$$m_{ij}(C) = \begin{cases} r_{ij}(C) \cdot 2 & \text{if } v^{ij}(C) = v_1 \\ r_{ij}(C) \cdot 3 & \text{if } v^{ij}(C) = v_0 \\ r_{ij}(C) \cdot 6 & \text{if } v^{ij}(C) = v_2 \\ r_{ij}(C) & \text{if } v^{ij}(C) \notin \{v_0, v_1, v_2\} \end{cases}$$

Again $m_{02}(C) = 2$ for all $C \in \mathscr{D}_O$. We define $\mathscr{D}(O) = (\mathscr{D}_O, m_{01}, m_{02}, m_{12})$ and in Theorem 5.3 we prove that it is a Delaney-Dress symbol. The operation gyro and its corresponding Delaney-Dress symbol are shown as an example in Figure 13. Once again, the tiling described by the Delaney-Dress symbol is the result of applying the operation to the hexagonal tiling of the plane. In Section 4 we named this tiling the associated tiling T_O of O. There are 2-, 3-, and 6-fold rotations at the copies of v_1, v_0, and v_2 respectively. In lopsp-operations there is no chamber C such that $C\sigma_i = C$ so there are no pure reflections encoded in the Delaney-Dress symbol. This is the symmetry required in the geometric definition of lopsp-operations.

Theorem 5.3. *If O is a lopsp-operation, then $\mathscr{D}(O) = (\mathscr{D}_O, m_{01}, m_{02}, m_{12})$ is the* Delaney-Dress symbol *of a tiling of the Euclidean plane.*

Proof. We prove the properties in Theorem 5.1. Again, the first two are obvious.

(3): As in the proof of Theorem 5.2.

(4): Let $\{i, j, k\} = \{0, 1, 2\}$. For a vertex $v \in V_O$ of colour k and $i < j$ we again define $\alpha(v) = \sum_{\substack{C \in \mathscr{D}_O \\ v \in C}} \left(\frac{1}{m_{ij}(C)}\right)$.

Counting the number of chambers with a given vertex v and using the definition of m_{ij}, we get that

$$\alpha(v) = \begin{cases} 2 & \text{if } v \notin \{v_0, v_1, v_2\} \\ 1 & \text{if } v = v_1 \\ 2/3 & \text{if } v = v_0 \\ 1/3 & \text{if } v = v_2 \end{cases}.$$

We can now compute $\mathscr{C}(\mathscr{D}_O, m_{01}, m_{02}, m_{12})$:

$$\begin{aligned}\mathscr{C}(\mathscr{D}_O, m_{01}, m_{02}, m_{12}) &= \sum_{C\in\mathscr{D}_O}\left(\frac{1}{m_{01}(C)}+\frac{1}{m_{12}(C)}-\frac{1}{m_{02}}\right)\\ &= \sum_{C\in\mathscr{D}_O}\left(\frac{1}{m_{01}(C)}+\frac{1}{m_{12}(C)}+\frac{1}{m_{02}}-1\right)\\ &= \sum_{v\in V_O}\alpha(v)-|\mathscr{D}_O|\\ &= (|V_O|-3)\cdot 2+\frac{2}{3}+1+\frac{1}{3}-|F_O|\\ &= 2|V_O|-|F_O|-4\end{aligned}$$

As O is a triangulation, we get that $2|E_O| = 3|F_O|$ and as O is plane, we have $|V_O| - |E_O| + |F_O| = 2$. It follows that:

$$\mathscr{C}(\mathscr{D}_O, m_{01}, m_{02}, m_{12}) = 2|V_O| - 2|E_O| + 2|F_O| - 4 = 0 \qquad \square$$

In Lemma 2.5 we proved that for every lsp-operation there is an equivalent lopsp-operation O_{lopsp}. Lemma 5.4 proves formally that the Delaney-Dress symbols of the lsp-operation and its corresponding lopsp-operation in fact encode isomorphic tilings.

Lemma 5.4. *The Delaney-Dress symbols $\mathscr{D}(O)$ and $\mathscr{D}(O_{lopsp})$ are Delaney-Dress symbols of combinatorially isomorphic tilings.*

Proof. Mapping each chamber C_{lopsp} of $\mathscr{D}(O_{lopsp})$ onto the corresponding chamber C of $\mathscr{D}(O)$, we have (in the notation of [10]) a morphism between the symbols and in the notation of [6] a Delaney map f, that is: For all $k \in \{0, 1, 2\}$, $(i, j) \in \{(0, 1), (0, 2), (1, 2)\}$, and chambers C of $\mathscr{D}(O_{lopsp})$ we have $f(C\sigma_k) = (f(C))\sigma_k$ and $m_{ij}(C) = m_{ij}(f(C))$.

The existence of such a morphism guarantees (see [6, 10]) that $\mathscr{D}(O)$ and $\mathscr{D}(O_{lopsp})$ code combinatorially isomorphic tilings and that the tiling coded by $\mathscr{D}(O_{lopsp})$ can be obtained from the tiling coded by $\mathscr{D}(O)$ by *symmetry breaking* — That is: modifying the tiling, so that the combinatorial structure is preserved, but some metric symmetries of the tiling are destroyed. $\square$

6 Future work

In the last section of [2] many open problems are described. They are sometimes just formulated for lsp-operations, but are often as relevant and interesting for lopsp-operations, so we refer the reader to [2]. A very interesting question is whether ambo is 'essentially' the only lsp-operation that can increase the symmetry of polyhedra, i.e. plane 3-connected maps. More specifically: Assume that for an lsp-operation O and a polyhedron M, the polyhedron $O(M)$ has more symmetries than M. Is M self-dual and can O be written as the product of ambo and other lsp-operations? For lopsp-operations this is certainly not true. For example, applying gyro to the tetrahedron gives the dodecahedron, which has a much larger symmetry group. Classifying lopsp-operations that can introduce new symmetries would be an interesting problem, but maybe even more difficult than solving the problem for lsp-operations.

We know that there is at least one lsp-operation (dual) that does not always preserve 3-connectivity for maps, if the face-width is at most two [1], so an obvious question is which other operations do not always preserve 3-connectivity. This was answered for lsp-operations in [24], where the class of such operations, called *edge-breaking operations*, was characterized. Recently, these results have been extended to lopsp-operations. An article with the new results has been submitted [25].

Another problem mentioned in [2] — the generation of lsp-operations for a given inflation factor — has been solved [13]. Such an algorithm not only allows the generation of lsp-operations, but also the generation of polyhedra and other maps with some specific symmetry groups of the embedding. For generating lopsp-operations a program has been written very recently, but it has not been published yet.

ORCID iDs

Gunnar Brinkmann https://orcid.org/0000-0003-4168-0877
Heidi Van den Camp https://orcid.org/0000-0001-7634-3681

References

[1] D. Bokal, G. Brinkmann and C. T. Zamfirescu, The connectivity of the dual, *J. Graph Theory* **101** (2022), 182–209, doi:10.1002/jgt.22819, https://doi.org/10.1002/jgt.22819.

[2] G. Brinkmann, P. Goetschalckx and S. Schein, Comparing the constructions of Goldberg, Fuller, Caspar, Klug and Coxeter, and a general approach to local symmetry-preserving operations, *Proc. R. Soc. Lond., A, Math. Phys. Eng. Sci.* **473** (2017), 14 pp., doi:10.1098/rspa.2017.0267, id/No 20170267, https://doi.org/10.1098/rspa.2017.0267.

[3] R. Bruce King and M. V. Diudea, The chirality of icosahedral fullerenes: a comparison of the tripling (leapfrog), quadrupling (chamfering), and septupling (capra) transformations, *J. Math. Chem.* **39** (2006), 597–604, doi:10.1007/s10910-005-9048-7, https://doi.org/10.1007/s10910-005-9048-7.

[4] D. L. Caspar and A. Klug, Physical principles in the construction of regular viruses, in: *Cold Spring Harbor Symposia on Quantitative Biology*, Cold Spring Harbor Laboratory Press, volume 27, 1962 pp. 1–24, doi:10.1101/sqb.1962.027.001.005, https://doi.org/10.1101/sqb.1962.027.001.005.

[5] H. Coxeter, Virus macromolecules and geodesic domes, *A spectrum of mathematics* (1971), 98–107.

[6] O. Delgado-Friedrichs, Data structures and algorithms for tilings I, *Theor. Comput. Sci.* **303** (2003), 431–445, doi:10.1016/S0304-3975(02)00500-5, https://doi.org/10.1016/S0304-3975(02)00500-5.

[7] A. Dress and G. Brinkmann, Phantasmagorical fulleroids, *MATCH Commun. Math. Comput. Chem.* **33** (1996), 87–100, https://match.pmf.kg.ac.rs/electronic_versions/Match33/match33_87-100.pdf.

[8] A. W. Dress, Regular polytopes and equivariant tessellations from a combinatorial point of view, in: *Algebraic Topology Göttingen 1984*, Springer, pp. 56–72, 1985.

[9] A. W. M. Dress, Presentations of discrete groups, acting on simply connected manifolds, in terms of parametrized systems of Coxeter matrices - a systematic approach, *Adv. Math.* **63** (1987), 196–212, doi:10.1016/0001-8708(87)90053-3, https://doi.org/10.1016/0001-8708(87)90053-3.

[10] A. W. M. Dress and D. Huson, On tilings of the plane, *Geom. Dedicata* **24** (1987), 295–310, doi:10.1007/bf00181602, https://doi.org/10.1007/bf00181602.

[11] F. V. Fomin and D. M. Thilikos, On self duality of pathwidth in polyhedral graph embeddings, *J. Graph Theory* **55** (2007), 42–54, doi:10.1002/jgt.20219, https://doi.org/10.1002/jgt.20219.

[12] M. D. R. Francos, Chamfering operation on k-orbit maps, *Ars Math. Contemp.* **7** (2014), 519–536, doi:10.26493/1855-3974.541.133, https://doi.org/10.26493/1855-3974.541.133.

[13] P. Goetschalckx, K. Coolsaet and N. Van Cleemput, Generation of local symmetry-preserving operations on polyhedra, *Ars Math. Contemp.* **18** (2020), 223–239, doi:10.26493/1855-3974.1931.9cf, https://doi.org/10.26493/1855-3974.1931.9cf.

[14] P. Goetschalckx, K. Coolsaet and N. Van Cleemput, Local orientation-preserving symmetry preserving operations on polyhedra, *Discrete Math.* **344** (2021), 10 pp., doi:10.1016/j.disc.2020.112156, id/No 112156, https://doi.org/10.1016/j.disc.2020.112156.

[15] M. Goldberg, A class of multi-symmetric polyhedra, *Tôhoku Math. J.* **43** (1937), 104–108.

[16] J. L. Gross and T. W. Tucker, *Topological Graph Theory*, Courier Corporation, 2001.

[17] B. Grünbaum, Graphs of polyhedra; polyhedra as graphs, *Discrete Math.* **307** (2007), 445–463, doi:10.1016/j.disc.2005.09.037, https://doi.org/10.1016/j.disc.2005.09.037.

[18] N. W. Johnson, Convex polyhedra with regular faces, *Can. J. Math.* **18** (1966), 169–200, doi:10.4153/cjm-1966-021-8, https://doi.org/10.4153/cjm-1966-021-8.

[19] J. Kovič, T. Pisanski, A. T. Balaban and P. W. Fowler, On symmetries of benzenoid systems, *MATCH Commun. Math. Comput. Chem.* **72** (2014), 3–26.

[20] B. Mohar, Face-width of embedded graphs, *Math. Slovaca* **47** (1997), 35–63.

[21] B. Mohar and C. Thomassen, *Graphs on Surfaces*, volume 16, Johns Hopkins University Press Baltimore, 2001.

[22] A. Orbanić, D. Pellicer and A. Ivić-Weiss, Map operations and k-orbit maps, *J. Comb. Theory, Ser. A* **117** (2010), 411–429, doi:10.1016/j.jcta.2009.09.001, https://doi.org/10.1016/j.jcta.2009.09.001.

[23] T. Pisanski and M. Randic, Bridges between geometry and graph theory, *MAA NOTES* (2000), 174–194.

[24] H. Van den Camp, *The effect of local symmetry-preserving operations on the connectivity of embedded graphs*, Master's thesis, Ghent University, Belgium, 2020.

[25] H. Van den Camp, The effect of symmetry-preserving operations on 3-connectivity, 2023, arXiv:2301.06913 [math.CO].

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 24 (2024) #P2.02 / 187–206
https://doi.org/10.26493/1855-3974.2896.7e6
(Also available at http://amc-journal.eu)

Algebraic degrees of 2-Cayley digraphs over abelian groups*

Yongjiang Wu, Jing Yang, Lihua Feng †

School of Mathematics and Statistics, HNP-LAMA, Central South University, Changsha, Hunan, 410083, P.R. China

Received 3 June 2022, accepted 22 March 2023, published online 8 September 2023

Abstract

A digraph Γ is called a 2-Cayley digraph over a group G if there exists a 2-orbit semiregular subgroup of $\mathrm{Aut}(\Gamma)$ isomorphic to G. In this paper, we completely determine the algebraic degrees of 2-Cayley digraphs over abelian groups. This generalizes the main results of Lu and Mönius in 2023. As applications, we consider the algebraic degrees of Cayley digraphs over finite groups admitting an abelian subgroup of index 2. Special attention is paid to the algebraic degrees of Cayley (di)graphs over generalized dihedral groups, generalized dicyclic groups and semi-dihedral groups.

Keywords: Algebraic degree, 2-Cayley digraph, Abelian group.

Math. Subj. Class. (2020): 05C25, 05C50

1 Introduction

A *digraph* Γ consists of a finite set $V(\Gamma)$ of vertices and a set $E(\Gamma)$ of directed edges, where $E(\Gamma) \subseteq V(\Gamma) \times V(\Gamma)$. If $(u, v) \in E(\Gamma)$ implies $(v, u) \in E(\Gamma)$, then Γ is said to be undirected. For a digraph Γ on n vertices, its *adjacency matrix* $A = (a_{uv})_{n\times n}$ is defined as

$$a_{uv} = \begin{cases} 1, & \text{if } (u, v) \in E(\Gamma), \\ 0, & \text{otherwise.} \end{cases}$$

The characteristic polynomial of Γ is the characteristic polynomial of A. The eigenvalues of A are called the *eigenvalues* of Γ. The collection of eigenvalues of Γ together with their

*This research was supported by NSFC (Nos. 12271527, 12071484), Hunan Provincial Natural Science Foundation (2020JJ4675, 2018JJ2479). The authors would like to express their sincere thanks to the referee for the valuable suggestions which greatly improved the presentation of the original manuscript.

†Corresponding author.

E-mail addresses: su15273815046@163.com (Yongjiang Wu), yj1147943429@163.com (Jing Yang), fenglh@163.com (Lihua Feng)

multiplicities is called the *spectrum* of Γ, denoted by $\mathrm{Spec}(\Gamma)$. Note that A is not always symmetric, so the eigenvalues of Γ need not be real numbers.

Let G be a finite group and $S \subseteq G \setminus \{e\}$, where e is the identity. The *Cayley digraph* $\Gamma = \mathrm{Cay}(G, S)$ of G with respect to S is defined by $V(\Gamma) = G$ and $E(\Gamma) = \{(g, sg) \mid g \in G, s \in S\}$. If $S = S^{-1}$, then $\Gamma = \mathrm{Cay}(G, S)$ is called a *Cayley graph*. For a digraph Γ, the set of all permutations of $V(\Gamma)$ that preserve the adjacency relation of Γ forms a group, called the *automorphism group* of Γ, and is denoted by $\mathrm{Aut}(\Gamma)$. By a theorem of Sabidussi [15], a digraph Γ is a Cayley digraph over G if and only if there exists a regular subgroup of $\mathrm{Aut}(\Gamma)$ isomorphic to G. As a generalization of Sabidussi's Theorem [1], a digraph Γ is called a 2-*Cayley digraph* over G if there exists a 2-orbit semiregular subgroup of $\mathrm{Aut}(\Gamma)$ isomorphic to G. A 2-Cayley graph is also termed as a semi-Cayley graph in [5, 6]. A special 2-Cayley graph is called a bi-Cayley graph in [19].

For a digraph Γ, its *splitting field* $\mathbb{SF}(\Gamma)$ is the smallest field extension of $\mathbb{Q}$ which contains all eigenvalues of the adjacency matrix of Γ. The extension degree $[\mathbb{SF}(\Gamma) : \mathbb{Q}]$ is called the *algebraic degree* of Γ, denoted by $\deg(\Gamma)$. A digraph Γ is called *integral* if all the eigenvalues of the adjacency matrix of Γ are integers. A digraph Γ is called *algebraically integral* over a number field K if all the eigenvalues of the adjacency matrix of Γ are algebraic integers of K. There is a close connection between the splitting field and the algebraic integrality of a digraph. For example, for any number field K, $\mathbb{SF}(\Gamma) \subseteq K$ if and only if Γ is algebraically integral over K. Integral graphs and algebraically integral graphs have been extensively studied in the literature [2, 3, 4, 8, 9, 11]. In recent years, the splitting field and algebraic degree have attracted much attention. In 2020, Mönius [13] studied the algebraic degrees of circulant graphs $\mathrm{Cay}(\mathbb{Z}_p, S)$ for a prime number p. In 2022, Mönius [14] generalized those results in [13] by determining the splitting fields and the algebraic degrees of circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ for arbitrary n. Based on Mönius's work, in 2022, Huang et al. [18] determined the splitting fields and algebraic degrees of mixed Cayley graphs over abelian groups. Lu et al. [12] determined the splitting fields of Cayley graphs over abelian groups and dihedral groups. They also gave bounds for the algebraic degrees of Cayley graphs over dihedral groups. Also in 2022, Sripaisan et al. [16] studied the algebraic degrees of Cayley hypergraphs. For more details, one may refer to the comprehensive survey [10] in this subject.

In this paper, inspired by the above mentioned results, we completely determine the splitting fields and algebraic degrees of 2-Cayley digraphs over abelian groups in Section 3, which generalizes the main results of [12]. From computational viewpoints, we also derive sharp upper and lower bounds for their algebraic degrees. As applications, in Section 4, we consider the algebraic degrees of Cayley digraphs over finite groups admitting an abelian subgroup of index 2. Furthermore, we consider the algebraic degrees of Cayley graphs over generalized dihedral groups and generalized dicyclic groups, and get improved upper bounds. Finally, we determine the algebraic degrees of Cayley digraphs over semi-dihedral groups.

2 Preliminaries

Let G be a finite group. A *representation* of G is a homomorphism $\rho\colon G \to \mathrm{GL}(V)$ for some n-dimensional vector space over the complex field $\mathbb{C}$, where $\mathrm{GL}(V)$ denotes the group of automorphisms of V. The dimension of V is called the *degree* of ρ. Two representations ρ_1 and ρ_2 of G on V_1 and V_2 respectively are *equivalent* if there is an

isomorphism $T\colon V_1 \to V_2$ such that $T\rho_1(g) = \rho_2(g)T$ for all $g \in G$.

Let $\rho\colon G \to GL(V)$ be a representation. The *character* $\chi_\rho\colon G \to \mathbb{C}$ of ρ is defined by setting $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$ for $g \in G$, where $\mathrm{Tr}(\rho(g))$ is the trace of the representation matrix of $\rho(g)$ with respect to a specified basis of V. By the degree of χ_ρ we mean the degree of ρ, which is simply $\chi_\rho(1)$. If W is a $\rho(g)$-invariant subspace of V for each $g \in G$, then we call W a $\rho(G)$-invariant subspace of V. If the only $\rho(G)$-invariant subspace of V are $\{0\}$ and V, we call ρ an *irreducible representation* of G, and the corresponding character χ_ρ an *irreducible character* of G. We denote by $\mathrm{IRR}(G)$ and $\mathrm{Irr}(G)$ the complete set of non-equivalent irreducible representations of G and the complete set of non-equivalent irreducible characters of G, respectively.

For any subset $X \subseteq G$, we denote by $\delta_X = (\delta_g)_{g\in G}$ the characteristic vector of X over G, where $\delta_g = 1$ if $g \in X$ and $\delta_g = 0$ if $g \notin X$. For any multi-subset $X \subseteq G$, we denote by $\delta'_X = \left(\delta'_g\right)_{g\in G}$ the characteristic vector of X over G, where $\delta'_g = k$ if g appears k times in X and $\delta'_g = 0$ if $g \notin X$. Throughout this paper, we use $X = [x \mid x \in X]$ to denote the multi-set X, and $\varphi(n)$ to denote the Euler totient function of a natural number n (it is the number of the positive integers which are smaller than n and coprime to n). Firstly, we state an equivalent definition of 2-Cayley digraphs.

Lemma 2.1 ([1])**.** *A digraph* Γ *is a* 2*-Cayley digraph over* G *if and only if there exist subsets* T_{ij} *of* G*, where* $1 \leqslant i, j \leqslant 2$*, such that* Γ *is isomorphic to a digraph* Υ *with*

$$V(\Upsilon) = G \times \{1, 2\}, \quad E(\Upsilon) = \bigcup_{1\leqslant i,j\leqslant 2} \{((g, i), (tg, j)) \mid g \in G \text{ and } t \in T_{ij}\}.$$

By Lemma 2.1, a 2-Cayley digraph is characterized by a group G and four subsets T_{ij} of G. Thus we denote a 2-Cayley digraph with respect to four subsets T_{ij} by $\Gamma = \mathrm{Cay}\,(G; T_{ij} \mid 1 \leqslant i, j \leqslant 2)$. Note that $V(\Gamma) = G \times \{1, 2\}$, $(g, i) \sim (h, j)$ if and only if $hg^{-1} \in T_{ij}$, and Γ is undirected if and only if for all $1 \leqslant i, j \leqslant 2$, $T_{ij} = T_{ji}^{-1}$. Note also that Γ is a digraph without loops if and only if $T_{ii} \subseteq G\backslash\{e\}$, for all $1 \leqslant i \leqslant 2$.

Let $\omega_n = \exp\left(\frac{2\pi \mathrm{i}}{n}\right)$ be the primitive n-th root of unity. We consider an abelian group G of order n. It is well known that

$$G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r},$$

where $n = \prod_{i=1}^{r} n_i$, and n_i is a prime power for $1 \leq i \leq r$. Without loss of generality, we assume that $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ and $\mathbf{0} = (0, \ldots, 0) \in G$ is the identity of G.

Lemma 2.2 ([17])**.** *Let* $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ *be an abelian group of order* n*. Then* $\mathrm{Irr}(G) = \{\chi_l \mid l \in G\}$*, where* $\chi_l(g) = \prod_{i=1}^{r} \omega_{n_i}^{l_i g_i}$ *for all* $l = (l_1, \ldots, l_r), g = (g_1, \ldots, g_r) \in G$*, and* $\omega_{n_i} = \exp(\frac{2\pi \mathrm{i}}{n_i})$.

For simplicity, for any (multi-)subset S of G, we denote

$$\chi_l(S) = \sum_{s\in S} \chi_l(s).$$

Arezoomand [1] obtained the following result.

Lemma 2.3 ([1])**.** *Let* $\Gamma = \mathrm{Cay}\,(G, T_{ij} \mid 1 \leqslant i, j \leqslant 2)$ *be a* 2*-Cayley digraph over an abelian group* $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ *of order* n*. Then* Γ *has eigenvalues*

$$\frac{\chi_l(T_{11}) + \chi_l(T_{22}) \pm \sqrt{(\chi_l(T_{11}) - \chi_l(T_{22}))^2 + 4\chi_l(T_{21})\chi_l(T_{12})}}{2}, \quad l \in G.$$

Let K be a field. In what follows, we will refer to the subgroup

$$K^{\times 2} = \left\{x^2 : x \in K\right\} \subset K^{\times},$$

where $K^{\times} = K \setminus \{0\}$. More precisely, we shall encounter quite often the quotient $K^{\times}/K^{\times 2}$. The image of $x \in K^{\times}$ in $K^{\times}/K^{\times 2}$ will be denoted by $[x]_K$.

Lemma 2.4 ([7, Corollary 1.23])**.** *Suppose K is a field containing a primitive 2-th root of unity, and let $F = K\left[\sqrt{a_1}, \ldots, \sqrt{a_k}\,\right]$, where $a_i \in K$. Then $\mathrm{Gal}(F/K)$ is isomorphic to the subgroup of $K^{\times}/K^{\times 2}$ generated by $[a_1]_K, \ldots, [a_k]_K$.*

3 2-Cayley digraphs over abelian groups

In this section, we always assume that $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ is an abelian group of order n. Let $\Gamma = \mathrm{Cay}\,(G, T_{ij} \mid 1 \leqslant i, j \leqslant 2)$ be a 2-Cayley digraph over G. For any two subsets X and Y of G, we define the multi-set $X + Y = [x + y \mid x \in X, y \in Y]$. For any (multi-)set X and $k \in \mathbb{N}$, $k * X$ denotes the multi-set in which each element of X appears k times. For example, if $X = [1, 1, 2, 2, 2, 3, 4]$ and $k = 2$, then $k * X = 4 * \{1\} \cup 6 * \{2\} \cup 2 * \{3, 4\}$, with duplicate elements allowed in the union.

For two multi-sets $U = k_1 * \{g_1\} \cup k_2 * \{g_2\} \cup \ldots \cup k_s * \{g_s\}$ and $V = q_1 * \{g_1\} \cup q_2 * \{g_2\} \cup \ldots \cup q_t * \{g_t\} \cup k_{s+1} * \{g_{s+1}\} \cup \ldots \cup k_{s+m} * \{g_{s+m}\}$, where $k_i \geq q_i, s > t$ and $g_i, 1 \leq i \leq s + m$ are pairwise distinct, we define $U \setminus V = (k_1 - q_1) * \{g_1\} \cup (k_2 - q_2) * \{g_2\} \cup \ldots \cup (k_t - q_t) * \{g_t\} \cup k_{t+1} * \{g_{t+1}\} \cup \ldots \cup k_s * \{g_s\}$, $V \setminus U = k_{s+1} * \{g_{s+1}\} \cup \ldots \cup k_{s+m} * \{g_{s+m}\}$.

Using the symbols in Lemma 2.3, we let

$$\begin{aligned} I_1 &= [t \mid t \in T_{11} \text{ or } t \in T_{22}], \\ I_2 &= [t \mid t \in (T_{11} + T_{11}) \text{ or } t \in (T_{22} + T_{22}) \text{ or } t \in 4 * (T_{12} + T_{21})], \\ I_3 &= [t \mid t \in 2 * (T_{11} + T_{22})], \end{aligned}$$

where I_1, I_2 and I_3 are multi-sets. For example, for the group $G = \mathbb{Z}_4$, if $T_{11} = \{1, 2\}$, $T_{12} = \{1\}$, $T_{21} = \{2\}$ and $T_{22} = \{3\}$, then $I_1 = \{1, 2, 3\}$, $I_2 = 6 * \{3\} \cup 2 * \{2\} \cup \{0\}$ and $I_3 = 2 * \{0, 1\}$.

By Lemma 2.3, we have the following result.

Lemma 3.1. *Let $\Gamma = \mathrm{Cay}\,(G, T_{ij} \mid 1 \leqslant i, j \leqslant 2)$ be a 2-Cayley digraph over an abelian group G of order n. Then Γ has eigenvalues*

$$\frac{\chi_l(I_1) \pm \sqrt{\chi_l(I_2 \setminus I_3) - \chi_l(I_3 \setminus I_2)}}{2}, \quad l \in G,$$

where I_1, I_2, I_3 are described as above.

Proof. Firstly, we have

$$\chi_l(T_{11}) + \chi_l(T_{22}) = \chi_l(I_1).$$

In addition,

$$\begin{aligned} &\left(\chi_l(T_{11}) - \chi_l(T_{22})\right)^2 + 4\chi_l(T_{21})\chi_l(T_{12}) \\ =&\chi_l(T_{11} + T_{11}) + \chi_l(T_{22} + T_{22}) + \chi_l\left(4 * (T_{12} + T_{21})\right) - \chi_l\left(2 * (T_{11} + T_{22})\right) \\ =&\chi_l(I_2) - \chi_l(I_3) \\ =&\chi_l(I_2 \setminus I_3) - \chi_l(I_3 \setminus I_2), \end{aligned}$$

so the result follows from Lemma 2.3. □

Using the symbols in Lemma 3.1, for $l \in G$, let

$$\beta_l = \chi_l(I_1) \text{ and } \gamma_l = \chi_l(I_2 \setminus I_3) - \chi_l(I_3 \setminus I_2). \tag{3.1}$$

As $\beta_l, \gamma_l \in \mathbb{Q}(\omega_n)$, where $n = |G|$, without loss of generality, we assume that K is a field such that $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\omega_n)$. Therefore, $\mathrm{Gal}(\mathbb{Q}(\omega_n)/K)) \leq \mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q}) \cong \mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$. Let

$$\eta\colon \mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q}) \to \mathbb{Z}_n^*$$

be the isomorphism such that $\sigma(\omega_n) = \omega_n^{\eta(\sigma)}$, where $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$. Let

$$H = \eta(\mathrm{Gal}(\mathbb{Q}(\omega_n)/K)).$$

Then H is a subgroup of $\mathbb{Z}_n^*$. We consider the action of $\mathbb{Z}_n^*$ on $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ by setting $kg = k(g_1, \ldots, g_r) = (kg_1, \ldots, kg_r)$ for any $k \in \mathbb{Z}_n^*$ and $g \in G$. Then

$$\sigma\left(\omega_{n_i}^{l_i}\right) = \sigma\left(\omega_n^{nl_i/n_i}\right) = \omega_n^{\eta(\sigma)\cdot nl_i/n_i} = \omega_{n_i}^{\eta(\sigma)l_i},$$

where $l_i \in \mathbb{Z}_{n_i} (1 \leq i \leq r)$. Note that for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$, we have

$$\begin{aligned}\sigma(\beta_l) = \sigma(\chi_l(I_1)) &= \sigma\left(\sum_{t\in I_1}\prod_{i=1}^{r}\omega_{n_i}^{l_i t_i}\right) = \sum_{t\in I_1}\prod_{i=1}^{r}\sigma\left(\omega_{n_i}^{l_i t_i}\right)\\ &= \sum_{t\in I_1}\prod_{i=1}^{r}\omega_{n_i}^{\eta(\sigma)l_i t_i} = \chi_l(\eta(\sigma)I_1),\end{aligned}$$

where $\eta(\sigma)I_1 = \{(\eta(\sigma)t_1, \ldots, \eta(\sigma)t_r) \mid (t_1, \ldots, t_r) \in I_1\}$. Similarly, we have

$$\begin{aligned}\sigma(\gamma_l) &= \sigma(\chi_l(I_2 \setminus I_3) - \chi_l(I_3 \setminus I_2))\\ &= \chi_l(\eta(\sigma)(I_2 \setminus I_3)) - \chi_l(\eta(\sigma)(I_3 \setminus I_2)),\end{aligned}$$

where $I_2 \setminus I_3$ and $I_3 \setminus I_2$ are multi-sets as stated in Lemma 3.1.

We first prove the following results.

Proposition 3.2. *For the symbols in* (3.1)*, we have $\beta_l \in K$ for all $l \in G$ if and only if $hI_1 = I_1$ for all $h \in H$, where $H = \eta(\mathrm{Gal}(\mathbb{Q}(\omega_n)/K))$.*

Proof. Assume that $hI_1 = I_1$ for all $h \in H$. Then for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_n)/K)$, we have $\eta(\sigma) \in H$. Thus for any $l \in G$, we have

$$\sigma(\beta_l) = \chi_l(\eta(\sigma)I_1) = \chi_l(I_1) = \beta_l.$$

It follows that $\beta_l \in K$ for all $l \in G$.

Conversely, assume that $\beta_l \in K$ for all $l \in G$. For any $h \in H$, there exists some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_n)/K)$ such that $\eta(\sigma) = h$. Then

$$\chi_l(hI_1) = \chi_l(\eta(\sigma)I_1) = \sigma(\beta_l) = \beta_l = \chi_l(I_1).$$

Let $M = (\chi_l(g))_{l,g\in G}$. We get

$$M\delta'_{hI_1} = M\delta'_{I_1}.$$

Note that M is invertible by the orthogonal relations of irreducible characters of G. So we have

$$\delta'_{hI_1} = \delta'_{I_1}.$$

This implies $hI_1 = I_1$. Since h is arbitrary, the result follows. □

Proposition 3.3. *For the symbols in* (3.1)*, we have $\gamma_l \in K$ for all $l \in G$ if and only if $h(I_2 \setminus I_3) = I_2 \setminus I_3$, $h(I_3 \setminus I_2) = I_3 \setminus I_2$ for all $h \in H$, where $H = \eta(\mathrm{Gal}(\mathbb{Q}(\omega_n)/K))$.*

Proof. Assume that $h(I_2 \setminus I_3) = I_2 \setminus I_3$, $h(I_3 \setminus I_2) = I_3 \setminus I_2$ for all $h \in H$. Then for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_n)/K)$, we have $\eta(\sigma) \in H$. Thus, for any $l \in G$, we have

$$\sigma(\gamma_l) = \chi_l(\eta(\sigma)(I_2 \setminus I_3)) - \chi_l(\eta(\sigma)(I_3 \setminus I_2)) = \chi_l(I_2 \setminus I_3) - \chi_l(I_3 \setminus I_2) = \gamma_l.$$

It follows that $\gamma_l \in K$ for all $l \in G$.

Conversely, assume that $\gamma_l \in K$ for all $l \in G$. For any $h \in H$, there exists some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_n)/K)$ such that $\eta(\sigma) = h$. Then

$$\chi_l(\eta(\sigma)(I_2 \setminus I_3)) - \chi_l(\eta(\sigma)(I_3 \setminus I_2)) = \sigma(\gamma_l) = \gamma_l = \chi_l(I_2 \setminus I_3) - \chi_l(I_3 \setminus I_2).$$

This means that

$$\chi_l(h(I_2 \setminus I_3)) - \chi_l(h(I_3 \setminus I_2)) = \chi_l(I_2 \setminus I_3) - \chi_l(I_3 \setminus I_2).$$

Let $M = (\chi_l(g))_{l,g\in G}$. We get

$$M\delta'_{h(I_2\setminus I_3)} - M\delta'_{h(I_3\setminus I_2)} = M\delta'_{I_2\setminus I_3} - M\delta'_{I_3\setminus I_2}.$$

Note that M is invertible and $I_2 \setminus I_3$ is disjoint with $I_3 \setminus I_2$. So we have $h(I_2 \setminus I_3) = I_2 \setminus I_3$ and $h(I_3 \setminus I_2) = I_3 \setminus I_2$. As h is arbitrary, the result follows. □

Note that $\beta_{\mathbf{0}}, \gamma_{\mathbf{0}} \in \mathbb{Z}$, so we let

$$L = K = \mathbb{Q}(\beta_l, \gamma_l \mid l \in G \setminus \{\mathbf{0}\}) \tag{3.2}$$

and

$$H' = \{h \in \mathbb{Z}_n^* \mid hI_1 = I_1, h(I_2 \setminus I_3) = I_2 \setminus I_3, h(I_3 \setminus I_2) = I_3 \setminus I_2\}. \tag{3.3}$$

Then we have the following result.

Proposition 3.4. *Using the symbols in* (3.2) *and* (3.3)*, we have $H' = \eta(\mathrm{Gal}(\mathbb{Q}(\omega_n)/L))$.*

Proof. By Propositions 3.2 and 3.3, it is clear that

$$\eta(\mathrm{Gal}(\mathbb{Q}(\omega_n)/L)) \subseteq H'.$$

Now we prove

$$H' \subseteq \eta(\mathrm{Gal}(\mathbb{Q}(\omega_n)/L)).$$

For each $h' \in H'$, let $\sigma = \eta^{-1}(h')$. It follows that $h' = \eta(\sigma)$. For any $l \in G$, we have

$$\sigma(\beta_l) = \chi_l(\eta(\sigma)I_1) = \chi_l(h'I_1) = \chi_l(I_1) = \beta_l.$$

Similarly, for any $l \in G$,

$$\sigma(\gamma_l) = \chi_l(\eta(\sigma)(I_2 \setminus I_3)) - \chi_l(\eta(\sigma)(I_3 \setminus I_2)) = \chi_l(I_2 \setminus I_3) - \chi_l(I_3 \setminus I_2) = \gamma_l.$$

Hence

$$\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_n)/L) \text{ and } h' = \eta(\sigma) \in \eta(\mathrm{Gal}(\mathbb{Q}(\omega_n)/L)).$$

Thus the result follows. □

Since H' is a subgroup of $\mathbb{Z}_n^*$, by Proposition 3.4, we have

$$L = \mathbb{Q}(\omega_n)^{\eta^{-1}(H')} = \{x \in \mathbb{Q}(\omega_n) \mid \sigma(x) = x \text{ for all } \sigma \in \eta^{-1}(H')\}. \tag{3.4}$$

Considering H' acting on G, assume that $H'g^{(1)}, H'g^{(2)}, \ldots, H'g^{(k)}$ are all distinct orbits of H' on G, where $g^{(i)} \in G$. Let

$$C = \left\{ g^{(i)} \mid G \cap H'g^{(i)} \neq \emptyset \right\}. \tag{3.5}$$

Let M be the subgroup of $L^\times/L^{\times 2}$ generated by all $[\gamma_l]_L$ for $l \in C$. Explicitly,

$$M = \langle [\gamma_l]_L \mid l \in C \rangle. \tag{3.6}$$

Now we are ready to prove our main result.

Theorem 3.5. *Let $\Gamma = \mathrm{Cay}(G, T_{ij} \mid 1 \leqslant i, j \leqslant 2)$ be a 2-Cayley digraph over an abelian group G of order n. Then the splitting field of Γ is $L\left(\sqrt{\gamma_l} \mid l \in C\right)$ and the algebraic degree of Γ satisfies*

$$\deg(\Gamma) = \frac{\varphi(n)|M|}{|H'|},$$

where γ_l, H', L, C, M are given in (3.1) *and* (3.3) – (3.6)*, respectively.*

Proof. If a, b are in the same orbit $H'g^{(i)}$, then there exists $h \in H'$ such that $b = ha$. It follows that

$$\begin{aligned}\gamma_b &= \chi_b(I_2 \setminus I_3) - \chi_b(I_3 \setminus I_2) = \chi_{ha}(I_2 \setminus I_3) - \chi_{ha}(I_3 \setminus I_2)\\ &= \chi_a(h(I_2 \setminus I_3)) - \chi_a(h(I_3 \setminus I_2)) = \chi_a(I_2 \setminus I_3) - \chi_a(I_3 \setminus I_2)\\ &= \gamma_a.\end{aligned}$$

Therefore, there are at most $|C|$ different elements in $\{\gamma_l \mid l \in G\}$.

Set $F = L\left(\sqrt{\gamma_l} \mid l \in C\right)$. Note that $F = \mathbb{Q}\left(\beta_l + \sqrt{\gamma_l}, \beta_l - \sqrt{\gamma_l} \mid l \in G\right)$. So the first assertion follows. By Lemma 2.4,

$$\deg(\Gamma) = [F : \mathbb{Q}] = [F : L][L : \mathbb{Q}] = \frac{[\mathbb{Q}(\omega_n) : Q][F : L]}{[\mathbb{Q}(\omega_n) : L]} = \frac{\varphi(n)|M|}{|H'|}.$$

This completes the proof. □

It is not easy to calculate $|M|$, but apparently $1 \leq |M| \leq 2^{|C|}$, thus we have

Corollary 3.6. *Let* $\Gamma = \mathrm{Cay}\,(G, T_{ij} \mid 1 \leqslant i, j \leqslant 2)$ *be a* 2*-Cayley digraph over an abelian group* G *of order* n*. Then the algebraic degree of* Γ *satisfies*

$$\frac{\varphi(n)}{|H'|} \leq \deg(\Gamma) \leq \frac{\varphi(n)2^{|C|}}{|H'|},$$

where H', C *are given in* (3.3) *and* (3.5)*, respectively.*

Remark 3.7. Theorem 3.5 and Corollary 3.6 still hold for a 2-Cayley graph. Indeed, we just need to restrict $T_{ij} = T_{ji}^{-1}$ for all $1 \leqslant i, j \leqslant 2$, and modify the associated multi-sets I_1, I_2 and I_3.

The next two examples tell us that both the lower and upper bound in Corollary 3.6 are sharp.

Example 3.8. Let $\Gamma = \mathrm{Cay}\,(\mathbb{Z}_3, T_{ij} \mid 1 \leqslant i, j \leqslant 2)$ be a 2-Cayley graph over $G = \mathbb{Z}_3$. Let $T_{11} = T_{22} = \{1, 2\}$ and $T_{12} = \{1\}$ and $T_{21} = \{2\}$. Then $I_1 = 2 * \{1, 2\}$, $I_2 \setminus I_3 = 4 * \{0\}$ and $I_3 \setminus I_2 = \emptyset$. It follows that $H' = \{1, 2\} = \mathbb{Z}_3^*$, $L = \mathbb{Q}$ and $\gamma_l = 4$ for all $l \in \mathbb{Z}_3$. Thus $|M| = 1$ and $\deg(\Gamma) = \frac{\varphi(3)}{|H'|} = 1$. In fact, $\mathrm{Spec}(\Gamma) = 2 * \{-2, 0\} \cup \{1, 3\}$.

Example 3.9. Let $\Gamma = \mathrm{Cay}\,(\mathbb{Z}_4, T_{ij} \mid 1 \leqslant i, j \leqslant 2)$ be a 2-Cayley digraph over $G = \mathbb{Z}_4$. Let $T_{11} = \{1, 2\}$ and $T_{12} = \{1\}$. Let $T_{21} = \{2\}$ and $T_{22} = \{3\}$. Then $I_1 = \{1, 2, 3\}$, $I_2 \setminus I_3 = 6 * \{3\} \cup 2 * \{2\}$ and $I_3 \setminus I_2 = 2 * \{1\} \cup \{0\}$. It follows that $H' = \{1\}$ and $C = \mathbb{Z}_4$. By Corollary 3.6, $\deg(\Gamma) \leq 2^5 = 32$. In fact, $L = \mathbb{Q}(\mathrm{i})$ and $F = L\left(\sqrt{5}, \sqrt{-8\mathrm{i} - 3}, \sqrt{-3}, \sqrt{8\mathrm{i} - 3}\right)$. Obviously, $\deg(\Gamma) = 32$.

Observe that $L = \mathbb{Q}$ if and only if $|H'| = \varphi(n)$, as an application of Theorem 3.5, the next corollary provides a class of integral 2-Cayley digraphs over abelian groups.

Corollary 3.10. *Let* $\Gamma = \mathrm{Cay}\,(G, T_{ij} \mid 1 \leqslant i, j \leqslant 2)$ *be a* 2*-Cayley digraph over an abelian group* G *of order* n*. If* $H' = \mathbb{Z}_n^*$ *and* γ_l *is a square of an integer for each* $l \in C$*, where* γ_l, H', C *are given in* (3.1)*,* (3.3) *and* (3.5)*, respectively, then* Γ *is integral.*

Sometimes, we need not to compute $|M|$ in Theorem 3.5.

Corollary 3.11. *Let* $\Gamma = \mathrm{Cay}\,(G, T_{ij} \mid 1 \leqslant i, j \leqslant 2)$ *be a* 2*-Cayley digraph over an abelian group* G *of order* n*. If* $T_{11} = T_{22}$ *and* $T_{12} = T_{12}^{-1} = T_{21}$*, then the splitting field of* Γ *satisfies*

$$\mathbb{SF}(\Gamma) = \mathbb{Q}(\omega_n)^{\eta^{-1}(H'')} = \{x \in \mathbb{Q}(\omega_n) \mid \sigma(x) = x \text{ for all } \sigma \in \eta^{-1}(H'')\},$$

the algebraic degree of Γ *satisfies*

$$\deg(\Gamma) = \frac{\varphi(n)}{|H''|},$$

where $H'' = \{h \in \mathbb{Z}_n^* \mid hT_{11} = T_{11}, hT_{12} = T_{12}\}$.

Proof. Since $I_1 = [t \mid t \in 2 * T_{11}]$, $I_2 \setminus I_3 = \left[t \mid t \in 4 * (T_{12} + T_{12}^{-1})\right]$ and $I_3 \setminus I_2 = \emptyset$, we have $\gamma_l = 4\chi_l(T_{12} + T_{12}^{-1}) = 4|\chi_l(T_{12})|^2 = 4\chi_l(T_{12})^2$. Note that $T_{12} = T_{12}^{-1}$. So $\chi_l(T_{12})$ is a real number. It follows that

$$\sqrt{\gamma_l} = 2\chi_l(T_{12}) \text{ or } \sqrt{\gamma_l} = -2\chi_l(T_{12}).$$

The rest of the proof is similar to that of Theorem 3.5. □

Corollary 3.12. *Let* $\Gamma = \mathrm{Cay}\,(G, T_{ij} \mid 1 \leqslant i, j \leqslant 2)$ *be a* 2*-Cayley digraph over an abelian group* G *of order* n*. If* $T_{11} = T_{22}$*,* $T_{12} = T_{12}^{-1} = T_{21}$*, and* $hT_{11} = T_{11}$*,* $hT_{12} = T_{12}$ *for all* $h \in \mathbb{Z}_n^*$*, then* Γ *is integral.*

4 Some applications

4.1 Cayley digraphs over groups admitting an abelian subgroup of index 2

A Cayley digraph over a finite group G with a subgroup of index 2 is a 2-Cayley digraph, as the following result shows.

Lemma 4.1 ([1])**.** *Let* $\Gamma = \mathrm{Cay}(G, S)$ *be a Cayley (di)graph. Suppose that there exists a subgroup* N *of* G *with index* 2*. If* $\{x_1, x_2\}$ *is a left transversal to* N *in* G*, then* $\Gamma \cong \mathrm{Cay}\,(N, S_{ij} \mid 1 \leqslant i, j \leqslant 2)$*, where* $S_{ij} = \{a \in N \mid x_j^{-1} a x_i \in S\} = N \cap x_j S x_i^{-1}$.

Let A be a finite abelian group of order $n \geq 3$. Let $f \in \mathrm{Aut}(A)$ be of order 2. Let $y \in A$ be such that $f(y) = y$. Let G be a non-abelian finite group admitting an abelian subgroup A of index 2. Then G admits a presentation

$$G = \left\langle A, x \mid x^2 = y, xax^{-1} = f(a), a \in A \right\rangle.$$

Observe that $G = A \cup xA$ and $B = \left\{f(a)a^{-1} \mid a \in A\right\}$ is a subgroup of A. In particular, if $f(a) = a^{-1}$ for $a \in A$, then $B = A^2$ and $y^2 = e$, where e is the identity of A. If $y = e$, then G is the generalized dihedral group $\mathrm{Dih}(A)$, with the presentation

$$\mathrm{Dih}(A) = \left\langle A, x \mid x^2 = e, xax^{-1} = a^{-1}, a \in A \right\rangle.$$

If $y \neq e$ (and so $n = |A|$ is even), then G is the generalized dicyclic group $\mathrm{Dic}(A, y)$, with the presentation

$$\mathrm{Dic}(A, y) = \left\langle A, x \mid x^2 = y, xax^{-1} = a^{-1}, a \in A \right\rangle.$$

As the group operation here is multiplication, we assume that $A = \langle a_1 \rangle_{n_1} \otimes \cdots \otimes \langle a_r \rangle_{n_r}$ and $\mathrm{Irr}(A) = \{\chi_l \mid (a_1^{l_1}, \ldots, a_r^{l_r}) \in A\}$, where $l = (l_1, \ldots, l_r)$. In this subsection, we always assume that G is a group admitting an abelian subgroup A of order n and of index 2. As an application of Theorem 3.5, we consider the algebraic degree of the Cayley digraph $\Gamma = \mathrm{Cay}(G, S)$. Note that $A \cong A' = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$. It is worth pointing out that the group operation here should correspond to the addition in Section 3.

By Lemmas 2.3 and 4.1, we get the following result.

Lemma 4.2. *Let* $\Gamma = \mathrm{Cay}(G, S)$ *be a Cayley digraph and* $A = \langle a_1 \rangle_{n_1} \otimes \cdots \otimes \langle a_r \rangle_{n_r}$ *be an abelian subgroup of* G *of order* n *and of index* 2 *with left transversal* $\{x_1, x_2\}$*. Then* Γ *has eigenvalues*

$$\frac{\chi_l(T_{11}) + \chi_l(T_{22}) \pm \sqrt{\left(\chi_l(T_{11}) - \chi_l(T_{22})\right)^2 + 4\chi_l(T_{21})\chi_l(T_{12})}}{2},\ l = (l_1, \ldots, l_r) \in A',$$

where $n = \prod_{i=1}^{r} n_i$, $T_{ij} = \left\{t = (t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in x_j S x_i^{-1}\right\}$ *and* $A' = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$.

Using the symbols in Lemma 4.2, in a similar way as in Section 3, we define

$$\begin{aligned} I_1 &= [t \mid t \in T_{11} \text{ or } t \in T_{22}], \\ I_2 &= [t \mid t \in (T_{11} + T_{11}) \text{ or } t \in (T_{22} + T_{22}) \text{ or } t \in 4 * (T_{12} + T_{21})], \\ I_3 &= [t \mid t \in 2 * (T_{11} + T_{22})]. \end{aligned}$$

Let

$$\beta_l = \chi_l(I_1) \text{ and } \gamma_l = \chi_l(I_2 \setminus I_3) - \chi_l(I_3 \setminus I_2). \tag{4.1}$$

Let $\eta\colon \mathrm{Gal}\left(\mathbb{Q}\left(\omega_n\right)/\mathbb{Q}\right) \to \mathbb{Z}_n^*$ be the isomorphism such that $\sigma\left(\omega_n\right) = \omega_n^{\eta(\sigma)}$, where $\sigma \in \mathrm{Gal}\left(\mathbb{Q}\left(\omega_n\right)/\mathbb{Q}\right)$. Let

$$L = \mathbb{Q}\left(\beta_l, \gamma_l \mid l \in A' \setminus \{\mathbf{0}\}\right) \tag{4.2}$$

and

$$H' = \left\{h \in \mathbb{Z}_n^* \mid hI_1 = I_1, h(I_2 \setminus I_3) = I_2 \setminus I_3, h(I_3 \setminus I_2) = I_3 \setminus I_2\right\}. \tag{4.3}$$

Since $\Gamma \cong \mathrm{Cay}\left(A', T_{ij} \mid 1 \leqslant i, j \leqslant 2\right)$, by Proposition 3.4, we have the following result.

Proposition 4.3. *Using the symbols in* (4.2) *and* (4.3)*, we have* $H' = \eta\left(\mathrm{Gal}\left(\mathbb{Q}\left(\omega_n\right)/L\right)\right)$.

Now we consider H' acting on $A' = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$. Assume that $H'a^{(1)}, H'a^{(2)}, \ldots,$ $H'a^{(k)}$ are all distinct orbits of H' on A', where $a^{(i)} \in A'$. Let

$$C = \left\{a^{(i)} \mid A' \cap H'a^{(i)} \neq \emptyset\right\} \tag{4.4}$$

and

$$M = \left\langle [\gamma_l]_L \mid l \in C \right\rangle. \tag{4.5}$$

Since $\Gamma \cong \mathrm{Cay}\left(A', T_{ij} \mid 1 \leqslant i, j \leqslant 2\right)$, using the conclusions in Section 3, we immediately get the following results.

Theorem 4.4. *Let* $\Gamma = \mathrm{Cay}(G, S)$ *be a Cayley digraph, and* $A = \langle a_1 \rangle_{n_1} \otimes \cdots \otimes \langle a_r \rangle_{n_r}$ *be an abelian subgroup of* G *of order* n *and of index* 2 *with left transversal* $\{x_1, x_2\}$*. Then the splitting field of* Γ *is* $L\left(\sqrt{\gamma_l} \mid l \in C\right)$ *and the algebraic degree of* Γ *satisfies*

$$\deg(\Gamma) = \frac{\varphi(n)|M|}{|H'|},$$

where $L = \mathbb{Q}\left(\omega_n\right)^{\eta^{-1}(H')} = \left\{x \in \mathbb{Q}\left(\omega_n\right) \mid \sigma(x) = x \text{ for all } \sigma \in \eta^{-1}(H')\right\}$ *and* γ_l, H', C, M *are given in* (4.1) *and* (4.3) – (4.5)*, respectively.*

Corollary 4.5. *Let $\Gamma = \mathrm{Cay}(G, S)$ be a Cayley digraph, and $A = \langle a_1\rangle_{n_1} \otimes \cdots \otimes \langle a_r\rangle_{n_r}$ be an abelian subgroup of G of order n and of index 2 with left transversal $\{x_1, x_2\}$. Then the algebraic degree of Γ satisfies*

$$\frac{\varphi(n)}{|H'|} \le \deg(\Gamma) \le \frac{\varphi(n)2^{|C|}}{|H'|},$$

where H', C are given in (4.3) *and* (4.4)*, respectively.*

Corollary 4.6. *Let $\Gamma = \mathrm{Cay}(G, S)$ be a Cayley digraph, and $A = \langle a_1\rangle_{n_1} \otimes \cdots \otimes \langle a_r\rangle_{n_r}$ be an abelian subgroup of G of order n and of index 2 with left transversal $\{x_1, x_2\}$. If $H' = \mathbb{Z}_n^*$ and γ_l is a square of an integer for each $l \in C$, where γ_l, H', C are given in* (4.1)*,* (4.3) *and* (4.4)*, respectively, then Γ is integral.*

Corollary 4.7. *Let $\Gamma = \mathrm{Cay}(G, S)$ be a Cayley digraph, and $A = \langle a_1\rangle_{n_1} \otimes \cdots \otimes \langle a_r\rangle_{n_r}$ be an abelian subgroup of G of order n and of index 2 with left transversal $\{x_1, x_2\}$. Let $T_{ij} = \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in x_j S x_i^{-1}\right\}$. If $T_{11} = T_{22}$ and $T_{12} = T_{12}^{-1} = T_{21}$, then the splitting field of Γ satisfies*

$$\mathbb{SF}(\Gamma) = \mathbb{Q}(\omega_n)^{\eta^{-1}(H'')} = \{x \in \mathbb{Q}(\omega_n) \mid \sigma(x) = x \text{ for all } \sigma \in \eta^{-1}(H'')\},$$

the algebraic degree of Γ satisfies

$$\deg(\Gamma) = \frac{\varphi(n)}{|H''|},$$

where $H'' = \{h \in \mathbb{Z}_n^* \mid hT_{11} = T_{11}, hT_{12} = T_{12}\}$.

Corollary 4.8. *Let $\Gamma = \mathrm{Cay}(G, S)$ be a Cayley digraph, and $A = \langle a_1\rangle_{n_1} \otimes \cdots \otimes \langle a_r\rangle_{n_r}$ be an abelian subgroup of G of order n and of index 2 with left transversal $\{x_1, x_2\}$. Let $T_{ij} = \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in x_j S x_i^{-1}\right\}$. If $T_{11} = T_{22}$, $T_{12} = T_{12}^{-1} = T_{21}$, and $hT_{11} = T_{11}$, $hT_{12} = T_{12}$ for all $h \in \mathbb{Z}_n^*$, then Γ is integral.*

4.2 Cayley graphs over generalized dihedral groups

In the following two subsections, we consider *Cayley graphs* but not digraphs. The generalized dihedral group $\mathrm{Dih}(A)$ is given by the following presentation

$$\mathrm{Dih}(A) = \left\langle A, x \mid x^2 = e, xax^{-1} = a^{-1}, a \in A\right\rangle.$$

Let $\Gamma = \mathrm{Cay}(\mathrm{Dih}(A), S)$ be a Cayley digraph. Using the symbols in Subsection 4.1, note that $A = \langle a_1\rangle_{n_1} \otimes \cdots \otimes \langle a_r\rangle_{n_r}$, and $|A| = n$, so $|\mathrm{Dih}(A)| = 2n$. Without loss of generality, let $x_1 = e$ and $x_2 = x$. Then

$$\begin{aligned}
T_{11} &= \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in S\right\},\\
T_{12} &= \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in xS\right\},\\
T_{21} &= \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in Sx\right\},\\
T_{22} &= \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in xSx\right\}.
\end{aligned} \tag{4.6}$$

For the algebraic degree of the digraph Γ, we just need to replace T_{ij} given in Subsection 4.1 with T_{ij} given in (4.6), so we omit the details here.

We are now interested in the algebraic degree of the undirected Cayley graph $\Gamma = \mathrm{Cay}(\mathrm{Dih}(A), S)$. Using the symbols in (4.6), as $S = S^{-1}$, we have $T_{22}^{-1} = T_{22} = T_{11} = T_{11}^{-1}$ and $T_{12}^{-1} = T_{21}$. Let $t = (t_1, \ldots, t_r)$. In a similar way as in Subsection 4.1, we define

$$\begin{aligned} I_1 &= [t \mid t \in T_{11} \text{ or } t \in T_{22}], \\ I_2 &= [t \mid t \in (T_{11} + T_{11}) \text{ or } t \in (T_{22} + T_{22}) \text{ or } t \in 4 * (T_{12} + T_{21})], \\ I_3 &= [t \mid t \in 2 * (T_{11} + T_{22})]. \end{aligned}$$

It follows that $I_1 = [t \mid t \in 2 * T_{11}]$, $I_2 \setminus I_3 = \left[t \mid t \in 4 * (T_{12} + T_{12}^{-1})\right]$ and $I_3 \setminus I_2 = \emptyset$. In fact, by Lemma 4.2, the eigenvalues of the Cayley graph $\Gamma = \mathrm{Cay}(\mathrm{Dih}(A), S)$ are

$$\chi_l(T_{11}) \pm |\chi_l(T_{12})|, \ l \in A',$$

where $A' = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$. Note that $|\chi_l(T_{12})| = \sqrt{\chi_l(T_{12})\chi_l(T_{12}^{-1})} = \sqrt{\chi_l(T_{12} + T_{12}^{-1})}$, the multi-sets I_1 and $I_2 \setminus I_3$ can be reduced to $I_1' = T_{11}$ and $(I_2 \setminus I_3)' = \left[t \mid t \in T_{12} + T_{12}^{-1}\right]$.

Let

$$\beta_l = \chi_l(I_1') \text{ and } \gamma_l = \chi_l((I_2 \setminus I_3)'). \tag{4.7}$$

Let $\eta\colon \mathrm{Gal}\left(\mathbb{Q}\left(\omega_n\right)/\mathbb{Q}\right) \to \mathbb{Z}_n^*$ be the isomorphism such that $\sigma\left(\omega_n\right) = \omega_n^{\eta(\sigma)}$, where $\sigma \in \mathrm{Gal}\left(\mathbb{Q}\left(\omega_n\right)/\mathbb{Q}\right)$. Let

$$L = \mathbb{Q}\left(\beta_l, \gamma_l \mid l \in A' \setminus \{\mathbf{0}\}\right) \tag{4.8}$$

and

$$H' = \{h \in \mathbb{Z}_n^* \mid hI_1' = I_1', h(I_2 \setminus I_3)' = (I_2 \setminus I_3)'\}. \tag{4.9}$$

Note that $I_1 = 2 * I_1'$ and $I_2 \setminus I_3 = 4 * (I_2 \setminus I_3)'$. So we have the following result by Proposition 4.3.

Proposition 4.9. *Using the symbols in* (4.8) *and* (4.9)*, we have* $H' = \eta\left(\mathrm{Gal}\left(\mathbb{Q}\left(\omega_n\right)/L\right)\right)$.

Similarly, we consider H' acting on A'. Assume that $H'a^{(1)}, H'a^{(2)}, \ldots H'a^{(k)}$ are all distinct orbits of H' on A', where $a^{(i)} \in A'$. Let $B = \{x \in A' \mid 2x = \mathbf{0}\}$ and $A' = B \cup E \cup E^{-1}$, where B, E, E^{-1} are disjoint. Let

$$C' = \left\{a^{(i)} \mid (B \cup E) \cap H'a^{(i)} \neq \emptyset\right\} \tag{4.10}$$

and

$$M = \langle [\gamma_l]_L \mid l \in C' \rangle. \tag{4.11}$$

Then the following results hold.

Theorem 4.10. *Let* $\Gamma = \mathrm{Cay}(\mathrm{Dih}(A), S)$ *be a Cayley graph over the generalized dihedral group* $\mathrm{Dih}(A)$ *of order* $2n$*. Then the splitting field of* Γ *is* $L\left(\sqrt{\gamma_l} \mid l \in C'\right)$ *and the algebraic degree of* Γ *satisfies*

$$\deg(\Gamma) = \frac{\varphi(n)|M|}{|H'|},$$

where $L = \mathbb{Q}(\omega_n)^{\eta^{-1}(H')} = \{x \in \mathbb{Q}(\omega_n) \mid \sigma(x) = x \text{ for all } \sigma \in \eta^{-1}(H')\}$ *and* γ_l, H', C', M *are given in* (4.7) *and* (4.9) – (4.11)*, respectively.*

Proof. Since $((I_2 \setminus I_3)')^{-1} = (I_2 \setminus I_3)'$, it follows that

$$\gamma_l = \chi_l((I_2 \setminus I_3)') = \chi_l(((I_2 \setminus I_3)')^{-1}) = \chi_{-l}((I_2 \setminus I_3)') = \gamma_{-l}.$$

Then the result follows from Theorem 4.4. □

Corollary 4.11. *Let* $\Gamma = \mathrm{Cay}(\mathrm{Dih}(A), S)$ *be a Cayley graph over the generalized dihedral group* $\mathrm{Dih}(A)$ *of order* $2n$*. Then the algebraic degree of* Γ *satisfies*

$$\frac{\varphi(n)}{|H'|} \le \deg(\Gamma) \le \frac{\varphi(n)2^{|C'|}}{|H'|},$$

where H', C' *are given in* (4.9) *and* (4.10)*, respectively.*

Corollary 4.12. *Let* $\Gamma = \mathrm{Cay}(\mathrm{Dih}(A), S)$ *be a Cayley graph over the generalized dihedral group* $\mathrm{Dih}(A)$ *of order* $2n$*. If* $H' = \mathbb{Z}_n^*$ *and* γ_l *is a square of an integer for each* $l \in C'$*, where* γ_l, H', C' *are given in* (4.7)*,* (4.9) *and* (4.10)*, respectively, then* Γ *is integral.*

Corollary 4.13. *Let* $\Gamma = \mathrm{Cay}(\mathrm{Dih}(A), S)$ *be a Cayley graph over the generalized dihedral group* $\mathrm{Dih}(A)$ *of order* $2n$*. Let*

$$T_{11} = \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in S\right\} \text{ and } T_{12} = \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in xS\right\}.$$

If $T_{12} = T_{12}^{-1}$*, then the splitting field of* Γ *satisfies*

$$\mathbb{SF}(\Gamma) = \mathbb{Q}(\omega_n)^{\eta^{-1}(H'')} = \{x \in \mathbb{Q}(\omega_n) \mid \sigma(x) = x \text{ for all } \sigma \in \eta^{-1}(H'')\},$$

the algebraic degree of Γ *satisfies*

$$\deg(\Gamma) = \frac{\varphi(n)}{|H''|},$$

where $H'' = \{h \in \mathbb{Z}_n^* \mid hT_{11} = T_{11}, hT_{12} = T_{12}\}$.

Corollary 4.14. *Let* $\Gamma = \mathrm{Cay}(\mathrm{Dih}(A), S)$ *be a Cayley graph over the generalized dihedral group* $\mathrm{Dih}(A)$ *of order* $2n$*. Let*

$$T_{11} = \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in S\right\} \text{ and } T_{12} = \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in xS\right\}.$$

If $T_{12} = T_{12}^{-1}$ *and for all* $h \in \mathbb{Z}_n^*$*,* $hT_{11} = T_{11}$ *and* $hT_{12} = T_{12}$*, then* Γ *is integral.*

In particular, let $\mathrm{Dih}(A) = D_{2n} = \langle a, b \mid a^n = b^2 = e, bab = a^{-1}\rangle$ be the dihedral group of order $2n$. Then $A' = \mathbb{Z}_n$, $I_1' = T_{11} = \{t \mid a^t \in S\}$, $T_{12} = \{t \mid ba^t \in S\}$ and $(I_2 \setminus I_3)' = \left[t \mid t \in T_{12} + T_{12}^{-1}\right]$. Note that

$$\beta_l = \chi_l(I_1') \text{ and } \gamma_l = \chi_l((I_2 \setminus I_3)'), \tag{4.12}$$

where $\chi_l(t) = \omega_n^{lt}$ and $0 \le l \le n-1$. Furthermore,

$$L = \mathbb{Q}(\beta_l, \gamma_l \mid 1 \le l \le n-1).$$

We first try to simplify the expression of L.

Lemma 4.15. *Let K be a field such that $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\omega_n)$. If $\beta_1, \gamma_1 \in K$, then $\beta_l, \gamma_l \in K$ for $1 \leq l \leq n-1$.*

Proof. For $1 \leq l \leq n-1$, let $\sigma_l : \mathbb{Q}(\omega_n) \to \mathbb{Q}(\omega_n)$ be defined by $\sigma_l(\omega_n) = \omega_n^l$. It is clear that σ_l is a homomorphism and $\beta_l = \sigma_l(\beta_1), \gamma_l = \sigma_l(\gamma_1)$. Thus, for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_n)/K)$, we have

$$\sigma(\beta_l) = \sigma(\sigma_l(\beta_1)) = \sigma\left(\sigma_l\left(\sum_{t\in I_1'} \omega_n^t\right)\right) = \sum_{t\in I_1'} \omega_n^{\eta(\sigma)tl} = \sigma_l(\sigma(\beta_1)) = \sigma_l(\beta_1) = \beta_l.$$

Similarly, $\sigma(\gamma_l) = \gamma_l$. Therefore, $\beta_l, \gamma_l \in K$. □

By Lemma 4.15, we have

$$L = \mathbb{Q}(\beta_1, \gamma_1).$$

Let

$$H' = \{h \in \mathbb{Z}_n^* \mid hI_1' = I_1', h(I_2 \setminus I_3)' = (I_2 \setminus I_3)'\}. \tag{4.13}$$

Then $H' = \eta(\mathrm{Gal}(\mathbb{Q}(\omega_n)/L))$. Note that

$$C' = \left\{a^{(i)} \mid \{0, 1, \ldots, \lfloor n/2 \rfloor\} \cap H'a^{(i)} \neq \emptyset\right\} \tag{4.14}$$

and

$$M = \langle [\gamma_l]_L \mid l \in C' \rangle, \tag{4.15}$$

where $H'a^{(1)}, H'a^{(2)}, \ldots H'a^{(k)}$ are all distinct orbits of H' on $\mathbb{Z}_n$. Consequently, we have the following corollaries.

Corollary 4.16. *Let $\Gamma = \mathrm{Cay}(D_{2n}, S)$ be a Cayley graph over the dihedral group D_{2n}. Then the splitting field of Γ is $L\left(\sqrt{\gamma_l} \mid l \in C'\right)$ and the algebraic degree of Γ satisfies*

$$\deg(\Gamma) = \frac{\varphi(n)|M|}{|H'|},$$

where $L = \mathbb{Q}(\omega_n)^{\eta^{-1}(H')} = \{x \in \mathbb{Q}(\omega_n) \mid \sigma(x) = x \text{ for all } \sigma \in \eta^{-1}(H')\}$ and γ_l, H', C', M are given in (4.12) – (4.15)*, respectively.*

Corollary 4.17. *Let $\Gamma = \mathrm{Cay}(D_{2n}, S)$ be a Cayley graph over the dihedral group D_{2n}. Then the algebraic degree of Γ satisfies*

$$\frac{\varphi(n)}{|H'|} \leq \deg(\Gamma) \leq \frac{\varphi(n)2^{|C'|}}{|H'|},$$

where H', C' are given in (4.13) *and* (4.14)*, respectively.*

Corollary 4.18. *Let $\Gamma = \mathrm{Cay}(D_{2n}, S)$ be a Cayley graph over the dihedral group D_{2n}. Let $T_{11} = \{t \mid a^t \in S\}$ and $T_{12} = \{t \mid ba^t \in S\}$. If $T_{12} = T_{12}^{-1}$, then the splitting field of Γ satisfies*

$$\mathbb{SF}(\Gamma) = \mathbb{Q}(\omega_n)^{\eta^{-1}(H'')} = \{x \in \mathbb{Q}(\omega_n) \mid \sigma(x) = x \text{ for all } \sigma \in \eta^{-1}(H'')\},$$

the algebraic degree of Γ *satisfies*

$$\deg(\Gamma) = \frac{\varphi(n)}{|H''|},$$

where $H'' = \{h \in \mathbb{Z}_n^* \mid hT_{11} = T_{11}, hT_{12} = T_{12}\}$.

There are results similar to Corollaries 4.12 and 4.14 as well, we omit them here. We end this subsection with the following example.

Example 4.19. Let $D_{16} = \langle a, b \mid a^8 = b^2 = e, bab = a^{-1}\rangle$ be the dihedral group of order 16 and $S = \{a, a^7, b\}$. We consider the algebraic degree of $\Gamma = \mathrm{Cay}(D_{16}, S)$. Then $T_{11} = \{1, -1\}$ and $T_{12} = \{0\} = T_{12}^{-1}$. It follows that $H'' = \{1, -1\} \leq \mathbb{Z}_8^*$. By Corollary 4.18, $\mathbb{SF}(\Gamma) = \mathbb{Q}\left(\omega_8\right)^{\eta^{-1}(H'')} = \mathbb{Q}(\sqrt{2})$ and $\deg(\Gamma) = \frac{\varphi(8)}{|H''|}$=2. In fact,

$$\mathrm{Spec}(\Gamma) = 2 * \{\sqrt{2}+1, \sqrt{2}-1, -\sqrt{2}+1, -\sqrt{2}-1\} \cup 3 * \{1, -1\} \cup \{-3, 3\}.$$

4.3 Cayley graphs over generalized dicyclic groups

For the generalized dicyclic group $\mathrm{Dic}(A, y)$, it has the following presentation

$$\mathrm{Dic}(A, y) = \left\langle A, x \mid x^2 = y, xax^{-1} = a^{-1}, a \in A\right\rangle.$$

We put our focus on the algebraic degree of the *Cayley graph* $\Gamma = \mathrm{Cay}(\mathrm{Dic}(A, y), S)$. Using the symbols in Subsection 4.1, since $A = \langle a_1\rangle_{n_1} \otimes \cdots \otimes \langle a_r\rangle_{n_r}$, and $|A| = n$ is even, say $n = 2m$, then $|\mathrm{Dic}(A, y)| = 4m$. Let $x_1 = e$ and $x_2 = x$. Then

$$\begin{aligned}
T_{11} &= \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in S\right\},\\
T_{12} &= \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in xS\right\},\\
T_{21} &= \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in Sx^{-1}\right\},\\
T_{22} &= \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in xSx^{-1}\right\}.
\end{aligned}$$

Since $S = S^{-1}$, we have $T_{22}^{-1} = T_{22} = T_{11} = T_{11}^{-1}$ and $T_{12}^{-1} = T_{21}$. Let $t = (t_1, \ldots, t_r)$. By similar arguments as those in Subsection 4.2, we just need to consider $I_1' = T_{11}$ and $(I_2 \setminus I_3)' = \left[t \mid t \in T_{12} + T_{12}^{-1}\right]$. Let

$$\beta_l = \chi_l(I_1') \text{ and } \gamma_l = \chi_l((I_2 \setminus I_3)'). \tag{4.16}$$

Let $\eta\colon\ \mathrm{Gal}\left(\mathbb{Q}\left(\omega_{2m}\right)/\mathbb{Q}\right) \to \mathbb{Z}_{2m}^*$ be the isomorphism such that $\sigma\left(\omega_{2m}\right) = \omega_{2m}^{\eta(\sigma)}$, where $\sigma \in \mathrm{Gal}\left(\mathbb{Q}\left(\omega_{2m}\right)/\mathbb{Q}\right)$.

Let $L = \mathbb{Q}\left(\beta_l, \gamma_l \mid l \in A' \setminus \{\mathbf{0}\}\right)$ and

$$H' = \{h \in \mathbb{Z}_{2m}^* \mid hI_1' = I_1', h(I_2 \setminus I_3)' = (I_2 \setminus I_3)'\}. \tag{4.17}$$

By Proposition 4.3, we have $H' = \eta\left(\mathrm{Gal}\left(\mathbb{Q}\left(\omega_{2m}\right)/L\right)\right)$.

Also, we consider H' acting on $A' = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$. Assume that $H'a^{(1)}, H'a^{(2)}, \ldots$ $H'a^{(k)}$ are all distinct orbits of H' on A', where $a^{(i)} \in A'$. Let $B = \{x \in A' \mid 2x = \mathbf{0}\}$ and $A' = B \cup E \cup E^{-1}$, where B, E, E^{-1} are disjoint. Let

$$C' = \left\{a^{(i)} \mid (B \cup E) \cap H'a^{(i)} \neq \emptyset\right\} \tag{4.18}$$

and

$$M = \langle [\gamma_l]_L \mid l \in C' \rangle . \tag{4.19}$$

In a similar way as in Theorem 4.10, we get the following result.

Theorem 4.20. *Let $\Gamma = \mathrm{Cay}(\mathrm{Dic}(A, y), S)$ be a Cayley graph over $\mathrm{Dic}(A, y)$ of order $4m$. Then the splitting field of Γ is $L\left(\sqrt{\gamma_l} \mid l \in C'\right)$, and the algebraic degree of Γ satisfies*

$$\deg(\Gamma) = \frac{\varphi(2m)|M|}{|H'|},$$

where $L = \mathbb{Q}\left(\omega_{2m}\right)^{\eta^{-1}(H')} = \{x \in \mathbb{Q}\left(\omega_{2m}\right) \mid \sigma(x) = x \text{ for all } \sigma \in \eta^{-1}(H')\}$ and γ_l, H', C', M are given in (4.16) – (4.19)*, respectively.*

Corollary 4.21. *Let $\Gamma = \mathrm{Cay}(\mathrm{Dic}(A, y), S)$ be a Cayley graph over $\mathrm{Dic}(A, y)$ of order $4m$. Then the algebraic degree of Γ satisfies*

$$\frac{\varphi(2m)}{|H'|} \leq \deg(\Gamma) \leq \frac{\varphi(2m)2^{|C'|}}{|H'|},$$

where H', C' are given in (4.17) *and* (4.18)*, respectively.*

Corollary 4.22. *Let $\Gamma = \mathrm{Cay}(\mathrm{Dic}(A, y), S)$ be a Cayley graph over $\mathrm{Dic}(A, y)$ of order $4m$. If $H' = \mathbb{Z}_{2m}^*$ and γ_l is a square of an integer for each $l \in C'$, where γ_l, H', C' are given in* (4.16) – (4.18)*, respectively, then Γ is integral.*

Corollary 4.23. *Let $\Gamma = \mathrm{Cay}(\mathrm{Dic}(A, y), S)$ be a Cayley graph over $\mathrm{Dic}(A, y)$ of order $4m$. Let*

$$T_{11} = \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in S\right\} \text{ and } T_{12} = \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in xS\right\}.$$

If $T_{12} = T_{12}^{-1}$, then the splitting field of Γ satisfies

$$\mathbb{SF}(\Gamma) = \mathbb{Q}\left(\omega_{2m}\right)^{\eta^{-1}(H'')} = \{x \in \mathbb{Q}\left(\omega_{2m}\right) \mid \sigma(x) = x \text{ for all } \sigma \in \eta^{-1}(H'')\},$$

the algebraic degree of Γ satisfies

$$\deg(\Gamma) = \frac{\varphi(2m)}{|H''|},$$

where $H'' = \{h \in \mathbb{Z}_{2m}^* \mid hT_{11} = T_{11}, hT_{12} = T_{12}\}$.

Corollary 4.24. *Let $\Gamma = \mathrm{Cay}(\mathrm{Dic}(A, y), S)$ be a Cayley graph over $\mathrm{Dic}(A, y)$ of order $4m$. Let*

$$T_{11} = \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in S\right\} \text{ and } T_{12} = \left\{(t_1, \ldots, t_r) \mid \left(a_1^{t_1}, \ldots, a_r^{t_r}\right) \in xS\right\}.$$

If $T_{12} = T_{12}^{-1}$ and for all $h \in \mathbb{Z}_{2m}^*$, $hT_{11} = T_{11}$ and $hT_{12} = T_{12}$, then Γ is integral.

Furthermore, for the dicyclic group $\mathrm{Dic}_{4m} = \left\langle a, b \mid a^{2m} = e, a^m = b^2, b^{-1}ab = a^{-1} \right\rangle$, as direct consequences of Theorem 4.20 and Corollaries 4.21 – 4.24, we have similar results, so we omit the details here.

Example 4.25. Let $\mathrm{Dic}_{12} = \langle a, b \mid a^6 = e, a^3 = b^2, b^{-1}ab = a^{-1} \rangle$ be the dicyclic group of order 12 and $S = \left\{a, a^5, ab, a^2b, a^4b, a^5b\right\}$. We consider the algebraic degree of $\Gamma = \mathrm{Cay}(\mathrm{Dic}_{12}, S)$. Then $T_{11} = \{1, 5\}$ and $T_{12} = \{1, 2, 4, 5\} = T_{12}^{-1}$. It follows that $H'' = \{1, 5\} = \mathbb{Z}_6^*$. By Corollary 4.24, $\deg(\Gamma) = 1$. In fact, $\mathrm{Spec}(\Gamma) = 4 * \{-1, 1\} \cup 3 * \{-2\} \cup \{6\}$.

4.4 Cayley digraphs over semi-dihedral groups

For the semi-dihedral group SD_{8m}, it has the following presentation

$$\mathrm{SD}_{8m} = \langle a, b \mid a^{4m} = b^2 = e, bab = a^{2m-1} \rangle.$$

We now consider the algebraic degree of the *Cayley digraph* $\Gamma = \mathrm{Cay}(\mathrm{SD}_{8m}, S)$. Using the symbols in Subsection 4.1, it follows that $A = \langle a \rangle_{4m}$ and $A' = \mathbb{Z}_{4m}$. Let $x_1 = e$ and $x_2 = b$. Then

$$\begin{aligned} T_{11} &= \left\{ t \mid a^t \in S \right\}, \\ T_{12} &= \left\{ t \mid ba^t \in S \right\}, \\ T_{21} &= \left\{ t \mid a^t b \in S \right\}, \\ T_{22} &= \left\{ t \mid a^{(2m-1)t} \in S \right\}. \end{aligned}$$

In a similar way as in Subsection 4.1, we define

$$\begin{aligned} I_1 &= [t \mid t \in T_{11} \text{ or } t \in T_{22}], \\ I_2 &= [t \mid t \in (T_{11} + T_{11}) \text{ or } t \in (T_{22} + T_{22}) \text{ or } t \in 4 * (T_{12} + T_{21})], \\ I_3 &= [t \mid t \in 2 * (T_{11} + T_{22})]. \end{aligned}$$

Let

$$\beta_l = \chi_l(I_1) \text{ and } \gamma_l = \chi_l(I_2 \setminus I_3) - \chi_l(I_3 \setminus I_2), \tag{4.20}$$

where $\chi_l(t) = \omega_{4m}^{lt}$ and $0 \le l \le 4m-1$. Let K be a field such that $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\omega_{4m})$. Then $\mathrm{Gal}(\mathbb{Q}(\omega_{4m})/K)) \le \mathrm{Gal}(\mathbb{Q}(\omega_{4m})/\mathbb{Q}) \cong \mathbb{Z}_{4m}^*$. Let $\eta\colon \mathrm{Gal}(\mathbb{Q}(\omega_{4m})/\mathbb{Q}) \to \mathbb{Z}_{4m}^*$ be the isomorphism such that $\sigma(\omega_{4m}) = \omega_{4m}^{\eta(\sigma)}$, where $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_{4m})/\mathbb{Q})$. Let

$$L = \mathbb{Q}(\beta_l, \gamma_l \mid 1 \le l \le 4m-1).$$

The following lemma helps to simplify the expression of L.

Lemma 4.26. *If* $\beta_1, \gamma_1 \in K$*, then* $\beta_l, \gamma_l \in K$ *for* $1 \le l \le 4m-1$.

Proof. The proof is similar to that of Lemma 4.15. □

By Lemma 4.26, we have

$$L = \mathbb{Q}(\beta_1, \gamma_1).$$

Let

$$H' = \{h \in \mathbb{Z}_{4m}^* \mid hI_1 = I_1, h(I_2 \setminus I_3) = I_2 \setminus I_3, h(I_3 \setminus I_2) = I_3 \setminus I_2\}. \tag{4.21}$$

By Proposition 4.3, we have $H' = \eta(\mathrm{Gal}(\mathbb{Q}(\omega_{4m})/L))$.

Assume that $H'a^{(1)}, H'a^{(2)}, \ldots H'a^{(k)}$ are all distinct orbits of H' on $\mathbb{Z}_{4m}$. Let

$$C = \{a^{(i)} \mid \mathbb{Z}_{4m} \cap H'a^{(i)} \ne \emptyset\} \tag{4.22}$$

and

$$M = \langle [\gamma_l]_L \mid l \in C \rangle. \tag{4.23}$$

By Theorem 4.4 and Corollaries 4.5 – 4.8, we have

Theorem 4.27. *Let $\Gamma = \mathrm{Cay}(\mathrm{SD}_{8m}, S)$ be a Cayley digraph over the semi-dihedral group SD_{8m}. Then the splitting field of Γ is $L\left(\sqrt{\gamma_l} \mid l \in C\right)$ and the algebraic degree of Γ satisfies*

$$\deg(\Gamma) = \frac{\varphi(4m)|M|}{|H'|},$$

where $L = \mathbb{Q}\left(\omega_{4m}\right)^{\eta^{-1}(H')} = \{x \in \mathbb{Q}\left(\omega_{4m}\right) \mid \sigma(x) = x \text{ for all } \sigma \in \eta^{-1}(H')\}$ and γ_l, H', C, M are given in (4.20) – (4.23)*, respectively.*

Corollary 4.28. *Let $\Gamma = \mathrm{Cay}(\mathrm{SD}_{8m}, S)$ be a Cayley digraph over the semi-dihedral group SD_{8m}. Then the algebraic degree of Γ satisfies*

$$\frac{\varphi(4m)}{|H'|} \leq \deg(\Gamma) \leq \frac{\varphi(4m)2^{|C|}}{|H'|},$$

where H', C are given in (4.21) *and* (4.22)*, respectively.*

Corollary 4.29. *Let $\Gamma = \mathrm{Cay}(\mathrm{SD}_{8m}, S)$ be a Cayley digraph over the semi-dihedral group SD_{8m}. If $H' = \mathbb{Z}_{4m}^*$ and γ_l is a square of an integer for each $l \in C$, where γ_l, H', C are given in* (4.20) – (4.22)*, respectively, then Γ is integral.*

Corollary 4.30. *Let $\Gamma = \mathrm{Cay}(\mathrm{SD}_{8m}, S)$ be a Cayley digraph over the semi-dihedral group SD_{8m}. If $T_{11} = T_{22}$ and $T_{12} = T_{12}^{-1} = T_{21}$, then the splitting field of Γ satisfies*

$$\mathbb{SF}(\Gamma) = \mathbb{Q}\left(\omega_{4m}\right)^{\eta^{-1}(H'')} = \{x \in \mathbb{Q}\left(\omega_{4m}\right) \mid \sigma(x) = x \text{ for all } \sigma \in \eta^{-1}(H'')\},$$

the algebraic degree of Γ satisfies

$$\deg(\Gamma) = \frac{\varphi(4m)}{|H''|},$$

where $H'' = \{h \in \mathbb{Z}_{4m}^* \mid hT_{11} = T_{11}, hT_{12} = T_{12}\}$.

Corollary 4.31. *Let $\Gamma = \mathrm{Cay}(\mathrm{SD}_{8m}, S)$ be a Cayley digraph over the semi-dihedral group SD_{8m}. If $T_{11} = T_{22}$, $T_{12} = T_{12}^{-1} = T_{21}$ and for all $h \in \mathbb{Z}_{4m}^*$, $hT_{11} = T_{11}$ and $hT_{12} = T_{12}$, then Γ is integral.*

We end this paper with the following example.

Example 4.32. Let $\mathrm{SD}_{16} = \langle a, b \mid a^8 = b^2 = e, b^{-1}ab = a^3\rangle$ be the semi-dihedral group of order 16 and $S = \left\{a^2, a^6, ba, ba^5\right\}$. We consider the algebraic degree of $\Gamma = \mathrm{Cay}(\mathrm{SD}_{16}, S)$. Then $T_{11} = T_{22} = \{2, 6\}$ and $T_{12} = \{1, 5\}, T_{12}^{-1} = T_{21} = \{3, 7\}$. Thus, $I_1 = 2 * \{2, 6\}$, $I_2 \setminus I_3 = 8 * \{0, 4\}$ and $I_3 \setminus I_2 = \emptyset$. It follows that $H' = \{1, 3, 5, 7\} = \mathbb{Z}_8^*$. Since $\gamma_1 = 8[1 + (-1)^l]$ is a square of integer for each $l \in \mathbb{Z}_8$, by Corollary 4.29, $\deg(\Gamma) = 1$. In fact, $\mathrm{Spec}(\Gamma) = 10 * \{0\} \cup 2 * \{-2, 1, 4\}$.

ORCID iDs

Lihua Feng https://orcid.org/0000-0003-4144-1649

References

[1] M. Arezoomand and B. Taeri, On the characteristic polynomial of n-Cayley digraphs, *Electron. J. Comb.* **20** (2013), research paper p57, 14, doi:10.37236/3105, https://doi.org/10.37236/3105.

[2] A. Behajaina and F. Legrand, On integral mixed cayley graphs over non-abelian finite groups admitting an abelian subgroup of index 2, 2022, arXiv:2203.08793 [math.CO].

[3] T. Cheng, L. Feng and H. Huang, Integral Cayley graphs over dicyclic group, *Linear Algebra Appl.* **566** (2019), 121–137, doi:10.1016/j.laa.2019.01.002, https://doi.org/10.1016/j.laa.2019.01.002.

[4] T. Cheng, L. Feng, W. Liu, L. Lu and D. Stevanović, Distance powers of integral Cayley graphs over dihedral groups and dicyclic groups, *Linear Multilinear Algebra* **70** (2022), 1281–1290, doi:10.1080/03081087.2020.1758609, https://doi.org/10.1080/03081087.2020.1758609.

[5] X. Gao, H. Lü and Y. Hao, The Laplacian and signless Laplacian spectrum of semi-Cayley graphs over abelian groups, *J. Appl. Math. Comput.* **51** (2016), 383–395, doi:10.1007/s12190-015-0911-9, https://doi.org/10.1007/s12190-015-0911-9.

[6] X. Gao and Y. Luo, The spectrum of semi-Cayley graphs over abelian groups, *Linear Algebra Appl.* **432** (2010), 2974–2983, doi:10.1016/j.laa.2009.12.040, https://doi.org/10.1016/j.laa.2009.12.040.

[7] P. Guillot, *A gentle course in local class field theory. Local number fields, Brauer groups, Galois cohomology*, Cambridge University Press, Cambridge, 2018, doi:10.1017/9781108377751, https://doi.org/10.1017/9781108377751.

[8] F. Li, Circulant digraphs integral over number fields, *Discrete Math.* **313** (2013), 821–823, doi:10.1016/j.disc.2012.12.025, https://doi.org/10.1016/j.disc.2012.12.025.

[9] F. Li, A method to determine algebraically integral Cayley digraphs on finite abelian group, *Contrib. Discrete Math.* **15** (2020), 148–152, doi:10.11575/cdm.v15i2.62327, https://doi.org/10.11575/cdm.v15i2.62327.

[10] X. Liu and S. Zhou, Eigenvalues of Cayley graphs, *Electron. J. Comb.* **29** (2022), research paper p2.9, 164, doi:10.37236/8569, https://doi.org/10.37236/8569.

[11] L. Lu, Q. Huang and X. Huang, Integral Cayley graphs over dihedral groups, *J. Algebr. Comb.* **47** (2018), 585–601, doi:10.1007/s10801-017-0787-x, https://doi.org/10.1007/s10801-017-0787-x.

[12] L. Lu and K. Mönius, Algebraic degree of Cayley graphs over abelian groups and dihedral groups, *J. Algebr. Comb.* (2023), doi:10.1007/s10801-022-01190-7, https://doi.org/10.1007/s10801-022-01190-7.

[13] K. Mönius, The algebraic degree of spectra of circulant graphs, *J. Number Theory* **208** (2020), 295–304, doi:10.1016/j.jnt.2019.08.002, https://doi.org/10.1016/j.jnt.2019.08.002.

[14] K. Mönius, Splitting fields of spectra of circulant graphs, *J. Algebra* **594** (2022), 154–169, doi:10.1016/j.jalgebra.2021.11.036, https://doi.org/10.1016/j.jalgebra.2021.11.036.

[15] G. Sabidussi, Vertex-transitive graphs, *Monatsh. Math.* **68** (1964), 426–438, http://eudml.org/doc/177267.

[16] N. Sripaisan and Y. Meemark, Algebraic degree of spectra of Cayley hypergraphs, *Discrete Appl. Math.* **316** (2022), 87–94, doi:10.1016/j.dam.2022.03.029, https://doi.org/10.1016/j.dam.2022.03.029.

[17] B. Steinberg, *Representation Theory of Finite Groups*, Springer, New York, 2009.

[18] L. L. X.Y. Huang and K. Mönius, Splitting fields of mixed cayley graphs over abelian groups, 2022, arXiv:2202.00987 [math.CO].

[19] H. Zou and J. Meng, Some algebraic properties of Bi-Cayley graphs, *Acta Math. Sin., Chin. Ser.* **50** (2007), 1075–1080.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 24 (2024) #P2.03 / 207–230
https://doi.org/10.26493/1855-3974.2894.b07
(Also available at http://amc-journal.eu)

A non-associative incidence near-ring with a generalized Möbius function*

John Johnson †, Max Wakefield ‡

US Naval Academy, 572-C Holloway Rd, Annapolis MD, 21402 USA

This paper is dedicated to the memory of John Johnson.

Received 1 June 2022, accepted 27 February 2023, published online 20 September 2023

Abstract

There is a convolution product on 3-variable partial flag functions of a locally finite poset that produces a generalized Möbius function. Under the product this generalized Möbius function is a one sided inverse of the zeta function and satisfies many generalizations of classical results. In particular we prove analogues of Phillip Hall's Theorem on the Möbius function as an alternating sum of chain counts, Weisner's Theorem, and Rota's Crosscut Theorem. A key ingredient to these results is that this function is an overlapping product of classical Möbius functions. Using this generalized Möbius function we define analogues of the characteristic polynomial and Möbius polynomials for ranked lattices. We compute these polynomials for certain families of matroids and prove that this generalized Möbius polynomial has -1 as root if the matroid is modular. Using results from Ardila and Sanchez we prove that this generalized characteristic polynomial is a matroid valuation.

Keywords: Incidence algebra, matroid, Möbius function, valuation.

Math. Subj. Class. (2020): 37K15, 42A99, 60E05, 05A17

*The authors are very thankful for detailed comments by the reviewer. The reviewers suggestions have significantly improved the article. The authors are thankful for discussions with Carolyn Chun, Joel Lewis, and Will Traves. The authors are also thankful to George Andrews for help on Lemma 6.14. Frederico Ardila and Mario Sanchez significantly helped with the material on valuations for which the authors are very thankful. Also, Jose Bastidas made multiple excellent comments for which the authors are very thankful. The authors would like to thank the US Naval Academy trident program for support during this project.

†Supported by the US Naval Academy as a Trident Scholar.

‡Corresponding author.

E-mail addresses: m213162@usna.edu (John Johnson), wakefiel@usna.edu (Max Wakefield)

1 Introduction

Combinatorial invariants in incidence algebras play a central role in many areas of combinatorics as well as in number theory, algebraic topology, algebraic geometry, and representation theory. In particular, the Möbius function appears in the inverse of the Riemann zeta function as well as the coefficients of the chromatic polynomial for graphs. In this note we study a generalization of the classical incidence algebra by looking at three variable incidence functions. A large portion of this study is focussed on studying a 3-variable generalized Möbius function inside this generalized incidence structure.

Incidence algebras and Möbius functions were popularized by Rota in [26]. Rota characterized the classical Möbius function from number theory (see [20] and [14]) as the inverse of the constant function **1** on the intervals of the poset which is called the zeta function. In [26] Rota gives many results on the Möbius function, including his Crosscut Theorem. Since then, many advances can be attributed to Möbius functions. Of particular importance are the counting theorems of Zaslavsky in [33] and Terao's factorization theorem (see [29]) using the Möbius function in the form of the characteristic polynomial of a hyperplane arrangement. The main motivation for this work is to build invariants which are finer than the classical Möbius function and characteristic polynomial to obtain more information about the underlying combinatorial structure.

More recently, there has been considerable developments in understanding of some classical invariants on matroids. One generalization came from Krajewski, Moffatt, and Tanasa who built Tutte polynomials from a Hopf algebra in [18]. Taking this a little further, in [11] Dupont, Fink and Moci construct a categorical framework to view various combinatorial invariants and they prove some convolution formulas. The work of Aguiar and Ardila in [1] framed many combinatorial structures like matroids in terms of generalized permutahedra, where there is a natural Hopf monoid governing classical operations. One possible starting place for this study could be the work of Joni and Rota in [16]. Then, in [6], Ardila and Sanchez use this Hopf monoid structure to build a concrete method for investigating valuations on many combinatorial structures. Another aim of this study is to add another invariant to the list of valuations. Concretely, we use the methods of Ardila and Sanchez to show that one of our invariants is a valuation on matroids. One view that one can take for many combinatorial structures is that of posets (e.g. matroids are geometric lattices) and this is the view that we take here.

The starting point for our study is the collection of 3-variable functions on ordered triples of elements in a poset. The set of these 3-variable functions also appears in the book [2] by Aguiar and Mahajan in Appendix C4 where they study 2-cochains and 2-cocycles. We differ from the work in Appendix C4 [2] by equipping this set of functions with a special convolution product. The motivation for this product comes from trying to symmetrize a more natural convolution product that was studied by the second author in [30] as well as making new invariants with special properties. This product provides a 3-variable Möbius function which is a sort of left inverse of the 3-variable analogue of the zeta function. We call this function the J-function and study many of its properties. It turns out that it is essentially a staggered product of the classical Möbius functions and hence satisfies generalizations of many of the classical theorems on the classical Möbius function. To prove these results we develop and use certain operations and formulas these 3-variable functions satisfy that give maps between various different types of incidence algebras. In [8] Jose Bastidas studies Type B Hopf monoids and defines an antipode via some convolution formulas which seem to have some similar properties to the work presented here.

As an application we build two different polynomials from the J-function: a generalized characteristic polynomial and a generalized Möbius polynomial (see [17] and [21] for Möbius polynomials). It turns out that these polynomials have some interesting properties that are not apparent from the surface. In the case of matroids, the generalized characteristic polynomial has positive coefficients. We then compute these polynomials for certain families of matroids and find special roots. Of particular interest is that the generalized Möbius function has -1 as a root for modular matroids, which mimics Theorem 1 in [21]. However, we show that the converse is not true and so one is led to question what do these polynomial count? Could there be some chromatic generalization for the generalized polynomials, or some lattice point or finite field counting formula for these polynomials (like [9] or [7])? Also, in [8], Bastidas defines some polynomial invariants via characters of a Hopf monoid. Can the polynomials we define here be put in the framework of [8]?

We finish by employing the methods of Ardila and Sanchez in [6] to show that our generalized characteristic polynomial is a matroid valuation. This follows from the fact that the J-function splits as a product of Möbius functions. In the case of the Möbius polynomial, we are not sure whether or not it is a valuation, yet we show that it does have a decomposition in terms of the classical characteristic polynomials. We find it interesting that this decomposition looks very similar to the recursive definition of the matroid Kazhdan-Lusztig polynomial originally defined in [12].

We begin this study with reviewing classical results on incidence algebras and Möbius functions in Section 2. Then we define our 3-variable incidence structure in Section 3. There we show that this structure has some interesting properties but that it is neither associative nor distributive. However, in Section 4 we develop multiple operations which give nice formulas between these different kinds of incidence functions. Using these formulas we define a generalized Möbius function, the J-function, and study its properties in Section 5. Finally in Section 6 we define our generalized characteristic and Möbius polynomials.

2 Incidence Algebras

Let R be a commutative ring and $\mathcal{P}$ be a locally finite poset. We follow [28] and [4] for combinatorics on posets. For the remainder of this note we refer to the order in $\mathcal{P}$ by $\leq$. Also, for $n \in \mathbb{N}$ let $[n] = \{1, 2, 3, \ldots, n\}$. In this section we review basic material of incidence algebras where we follow [27]. First we define the poset of partial flags.

Definition 2.1. The poset of *partial flags of length* k on $\mathcal{P}$ is

$$\mathcal{F}l^k(\mathcal{P}) = \left\{(x_1, x_2, \ldots, x_k) \in \mathcal{P}^k \middle| \, x_1 \leq x_2 \leq \cdots \leq x_k\right\}$$

with order given by $(x_1, \ldots, x_k) \preceq (y_1, \ldots, y_k)$ if and only if for all $i \in [k]$ we have $x_i \leq y_i$.

Now we define the classical incidence algebras.

Definition 2.2. The *incidence algebra* on $\mathcal{P}$ is the set

$$\mathbb{I}(\mathcal{P}, R) = \mathrm{Hom}(\mathcal{F}l^2(\mathcal{P}), R)$$

where R is a commutative ring. Addition in $\mathbb{I}(\mathcal{P}, R)$ is given by

$$(f + g)(x, y) = f(x, y) + g(x, y),$$

the multiplication is given by convolution

$$(f * g)(x, y) = \sum_{x \leq a \leq b} f(x, a)g(a, y),$$

and the scalar product is given by $(rf)(x, y) = rf(x, y)$ for all $r \in R$.

In this note, we will examine multiple different operations on functions on posets. For this reason we will reserve juxtaposition only for products of elements in the ring R. Otherwise we will denote products of functions with specific operation names like $*$.

It turns out that $\mathbb{I}(\mathcal{P}, R)$ is a non-commutative R-algebra with identity element given by the Kronecker delta function

$$\delta(x, y) = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{else.} \end{cases}$$

There are two other very important elements in $\mathbb{I}(\mathcal{P}, R)$.

Definition 2.3. The *zeta function* $\zeta \in \mathbb{I}(\mathcal{P}, R)$ is defined as the constant function on $\mathcal{F}l^2(\mathcal{P})$

$$\zeta(x, y) = 1$$

for all $(x, y) \in \mathcal{F}l^2(\mathcal{P})$. The *Möbius function* $\mu \in \mathbb{I}(\mathcal{P}, R)$ is defined by

$$\sum_{x \leq a \leq y} \mu(x, a) = \sum_{x \leq a \leq y} \mu(a, y) = \delta(x, y)$$

for all $(x, y) \in \mathcal{F}l^2(\mathcal{P})$.

The Möbius function was originally defined by Möbius (see [20]) on the poset of the natural numbers ordered by division for the purpose of inverting the Riemann zeta function. Since then the Möbius function has been used in many different contexts and broadened by the work of Rota in [26]. For our discussion, it is important to note that μ is the multiplicative inverse of the zeta function

$$\mu * \zeta = \zeta * \mu = \delta.$$

Now we review how the incidence algebra functor factors over products. Recall that for posets $\mathcal{P}$ and $\mathcal{Q}$ the product poset is $\mathcal{P} \times \mathcal{Q}$ with order given by $(x_1, x_2) \leq (y_1, y_2)$ if and only if $x_1 \leq y_1$ and $x_2 \leq y_2$.

Proposition 2.4 (Proposition 2.1.12 [27])**.** *If $\mathcal{P}$ and $\mathcal{Q}$ are locally finite posets then*

$$\mathbb{I}(\mathcal{P}, R) \otimes_R \mathbb{I}(\mathcal{Q}, R) \cong \mathbb{I}(\mathcal{P} \times \mathcal{Q}, R).$$

Because of Proposition 2.4 we define the following operation on functions. In order to the make the exposition clear in the case when we are dealing with functions over different posets, we will put the poset in the subscript. For $f_{\mathcal{P}} \in \mathbb{I}(\mathcal{P}, R)$ and $g_{\mathcal{Q}} \in \mathbb{I}(\mathcal{Q}, R)$ define $f_{\mathcal{P}} \times g_{\mathcal{Q}} \in \mathbb{I}(\mathcal{P} \times \mathcal{Q}, R)$ by

$$(f_{\mathcal{P}} \times g_{\mathcal{Q}})((x_1, x_2), (y_1, y_2)) = f_{\mathcal{P}}(x_1, y_1)g_{\mathcal{Q}}(x_2, y_2).$$

We will use this notation and the following consequence of Proposition 2.4 in our study in Section 5.

Corollary 2.5. *If $\mathcal{P}$ and $\mathcal{Q}$ are locally finite posets then $\mu_{\mathcal{P}} \times \mu_{\mathcal{Q}} = \mu_{\mathcal{P}\times\mathcal{Q}}$.*

Next we recall how the Möbius function counts chains (or is an Euler characteristic for the order complex). For $(x, y) \in \mathcal{F}l^2(\mathcal{P})$ let

$$c_i(x, y) = \left|\{(a_0, \ldots, a_i) \in \mathcal{F}l^{i+1} : \forall k,\ a_k < a_{k+1} \text{ and } a_0 = x \text{ and } a_i = y\}\right|$$

be the number of chains of length i between x and y.

Theorem 2.6 (Phillip Hall's Theorem [13]; Proposition 3.8.5 [28])**.** *If $\mathcal{P}$ is a locally finite poset and $(x, y) \in \mathcal{F}l^2(\mathcal{P})$ then*

$$\mu(x, y) = \sum_i (-1)^i c_i(x, y).$$

Now we review Rota's Crosscut Theorem. Let L be a finite lattice with $\hat{0}$ the minimum element and $\hat{1}$ the maximum element. Usually, Rota's Crosscut Theorem is stated globally in the lattice giving a formula for $\mu(\hat{0}, \hat{1})$. However, for our generalization we will need a local version.

Definition 2.7. Let $(x, y) \in \mathcal{F}l^2(L)$. A *lower crosscut* of the interval $[x, y] = \{a \in L | x \leq a \leq y\}$ is a set $S_{x,y} \subseteq [x, y]\backslash\{x\}$ such that if $b \in [x, y]\backslash(\mathcal{S}_{x,y} \cup \{x\})$ then there is some $a \in S_{x,y}$ with $a < b$. A *upper crosscut* of the interval $[x, y]$ is a set $T_{x,y} \subseteq [x, y]\backslash\{y\}$ such that if $a \in [x, y]\backslash(T_{x,y} \cup \{y\})$ then there is some $b \in T_{x,y}$ with $a < b$.

This definition gives Rota's famous Crosscut Theorem which we state in the style of Lemma 2.35 in [22] for use in arrangement theory.

Theorem 2.8 ([26, Theorem 3])**.** *If L is a lattice, $(x, y) \in \mathcal{F}l^2(L)$, and $S_{x,y}$ is a lower crosscut of $[x, y]$ then*

$$\mu(x, y) = \sum_{\substack{A \subseteq S_{x,y} \\ \bigvee A = y}} (-1)^{|A|}.$$

Dually, if $T_{x,y}$ is an upper crosscut of $[x, y]$ then

$$\mu(x, y) = \sum_{\substack{B \subseteq T_{x,y} \\ \bigwedge B = x}} (-1)^{|B|}.$$

Next we consider Weisner's Theorem (see [31]).

Theorem 2.9 ([28, Weisner's Theorem, Corollary 3.9.3])**.** *If L is a finite lattice with at least two elements and $\hat{1} \neq a \in L$ then*

$$\sum_{\substack{x \in L \\ x \wedge a = \hat{0}}} \mu(x, \hat{1}) = 0.$$

Now we recall one more result that follows from this classical result for matroids: the Mobius function of the lattice of flats of a matroid alternates in sign.

Lemma 2.10. *If L is a finite semimodular lattice then* $\operatorname{sgn}(\mu(x, y)) = (-1)^{\mathrm{rk}(x)+\mathrm{rk}(y)}$.

3 A 3-variable incidence non-associative near-ring

In this section, we define the algebraic structures where our invariants live. It turns out that these algebraic structures support various operations that can yield nice formulas. Later these formulas will be used to show certain formulas and relations on our new invariants.

Definition 3.1. Let R be a commutative ring and $\mathcal{P}$ be a locally finite poset. Define the 3-variable incidence left near-ring as

$$\mathbb{J}(\mathcal{P}, R) = \mathrm{Hom}(\mathcal{F}l^3(\mathcal{P}), \mathbb{R})$$

with binary operations as follows:

- For $f, g \in \mathbb{J}(\mathcal{P}, R)$ we define addition by

$$(f + g)(x, y, z) = f(x, y, z) + g(x, y, z).$$

- For $f, g \in \mathcal{J}(\mathcal{P}, R)$ we define a multiplication by

$$(f \succ g)(x, y, z) = \sum_{(a,b) \trianglelefteq (x,y,z)} f(x, a, a)g(a, y, b)f(b, b, z)$$

  where the juxtaposition in each term is multiplication in the ring R and $(a, b) \trianglelefteq (x, y, z)$ means $x \leq a \leq y \leq b \leq z$ in $\mathcal{P}$.

First we show that $\mathbb{J}(\mathcal{P}, R)$ is indeed left distributive.

Proposition 3.2. *If $\mathcal{P}$ is any poset then the multiplication $\succ$ in $\mathbb{J}(\mathcal{P}, R)$ is left distributive.*

Proof. Let $f, g, h \in \mathbb{J}(\mathcal{P}, R)$ and $(x, y, z) \in \mathcal{F}l^3(\mathcal{P})$. Then

$$\begin{aligned}
(f \succ (g + h))(x, y, z) &= \sum_{(a,b) \trianglelefteq (x,y,z)} f(x, a, a)(g + h)(a, y, b)f(b, b, z) \\
&= \sum_{(a,b) \trianglelefteq (x,y,z)} f(x, a, a)(g(a, y, b) + h(a, y, b))f(b, b, z) \\
&= \sum_{(a,b) \trianglelefteq (x,y,z)} f(x, a, a)g(a, y, b)f(b, b, z) \\
&\quad + \sum_{(a,b) \trianglelefteq (x,y,z)} f(x, a, a)h(a, y, b)f(b, b, z) \\
&= (f \succ g)(x, y, z) + (f \succ h)(x, y, z).
\end{aligned}$$

□

Remark 3.3. With this $+$ the set $\mathbb{J}(\mathcal{P}, R)$ is an abelian group. It would be convenient if $\mathbb{J}(\mathcal{P}, R)$ were naturally an R-algebra. However, this is far from the case as we will see. Even the natural action of R on $\mathbb{J}(\mathcal{P}, R)$ is flawed. Let $r \in R$ and $f, g \in \mathbb{J}(\mathcal{P}, R)$ then $r \cdot (f \succ g) = f \succ (r \cdot g)$ but $(r \cdot f) \succ g = r^2 \cdot (f \succ g)$.

Fortunately, though, there are a few special functions in $\mathbb{J}(\mathcal{P}, R)$ that provide substantial information. We will use these to study the structure of $\mathbb{J}(\mathcal{P}, R)$ and define other special elements later.

Definition 3.4. Assume that 1 is the multiplicative identity and 0 is the additive identity in R.

- Define $\delta_3 \in \mathbb{J}(\mathcal{P}, R)$ by

$$\delta_3(x,y,z) = \begin{cases} 1 & \text{if } x = y = z \\ 0 & \text{otherwise} \end{cases}$$

- Define $\zeta_3 \in \mathbb{J}(\mathcal{P}, R)$ by setting $\zeta_3(x,y,z) = 1$ for all $(x,y,z) \in \mathcal{F}l^3(\mathcal{P})$.

With these functions we can investigate basic properties of $\mathbb{J}(\mathcal{P}, R)$.

Proposition 3.5. *The element $\delta_3 \in \mathbb{J}(\mathcal{P}, R)$ is a left multiplicative identity.*

Proof. Let $f \in \mathbb{J}(\mathcal{P}, R)$ and $(x,y,z) \in \mathcal{F}l^3(\mathcal{P})$. Then

$$\begin{aligned}(\delta_3 \succ f)(x,y,z) &= \sum_{(a,b) \trianglelefteq (x,y,z)} \delta_3(x,a,a) f(a,y,b) \delta_3(b,b,z) \\ &= \delta_3(x,x,x) f(x,y,z) \delta_3(z,z,z) = f(x,y,z). \end{aligned}$$ □

In the next three propositions we note that in general $\mathbb{J}(\mathcal{P}, R)$ is not commutative, associative, or right distributive. We could do this with a single example, however these propositions show that $\mathbb{J}(\mathcal{P}, R)$ is basically never commutative, associative, or right distributive.

Proposition 3.6. *If $\mathcal{P}$ is a non-trivial poset (it has at least two comparable elements) or the base ring is not Boolean (not idempotent), then the multiplication $\succ$ in $\mathbb{J}(\mathcal{P}, R)$ is non-commutative and δ_3 is not a right multiplicative identity.*

Proof. Let $(x,y,z) \in \mathcal{F}l^3(\mathcal{P})$ and suppose that either $x < y$ or that $y < z$ in $\mathcal{P}$ or that R is not Boolean. Under these assumptions we can construct a function $f \in \mathbb{J}(\mathcal{P}, R)$ that has $f(x,y,z) \neq f(x,y,y) f(y,y,z)$. Then from Proposition 3.5 we have $(\delta_3 \succ f)(x,y,z) = f(x,y,z)$ but $(f \succ \delta_3)(x,y,z) = f(x,y,y) f(y,y,z)$. □

The proof for the next fact is very similar.

Proposition 3.7. *If $\mathcal{P}$ is a poset with three elements x, y, z satisfying $x < y < z$ or the base ring is not Boolean (not idempotent), then the multiplication $\succ$ in $\mathbb{J}(\mathcal{P}, R)$ is non-associative.*

Proof. Let $(x,y,z) \in \mathcal{F}l^3(\mathcal{P})$ be three elements satisfying $x < y < z$ in $\mathcal{P}$ or that R is not Boolean. Under these assumptions we can construct a function $f \in \mathbb{J}(\mathcal{P}, R)$ that has $f(x,y,y) f(y,y,y)^2 f(y,y,z) \neq f(x,y,y) f(y,y,z)$. Compute

$$\begin{aligned}((f \succ \delta_3) \succ \delta_3))(x,y,z) &= \sum_{(a,b) \trianglelefteq (x,y,z)} (f \succ \delta_3)(x,a,a) \delta_3(a,y,b) (f \succ \delta_3)(b,b,z) \\ &= [(f \succ \delta_3)(x,y,y)][(f \succ \delta_3)(y,y,z)] \\ &= [f(x,y,y) f(y,y,y)][f(y,y,y) f(y,y,z)]. \end{aligned}$$

Then from Proposition 3.5 we have $(f \succ (\delta_3 \succ \delta_3))(x,y,z) = (f \succ \delta_3)(x,y,z) = f(x,y,y) f(y,y,z)$ which is different from $((f \succ \delta_3) \succ \delta_3))(x,y,z)$ by our assumption on f. □

Proposition 3.8. *If $\mathcal{P}$ is a non-trivial poset (it has at least two comparable elements) and R is any non-trivial commutative ring, then the multiplication $\succ$ in $\mathbb{J}(\mathcal{P}, R)$ is not right distributive.*

Proof. Let $(x, y, z) \in \mathcal{F}l^3(\mathcal{P})$ and $f \in \mathbb{J}(\mathcal{P}, R)$ be any function such that $f(x, y, y) + f(y, y, z) \neq 0$. Then

$$\begin{aligned}((f + \zeta_3) \succ \delta_3)(x, y, z) &= \sum_{(a,b) \trianglelefteq (x,y,z)} (f + \zeta_3)(x, a, a)\delta_3(a, y, b)(f + \zeta_3)(b, b, z) \\ &= [(f + \zeta_3)(x, y, y)][(f + \zeta_3)(y, y, z)] \\ &= f(x, y, y)f(y, y, z) + f(x, y, y) + f(y, y, z) + 1.\end{aligned}$$

On the other hand we have

$$\begin{aligned}((f \succ \delta_3) + (\zeta_3 \succ \delta_3))(x, y, z) &= f(x, y, y)f(y, y, z) + \zeta_3(x, y, y)\zeta_3(y, y, z) \\ &= f(x, y, y)f(y, y, z) + 1\end{aligned}$$

which by the hypothesis on f we have the right distributive property not holding. □

With Propositions 3.5, 3.6, 3.7, 3.2, and 3.8 we conclude that $J(\mathcal{P}, R)$ is a left only unital, non-commutative, non-associative, near-ring (see [25] for this terminology). Also, note that there is the zero function $Z \in \mathbb{J}(\mathcal{P}, R)$ which satisfies $Z \succ f = f \succ Z = Z$ for all $f \in \mathbb{J}(\mathcal{P}, R)$. Further note that addition in $\mathbb{J}(\mathcal{P}, R)$ is abelian. Hence $\mathbb{J}(\mathcal{P}, R)$ is an abelian, zero-symmetric, left only unital, non-commutative, non-associative, near-ring. It is worth noting that in general $\mathbb{J}(\mathcal{P}, R)$ is not even close to being associative on both sides and is not an alternative algebra or any similar generalization.

Now we look at a few special cases that do not satisfy the hypothesis of some of these propositions.

Example 3.9. Let $\mathcal{P} = B_0 = \{0\}$ be the poset with just one element and R any commutative ring. Then as a set $\mathbb{J}(B_0, R) = R$, but multiplication is given by $a \succ b = aba = a^2b$. If R is Boolean then $\mathbb{J}(B_0, R) \cong R$. Otherwise, this near-ring is not associative, not commutative, and is only left unital.

Example 3.10. Let $\mathcal{P} = B_1 = \{0, 1\}$ be the Boolean poset of rank 1 and R be any Boolean ring (one example would be $\mathbb{F}_2$). Then the hypothesis of Proposition 3.7 is not satisfied and the non-equality $f(x, y, y)f(y, y, y)^2 f(y, y, z) \neq f(x, y, y)f(y, y, z)$ used in the proof is always equal. It turns out that in this case $\mathbb{J}(B_1, R)$ is associative and we prove this now. In order to shorten the calculation we will denote $(0, 0, 0)$ by $\vec{0}$ and $(1, 1, 1)$ by $\vec{1}$. First we see that

$$((f \succ g) \succ h)(\vec{0}) = f(\vec{0})g(\vec{0})h(\vec{0}) = (f \succ (g \succ h))(\vec{0}).$$

Then for the non-trivial tuple $(0, 0, 1)$ we compute

$$\begin{aligned}((f \succ g) \succ h)(0, 0, 1) =& (f \succ g)(\vec{0})h(\vec{0})(f \succ g)(0, 0, 1) \\ &+ (f \succ g)(\vec{0})h(0, 0, 1)(f \succ g)(\vec{1}) \\ =& f(\vec{0})g(\vec{0})h(\vec{0})[f(\vec{0})g(\vec{0})f(0, 0, 1) + f(\vec{0})g(0, 0, 1)f(\vec{1})] \\ &+ f(\vec{0})g(\vec{0})h(0, 0, 1)f(\vec{1})g(\vec{1}) \\ =& f(\vec{0})g(\vec{0})h(\vec{0})f(0, 0, 1) + f(\vec{0})g(\vec{0})h(\vec{0})g(0, 0, 1)f(\vec{1}) \\ &+ f(\vec{0})g(\vec{0})h(0, 0, 1)f(\vec{1})g(\vec{1}).\end{aligned}$$

Then the other side of the associative identity is

$$\begin{aligned}(f \succ (g \succ h))(0,0,1) =& f(\vec{0})(g \succ h)(\vec{0})f(0,0,1) + f(\vec{0})\big[(g \succ h)(0,0,1)\big]f(\vec{1}) \\ =& f(\vec{0})g(\vec{0})h(\vec{0})f(0,0,1) + f(\vec{0})\big[g(\vec{0})h(\vec{0})g(0,0,1) \\ &+ g(\vec{0})h(0,0,1)g(\vec{1})\big]f(\vec{1}) \\ =& ((f \succ g) \succ h)(0,0,1).\end{aligned}$$

Hence $\mathbb{J}(B_1, R)$ is associative. This example does satisfy the hypothesis of Proposition 3.8. Hence $\mathbb{J}(B_1, R)$ is a (associative) left abelian (addition is commutative) near-ring. That's about as good as it gets though. For example, if $R = \mathbb{F}_2$ then $\mathbb{J}(B_1, \mathbb{F}_2)$ is not a near-field because any function with $f(\vec{0}) = 0$ and $f(0,0,1) = 1$ does not have an inverse. For exactly the same reason $\delta_3 \in \mathbb{J}(B_1, \mathbb{F}_2)$ is still not a right identity element.

4 Operations on incidence functions

In this section we look at a relationship between the classical incidence algebra $\mathbb{I}(\mathcal{P}, R)$ and $\mathbb{J}(\mathcal{P}, R)$. For $f, g \in \mathbb{I}(\mathcal{P}, R)$ we define $f \diamondsuit g \in \mathbb{J}(\mathcal{P}, R)$ by setting

$$(f \diamondsuit g)(x, y, z) = f(x, y)g(y, z).$$

We can use the $\diamondsuit$ operation to construct interesting elements in $\mathbb{J}(\mathcal{P}, R)$. There are relationships between the operations $*$ in $\mathbb{I}(\mathcal{P}, R)$, $\succ$ in $\mathbb{J}(\mathcal{P}, R)$, and $\diamondsuit$.

Proposition 4.1. *If $f, g, r, s \in \mathbb{I}(\mathcal{P}, R)$ and $f(b,b)g(a,a) = 1$ for all $a, b \in \mathcal{P}$ then*

$$(f \diamondsuit g) \succ (r \diamondsuit s) = (f * r) \diamondsuit (s * g).$$

Proof. Let $(x, y, z) \in \mathcal{F}l^3(\mathcal{P})$ and $f, g, r, s \in I(\mathcal{P}, R)$. Then

$$\begin{aligned}((f \diamondsuit g) \succ (r \diamondsuit s))(x, y, z) =& \sum_{(a,b) \trianglelefteq (x,y,z)} (f \diamondsuit g)(x, a, a)(r \diamondsuit s)(a, y, b)(f \diamondsuit g)(b, b, z) \\ =& \sum_{(a,b) \trianglelefteq (x,y,z)} f(x, a)g(a, a)r(a, y)s(y, b)f(b, b)g(b, z) \\ =& \left[\sum_{x \le a \le y} f(x, a)r(a, y)\right]\left[\sum_{y \le b \le z} s(y, b)g(b, z)\right] \\ =& \left[(f * r)(x, y)\right]\left[(s * g)(y, z)\right] \\ =& ((f * r) \diamondsuit (s * g))(x, y, z)\end{aligned}$$

where the third equality only holds due the the assumption. □

One can see from the proof that without the hypothesis on f and g that the equality will not hold. Hence there is no hope for this to give any kind of near-ring homomorphism from a twisted product version of $\mathbb{I}(\mathcal{P}, R) \times \mathbb{I}(\mathcal{P}, R)$. Also, the natural addition homomorphism assumption does not hold. Instead we have the following proposition which does not have special hypothesis on the functions. For this proposition there are two different additions, for $\mathbb{I}(\mathcal{P}, R)$ and $\mathbb{J}(\mathcal{P}, R)$, which for brevity we use the same addition symbol.

Proposition 4.2. *If $f, g, r, s \in \mathbb{I}(\mathcal{P}, R)$ then*

$$(f+g)\Diamond(r+s) = (f\Diamond r) + (f\Diamond s) + (g\Diamond r) + (g\Diamond s).$$

Proof. For all $(x, y, z) \in \mathcal{F}l^3(\mathcal{P})$

$$\begin{aligned}((f+g)\Diamond(r+s))(x,y,z) =& (f(x,y)+g(x,y))(r(y,z)+s(y,z)) \\ =& f(x,y)r(y,z) + f(x,y)s(y,z) + g(x,y)r(y,z) + \\ & g(x,y)s(y,z) \\ =& ((f\Diamond r) + (f\Diamond s) + (g\Diamond r) + (g\Diamond s))(x,y,z)\end{aligned}$$

which is the identity we are looking for. □

We can also define products of functions on products of posets over 3-flags. We prefer to limit our study of $\mathbb{J}(\mathcal{P}, R)$ to this product definition since the technicalities of tensor products over non-associative near-rings would present significant and unnecessary complications.

Definition 4.3. Let $\mathcal{P}$ and $\mathcal{Q}$ be locally finite posets, $f_\mathcal{P} \in \mathbb{J}(\mathcal{P}, R)$, and $g_\mathcal{Q} \in \mathbb{J}(\mathcal{Q}, R)$. Define $f_\mathcal{P} \times g_\mathcal{Q} \in \mathbb{J}(\mathcal{P} \times \mathcal{Q}, R)$ by

$$(f_\mathcal{P} \times g_\mathcal{Q})((x_1, x_2), (y_1, y_2), (z_1, z_2)) = f_\mathcal{P}(x_1, y_1, z_1) g_\mathcal{Q}(x_2, y_2, z_2).$$

Now we show how the $\Diamond$ operation is compatible with products of posets.

Proposition 4.4. *If $\mathcal{P}$ and $\mathcal{Q}$ are locally finite posets, $f_\mathcal{P}, g_\mathcal{P} \in \mathbb{I}(\mathcal{P}, R)$, and $r_\mathcal{Q}, s_\mathcal{Q} \in \mathbb{I}(\mathcal{Q}, R)$ then*

$$(f_\mathcal{P}\Diamond g_\mathcal{P}) \times (r_\mathcal{Q}\Diamond s_\mathcal{Q}) = (f_\mathcal{P} \times r_\mathcal{Q})\Diamond(g_\mathcal{P} \times s_Q).$$

Proof. Let $((x_1, x_2), (y_1, y_2), (z_1, z_2)) \in \mathcal{F}l^3(\mathcal{P} \times \mathcal{Q})$. Then

$$\begin{aligned}&((f\Diamond g) \times (r\Diamond s))((x_1,x_2),(y_1,y_2),(z_1,z_2)) \\ &= [(f\Diamond g)(x_1,y_1,z_1)]\,[(r\Diamond s)(x_2,y_2,z_2)] \\ &= [f(x_1,y_1)g(y_1,z_1)]\,[r(x_2,y_2)s(y_2,z_2)] \\ &= [f(x_1,y_1)r(x_2,y_2)]\,[g(y_1,z_1)s(y_2,z_2)] \\ &= [(f\times r)((x_1,y_1),(x_2,y_2))]\,[(g\times s)((y_1,z_1),(y_2,z_2))] \\ &= ((f\times r)\Diamond(g\times s))((x_1,x_2),(y_1,y_2),(z_1,z_2))\end{aligned}$$

which completes the proof. □

As in Proposition 4.4 we will now show how the operations $\times$ and $\succ$ factor over products of posets. We use subscripts on these operations to keep track of which poset the operation is applied.

Proposition 4.5. *If $\mathcal{P}$ and $\mathcal{Q}$ be locally finite posets, $f_\mathcal{P}, g_\mathcal{P} \in \mathbb{J}(\mathcal{P}, R)$, and $r_\mathcal{Q}, s_\mathcal{Q} \in \mathbb{J}(\mathcal{Q}, R)$ then*

$$(f_\mathcal{P} \succ_\mathcal{P} g_\mathcal{P}) \times (r_\mathcal{Q} \succ_\mathcal{Q} s_\mathcal{Q}) = (f_\mathcal{P} \times r_\mathcal{Q}) \succ_{\mathcal{P}\times\mathcal{Q}} (g_\mathcal{P} \times s_\mathcal{Q}).$$

Proof. Let $\overline{x} = (x_1, x_2), \overline{y} = (y_1, y_2), \overline{z} = (z_1, z_2) \in \mathcal{P} \times \mathcal{Q}$ so that $(\overline{x}, \overline{y}, \overline{z}) \in \mathcal{F}l^3(\mathcal{P} \times \mathcal{Q})$ and $\overline{a} = (a_1, a_2), \overline{b} = (b_1, b_2) \in \mathcal{P} \times \mathcal{Q}$ so that $(\overline{a}, \overline{b}) \in \mathcal{F}l^2(\mathcal{P} \times \mathcal{Q})$. Then

$$\begin{aligned}
&((f_{\mathcal{P}} \times r_{\mathcal{Q}}) \succ_{\mathcal{P}\times\mathcal{Q}} (g_{\mathcal{P}} \times s_{\mathcal{Q}}))(\overline{x}, \overline{y}, \overline{z}) \\
&\quad = \sum_{(\overline{a},\overline{b}) \trianglelefteq (\overline{x},\overline{y},\overline{z})} (f_{\mathcal{P}} \times r_{\mathcal{Q}})(\overline{x}, \overline{a}, \overline{a})(g_{\mathcal{P}} \times s_{\mathcal{Q}})(\overline{a}, \overline{y}, \overline{b})(f_{\mathcal{P}} \times r_{\mathcal{Q}})(\overline{b}, \overline{b}, \overline{z}) \\
&\quad = \sum_{(a_1,b_1)} \sum_{(a_2,b_2)} f_{\mathcal{P}}(x_1, a_1, a_1) g_{\mathcal{P}}(a_1, y_1, b_1) f_{\mathcal{P}}(b_1, b_1, z_1) \\
&\qquad\qquad\qquad\qquad r_{\mathcal{Q}}(x_2, a_2, a_2) s_{\mathcal{Q}}(a_2, y_2, b_2) r_{\mathcal{Q}}(b_2, b_2, z_2) \\
&\quad = [(f_{\mathcal{P}} \succ g_{\mathcal{P}})(x_1, y_1, z_1)] \, [(r_{\mathcal{Q}} \succ s_{\mathcal{Q}})(x_2, y_2, z_2)] \\
&\quad = ((f_{\mathcal{P}} \succ_{\mathcal{P}} g_{\mathcal{P}}) \times (r_{\mathcal{Q}} \succ_{\mathcal{Q}} s_{\mathcal{Q}}))(\overline{x}, \overline{y}, \overline{z})
\end{aligned}$$

which is the required identity. □

5 The J-function

Let $\mathcal{P}$ be a locally finite poset. In this section we define the central invariant of this note which we call the J function. This function is a generalization of the classical Möbius function μ. We show that it satisfies generalizations of the classical theorems on μ. A key ingredient for these results is the operation $\diamondsuit$.

Definition 5.1. Define $J \colon \mathcal{F}l^3(\mathcal{P}) \to \mathbb{Z}$ for all fixed $(x, y, z) \in \mathcal{F}l^3(P)$ by

$$\sum_{(a,b) \trianglelefteq (x,y,z)} J(a, y, b) = \delta_3(x, y, z).$$

This function is well defined because either $x = y = z$ with $J(x, y, z) = 1$ or otherwise all of the following summations are finite

$$\begin{aligned}
J(x, y, z) = &- \sum_{x<a<y} \left[\sum_{y<b<z} J(a, y, b) \right] \\
&- \sum_{x<a\leq y} J(a, y, z) - \sum_{y\leq b<z} J(x, y, b).
\end{aligned}$$

Note that J is exactly the function in $\mathbb{J}(\mathcal{P}, R)$ such that

$$\zeta_3 \succ J = \delta_3. \tag{5.1}$$

This is a good reason why we say it is a generalization of the classical Möbius function and below we show that there are a few more interesting reasons. It turns out that this function was actually defined before in [30] with the notation μ_3^p and is exactly given by the $\diamondsuit$ product construction in the previous section.

Theorem 5.2. *For any locally finite poset $\mathcal{P}$ we have $J = \mu_3^p = \mu \diamondsuit \mu$.*

Proof. This follows from Proposition 4.1 since $\zeta \in \mathbb{I}(\mathcal{P}, R)$ satisfies the hypothesis and

$$\zeta_3 \succ (\mu \diamondsuit \mu) = (\zeta \diamondsuit \zeta) \succ (\mu \diamondsuit \mu) = (\zeta * \mu) \diamondsuit (\mu * \zeta) = \delta \diamondsuit \delta = \delta_3.$$

Hence J and $\mu \diamondsuit \mu$ satisfy the same recursive definition. □

Now we can use all the classical properties of μ to conclude information about J. We start by noticing that J is also a left inverse of ζ_3.

Corollary 5.3. $J \succ \zeta_3 = \delta_3$.

Proof. Since μ satisfies the hypothesis of Proposition 4.1 we get

$$J \succ \zeta_3 = (\mu \diamondsuit \mu) \succ (\zeta \diamondsuit \zeta) = (\mu * \zeta) \diamondsuit (\zeta * \mu) = \delta \diamondsuit \delta = \delta_3$$

which is the desired result. □

Interpreting Corollary 5.3 in terms of the definition and sums in the ring R we get the following.

Corollary 5.4. *For any locally finite poset $\mathcal{P}$ and $(x, y, z) \in \mathcal{F}l^3(\mathcal{P})$ we have*

$$\sum_{(a,b) \trianglelefteq (x,y,z)} J(x, a, a) J(b, b, z) = \delta_3(x, y, z)$$

and in particular

$$\sum_{(a,b) \trianglelefteq (x,y,z)} \mu(x, a) \mu(b, z) = \delta_3(x, y, z).$$

Now we look at how the J function behaves over products. It turns out that J factors over products.

Proposition 5.5. *If $\mathcal{P}$ and $\mathcal{Q}$ are locally finite posets then $J_{\mathcal{P}} \times J_{\mathcal{Q}} = J_{\mathcal{P} \times \mathcal{Q}}$.*

Proof. For posets $\mathcal{P}$ and $\mathcal{Q}$ we have $J_{\mathcal{P}} \times J_{\mathcal{Q}} = (\mu_{\mathcal{P}} \diamondsuit \mu_{\mathcal{P}}) \times (\mu_{\mathcal{Q}} \diamondsuit \mu_{\mathcal{Q}})$ by definition. By Proposition 4.4 $(\mu_{\mathcal{P}} \diamondsuit \mu_{\mathcal{P}}) \times (\mu_{\mathcal{Q}} \diamondsuit \mu_{\mathcal{Q}}) = (\mu_{\mathcal{P}} \times \mu_{\mathcal{Q}}) \diamondsuit (\mu_{\mathcal{P}} \times \mu_{\mathcal{Q}})$. Then using Proposition 2.5 we get $(\mu_{\mathcal{P}} \times \mu_{\mathcal{Q}}) \diamondsuit (\mu_{\mathcal{P}} \times \mu_{\mathcal{Q}}) = \mu_{\mathcal{P} \times \mathcal{Q}} \diamondsuit \mu_{\mathcal{P} \times \mathcal{Q}} = J_{\mathcal{P} \times \mathcal{Q}}$. □

Next we look at a generalization of Phillip Hall's Theorem. For $(x, y, z) \in \mathcal{F}l^3(\mathcal{P})$ set

$$c_{i,j}(x, y, z) = \left| \{ (a_0, \ldots, a_{i+j}) \in \mathcal{F}l^{i+j+1} : \forall k,\ a_k < a_{k+1} \text{ and } a_0 = x, a_i = y, a_{i+j} = z \} \right|.$$

There is a bijection between the underlying set of $c_{i,j}(x, y, z)$ to the product of the under lying sets of $c_i(x, y)$ and $c_j(y, z)$. This results in the following.

Lemma 5.6. *If $\mathcal{P}$ is a locally finite poset and $(x, y, z) \in \mathcal{F}l^3(\mathcal{P})$ then $c_{i,j}(x, y, z) = c_i(x, y) c_j(y, z)$.*

This leads to a generalization of Phillip Hall's Theorem for the J function.

Theorem 5.7. *If $\mathcal{P}$ is a locally finite poset and $(x, y, z) \in \mathcal{F}l^3(\mathcal{P})$ then*

$$J(x, y, z) = \sum_{i,j \in \mathbb{N}} (-1)^{i+j} c_{i,j}(x, y, z).$$

Proof. Let $(x,y,z) \in \mathcal{F}l^3(\mathcal{P})$. By Theorem 5.2 $J(x,y,z) = \mu(x,y)\mu(y,z)$. Then using Theorem 2.6 we get

$$\begin{aligned} J(x,y,z) &= \left[\sum_{i\in\mathbb{N}}(-1)^i c_i(x,y)\right]\left[\sum_{j\in\mathbb{N}}(-1)^j c_j(y,z)\right] \\ &= \sum_{i,j\in\mathbb{N}}(-1)^{i+j}c_i(x,y)c_i(y,z). \end{aligned}$$

Lemma 5.6 finishes the proof. □

Now we focus on a version of Rota's Crosscut Theorem for the J function. We state this following the style of Lemma 2.35 in [22] and Theorem 2.4.9 in [19], which are forms of Rota's original Crosscut Theorem in [26]. To state this result we need the following definition.

Definition 5.8. Let L be a finite lattice, $(x,y,z) \in \mathcal{F}l^3(L)$, $S_{x,y}$ be a lower crosscut of $[x,y]$, and $S_{y,z}$ be a lower crosscut of $[y,z]$ as in Definition 2.7. We call $S_{x,y,z} = S_{x,y} \bigsqcup S_{y,z}$ a double lower crosscut of (x,y,z) and call $S_{x,y}$ and $S_{y,z}$ the components of $S_{x,y,z}$. Similarly we can define $T_{x,y,z} = T_{x,y} \bigsqcup T_{y,z}$ (as well as $ST_{x,y,z} = S_{x,y} \bigsqcup T_{y,z}$ and $TS_{x,y,z} = T_{x,y} \bigsqcup S_{y,z}$).

Theorem 5.9. *If L is a finite lattice, $(x,y,z) \in \mathcal{F}l^3(L)$, $S_{x,y,z}$ is a double lower crosscut of (x,y,z) with components $S_{x,y}$ and $S_{y,z}$ then*

$$J(x,y,z) = \sum_{\substack{A\subseteq S_{x,y,z} \\ \bigvee(A\cap S_{x,y})=y \\ \bigvee(A\cap S_{y,z})=z}} (-1)^{|A|}.$$

Proof. Again we use Theorem 5.2 together with the classical Theorem 2.8

$$\begin{aligned} J(x,y,z) =& \mu(x,y)\mu(y,z) \\ &= \left[\sum_{\substack{A_1\subseteq S_{x,y} \\ \bigvee A_1=y}} (-1)^{|A_1|}\right]\left[\sum_{\substack{A_2\subseteq S_{y,z} \\ \bigvee A_2=z}} (-1)^{|A_2|}\right] \\ &= \sum_{\substack{A_1\subseteq S_{x,y} \\ \bigvee A_1=y}}\sum_{\substack{A_2\subseteq S_{y,z} \\ \bigvee A_2=z}} (-1)^{|A_1|+|A_2|}. \end{aligned}$$

Since the union in Definition 5.8 is disjoint $|A_1| + |A_2| = |A_1 \bigsqcup A_2|$ and we have finished the proof. □

We end this section with a generalization of Weisner's Theorem 2.9. The interesting observation of this fact is that the middle variable of the function is crucial.

Theorem 5.10. *If L is a finite lattice with at least three elements and $\hat{0} < a < b \in L$ then*

$$\sum_{\substack{x\in L \\ x\wedge a=\hat{0}}} J(x,b,\hat{1}) = 0.$$

Proof. We compute the sum again using Theorem 5.2:

$$\begin{aligned}\sum_{\substack{x\in L\\ x\wedge a=\hat{0}}} J(x,b,\hat{1}) &= \sum_{\substack{x\\ x\wedge a=\hat{0}}} \mu(x,b)\mu(b,\hat{1})\\ &= \mu(b,\hat{1}) \sum_{\substack{x\\ x\wedge a=\hat{0}}} \mu(x,b)\\ &= \mu(b,\hat{1})\cdot 0 = 0\end{aligned}$$

since $a < b$ we can apply Weisner's Theorem 2.9. □

Remark 5.11. There is a dual version of this result where we sum over the left most variable as in [26]. However, we do not see a version that sums over the middle variable.

6 Generalized characteristic and Möbius polynomials

In this section we examine two polynomials defined by summing over all values of the J function on a ranked poset. One mimics the characteristic polynomial of a matroid and the other looks like a one variable Möbius polynomial. We find more interesting information inside the generalized Möbius polynomial than the generalized characteristic polynomial. That is opposite of the state of affairs in the literature on the classical polynomials, but we do not know why.

Definition 6.1. For $\mathcal{P}$ a ranked finite poset with minimum element $\hat{0}$ and maximum element $\hat{1}$ the J-characteristic polynomial of $\mathcal{P}$ is

$$\mathcal{J}(\mathcal{P},t) = (-1)^{\mathrm{rk}(\mathcal{P})} \sum_{x\in\mathcal{P}} J(\hat{0},x,\hat{1}) t^{\mathrm{rk}(\mathcal{P})-\mathrm{rk}(x)}.$$

Definition 6.2. Let $\mathcal{P}$ be a ranked finite poset and for $(x,y,z) \in \mathcal{F}l^3(\mathcal{P})$ let $\rho(x,y,z) = 3\mathrm{rk}(\mathcal{P}) - \mathrm{rk}(x) - \mathrm{rk}(y) - \mathrm{rk}(z)$. The J-Möbius polynomial of $\mathcal{P}$ is

$$\mathcal{M}(\mathcal{P},t) = \sum_{(x,y,z)\in\mathcal{F}l^3(\mathcal{P})} J(x,y,z) t^{\rho(x,y,z)}.$$

We may sometimes refer to $\mathrm{rk}(\mathcal{P}) - \mathrm{rk}(x)$ as $\mathrm{crk}(x)$. These polynomials satisfy some nice basic properties. For example it turns out that the coefficients of $\mathcal{J}(\mathcal{P},t)$ are positive for nice $\mathcal{P}$. For convenience if L is a ranked poset let $L_k = \{x \in L | \mathrm{rk}(x) = k\}$.

Proposition 6.3. *If L is a finite semimodular lattice then the coefficients of $\mathcal{J}(L,t)$ are positive.*

Proof. Using Theorem 5.2 we get that

$$\mathcal{J}(L,t) = (-1)^{\mathrm{rk}(L)} \sum_{x\in L} \mu(\hat{0},x)\mu(x,\hat{1}) t^{\mathrm{rk}(L)-\mathrm{rk}(x)}.$$

So, the coefficient of t^k is

$$c_k = (-1)^{\mathrm{rk}(L)} \sum_{x\in L_k} \mu(\hat{0},x)\mu(x,\hat{1}).$$

Then note that by applying Lemma 2.10 we have

$$\operatorname{sgn}(\mu(\hat{0},x)\mu(x,\hat{1})) = (-1)^{\operatorname{rk}(\hat{0})+\operatorname{rk}(x)}(-1)^{\operatorname{rk}(x)+\operatorname{rk}(\hat{1})} = (-1)^{\operatorname{rk}(L)}.$$

Hence $\operatorname{sgn}(c_k) = (-1)^{2\operatorname{rk}(L)} = 1$. □

Now we look at a foundational property for the J-Möbius polynomial.

Proposition 6.4. *If L is a finite lattice with at least two elements then $\mathcal{M}(L,1) = 0$.*

Proof. Since L is a finite lattice with at least two elements we know there is a minimum element $\hat{0}$ and a maximum element $\hat{1}$. Then

$$\begin{aligned}\mathcal{M}(\mathcal{P},1) &= \sum_{(x,y,z)\in\mathcal{F}l^3(L)} J(x,y,z)\\ &= \sum_{y\in L}\left[\sum_{(x,z)\trianglelefteq(\hat{0},y,\hat{1})} J(x,y,z)\right]\\ &= \sum_{y\in L}\left[\delta_3(\hat{0},y,\hat{1})\right].\end{aligned}$$

Since L has at least two elements $\hat{0}\neq\hat{1}$ so $\delta_3(\hat{0},y,\hat{1})$ is zero for all y. □

We also have products formulas for both of these polynomials.

Proposition 6.5. *If $\mathcal{P}$ and $\mathcal{Q}$ are ranked finite posets then $\mathcal{J}(\mathcal{P}\times\mathcal{Q},t) = \mathcal{J}(\mathcal{P},t)\mathcal{J}(\mathcal{Q},t)$.*

Proof. Using Proposition 5.5 we get that

$$\begin{aligned}\mathcal{J}(\mathcal{P},t)\mathcal{J}(\mathcal{Q},t) &= \left[(-1)^{\operatorname{rk}(\mathcal{P})}\sum_{p\in\mathcal{P}} J_{\mathcal{P}}(\hat{0},p,\hat{1})t^{\operatorname{crk}(p)}\right]\left[(-1)^{\operatorname{rk}(\mathcal{Q})}\sum_{q\in\mathcal{Q}} J_{\mathcal{Q}}(\hat{0},q,\hat{1})t^{\operatorname{crk}(q)}\right]\\ &= (-1)^{\operatorname{rk}(\mathcal{P})+\operatorname{rk}(\mathcal{Q})}\sum_{p\in\mathcal{P}}\sum_{q\in\mathcal{Q}} J_{\mathcal{P}}(\hat{0},p,\hat{1})J_{\mathcal{Q}}(\hat{0},q,\hat{1})t^{\operatorname{crk}(p)+\operatorname{crk}(q)}\\ &= (-1)^{\operatorname{rk}(\mathcal{P}\times\mathcal{Q})}\sum_{(p,q)\in\mathcal{P}\times\mathcal{Q}} J_{\mathcal{P}\times\mathcal{Q}}((\hat{0},\hat{0}),(p,q),(\hat{1},\hat{1}))t^{\operatorname{crk}(p,q)}\\ &= \mathcal{J}(\mathcal{P}\times\mathcal{Q},t).\end{aligned}$$

□

The proof of the following is almost identical.

Proposition 6.6. *If $\mathcal{P}$ and $\mathcal{Q}$ are ranked finite posets then $\mathcal{M}(\mathcal{P}\times\mathcal{Q},t) = \mathcal{M}(\mathcal{P},t)\mathcal{M}(\mathcal{Q},t)$.*

Now we can use these product formulas to establish formulas for Boolean matroids.

Proposition 6.7. *If B_n is the Boolean lattice then*

$$\mathcal{J}(B_n,t) = (t+1)^n.$$

Proof. We start with B_1. This poset has two elements $B_1 = \{0, 1\}$. So, $\mathcal{J}(B_1, t) = (-1)(J(0,0,1)t^1 + J(0,1,1)t^0) = t + 1$. Then the result follows since $B_n = (B_1)^n$. □

Proposition 6.8. *If B_n is the Boolean lattice then*

$$\mathcal{M}(B_n, t) = (t+1)^n (t-1)^{2n}.$$

Proof. Again we first compute $\mathcal{M}(B_1, t)$. The only coefficients are $J(0,0,0) = 1$, $J(0,0,1) = -1$, $J(0,1,1) = -1$ and $J(1,1,1) = 1$. Then the result follows from

$$\begin{aligned}\mathcal{M}(B_1, t) =& J(0,0,0)t^3 + J(0,0,1)t^2 + J(0,1,1)t + J(1,1,1)\\ =& t^3 - t^2 - t + 1\\ =& (t+1)(t-1)^2\end{aligned}$$

and the application of Proposition 6.6. □

Proposition 6.9. *Let $\mathcal{P}_n$ be a geometric lattice of rank two with n atoms (rank 2 matroid with n elements a.k.a. $U_{2,n}$). Then $\mathcal{M}(\mathcal{P}_n, t) = (t^2 - nt + 1)(t+1)^2(t-1)^2$.*

Proof. We prove this by induction on n. The base case is $n = 2$ and is given by the $n = 2$ version of Proposition 6.8. Now assume $n > 2$. The lattice $\mathcal{P}_n$ consists of $\hat{0}$, $\hat{1}$, and n atoms $\alpha_1, \ldots, \alpha_n$. Now $J_{\mathcal{P}_n}(\hat{0}, \hat{0}, \hat{1}) = n - 1$ and $J_{\mathcal{P}_n}(\hat{0}, \hat{1}, \hat{1}) = n - 1$ are the only $J_{\mathcal{P}_n}$ values that do not have α_n as an entry and incorporate α_n in it's recursive definition. So, $J_{\mathcal{P}_n}(\hat{0}, \hat{0}, \hat{1}) = J_{\mathcal{P}_{n-1}}(\hat{0}, \hat{0}, \hat{1}) + 1$ and similarly for $(\hat{0}, \hat{1}, \hat{1})$. Incorporating this difference into the calculation we get that

$$\begin{aligned}\mathcal{M}(\mathcal{P}_n, t) =& \mathcal{M}(\mathcal{P}_{n-1}, t) + t^4 + t^2 + J(\hat{0}, \hat{0}, \alpha_n)t^5 + J(\hat{0}, \alpha_n, \alpha_n)t^4 + J(\hat{0}, \alpha_n, \hat{1})t^3\\ &+ J(\alpha_n, \alpha_n, \alpha_n)t^3 + J(\alpha_n, \alpha_n, \hat{1})t^2 + J(\alpha_n, \hat{1}, \hat{1})t\\ =& (t^2 - (n-1)t + 1)(t+1)^2(t-1)^2 - (t^5 - 2t^3 + t)\\ =& (t^2 - nt + 1)(t+1)^2(t-1)^2\end{aligned}$$

which is the desired formula. □

Now we consider a decomposition of $\mathcal{M}(L, t)$ for a finite lattice L. If L is a finite lattice then L^{op} is the same underlying set as L but with the order reversed (i.e. $x \leq^{\mathrm{op}} y$ in L^{op} if and only if $x \geq y$ in L). Also for $y \in L$ let $L_y = \{x \in L | x \leq y\}$ and $L^y = \{x \in L | x \geq y\}$. Now we can state the result.

Proposition 6.10. *If L is a finite ranked lattice then*

$$\mathcal{M}(L, t) = t^{\mathrm{rk}(L)} \sum_{y \in L} t^{\mathrm{crk}(y)} \chi(L^y, t) \chi((L^{\mathrm{op}})^y, t^{-1}).$$

Proof. First we note that for $x \leq y \in L$ the Möbius function on L^{op} has $\mu^{\mathrm{op}}(y,x) = \mu(x,y)$ and that rank is corank in L^{op}. Then again using Theorem 5.2 we compute

$$\begin{aligned}
\mathcal{M}(L,t) &= \sum_{(x,y,z)\in\mathcal{F}l^3(\mathcal{P})} J(x,y,z)t^{\rho(x,y,z)} \\
&= \sum_{y\in L}\sum_{x\leq y}\sum_{z\geq y} \mu(x,y)\mu(y,z)t^{\mathrm{crk}(x)+\mathrm{crk}(y)+\mathrm{crk}(z)} \\
&= \sum_{y\in L} t^{\mathrm{crk}(y)} \sum_{x\leq y} \mu(x,y)t^{\mathrm{crk}(x)} \sum_{z\geq y} \mu(y,z)t^{\mathrm{crk}(z)} \\
&= \sum_{y\in L} t^{\mathrm{crk}(y)} \chi(L^y,t) \sum_{x\leq y} \mu(x,y)t^{\mathrm{rk}(L)-\mathrm{rk}(x)} \\
&= \sum_{y\in L} t^{\mathrm{crk}(y)} \chi(L^y,t)t^{\mathrm{rk}(L)} \sum_{x\geq^{\mathrm{op}} y} \mu^{\mathrm{op}}(y,x)t^{-\mathrm{rk}(x)} \\
&= t^{\mathrm{rk}(L)} \sum_{y\in L} t^{\mathrm{crk}(y)} \chi(L^y,t)\chi((L^{\mathrm{op}})^y,t^{-1}).
\end{aligned}$$

□

We can use Proposition 6.10 to compute $\mathcal{M}(\mathcal{P},t)$ for cases where $\chi(\mathcal{P},t)$ is well known. Let L_q^n be the modular lattice of all subspaces in $\mathbb{F}_q^n$, a vector space of dimension n over a field with q elements. The Möbius function and the characteristic polynomial of L_q^n are well known.

Proposition 6.11 ([34, Proposition 7.5.3])**.** *In L_q^n we have*

$$\mu(\hat{0},\hat{1}) = (-1)^n q^{\binom{n}{2}}$$

and

$$\chi(L_q^n,t) = \prod_{i=0}^{n-1}(t-q^i).$$

Using this we can get a nice formulation for $\mathcal{M}(L_q^n,t)$. First we need to recall some terminology from q-series. Let

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)\cdots(q-1)}{(q^k-1)\cdots(q-1)\cdot(q^{n-k}-1)\cdots(q-1)}$$

be the q-binomial coefficient (aka Gaussian coefficient). Also, we denote by

$$\begin{bmatrix} n \\ k_1,k_2,\ldots,k_m \end{bmatrix}_q = \begin{bmatrix} n \\ k_1 \end{bmatrix}_q \begin{bmatrix} n-k_1 \\ k_2 \end{bmatrix}_q \cdots \begin{bmatrix} n-(k_1+\cdots k_{m-1}) \\ k_m \end{bmatrix}_q$$

the q-multinomial coefficient. We also use the q-Pochhammer symbol

$$(a;q)_n = \prod_{i=0}^{n-1}(1-aq^i).$$

We use [3] for a general reference for q-series. Using Proposition 6.11 we get the following.

Proposition 6.12. *If L_q^n is the modular lattice of subspaces of $\mathbb{F}_q^n$ then*

$$\mathcal{M}(L_q^n, t) = \sum_{0 \le i \le j \le k \le n} (-1)^{k-i} \begin{bmatrix} n \\ i, j-i, k-j, n-k \end{bmatrix}_q q^{\binom{j-i}{2}+\binom{k-j}{2}} t^{3n-i-j-k}.$$

Proof. Use that $\begin{bmatrix} n \\ k \end{bmatrix}_q$ counts the number of subspaces of dimension k in $\mathbb{F}_q^n$ and apply Theorem 5.2 to J in $\mathcal{M}(L_q^n, t)$ together with Proposition 6.11. □

Now we can reformulate Proposition 6.12 using Proposition 6.10 together with Proposition 6.11 to get a nice identity in q-series.

Proposition 6.13. *If L_q^n is the modular lattice of subspaces of $\mathbb{F}_q^n$, then*

$$\mathcal{M}(L_q^n, t) = t^n \sum_{0 \le k \le n} t^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}_q \prod_{i=0}^{n-k-1} (t - q^i) \prod_{j=0}^{k-1} (t - q^j).$$

It turns out that -1 is a root of $\mathcal{M}(L_q^n, t)$. We need a few results in order to prove this. First we present a formula or q-identity which seems to be a kind of q-generalized binomial theorem (the authors could not find it in the literature). It's interesting that in the odd case the sum trivially collapses but not for the even case.

Lemma 6.14. *If $n > 0$ then*

$$\sum_{k=0}^{n} (-1)^k \begin{bmatrix} n \\ k \end{bmatrix}_q (-1 : q)_{n-k} (-1; q)_k = 0.$$

Proof. Let

$$S(n) = \sum_{k=0}^{n-1} (-1)^k \begin{bmatrix} n \\ k \end{bmatrix}_q \frac{(-1; q)_{n-k} (-1; q)_k}{(-1; q)_n}$$

which is the left hand side up to the $n-1$ term divided by the n^{th} term. Using techniques from [24] and Mathematica [15] we build a recursion for $S(n)$. We compute

$$
\begin{aligned}
(1+q^{n-1})S(n) =& \sum_{k=0}^{n-1}(-1)^k \left(q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q \right) \frac{(-1;q)_{n-k}(-1;q)_k}{(-1;q)_{n-1}} \\
=& \sum_{k=0}^{n-1}(-1)^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q \frac{(-1;q)_{n-k-1}(-1;q)_k}{(-1;q)_{n-1}}(q^k+q^{n-1}) \\
&+ \sum_{k=1}^{n-1}(-1)^k \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q \frac{(-1;q)_{n-k}(-1;q)_k}{(-1;q)_{n-1}} \\
=&(-1)^{n-1}2q^{n-1} + \sum_{k=0}^{n-2}(-1)^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q \frac{(-1;q)_{n-k-1}(-1;q)_k}{(-1;q)_{n-1}}q^k \\
&+ \sum_{k=0}^{n-2}(-1)^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q \frac{(-1;q)_{n-k-1}(-1;q)_k}{(-1;q)_{n-1}}q^{n-1} \\
&+ \sum_{k=0}^{n-2}(-1)^{k+1} \begin{bmatrix} n-1 \\ k \end{bmatrix}_q \frac{(-1;q)_{n-(k+1)}(-1;q)_{k+1}}{(-1;q)_{n-1}} \\
=&(-1)^{n-1}2q^{n-1} + \sum_{k=0}^{n-2}(-1)^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q \frac{(-1;q)_{n-k-1}(-1;q)_k}{(-1;q)_{n-1}}q^k \\
&+ q^{n-1}S(n-1) - \sum_{k=0}^{n-2}(-1)^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q \frac{(-1;q)_{n-k-1}(-1;q)_k}{(-1;q)_{n-1}}(1+q^k) \\
=&(-1)^{n-1}2q^{n-1} + q^{n-1}S(n-1) - S(n-1).
\end{aligned}
$$

Now we prove with induction that $S(n) = (-1)^{n-1}$. First we see that $S(1) = 1$. Then using the recursion above we have

$$(1+q^{n-1})S(n) = (-1)^{n-1}2q^{n-1} - q^{n-1}(-1)^{n-1} + (-1)^{n-1} = (-1)^{n-1}(q^{n-1}+1)$$

which finishes the proof. □

Proposition 6.15. *If L_q^n is the modular lattice of subspaces of $\mathbb{F}_q^n$ then $\mathcal{M}(L_q^n, -1) = 0$.*

Proof. Evaluate the expression in Proposition 6.13 and apply Lemma 6.14. □

Now we can prove the main result of this section.

Theorem 6.16. *If L is a modular geometric lattice (modular matroid) then $\mathcal{M}(L, -1) = 0$.*

Proof. Use the classical result that a modular geometric lattice is product of Boolean and projective spaces (see 12.1 Theorem 4 in [32] or Proposition 6.9.1 in [23]). Then the result follows from Propositions 6.15, 6.8, and 6.6. □

Remark 6.17. The proof of Theorem 6.16 is done in cases. It would be interesting if there was a case free proof just using the modular property.

Remark 6.18. At first when looking at examples of $\mathcal{M}$ on the lattice of flats $L(M)$ of a matroid M it seems that the converse of Theorem 6.16 might be true. As for even the simplest non-modular matroid $U_{3,4}$ has $\mathcal{M}$ polynomial

$$\mathcal{M}(L(U_{3,4}), t) = (t-1)(t^8 - 3t^7 - t^6 + 12t^5 - 2t^4 - 12t^3 + 3t^2 + 5t - 1)$$

which does not have a factor of $(t+1)$. However, the converse is false, but the example seems rather special. Using the SageMath computer algebra system [10] we compute

$$\begin{aligned}\mathcal{M}(L(M^*(K_{3,3})), t) = (t^{10} - 9t^9 + 22t^8 + 12t^7 - 81t^6 + 21t^5 \\ + 69t^4 - 18t^3 - 34t^2 + 15t - 1)(t+1)(t-1)\end{aligned}$$

where $M^*(K_{3,3})$ is the dual matroid of the graphic matroid corresponding to the complete bipartite graph $K_{3,3}$. Since $M^*(K_{3,3})$ is a connected non-modular matroid (it does not have a modular direct summand) this example gives a connected non-modular matroid that has -1 as a root of $\mathcal{M}$. This example and Theorem 6.16 motivate a few questions.

Question 6.19. Is there a rank 3 non-modular connected matroid M such that $\mathcal{M}(M, -1) = 0$?

Question 6.20. Is there a classification of all matroids whose $\mathcal{M}$ polynomial has -1 as a root?

Question 6.21. Is there a nice enumerative combinatorial interpretation for $\mathcal{M}(M, -1)$ where M is a matroid (i.e. what does it count)?

6.1 No Deletion-Contraction

We now show that $\mathcal{J}$ and $\mathcal{M}$ are not some evaluation of the Tutte polynomial for matroids. We first recall the following definition.

Definition 6.22. We say that a function f from matroids to a ring R is a *generalized Tutte-Grothendieck invariant* (following [4] Sec 1.8.6) if there exists $a, b \in R$ such that for every matroid M and element of the ground set $e \in M$

$$f(M) = \begin{cases} f(M\backslash e)f(L) & \text{if } e \text{ is a loop} \\ f(M/e)f(C) & \text{if } e \text{ is a coloop} \\ af(M\backslash e) + bf(M/e) & \text{otherwise.} \end{cases}$$

where L is the matroid consisting of exactly one loop and C is the matroid consisting of exactly one coloop.

Let $U_{r,n}$ be the uniform matroid of rank r on n elements and recall that $U_{r,r} \cong B_r$ are Boolean or free matroids. Then, a direct computation gives $\mathcal{J}(B_1, t) = t + 1$ and

$$\mathcal{J}(U_{2,n}, t) = (n-1)t^2 + nt + n - 1.$$

Hence $J(U_{2,3}, t) = 2t^2 + 3t + 2$. Then any deletion is $U_{2,3}\backslash e \cong B_2$ and any contraction is $U_{2,3}/e \cong U_{1,2}$. Putting this together with Definition 6.22 and assuming that $\mathcal{J}$ is a Tutte-Grothendieck invariant

$$2t^2 + 3t + 2 = a(t^2 + 2t + 1) + b(t+1).$$

However, this is a contradiction since $t+1$ is not a factor of the left hand side.

The same result for $\mathcal{M}$ needs two more steps. Looking at the same matroid and using Proposition 6.9 we get

$$\mathcal{M}(U_{2,3},t) = (t^2-3t+1)(t+1)^2(t-1)^2 = a(t+1)^2(t-1)^4 + b(t+1)(t-1)^2$$

which reduces to

$$b = (t+1)(t^2-3t+1) - a(t+1)(t-1)^2.$$

Then we look at $U_{2,4}$ and again assume $\mathcal{M}$ is a Tutte-Grothendieck invariant

$$\mathcal{M}(U_{2,4},t) = (t^2-4t+1)(t+1)^2(t-1)^2 = a(t^2-3t+1)(t+1)^2(t-1)^2 + b(t+1)(t-1)^2.$$

Inserting the above value for b and reducing we get

$$t^2-4t+1 = a(t^2-3t+1) + (t^2-3t+1) - a(t-1)^2$$

which gives $a=1$ and makes $b=-t(t+1)$. But then

$$\mathcal{M}(U_{3,4},t) = (t-1)(t^8-3t^7-t^6+12t^5-2t^4-12t^3+3t^2+5t-1)$$

which does not have a factor of $t+1$. This is a contradiction since the right hand side

$$\mathcal{M}(U_{3,4}\backslash e,t) - t(t+1)\mathcal{M}(U_{3,4}/e,t) = \mathcal{M}(U_{3,3},t) - t(t+1)\mathcal{M}(U_{2,3},t)$$

does have a $t+1$ factor.

6.2 Valuations

Here we study the invariant $\mathcal{M}$ over matroid subdivisions. One could focus on a wider range combinatorial objects like posets but we are motived by applications to matroid theory. First we recall the basis matroid polytope (using [6] as our general reference for this material). A matroid M can be defined via its set of bases $\mathcal{B}(M)$ which are all the independent sets of M whose size is the rank of M. Then, the matroid polytope of M is

$$P(M) = \text{Conv}\{e_B | B \in \mathcal{B}(M)\}$$

where $e_B = e_{i_1} + \cdots + e_{i_r}$ with $B = \{i_1, \ldots, i_r\}$. Now we need a few key definitions to state our main result.

Definition 6.23. A *matroid polyhedral subdivision* of a matroid polytope $P(M)$ is a collection of polyhedra $\{P_i\}$ such that $\bigcup P_i = P(M)$, each P_i is a matroid polytope whose vertices are vertices of $P(M)$, and for $i \neq j$ if $P_i \bigcap P_j \neq \emptyset$, then $P_i \bigcap P_j$ is a proper face of both P_i and P_j.

Now we want to know how invariants decompose across subdivisions which gives rise to valuations. We will use what is called a weak valuation in [6] but we follow [5] and just say valuation. This makes sense since by Theorem 4.2 in [6] for matroids weak valuations are actually strong valuations.

Definition 6.24. Let $\mathcal{P}$ be the collection of matroid polytopes and R a commutative ring. A function $f\colon \mathcal{P} \to R$ is a (weak) *valuation* if for any matroid polytope $P(M)$ and any matroid polyhedral subdivision with maximal pieces $\{P(M_1), \ldots, P(M_k)\}$ we have that $f(\emptyset) = 0$ and

$$f(P(M)) = \sum_{\{j_1,\ldots,j_i\}\subseteq[k]} (-1)^i f(P(M_{j_1}) \cap \cdots \cap P(M_{j_i})).$$

Finally we can state the result for the invariant $\mathcal{J}$ in terms of valuations.

Proposition 6.25. *The polynomial $\mathcal{J}$ is a valuation on matroids.*

Proof. Using the decomposition of the J-function given in Theorem 5.2 we know that

$$\mathcal{J}(M,t) = (-1)^{\mathrm{rk}(M)} \sum_{X\in L(M)} \mu(\emptyset, X)\mu(X, \hat{1})t^{\mathrm{rk}(X)}$$

where $\hat{1}$ is the maximal flat of M. Hence as a function from the collection of matroids to $\mathbb{Z}[t]$ we can represent the function $\mathcal{J}$ as

$$\mathcal{J} = (\pm 1) \sum f_1 \star f_2$$

where $f_1 \star f_2 = m \circ (f_1 \otimes f_2) \circ \Delta_{S,T}$ from the notation in Theorem C in [6] and $f_1 = \chi_M(0)$ and $f_2 = \chi_M(0)t^{\mathrm{rk}(M)}$. Since f_1 and f_2 are both Tutte-Grothendieck invariants for matroids and are evaluations of the Tutte polynomial we can conclude that f_1 and f_2 are both valuations from Proposition 7.5 in [6]. Finally putting it all together Theorem C in [6] finished the result. □

We conclude with a natural question. The polynomial $\mathcal{M}(L,t)$ is slightly more complicated but has promising properties that seems to imply it should be a valuation.

Question 6.26. Is the polynomial $\mathcal{M}$ a matroid valuation? It seems that Proposition 6.10 with Proposition 7.5 and Theorem C in [6] is essentially the proof. However that would use that the characteristic polynomial on the flipped lattice of flats $L(M)^{op}$ is a matroid valuation.

References

[1] M. Aguiar and F. Ardila, Hopf monoids and generalized permutahedra, 2017, arXiv:1709.075048 [math.CO].

[2] M. Aguiar and S. Mahajan, *Topics in Hyperplane Arrangements*, volume 226 of *Mathematical Surveys and Monographs*, American Mathematical Society, Providence, RI, 2017, doi:10.1090/surv/226, https://doi.org/10.1090/surv/226.

[3] G. E. Andrews, *q-series: Their Development and Application in Analysis, Nnumber Theory, Combinatorics, Physics, and Computer Algebra*, volume 66 of *CBMS Regional Conference Series in Mathematics*, Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1986.

[4] F. Ardila, Algebraic and geometric methods in enumerative combinatorics, in: *Handbook of enumerative combinatorics*, CRC Press, Boca Raton, FL, Discrete Math. Appl., pp. 3–172, 2015.

[5] F. Ardila, A. Fink and F. Rincón, Valuations for matroid polytope subdivisions, *Canad. J. Math.* **62** (2010), 1228–1245, doi:10.4153/cjm-2010-064-9, https://doi.org/10.4153/cjm-2010-064-9.

[6] F. Ardila and M. Sanchez, Valuations and the Hopf monoid of generalized permutahedra, *Int. Math. Res. Not. IMRN* (2023), 4149–4224, doi:10.1093/imrn/rnab355, https://doi.org/10.1093/imrn/rnab355.

[7] C. A. Athanasiadis, Characteristic polynomials of subspace arrangements and finite fields, *Adv. Math.* **122** (1996), 193–233, doi:10.1006/aima.1996.0059, https://doi.org/10.1006/aima.1996.0059.

[8] J. Bastidas, *Species and hyperplane arrangements*, Ph.D. thesis, Cornell University, 2021.

[9] A. Cameron and A. Fink, The Tutte polynomial via lattice point counting, *J. Comb. Theory Ser. A* **188** (2022), Paper No. 105584, doi:10.1016/j.jcta.2021.105584, https://doi.org/10.1016/j.jcta.2021.105584.

[10] T. S. Developers, *Sage Mathematics Software (Version 8.1)*, 2020, http://www.sagemath.org.

[11] C. Dupont, A. Fink and L. Moci, Universal Tutte characters via combinatorial coalgebras, *Algebr. Comb.* **1** (2018), 603–651, doi:10.5802/alco, https://doi.org/10.5802/alco.

[12] B. Elias, N. Proudfoot and M. Wakefield, The Kazhdan-Lusztig polynomial of a matroid, *Adv. Math.* **299** (2016), 36–70, doi:10.1016/j.aim.2016.05.005, https://doi.org/10.1016/j.aim.2016.05.005.

[13] P. Hall, A Contribution to the Theory of Groups of Prime-Power Order, *Proc. London Math. Soc. (2)* **36** (1934), 29–95, doi:10.1112/plms/s2-36.1.29, https://doi.org/10.1112/plms/s2-36.1.29.

[14] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford, sixth edition, 2008.

[15] W. R. Inc., Mathematica, Version 12.3.1, Champaign, IL, 2021, https://www.wolfram.com/mathematica.

[16] S. A. Joni and G.-C. Rota, Coalgebras and bialgebras in combinatorics, *Stud. Appl. Math.* **61** (1979), 93–139, doi:10.1002/sapm197961293, https://doi.org/10.1002/sapm197961293.

[17] R. Jurrius, Relations between Möbius and coboundary polynomials, *Math. Comput. Sci.* **6** (2012), 109–120, doi:10.1007/s11786-012-0117-6, https://doi.org/10.1007/s11786-012-0117-6.

[18] T. Krajewski, I. Moffatt and A. Tanasa, Hopf algebras and Tutte polynomials, *Adv. in Appl. Math.* **95** (2018), 271–330, doi:10.1016/j.aam.2017.12.001, https://doi.org/10.1016/j.aam.2017.12.001.

[19] J. L. Martin, Lecture notes on algebraic combinatorics, 2012 .

[20] A. F. Möbius, Über eine besondere Art von Umkehrung der Reihen, *J. Reine Angew. Math.* **9** (1832), 105–123, doi:10.1515/crll.1832.9.105, https://doi.org/10.1515/crll.1832.9.105.

[21] W. Murray, Möbius polynomials, *Math. Mag.* **85** (2012), 376–383, doi:10.4169/math.mag.85.5.376, https://doi.org/10.4169/math.mag.85.5.376.

[22] P. Orlik and H. Terao, *Arrangements of Hyperplanes*, volume 300 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*, Springer-Verlag, Berlin, 1992, doi:10.1007/978-3-662-02772-1, https://doi.org/10.1007/978-3-662-02772-1.

[23] J. Oxley, *Matroid Theory*, volume 21 of *Oxford Graduate Texts in Mathematics*, Oxford University Press, Oxford, 2nd edition, 2011, doi:10.1093/acprof:oso/9780198566946.001.0001, https://doi.org/10.1093/acprof:oso/9780198566946.001.0001.

[24] P. Paule and A. Riese, A Mathematica q-analogue of Zeilberger's algorithm based on an algebraically motivated approach to q-hypergeometric telescoping, in: *Special functions, q-series and related topics (Toronto, ON, 1995)*, Amer. Math. Soc., Providence, RI, volume 14 of *Fields Inst. Commun.*, pp. 179–210, 1997.

[25] G. Pilz, *Near-Rings*, volume 23 of *North-Holland Mathematics Studies*, North-Holland Publishing Co., Amsterdam, 2nd edition, 1983, the theory and its applications.

[26] G.-C. Rota, On the foundations of combinatorial theory. I. Theory of Möbius functions, *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **2** (1964), 340–368 (1964), doi:10.1007/bf00531932, https://doi.org/10.1007/bf00531932.

[27] E. Spiegel and C. J. O'Donnell, *Incidence Algebras*, volume 206 of *Monographs and Textbooks in Pure and Applied Mathematics*, Marcel Dekker, Inc., New York, 1997.

[28] R. P. Stanley, *Enumerative Combinatorics. Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, 2nd edition, 2012.

[29] H. Terao, Free arrangements of hyperplanes and unitary reflection groups, *Proc. Japan Acad. Ser. A Math. Sci.* **56** (1980), 389–392, http://projecteuclid.org/euclid.pja/1195516722.

[30] M. Wakefield, Partial flag incidence algebras, 2022, arXiv:1605.01685 [math.CO].

[31] L. Weisner, Abstract theory of inversion of finite series, *Trans. Am. Math. Soc.* **38** (1935), 474–484, doi:10.2307/1989808, https://doi.org/10.2307/1989808.

[32] D. J. A. Welsh, *Matroid Theory*, Academic Press [Harcourt Brace Jovanovich, Publishers], London-New York, 1976, l. M. S. Monographs, No. 8.

[33] T. Zaslavsky, Facing up to arrangements: face-count formulas for partitions of space by hyperplanes, *Mem. Am. Math. Soc.* **1** (1975), vii+102.

[34] T. Zaslavsky, The Möbius function and the characteristic polynomial, in: *Combinatorial Geometries*, Cambridge Univ. Press, Cambridge, volume 29 of *Encyclopedia Math. Appl.*, pp. 114–138, 1987.

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 24 (2024) #P2.04 / 231–271
https://doi.org/10.26493/1855-3974.2968.d23
(Also available at http://amc-journal.eu)

Valuations and orderings on the real Weyl algebra

Lara Vukšić *

Institute of Mathematics, Physics, and Mechanics, Ljubljana, Slovenia and
Faculty of Mathematics and Physics, University of Ljubljana, Slovenia

Received 19 September 2022, accepted 12 February 2023, published online 20 September 2023

Abstract

The first Weyl algebra $\mathcal{A}_1(k)$ over a field k is the k-algebra with two generators x, y subject to $[y, x] = 1$ and was first introduced during the development of quantum mechanics. In this article, we classify all valuations on the real Weyl algebra $\mathcal{A}_1(\mathbb{R})$ whose residue field is $\mathbb{R}$. We then use a noncommutative version of the Baer-Krull theorem to classify all orderings on $\mathcal{A}_1(\mathbb{R})$. As a byproduct of our studies, we settle two open problems in real algebraic geometry. First, we show that not all orderings on $\mathcal{A}_1(\mathbb{R})$ extend to an ordering on a larger ring $R[y; \delta]$, where R is the ring of Puiseux series, introduced by Marshall and Zhang in 2000, and characterize the orderings that do have such an extension. Second, we show that for valuations on noncommutative division rings, Kaplansky's theorem that extensions by limits of pseudo-Cauchy sequences are immediate fails in general.

Keywords: Weyl algebra, noncommutative valuations, skew polynomial rings, orderings, extensions of valuations, extensions of orderings.

Math. Subj. Class. (2020): 16W60, 06F25, 13J30, 14A22, 16S3

1 Introduction

Valuation theory was first developed for commutative fields in the context of number theory and was first defined by József Kürschák [12] in 1913. For modern treatments, we refer to the books of Engler and Prestel [5] or Kuhlmann [10]. Oscar Schilling wrote the first major work on valuations on (noncommutative) division rings in 1945 [21].

A valuation on a division ring D is a map $v\colon D \to \Gamma \cup \{\infty\}$, where Γ is an ordered group written additively and $\infty \notin \Gamma, \infty > \gamma$ for each $\gamma \in \Gamma$, with the following properties:

*I would like to thank my advisor Igor Klep for his guidance and many helpful comments and suggestions.
E-mail address: lara.vuksic@fmf.uni-lj.si (Lara Vukšić)

1. $\forall x \in D : v(x) = \infty \Leftrightarrow x = 0$,
2. $\forall x, y \in D : v(xy) = v(x) + v(y)$,
3. $\forall x, y \in D : v(x + y) \geq \min\{v(x), v(y)\}$.

It follows that v is a homomorphism from D^* to Γ. The set $\mathcal{O}_v := \{x \in D \mid v(x) \geq 0\}$ is called the valuation ring associated to v, and $\mathcal{M}_v := \{x \in M \mid v(x) > 0\}$ is its maximal ideal. The division ring $\overline{D} := \mathcal{O}_v/\mathcal{M}_v$ is called the associated residue division ring. Since v is a group homomorphism, the subgroup $\mathcal{O}_v^*$ is normal in D^*. Several alternative approaches to noncommutative valuations, where v does not define a group homomorphism, were introduced and studied recently by Nicolai Ivanovich Dubrovin in [7] and [4] (see also [17] for a more thorough treatment), and by Jean-Pierre Tignol and Adrien Wadsworth in [23].

Suppose F is a field. Then all valuations on the field or rational functions $F(x)$ with residue field F are well-known, namely, the p-adic valuations for irreducible polynomials $p(x) \in F[x]$, and the $v_{\deg}$ valuation, defined by

$$v_{\deg}(\frac{p}{q}) := \deg(q) - \deg(p).$$

The description of all valuations on the field of rational functions in several variables with residue field equal to the base field is much more involved. There are many descriptions of constructions of such valuations in the literature. Among famous examples of such descriptions are the one given by Saunders MacLane in [13] and the one given by Franz-Viktor Kuhlmann in [11].

As valuations on Ore extensions uniquely extend to their quotient division ring, the description of all valuations on Ore division rings is equivalent to the description of all valuations on corresponding quotient division rings. The description of all valuations on noncommutative Ore extensions $R[x; \sigma, \delta]$ where R is a domain, $\sigma\colon R \to R$ is a ring homomorphism and $\delta\colon R \to R$ a σ-derivation is even more complex than in the commutative case. Additional difficulties arise from the fact that $[f, g] = 0$ does not hold for all $f, g \in R[x; \sigma, \delta]$. Granja, Martínez, and Rodríguez have shown in [6] that the set of all real valuations extending to the skew polynomial ring has the structure of a parameterized complete non-metric tree. Further recent progress on valuations on Ore extensions is given by Onay in [18] and Rohwer in his PhD thesis [20].

1.1 Results

Our main goal is to classify all orderings and real valuations on the real Weyl algebra $\mathcal{A}_1(\mathbb{R})$ or, equivalently, its quotient division ring $\mathcal{D}_1(\mathbb{R})$. The Weyl algebra is the noncommutative algebra generated by two elements x, y satisfying $[y, x] = 1$. Hence its elements are all of the form

$$\sum_{i,j} \alpha_{i,j} x^i y^j,\ \alpha_{i,j} \in \mathbb{R}.$$

Because of this, our approach to constructing valuations on $\mathcal{A}_1(\mathbb{R})$ is inspired by classical constructions of valuations on commutative rational functions in two unknowns mentioned above. However, the relation $[y, x] = 1$ gives rise to additional constraints and far fewer valuations than in the commutative case.

As we will show, the valuations on $\mathcal{A}_1(\mathbb{R})$ we are interested in all satisfy $v[a,b] > v(ab)$ for all nonzero a, b. We call such valuations *strongly abelian*. They have an abelian value group and commutative residue field. In Section 2 we give some properties of strongly abelian valuations. We show that if a valuation v on a division ring D satisfies $\overline{D} = \overline{Z(D)}$ and the value group is of rational rank one, then v is strongly abelian. Under additional constraints on the residue field and the value group we extend this statement to valuations of higher rational rank.

In Section 3 we give a characterization of all valuations v on the real Weyl algebra $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$ in the spirit of MacLane [13]. The construction is inspired by the outline given by Shtipelman in [22] for valuations on the complex Weyl algebra $\mathcal{A}_1(\mathbb{C})$. We also explicitly describe the associated value groups and show that they are all isomorphic to subgroups of $\mathbb{Q}$ or $\mathbb{Q} \times \mathbb{Z}$.

In their attempt to describe all orderings on $\mathcal{A}_1(\mathbb{R})$ in [16], Murray Marshall and Yufei Zhang introduced the Ore extensions $R[y;\delta]$ and $\tilde{R}[y;\delta]$, with

$$R := \{\sum_{k \geq m} a_k x^{-\frac{k}{n}} \mid a_k \in \mathbb{R}, m \in \mathbb{Z}, n \in \mathbb{N}\},$$
$$\tilde{R} := \{\sum_{q \in A} a_q x^{-q} \mid A \subset \mathbb{Q} \text{ is well-ordered}\}$$

and $\delta(p(x)) = p'(x)$. As is often done in real algebraic geometry, all orderings are described by classifying all real valuations via the Baer-Krull theorem. Marshall and Zhang described *almost* all valuations v on $R[y;\delta]$ with residue field $\mathbb{R}$; in one case, they did not prove that v is a valuation. In Section 4, we complete their characterization. Marshall and Zhang also conjectured that all valuations on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$ extend to a valuation on $R[y;\delta]$ with the same residue field. We refute their conjecture in Section 4. Further, we combine our classification of valuations on $\mathcal{A}_1(\mathbb{R})$ with Marshall and Zhang's description of valuations on $R[y;\delta]$ to characterize the valuations on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$ that extend to a valuation $R[y,\delta]$ with the same residue field. All such extensions are again strongly abelian.

In Section 5, we show that all valuations on $R[y;\delta]$ with residue field $\mathbb{R}$ uniquely extend to a strongly abelian valuation on $\tilde{R}[y;\delta]$ with the same residue field. We also show that the value group of such an extension is not of rational rank one.

As a byproduct of our investigations, we show that Kaplansky's theorem that all extensions by limits of pseudo-Cauchy sequences are immediate (in particular, they do not change the rational rank of the value group) fails for noncommutative division rings.

As Marshall and Zhang observe in [15], all strongly abelian valuations v on a division ring D with a formally real residue field are compatible with an order on D. In Section 6, we describe all v-compatible orders on $\mathcal{A}_1(\mathbb{R})$ for every valuation v on $\mathcal{A}_1(\mathbb{R})$ constructed in Section 3 using a noncommutative version of the Baer-Krull theorem as given in [2] (see also [1, 3, 24] and [9] for modern treatments and extensions). We also characterize the v-compatible orders on $\mathcal{A}_1(\mathbb{R})$ that extend to an order on $R[y;\delta]$ compatible with v's extension to $R[y;\delta]$.

2 Strongly abelian valuations

We present some properties of valuations on noncommutative division rings which we will use later to describe order-compatible valuations on the real Weyl algebra $\mathcal{A}_1(\mathbb{R})$ and some of its ring extensions. First, we define a property of valuations on division rings.

Definition 2.1. Suppose v is a valuation on a division ring D. We say v is *strongly abelian* if $v[a,b] > v(ab)$ holds for all nonzero $a, b \in D$.

Any valuation on a field is strongly abelian. In this section, we describe a sufficient condition for a valuation v to be strongly abelian. This property will be important for us for two reasons. Firstly, it is obvious that if a valuation v on a division ring D is strongly abelian, then the associated value group and residue division ring are commutative. Secondly, we are particularly interested in order-compatible valuations on $\mathcal{A}_1(\mathbb{R})$; minimal such have residue field $\mathbb{R}$, as it was shown in [16]. It follows from Theorem 2.5 of [15] that a strongly abelian valuation v on a division ring D with a formally real residue field is compatible with an order on D by the noncommutative version of the Baer-Krull theorem as given in [24].

Proposition 2.2. *Let v be a valuation on a division ring D such that $\overline{D} = \overline{Z(D)}$. Let $a, b \in D^*$ be such that $v(a)$ and $v(b)$ are rationally dependent. Then $v[a,b] > v(ab)$.*

Proof. Since $v(a)$ and $v(b)$ are rationally dependent, $v(ab) = v(ba) \leq v[a,b]$. Suppose $v[a,b] = v(ab)$. In particular, a and b do not commute. Let $\beta := \overline{aba^{-1}b^{-1}} \in \overline{D}$. We have

$$\beta = \overline{aba^{-1}b^{-1}} = \overline{([a,b]+ba)a^{-1}b^{-1}} = \overline{[a,b]a^{-1}b^{-1}+1} \neq 1.$$

Let $v(b) = -\frac{\ell}{k}v(a)$ for $\ell, k \in \mathbb{Z}$, ℓ and k coprime. It follows that $v[a,b] = \frac{k-\ell}{k}v(a)$. Define $\gamma := \overline{(ba)^k a^{\ell-k}} \in \overline{D}$. Let $\beta', \gamma' \in Z(D)$ be such that $v(\beta') = v(\gamma') = 0$, $\overline{\beta'} = \beta$ and $\overline{\gamma'} = \gamma$. Then on one hand,

$$v(a(ba)^k - \gamma' a^{k-\ell+1}) = v(a((ba)^k a^{\ell-k} - \gamma')a^{k-\ell}) > (k-\ell+1)v(a),$$

and on the other,

$$\begin{aligned} v(a(ba)^k - \gamma' a^{k-\ell+1}) &= v((ab)^k a - \gamma' a^{k-\ell+1}) = v(((ab)^k a^{\ell-k} - \gamma')a^{k-\ell+1}) \\ &= (k-\ell+1)v(a) \end{aligned}$$

since

$$\overline{(ab)^k a^{\ell-k} - \gamma'} = \overline{(aba^{-1}b^{-1}ba)^k a^{\ell-k}} - \gamma = \beta^k \overline{(ba)^k a^{\ell-k}} - \gamma \neq 0.$$

In the last equation, we used that $\overline{(aba^{-1}b^{-1}ba)^k a^{\ell-k}} = \overline{(\beta' ba)^k a^{\ell-k}} = \overline{\beta'^k (ba)^k a^{\ell-k}} = \beta^k \overline{(ba)^k a^{\ell-k}}$ since $\overline{D} = \overline{Z(D)}$ as presumed. This holds if $\beta^k \neq 1$. If $\beta^k = 1$, we repeat our calculations with roles of a and b interchanged. The new β will now be the inverse value of the former and since $\gcd(\ell, k) = 1$, $\beta^{-\ell} \neq 1$. In either case, we get a contradiction from which we deduce $v[a,b] > v(ab)$. □

Remark 2.3. The condition $\overline{D} = \overline{Z(D)}$ is fulfilled by every valuation on an algebra over a field that is isomorphic to the residue field. In particular, this holds for minimal order-compatible valuations on $\mathbb{R}$-algebras.

Corollary 2.4. *Let v be a valuation on a division ring D such that $\overline{D} = \overline{Z(D)}$. If the value group has rational rank one, then v is strongly abelian.*

Lemma 2.5. *Let v be a valuation on a division ring D such that the value group is abelian and $\overline{D} = \overline{Z(D)}$. Then for all $x, y \in D \setminus \{0\}$:*

(1) *If $v[x,y] > v(xy)$, then $v[x^m, y] > v(x^m y)$ for all $m \in \mathbb{Z}$.*

(2) *Suppose $v[x,y] = v(xy)$. Then $v[x^{-1}, y] = v(x^{-1}y)$ and for each $m \in \mathbb{N}$, $v[x^m, y] > v(x^m y)$ holds if and only if $\alpha := y^{-1}x^{-1}yx$ satisfies $1 + \overline{\alpha} + \cdots + \overline{\alpha}^{m-1} = 0$ in $\overline{D}$.*

Proof. To prove (1), first observe

$$[x^{-1}, y] = x^{-1}y - yx^{-1} = x^{-1}(yx - xy)x^{-1},$$

so if $v[x,y] > v(x,y)$, then

$$v[x^{-1}, y] = v[x,y] - 2v(x) > v(xy) - 2v(x) = v(x^{-1}y).$$

Suppose $m \in \mathbb{N}$. Then

$$[x^m, y] = \sum_{\ell=1}^{m} x^{m-\ell}[x,y]x^{\ell-1}$$

and since the value group is commutative, $v(x^{m-\ell}[x,y]x^{\ell-1}) = (m-1)v(x) + v[x,y] > v(x^m y)$ for each $1 \leq \ell \leq m$. Item (1) is thus proved.

To prove (2), suppose $v[x,y] = v(xy)$. Then $v[x^{-1}, y] = v(x^{-1}y)$ is proved as for the first case. Since the value group is abelian, $v[x^m, y] \geq v(x^m y)$ holds, so we can observe

$$\overline{y^{-1}x^{-m}[x^m, y]} = \overline{y^{-1}x^{-m}\sum_{\ell=1}^{m} x^{m-\ell}[x,y]x^{\ell-1}} = \sum_{\ell=1}^{m} \overline{y^{-1}x^{-\ell}[x,y]x^{\ell-1}}.$$

For each $1 \leq \ell \leq m$,

$$\begin{aligned}\overline{y^{-1}x^{-\ell}[x,y]x^{\ell-1}} &= \overline{(\alpha x^{-1})^{\ell-1}y^{-1}x^{-1}[x,y]x^{\ell-1}} \\ &= \overline{\alpha^{\ell-1}x^{-\ell+1}y^{-1}x^{-1}[x,y]x^{\ell-1}} = \overline{y^{-1}x^{-1}[x,y]\alpha^{\ell-1}}.\end{aligned}$$

We can change the order of α and x^{-1} by Proposition 2.2 since $v(\alpha) = 0$. The last equation follows from $v(y^{-1}x^{-1}[x,y]) = 0$ and Proposition 2.2. So now we have

$$\overline{y^{-1}x^{-m}[x^m, y]} = \overline{y^{-1}x^{-1}[x,y]}\sum_{\ell=0}^{m-1} \alpha^{\ell},$$

which proves the equivalence in (2). □

Proposition 2.6. *Let v be a valuation on a division ring D such that the value group is abelian and $\overline{D} = \overline{Z(D)}$. Suppose the residue field is formally real and suppose $v[x,y] = v(xy)$ for some $x, y \in D$. Then $v[x^m, y] = v(x^m y)$ for all odd $m > 2$. If $v[x^m, y] > v(x^m y)$ for some even m, then $v[x^2, y] > v(x^2 y)$ and there is no $a \in D$ such that $v(a^2) = v(x)$.*

Proof. Suppose $v[x,y] = v(xy)$. If m is odd, $\sum_{\ell=0}^{m-1} \overline{\alpha}^{\ell} = 0$ does not have a solution in the residue field. By Lemma 2.5, it follows that $v[x^m, y] = v(x^m y)$. Now consider the case for even m. If $v[x^m, y] > v(x^m y)$, then $\overline{\alpha} = -1$ by Lemma 2.5 and $v[x^2, y] > v(x^2 y)$. Suppose $a \in D$ satisfies $v(a^2) = v(x)$. We will first show that $v[a^2, y] = v(a^2 y)$. Assume that $v[a^2, y] > v(a^2 y)$. Then on one hand,

$$\overline{a^{-2}x} = \overline{a^{-2}xy^{-1}y} = \overline{y^{-1}a^{-2}xy},$$

since $v(a^{-2}x) = 0$. On the other hand,

$$\overline{a^{-2}x} = \overline{y^{-1}ya^{-2}x} = \overline{y^{-1}a^{-2}yx},$$

where the last equation follows from $v[a^2, y] > v(a^2 y)$, or, by Lemma 2.5 equivalently, $v[a^{-2}, y] > v(a^{-2}y)$. From $\overline{x^{-1}a^{-2}(xy - yx)} = 0$ we conclude $v[x,y] > v(xy)$, which is a contradiction. So $v[a^2, y] = v(a^2 y)$ and $v[a, y] = v(ay)$ follows from Lemma 2.5. Now we show $v[a^4, y] > v(a^4 y)$. On one hand, we can write

$$\overline{a^{-4}x^2} = \overline{y^{-1}a^{-4}x^2 y} = \overline{y^{-1}a^{-4}yx^2}$$

since $v[x^2, y] > v(x^2 y)$. On the other hand,

$$\overline{a^{-4}x^2} = \overline{y^{-1}ya^{-4}x^2},$$

so we conclude $v[a^4, y] > v(a^4 y)$. But by Lemma 2.5, $v[a^4, x] > v(a^4 x)$ gives us $\overline{xax^{-1}a^{-1}} = -1$. But then, again by Lemma 2.5, $v[a^2, x] > v(a^2 x)$. The proposition is thus proved. □

Proposition 2.7. *Let v be a valuation on a division ring D such that such that $\overline{D} = \overline{Z(D)}$, the value group is abelian and 2-divisible and the residue field is formally real. Suppose the value group of v is of rational rank 2 and suppose there are $x, y \in D^*$ such that $v(x)$ and $v(y)$ are rationally independent with $v[x,y] > v(xy)$. Then v is strongly abelian.*

Proof. Suppose $a, b \in D$. Since the value group is abelian, $v[a,b] \geq v(ab)$. Suppose $v[a,b] = v(ab)$. Then $v(a^{k_1}) = v(x^{-m_1}y^{-n_1})$ and $v(b^{k_2}) = v(x^{-m_2}y^{-n_2})$ for some $k_i, m_i, n_i \in \mathbb{Z}$, $i = 1, 2$. We conclude from Lemma 2.5 that $v[a^{k_1}, b^{k_2}] = v(a^{k_1}b^{k_2})$. This is immediate if k_1 and k_2 are both odd. If k_1 or k_2 is even, $v[a^{k_1}, b^{k_2}] = v(a^{k_1}b^{k_2})$ follows from the 2-divisibility of the value group and Proposition 2.6. Let $c := x^{m_1}y^{n_1}$ and $d := x^{m_2}y^{n_2}$. Then on the one hand,

$$\overline{a^{k_1}cb^{k_2}d} = \overline{ca^{k_1}db^{k_2}} = \overline{dca^{k_1}b^{k_2}}$$

since $v(a^{k_1})$ and $v(c)$ are rationally dependent, $v(b^{k_2})$ and $v(d)$ are rationally dependent and $v(b^{k_2}d) = v(a^{k_1}c) = 0$. On the other hand,

$$\overline{a^{k_1}cb^{k_2}d} = \overline{b^{k_2}da^{k_1}c} = \overline{db^{k_2}ca^{k_1}} = \overline{cdb^{k_2}a^{k_1}} = \overline{dcb^{k_2}a^{k_1}}.$$

Here, the last equality follows from $v[x,y] > v(xy)$ and Lemma 2.5. Thus we have $v(dc(a^{k_1}b^{k_2} - b^{k_2}a^{k_1})) > 0$, so we get $v[a^{k_1}, b^{k_2}] > v(a^{k_1}b^{k_2})$ which contradicts our assumption $v[a,b] = v(a,b)$. We conclude $v[a,b] > v(ab)$. □

The proof of the following proposition is the same as the proof of Proposition 2.7.

Proposition 2.8. *Let v be a valuation on a division ring D such that $\overline{D} = \overline{Z(D)}$, the value group is abelian and the residue field is formally real. Suppose the value group of v is of rational rank 2 and suppose there are $x, y \in D^*$ such that for every $z \in D$, $v(z^k) = v(x^{-m}y^{-n})$ holds for some $k, m, n \in \mathbb{Z}$ where k is odd. Then v is strongly abelian.*

We will later use this result to show that all valuations v on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$ are strongly abelian. Propositions 2.7 and 2.8 can be easily generalized to higher rational ranks of the value group. The proofs are analogous.

Corollary 2.9. *Let v be a valuation on a division ring D such that $\overline{D} = \overline{Z(D)}$. Suppose the value group is abelian and 2-divisible of rational rank n and that there are $x_1, \ldots, x_n \in D$ such that $v(x_1), \ldots, v(x_n)$ are rationally independent with $v[x_i, x_j] > v(x_i x_j)$ for all i, j. Then v is strongly abelian.*

Corollary 2.10. *Let v be a valuation on division ring D such that $\overline{D} = \overline{Z(D)}$. Suppose the value group is abelian and of rational rank n and that there are $x_1, \ldots, x_n \in D$ such that for every $z \in D$, $v(z^k) = v(x_1^{m_1} \cdots x_n^{m_n})$ for some $k, m_1, \ldots, m_n \in \mathbb{Z}$ with k odd. Then v is strongly abelian.*

3 Valuations on $\mathcal{A}_1(\mathbb{R})$

We now describe the construction of all valuations on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$ that was sketched in [22] over the ground field of $\mathbb{C}$. Since every $f \in \mathcal{A}_1(\mathbb{R})$ can be written as $\sum_{m,n\geq 0} \alpha_{m,n} x^m y^n$, the construction will be similar to the construction of all valuations on the field of rational functions $\mathbb{R}(x, y)$ with residue field $\mathbb{R}$ (examples of constructions of such valuations can be found in [11] or [13]), but with some additional constraints arising from the fact that the generators $x, y \in \mathcal{A}_1(\mathbb{R})$ satisfy $[y, x] = 1$. We first note that it follows from Theorem 5.3 of [16] that the value group of any valuation on $\mathcal{A}_1(\mathbb{R})$ is commutative. Also, since every valuation v on $\mathcal{A}_1(\mathbb{R})$ can be uniquely extended to its quotient division ring $\mathcal{D}_1(\mathbb{R})$, our construction will take place in the quotient ring as we will use inverses.

To construct a valuation v trivial on $\mathbb{R}$ with residue field $\mathbb{R}$, we compare $v(x)$ and $v(y)$. It is easy to show, as it was done in [16], that $v(xy) = v(yx) < 0$, so $v(x)$ or $v(y)$ will be less than zero. Without loss of generality, we can set $v(x) = -1 \in \mathbb{Q}$ and compare it to $v(y)$. If $v(y) \notin \mathbb{Q}$, then we get

$$v(\sum_{m,n\geq 0} \alpha_{m,n} x^m y^n) = \min_{m,n}\{mv(x) + nv(y)\}$$

for all elements of $\mathcal{A}_1(\mathbb{R})$. Otherwise, $v(y) = \frac{m_1}{n_1} \in \mathbb{Q}$. It follows that $\overline{x^{m_1} y^{n_1}} = \beta_1 \in \mathbb{R}$, so $v(x^{m_1} y^{n_1} - \beta_1) > 0$. Set

$$\omega_1 := x^{m_1} y^{n_1} - \beta_1$$

and as before compare $v(\omega_1)$ to $v(x)$ in terms of rational dependence. If $v(\omega_1) = \frac{m_2}{n_2} \in \mathbb{Q}$, then $\overline{x^{m_2} \omega_1^{n_2}} = \beta_2$ for some $\beta_2 \in \mathbb{R}$. Hence

$$\omega_2 := x^{m_2} \omega_1^{n_2} - \beta_2$$

also has value greater than zero. We continue this procedure. If we additionally define $\omega_{-1} = x$ and $\omega_0 = y$, we thus get a sequence

$$(\omega_i)_{i\geq -1}, \omega_i \in \mathcal{A}_1(\mathbb{R})$$

which ends with ω_n for some $n \in \mathbb{N}$ if $v(\omega_n) \notin \mathbb{Q}$ or is infinite otherwise.

By the end of this section, we will prove a necessary and sufficient condition for the possibility to extend v from $(\omega_i)_{i\geq -1}$ to a valuation on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$. Every such extension from $(\omega_i)_{i\geq -1}$ to $\mathcal{A}_1(\mathbb{R})$ will be uniquely determined. We will also show that every valuation on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$ is strongly abelian.

3.1 Properties of the sequence $(\omega_i)_{i\geq -1}$ associated to a valuation on $\mathcal{A}_1(\mathbb{R})$

Thorough this subsection let v be a valuation on $\mathcal{A}_1(\mathbb{R})$.

Lemma 3.1. *Suppose $(\omega_i)_{i\geq -1} \subseteq \mathcal{A}_1(\mathbb{R})$ is a sequence as described above, with $\omega_{-1} = x$, $\omega_0 = y$, $\omega_i = x^{m_i}\omega_{i-1}^{n_i} - \beta_i$ for all $i \geq 0$. Then $[\omega_i, x]$ equals*

$$x^{m_i}\sum_{\ell_i=1}^{n_i}\omega_{i-1}^{n_i-\ell_i}\Bigg(x^{m_{i-1}}\sum_{\ell_{i-1}=1}^{n_{i-1}}\omega_{i-2}^{n_{i-1}-\ell_{i-1}} \Bigg(\cdots\Bigg(x^{m_2}\sum_{\ell_2=1}^{n_2}\omega_1^{n_2-\ell_2}n_1x^{m_1}y^{n_1-1}\omega_1^{\ell_2}\Bigg)\omega_2^{\ell_3}\Bigg)\cdots\Bigg)\omega_{i-1}^{\ell_i}$$

for each $i \geq 1$.

Proof. We prove the lemma by induction on i. If $i = 1$,

$$[\omega_1, x] = [x^{m_1}y^{n_1} - \beta_1, x] = x^{m_1}\sum_{\ell_1=1}^{n_1} y^{n_1-\ell_1}[y, x]y^{\ell_1-1} = n_1x^{m_1}y^{n_1-1}.$$

Now suppose that the equality holds for $[\omega_i, x]$. Then we have

$$\begin{aligned}[\omega_{i+1}, x] &= [x^{m_{i+1}}\omega_i^{n_{i+1}} - \beta_{i+1}, x] = x^{m_{i+1}}[\omega_i^{n_{i+1}}, x]\\ &= x^{m_{i+1}}\sum_{\ell_{i+1}=1}^{n_{i+1}}\omega_i^{n_{i+1}-\ell_{i+1}}[\omega_i, x]\omega_i^{\ell_{i+1}-1}\end{aligned}$$

We can then proceed by the induction hypothesis. □

Before proving the next lemma, we define an equivalence relation between nonzero elements of $\mathcal{A}_1(\mathbb{R})$ that have the same v-value, but their difference does not. For any $a, b \in \mathcal{A}_1(\mathbb{R}) \setminus \{0\}$, we write $a \sim b$ if $v(a) = v(b) < v(a - b)$. This is also a congurence relation, as $ac \sim bc$ and $ca \sim cb$ holds for all $a, b, c \in \mathcal{A}_1(\mathbb{R}) \setminus \{0\}$ with $a \sim b$.

Lemma 3.2. *Suppose v is a valuation on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$ and suppose $(\omega_i)_{i\geq -1}$ is a sequence such that $\omega_{-1} = x$, $\omega_0 = y$, $\omega_i = x^{m_i}\omega_{i-1}^{n_i} - \beta_i$, $v(x) = -1$ and $v(\omega_i) = \frac{m_{i+1}}{n_{i+1}}$ for all $i \geq 0$ up to either some $n \geq 0$ in which case $v(\omega_n) \notin \mathbb{Q}$, or up to infinity. Then $v[\omega_j, \omega_i] > v(\omega_i\omega_j)$ for all $i, j \leq k$ if and only if $v(\Pi_{\ell=-1}^{k}\omega_\ell) < 0$, where $k \leq n$ in case $v(\omega_n) \notin \mathbb{Q}$ for some $n \geq 0$.*

If any and hence both sides of the equivalence hold, then

$$v[\omega_j, \omega_i] = -v(xy\omega_1 \cdots \omega_{i-1}\omega_{i+1} \cdots \omega_{j-1})$$

for all $i < j \leq k$.

Proof. Suppose v is a valuation on $\mathcal{A}_1(\mathbb{R})$ and $(\omega_i)_{i\geq -1}$ is a sequence as described in the lemma. So $v(\omega_i) \in \mathbb{Q}$ either for all $i \geq 0$ or for all $0 \leq i < n$ for some $n \geq 0$ and $v(\omega_n) \notin \mathbb{Q}$. It follows from Proposition 2.2 that $v[\omega_i, \omega_j] > v(\omega_i\omega_j)$ for all $i, j < n$ since $v(\omega_i)$ and $v(\omega_j)$ are rationally dependent. We shall use this fact to evaluate $v[\omega_i, \omega_j]$ for all $i, j \leq k \leq n$. It follows from Lemma 3.1 that $[\omega_k, x]$ is a sum of products P, all equal to $y^{n_1-1}x^{m_1}\omega_1^{n_2-1}x^{m_2} \cdots \omega_{k-1}^{n_k-1}x^{m_k}$ up to the order of factors. Since $v[\omega_i, \omega_j] > v(\omega_i\omega_j)$ for all $i, j \leq k-1$,

$$P \sim y^{n_1-1}x^{m_1}\omega_1^{n_2-1}x^{m_2} \cdots \omega_{k-1}^{n_k-1}x^{m_k}$$

holds for every product P of the sum. Since

$$v(y^{n_1-1}x^{m_1}\omega_1^{n_2-1}x^{m_2} \cdots \omega_{k-1}^{n_k-1}x^{m_k}) + v(y\omega_1 \cdots \omega_{k-1}) = \sum_{i=1}^{k} v(x^{m_i}\omega_{i-1}^{n_i}) = 0,$$

we can conclude $v[\omega_k, x] = v(y^{n_1-1}x^{m_1}\omega_1^{n_2-1}x^{m_2} \cdots \omega_{k-1}^{n_k-1}x^{m_k}) = -v(y\omega_1 \cdots \omega_{k-1})$. It follows that $v[x, \omega_k] > v(x\omega_k)$ if and only if $v(xy\omega_1 \cdots \omega_k) < 0$.

We will now prove that $v[\omega_{i+k}, \omega_i] = -v(xy\omega_1 \cdots \omega_{i-1}\omega_{i+1} \cdots \omega_{i+k-1})$ by induction on k, $1 \leq k \leq n-i$. It will then follow that $v[\omega_i, \omega_j] > v(\omega_i\omega_j)$ for all $i, j \leq n$ if and only if $v(\Pi_{\ell=-1}^{n}\omega_\ell) < 0$. If $k = 1$, then

$$\begin{aligned}[\omega_{i+1}, \omega_i] &= [x^{m_{i+1}}\omega_i^{n_{i+1}} - \beta_{i+1}, \omega_i] = [x^{m_{i+1}}, \omega_i]\omega_i^{n_{i+1}} \\ &= (\sum_{\ell=1}^{m_{i+1}} x^{m_{i+1}-\ell}[x, \omega_i]x^{\ell-1})\omega_i^{n_{i+1}},\end{aligned}$$

and since $[x, \omega_i]$ is a sum of products all equal to $y^{n_1-1}x^{m_1}\omega_1^{n_2-1}x^{m_2} \cdots \omega_{i-1}^{n_i-1}x^{m_i}$ up to the order of factors, we can, using $v[\omega_i, \omega_j] > v(\omega_i\omega_j)$ for $j < i$, deduce that $v[\omega_{i+1}, \omega_i] = -v(xy\omega_1 \cdots \omega_{i-1})$ just like we did when evaluating $v[\omega_i, x]$. For $k > 1$, we have

$$\begin{aligned}[\omega_{i+k}, \omega_i] &= [x^{m_{i+k}}\omega_{i+k-1}^{n_{i+k}} - \beta_{i+k}, \omega_i] = [x^{m_{i+k}}, \omega_i]\omega_{i+k-1}^{n_{i+k}} + x^{m_{i+k}}[\omega_{i+k-1}^{n_{i+k}}, \omega_i] \\ &= (\sum_{\ell=1}^{m_{i+k}} x^{m_{i+k}-\ell}[x, \omega_i]x^{\ell-1})\omega_{i+k-1}^{n_{i+k}} + \\ &\qquad x^{m_{i+k}}(\sum_{\ell=1}^{n_{i+k}} \omega_{i+k-1}^{n_{i+k}-\ell}[\omega_{i+k-1}, \omega_i]\omega_{i+k-1}^{\ell}) \\ &\sim m_{i+k}x^{m_{i+k}-1}\omega_{i+k-1}^{n_{i+k}}[x, \omega_i] + n_{i+k}x^{m_{i+k}}\omega_{i+k-1}^{n_{i+k}-1}[\omega_{i+k-1}, \omega_i]\end{aligned}$$

and using both Lemma 3.1 and induction on k, we see that the first sum has v-value equal to $-v(xy\omega_1 \cdots \omega_{i-1})$ and the second has v-value equal to $-v(xy\omega_1 \cdots \omega_{i+k-1})$. Since the latter is smaller, it is equal to $v[\omega_{i+k}, \omega_i]$. This proves the lemma. □

It follows that if v can be extended from $(\omega_i)_{i\geq -1}$ to a valuation on $\mathcal{A}_1(\mathbb{R})$, $\sum_{i\geq -1}^{k} v(\omega_i)$ must be strictly less than 0 for all $k \leq n$ in case $v(\omega_n) \notin \mathbb{Q}$ for some n, and for all $k \geq 0$ if $v(\omega_i) \in \mathbb{Q}$ for all $i \in \mathbb{N}$. We will now describe a necessary condition for the residue field to be $\mathbb{R}$ and then proceed to show that if both conditions are fulfilled, v can be extended from $(\omega_i)_{i\geq -1}$ to a valuation on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$.

To ensure that the residue field is $\mathbb{R}$, it is obviously necessary that $\overline{\omega_{i-1}^{k_i}\omega_{j-1}^{k_j}} \in \mathbb{R}$ holds for all $k_i, k_j \in \mathbb{Z}$ with $k_i \frac{m_i}{n_i} + k_j \frac{m_j}{n_j} = 0$. For given $i, j \geq 0$, all solutions $(k_i, k_j) \in \mathbb{Z}^2$ to the diophantine equation

$$k_i m_j n_i + k_j m_i n_j = 0 \tag{3.1}$$

are integer multiples of the pair $(K_{i,j}, -K_{j,i})$ with

$$K_{i,j} = \frac{m_j n_i}{d_{i,j}},$$
$$K_{j,i} = \frac{m_i n_j}{d_{i,j}},$$
$$\text{where } d_{i,j} = \gcd\{m_j n_i, m_i n_j\}.$$

So for all $k_i, k_j \in \mathbb{Z}$ with $k_i \frac{m_i}{n_i} + k_j \frac{m_j}{n_j} = 0$, we can write

$$\overline{\omega_{i-1}^{k_i}\omega_{j-1}^{k_j}} = \overline{\omega_{i-1}^{nK_{i,j}}\omega_{j-1}^{-nK_{j,i}}} = (\overline{\omega_{i-1}^{K_{i,j}}\omega_{j-1}^{-K_{j,i}}})^n$$

for some $n \in \mathbb{Z}$, where we used Proposition 2.2 in the second equality. So for every $k_i, k_j \in \mathbb{Z}$ satisfying 3.1, $\overline{\omega_{i-1}^{k_i}\omega_{j-1}^{k_j}}$ is uniquely determined by $\overline{\omega_{i-1}^{K_{i,j}}\omega_{j-1}^{-K_{j,i}}}$. For each $i, j \geq 0$, we define $\alpha_{i,j} = \overline{\omega_{i-1}^{K_{i,j}}\omega_{j-1}^{-K_{j,i}}}$. We immediately see that $\alpha_{j,i} = \alpha_{i,j}^{-1}$ and hence $\alpha_{i,i} = 1$ for all $i, j \geq 0$. As

$$\alpha_{i,j}^{d_{i,j}} = \overline{\omega_{i-1}^{K_{i,j}d_{i,j}}\omega_{j-1}^{-K_{j,i}d_{i,j}}} = \overline{\omega_{i-1}^{m_j n_i}\omega_{j-1}^{-m_i n_j}} = \beta_i^{m_j}\beta_j^{-m_i}$$

for all $i, j \geq 0$, $\alpha_{i,j}$ is one of the possible $d_{i,j}$-th roots for $\beta_i^{m_j}\beta_j^{-m_i}$. If v is a valuation on $\mathcal{D}_1(\mathbb{R})$ with residue field $\mathbb{R}$, $\alpha_{i,j}$ must be real for all $i, j \geq 0$. For every $i, j \geq 0$ with even $d_{i,j}$, this means that $\beta_i^{m_j}\beta_j^{-m_i} > 0$ must hold. In the next lemma, we present a necessary condition on the sequence $(\beta_i)_{i\geq 1}$ so that $\alpha_{i,j} \in \mathbb{R}$ can be chosen for all i, j. We also prove that if n_i is odd, $\alpha_{i,j}$ is uniquely determined for all $j \geq 0$.

Lemma 3.3. *Let v be a valuation on $\mathcal{D}_1(\mathbb{R})$ as in Lemma 3.2. Then the following holds:*

(1) *If n_i is odd, there is a unique possible choice for $\alpha_{i,j} \in \mathbb{R}$ for all $j \geq 0$.*

(2) *Only if $\operatorname{sgn}(\beta_i)$ is constant on the set of all $i \geq 0$ for which n_i is even can we choose $\alpha_{i,j} \in \mathbb{R}$ for all $i, j \geq 0$.*

Proof. Suppose n_i is odd. Then for any $j \geq 0$, let $\tilde{d}_{i,j}$ be the highest odd number dividing $d_{i,j}$. Since n_i is odd, $\ell_1 := \frac{\tilde{d}_{i,j}m_j}{d_{i,j}} \in \mathbb{Z}$. If n_j is odd as well, $\ell_2 := \frac{\tilde{d}_{i,j}m_i}{d_{i,j}} \in \mathbb{Z}$ holds too. If n_j is even, m_j is odd, so $d_{i,j} = \tilde{d_{i,j}}$ as $d_{i,j}$ divides $m_j n_i$. In both cases, $\ell_2 \in \mathbb{Z}$ holds.

Then for $\ell := \ell_1 m_i = \ell_2 m_j = \frac{\tilde{d}_{i,j} m_i m_j}{d_{i,j}}$ we can evaluate

$$\begin{aligned}\alpha_{i,j}^{\tilde{d}_{i,j}} &= \overline{\omega_{i-1}^{K_{i,j}\tilde{d}_{i,j}} \omega_{j-1}^{-K_{j,i}\tilde{d}_{i,j}}} = \overline{x^{\ell} x^{-\ell} \omega_{i-1}^{\ell_1 n_i} \omega_{j-1}^{-\ell_2 n_j}} = \overline{(x^{m_i}\omega_{i-1}^{n_i})^{\ell_1} (x^{m_j}\omega_{j-1}^{n_j})^{-\ell_2}} \\ &= \beta_i^{\ell_1} \beta_j^{-\ell_2},\end{aligned}$$

and since $\tilde{d}_{i,j}$ is odd, $\alpha_{i,j} \in \mathbb{R}$ is uniquely determined. The first point of the lemma is thus proven.

To prove the second point of the lemma, suppose $i, j \geq 0$ are such that n_i and n_j are both even. As a consequence, both m_i and m_j are odd while $d_{i,j}$ is even. So, provided $\alpha_{i,j} \in \mathbb{R}$, we compute

$$1 = \operatorname{sgn}(\alpha_{i,j}^{d_{i,j}}) = \operatorname{sgn}(\beta_i^{m_j} \beta_j^{-m_i}) = \operatorname{sgn}(\beta_i \beta_j),$$

which proves the second part of the lemma. □

For even $d_{i,j}$ we have seemingly two choices for $\alpha_{i,j} \in \mathbb{R}$ – a positive and a negative one. We will show that in most cases, we cannot choose $\operatorname{sgn}(\alpha_{i,j})$ for all $i, j \geq 0$ independently of each other.

Before that, we observe that for any $i, j \geq 0$, at most one of $K_{i,j}$ and $K_{j,i}$ is even. In fact, if at most one of n_i and n_j is odd, $K_{i,j}$ is odd if and only if n_i is divisible by the greatest power of two that divides n_j. For each $i \geq 1$, let 2^{h_i} be the biggest power of two that divides n_i. Define also $m_0 = 1$ and $n_0 = -1$.

Proposition 3.4. *Let v be a valuation on $\mathcal{D}_1(\mathbb{R})$ associated to a sequence $(\omega_i)_{i \geq -1}$ with $v(\omega_{-1}) = v(x) = -1$, $v(\omega_{i-1}) = \frac{m_i}{n_i}$ with $\gcd(m_i, n_i) = 1$ and $\overline{x^{m_i}\omega_{i-1}^{n_i}} = \beta_i \in \mathbb{R}$ for each $i \geq 1$. Suppose $\operatorname{sgn}(\beta_i)$ is constant on the set of all $i \geq 0$ for which n_i is even. Suppose $\alpha_{i,j} \in \mathbb{R}$ is determined for all $i, j \geq 0$. Then $\overline{\prod_{i=0}^{r} \omega_{i-1}^{k_i}} \in \mathbb{R}$ is uniquely determined for each set of integers $k_0, k_1, \ldots, k_r \in \mathbb{Z}$ with $\sum_{i=0}^{r} k_i \frac{m_i}{n_i} = 0$ if and only if for each $a, b, c \geq 0$, $\alpha_{a,b}\alpha_{a,c}\alpha_{b,c} > 0$ whenever $h_a = h_b \leq h_c$ holds.*

Proof. To prove the necessity of the condition, suppose $a, b, c \geq 0$ are such that $h_a = h_b \leq h_c$ holds. Suppose $K_{a,b}$ and $K_{b,c}$ are both odd. Choose $k_a, k_b, k_c \in \mathbb{Z} \setminus \{0\}$ such that $k_a \frac{m_a}{n_a} + k_b \frac{m_b}{n_b} + k_c \frac{m_c}{n_c} = 0$ and that k_a and k_b are odd while k_c is even. Then on one hand,

$$\begin{aligned}\operatorname{sgn}(\overline{\omega_{a-1}^{k_a}\omega_{b-1}^{k_b}\omega_{c-1}^{k_c}}) &= \operatorname{sgn}(\overline{\omega_{a-1}^{k_a}\omega_{b-1}^{k_b}\omega_{c-1}^{k_c}}^{K_{a,b}}) \\ &= \operatorname{sgn}(\overline{\omega_{a-1}^{k_a}\omega_{b-1}^{k_b}\omega_{c-1}^{k_c}}^{K_{a,b}} \overline{\omega_{b-1}^{-k_a K_{b,a}} \omega_{b-1}^{k_a K_{b,a}}}) \\ &= \operatorname{sgn}(\alpha_{a,b}^{k_a} \overline{\omega_{b-1}^{\ell_b}\omega_{c-1}^{\ell_c}})\end{aligned}$$

with

$$\begin{aligned}\ell_b &= k_b K_{a,b} + k_a K_{b,a}, \\ \ell_c &= k_c K_{a,b}.\end{aligned}$$

As $v(\omega_{b-1}^{\ell_b}\omega_{c-1}^{\ell_c}) = 0$, $(\ell_b, \ell_c) = \ell(K_{b,c}, -K_{c,b})$ for some $\ell \in \mathbb{Z}$ with $-\ell K_{c,b} = \ell_c = k_c K_{a,b}$. So we can conclude

$$\operatorname{sgn}(\overline{\omega_{a-1}^{k_a}\omega_{b-1}^{k_b}\omega_{c-1}^{k_c}}) = \operatorname{sgn}(\alpha_{a,b}^{k_a}\alpha_{b,c}^{\ell}).$$

On the other hand, we see by analogous computations that

$$\begin{aligned}\operatorname{sgn}(\overline{\omega_{a-1}^{k_a}\omega_{b-1}^{k_b}\omega_{c-1}^{k_c}}) &= \operatorname{sgn}(\overline{\omega_{a-1}^{k_a}\omega_{b-1}^{k_b}\omega_{c-1}^{k_c}}^{K_{a,c}})\\ &= \operatorname{sgn}(\overline{\omega_{a-1}^{k_a}\omega_{b-1}^{k_b}\omega_{c-1}^{k_c}}^{K_{a,c}}\overline{\omega_{c-1}^{-k_aK_{c,a}}\omega_{c-1}^{k_aK_{c,a}}})\\ &= \operatorname{sgn}(\alpha_{a,c}^{k_a}\overline{\omega_{b-1}^{\ell'_b}\omega_{c-1}^{\ell'_c}}) = \operatorname{sgn}(\alpha_{a,c}^{k_a}\alpha_{b,c}^{\ell'})\end{aligned}$$

for some $\ell'_b, \ell'_c, \ell' \in \mathbb{Z}$ with

$$\begin{aligned}\ell'_b &= k_bK_{a,c} = \ell' K_{b,c},\\ \ell'_c &= k_cK_{a,c} + k_aK_{c,a}.\end{aligned}$$

We have chosen k_a, k_b odd and k_c even. In this case, the greatest power of two that divides k_c is $2^{h_c-h_a+1}$. On the other hand, the greatest power of two that divides $K_{c,a}$ and $K_{c,b}$ is $2^{h_c-h_a}$. We can thus conclude from $\ell K_{c,b} = -k_cK_{a,b}$ and $\ell' K_{b,c} = k_bK_{a,c}$ that ℓ is even while ℓ' is odd since $K_{a,b}, K_{a,c}$ and $K_{b,c}$ are all odd. So we see that

$$\operatorname{sgn}(\overline{\omega_{a-1}^{k_a}\omega_{b-1}^{k_b}\omega_{c-1}^{k_c}}) = \operatorname{sgn}(\alpha_{a,b}) = \operatorname{sgn}(\alpha_{a,c}\alpha_{b,c}),$$

which proves the necessity of the condition.

Now suppose $\operatorname{sgn}(\alpha_{a,b}\alpha_{a,c}\alpha_{b,c}) = 1$ for all $a, b, c \geq 0$ with $h_a = h_b \leq h_c$. Let $K := (k_0, \dots, k_r) \in \mathbb{Z}^{r+1}$ be such that $\sum_{i=0}^r k_i \frac{m_i}{n_i} = 0$. Let $\operatorname{supp} K := \{i \mid k_i \neq 0\}$ and $n := |\operatorname{supp} K|$. We prove that $\overline{\Pi_{i=0}^r \omega_{i-1}^{k_i}} \in \mathbb{R}$ is uniquely determined by induction on $n \geq 2$. We first suppose $0 \notin \operatorname{supp} K$. We will deal with the case $0 \in \operatorname{supp} K$ at the end of our proof.

If $n = 2$, then $\Pi_{i=0}^r \omega_{i-1}^{k_i} = \omega_{i-1}^{k_i}\omega_{j-1}^{k_j}$ for some $i, j > 0$, and its value in the residue field is a power of $\alpha_{i,j}$.

Now suppose $n > 2$. Take two distinct $a, b \in \operatorname{supp} K$. As at least one of $K_{a,b}$ and $K_{b,a}$ is odd, so suppose $K_{a,b}$ is odd. Then

$$\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}^{K_{a,b}} = \overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}^{K_{a,b}}\overline{\omega_{b-1}^{-k_aK_{b,a}}\omega_{b-1}^{k_aK_{b,a}}} = \overline{\Pi_{i=1}^r \omega_{i-1}^{\ell_{i,1}}}\alpha_{a,b}^{k_a}$$

with $\ell_{a,1} = 0, \ell_{b,1} = k_aK_{a,b} + k_bK_{b,a}$ and $\ell_{i,1} = k_iK_{a,b}$ for $i \neq a, b$. Since $|\{i \mid \ell_{i,1} \neq 0\}|$ is strictly smaller than n, $\overline{\Pi_{i=0}^r \omega_{i-1}^{\ell_{i,1}}} \in \mathbb{R}$ is uniquely determined by the induction hypothesis. So we have determined $\overline{\Pi_{i=0}^r \omega_{i-1}^{k_i}}^{K_{a,b}} \in \mathbb{R}$. As $K_{a,b}$ is odd, $\overline{\Pi_{i=0}^r \omega_{i-1}^{k_i}} \in \mathbb{R}$ is determined as well.

We now need to show that in this way, $\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}$ is uniquely determined, that is, if we choose another $a', b' \in \operatorname{supp} K$ instead of a, b, we get the same value for $\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}} \in \mathbb{R}$. We will show this by choosing $c \in \operatorname{supp} K \setminus \{a, b\}$ and proving that the evaluated value of $\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}$ is the same whether we factor a power of $\alpha_{a,b}$ as above, or $\alpha_{a,c}$ or $\alpha_{b,c}$ instead. By transitivity of the equality relation, this will imply that the obtained value of $\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}$ is independent of the choice of $a, b \in \operatorname{supp} K$. Suppose without loss of generality that $h_a \leq h_b \leq h_c$ and that $K_{a,b}, K_{a,c}$ and $K_{b,c}$ are odd. Above, we have evaluated

$$\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}^{K_{a,b}} = \overline{\Pi_{i=1}^r \omega_{i-1}^{\ell_{i,1}}}\alpha_{a,b}^{k_a}$$

with $\ell_{a,1} = 0, \ell_{b,1} = k_a K_{a,b} + k_b K_{b,a}$ and $\ell_{i,1} = k_i K_{a,b}$ for $i \neq a, b$. We proceed by evaluating, in the same way as before,

$$\overline{\Pi_{i=1}^r \omega_{i-1}^{\ell_{i,1}}}^{K_{b,c}} = \overline{\Pi_{i=1}^r \omega_{i-1}^{p_{i,1}}} \alpha_{b,c}^{\ell_{b,1}}$$

with $p_{a,1} = p_{b,1} = 0, p_{c,1} = \ell_{c,1} K_{b,c} + \ell_{b,1} K_{c,b}$ and $p_{i,1} = \ell_{i,1} K_{b,c}$ for $i \neq a, b, c$. So

$$\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}^{K_{a,b} K_{b,c}} = \overline{\Pi_{i=1}^r \omega_{i-1}^{p_{i,1}}} \alpha_{a,b}^{k_a K_{b,c}} \alpha_{b,c}^{\ell_{b,1}} \tag{3.2}$$

with $\ell_{i,1}$ and $p_{i,1}$ for all $0 \leq i \leq r$ as above. In particular, we see that for $i \neq a, b, c$, $p_{i,1} = \ell_{i,1} K_{b,c} = k_i K_{a,b} K_{b,c}$. Similarly, we can compute

$$\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}^{K_{a,c} K_{b,c}} = (\overline{\Pi_{i=1}^r \omega_{i-1}^{\ell_{i,2}}} \alpha_{a,c}^{k_a})^{K_{b,c}} = \overline{\Pi_{i=1}^r \omega_{i-1}^{p_{i,2}}} \alpha_{a,c}^{k_a K_{b,c}} \alpha_{b,c}^{\ell_{b,2}} \tag{3.3}$$

with

1. $\ell_{a,2} = 0, \ell_{c,2} = k_a K_{a,c} + k_c K_{c,a}$ $\ell_{i,1} = k_i K_{a,c}$ for $i \neq a, c$, and
2. $p_{a,2} = p_{b,2} = 0, p_{c,2} = \ell_{b,2} K_{c,b} + \ell_{c,2} K_{b,c}, p_{i,2} = k_i K_{a,c} K_{b,c}$ for $i \neq a, b, c$.

Let $N := K_{a,b} K_{a,c} K_{b,c}$. On one hand, we see from 3.2 that

$$\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}^{N} = \overline{\Pi_{i=1}^r \omega_{i-1}^{p_{i,1}}}^{K_{a,c}} \alpha_{a,b}^{k_a K_{b,c} K_{a,c}} \alpha_{b,c}^{\ell_{b,1} K_{a,c}}, \tag{3.4}$$

and on the other hand, we see from 3.3 that

$$\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}^{N} = \overline{\Pi_{i=1}^r \omega_{i-1}^{p_{i,2}}}^{K_{a,b}} \alpha_{a,c}^{k_a K_{b,c} K_{a,b}} \alpha_{b,c}^{\ell_{b,2} K_{a,b}}. \tag{3.5}$$

We need to show that in both equations, we get the same value. We first see that for all $i \neq c$, $p_{i,1} K_{a,c} = p_{i,2} K_{a,b}$. So, given that

$$\sum_{i=1}^{r} p_{i,1} \frac{m_i}{n_i} = \sum_{i=1}^{r} p_{i,2} \frac{m_i}{n_i} = 0,$$

we can see $p_{c,1} K_{a,c} = p_{c,2} K_{a,b}$ holds as well, and thus we conclude

$$\overline{\Pi_{i=1}^r \omega_{i-1}^{p_{i,1}}}^{K_{a,c}} = \overline{\Pi_{i=1}^r \omega_{i-1}^{p_{i,2}}}^{K_{a,b}}.$$

It then follows that

$$\alpha_{a,b}^{k_a K_{a,c} K_{b,c}} \alpha_{b,c}^{\ell_{b,1} K_{a,c}} = \alpha_{a,c}^{k_a K_{b,c} K_{a,b}} \alpha_{b,c}^{\ell_{b,2} K_{a,b}},$$

since both sides of the equation are equal to $\overline{\omega_{a-1}^{N k_a} \omega_{b-1}^{N k_b} \omega_{c-1}^{N k_c - p_{c,1} K_{a,c}}}$ and the signs of $\alpha_{a,b}, \alpha_{a,c}$ and $\alpha_{b,c}$ were chosen so that the signs of both sides of the equality match. We conclude that the value of $\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}^{N}$ is the same in both 3.4 and 3.5. As N is odd (since $K_{a,b}$, $K_{a,c}$ and $K_{b,c}$ are all odd), we conclude that $\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}$ is the same whether we factor a power of $\alpha_{a,b}$ or $\alpha_{a,c}$. If we factored a power of $\alpha_{b,c}$, we would, as similar computations as above would show, get the same value for $\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}$.

We have now shown that if the condition of the proposition is fulfilled, $\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i}}$ is uniquely determined for all $k_1, \dots, k_r \in \mathbb{Z}$ with $\sum_{i=1}^r k_i \frac{m_i}{n_i} = 0$.

Now we consider the case $0 \in \operatorname{supp} K$. Let $K = (k_0, \dots, k_r) \in \mathbb{Z}^{r+1}$ be such that $k_0 \neq 0$ and $\sum_{i=0}^r k_i \frac{m_i}{n_i} = 0$. Let $N := \gcd\{n_i \mid i \in \operatorname{supp} K\}$. If N is odd, i.e., if n_i is odd for every $i \in \operatorname{supp} K$, then $\overline{\Pi_{i=0}^r \omega_{i-1}^{k_i}}$ is uniquely determined. This is because

$$\overline{\Pi_{i=0}^r \omega_{i-1}^{k_i}}^N = (\overline{\Pi_{i=0}^r x^{k_i \frac{m_i}{n_i}} \Pi_{i=0}^r \omega_{i-1}^{k_i}})^N = \overline{\Pi_{i=1}(x^{m_i} \omega_{i-1}^{ni})^{k_i c_i}} = \Pi_{i=1}^r \beta_i^{k_i c_i}$$

where $c_i := \frac{N}{n_i}$ for each $i \leq i \leq r$. We thus conclude $\overline{\Pi_{i=0}^r \omega_{i-1}^{k_i}} \in \mathbb{R}$ is the uniquely determined N-the real root of $\Pi_{i=1}^r \beta_i^{k_i c_i}$. Now suppose n_j is even for some $j \in \operatorname{supp} K$. Then m_j must be odd since $\gcd(m_j, n_j) = 1$. Let $k_j' := k_j - k_0 n_j$ and $k_i' := k_i$ for all $i \in \operatorname{supp} K \setminus \{0, j\}$. Then $\sum_{i=1}^r k_i' \frac{m_i}{n_i} = 0$ and

$$\overline{\Pi_{i=0}^r \omega_{i-1}^{k_i}}^{m_j} = (\overline{x^{m_j} \omega^{n_j}})^{k_0} (\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i'}})^{m_j} = \beta_j^{k_0} (\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i'}})^{m_j}.$$

We evaluate $(\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i'}})^{m_j}$ as above $k_0 = 0$ and conclude that $\overline{\Pi_{i=0}^r \omega_{i-1}^{k_i}} \in \mathbb{R}$ is the unique m_j-th real root of $\beta_j^{k_0} (\overline{\Pi_{i=1}^r \omega_{i-1}^{k_i'}})^{m_j}$.

This concludes the proof of our proposition. □

In Lemma 3.6, we suppose that v is a valuation on $\mathcal{D}_1(\mathbb{R})$ extended from $(\omega_i)_{i \geq -1}$ to $\mathcal{D}_1(\mathbb{R})$ and compute the value of certain elements of $\mathcal{D}_1(\mathbb{R})$ in this case.

Lemma 3.5. *Let D be a division ring endowed with a valuation v with an abelian value group and a commutative residue field with characteristic zero. Let $a, b \in D$ be such that $a \sim b$, $v(a) = v(b) = 0$ and $v(ab) < v[a, b]$. Then $v(a^n - b^n) = v(a - b)$ for all $n \in \mathbb{Z} \setminus \{0\}$. If there exist $c, d \in D$ such that $c^n = a, d^n = b$, $\overline{c} = \overline{d}$ for some $n \in \mathbb{N}$, then $v(c^m - d^m) = v(a - b)$ for all $m \in \mathbb{Z}$.*

Proof. For $n \in \mathbb{N}$, write $a^n - b^n = (a - b) \sum_{i=0}^{n-1} a^{n-1-i} b^i +$ terms with higher v-value. Since $\overline{a^{n-1-i} b^i}$ is the same for all $0 \leq i \leq n - 1$, the v-value of the sum is equal to zero, proving the statement for positive integers n. For negative $n \in \mathbb{Z}$, the statement follows from $a^n - b^n = -a^n (a^{-n} - b^{-n}) b^n$. The last statement of the lemma follows from $a - b \sim (c - d) \sum_{i=0}^{n-1} c^{n-1-i} b^i$. □

Lemma 3.6. *Suppose v is a valuation on $\mathcal{A}_1(\mathbb{R})$ and suppose $i_1, i_2, \dots, i_r \in \mathbb{N}$ and $k_0 \in \mathbb{Z}$, $k_{i_1}, k_{i_2}, \dots, k_{i_r} \in \mathbb{Z} \setminus \{0\}$ are such that $v(x^{k_0} \omega_{i_1-1}^{k_{i_1}} \cdots \omega_{i_r-1}^{k_{i_r}}) = 0$. If $\min_{1 \leq j \leq r}\{v(\omega_{i_j})\}$ is achieved at exactly one j, then*

$$v(x^{k_0} \omega_{i_1-1}^{k_{i_1}} \cdots \omega_{i_r-1}^{k_{i_r}} - \overline{x^{k_0} \omega_{i_1-1}^{k_{i_1}} \cdots \omega_{i_r-1}^{k_{i_r}}}) = \min\{v(\omega_{i_j}) \mid 1 \leq j \leq r\}.$$

Proof. Let n be the least common multiple of $n_{i_1}, \dots, n_{i_r}$ and $c_{i_j} = \frac{n}{n_{i_j}}$ for each i_j. Since

$$\begin{aligned} \overline{(x^{k_0} \omega_{i_1-1}^{k_{i_1}} \cdots \omega_{i_r-1}^{k_{i_r}})^n} &= \overline{\Pi_{j=1}^r x^{n k_{i_j} \frac{m_{i_j}}{n_{i_j}}} (\omega_{i_1-1}^{k_{i_1}} \cdots \omega_{i_r-1}^{k_{i_r}})^n} \\ &= \overline{\Pi_{j=1}^r (x^{m_{i_j}} \omega_{i_j-1}^{n_{i_j}})^{k_{i_j} c_{i_j}}} = \Pi_{j=1}^r \beta_{i_j}^{k_{i_j} c_{i_j}}, \end{aligned}$$

by Proposition 2.2, we can compute

$$\begin{aligned}&(x^{k_0}\omega_{i_1-1}^{k_{i_1}}\cdots\omega_{i_r-1}^{k_{i_r}})^n-\Pi_{j=1}^r\beta_{i_j}^{k_{i_j}c_{i_j}}\\&\sim\sum_{j=1}^r(x^{m_{i_1}}\omega_{i_1-1}^{n_{i_1}})^{k_{i_1}c_{i_1}}\cdots(x^{m_{i_{j-1}}}\omega_{i_{j-1}-1}^{n_{i_{j-1}}})^{k_{i_{j-1}}c_{i_{j-1}}}\cdot\\&((x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}}-\beta_{i_j}^{k_{i_j}c_{i_j}})\beta_{i_{j+1}}^{k_{i_j}c_{i_j}}\cdots\beta_{i_r}^{k_{i_j}c_{i_j}}.\end{aligned}$$

For each j such that $k_{i_j}>0$,

$$(x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}}-\beta_{i_j}^{k_{i_j}c_{i_j}}\sim\omega_{i_j}\sum_{i=0}^{k_{i_j}c_{i_j}-1}(x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}-i}\beta_{i_j}^i,$$

which gives us $v((x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}}-\beta_{i_j}^{k_{i_j}c_{i_j}})=v(\omega_{i_j})$. In case $k_{i_j}<0$, we see that

$$\begin{aligned}&(x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}}-\beta_{i_j}^{k_{i_j}c_{i_j}}=\\&-(x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}}\beta_{i_j}^{k_{i_j}c_{i_j}}((x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{-k_{i_j}c_{i_j}}-\beta_{i_j}^{-k_{i_j}c_{i_j}}),\end{aligned}$$

which again implies $v((x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}}-\beta_{i_j}^{k_{i_j}c_{i_j}})=v(\omega_{i_j})$. We conclude, using Lemma 3.5,

$$\begin{aligned}&v(x^{k_0}\omega_{i_1-1}^{k_{i_1}}\cdots\omega_{i_r-1}^{k_{i_r}}-\overline{x^{k_0}\omega_{i_1-1}^{k_{i_1}}\cdots\omega_{i_r-1}^{k_{i_r}}})\\&=v((x^{k_0}\omega_{i_1-1}^{k_{i_1}}\cdots\omega_{i_r-1}^{k_{i_r}})^n-\overline{(x^{k_0}\omega_{i_1-1}^{k_{i_1}}\cdots\omega_{i_r-1}^{k_{i_r}})^n})\\&=\min\{v(\omega_{i_j})\mid 1\le j\le r\}.\end{aligned}$$

□

With the help of Lemma 3.6, we will evaluate $v(x^{k_0}\omega_{i_1-1}^{k_{i_1}}\cdots\omega_{i_r-1}^{k_{i_r}}-\overline{x^{k_0}\omega_{i_1-1}^{k_{i_1}}\cdots\omega_{i_r-1}^{k_{i_r}}})$ when $v(x^{k_0}\omega_{i_1-1}^{k_{i_1}}\cdots\omega_{i_r-1}^{k_{i_r}})=0$ in general. As in Lemma 3.6, we assume $k_0\in\mathbb{Z}$, $k_{i_j}\in\mathbb{Z}\setminus\{0\}$ for all $1\le j\le r$. This will be helpful when we will later construct a valuation v associated to a sequence $(\omega_i)_{i\ge -1}$. Let us assume for now that $i_1<i_2<\cdots<i_r$; at the end of the calculation we will see that the order of i_j does not affect the v-value.

To start, we introduce some abbreviations to make the written equations easier to read. Let n and c_{i_j} for all j be as in the proof of Lemma 3.6,

$$\begin{aligned}A_0&:=x^{k_0}\omega_{i_1-1}^{k_{i_1}}\cdots\omega_{i_r-1}^{k_{i_r}}\\B_0&:=\overline{A_0}\\A_0^{(n)}&:=x^{nk_0}\omega_{i_1-1}^{nk_{i_1}}\cdots\omega_{i_r-1}^{nk_{i_r}}\\B_0^{(n)}&:=\overline{A_0^{(n)}}=\Pi_{j=1}^r\beta_{i_j}^{k_{i_j}c_{i_j}}.\end{aligned}$$

Since B_0 is in $\mathbb{R}$, we can write

$$A_0-B_0=(A_0^n-B_0^n)(\sum_{i=0}^{n-1}A_0^{n-i-1}B_0^i)^{-1}\sim(A_0^{(n)}-B_0^{(n)})(\sum_{i=0}^{n-1}A_0^{n-i-1}B_0^i)^{-1}.\quad(3.6)$$

Since $v(\sum_{i=0}^{n-1} A_0^{n-i-1}B_0^i) = v(A_0^{n-i-1}B_0^i) = 0$ for all i, which holds due to $\overline{A_0^{n-i-1}B_0^i} = B_0^{n-1}$ for all i, $v(A_0 - B_0) = v(A_0^{(n)} - B_0^{(n)})$. To evaluate the right-hand side of (3.6), we first proceed as we have done in the proof of Lemma 3.6, so

$$A_0^{(n)} - B_0^{(n)} \sim \sum_{j=1}^{r} \Pi_{\ell=1}^{j-1}(x^{m_{i_\ell}}\omega_{i_\ell-1}^{n_{i_\ell}})^{k_{i_\ell}c_{i_\ell}} \cdot ((x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}} - \beta_{i_j}^{k_{i_j}c_{i_j}}) \cdot \Pi_{\ell=j+1}^{r}\beta_{i_\ell}^{k_{i_j}c_{i_j}}.$$

If $k_{i_j} > 0$, we proceed by

$$(x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}} - \beta_{i_j}^{k_{i_j}c_{i_j}} \sim \omega_{i_j} \sum_{p=0}^{k_{i_j}c_{i_j}-1} (x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}-p-1}\beta_{i_j}^{p}.$$

For $i_j > 0, k_{i_j} < 0$, we can on the other hand write

$$(x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}} - \beta_{i_j}^{k_{i_j}c_{i_j}} \sim -\omega_{i_j}(x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}}\beta_{i_j}^{k_{i_j}c_{i_j}} \sum_{p=0}^{-k_{i_j}c_{i_j}-1} (x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{-k_{i_j}c_{i_j}-p-1}\beta_{i_j}^{p}.$$

We now define, if $k_j > 0$,

$$C_j := \sum_{p=0}^{k_{i_j}c_{i_j}-1} \Pi_{\ell=1}^{j-1}(x^{m_{i_\ell}}\omega_{i_\ell-1}^{n_{i_\ell}})^{k_{i_\ell}c_{i_\ell}} \cdot (x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}-p-1}\beta_{i_j}^{p} \cdot \Pi_{\ell=j+1}^{r}\beta_{i_\ell}^{k_{i_\ell}c_{i_\ell}},$$

and, if $k_j < 0$,

$$C_j := -(x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{k_{i_j}c_{i_j}}\beta_{i_j}^{k_{i_j}c_{i_j}} \sum_{p=0}^{-k_{i_j}c_{i_j}-1} \Pi_{\ell=1}^{j-1}(x^{m_{i_\ell}}\omega_{i_\ell-1}^{n_{i_\ell}})^{k_{i_\ell}c_{i_\ell}} \cdot (x^{m_{i_j}}\omega_{i_j-1}^{n_{i_j}})^{-k_{i_j}c_{i_j}-p-1}\beta_{i_j}^{p} \cdot \Pi_{\ell=j+1}^{r}\beta_{i_\ell}^{k_{i_\ell}c_{i_\ell}}$$

for each $1 \le j \le r$. Further, we define

$$A_{1,j} = \omega_{i_j}C_j$$
$$A_0^{(n)} - B_0^{(n)} \sim \sum_{j=1}^{r} \omega_{i_j}C_j = \sum_{j=1}^{r} A_{1,j}$$

for each $1 \le j \le r$. Thus we can conclude that $v(A_{1,j}) = v(\omega_{i_j})$, since the image of C_j in the residue field is equal $k_{i_j}c_{i_j} \cdot \Pi_{\ell=1}^{r}\beta_{i_\ell}^{k_{i_\ell}c_{i_\ell}} \neq 0$ if $k_{i_j} > 0$ and $-\beta_{i_j}^{2k_{i_j}c_{i_j}}|k_{i_j}c_{i_j}| \cdot \Pi_{\ell=1}^{r}\beta_{i_\ell}^{k_{i_\ell}c_{i_\ell}} \neq 0$ if $k_{i_j} < 0$, making $v(C_j) = 0$. We can now write

$$A_0^{(n)} - B_0^{(n)} = \sum_{j=1}^{r} A_{1,j} + A = \sum_{v(A_{1,j}) \text{ is minimal}} A_{1,j} + \sum_{v(A_{1,j}) \text{ is not minimal}} A_{1,j}.$$

Here we note that the second of both finite sums on the right-hand side of this equation includes A, which denotes the sum of all terms obtained by changing the order of factors of the form ω_{i_ℓ} (which was not explicitly written above). The fact that the v-value of these terms is higher than the v-value of the terms of the first sum (the ones with minimal v-value) follows from Lemma 3.2.

If $\min_{1\leq j\leq r}\{v(\omega_{i_j})\}$ is achieved at more than one j, we take the sum of all $\omega_{i_j}C_j$ that have the minimal v-value, i.e., $\sum_{v(A_{1,j}) \text{ is minimal}} A_{1,j}$, then factor ω_{i_1}, so the sum now looks like

$$\sum_{v(A_{1,j}) \text{ is minimal}} A_{1,j} = \omega_{i_1} \sum_{v(A_{1,j}) \text{ is minimal}} \omega_{i_1}^{-1}A_{1,j} = \omega_{i_1} \sum_{v(A_{1,j}) \text{ is minimal}} \omega_{i_1}^{-1}\omega_{i_j}C_j$$

and, since $v(\omega_{i_1}^{-1}\omega_{i_j}C_j) = 0$, for each j, we can evaluate the sum of their images in the residue field. If this sum is not equal to zero, then $v(A_0 - B_0) = \min_{1\leq j\leq r}\{v(A_{1,j})\}$. Otherwise write

$$\omega_{i_1}\sum_j \omega_{i_1}^{-1}\omega_{i_j}C_j = \sum_j \omega_{i_1}(\omega_{i_1}^{-1}\omega_{i_j}C_j - \overline{\omega_{i_1}^{-1}\omega_{i_j}C_j}).$$

For every j, we write $\omega_{i_1}^{-1}\omega_{i_j}C_j - \overline{\omega_{i_1}^{-1}\omega_{i_j}C_j}$ as an $\mathbb{R}$-linear sum of terms of the form $\Pi_\ell \omega_{i_\ell-1}^{n_\ell}$ (in the same way we did with $A_0 - B_0$). We sum all of the newly obtained terms, as well as the terms in $\sum_{v(A_{1,j}) \text{ is not minimal}} A_{1,j}$, and relabel them as $A_{2,j}$ where j goes from 1 to the number of all terms.

As $A_0 - B_0$ can be written in the form

$$A_0 - B_0 = (\sum_{v(A_{2,j}) \text{ is minimal}} A_{2,j} + \sum_{v(A_{2,j}) \text{ is not minimal}} A_{2,j})D,$$

where we use D as the label of the product of all terms of the form $(\sum_i A^{k-i}B^i)^{-1}$ where $A = \overline{x^{k_0'}\Pi_{j=1}^r \omega_{i_j-1}^{k_{i_j}'}}$ for some $i_1, \ldots, i_r \in \mathbb{N}$, $k_0', k_{i_1}', \ldots, k_{i_r}' \in \mathbb{Z}$ and $B = \overline{A}$, that we factor out when we evaluate $\omega_{i_1}^{-1}\omega_{i_j}C_j - \overline{\omega_{i_1}^{-1}\omega_{i_j}C_j}$ for each j. All terms $(\sum_i A^{k-i}B^i)^{-1}$ have v-value equal to zero and their image in the residue field, which is of the form $(mB^{m-1})^{-1} \in \mathbb{R}$ for some $m \in \mathbb{N}$, is easy to determine.

We repeat the described procedure, writing $A_0 - B_0 = (\sum_j A_{k,j})D$ for increasing k. We stop when for some k, $\sum_{j,v(A_{k,j}) \text{ is minimal}} A_{k,j}$ is either composed of one single term or, after factoring out one of the terms, the image of the sum in the residue field is not zero. In this case, we conclude that $v(A_0 - B_0)$ is equal to $v(A_{k,j})$ for any term of the sum $\sum_{j,v(A_{k,j}) \text{ is minimal}} A_{k,j}$.

We must show that the process ends at some point even if the number of terms whose v-value we evaluate at each step is growing. We see that whenever we write $x^{k_0}\Pi_{\ell=1}^r \omega_{i_\ell-1}^{k_\ell} - \overline{x^{k_0}\Pi_{\ell=1}^r \omega_{i_\ell-1}^{k_\ell}}$ as a sum of terms with strictly positive v-value, the value of each of these terms is $v(\omega_{i_\ell})$ for some $\ell = 1, \ldots, r$. It follows that $v(A_0 - \overline{A_0})$ is a sum of $v(\omega_\ell)$ for some $\ell \geq 1$.

If $v(\omega_N)$ is irrational for some $N \geq 0$, the process either stops beforehand or, after $k \geq N - i_r$ steps we get a unique term $A_{k,j}$ that has v-value equal to $v(\omega_{i_r}\omega_{i_r+1}\cdots\omega_N)$. This is the term we get when we take the last term of $A_0^{(n)} - B_0^{(n)}$, written as a sum of terms $A_{1,j}$ with higher v-value and in each of the following steps whenever the v-value of

this term is minimal, take the last term when $A_{k,j}$ is written as a sum of terms with higher v-value.

If on the other hand, $v(\omega_k) \in \mathbb{Q}$ for an infinite sequence $(\omega_k)_{k\geq -1}$, then $\lim_{k\to\infty} v(\omega_k) = 0$ since by Lemma 3.2, $\sum_{i\geq -1}^{k} v(\omega_k) < 0$ for all $k \geq -1$ and $v(\omega_i) > 0$ for $i \geq 1$. Then for some $N \geq 1$, $v(\omega_N) < v(\omega_i)$ for all $1 \leq i < N$. The evaluation of $v(A_0 - B_0)$ again either stops beforehand or we get a unique term $A_{k,j}$ that has v-value equal to $v(\omega_{i_r}\omega_{i_r+1}\cdots\omega_N)$. As in the first case, this term is the one we get when we take the last term of $A_0^{(n)} - B_0^{(n)}$, written as a sum of terms $A_{1,j}$ with higher v-value and in each of the following steps whenever the v-value of this term is minimal, take the last term when $A_{k,j}$ is written as a sum of terms with higher v-value.

In both cases, the value of this term, $v(\omega_{i_r}\omega_{i_r+1}\cdots\omega_N)$ is strictly smaller than the value of all additional terms we get when we change the order of the factors in a product. It follows that given the v-values of $(\omega_i)_{i\geq -1}$, $v(A_0 - B_0)$ is the same as it would be if all elements of the sequence $(\omega_i)_{i\geq -1}$ commuted. This follows from the fact that when we change the order of factors ω_i and ω_j in some A_{k,j_1}, the term we obtain has v-value greater by $v[\omega_i,\omega_j] - v(\omega_i\omega_j) = -v(xy\omega_1\cdots\omega_j)$ for $-1 \leq i < j \leq N$ while $v(A_{k+1,j_1}) - v(A_{k,j_2})$ is for any j_1, j_2 equal to $v(\omega_{i_\ell+1})$ for some i_ℓ such that A_{k,j_2} contains a power of ω_{i_ℓ}. Since, as we have shown in the proof of Lemma 3.2, $\sum_{i=-1}^{N} v(\omega_i) < 0$, it follows that the terms we obtain by changing the order of the factors have v-value greater than $v(A_0 - B_0)$. And since $v(x^{k_0}\omega_{i_1-1}^{k_{i_1}}\cdots\omega_{i_r-1}^{k_{i_r}} - \overline{x^{k_0}\omega_{i_1-1}^{k_{i_1}}\cdots\omega_{i_r-1}^{k_{i_r}}})$ is higher than the v-value of any terms we get when we change the order of factors, the order of $\omega_{i_1},\ldots,\omega_{i_r}$ does not matter.

3.2 Extending v from the sequence $(\omega_i)_{i\geq -1}$ to $\mathcal{A}_1(\mathbb{R})$

We can now prove that every v associated to either a finite or an infinite sequence $(\omega_i)_{i\geq -1}$ can be extended to a valuation on $\mathcal{D}_1(\mathbb{R})$.

Lemma 3.7. *For every $r \geq 0$, there exists a finite number M of elements of the form $a_i := \omega_{-1}^{k_{i,-1}}\omega_0^{k_{i,0}}\omega_1^{k_{i,1}}\cdots\omega_{r-1}^{k_{i,r-1}}$ for some $k_{i,1},\ldots,k_{i,r-1} \in \mathbb{Z}$ such that $v(a_i) = 0$ for all $1 \leq i \leq M$ and every $\omega_{-1}^{\ell_{-1}}\cdots\omega_{r-1}^{\ell_{r-1}} \in \mathcal{D}_1(\mathbb{R})$ with v-value zero is $\sim$-equivalent to a product of positive integer powers of $a_1,\ldots,a_M$.*

Proof. Since $v(\omega_{-1}) = -1$ and $v(\omega_j) = \frac{m_{j+1}}{n_{j+1}} \in \mathbb{Q}$ for $j \geq 0$, the problem translates to finding general classes of solutions to the diophantine equation $x_0a_0 + \cdots x_ka_k = 0$ with $a_0 = -\Pi_{j=1}^{k} n_i$ and $a_i = \frac{m_i}{n_i}\Pi_{j=1}^{k} n_i$ for all $0 \leq i \leq k$. □

Theorem 3.8. *Let v and $(\omega_i)_{i\geq -1}$ be as described in the beginning of the section, i.e., $\omega_{-1} = x$, $\omega_0 = y$, $v(\omega_{-1}) = -1$, $v(\omega_i) = \frac{m_{i+1}}{n_{i+1}} \in \mathbb{Q}$, $\overline{x^{m_{i+1}}\omega_i^{n_{i+1}}} = \beta_{i+1} \in \mathbb{R}$, $\omega_{i+1} = x^{m_{i+1}}\omega_i^{n_{i+1}} - \beta_{i+1}$ for $i, 0 \leq i \leq N-1$ and $v(\omega_N) \notin \mathbb{Q}$ for some $N \geq 0$ or $v(\omega_i) \in \mathbb{Q}$ for infinitely many i, that $\sum_{i=-1}^{k} v(\omega_i) < 0$ for all $k \geq -1$. Supposse that $\operatorname{sgn}\beta_i$ is constant on the set of all i for which n_i is even. Then v can be extended to a valuation on $\mathcal{D}_1(\mathbb{R})$ with residue field $\mathbb{R}$. The valuation is unique for every choice of $\{\alpha_{i,j}\}_{i,j\geq 0}$ where $\alpha_{i,j} = \overline{\omega_{i-1}^{K_{i,j}}\omega_{j-1}^{K_{j,i}}}, K_{i,j} = \frac{m_jn_i}{d_{i,j}}, K_{j,i} = -\frac{m_in_j}{d_{i,j}}$ with $d_{i,j} = \gcd\{m_jn_i, m_in_j\}$. The associated value group is group-isomorphic to a subgroup of $\mathbb{Q}\times\mathbb{Z}$ generated by $\{v(\omega_i)\}_{i\geq -1}$.*

Proof. The following construction of the valuation v associated to the sequence $(\omega_i)_{i\geq -1}$ was first sketched in [22]. Here we present it in full detail.

Before we begin with the construction of the v-value for an arbitrary element of $\mathcal{D}_1(\mathbb{R})$, we define it for some specific elements of $\mathcal{D}_1(\mathbb{R})$.

1. Since we have defined $v(\omega_i)$ for all $-1 \leq i \leq N$, $v(\Pi_{i=-1}^{N}\omega_i^{k_i}) = \sum_{i=-1}^{N} k_i v(\omega_i)$ must hold for all $k_{-1}, \ldots, k_N \in \mathbb{Z}$.

2. Since we supposed $\sum_{i=-1}^{k} v(\omega_i) < 0$ for all $k \geq -1$, it follows from Lemma 3.2 that
$$v[\omega_i, \omega_j] = -v(\omega_{-1}\omega_0 \cdots \omega_{i-1}\omega_{i+1} \cdots \omega_{j-1}),$$
which must be strictly greater than $v(\omega_i\omega_j)$ for all $i < j$.

3. We also see that if $v(\omega_{-1}^{k_0} \cdots \omega_{r-1}^{k_r}) = 0$ for some $k_0, \ldots, k_r \in \mathbb{Z}$, then $\overline{\omega_{-1}^{k_0} \cdots \omega_{r-1}^{k_r}}$ is uniquely determined by $\{\alpha_{i,j}\}_{i,j\geq 0}$ as in shown in Proposition 3.4. In this case, $v(\omega_{-1}^{k_0} \cdots \omega_{r-1}^{k_r} - \overline{\omega_{-1}^{k_0} \cdots \omega_{r-1}^{k_r}})$ must be equal to the value determined in Lemma 3.6 and the discussion following it.

In all three cases, the chosen values were the only possible extensions of v from $(\omega_i)_{i\geq -1}$ if we want v to be a valuation.

To determine $v(F)$ for any $F \in \mathcal{A}_1(\mathbb{R})$, we first note that F can be written as a finite sum
$$F = \sum_{\ell} \alpha_\ell x^{i_\ell} y^{j_\ell}, \alpha_\ell \in \mathbb{R}.$$
Let F_1 be the sum of all terms $\alpha_\ell x^{i_\ell} y^{j_\ell}$ such that $i_\ell v(x) + j_\ell v(y)$ is equal to $u := \min_\ell\{i_\ell v(x) + j_\ell v(y)\}$.

If F_1 consists of only one such term, then we define $v(F) = u$; this is obviously always the case whenever $v(y) \notin \mathbb{Q}$. Otherwise, we factor out $x^{i_1}y^{j_1}$ with the smallest power of x and get
$$F_1 \sim x^{i_1}y^{j_1} \sum_{\ell,\ i_\ell v(x)+j_\ell v(y)=u} \alpha_\ell x^{i_\ell - i_1} y^{j_\ell - j_1}.$$
Since
$$(i_\ell - i_1)v(x) + (j_\ell - j_1)v(y) = 0,$$
for each ℓ in the sum, $\frac{i_\ell - i_1}{j_\ell - j_1} = K_\ell \frac{m_1}{n_1}$ for some $K_\ell \in \mathbb{Z}$. We can write
$$F_1 \sim x^{i_1}y^{j_1} f(x^{m_1}y^{n_1})$$
where $f(t)$ is a polynomial in $\mathbb{R}[t]$. Since we know $v(\omega_1) > 0$ and $v(\alpha) = 0$ for $\alpha \in \mathbb{R}^*$, v is uniquely determined on $\mathbb{R}[\omega_1]$. From this, it follows that $v(f(x^{m_1}y^{n_1})) = 0$ if and only if $f(\beta_1) \neq 0$ since $x^{m_1}y^{n_1} = \omega_1 + \beta_1$.

In this case, $v(F_1) = u$ and since all terms in $F - F_1$ have v-value strictly greater than u, $v(F) = u$ must hold. Since $v(u)$ is a sum of integer powers of $v(x)$ and $v(y)$, $v(F)$ is in

the abelian group, generated by $\{v(\omega_i)\}_{i\geq -1}$. If $u=0$, $\overline{F}=\beta_1^k f(\beta_1)\in\mathbb{R}$. If on the other hand $f(\beta_1)=0$, write $f(t)=g_1(t)(t-\beta_1)^{k_1}$ with $g_1(\beta_1)\neq 0$ and we have

$$F_1 \sim x^{i_1}y^{j_1}g_1(x^{m_1}y^{n_1})\omega_1^{k_1}.$$

We set $v(F_1)=u+k_1v(\omega_1)$ and add all terms we get from exchanging the order of factors, whose v-value can be lower than the newly set $v(F_1)$, although still strictly higher than u due to $v[x,y]>v(xy)$, to $F-F_1$. It is immediate that $v(F_1)$ is in the subgroup of Γ, generated by $v(x), v(y)$ and $v(\omega_1)$ and that if $v(F_1)=0$, $\overline{F_1}\in\mathbb{R}$. It is important to note that in both cases, we consider F_1 as a single term. It follows that during our transformation, the number of terms (if we ignore the ones we got when we changed the order of factors in a product) is strictly smaller than before (unless, of course, F_1 was just a single term in the beginning and we get $v(F)=v(F_1)$).

We now consider the values of the terms in $F-F_1$. If all of them have v-value strictly greater than that of F_1, we conclude $v(F)=v(F_1)$. Otherwise, we take all terms of

$$F-F_1=\sum_{\ell',\ i_{\ell'}v(x)+j_{\ell'}v(y)>u}\alpha_{\ell'}x^{i_{\ell'}}y^{j_{\ell'}},\alpha_{\ell'}\in\mathbb{R}$$

for which $i_{\ell'}v(x)+j_{\ell'}v(y)=u':=\min_{\ell'}\{i_{\ell'}v(x)+j_{\ell'}v(y)\}$ and then as before define

$$F_2=x^{i_2}y^{j_2}\sum_{\ell',\ i_{\ell'}v(x)+j_{\ell'}v(y)=u'}\alpha_{\ell'}x^{i_{\ell'}-i_2}y^{j_{\ell'}-j_2}.$$

As above, we write $F_2\sim x^{i_2}y^{j_2}g_2(x^{m_1}y^{n_1})(x-\beta_1)^{k_2}$, $k_2\geq 0$, $g_2(\beta_1)\neq 0$ and add all the terms we get when we change the order of factors to $F-F_1-F_2$. Their v-value is strictly greater than u' due to $v[x,y]>v(xy)$.

We continue this process, defining $F_1,F_2,\dots,F_k$ until all terms in $F-F_1-\cdots-F_k$ have v-value strictly greater than $\min\{F_1,\dots,F_k\}$. Note that it is possible that F_k consists of only one term from $F-F_1-\cdots-F_{k-1}$.

Afterwards, we sum together all those F_i for $1\leq i\leq k$ for which $v(F_i)=u_1:=\min\{v(F_1),\dots,v(F_k)\}$. If the minimum is achieved at exactly one such F_i, we set $v(F)=v(F_i)$. This is always the case whenever $v(\omega_1)\notin\mathbb{Q}$. Otherwise we can relabel the terms so the minimum is achieved at $F_1,\dots,F_r$ for some $r\leq k$. As we have shown, each F_i can be written as $F_i=x^{i_i}y^{j_i}g_i(x^{m_1}y^{n_1})\omega_1^{k_i}$. We sum the terms together, factor out $x^{i_1}y^{j_1}\omega_1^{k_1}$, the term that has, written as a polynomial in x and y, the lowest power of x, and label the new sum $F_{1,1}$.

To evaluate $v(F_{1,1})$, we follow a procedure similar to the one evaluating $v(F_1)$. After factoring $x^{i_1}y^{j_1}\omega_1^{k_1}$, we are left with

$$\begin{aligned}F_{1,1}&\sim x^{i_1}y^{j_1}\omega_1^{k_1}(g_1(x^{m_1}y^{n_1})+g_2(x^{m_1}y^{n_1})x^{i_2-i_1}y^{j_2-j_1}\omega_1^{k_2-k_1}+\cdots\\&\quad+g_r(x^{m_1}y^{n_1})x^{i_r-i_1}y^{j_r-j_1}\omega_1^{k_r-k_1})\\&\sim x^{i_1}y^{j_1}\omega_1^{k_1}\sum_{J=1}^{R}\alpha_J x^{i_J}y^{j_J}\omega_1^{k_J},\text{ with }\alpha_J\in\mathbb{R},i_J,j_J,k_j\in\mathbb{Z},R\geq 1.\end{aligned}$$

Each term in the sum has v-value zero. Let $a_1,a_2,\cdots,a_\ell$ be the terms such that each product of the form $x^iy^j\omega_1^k$, $i,j,k\in\mathbb{Z}$ that fulfills the condition $v(x^iy^j\omega_1^k)=0$ is a

product of positive integer powers of some of a_i up to the order of factors x, y and ω_1. The existence of $a_1, \dots, a_\ell$ is assured by Lemma 3.7. We can then write

$$\begin{aligned} F_{1,1} &\sim x^{i_1} y^{j_1} \omega_1^{k_1} \sum_{J=1}^{R} \gamma_J a_1^{m_{1,J}} a_2^{m_{2,J}} \cdots a_\ell^{m_{\ell,J}} \\ &\sim x^{i_1} y^{j_1} \omega_1^{k_1} g(a_1, \cdots, a_\ell), g \in \mathbb{R}[t_1, \cdots, t_\ell] \end{aligned} \tag{3.7}$$

with $\gamma_J \in \mathbb{R}$, $m_{I,J} \in \mathbb{Z}$ for all $1 \leq I \leq \ell$ and $1 \leq J \leq R$. As before, we add all terms we get when we change the order of multiplication of x, y or ω_1 in a product to $F - F_{1,1}$ since the value of its terms is strictly greater than u_1. Since, as we have determined in the beginning, each term in the sum (3.7) has v-value equal to zero and we know what $\overline{a_i} \in \mathbb{R}$ is for each $1 \leq i \leq \ell$, $v(g(a_1, \dots, a_\ell))$ will have to be greater than or equal to zero, we can define $\overline{g(a_1, \dots, a_\ell)} = g(\overline{a_1}, \dots, \overline{a_\ell})$.

If $g(\overline{a_1}, \dots, \overline{a_\ell}) \neq 0$, then we set $v(g(a_1, \dots, a_\ell)) = 0$ and $v(F) = v(F_{1,1}) = i_1 v(x) + j_1 v(y) + k_1 v(\omega_1)$. Otherwise write

$$g(t_1, \dots, t_\ell) = h(t_1 - \overline{a_1}, \dots, t_\ell - \overline{a_\ell}) = \sum_{i=1}^{L} \Pi_{j=1}^{\ell} (t_j - \overline{a_j})^{m_{i,j}} h_i(t_1, \dots, t_\ell)$$

with $h, h_1, \dots, h_L \in \mathbb{R}[t_1, \dots, t_n]$ and $h_i(\overline{a_1}, \dots, \overline{a_\ell}) \neq 0$ for all i. We factor out the $\Pi_j (t_j - \overline{a_j})^{m_{i,j}}$ for those i for which $\sum_j v(a_j - \overline{a_j})^{m_{i,j}}$ is minimal. Then

$$g(t_1, \dots, t_\ell) = \Pi_j (t_j - \overline{a_j})^{m_{i,j}} \tilde{g}(t_1, \dots, t_k), \text{ with } \tilde{g} \in \mathbb{R}[t_1, \dots, t_\ell].$$

If $\tilde{g}(\overline{a_1}, \dots, \overline{a_k}) \neq 0$, we set

$$v(F_{1,1}) = v(x^{i_1} y^{j_1}) + \sum_j m_{i,j} v(a_j - \overline{a_j}).$$

If on the other hand, $\tilde{g}(\overline{a_1}, \dots, \overline{a_k}) = 0$, we do the same thing as we did with g. The process cannot go on indefinitely since g is a polynomial and hence of finite degree. All terms we get when we exchange the order of x, y and ω_1 are added to $F - F_{1,1}$. Their v-value must be strictly greater than u_1. It follows from the construction that $v(F_{1,1})$ must be in the group generated by $\{v(\omega_i)\}_{i \geq -1}$ since this holds for $v(a_i - \overline{a_i})$ for all i and that if $v(F_{1,1}) = 0$, $\overline{F_{1,1}} \in \mathbb{R}$.

Since $v(a_i - \overline{a_i})$ is, as we have shown in Lemma 3.6 and the discussion following it, a sum of $v(\omega_j)$ and thus $v(\Pi_j \omega_j^{-1}(a_i - \overline{a_i})) = 0$, we can write $F_{1,1}$ as one term of the form $\Pi_{i=-1}^{n} \omega_i^{k_i} g(a_1, a_2, \dots, a_\ell)$ with $n \in \mathbb{N}$ and $g \in \mathbb{R}[t_1, \dots, t_\ell]$ and $g(\overline{a_1}, \overline{a_2}, \dots, \overline{a_\ell}) \neq 0$.

After $v(F_{1,1})$ is set, we compare it to both $v(F_i)$ for all F_i that are not part of $F_{1,1}$ and the terms of $F - F_1 - \cdots - F_k - F_{1,1}$. If all of these terms have v-value strictly greater than $v(F_{1,1})$, then we can set $v(F) = v(F_{1,1})$. Otherwise, we collect all terms with minimal v-value in a sum which we label $F_{1,2}$. We determine $v(F_{1,2})$ in the same way we determined $F_{1,1}$ and then sum all of the remaining terms that have v-value less or equal to $\min\{v(F_{1,1}), v(F_{1,2})\}$ to a sum labeled $F_{1,3}$.

We repeat the process until for some k, $\min\{v(F_{1,1}), \cdots, v(F_{1,k})\}$ is strictly smaller than the v-value of any of the remaining terms.

If $\min\{v(F_{1,1}), \cdots, v(F_{1,k})\}$ is achieved at exactly one i, we set $v(F) = v(F_{1,i})$. Otherwise we sum all the terms with the minimal v-value and label the sum $F_{2,1}$. We

evaluate $v(F_{2,1})$ in the same way we evaluated $v(F_{1,1})$. We repeat the process, defining $F_{i,j}$ and determining its v-value in the same way as above. We point out that after $v(F_{i,j})$ is defined, we regard $F_{i,j}$ as one single term in future evaluations.

Now we must show that at one point, the process ends, i.e., that for some i, j, $v(F_{i,j})$ is strictly smaller than the v-value of all other terms. This holds because each time we define $F_{i,j}$ for some i, j, we sum a number of different terms into one single term and because whenever we change the order of factors in a term, the degree of x and y in the difference is strictly smaller. This means that we eventually run out of terms. We have thus defined v for an arbitrary polynomial $F \in \mathcal{A}_1(\mathbb{R})$. What we essentially did was that we wrote

$$F = \tilde{F} + \tilde{F}_1$$

where $\tilde{F}$ is written as a single term, $v(\tilde{F})$ is computed as if x and y commuted and the v-value of each term of $\tilde{F}_1$ is strictly greater than $v(\tilde{F})$. For another $G \in \mathcal{A}_1(\mathbb{R})$, we can write

$$FG = \tilde{FG} + (F\tilde{G})_1$$

and since we evaluate $v(\tilde{F})$ and $v(\tilde{G})$ as if x and y commuted, $v(\tilde{FG}) = v(\tilde{F}) + v(\tilde{G})$. We use the same reasoning to show $v(F + G) \geq \min\{v(F), v(G)\}$.

It follows from the construction that for each i, j, $v(F_{i,j})$ is a linear combination of $\{v(\omega_i)\}_{i \geq -1}$ and that in case $v(F_{i,j}) = 0$, $\overline{F_{i,j}} \in \mathbb{R}$. □

Theorem 3.9. *Let v be a valuation on $\mathcal{A}_1(\mathbb{R})$ trivial on $\mathbb{R}$ with residue field $\mathbb{R}$. Then v is strongly abelian.*

Proof. If v's value group is $\mathbb{Q}$, then the theorem follows from Corollary 2.4. Otherwise, $v(\omega_N) \notin \mathbb{Q}$ for some N by our construction. But as we have shown in Lemma 3.2, $v[\omega_N, x] = -v(y\omega_1 \cdots \omega_{N-1})$. If $v(\omega_N x) = v[\omega_N, x]$, it follows that $v(\omega_N) \in \mathbb{Q}$, a contradiction. Since the value group is generated by $\{v(\omega_i)\}_{i \geq -1}$, it follows from Proposition 2.7 that v is strongly abelian. □

4 Valuations on $R[y; \delta]$

In this section, we explain a construction of valuations on the ring $R[y; \delta]$ with

$$R := \{\sum_{k \geq m} a_k x^{-\frac{k}{n}} \mid a_k \in \mathbb{R}, m \in \mathbb{Z}, n \in \mathbb{N}\}$$

and $\delta(p(x)) = p'(x)$. This construction, which was first introduced in [16], will, as we will see in this section, give us all valuations on $R[y; \delta]$ with residue field $\mathbb{R}$. Then, we will prove exactly which valuations on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$ extend to a valuation on $R[y; \delta]$ with the same residue field, answering the question posed by Marshall and Zhang in [16]. We will see the extensions of valuations on $R[y; \delta]$ are strongly abelian.

Every valuation on $R[y; \delta]$ can be uniquely extended to its quotient ring, which we label as D, because $R[y; \delta]$ is an Ore domain. Since $[y, x] = 1$ as before, $v(xy) < 0$ must hold. We set $v(x) = -1$, $z_0 := y$ and consider $v(y)$. If $v(y) \notin \mathbb{Q}$, then

$$v(\sum_{i=0}^{n} p_i(x) y^i) = \min_{0 \leq i \leq n} \{v(p_i(x)) + iv(y)\}$$

for any $\sum_{i=0}^{n} p_i(x)y^i \in R[y;\delta]$. Otherwise $v(y) = r_1 \in \mathbb{Q}$ and hence $v(y - \gamma_1 x^{-r_1}) > v(y)$ for some $\gamma_1 \in \mathbb{R}$. If $v(z_1) = r_2 \in \mathbb{Q}$ for $z_1 := y - \gamma_1 x^{-r_1}$, we proceed to find $z_2 = z_1 - \gamma_2 x^{-r_2}$ such that $v(z_2)$ is greater than r_2. We repeat this process to construct a sequence $(z_i)_{i\geq 0}$.

If $v(z_k) \notin \mathbb{Q}$ for some $k \in \mathbb{N}$, then we can write every $f \in R[y;\delta]$ as $\sum_{i=0}^{n} p_i(x)z_k^i$ and deduce

$$v(f) = \min_{0\leq i\leq n} \{v(p_i(x)) + iv(z_k)\}.$$

The value group is then group-isomorphic to $\mathbb{Q}\times\mathbb{Z}$. Since $v[x, z_k] = v[x, y] = 0 > v(xz_k)$, v is strongly abelian by Proposition 2.7. Otherwise, the sequence $(z_i)_{i\geq 0}$, $v(z_i) = r_{i+1} \in \mathbb{Q}$ is infinite. We take note of the fact that $v(z_{i+1}) > v(z_i)$ and since $[z_i, x] = [y, x] = 1$ for all i, $v(z_i) < 1$ for all i. We define $r := \lim_{i\to\infty} r_i \leq 1$.

4.1 Case $r < 1$

If $r < 1$, it has been shown in [16] that v can be extended to a valuation on $R[y;\delta]$ with residue field $\mathbb{R}$. We first extend v from R to

$$\tilde{R} = \{\sum_{q\in A} a_q x^{-q} \mid a_q \in \mathbb{R}, A \subset \mathbb{Q} \text{ is well-ordered}\}$$

in a natural way, i.e., by defining

$$v(\sum_{q\in A} a_q x^{-q}) = \min A$$

for each $\sum_{q\in A} a_q x^{-q} \in \tilde{R}[y;\delta]$. Then for every $f(t) \in R[t]$, define $v(f(y)) = v(f(z))$ with $z := \sum_{i\geq 1}^{\infty} a_i x^{-r_i}$ and $f(y) = \sum_{i=0}^{n} p_i y^i$ for $f(t) = \sum_{i=0}^{n} p_i t^i$. This gives rise to a valuation on $\tilde{R}[y;\delta]$.

However if $r = 1$, we cannot define a valuation in this way. Let $k \in \mathbb{N}$ be such that $2r_k > 1 + r_1$, which exists since $r = 1$, and $a_k = y - z_k = \sum_{i=1}^{k} \gamma_i x^{-r_i}$. Let

$$f(t) = (t - a_k)(t - a_k) = t^2 - 2ta_k + a_k^2 \in R[t].$$

On one hand,

$$v(f(y)) = v(f(z)) = 2v(z - a_k) = 2r_{k+1}.$$

On the other,

$$2r_{k+1} = v((y-a_k)(y-a_k)) = v(y^2-2ya_k+a_k^2+[y, a_k]) = \min\{2r_{k+1}, 1+r_1\} = 1+r_1,$$

contradicting the assumption that v is a valuation, as shown in [16].

Of course, even in case $r < 1$, there may also exist a k such that $2r_k > 1 + r_1$. But the important difference between the two cases is that if $r < 1$, there is always an $\ell \in \mathbb{N}$ such that $1 + r_\ell > 2r_k$ for all $k \in \mathbb{N}$, which does not hold in case $r = 1$. Then, since

$$f\colon R[y;\delta] \to R[y;\delta], f(y) = z_\ell, f(a) = a \text{ for } a \in R$$

is a real algebra automorphism of $R[y;\delta]$, we can translate the sequence by replacing y with z_ℓ.

We see that since the associated value group is $\mathbb{Q}$, v is a strongly abelian valuation by Corollary 2.4.

4.2 Case $r = 1$

The question whether in case $r = 1$, v can be extended from a sequence $(z_i)_{i\geq 0}$ to a valuation on $R[y;\delta]$ was left open in [16]. In this subsection, we show that it can be done using model theory (for reference, see for example [19]). We also show that the valuation we get in this way is uniquely determined.

Suppose we have infinite sequences $(z_i)_{i\geq 0} \subseteq R[y;\delta]$, $(r_i)_{i\geq 1} \subseteq \mathbb{Q}$ and $(\gamma_i)_{i\geq 1} \subseteq \mathbb{R}$ and $v\colon (z_i)_{i\geq 0} \to \mathbb{Q}$ with $z_0 = y$, $z_{i+1} = z_i - \gamma_{i+1}x^{-r_{i+1}}$ and $v(z_i) = r_{i+1} \in \mathbb{Q}$ with $(r_i)_{i\geq 1}$ a strictly increasing sequence with $r = \lim_{i\to\infty} r_i = 1$. Then for each $n \geq 0$, there is a valuation v_n on $R[y;\delta]$ such that $v_n(z_i) = r_{i+1}$ for all $0 \leq i \leq n-1$ and $v_n(z_n) \notin \mathbb{Q}$.

We now present the first-order theory that the valuation associated to the infinite sequence we wish to prove exists is a model of. The theory will be a union of the theory of D, the quotient division ring of $R[y;\delta]$ and the theory of valuations. We will see that each finite subset of this theory has a model. By compactness, so does the whole theory.

The language of our theory will be

$$F \cup \{+, -, \cdot, ^{-1}, O, <\} \cup \{c_{z_i} \mid i \geq -1\}$$

where F is the set of all constants c_a for each $a \in D$, $+$, $\cdot$ and $<$ are binary function symbols, $-$ and $^{-1}$ are unary function symbols, O is an unary relation symbol and c_{z_i} is a constant for all $i \geq 0$. Let $\mathcal{A}$ be the theory of the quotient division ring of the ring $R[y;\delta]$. By $\mathcal{B}$ we will denote the set of axioms for valuation rings O on division rings:

1. $O(0) \wedge O(1)$
2. $\forall a : O(a) \vee O(a^{-1})$
3. $\forall a, b : O(a) \wedge O(b) \to O(a+b) \wedge O(ab) \wedge O(ba)$

We add all sentences $\mathcal{C}$ that will give proper meaning to the constants c_{z_i} for all $i \geq -1$:

4. $c_{z_0} = c_y$
5. $c_{z_{i+1}} = c_{z_i} - c_{\gamma_{i+1}x^{-r_{i+1}}}$
6. $O(c_{x^{r_{i+1}}z_i}) \wedge O(c_{(x^{r_{i+1}}z_i)^{-1}})$

Our theory is then the union of all the above axioms from $\mathcal{A}$ to $\mathcal{C}$. Since all finite subsets of the theory have a model, namely, the valuation v_n described in the beginning of this subsection, so does, by compactness, the whole theory. Since the theory contains F, the set of all constants c_a for each $a \in D$, the models are valued division rings which all contain D. We pick a model of the theory, a pair (D_1, v), where D_1 is a division ring with valuation v.

We now show that the v-value is uniquely determined for every $f \in R[y;\delta]$. It will then follow that v is uniquely determined on the whole quotient ring D. Every $f \in R[y;\delta]$ can be written as

$$f = \sum_{i=0}^{n} p_i^{(0)}(x)y^i, \text{ with } p_i^{(0)}(x) \in R \text{ for each } 0 \leq i \leq n.$$

For the time being, we ignore the terms we get when we change the order of multiplication. At the end of this subsection, we will see that they do not influence $v(f)$. For each $k \geq 1$, we define

$$a_k := y - z_k = \sum_{i=1}^{k} \gamma_i x^{-r_i}$$

and write

$$f = \sum_{i=0}^{n} p_i^{(0)}(x) y^i = \sum_{i=0}^{n} p_i^{(0)}(x)(a_k + z_k)^i$$
$$\sim \sum_{i=0}^{n} p_i^{(0)}(x) \sum_{j=0}^{i} \binom{i}{j} a_k^{i-j} z_k^j = \sum_{j=0}^{n} p_j^{(k)}(x) z_k^j$$

with

$$p_j^{(k)}(x) := \sum_{i=j}^{n} \binom{i}{j} p_i^{(0)}(x) a_k^{i-j}$$

for each $0 \leq j \leq n$ and $k \geq 1$. For each $0 \leq j \leq n$, $g_j(t) := \sum_{i=j}^{n} \binom{i}{j} p_i^{(0)}(x) t^i$ is a polynomial in $R[t]$. The quotient field of

$$C := \{ \sum_{k \geq m} a_k x^{-\frac{k}{n}} \mid a_k \in \mathbb{C}, m \in \mathbb{Z}, n \in \mathbb{N} \}$$

is the algebraic closure of the quotient field of R, as shown in for example [14]. Since $\sum_{i=1}^{\infty} \gamma_i x^{-r_i}$ is not in the quotient field of C, it is not a root of $g_j(t)$ for any $0 \leq j \leq n$. We conclude that for some $K \in \mathbb{N}$, $v(p_j^{(k)}(x)) = v(p_j^{(K)}(x))$ for all $k \geq K$ and all $0 \leq j \leq n$. We can then write

$$f = \sum_{i=0}^{n} p_i^{(0)}(x) y^i = \sum_{i=0}^{n} p_i^{(K)}(x) z_K^i = \sum_{i=0}^{n} p_i^{(k)}(x) z_k^i$$

with $v(p_i^{(k)}(x)) = v(p_i^{(K)}(x))$ for all $k \geq K$.

We now show that from some $K' \geq K$, $v(p_0^{(k)}) < v(p_i^{(k)} z_k^i)$ for all $1 \leq i \leq n$ and all $k > K'$. For all $k > K$,

$$p_0^{(k+1)}(x) = \sum_{i=0}^{n} p_i^{(k)}(x)(a_{k+1} - a_k)^i = \sum_{i=0}^{n} p_i^{(k)}(x)(\gamma_{k+1} x^{-r_{k+1}})^i$$

with $v(p_i^{(k)}(x)) = v(p_i^{(K)}(x))$. Since $(r_i)_{i \geq 1}$ is an increasing sequence with $\lim_{i \to \infty} r_i = 1$, there exists $K' \geq K$ such that

$$\min_{i=0,\ldots,n} \{ v(p_i^{(K')}(x)) + i r_{K'+1} \} = \min_{i=0,\ldots,n} \{ v(p_i^{(K)}(x)) + i r_{K'+1} \}$$

is achieved at exactly one $0 \leq i \leq n$. We conclude $v(p_0^{(K'+1)}) = v(p_0^{(K)})$. Then for each $1 \leq i \leq n$,

$$v(p_i^{(k)}(x) z_k^i) = v(p_i^{(k)}(x)) + i r_{k+1} = v(p_i^{(K)}(x)) + i r_{k+1} > v(p_i^{(K)}(x)) + i r_k \geq v(p_0^{(K)}).$$

To show that $v(f)$ is equal to $v(p_0^{(K)}(x)) \in \mathbb{Q}$, we must show that the v-value of all the terms we get when we change the order of multiplication must be strictly greater than $v(p_0^{(K)}(x))$. For all $k \geq 1$, we write

$$p_0^{(k)}(x) = \sum_{i=0}^{n} p_i^{(0)}(x) a_k^i = \sum_{i=0}^{n} p_i^{(0)}(x) (\sum_{j=1}^{k} \gamma_j x^{-r_j})^i = \sum_{i=0}^{n} \sum_{j=1}^{k_i} p_i^{(0)}(x) \alpha_i x^{-q_j},$$

with $q_j \in \mathbb{Q}$ for all $1 \leq j \leq k_i$ and $1 \leq i \leq n$. Since for all $0 \leq i \leq n$, $p_i^{(0)}(x) \in R$ and $(r_i)_{i \geq 1}$ is an increasing sequence with $\lim_{i \to \infty} r_i = 1$, there exists some $k \geq 1$ such that the term of the sum with v-value

$$\min_{i=1,\ldots,n} \{v(p_i^{(0)}(x)) + (i-1)r_1 + r_k\}$$

is the only term in the sum with its v-value. We conclude

$$v(p_0^{(K)}(x)) = v(p_0^{(k)}(x)) \leq v(p_i^{(0)}(x)) + (i-1)r_1 + r_k \tag{4.1}$$

for all $1 \leq i \leq n$. On the other hand, we can write

$$f = \sum_{i=0}^{n} p_i^{(0)}(x) y^i = \sum_{i=0}^{n} p_i^{(0)}(x)(a_k + z_k)^i.$$

For all $0 \leq i \leq n$, all terms of $(a_k + z_k)^i$ when expaned are of the form $a_k^{\ell_1} z_k^{\ell_2} \ldots a_k^{\ell_{i-1}} z_k^{\ell_i}$ with $\ell_1, \ldots, \ell_i \geq 0$ and $\ell_1 + \cdots + \ell_i = i$. Since $v(a_k) = r_1$, $v(z_k) = r_{k+1}$ and

$$v[a_k, z_k] = v[\sum_{j=1}^{k} \gamma_j x^{-r_j}, y - \sum_{j=1}^{k} \gamma_j x^{-r_j}] = v(\sum_{j=1}^{k} \gamma_j [x^{-r_j}, y]) = 1 + r_1,$$

it follows that the v-value of each term we get when we change the order of multiplication is at least $v(p_i^{(0)}(x)) + (i-1)r_1 + 1$ for each $1 \leq i \leq n$, which is, as is immediate from (4.1), strictly greater than $v(p_0^{(K)}(x))$. We thus conclude $v(f) = v(p_0^{(K)}(x)) \in \mathbb{Q}$. It also follows that $v(f) = v_k(f)$ for all $k \geq K'$ with v_k as defined in the beginning of this section. As every element of D, the quotient ring for $R[y;\delta]$, can be written as fg^{-1} with $f, g \in R[y;\delta]$, it follows that v is uniquely determined on D. We see that the value group for v is equal to $\mathbb{Q}$. We conclude from Corollary 2.4 that v is strongly abelian.

It remains to show that the residue field for v is equal to $\mathbb{R}$. Suppose $v(f) = 0$ for some $f \in D$. Then $v_k(f) = 0$ for all $k \geq K$ for some $K \in \mathbb{N}$. We can write

$$f = (\sum_{i=0}^{m} p_i^{(K)} z_K^i)(\sum_{j=0}^{n} q_j^{(K)} z_K^j)^{-1}$$

with $p_i^{(K)}, q_j^{(K)} \in R$ and

$$v(\sum_{i=0}^{m} p_i^{(K)} z_K^i) = v(p_0^{(K)}) = v(\sum_{j=0}^{n} q_j^{(K)} z_K^j) = v(q_0^{(K)}) = q \in \mathbb{Q}.$$

It follows that $v(x^q \sum_{i=0}^{m} p_i^{(K)} z_K^i) = v(x^q \sum_{j=0}^{n} q_j^{(K)} z_K^j) = 0$ and $\alpha := \overline{x^q \sum_{i=0}^{m} p_i^{(K)} z_K^i} = \overline{x^q p_0^{(K)}} \in \overline{R} = \mathbb{R}$, $\beta := \overline{x^q \sum_{j=0}^{n} q_j^{(K)} z_K^j} = \overline{x^q q_0^{(K)}} \in \overline{R} = \mathbb{R}$. We conclude $\overline{f} = \alpha\beta^{-1} \in \mathbb{R}$. So the residue field for v is indeed equal to $\mathbb{R}$.

4.3 Extensions of valuations from $\mathcal{A}_1(\mathbb{R})$ to $R[x;\delta]$

In this section, we characterize the valuations on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$ that have an extension to $R[y;\delta]$ with the same residue field.

Since $x^{\frac{m_i}{n_i}} \in R[y;\delta]$, it follows that any valuation v' that extends v to a valuation on $R[y;\delta]$ with residue field $\mathbb{R}$ must satisfy $v'(x^{\frac{m_i}{n_i}}\omega_{i-1}) = 0$ and $\tilde{\gamma_i} := \overline{x^{\frac{m_i}{n_i}}\omega_{i-1}} \in \mathbb{R}$. In the next proposition, we show the necessary condition for a valuation v on $\mathcal{A}_1(\mathbb{R})$ to have an extension v' to $\mathbb{R}[y;\delta]$ with the same residue field.

Proposition 4.1. *Let v be a valuation on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$ associated to a sequence $(\omega_i)_{i\geq -1}$ with $v(\omega_{i-1}) = \frac{m_i}{n_i}$ for $i \geq 1$ and $\overline{x^{m_i}\omega_{i-1}^{n_i}} = \beta_i \in \mathbb{R}$. Let $\alpha_{i,j} \in \mathbb{R}$ be as in* Section 3. *Let 2^{h_i} be the greatest power of two dividing n_i for all $i \geq 0$. Then v can be extended to a valuation on $R[y;\delta]$ with the same residue field only if it fulfils the following conditions:*

(1) *For each i such that n_i is even, $\beta_i > 0$ must hold, and*

(2) *for each i, j, ℓ with $h_i < h_j \leq h_\ell$, $\alpha_{i,j}\alpha_{i,\ell} > 0$ must hold.*

Proof. Since

$$\tilde{\gamma_i}^{n_i} = \overline{(x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i}} = \overline{x^{m_i}\omega_{i-1}^{n_i}} = \beta_i$$

due to Proposition 2.2, it is obvious that $\tilde{\gamma_i}$ must be equal to an n_i-th root of β_i. If n_i is odd, $\tilde{\gamma_i} \in \mathbb{R}$ is uniquely determined regardless of $\operatorname{sgn}(\beta_i)$, while if n_i is even, $\tilde{\gamma_i} \in \mathbb{R}$ only if $\beta_i > 0$. It is thus obvious that $\beta_i > 0$ must hold for all i where n_i is even if v can be extended from a valuation on $\mathcal{A}_1(\mathbb{R})$ to a valuation on $R[y;\delta]$ with the same residue field. This proves the necessity of the first condition.

To prove the necessity of the second condition, we first observe that

$$\alpha_{i,j} = \overline{\omega_{i-1}^{K_{i,j}}\omega_{j-1}^{-K_{j,i}}} = \tilde{\gamma_i}^{K_{i,j}}\tilde{\gamma_j}^{-K_{j,i}},$$

holds for all $i, j \geq 0$. If $h_i < h_j$, $K_{i,j}$ is odd while $K_{j,i}$ is even, so $\operatorname{sgn}(\gamma_i) = \operatorname{sgn}(\alpha_{i,j})$ must hold. We can therefore see that

$$\alpha_{i,j}\alpha_{i,\ell} = \tilde{\gamma_i}^{K_{i,j}+K_{i,\ell}}\tilde{\gamma_j}^{-K_{j,i}}\tilde{\gamma_\ell}^{-K_{\ell,i}}$$

for all $i, j, \ell \geq 0$. If $h_i < h_j \leq h_\ell$, both $K_{i,j}$ and $K_{i,\ell}$ are odd while $K_{j,i}$ and $K_{\ell,i}$ are even. It follows that if v can be extended to a valuation on $R[y;\delta]$ with residue field $\mathbb{R}$, $\alpha_{i,j}\alpha_{i,\ell} > 0$ must hold for all $i, j, \ell \geq 0$ with $h_i < h_j \leq h_\ell$. □

In this section, we show that the conditions (1) and (2) of Proposition 4.1 are also sufficient for v to have an extension to $R[y;\delta]$ with residue field $\mathbb{R}$. Let v be any valuation on $\mathcal{A}_1(\mathbb{R})$ satisfying the conditions described in Proposition 4.1. We will first determine $\tilde{\gamma_i} \in \mathbb{R}$ for all $i \geq 0$. If n_i is odd, there is a unique choice of $\tilde{\gamma_i} \in \mathbb{R}$. Suppose then n_i is even and $\beta_i > 0$ for some $i \geq 0$. If $h_i < h_j$ for some j, then $\operatorname{sgn}(\tilde{\gamma_i}) = \operatorname{sgn}(\alpha_{i,j}) = \operatorname{sgn}(\tilde{\gamma_i}^{K_{i,j}}\tilde{\gamma_j}^{-K_{j,i}})$ since $K_{i,j}$ is even while $K_{j,i}$ is odd.

We can conclude that if for every power of two 2^h there is an $i \geq 0$ (or, equivalently, if the v-value group is 2-divisible), $\tilde{\gamma_i} \in \mathbb{R}$ is uniquely determined for all $i \geq 0$. If on the other hand, the value group is non-2-divisible, there is an $i \geq 0$ such that 2^{h_i} is maximal

for all $i \geq 0$. We then have two choices for $\tilde{\gamma_i}$ - a positive or a negative one. The sign of $\tilde{\gamma_j}$ is then uniquely determined for all $j \geq 0$ since

$$\alpha_{i,j} = \tilde{\gamma_i}^{K_{i,j}} \tilde{\gamma_j}^{-K_{j,i}},$$

where $K_{i,j}$ is even and $K_{j,i}$ is odd. We will now take an arbitrary valuation v on $\mathcal{A}_1(\mathbb{R})$ satisfying the conditions of Proposition 4.1, constructed by a sequence of $(\omega_i)_{i\geq -1}$ as shown in Section 3. We also pick $\tilde{\gamma_i} \in \mathbb{R}$ for all i. Then we will describe v's extension to $R[y;\delta]$ with a sequence of $(z_i)_{i\geq 0}$ like in the beginning of Section 4.

Suppose the valuation v on $\mathcal{A}_1(\mathbb{R})$ is given by a sequence $(\omega_i)_{i\geq -1}$ with $\omega_{-1} = x, \omega_0 = y$ and $\omega_i = x^{m_i}\omega_{i-1}^{n_i} - \beta_i$, $\beta_i \in \mathbb{R}$ and $\gcd(m_i, n_i) = 1$ for all i. Suppose also that v satisfies conditions (1) and (2) of Proposition 4.1. We will show that there is exactly one extension of v from $\mathcal{A}_1(\mathbb{R})$ to $R[y;\delta]$ for each appropriate choice of $(\tilde{\gamma_i})_{i\geq 1}$.

Lemma 4.2. *For each $k \geq \ell \geq 0$, ω_k can be written in the following form:*

$$\omega_k = (\Pi_{i=\ell+1}^{k} x^{\frac{m_i}{n_i}})\omega_\ell(\Pi_{i=\ell+1}^{k} B_i) - \sum_{i=\ell+1}^{k} (\Pi_{j=i+1}^{k} x^{\frac{m_j}{n_j}})\tilde{\gamma_i}(\Pi_{j=i}^{k} B_j)$$
$$+ \sum_{i=\ell+1}^{k} (\Pi_{j=i+1}^{k} x^{\frac{m_j}{n_j}})A_i(\Pi_{j=i+1}^{k} B_i),$$

with

$$A_i = \sum_{j=1}^{n_i-1} (x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-j-1} x^{\frac{m_i}{n_i}} [x^j{}^{\frac{m_i}{n_i}}, \omega_{i-1}]\omega_{i-1}^j$$
$$B_i = \sum_{j=1}^{n_j} (x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-j}\tilde{\gamma_i}^{j-1}$$

for each $1 \leq i \leq k$.

Proof. We prove the lemma by induction on $k \geq \ell$. For $k = \ell$, it is trivially true since we get $\omega_k = \omega_k$.

Suppose now the equation holds for some $k \geq \ell$. Then

$$\omega_{k+1} = x^{m_{k+1}}\omega_k^{n_{k+1}} - \beta_{k+1} = (x^{\frac{m_{k+1}}{n_{k+1}}}\omega_k - \tilde{\gamma}_{k+1})B_{k+1} + A_{k+1}$$
$$= x^{\frac{m_{k+1}}{n_{k+1}}}((\Pi_{i=\ell+1}^{k} x^{\frac{m_i}{n_i}})\omega_\ell(\Pi_{i=\ell+1}^{k} B_i) - \sum_{i=\ell+1}^{k} (\Pi_{j=i+1}^{k} x^{\frac{m_j}{n_j}})\tilde{\gamma_i}(\Pi_{j=i}^{k} B_j)$$
$$+ \sum_{i=\ell+1}^{k} (\Pi_{j=i+1}^{k} x^{\frac{m_j}{n_j}})A_i(\Pi_{j=i+1}^{k} B_i))B_{k+1} - \tilde{\gamma}_{k+1}B_{k+1} + A_{k+1}$$
$$= (\Pi_{i=\ell+1}^{k+1} x^{\frac{m_i}{n_i}})\omega_\ell(\Pi_{i=\ell+1}^{k+1} B_i) - \sum_{i=\ell+1}^{k+1} (\Pi_{j=i+1}^{k+1} x^{\frac{m_j}{n_j}})\tilde{\gamma_i}(\Pi_{j=i}^{k+1} B_j)$$
$$+ \sum_{i=\ell+1}^{k+1} (\Pi_{j=i+1}^{k+1} x^{\frac{m_j}{n_j}})A_i(\Pi_{j=i+1}^{k+1} B_i),$$

where we used the induction hypothesis, which is

$$\omega_k = (\Pi_{i=\ell+1}^{k} x^{\frac{m_i}{n_i}})\omega_\ell(\Pi_{i=\ell+1}^{k} B_i) - \sum_{i=\ell+1}^{k} (\Pi_{j=i+1}^{k} x^{\frac{m_j}{n_j}})\tilde{\gamma_i}(\Pi_{j=i}^{k} B_j)$$
$$+ \sum_{i=\ell+1}^{k} (\Pi_{j=i+1}^{k} x^{\frac{m_j}{n_j}})A_i(\Pi_{j=i+1}^{k} B_i)$$

in the second equation. □

Since $v(\omega_{i-1}) = \frac{m_i}{n_i}$ and $\overline{x^{\frac{m_i}{n_i}}\omega_{i-1}} = \tilde{\gamma_i}$, $v(B_i) = 0$ and $\overline{B_i} = n_i\tilde{\gamma_i}^{n_i-1}$ must hold for all $i \geq 1$. From

$$[x^{m_i}, \omega_{i-1}] = \sum_{j=0}^{n_i-1} x^{\frac{m_i}{n_i}\cdot j}[x^{\frac{m_i}{n_i}}, \omega_{i-1}]x^{\frac{m_i}{n_i}\cdot(n_i-j)},$$

we can see that $v(A_i) = v[x^{\frac{m_i}{n_i}}, \omega_{i-1}] = v[x, \omega_{i-1}] + 1 - \frac{m_i}{n_i} = -v(xy\omega_1 \dots \omega_{i-1})$. Since $\sum_{i\geq -1}^{k} v(\omega_i) < 0$ for every k by Lemma 3.2,

$$v(\sum_{i=\ell+1}^{k} (\Pi_{j=i+1} x^{\frac{m_j}{n_j}})A_i(\Pi_{j=i}^{k} B_i)) > v(\omega_k)$$

will hold for every k, which is why we can ignore the terms containing A_i during our evaluations of $v(z_i)$ where for each i, $z_i \in R[y;\delta]$ is as in the beginning of this section.

Lemma 4.3. *Suppose v is a valuation on $\mathcal{A}_1(\mathbb{R})$ constructed from a sequence $(\omega_i)_{i\geq -1}$ that extends to a valuation on $R[y;\delta]$ and thus D, its quotient division ring. For a given $i \geq 1$, define a sequence $(S_{i,j})_{j\geq 1}$ by:*

(a) $S_{i,1} := (x^{\frac{m_i}{n_i}}\omega_{i-1} - \tilde{\gamma_i})^{-1}(B_i - \overline{B_i})$,

(b) $S_{i,j+1} := (x^{\frac{m_i}{n_i}}\omega_{i-1} - \tilde{\gamma_i})^{-1}(S_{i,j} - \overline{S_{i,j}})$ *for* $j \geq 1$.

Then for each $j \geq 1$:

1 $S_{i,j} = \sum_{k=1}^{n_i-j} N_{k,j}(x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-j-k}\tilde{\gamma_i}^{k-1}$ *with* $N_{k,1} = k$ *and* $N_{k,j+1} = \sum_{\ell=k}^{n_i-j} N_{\ell,j}$, *and*

2 $v(S_{i,j}) = 0$, $\overline{S_{i,j}} = N_{1,j+1}\tilde{\gamma_i}^{n_i-j-1}$

for all $1 \leq j \leq n_i - 1$.

Proof. We prove the first statement of the lemma by induction on $j \geq 1$. To show the basis of induction, we evaluate

$$B_i - \overline{B_i} = (x^{\frac{m_i}{n_i}}\omega_{i-1} - \tilde{\gamma_i})(\sum_{k=1}^{n_i}((x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-k-1} +$$
$$(x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-k-2}\tilde{\gamma_i} + \dots + \tilde{\gamma_i}^{n_i-k-1})\tilde{\gamma_i}^{k-1})$$
$$= (x^{\frac{m_i}{n_i}}\omega_{i-1} - \tilde{\gamma_i}) \sum_{k=1}^{n_i-1} k(x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-k-1}\tilde{\gamma_i}^{k-1}.$$

We can thus see $S_{i,1} = \sum_{k=1}^{n_i-1} k(x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-k-1}\tilde{\gamma_i}^{k-1}$ and since $\overline{x^{\frac{m_i}{n_i}}\omega_{i-1}} = \tilde{\gamma_i}$, we see that the lemma holds in case $j = 1$. Now we suppose that the statement is true for some $j \geq 1$, i.e., $S_{i,j} = \sum_{k=1}^{n_i-j} N_{k,j}(x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-j-k}\tilde{\gamma_i}^{k-1}$ and $v(S_{i,j}) = 0$, $\overline{S_{i,j}} = N_{1,j+1}\tilde{\gamma_i}^{n_i-j-1}$. We then write

$$\begin{aligned}
S_{i,j} - \overline{S_{i,j}} &= \sum_{k=1}^{n_i-j} N_{k,j}(x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-j-k}\tilde{\gamma_i}^{k-1} - N_{1,j+1}\tilde{\gamma_i}^{n_i-j-1} \\
&= \sum_{k=1}^{n_i-j} N_{k,j}(x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-j-k}\tilde{\gamma_i}^{k-1} - \sum_{k=1}^{n_i-j} N_{k,j}\tilde{\gamma_i}^{n_i-j-1} \\
&= \sum_{k=1}^{n_i-j-1} N_{k,j}((x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-j-k} - \tilde{\gamma_i}^{n_i-j-1})\tilde{\gamma_i}^{k-1} \\
&= (x^{\frac{m_i}{n_i}}\omega_{i-1} - \tilde{\gamma_i}) \sum_{k=1}^{n_i-j-1} N_{k,j}((x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-j-1-k} + \cdots + \tilde{\gamma_i}^{n_i-j-1-k})\tilde{\gamma_i}^{k-1} \\
&= (x^{\frac{m_i}{n_i}}\omega_{i-1} - \tilde{\gamma_i}) \sum_{k=1}^{n_i-j-1} (N_{k,j} + N_{k+1,j} + \cdots + N_{n_i-j-1,j}) \\
&\qquad\qquad (x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-j-k}\tilde{\gamma_i}^{k-1} \\
&= (x^{\frac{m_i}{n_i}}\omega_{i-1} - \tilde{\gamma_i}) \sum_{k=1}^{n_i-j-1} N_{k,j+1}(x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-j-k}\tilde{\gamma_i}^{k-1}
\end{aligned}$$

proving the first statement of the lemma. The second statement immediately follows from the first since $\overline{x^{\frac{m_i}{n_i}}\omega_{i-1}} = \tilde{\gamma_i}$ and thus

$$\begin{aligned}
v(S_{i,j}) &= v(\sum_{k=1}^{n_i-j} N_{k,j}(x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-j-k}\tilde{\gamma_i}^{k-1}) = 0, \\
\overline{S_{i,j}} &= \overline{\sum_{k=1}^{n_i-j} N_{k,j}(x^{\frac{m_i}{n_i}}\omega_{i-1})^{n_i-j-k}\tilde{\gamma_i}^{k-1}} = N_{1,j+1}\tilde{\gamma_i}^{n_i-j-1}.
\end{aligned}$$

□

Lemma 4.4. *Supose v is as in* Lemma 4.3. *For a given $i \geq 1$, define a sequence $(D_{i,j})_{j\geq 1}$ by:*

(a) $D_{i,1} = B_1B_2\cdots B_i - \overline{B_1B_2\cdots B_i}$,

(b) $D_{i,j+1} = x^{v(D_{i,j})}D_{i,j} - \overline{x^{v(D_{i,j})}D_{i,j}}$.

Then for each $j \geq 1$:

1. *$D_{i,j}$ is a $\mathbb{R}$-linear sum of terms which are products of elements from the set*

$$\{\omega_i\}_i \cup \{B_i\}_i \cup \{B_i^{-1}\}_i \cup \{S_{i,j}\}_{i,j}, \tag{4.2}$$

where parts of the product are conjugated by a rational power of x.

2. $v(D_{i,j})$ *is a sum of* $v(\omega_\ell)$ *for finitely many* ω_ℓ.

3. $\overline{x^{v(D_{i,j})}D_{i,j}}$ *is sum of products of* $\tilde{\gamma_k}$ *for various* k.

Proof. Since

$$\begin{aligned} B_1B_2\cdots B_i - \overline{B_1B_2\cdots B_i} &= \sum_{j=1}^{i} B_1\cdots B_{j-1}(B_j - \overline{B_j})\overline{B_{j+1}\cdots B_i} \\ &= \sum_{j=1}^{i} B_1\cdots B_{j-1}\omega_j B_j^{-1} S_{j,1}\overline{B_{i+1}\cdots B_i}, \end{aligned}$$

and

$$\begin{aligned} & x^{\frac{m_{j+1}}{n_{j+1}}} B_1\cdots B_{j-1}\omega_j B_j^{-1} S_{j,1}\overline{B_{i+1}\cdots B_i} \\ &= (x^{\frac{m_{j+1}}{n_{j+1}}} B_1\cdots B_{j-1} x^{-\frac{m_{j+1}}{n_{j+1}}}) x^{\frac{m_{j+1}}{n_{j+1}}} \omega_j B_j^{-1} S_{j,1}\overline{B_{i+1}\cdots B_i}, \end{aligned}$$

for each $1 \leq j \leq k$, the first two statements of the lemma follow from:

1. $x^{\frac{m_i}{n_i}}\omega_{i-1} - \tilde{\gamma_i} = \omega_i B_i^{-1}$,

2. $B_i - \overline{B_i} = (x^{\frac{m_i}{n_i}}\omega_{i-1} - \tilde{\gamma})S_{i,1} = \omega_i B_i^{-1} S_{i,1}$,

3. $S_{i,j} - \overline{S_{i,j}} = (x^{\frac{m_i}{n_i}}\omega_{i-1} - \tilde{\gamma} S_{i,j+1} = \omega_i B_i^{-1} S_{i,j+1}$,

4. $B_i^{-1} - \overline{B_i}^{-1} = -{B_i}^{-1}(B_i - \overline{B_i})\overline{B_i}^{-1} = -{B_i}^{-1}\omega_i B_i^{-1} S_{i,1}\overline{B_i}^{-1}$,

where we ignore the terms we get when we change the order of multiplication. We can do that that since these terms are procucts of A_i as defined in Lemma 4.2 and terms with zero v-value. As we have already mentioned, these terms will not influence the construction of the extension of a valuation on $\mathcal{A}_1(\mathbb{R})$ to $R[y;\delta]$. Indeed - we can see by induction on $j \geq 1$ that each term of the sum is a product of factors equal to, modulo conjugation by a rational power of x, one of the elements of the set (4.2); that is,

1. either equal to ω_i, or

2. equal to a power of B_j or $S_{j,i}$ for some i, j.

Since the latter have v-value equal to zero and since both $B_i - \overline{B_i}$ and $S_{i,j} - \overline{S_{i,j}}$ are products of ω_i, a power of B_i^{-1} and $S_{i,j}$ for some i, j, $v(D_{i,j})$ is a sum of $v(\omega_i)$ for some i. The last statement of the lemma follows from the fact that for all i, j, $\overline{B_i}$ and $\overline{S_{i,j}}$ are of the form $N\tilde{\gamma_i}$ for $N \in \mathbb{N}$. □

If v is a valuation on $R[y;\delta]$ with residue field $\mathbb{R}$, then, as we have presented in Section 4, v can be constructed from a sequence $(z_i)_{i\geq 0} \subset R[y;\delta]$. In the next proposition, we make the first comparison between this construction and the construction of a valuation on $\mathcal{A}_1(\mathbb{R})$ from a sequence $(\omega_i)_{i\geq -1}$ described in Section 3.

Lemma 4.5. *Suppose v is as in* Lemma 4.3. *Suppose that for some $k, \ell \geq 0$, we can write*

$$\omega_k = (\Pi_{i=1}^k x^{\frac{m_i}{n_i}}) z_\ell (\Pi_{i=1}^k B_i) + C,$$

where C is a $\mathbb{R}$-linear sum of elements of the form $D_{i,j}$ for some $i, j \geq 0$. Then:

1. *If $v(\omega_k) > v(\Pi_{i=1}^k x^{\frac{m_i}{n_i}} z_\ell) \in \mathbb{Q}$, then*

$$\omega_k = (\Pi_{i=1}^k x^{\frac{m_i}{n_i}}) z_{\ell+1} (\Pi_{i=1}^k B_i) + C_1.$$

2. *If $v(\omega_k) = v(\Pi_{i=1}^k x^{\frac{m_i}{n_i}} z_\ell) \in \mathbb{Q}$, then*

$$\omega_{k+1} = (\Pi_{i=1}^{k+1} x^{\frac{m_i}{n_i}}) z_{\ell+1} (\Pi_{i=1}^{k+1} B_i) + C_2.$$

3. *If $v(\omega_k) < v(\Pi_{i=1}^k x^{\frac{m_i}{n_i}} z_\ell)$, then, if $v(\omega_k) \in \mathbb{Q}$,*

$$\omega_{k+1} = (\Pi_{i=1}^{k+1} x^{\frac{m_i}{n_i}}) z_\ell (\Pi_{i=1}^{k+1} B_i) + C_3.$$

Here, C_1, C_2 and C_3 are other $\mathbb{R}$-linear sums of elements of the form $D_{i,j}$ as in Lemma 4.5 *for some $i, j \geq 0$.*

Proof. Suppose first $v(\omega_k) > v(\Pi_{i=1}^k x^{\frac{m_i}{n_i}} z_\ell) = v(C)$. Since $v(C) = r_{\ell+1} - \sum_{i=1}^k \frac{m_i}{n_i} \in \mathbb{Q}$, then $r_{\ell+1} := v(z_\ell) \in \mathbb{Q}$ as well. So, for $z_{\ell+1} = z_\ell - x^{-r_{\ell+1}} \gamma_{\ell+1}$, we can write

$$\begin{aligned}\omega_k &= (\Pi_{i=1}^k x^{\frac{m_i}{n_i}}) z_{\ell+1} (\Pi_{i=1}^k B_i) + \gamma_{\ell+1} (\Pi_{i=1}^k x^{\frac{m_i}{n_i}}) x^{-r_{\ell+1}} (\Pi_{i=1}^k B_i) + C \\ &= (\Pi_{i=1}^k x^{\frac{m_i}{n_i}}) z_{\ell+1} (\Pi_{i=1}^k B_i) + x^{-v(C)} (\gamma_{\ell+1} (\Pi_{i=1}^k B_i) + x^{v(C)} C)\end{aligned}$$

Since $v(z_{\ell+1}) > v(z_\ell)$, we see that $v(\gamma_{\ell+1} \Pi_{i=1}^k B_i + x^{v(C)} C) > 0$. It follows that $\gamma_{i+1} = -\Pi_{i=1}^k \overline{B_i}^{-1} \overline{x^{-v(C)} C}$, hence

$$\begin{aligned}C_1 := \gamma_{\ell+1} \Pi_{i=1}^k B_i + x^{-v(C)} C &= \gamma_{\ell+1} \Pi_{i=1}^k B_i + \overline{x^{-v(C)} C} - \overline{x^{-v(C)} C} + x^{-v(C)} C \\ &= \gamma_{\ell+1} (\Pi_{i=1}^k B_i - \Pi_{i=1}^k \overline{B_i}) + (x^{-v(C)} C - \overline{x^{-v(C)} C})\end{aligned}$$

We see that since C is an $\mathbb{R}$-linear sum of $D_{i,j}$ for various i, j, so is, by Lemma 4.4, $x^{-v(C)} C - \overline{x^{-v(C)} C}$. Hence, C_1 is an $\mathbb{R}$-linear sum of $D_{i,j}$.

Now consider the case $v(\omega_k) = v(\Pi_{i=1}^k x^{\frac{m_i}{n_i}} z_\ell) \leq v(C)$. Since $v(\omega_k) = \frac{m_{k+1}}{n_{k+1}} \in \mathbb{Q}$, we can evaluate

$$\begin{aligned}\tilde{\gamma_{k+1}} = \overline{x^{\frac{m_{k+1}}{n_{k+1}}} \omega_k} &= \overline{(\Pi_{i=1}^{k+1} x^{\frac{m_i}{n_i}}) z_\ell (\Pi_{i=1}^k B_i)} + \overline{x^{\frac{m_{k+1}}{n_{k+1}}} C} \\ &= \gamma_{\ell+1} \Pi_{i=1}^k \overline{B_i} + \overline{x^{\frac{m_{k+1}}{n_{k+1}}} C},\end{aligned}$$

and then deduce

$$\begin{aligned}
\omega_{k+1} &= (x^{\frac{m_{k+1}}{n_{k+1}}}\omega_k - \tilde{\gamma_{k+1}})B_{k+1} \\
&= (\Pi_{i=1}^{k+1}x^{\frac{m_i}{n_i}})z_\ell(\Pi_{i=1}^{k+1}B_i) + x^{\frac{m_{k+1}}{n_{k+1}}}CB_{k+1} - \tilde{\gamma_{k+1}}B_{k+1} \\
&= (\Pi_{i=1}^{k+1}x^{\frac{m_i}{n_i}})z_{\ell+1}(\Pi_{i=1}^{k+1}B_i) + \gamma_{\ell+1}(\Pi_{i=1}^{k+1}B_i) + x^{\frac{m_{k+1}}{n_{k+1}}}CB_{k+1} - \tilde{\gamma_{k+1}}B_{k+1} \\
&= (\Pi_{i=1}^{k+1}x^{\frac{m_i}{n_i}})z_{\ell+1}(\Pi_{i=1}^{k+1}B_i) + \gamma_{\ell+1}(\Pi_{i=1}^{k}B_i - \Pi_{i=1}^{k}\overline{B_i})B_{k+1} + \\
&\qquad\qquad (x^{\frac{m_{k+1}}{n_{k+1}}}C - \overline{x^{\frac{m_{k+1}}{n_{k+1}}}C})B_{k+1} \\
&= (\Pi_{i=1}^{k+1}x^{\frac{m_i}{n_i}})z_{\ell+1}(\Pi_{i=1}^{k+1}B_i) + C_2
\end{aligned}$$

where C_2 is, again, an $\mathbb{R}$-linear sum of $D_{i,j}$ for some i, j.

Lastly, we consider the case $v(\Pi_{i=1}^{k}x^{\frac{m_i}{n_i}}z_\ell) > v(\omega_k) = v(C) \in \mathbb{Q}$. In this case, $\tilde{\gamma_{k+1}} = \overline{x^{\frac{m_{k+1}}{n_{k+1}}}\omega_k} = \overline{x^{\frac{m_{k+1}}{n_{k+1}}}C}$, so we can write

$$\begin{aligned}
\omega_{k+1} &= (x^{\frac{m_{k+1}}{n_{k+1}}}\omega_k - \tilde{\gamma_{k+1}})B_{k+1} \\
&= (\Pi_{i=1}^{k+1}x^{\frac{m_i}{n_i}})z_\ell(\Pi_{i=1}^{k+1}B_i) + (x^{\frac{m_{k+1}}{n_{k+1}}}C - \overline{x^{\frac{m_{k+1}}{n_{k+1}}}C})B_{k+1}
\end{aligned}$$

and the statement again follows. □

Theorem 4.6. *Suppose v is a valuation on $\mathcal{A}_1(\mathbb{R})$, constructed from an either finite or infinite sequence $(\omega_i)_{i\geq -1}$ with $v(\omega_i) = \frac{m_{i+1}}{n_{i+1}}$. Suppose also that v satisfies the following conditions:*

1. *For each i such that n_i is even, $\beta_i > 0$ must hold, and*
2. *for each $i, j, \ell \geq 0$ with $h_i < h_j \leq h_\ell$, $\alpha_{i,j}\alpha_{i,\ell} > 0$ must hold.*

Then v has a unique extension to a valuation on $R[y;\delta]$ with residue field $\mathbb{R}$ for each choice of $(\tilde{\gamma_i})_{i\geq 1}$.

Proof. As we know from the beginning of Section 4, each valuation on $R[y;\delta]$ and D with residue field $\mathbb{R}$ can be constructed by either a finite or an infinite sequence $(z_i)_{i\geq 0}$. For every sequence $(\omega_i)_{i\geq -1}$, we will use the lemmas proved in this section to find the unique sequence $(z_i)_{i\geq 0}$ which, as we have shown in the beginning of this section, uniquely determines a valuation on $R[y;\delta]$. Our calculations will then show that the valuation on D defined by the sequence $(z_i)_{i\geq 0}$ is the extension of the valuation on $\mathcal{A}_1(\mathbb{R})$ associated to the sequence $(\omega_i)_{i\geq -1}$.

We determine the finite or infinite sequence $(z_i)_{i\geq 0}$ associated to v's extension to $R[y;\delta]$. In the first step, we consider $v(y)$. If $v(y) \notin \mathbb{Q}$, then v's extension to $R[y;\delta]$ is clearly uniquely determined, namely the one defined by

$$v(\sum_{i=0}^{n} p_i(x)y^i) = \min_{0\leq i\leq n}\{v(p_i(x)) + iv(y)\}$$

for every $\sum_{i=0}^{n} p_i(x)y^i \in R[y;\delta]$.

So suppose $v(y) = \frac{m_1}{n_1} \in \mathbb{Q}$. Then, in the second step of our evaluation, we write

$$\omega_1 = x^{m_1}y^{n_1} - \beta_1 = (x^{\frac{m_1}{n_1}}y - \tilde{\gamma_1})B_1 = x^{\frac{m_1}{n_1}}(y - x^{-\frac{m_1}{n_1}}\tilde{\gamma_1})B_1$$

and since $v(\omega_1) > 0$, $v(y - x^{-\frac{m_1}{n_1}}\tilde{\gamma_1}) > \frac{m_1}{n_1} = v(y)$. We deduce $z_1 = y - x^{-\frac{m_1}{n_1}}\gamma_1$ with $\gamma_1 = \tilde{\gamma_1}$. Obviously, $v(z_1) = v(\omega_1) + \frac{m_1}{n_1} \in \mathbb{Q}$ if and only if $v(\omega_1) \in \mathbb{Q}$. If either and hence both values are irrational, we get a unique extension of v to $R[y;\delta]$. Otherwise, if $v(\omega_1) = \frac{m_2}{n_2} \in \mathbb{Q}$ and hence $r_2 = v(z_2) = \frac{m_1}{n_1} + \frac{m_2}{n_2}$, we continue with the third step of our evaluation by writing

$$\omega_2 = (x^{\frac{m_2}{n_2}}\omega_1 - \tilde{\gamma_2})B_2 = (x^{\frac{m_2}{n_2}}x^{\frac{m_1}{n_1}}z_1B_1 - \tilde{\gamma_2})B_2.$$

Since $v(\omega_2) > 0$, we conclude that $\gamma_2 = \overline{x^{\frac{m_2}{n_2}}x^{\frac{m_1}{n_1}}z_1}$ must be equal to $\tilde{\gamma_2}\overline{B_1}^{-1}$. To evaluate the v-value of $z_2 = z_1 - \gamma_2 x^{-r_2}$, we write

$$\omega_2 = (x^{\frac{m_2}{n_2}}x^{\frac{m_1}{n_1}}z_2B_1 + \gamma_2B_1 - \tilde{\gamma_2})B_2 = x^{\frac{m_2}{n_2}}x^{\frac{m_1}{n_1}}z_2B_1B_2 + (\gamma_2B_1 - \tilde{\gamma_2})B_2.$$

We note that ω_2 is here written as a sum of $\Pi_{i=1}^2 x^{\frac{m_i}{n_i}}z_2\Pi_{i=1}^2 B_i + C$ where C is as in Lemma 4.5. To determine $v(z_2)$, we compare $v(\omega_2)$ and $v(\gamma_2B_1 - \tilde{\gamma_2})$, the latter being equal to $v(\omega_1)$ since $\gamma_2B_1 - \tilde{\gamma_2} = \gamma_2(B_1 - \overline{B_1})$. There are three possible cases:

1. If $v(\omega_2) < v(\omega_1)$, then $v(x^{\frac{m_2}{n_2}}x^{\frac{m_1}{n_1}}z_2)$ must be equal to $v(\omega_2)$, so $r_3 = v(z_2)$ is determined by $v(z_2) = v(\omega_2) - \frac{m_1}{n_1} - \frac{m_2}{n_2}$. If $v(\omega_2) = \frac{m_3}{n_3} \in \mathbb{Q}$, then $v(z_2) = r_3 \in \mathbb{Q}$ and $\gamma_3 = \tilde{\gamma_3}(\overline{B_1B_2})^{-1}$ must hold. It follows that $v(z_2) \in \mathbb{Q}$ if and only if $v(\omega_2) \in \mathbb{Q}$. In this case, the v-value of $z_3 = z_2 - \gamma_3 x^{-r_3}$ will be determined in the subsequent steps, i.e., by considering $(v(\omega_i))_{i\geq 3}$ and $(\tilde{\gamma_i})_{i\geq 3}$. By Lemma 4.5, $\omega_3 = \Pi_{i=1}^3 x^{\frac{m_i}{n_i}}z_3\Pi_{i=1}^3 B_i + C_1$, C_1 being an $\mathbb{R}$-linear sum of $D_{i,j}$.

2. If $v(\omega_2) = v(\omega_1)$, then $v(z_2)$ depends on $\tilde{\gamma_3}$:

   (a) If $\tilde{\gamma_3} = \overline{x^{\frac{m_2}{n_2}}(\gamma_2B_1 - \tilde{\gamma_2})B_2}$, then $v(x^{\frac{m_2}{n_2}}x^{\frac{m_1}{n_1}}z_2)$ must be greater than $v(\omega_1)$ since in this case, $\omega_2 \sim (\gamma_2B_1 - \tilde{\gamma_2})B_2$ and will be determined in the subsequent steps, i.e., by considering $(v(\omega_i))_{i\geq 3}$ and $(\tilde{\gamma_i})_{i\geq 3}$. By Lemma 4.5, $\omega_3 = \Pi_{i=1}^3 x^{\frac{m_i}{n_i}}z_2\Pi_{i=1}^3 B_i + C_2$, C_2 being an $\mathbb{R}$-linear sum of $D_{i,j}$.

   (b) Otherwise, $v(x^{\frac{m_2}{n_2}}x^{\frac{m_1}{n_1}}z_2) = v(\omega_2)$. In this case, we get

   $$\gamma_3 = \tilde{\gamma_3} - \overline{x^{\frac{m_2}{n_2}}(\gamma_2B_1 - \tilde{\gamma_2})B_2}.$$

   By Lemma 4.5, $\omega_3 = \Pi_{i=1}^3 x^{\frac{m_i}{n_i}}z_3\Pi_{i=1}^3 B_i + C_3$, with C_3 an $\mathbb{R}$-linear sum of $D_{i,j}$.

3. If $v(\omega_2) > v(\omega_1)$, then $v(x^{\frac{m_2}{n_2}}x^{\frac{m_1}{n_1}}z_2) = v(\omega_1)$ and $\gamma_3 = \overline{-x^{\frac{m_2}{n_2}}(\gamma_2B_1 - \tilde{\gamma_2})B_1^{-1}}$. By Lemma 4.5, $\omega_2 = \Pi_{i=1}^2 x^{\frac{m_i}{n_i}}z_3\Pi_{i=1}^2 B_i + C_4$, with C_4 an $\mathbb{R}$-linear sum of $D_{i,j}$.

The general step of the evaluation is similar to the first three. Suppose that in the previous steps, we have evaluated $v(z_1) = r_2, \ldots, v(z_{\ell-1}) = r_\ell \in \mathbb{Q}$. In the last step, we have, by considering $(\omega_i)_{i=-1}^{k}$ for some k, begun to evaluate $v(z_\ell)$ and we are, with

$$\omega_k = (\Pi_{i=1}^{k} x^{\frac{m_i}{n_i}}) z_{\ell+1} (\Pi_{i=1}^{k} B_i) + C,$$

where C is as in Lemma 4.5, in one of the five situations:

1. If $v(\omega_k) < v(C)$, then $v(z_\ell) = v(\omega_k) - \sum_{i=1}^{k} \frac{m_i}{n_i}$ and $\gamma_{\ell+1} = \tilde{\gamma_{\ell+1}} \Pi_{i=1}^{k} \overline{B_i}^{-1}$. In case $r_{\ell+1} = v(z_\ell) \in \mathbb{Q}$, our next step is to evaluate the v-value of $z_{\ell+1} = z_\ell - r^{\ell+1}\gamma_{\ell+1}$ by writing

$$\omega_{k+1} = (\Pi_{i=1}^{k+1} x^{\frac{m_i}{n_i}}) z_\ell (\Pi_{i=1}^{k+1} B_i) + C_1.$$

2. If $v(\omega_k) > v(C)$, then $v(z_\ell) = v(C)$ and $\gamma_{\ell+1} = \overline{C} \Pi_{i=1}^{k} \overline{B_i}^{-1}$. In case $r_{\ell+1} = v(z_\ell) \in \mathbb{Q}$, our next step is to evaluate the v-value of $z_{\ell+1} = z_\ell - r^{\ell+1}\gamma_{\ell+1}$ by writing

$$\omega_k = (\Pi_{i=1}^{k} x^{\frac{m_i}{n_i}}) z_{\ell+1} (\Pi_{i=1}^{k} B_i) + C_2.$$

3. If $v(\omega_k) = v(C) \notin \mathbb{Q}$, then $v(z_\ell) = v(\omega_k - C) - \sum_{i=1}^{k} \frac{m_i}{n_i} \notin \mathbb{Q}$ since in case $v(\omega_k - C) > v(\omega_k)$, $C \sim \omega_k$ must hold, but since, given that $C \neq \omega_k$ and that C is a sum of $D_{i,j}$, $v(\omega_k - C)$ must be in $\mathbb{Q}$. This terminates our evaluation of the sequence $(z_i)_{i \geq 0}$ associated to v's extension to $R[y;\delta]$.

4. If $v(\omega_k) = v(C) = \frac{m_{k+1}}{n_{k+1}} \in \mathbb{Q}$ and $\overline{x^{\frac{m_{k+1}}{n_{k+1}}} \omega_k} = \overline{x^{\frac{m_{k+1}}{n_{k+1}}} C}$, $v((\Pi_{i=1}^{k} x^{\frac{m_i}{n_i}}) z_\ell) > v(\omega_k)$. We continue with our evaluation by writing

$$\omega_{k+1} = (\Pi_{i=1}^{k+1} x^{\frac{m_i}{n_i}}) z_\ell (\Pi_{i=1}^{k+1} B_i) + C_3.$$

5. If $v(\omega_k) = v(C) = \frac{m_{k+1}}{n_{k+1}} \in \mathbb{Q}$ and $\overline{x^{\frac{m_{k+1}}{n_{k+1}}} \omega_k} \neq \overline{x^{\frac{m_{k+1}}{n_{k+1}}} C}$, then $v((\Pi_{i=1}^{k} x^{\frac{m_i}{n_i}}) z_\ell) = v(\omega_k)$ and $\gamma_{\ell+1} = (\overline{x^{\frac{m_{k+1}}{n_{k+1}}} \omega_k} - \overline{x^{\frac{m_{k+1}}{n_{k+1}}} C}) \Pi_{i=1}^{k} \overline{B_i}^{-1}$. We write

$$\omega_{k+1} = (\Pi_{i=1}^{k+1} x^{\frac{m_i}{n_i}}) z_{\ell+1} (\Pi_{i=1}^{k+1} B_i) + C_4.$$

For each $1 \leq i \leq 4$, C_i is, as is C, an $\mathbb{R}$-linear sum of $D_{i,j}$ for various i, j. This is assured by Lemma 4.5.

We point out that for each ℓ, $v(z_\ell)$ is determined in a finite number of steps. In case v is determined by a finite sequence $(\omega_i)_{i \geq -1}^{N}$ for some $N \geq 0$, this is immediate. In the infinite case, it follows from Lemma 3.2 that $\lim_{k \to \infty} v(\omega_k) = 0$, so, given that by Lemma 4.4, $v(C)$ is a sum of $v(\omega_i)$, $v(\omega_k) < v(C)$ must hold for some k. And since, in the step where $v(z_\ell)$ is determined, we get $v(\Pi_{i=1}^{k} x^{\frac{m_i}{n_i}} z_\ell) = v(z_\ell) - \sum_{i=1}^{k} v(\omega_{i-1}) \leq v(\omega_k)$ for each $\ell \geq 0$, we get $v(z_\ell) \leq \sum_{i=0}^{k} v(\omega_i) < 1$ by Lemma 3.2. Since for each $\ell \geq 0$, $z_{\ell+1} = z_\ell - x^{-r_{\ell+1}}\gamma_{\ell+1}$, we did indeed find a unique sequence $(z_i)_{i \geq 0}$ that uniquely determines a valuation v on $R[y;\delta]$. This valuation is v's extension from $\mathcal{A}_1(\mathbb{R})$ to $R[y;\delta]$. □

The construction introduced in the proof of Theorem 4.6 can be reversed. Given a valuation v on $R[y;\delta]$, we could use the reverse construction to find the sequence $(\omega_i)_{i \geq -1} \subseteq \mathcal{A}_1(\mathbb{R})$ associated to v's restriction to $\mathcal{A}_1(\mathbb{R})$.

5 Valuations on $\tilde{R}[y;\delta]$

The ring $\tilde{R}[y;\delta]$ is an extension of $R[y,\delta]$ where $\tilde{R}$ is defined as $\mathbb{R}((x^{\mathbb{Q}}))$, the generalized power ring of sums $\sum_{q\in\mathbb{Q}} \alpha_q x^{-q}$ with well-ordered support. We first show that every valuation on $R[y;\delta]$ can be easily extended to $\tilde{R}[y;\delta]$.

Lemma 5.1. *Every valuation on $R[y;\delta]$ with residue field $\mathbb{R}$ can be extended to a valuation on $\tilde{R}[y;\delta]$ with the same residue field.*

Proof. Suppose first v is defined on $R[y;\delta]$ by a finite sequence $(z_i)_{i=0}^k$ with $v(z_k) \notin \mathbb{Q}$. Then, as we can write every $f \in \tilde{R}[y;\delta]$ as $\sum_{i=0}^n p_i(x) z_k^i$ with $p_i(x) \in \tilde{R}$, we define $v(f) = \min_{1\le i\le n}\{v(p_i(x)) + iv(z_k)\}$. This gives us a well-defined valuation on $\tilde{R}[y;\delta]$ which clearly extends the one we defined on $R[y;\delta]$ in the previous section.

Now suppose v is defined by an infinite sequence $(z_i)_{i\ge 0}$ with $r = \lim_{i\to\infty} v(z_i) \le 1$. Define $z := y - \sum_{i=1}^{\infty} \alpha_i x^{-r_i} \in \tilde{R}[y;\delta]$. In the same way as before, write every $f \in \tilde{R}[y;\delta]$ as $\sum_{i=0}^n p_i(x) z^i$ with $p_i(x) \in \tilde{R}$ and define $v(f) = \min_{1\le i\le n}\{v(p_i(x))y + i(r-\mu)\}$ where μ is a positive infinitesimal. Thus we once more get v's extension to $\tilde{R}[y;\delta]$. □

In case $r = 1$, this is the only possible extension up to isomorphism of the value group, for $v(z)$ must be $1 - \mu$. This is because on the one hand, since $v(z) > v(z_k) = r_{k+1}$ for all $k \ge 0$, $v(z)$ is greater than any rational number $q < 1$. On the other hand, since $v[y - z, x] = v[y, x] = 0$ and the value group is commutative, $v(z) \le 1$. Thus if $v(z) \in \mathbb{R}$, $v(z) = 1$. But if we restricted v to the quotient ring of the $\mathbb{R}$-algebra, generated by x and z, we would get a valuation on a division ring, isomorphic to $\mathcal{D}_1(\mathbb{R})$, with a rational value group, residue field $\mathbb{R}$ and $v[z, x] = v(zx)$, which contradicts Corollary 2.4.

Proposition 5.2. *Let v be a valuation on $\tilde{R}[y;\delta]$ with residue field $\mathbb{R}$. Then the value group is not of rational rank one.*

Proof. The only case in the proof of Lemma 5.1 where it does not immediately follow that the value group is not $\mathbb{Q}$ is when v's restriction to $R[y;\delta]$ is constructed by an infinite sequence $(z_i)_{i\ge 0}$ with $r := \lim_{i\to\infty} v(y - z_i) < 1$. In this case, we can set $v(z) = r \in \mathbb{R}$ and if $r \in \mathbb{Q}$, define $y^{(1)} := z$ and restart the construction of v. We may get another infinite sequence $(z_i^{(1)})_{i\ge 0}$ with $r^{(1)} := \lim_{i\to\infty} v(z_i^{(1)}) < 1$. If $r^{(1)} \in \mathbb{Q}$, we start over with $y^{(2)} := z^{(1)}$. Though we may have to repeat the process infinitely many times, the set $\{z_k^{(j)}\}_{j\ge 1, k\ge 0}$ is countable and $A := \{v(z_k^{(j)})\}_{j\ge 1,k\ge 0}$ is a well-ordered set of rational numbers smaller than one. At one point, $v(z)$ will have to be irrational for some $z = \sum_{q\in A} \alpha_q x^{-q}$ since we would otherwise get $z \in \tilde{R}$ such that $v(z) = 1$ which, as we have shown, contradicts the fact that the value group is rational. □

Recall that a pseudo-Cauchy sequence in a division ring D with a valuation v is a sequence $(a_\lambda)_{\lambda\in\Lambda} \subseteq D$, where Λ is an ordinal such that there exists $\lambda \in \Lambda$ for which $v(a_\sigma - a_\rho) < v(a_\rho - a_\tau)$ for all $\sigma, \rho, \tau \in \Lambda$ with $\lambda \le \sigma < \rho < \tau$. Let D' be an extension of D and v' and extension of v to D'. Then $a \in D'$ is a limit of the pseudo-Cauchy sequence $(a_\lambda)_{\lambda\in\Lambda}$ if $v'(a - a_\sigma) = v'(a_{\sigma+1} - a_\sigma)$ for all $\sigma \in \Lambda$, $\lambda \le \sigma$. Recall also the definition of a immediate extension of a valuation.

Definition 5.3. Let v be a valuation on a division ring D, the division ring D' an extension of D and v' a valuation on D' that extends v. Let Γ and $\overline{D}$ and Γ' and $\overline{D'}$ be the value groups and residue division rnigs associated to v and v'. Then we say v' is an *immediate* extension of v if $[\Gamma' : \Gamma] = 1$ and $[\overline{D'} : \overline{D}]$.

As a byproduct of our investigations, we show that not every extension of a valued division ring by limits of pseudo-Cauchy sequences is immediate. This differs from the commutative case since, as Kaplansky proved in [8], every extension of a valued field by limits of pseudo-Cauchy sequences is immediate.

Corollary 5.4. *There exist division rings $D \subseteq D'$ and a valuation v on D which extends to a valuation v' on D' such that D' is an extension of D by limits of pseudo-Cauchy sequences in D whereas v' is not an immediate extension of v.*

Proof. Let v be a valuation on $R[y;\delta]$ with residue field $\mathbb{R}$ and value group $\mathbb{Q}$ as described in Section 4. Then $v(x) = -1$ and $\tilde{R}[y;\delta]$ is an extension of $R[y;\delta]$ by limits of pseudo-Cauchy sequences. This holds because every $\sum_{i\in\mathbb{Q}} a_i x^{-i} \in \tilde{R}$ is a limit of the pseudo-Cauchy sequence $(\sum_{i=1}^{k} a_i x^{-q_i})_{k\geq 1}$ in $R[y;\delta]$.

As we have shown in this section, v can be uniquely extended to $\tilde{R}[y;\delta]$. By Proposition 5.2, this extension is not immediate. Let D be the quotient division ring of $R[y,\delta]$, to which v uniquely extends, and D' the quotient division ring of $\tilde{R}[y;\delta]$, to which v' uniquely extends, since both rings are Ore domains. D' is not an immediate extension of the ring D with valuation v, even though D' is an extension of D by limits of pseudo-Cauchy sequences. □

6 Compatibility with orderings on $\mathcal{A}_1(\mathbb{R})$ and $R[y;\delta]$

In Section 3, we mentioned that every strongly abelian valuation on a division ring with an ordered residue field is compatible with an ordering on the valued division ring. In this section, we will use a noncommutative version of the Baer-Krull theorem to determine all orderings on $\mathcal{A}_1(\mathbb{R})$ compatible with one of the valuations v we have described in the previous sections. We will then show which of these orderings on $\mathcal{A}_1(\mathbb{R})$ can be extended to an ordering on $R[y;\delta]$ compatible with a v's extension to $R[y;\delta]$.

Recall that an order P on a division ring D is compatible with a valuation v on D if for every $a, b \in D^*$ such that $v(a) = v(b) < v(a-b)$, $ab \in P$ holds.

Let v be a strongly abelian valuation on a division ring D with a formally real residue field $\overline{D}$. Let Γ be its value group. Let $s\colon \Gamma \to D^*$ be a semisection of v, i.e., a map for which

1. $s(0) = 1$,
2. $v(s(g)) = g$ for all $g \in \Gamma$,
3. $s(g_1 + g_2) = s(g_1)s(g_2)u^2$ for some $u \in D^*$ for all $g_1, g_2 \in \Gamma$.

Let $\chi\colon \Gamma/2\Gamma \to \{-1, 1\}$ be a group homomorphism called a character and let $\overline{P}$ be an ordering of $\overline{D}$. Then, as it was shown in [24],

$$P_\chi = \{a \in D \mid \overline{a \cdot s(v(a))^{-1}}\chi(v(a) + 2\Gamma) \in \overline{P}\}$$

is an order of D compatible with v. Moreover, if $\overline{X}$ denotes all orders of the residue field, X_v denotes all v-compatible orders on D and $(\Gamma/2\Gamma)^*$ denotes the set of all characters on $\Gamma/2\Gamma$, then by Proposition 3 of [24], the map

$$f\colon \overline{X} \times (\Gamma/2\Gamma)^* \to X_v$$
$$f((\overline{P}, \chi)) = P_\chi$$

is a bijection. The choice of a semisection s on Γ does not matter. Using f, we will now describe all orders on $\mathcal{A}_1(\mathbb{R})$ that are compatible with a valuation described in Section 3.

Suppose v is a valuation on $\mathcal{A}_1(\mathbb{R})$ associated to an infinite sequence $(\omega_i)_{i\geq -1}$ with $\mathbb{R}$ as a residue field. There is only one possible order of $\mathbb{R}$, so the orders of $\mathcal{A}_1(\mathbb{R})$ compatible with v will only depend on the characters $\chi\colon \Gamma/2\Gamma \to \{-1, 1\}$. Then there are three different options for the value group $\Gamma \subseteq \mathbb{Q} \times \mathbb{Z}$.

1. Γ is a 2-divisible subgroup of $\mathbb{Q}$,

2. Γ is a non-2-divisible subgroup of $\mathbb{Q}$,

3. Γ is a direct sum of a non-2-divisible subgroup of $\mathbb{Q}$ with $\mathbb{Z}$.

Since in each case the value group Γ is generated by $\{v(\omega_i)\}_{i\geq -1}$, the characters and thus the v-compatible orders will be determined by the signs of the ω_i.

In the first two cases, v is determined by an infinite sequence $(\omega_i)_{i\geq -1}$ with $v(\omega_i) = \frac{m_{i+1}}{n_{i+1}} \in \mathbb{Q}$ for each $i \geq -1$. In the third case, v is determined by a finite sequence $(\omega_i)_{i=-1}^{N}$ with $v(\omega_i) = \frac{m_{i+1}}{n_{i+1}} \in \mathbb{Q}$ for each $-1 \leq i \leq N-1$ and $v(\omega_N) \notin \mathbb{Q}$.

If the value group is a 2-divisible subgroup of $\mathbb{Q}$, then for each ω_i, there is a $j \neq i$ such that $K_{i,j} \in \mathbb{Z}$ is odd while $K_{j,i} \in \mathbb{Z}$ is even. Since $\overline{\omega_{i-1}^{K_{i,j}} \omega_{j-1}^{K_{j,i}}} = \alpha_{i,j}$, it follows that $\omega_{i-1} > 0$ if and only if $\alpha_{i,j} > 0$.

Conversely, if the value group is a non-2-divisible subgroup of $\mathbb{Q}$, we choose one i such that n_i is divisible by the greatest power of two that divides n_j for any $j \geq 0$. After choosing either $\omega_i < 0$ or $\omega_i > 0$, the order on $\mathcal{A}_1(\mathbb{R})$ is defined.

In the last case, where the value group is a direct sum of a non-2-divisible subgroup of $\mathbb{Q}$ and $\mathbb{Z}$, the order is determined by choosing either $\omega_i < 0$ or $\omega_i > 0$ and, independently, either $\omega_N > 0$ or $\omega_N < 0$ where i is as in the second case and $v(\omega_N) \notin \mathbb{Q}$. All four combinations define an ordering on $\mathcal{A}_1(\mathbb{R})$.

We have thus proven the following proposition.

Proposition 6.1. *Suppose v is a valuation on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$ and value group Γ. Then:*

1. *If Γ is a 2-divisible subgroup of $\mathbb{Q}$, there is a unique v-compatible ordering on $\mathcal{A}_1(\mathbb{R})$.*

2. *If Γ is a non-2-divisible subgroup of $\mathbb{Q}$, there are two v-compatible orderings on $\mathcal{A}_1(\mathbb{R})$.*

3. *If Γ is a direct sum of a non-2-divisible subgroup of $\mathbb{Q}$ with $\mathbb{Z}$, there are four possible v-compatible orderings on $\mathcal{A}_1(\mathbb{R})$.*

6.1 Extensions of orderings on $\mathcal{A}_1(\mathbb{R})$ to orders on $R[y;\delta]$

In this section, we show which orders on $\mathcal{A}_1(\mathbb{R})$ are extendable to an order on $R[y;\delta]$, thereby answering the question posed by Marshall and Zhang in [15].

Every order on $\mathcal{A}_1(\mathbb{R})$ is compatible with a unique finest valuation v on the same ring with residue field $\mathbb{R}$, as proved in [15]. Suppose v is a valuation on $\mathcal{A}_1(\mathbb{R})$ associated to an infinite sequence $(\omega_i)_{i\geq -1}$ with $v(\omega_{i-1}) = \frac{m_i}{n_i}$ and $\omega_i = x^{m_i}\omega_{i-1}^{n_i} - \beta_i$. In Section 4, we showed that provided both conditions of Theorem 4.6 are fulfilled, v can be uniquely extended to a valuation v' on $R[y;\delta]$ with residue field $\mathbb{R}$ if the value group is 2-divisible and that it has two extensions to $R[y;\delta]$ with the same residue field if the value group is non-2-divisible. Here we show all v-compatible orders on $\mathcal{A}_1(\mathbb{R})$ we have described in the first part of this section can be extended to a v'-compatible order on $R[y;\delta]$ for some extension v' of v from $\mathcal{A}_1(\mathbb{R})$ to $R[y;\delta]$.

Theorem 6.2. *Let P be an ordering on $\mathcal{A}_1(\mathbb{R})$ and v be the unique finest valuation on $\mathcal{A}_1(\mathbb{R})$ compatible with P. Then:*

1. *The order P can be extended to an ordering on $R[y;\delta]$ if and only if v can be extended to a valuation on $R[y;\delta]$ with residue field $\mathbb{R}$.*

2. *If the v-value group Γ is a 2-divisible subgroup of $\mathbb{Q}$, then the extension of P is unique. If on the other hand, Γ is a subgroup of $\Gamma_1 \times \mathbb{Z}$, where Γ_1 is a non-2-divisible subgroup of $\mathbb{Q}$, i.e., when Γ is not a 2-divisible subgroup of $\mathbb{Q}$, there are two extensions of P to $R[y;\delta]$. Each of the two extensions of v to a valuation v' on $R[y;\delta]$ with residue field $\mathbb{R}$ uniquely determines one of the two of P's extensions to $R[y;\delta]$.*

Proof. The first statement of the theorem follows from the fact that every ordering on $R[y;\delta]$ is compatible with a valuation on the same ring with residue field $\mathbb{R}$.

To prove the second statement, suppose that v is the unique P-compatible valuation on $\mathcal{A}_1(\mathbb{R})$ with residue field $\mathbb{R}$ that extends to a valuation on $R[y;\delta]$ with the same residue field.

If the value group Γ of v on $\mathcal{A}_1(\mathbb{R})$ is either a 2-divisible or non-2-divisible subgroup of $\mathbb{Q}$, then the value group Γ' of v's extension to $R[y;\delta]$ is $\mathbb{Q}$. In this case, there is exactly one v'-compatible order of $R[y;\delta]$ for each of v's extensions v' to $R[y;\delta]$.

Suppose Γ is a 2-divisible subgroup of $\mathbb{Q}$. Then there is a unique extension v' of v to $R[y;\delta]$. It follows that in case Γ is a 2-divisible subgroup of $\mathbb{Q}$, the only v-compatible order on $\mathcal{A}_1(\mathbb{R})$ extends to an order of $R[y;\delta]$ that is compatible with v'.

If, on the other hand, Γ is a non-2-divisible subgroup of $\mathbb{Q}$, there are two extensions v' of v to $R[y;\delta]$. We will now show that for each of the v-compatible orderings on $\mathcal{A}_1(\mathbb{R})$, there is a unique extension v' of v to $R[y;\delta]$ such that the ordering on $\mathcal{A}_1(\mathbb{R})$ can be extended to the unique v'-compatible ordering on $R[y;\delta]$.

In this case, a v-compatible ordering on $\mathcal{A}_1(\mathbb{R})$ is, as we have shown in the beginning of this section, uniquely determined by the sign of ω_{i-1} where $i \geq 1$ is such that n_i is divisible by the greatest power of two that divides n_j for any $j \geq 1$. Furthermore, v', the extension of v to $R[y;\delta]$, is uniquely determined by choosing the sign of $\tilde{\gamma}_i$ for this i.

We first choose an extension v' of v to $R[y;\delta]$. We observe that $\overline{x^{\frac{m}{n}} > 0}$ must hold for every $\frac{m}{n} \in \mathbb{Q}$ since all rational powers of x are in $R[y;\delta]$. Since $\overline{x^{\frac{m_i}{n_i}}\omega_{i-1}} = \tilde{\gamma}_i$ for each $i \geq 1$, $\tilde{\gamma}_i\omega_{i-1} > 0$ must hold for all $i \geq 0$ for the order to be extendable to a v-compatible

order on $R[y;\delta]$. This holds for exactly one of the two v-compatible orders on $\mathcal{A}_1(\mathbb{R})$. It is clear from the construction that for each ordering on $\mathcal{A}_1(\mathbb{R})$, there is exactly one extension v' of v to $R[y;\delta]$ such that this ordering is extendable to the unique v'-compatible ordering on $R[y;\delta]$.

In case Γ is a subgroup of $\mathbb{Q}\times\mathbb{Z}$ of rational rank two, $\Gamma' = \mathbb{Q}\times\mathbb{Z}$ holds. In this case, there are two v'-compatible orderings on $R[y;\delta]$ for every extension v' of v to $R[y;\delta]$. We will now show that for each of the four v-compatible orders on $\mathcal{A}_1(\mathbb{R})$, there is a unique extension v' of v to $R[y;\delta]$ and a unique v'-compatible ordering P' on $R[y;\delta]$ such that P' is an extension of P. The ordering P compatible to a valuation v on $\mathcal{A}_1(\mathbb{R})$ is determined by the signs of ω_{i-1} and ω_N where $i\geq 1$ is such that n_i is divisible by the greatest power of two that divides n_j for any $j\geq 1$, and $v(\omega_N)\notin\mathbb{Q}$. The extension v' of v to $R[y;\delta]$ and the v'-compatible ordering on $R[y;\delta]$ that extends P are the valuation v' for which $\omega_{i-1}\tilde{\gamma_i}>0$ and the v'-compatible ordering that agrees with the signs of ω_{i-1} and ω_N in P.

We have thus proved the second statement of the theorem. □

References

[1] J. Cimprič, Real spectra of quantum groups, *J. Algebra* **277** (2004), 282–297, doi:10.1016/j.jalgebra.2004.03.011, https://doi.org/10.1016/j.jalgebra.2004.03.011.

[2] P. Conrad, On ordered division rings, *Proc. Am. Math. Soc.* **5** (1954), 323–328, doi:10.2307/2032248, https://doi.org/10.2307/2032248.

[3] T. C. Craven, Witt rings and orderings of skew fields, *J. Algebra* **77** (1982), 74–96, doi:10.1016/0021-8693(82)90278-2, https://doi.org/10.1016/0021-8693(82)90278-2.

[4] N. I. Dubrovin, Noncommutative valuation rings in simple finite-dimensional algebras over a field, *Math. USSR, Sb.* **51** (1985), 493–505, doi:10.1070/SM1985v051n02ABEH002871, https://doi.org/10.1070/SM1985v051n02ABEH002871.

[5] A. Engler and A. Prestel, *Valued Fields*, Springer Monographs in Mathematics, Springer, Berlin, 2005.

[6] Á. Granja, M. C. Martínez and C. Rodríguez, Real valuations on skew polynomial rings, *Algebr. Represent. Theory* **17** (2014), 1413–1436, doi:10.1007/s10468-013-9454-7, https://doi.org/10.1007/s10468-013-9454-7.

[7] D. N. I., Noncommutative valuation rings, *Trans. Moscow Math. Soc.* **45** (1984), 273–287.

[8] I. Kaplansky, Maximal fields with valuations, *Duke Math. J.* **9** (1942), 303–321, doi:10.1215/S0012-7094-42-00922-0, https://doi.org/10.1215/S0012-7094-42-00922-0.

[9] I. Klep and D. Velušček, n-real valuations and the higher level version of the Krull-Baer theorem., *J. Algebra* **279** (2004), 345–361, doi:10.1016/j.jalgebra.2004.05.012, https://doi.org/10.1016/j.jalgebra.2004.05.012.

[10] F.-V. Kuhlmann, *Book on Valuation Theory*, in preparation.

[11] F.-V. Kuhlmann, Value groups, residue fields and bad places od rational function fields, *Trans. Am. Math. Soc.* **356** (2004), 4559–4600.

[12] J. Kürschak, Über Limesbildung und allgemeine Körpertheorie., *J. für die Reine und Angew. Math.* **142** (1913), http://eudml.org/doc/149394.

[13] S. MacLane, A construction for absolute values in polynomial rings, *Trans. Am. Math. Soc.* **40** (1936), 363–395, doi:10.2307/1989629, https://doi.org/10.2307/1989629.

[14] T. Markwig, A field of generalised Puiseux series for tropical geometry, *Rend. Semin. Mat., Univ. Politec. Torino* **68** (2010), 79–92.

[15] M. Marshall and Y. Zhang, Orderings, real places, and valuations on noncommutative integral domains, *J. Algebra* **212** (1999), 190–207, doi:10.1006/jabr.1998.7630, https://doi.org/10.1006/jabr.1998.7630.

[16] M. Marshall and Y. Zhang, Orderings and valuations on twisted polynomial rings, *Commun. Algebra* **28** (2000), 3763–3776, doi:10.1080/00927870008827055, https://doi.org/10.1080/00927870008827055.

[17] H. Marubayashi, H. Miyamoto and A. Ueda, *Non-commutative Valuation Rings and Semi-Hereditary Orders*, volume 3 of *K-Monogr. Math.*, Kluwer Academic Publishers, Dordrecht, 1997, doi:10.1007/978-94-017-2436-4, https://doi.org/10.1007/978-94-017-2436-4.

[18] G. Onay, Valued modues over skew-polynomial rings I, *J. Symb. Log.* **82** (2017), 1519–1540, https://www.jstor.org/stable/26600297.

[19] A. Prestel and C. Delzell, *Mathematical Logic and Model Theory*, Springer, London, 2011, doi:10.1007/978-1-4471-2176-3, https://doi.org/10.1007/978-1-4471-2176-3.

[20] T. Rohwer, *Valued difference fields as modules over twisted polynomial rings*, Ph.D. thesis, University of Illinois at Urbana-Champaign, 2003, https://www.ideals.illinois.edu/items/88103.

[21] O. F. G. Schilling, Noncommutative valuations, *Bull. Am. Math. Soc.* **51** (1945), 297–304, https://projecteuclid.org/journals/bulletin-of-the-american-mathematical-society/volume-51/issue-4/Noncommutative-valuations/bams/1183506882.full.

[22] J. I. Stipel'man, Valuations of the quotient field of the ring of quantum mechanics, *Funct. Anal. Appl.* **7** (1973), 46–52, doi:10.1007/bf01075649, https://doi.org/10.1007/bf01075649.

[23] J.-P. Tignol and A. R. Wadsworth, *Value Functions on Simple Algebras, and Associated Graded Rings*, Springer Monogr. Math., Springer, Berlin, 2015, doi:10.1007/978-3-319-16360-4, https://doi.org/10.1007/978-3-319-16360-4.

[24] A. Tschimmel, Lokal-global Prinzipien für Anordnungen bewerteter Schiefkörper, *Arch. Math.* **44** (1985), 48–58, doi:10.1007/bf01193780, https://doi.org/10.1007/bf01193780.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 24 (2024) #P2.05 / 273–292
https://doi.org/10.26493/1855-3974.2764.fe5
(Also available at http://amc-journal.eu)

Regular dessins with moduli fields of the form $\mathbb{Q}(\zeta_p, \sqrt[p]{q})^*$

Nicolas Daire

Département de Mathématiques et Applications, École Normale Supérieure, 45 rue d'Ulm, 75005 Paris, France

Fumiharu Kato, Yoshiaki Uchino

Department of Mathematics, Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro, Tokyo 152-8551, Japan

Received 10 December 2021, accepted 29 March 2023, published online 27 September 2023

Abstract

Gareth Jones asked during the 2014 SIGMAP conference for examples of regular dessins with nonabelian fields of moduli. In this paper, we first construct dessins whose moduli fields are nonabelian Galois extensions of the form $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$, where p is an odd prime and ζ_p is a pth root of unity and $q \in \mathbb{Q}$ is not a pth power, and we then show that their regular closures have the same moduli fields. Finally, in the special case $p = q = 3$ we give another example of a regular dessin of degree $2^{19} \cdot 3^4$ and genus 14155777 with moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$.

Keywords: Dessins d'enfants, coverings.

Math. Subj. Class. (2020): 14H57, 14H30

1 Introduction

Grothendieck first coined the term *Dessin d'enfant* in *Esquisse d'un Programme* [4] to denote a connected bicolored graph embedded on a compact connected oriented topological surface. The study was motivated by the one to one correspondance between dessins d'enfant, the combinatorial data of the associated cartographical group, and the geometric concept of coverings of $\mathbb{P}^1$ by compact Riemann surfaces ramified at most over three

*The authors are grateful to Professor Jürgen Wolfart for valuable comments.

E-mail addresses: nicolas.daire@ens.psl.eu (Nicolas Daire), bungen@math.titech.ac.jp (Fumiharu Kato), uchino.y.ab@m.titech.ac.jp (Yoshiaki Uchino)

points. Moreover, by Belyi's theorem any such covering is given the structure of an algebraic curve defined over a number field, therefore we obtain a natural action of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the set of isomorphism classes of dessins. A lot of the interest for dessins stems from the fact that this action is faithful, providing a way to study the absolute Galois group through its action on the set of dessins. A particularly interesting family of dessins is that of regular dessins, characterized by the fact that their automorphism groups act transitively on their sets of edges, and the Galois action was proved to remain faithful when restricted to the subset of isomorphism classes of regular dessins [3].

To any dessin we associate a number field called its moduli field, which is defined as the subfield of $\bar{\mathbb{Q}}$ fixed by the subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ that fixes the dessin up to isomorphism. Conder, Jones, Streit and Wolfart noted in [1] that the moduli fields of all the examples of regular dessins known at the time were abelian Galois extensions of $\mathbb{Q}$. Herradón constructed in [6] an explicit equation for a regular dessin whose moduli field $\mathbb{Q}(\sqrt[3]{2})$ is not a Galois extension of $\mathbb{Q}$, and Hidalgo later generalized his construction in [7] to produce regular dessins whose moduli fields are of the form $\mathbb{Q}(\sqrt[p]{2})$ where p is an odd prime number. However there is as of yet no known example of regular dessin whose moduli field is a nonabelian Galois extension of $\mathbb{Q}$. This is the starting point of this paper, in which we will exhibit examples of regular dessins with moduli fields that are nonabelian Galois extensions of $\mathbb{Q}$.

In the present paper, we begin by recalling the main definitions and results on dessins d'enfant. We will then expose constructions of regular dessins whose moduli fields are nonabelian Galois extensions of $\mathbb{Q}$. We first exhibit dessins whose moduli fields are of the form $\mathbb{Q}(\zeta_3, \sqrt[3]{q})$, where ζ_3 is a primitive third root of unity and $q \in \mathbb{Q}$ is not a third power, and show that the regular closures of these dessins possess the same moduli fields. We then generalize this construction to show that there exist regular dessins with moduli fields $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$, where ζ_p is a primitive pth root of unity and $q \in \mathbb{Q}_{>0}$ is not a pth power. Finally, we give an example of a regular dessin of degree $2^{19} \cdot 3^4$ and genus 14155777 with moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$.

Notations

- $\mathfrak{S}_E$: the group of self-bijections of the set E, similarly $\mathfrak{S}_n$ is the group of permutations of a set of n elements (we favor a right action, hence we write the product $\sigma\tau \coloneqq \tau \circ \sigma$)
- $\mathrm{Gal}(E/F)$: the Galois group of F-automorphisms of E
- ζ_k: the kth primitive root of unity $\exp(\frac{2i\pi}{k})$
- F_2: the free group of rank 2 with generators (ξ, η)
- Crit: the set of critical values of a function

2 Preliminaries on dessins d'enfant

We refer the reader to existing expositions of the theory such as [5, 8, 9] and [2] for proofs of the presented facts and further details.

A *dessin d'enfant* is a connected bipartite graph embedded on a compact connected orientable topological surface, such that the complement of the graph is a disjoint union of

2-cells. Two such dessins are equivalent if there exists an orientation preserving homeomorphism between the underlying surfaces that induces an isomorphism between the embedded bipartite graphs.

A dessin is determined up to isomorphism by a pair (C, β) where C is a smooth algebraic curve and $\beta\colon C \to \mathbb{P}^1$ is a meromorphic mapping ramified at most over $\{0, 1, \infty\}$, and by Belyi's theorem we can further ask for C and β to both be defined over a number field. We call (C, β) a *Belyi pair* and β a *Belyi function*. The corresponding graph embedding on the underlying surface is recovered by pulling back the segment $[0, 1]$ along β, we define black and white vertices as the preimages of 0 and 1 respectively, and the edges as the preimages of $]0, 1[$.

By covering theory a dessin is also determined up to isomorphism by the *monodromy action* of the fundamental group of the complex projective line $\pi_1(\mathbb{P}^1)$ on the fiber over the point $\frac{1}{2}$ which is identified to the set of edges of the dessin. The fundamental group $\pi_1(\mathbb{P}^1)$ is isomorphic to the free group of rank two $F_2 = \langle \xi, \eta \rangle$ with generators ξ and η which are two loops with base point $\frac{1}{2}$ and circling counter-clockwise around 0 and 1 respectively. The monodromy action of the generators ξ and η then corresponds to the product of the counter-clockwise cyclic permutation of the edges around black and white vertices respectively. We call *monodromy map* $M\colon F_2 \to \mathfrak{S}_E$ the map that associates to each element of F_2 the corresponding permutation of the set of edges, and we call *cartographic group* the image of the monodromy map, which is a transitive subgroup of the group of permutations of the set of edges.

When the *automorphism group* of a dessin $\mathcal{D}$ acts transitively on the set of edges, we say that $\mathcal{D}$ is a *regular dessin*. When that is the case the cartographic group G acts transitively and freely on the set of edges, the monodromy action is thus given by the canonical action of G on itself. There is a natural bijection between regular dessins and finite groups generated by two distinguished elements ξ and η up to isomorphism. Two regular dessins determined by $G_1 = \langle \xi_1, \eta_1 \rangle$ and $G_2 = \langle \xi_2, \eta_2 \rangle$ respectively are isomorphic if and only if there exists an isomorphism between G_1 and G_2 that preserves the distinguished generators. Given a dessin $\mathcal{D}$, there exists a unique regular dessin $\widetilde{\mathcal{D}}$ with a morphism $\phi\colon \widetilde{\mathcal{D}} \to \mathcal{D}$ such that any morphism from a regular dessin to $\mathcal{D}$ factors through ϕ. We call $\widetilde{\mathcal{D}}$ the *regular closure* of $\mathcal{D}$. Moreover, there exists an isomorphism $\mathrm{Cart}(\widetilde{\mathcal{D}}) \cong \mathrm{Cart}(\mathcal{D})$ that preserves the distinguished generators. There exists a natural action of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the set of isomorphism classes of dessins, we denote by $\mathcal{D}^\sigma$ the action of an automorphism σ on a dessin $\mathcal{D}$, and this Galois action commutes with regular closure, i.e. we have $(\widetilde{\mathcal{D}})^\sigma \cong \widetilde{(\mathcal{D}^\sigma)}$.

Given a dessin $\mathcal{D}$, we say that a number field k is a *field of definition* of $\mathcal{D}$ if $\mathcal{D}$ is isomorphic to a dessin defined over k. However there does not necessarily exist a smallest field of definition. We thus define the *moduli field* of a dessin $\mathcal{D}$ as the subfield of $\bar{\mathbb{Q}}$ fixed by the subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ constituted of the elements fixing $\mathcal{D}$ up to isomorphism. The moduli field of a dessin is contained in all fields of definition but is not necessarily itself a field of definition, however it is the case in particular for regular dessins.

3 Constructions of regular dessins with nonabelian moduli fields

We are now ready to give examples of regular dessins whose moduli fields are nonabelian Galois extensions of $\mathbb{Q}$. To do so, we will first exhibit dessins with such moduli fields, and then prove that their regular closures admit the same moduli fields.

Before proceeding with the examples, let us first present a classic family of Belyi polynomials that we will use in the following constructions. For positive integers $m, n \in \mathbb{N}$ we define the polynomial

$$B_{m,n} \coloneqq \frac{(m+n)^{m+n}}{m^m n^n} X^m (1-X)^n \in \mathbb{Q}[X].$$

By computing the derivative $B'_{m,n} = \frac{(m+n)^{m+n}}{m^m n^n} X^{m-1}(1-X)^{n-1}(m-(m+n)X)$ we verify that $B_{m,n} : \mathbb{P}^1 \to \mathbb{P}^1$ is a Belyi function that ramifies only at 0, 1, ∞ and $\frac{m}{m+n}$ with ramification indices m, n, $m+n$ and 2 respectively, and $B_{m,n}(0) = 0$, $B_{m,n}(1) = 0$, $B_{m,n}(\infty) = \infty$ and $B_{m,n}(\frac{m}{m+n}) = 1$ (see Figure 1).

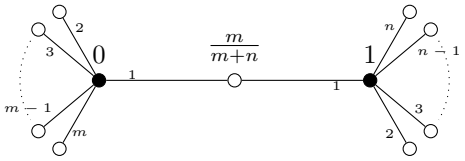


Figure 1: Dessin corresponding to the Belyi pair $(\mathbb{P}^1, B_{m,n})$.

3.1 Regular dessins with moduli fields of the form $\mathbb{Q}(\zeta_3, \sqrt[3]{q})$

Let $q \in \mathbb{Q}_{>0}$ be a positive rational number that is not a third power.

Let $m, n \in \mathbb{N}$ be coprime positive integers such that $\frac{27}{27+q^2} = \frac{m}{m+n}$, and let

$$C\colon y^2 = x(x-(1-\zeta_3))(x-\sqrt[3]{q}),$$
$$\beta\colon C \to \mathbb{P}^1,\ (x,y) \mapsto \frac{1}{27^m q^{2n}}(x^6+27)^m (q^2-x^6)^n.$$

The function β is given by the composition $\beta = \beta_1 \circ \beta_0 \circ \pi$ of the following maps.

1. $\pi\colon C \to \mathbb{P}^1$ is the projection on the coordinate x, which is ramified over $\{0, 1-\zeta_3, \sqrt[3]{q}, \infty\}$.
2. $\beta_0 \coloneqq X^6 \in \mathbb{Q}[X]$, $\mathrm{Crit}(\beta_0) = \{0\}$ so $\beta_1 \circ \pi$ ramifies over $\{0, (1-\zeta_3)^6 = -27, q^2, \infty\}$.
3. $\beta_1 \coloneqq B_{m,n}(\frac{X+27}{q^2+27})$, so $\beta = \beta_1 \circ \beta_0 \circ \pi$ ramifies over $\{0, 1, \infty\}$.

The pair (C, β) is thus a Belyi pair, and we call $\mathcal{D}$ the corresponding dessin. The dessin $\mathcal{D}$ is defined over $\mathbb{Q}(\zeta_3, \sqrt[3]{q})$, so its moduli field is a subfield of $\mathbb{Q}(\zeta_3, \sqrt[3]{q})$. By taking the regular closure we then obtain the inclusion of moduli fields $\mathcal{M}(\widetilde{D}) \subseteq \mathcal{M}(D) \subseteq \mathbb{Q}(\zeta_3, \sqrt[3]{q})$, and moreover $\widetilde{D}$ is regular so it is defined over $\mathcal{M}(\widetilde{D})$. We shall prove that $\mathcal{M}(\widetilde{\mathcal{D}})$ is in fact exactly $\mathbb{Q}(\zeta_3, \sqrt[3]{q})$, which is a nonabelian Galois extension of $\mathbb{Q}$ with Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{q})/\mathbb{Q}) \cong \mathfrak{S}_3.$$

To that end we must show that an automorphism $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ fixes $\widetilde{\mathcal{D}}$ if and only if it fixes ζ_3 and $\sqrt[3]{q}$, or equivalently that $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{q})/\mathbb{Q})$ acts freely on the orbit of $\widetilde{\mathcal{D}}$.

Let $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, the Galois conjugate $\mathcal{D}^\sigma$ is given by the Belyi pair (C^σ, β^σ), where

$$C^\sigma : y^2 = x(x - (1 - \sigma(\zeta_3)))(x - \sigma(\sqrt[3]{q})),$$

and β^σ has the same expression as β because all of its coefficients are rational. The orbit of the pair $(\zeta_3, \sqrt[3]{q})$ by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is $\{\zeta_3^i, \zeta_3^j \sqrt[3]{q}\}_{1\leq i\leq 2, 0\leq j\leq 2}$. Elliptic curves given by equations of the form $y^2 = (x-a)(x-b)(x-c)$ are isomorphic if and only if the cross-ratios of the tuples (a, b, c, ∞) coincide. We verify that the cross-ratios are all distinct, so the orbit of $\mathcal{D}$ is given by the six dessins $\mathcal{D}^\sigma$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{q})/\mathbb{Q})$. As a consequence $\mathcal{M}(\mathcal{D}) = \mathbb{Q}(\zeta_3, \sqrt[3]{q})$. To prove that the regular closures $\widetilde{\mathcal{D}^\sigma}$ constituting the orbit of $\widetilde{\mathcal{D}}$ are also non isomorphic, we must first draw the dessins $\mathcal{D}^\sigma$ to compute their cartographic groups.

Let us first draw the dessin $\mathcal{D}_0$ corresponding to the Belyi pair $(\mathbb{P}^1, \beta_1 \circ \beta_0)$ (see Figure 3). The dessin $\mathcal{D}_0$ is defined over $\mathbb{Q}$, so the dessins $\mathcal{D}^\sigma$ in the orbit are then obtained by lifting $\mathcal{D}_0$ to the curves C^σ. To simplify the graphical representations of the dessins, we will use the notation in Figure 2 for consectutive edges incident to a vertex.

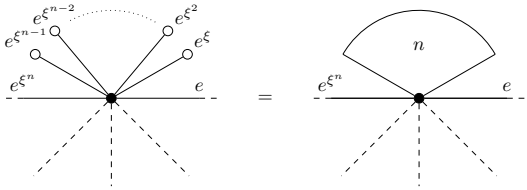


Figure 2: Notation for consecutive edges.

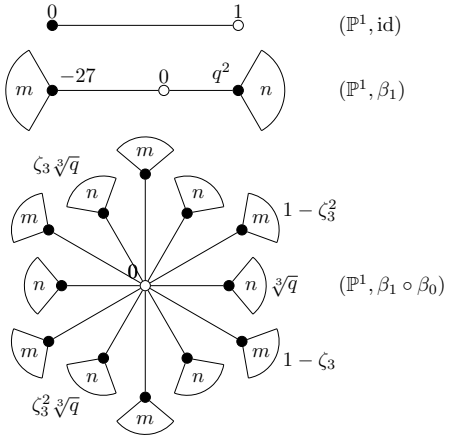
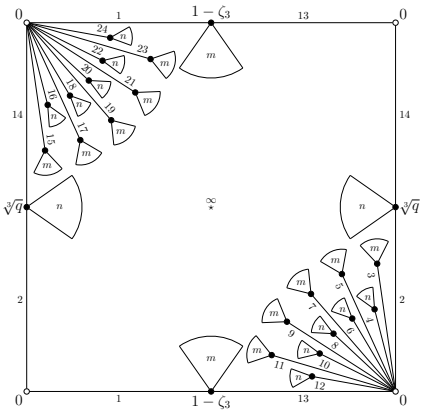
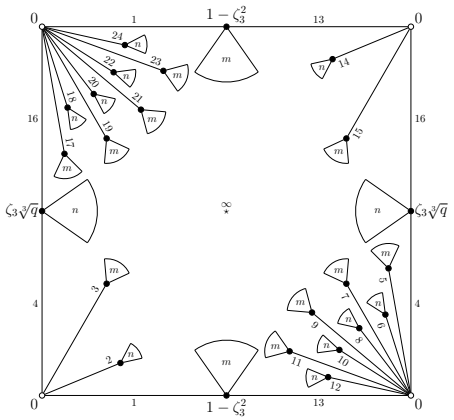


Figure 3: Construction of $\mathcal{D}_0$.

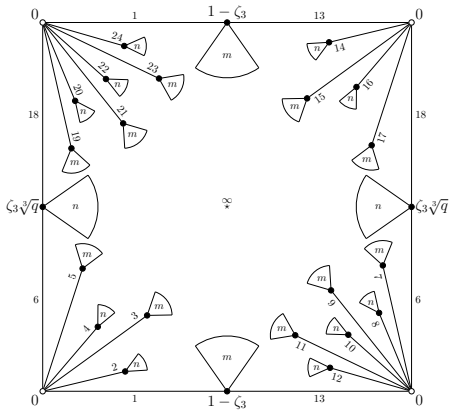
The dessins $\mathcal{D}_1, \ldots, \mathcal{D}_6$ conjugate to $\mathcal{D}$ are embedded on a torus, so in the representations in Figure 4 we will identify the outermost edges on opposite sides.



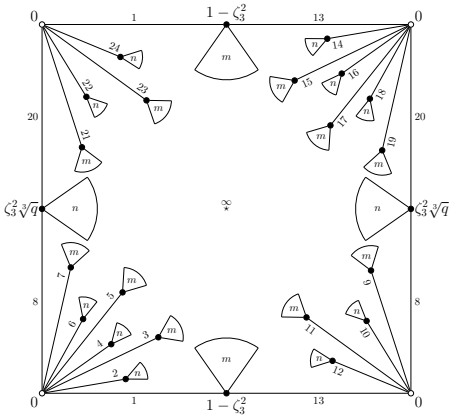
(a) $\mathcal{D}_1 \coloneqq \mathcal{D}$



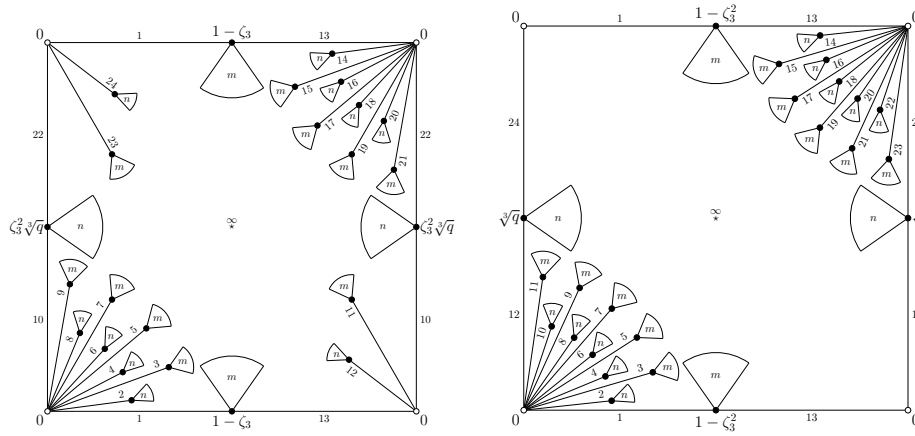
(b) $\mathcal{D}_2 \coloneqq \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3^2, \zeta_3 \sqrt[3]{q})$



(c) $\mathcal{D}_3 \coloneqq \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3, \zeta_3 \sqrt[3]{q})$



(d) $\mathcal{D}_4 \coloneqq \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3^2, \zeta_3^2 \sqrt[3]{q})$



(e) $\mathcal{D}_5 := \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3, \zeta_3^2\sqrt[3]{q})$ (f) $\mathcal{D}_6 := \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3^2, \sqrt[3]{q})$

Figure 4: Dessins $\mathcal{D}_1, \ldots, \mathcal{D}_6$ in the Galois orbit of $\mathcal{D}$.

We will now establish that $\widetilde{\mathcal{D}_1}$ is not isomorphic to $\widetilde{\mathcal{D}_2}, \ldots, \widetilde{\mathcal{D}_6}$. To that end it suffices to show that there is no isomorphism between the cartographic groups fixing the canonical generators. We shall therefore exhibit an element $\omega \in F_2 = \langle \xi, \eta \rangle$ such that $M_k(\omega)$ commutes with $M_k(\eta^2)$ only when $k = 1$, where M_k is the monodromy map of $\mathcal{D}_k$.

We have defined m and n to be positive coprime integers such that $\frac{27}{27+q^2} = \frac{m}{m+n}$, so we cannot have $m = n = 1$. We will treat the case where $m \neq 1$ does not divide n, the other case being treated similarly. Let

$$\omega := \xi^n \eta^{-1} \xi^{m-n} \eta \xi^n.$$

We shall show that $M_k(\omega)$ commutes with $M_k(\eta^2)$ only when $k = 1$.

Let $E_k := \{1, 2, \ldots, 24\}$ be the set of edges of $\mathcal{D}_k$ incident to 0. The action of η fixes the set E_k on which it induces the cyclic permutation $(1, 2, \ldots, 24)$, and every white vertex except 0 has degree one so the action of η is trivial on the complement of E_k.

We can write $E_k = E_k^{\text{odd}} \sqcup E_k^{\text{even}}$ as the disjoint union of the sets of respectively odd and even numbered edges incident to 0, such that η sends one to the other. The black vertices of E_k^{odd} are of degree m except for the two black vertices of the edges 1 and 13 that are of degree $2m$. Therefore if m does not divide some integer l then ξ^l sends every edge of E_k^{odd} to the complement of E_k, and otherwise the action of ξ^m on E_k^{odd} corresponds to the sole transposition $(1, 13)$. Similarly if n does not divide l then ξ^l sends every edge of E_k^{even} to the complement of E_k, and the action of ξ^n on E_k^{even} is the transposition $(2k, 2k + 12)$.

In particular, by hypothesis n is not a multiple of m, so $m - n$ is not a multiple of m either, hence both ξ^n and ξ^{m-n} send the edges of E_k^{odd} to the complement of E_k. However η acts trivially on the latter, so $\xi^n \eta^{-1} \xi^{m-n}$ and $\xi^{m-n} \eta \xi^n$ both fix the set E_k^{odd} on which they induce the same action as ξ^m, i.e. the transposition $(1, 13)$. Therefore the action of $\omega = \xi^n \eta^{-1} \xi^{m-n} \eta \xi^n$ is the same as that of $\xi^m \eta \xi^n$ on E_k^{odd} and the same as that of $\xi^n \eta^{-1} \xi^m$ on E_k^{even}. See Figure 5.

The action of ω fixes the set E_k on which it induces the permutation

$$M_k(\omega)|_{E_k} = (1, 13)(2k, 2k + 12) \cdot (1, 2)(3, 4) \cdots (23, 24) \cdot (1, 13)(2k, 2k + 12)$$

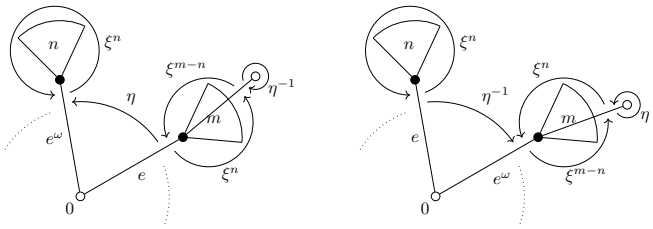


Figure 5: Action of ω on $E_k^{\mathrm{odd}} \setminus \{1, 2k-1\}$ and on $E_k^{\mathrm{even}} \setminus \{2, 2k\}$.

Therefore for $k = 1$,

$$\begin{aligned} M_1(\omega)|_{E_1} &= (1,13)(2,14) \cdot (1,2)(3,4)\cdots(23,24) \cdot (1,13)(2,14) \\ &= (1,2)(3,4)\cdots(23,24) \end{aligned}$$

so ω and η^2 commute on E_1. Moreover η acts trivially on the complement of E_1 so $M_1(\omega)|_{\mathcal{D}_1 \setminus E_1}$ and $M_1(\eta^2)|_{\mathcal{D}_1 \setminus E_1}$ automatically commute. Finally, we obtain that $M_1(\omega)$ and $M_1(\eta^2)$ commute.

For $k = 2$, we observe that $4^{\omega\eta^2} = 15^{\eta^2} = 17$ but $4^{\eta^2\omega} = 6^\omega = 5$. Similarly, for $3 \le k \le 6$, we observe that $1^{\omega\eta^2} = 14^{\eta^2} = 16$ but $1^{\eta^2\omega} = 3^\omega = 4$. We have thus shown that $M_k(\omega)$ and $M_k(\eta^2)$ commute only for $k = 1$.

This concludes the proof that $\widetilde{\mathcal{D}}$ is a regular dessin with moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{q})$.

3.2 Regular dessins with moduli fields of the form $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$

Let p be an odd prime, and $q \in \mathbb{Q}_{>0}$ a positive rational number that is not a pth power. In this example we will need an additional parameter $\gamma \in \mathbb{Q} \setminus \{0\}$. Let

$$C\colon y^2 = x(x - (1-\zeta_p))(x - \gamma\sqrt[p]{q}).$$

We construct the Belyi function $\beta\colon C \to \mathbb{P}^1$ as the composition $\beta = \beta_2 \circ \beta_1 \circ \beta_0 \circ \pi$ of the following maps.

1. $\pi\colon C \to \mathbb{P}^1$ is the projection on the coordinate x, which ramifies over $\{0, 1-\zeta_p, \gamma\sqrt[p]{q}, \infty\}$.
2. $\beta_0 := X^{2p} \in \mathbb{Q}[X]$, and $\mathrm{Crit}(\beta_0) = \{0, \infty\}$ so $\beta_0 \circ \pi$ ramifies over $\{0, (1-\zeta_p)^{2p}, \gamma^{2p}q^2, \infty\}$.
3. $\beta_1 \in \mathbb{Q}[X]$ is chosen independently of γ such that $\mathrm{Crit}(\beta_1) \cup \{\beta_1((1-\zeta_p)^{2p})\} = \{0, 1, \infty\}$, $\beta_1((1-\zeta_p)^{2p}) = 0 < \beta_1(0) < 1$ and $\beta_1'(0) > 0$. The existence of β_1 verifying those conditions is assured by Proposition 3.2 below. Under those assumptions $\beta_1 \circ \beta_0 \circ \pi$ ramifies over $\{0, 1, \beta_1(0), \beta_1(\gamma^{2p}q^2), \infty\}$.
4. $\gamma \in \mathbb{Q}_{>0}$ is then chosen small enough so that $\beta_1' > 0$ on $[0, \gamma^{2p}q^2]$. This guarantees us that we have $0 < \beta_1(0) < \beta_1(\gamma^{2p}q^2) < 1$.
5. $\beta_2 := B_{r,s} \circ B_{m,n}$, where (m,n) and (r,s) are pairs of coprime positive integers such that $\beta_1(\gamma^{2p}q^2) = \frac{m}{m+n}$ and $B_{m,n}(\beta_1(0)) = \frac{r}{r+s}$. Finally, $\beta = \beta_2 \circ \beta_1 \circ \beta_0 \circ \pi$ ramifies over $\{0, 1, \infty\}$.

The pair (C, β) is thus a Belyi pair, and we call $\mathcal{D}$ the corresponding dessin. With the same arguments as before, the moduli field of $\mathcal{D}$ is $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$, which is a nonabelian Galois extension of $\mathbb{Q}$ with Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p, \sqrt[p]{q})/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$$

generated by $\sigma\colon \zeta_p^i \sqrt[p]{q} \mapsto \zeta_p^{i+1} \sqrt[p]{q}$ and $\tau\colon \zeta_p^i \sqrt[p]{q} \mapsto \zeta_p^{gi} \sqrt[p]{q}$ where g generates $(\mathbb{Z}/p\mathbb{Z})^\times$. We shall show that there exists $\gamma \in \mathbb{Q} \setminus \{0\}$ such that the regular closure of the dessin $\mathcal{D}$ thus obtained also has moduli field $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$.

Remark 3.1. In the previous subsection we treated the case $p = 3$. In that specific case we gave a simpler expression for β, mainly due to the fact that $\beta_0 \circ \pi$ already had all of its critical values in $\mathbb{Q} \cup \{\infty\}$. However in the general case we must use the intermediate map β_1 as well as the parameter γ to conclude the proof.

Let us first prove the existence of β_1.

Proposition 3.2. *Let $E \subset \bar{\mathbb{Q}} \cap \mathbb{R} \setminus \{0\}$ be a finite set. Then there exists $P \in \mathbb{Q}[X]$ such that $P(E) \subseteq \{0\}$, $\mathrm{Crit}(P) \subseteq \{0, 1\}$, $0 < P(0) < 1$ and $P'(0) > 0$.*

Remark 3.3. In the context of this proposition we only deal with polynomials so for $P \in \mathbb{Q}[X]$ we define $\mathrm{Crit}(P) := \{P(z) |\ z \in \mathbb{C}, P'(z) = 0\}$, which does not include the point at infinity to simplify notations.

Proof. To show this we will proceed similarly as in the proof of the *only if* part of Belyi's theorem, by applying additional transformations to ensure that $0 < P(0) < 1$. Let us first prove that we can reduce to the case where E is a subset of rational numbers.

Lemma 3.4. *Let $E \subset \bar{\mathbb{Q}} \cap \mathbb{R} \setminus \{0\}$ be a finite set fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then there exists $P \in \mathbb{Q}[X]$ such that $P(0) = 0$ and $\mathrm{Crit}(P) \cup P(E) \subset \mathbb{Q} \setminus \{0\}$.*

Proof. Let $\{a_1, \ldots, a_m\} = E \cap \mathbb{Q}$ and $\{b_1, \ldots, b_n\} = E \setminus \mathbb{Q}$. We construct P by induction on the number n of non rational elements of E.

For $\alpha \in \mathbb{Q}$, define $F_\alpha, G_\alpha \in \mathbb{Q}[X]$ by

$$F_\alpha := \prod_{j=1}^{n} (X - (b_j - \alpha)^2) \quad \text{and} \quad G_\alpha := F_\alpha((X-\alpha)^2) = \prod_{j=1}^{n} (X - b_j)(X + b_j - 2\alpha).$$

Let us first assume that there exists $\alpha \in \mathbb{Q}$ such that $G_\alpha(0) \notin \mathrm{Crit}(G_\alpha) \cup G_\alpha(E)$. Define $P_1(X) := G_\alpha(X) - G_\alpha(0) \in \mathbb{Q}[X]$, then $P_1(0) = 0 \notin E' := \mathrm{Crit}(P_1) \cup P_1(E) \subset \bar{\mathbb{Q}} \cap \mathbb{R} \setminus \{0\}$. Note that E' is stable under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and $|E' \setminus \mathbb{Q}| = |\mathrm{Crit}(F_\alpha) \cup F_\alpha(0) \setminus \mathbb{Q}| = |\mathrm{Crit}(F_\alpha) \setminus \mathbb{Q}| < \deg F_\alpha = n$. By induction, there exists $P_2 \in \mathbb{Q}[X]$ such that $P_2(0) = 0$ and $\mathrm{Crit}(P_2) \cup P_2(E') \subset \mathbb{Q} \setminus \{0\}$. Now $P := P_2 \circ P_1$ has the desired properties, since $P(0) = 0$ and $\mathrm{Crit}(P) \cup P(E) = \mathrm{Crit}(P_2) \cup P_2(\mathrm{Crit}(P_1)) \cup P_2(P_1(E)) = \mathrm{Crit}(P_2) \cup P_2(E') \subset \mathbb{Q} \setminus \{0\}$.

Let us now prove that there exists $\alpha \in \mathbb{Q}$ such that $G_\alpha(0) \notin \mathrm{Crit}(G_\alpha) \cup G_\alpha(E)$. Let us first treat the case where $0 < b_1 < b_2, \ldots, b_n$. When α approaches $\frac{1}{2}$, $G_\alpha(0) = \prod_{j=1}^{n} -b_j(b_j - 2\alpha)$ approaches 0 but the critical values of G_α do not. Indeed, $\mathrm{Crit}(G_\alpha) = \mathrm{Crit}\, F_\alpha \cup F_\alpha(\mathrm{Crit}((X-\alpha)^2)) = \mathrm{Crit}(F_\alpha) \cup \{F_\alpha(0)\}$; $F_\alpha(0)$ approaches $F_{\frac{b_1}{2}}(0) \neq 0$, and since $F_{\frac{b_1}{2}}$ does not have multiple roots, the critical values of F_α approach the critical values

of $F_{\frac{b_1}{2}}$ which are all non zero. Therefore for $\alpha \neq \frac{b_1}{2}$ in the neighborhood of $\frac{b_1}{2}$ we have $G_\alpha(0) \notin \mathrm{Crit}(G_\alpha)$. Moreover $G_\alpha(0), G_\alpha(a_1), \ldots, G_\alpha(a_m)$ are all distinct polynomials in the indeterminate α, so they coincide at only finitely many points. In particular for $\alpha \neq \frac{b_1}{2}$ in the neighborhood of $\frac{b_1}{2}$ we have $G_\alpha(0) \notin \{G_\alpha(a_1), \ldots, G_\alpha(a_m)\}$. Since $\alpha \in \mathbb{Q}$ we also have $G_\alpha(0) \neq 0 = G_\alpha(b_1) = \cdots = G_\alpha(b_n)$ hence $G_\alpha(0) \notin G_\alpha(E)$, proving the existence of α as desired.

Let us now treat the general case where $b_1, \ldots, b_n$ are not assumed to be positive by reducing it to the previous case. For $\alpha' \in \mathbb{Q}$, define $H_{\alpha'} \in \mathbb{Q}[X]$ by

$$H_{\alpha'} \coloneqq (X - \alpha')^2 - \alpha'^2 \in \mathbb{Q}[X].$$

Note that $\mathrm{Crit}(H_{\alpha'}) = \{-\alpha'\}$. For $\alpha' > 0$ sufficiently small we have $-\alpha'^2 < H_{\alpha'}(0) = 0 < H_{\alpha'}(a_1), \ldots, H_{\alpha'}(a_m), H_{\alpha'}(b_1), \ldots, H_{\alpha'}(b_n)$. Let $E'' \coloneqq \mathrm{Crit}(H_{\alpha'}) \cup H_{\alpha'}(E)$. The set E'' is a finite subset of $\bar{\mathbb{Q}} \cap \mathbb{R} \setminus \{0\}$ fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and E'' has at most n non rational elements, which are all positive. By the above, there exists $P_3 \in \mathbb{Q}[X]$ such that $\mathrm{Crit}(P_3) \cup P_3(E'') \subset \mathbb{Q} \setminus \{0\}$ and $P_3(0) = 0$. Then $P \coloneqq P_3 \circ H_{\alpha'}$ has the desired properties, since $P(0) = 0$ and $\mathrm{Crit}(P) \cup P(E) = \mathrm{Crit}(P_3) \cup P_3(\mathrm{Crit}(H_{\alpha'})) \cup P_3(H_{\alpha'}(E)) = \mathrm{Crit}(P_3) \cup P_3(E'') \subset \mathbb{Q} \setminus \{0\}$. □

Let us denote by P_1 the polynomial obtained using this lemma, which verifies $P_1(0) = 0$ and $E' \coloneqq \mathrm{Crit}(P_1) \cup P_1(E) \subset \mathbb{Q} \setminus \{0\}$. We can further assume that $P_1'(0) > 0$ by taking $(-P_1)$ if necessary. We now send the points E' to $\{0, 1\}$.

Lemma 3.5. *Let $E \subset \mathbb{Q} \setminus \{0\}$ a finite set. Then there exists $P \in \mathbb{Q}[X]$ such that $P(E) \subseteq \{0\}$, $\mathrm{Crit}(P) \subseteq \{0, 1\}$, $0 < P(0) < 1$ and $P'(0) > 0$.*

Proof. For $\alpha \in \mathbb{Q}$, let $F_\alpha \coloneqq (X - \alpha)^2 \in \mathbb{Q}[X]$, and note that $\mathrm{Crit}(F_\alpha) = \{0\}$. There exists $\alpha < 0$ sufficiently small such that $0 < F_\alpha(0) < F_\alpha(a)$ for all $a \in E$. We take

$$F \coloneqq \frac{F_\alpha}{\max_{a \in E} F_\alpha(a)}.$$

Let $\{a_1, \ldots, a_l\} = F(E)$ such that $0 < F(0) < a_1 < \cdots < a_l = 1$. We also add a rational point $a_0 \in \mathbb{Q}$ such that $F(0) < a_0 < a_1$.

Let m and n be the coprime positive integers such that $a_{l-1} = \frac{m}{m+n}$. We recall that $B_{m,n}$ verifies $\mathrm{Crit}(B_{m,n}) = \{0, 1\}$, $B_{m,n}(0) = B_{m,n}(1) = 0$, $B_{m,n}(\frac{m}{m+n}) = 1$, and $B_{m,n}$ is strictly increasing between 0 and $\frac{m}{m+n}$. Let $P_1 \coloneqq B_{m,n}$, then $\mathrm{Crit}(P_1) = \{0, 1\}$ and $0 < P_1 \circ F(0) < P_1(a_0) < \cdots < P_1(a_{l-1}) = 1$. There is one point fewer than before, so we can iteratively construct $P_2, \ldots, P_l$ in the same way, so that $P \coloneqq P_l \circ \cdots \circ P_1$ verifies $\mathrm{Crit}(P) \subseteq \{0, 1\}$, $P(a_1) = \cdots = P(a_l) = 0 < P(F(0)) < 1 = P(a_0)$ and $P'(F(0)) > 0$. Therefore $P \circ F$ has the desired properties. □

Let us denote by P_2 the polynomial obtained using this lemma with the finite set E' obtained previously. Then the polynomial $P \coloneqq P_2 \circ P_1$ verifies $P(E) \subseteq \{0\}$, $\mathrm{Crit}(P) \subseteq \{0, 1\}$, $0 < P(0) < 1$ and $P'(0) > 0$, thus concluding the proof of Proposition 3.2. □

We can now use Proposition 3.2 with the finite set

$$E \coloneqq \{(1 - \zeta_p^k)^{2p}\}_{1 \leq k \leq \frac{p-1}{2}}$$

to obtain the map β_1 as desired. For $1 \leq k \leq \frac{p-1}{2}$ we have $(1-\zeta_p^k)^{2p} = (|1-\zeta_p^k|\zeta_{2p}^{2k-1})^{2p} = |1-\zeta_p^k|^{2p} \in \mathbb{R}$ so $E \subset \bar{\mathbb{Q}} \cap \mathbb{R}$, and the set E is the Galois orbit of $(1-\zeta_p)^{2p}$ so it is fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, hence E verifies the conditions of Proposition 3.2.

Let us denote by $\mathcal{D}(\beta_1)$ the dessin corresponding to the Belyi pair $(\mathbb{P}^1, \beta_1)$. The Belyi pair $(\mathbb{P}^1, \beta_1)$ is fixed by the action of the complex conjugation, so the embedding of $\mathcal{D}(\beta_1)$ on $\mathbb{P}^1$ admits a symmetry along the real line. Moreover the Belyi function β_1 is a polynomial, so $\mathcal{D}(\beta_1) \cap \mathbb{R}$ is a (graph theoretic) path. Let $v_l < \cdots < v_1$ be the negative vertices on the path, and let e_k denote the edge (v_{k-1}, v_k). By hypothesis $\beta_1'(0) > 0$ so v_1 is a black vertex, and for $k < l$, the vertex v_k is of even degree $2d_k$. We then have $e_k^{\xi^{d_k}} = e_{k+1}$ and $e_{k+1}^{\xi^{d_k}} = e_k$ if k is odd, or $e_k^{\eta^{d_k}} = e_{k+1}$ and $e_{k+1}^{\eta^{d_k}} = e_k$ if k is even. See Figure 6.

As remarked earlier, the Galois orbit of $(1-\zeta_p)^{2p}$ is $\{(1-\zeta_p^k)^{2p}\}_{1\leq k\leq \frac{p-1}{2}} \subset \mathbb{R}_-$, and $(1-\zeta_p^{\frac{p-1}{2}})^{2p} < \cdots < (1-\zeta_p)^{2p} < 0$. By construction $\beta_1((1-\zeta_p)^{2p}) = 0$, so $(1-\zeta_p)^{2p}$ and all its Galois conjugates are black vertices of $\mathcal{D}(\beta_1)$ lying on the path $(v_1, \cdots, v_l)$. Let $t > 0$ be the index such that $v_t = (1-\zeta_p)^{2p}$, and v_t is a black vertex so t is odd. Then

$$\mu_0 \coloneqq \xi^{d_1}\eta^{d_2}\cdots\eta^{d_{t-1}}\xi^{2d_t}\eta^{d_{t-1}}\cdots\eta^{d_2}\xi^{d_1}$$

fixes the edge e_1 (Figure 6).

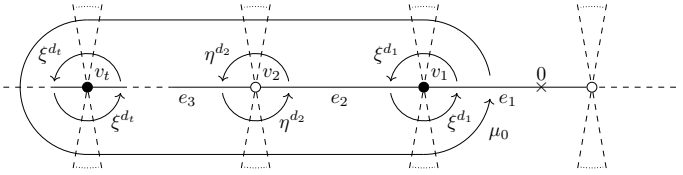


Figure 6: Dessin $\mathcal{D}(\beta_1)$ corresponding to $(\mathbb{P}^1, \beta_1)$.

Let $\gamma > 0$ small enough so that $\beta_1' > 0$ on $[0, \gamma^{2p}q^2]$. Let us next draw the dessin $\mathcal{D}(\beta_2)$ corresponding to the Belyi pair $(\mathbb{P}^1, \beta_2 = B_{r,s} \circ B_{m,n})$. See Figure 7.

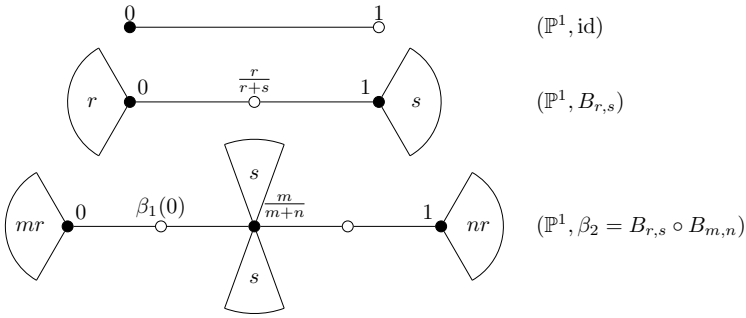


Figure 7: Dessin $\mathcal{D}(\beta_2)$ corresponding to $(\mathbb{P}^1, \beta_2)$.

By lifting the dessin $\mathcal{D}(\beta_2)$ along β_1 we obtain the dessin $\mathcal{D}(\beta_2 \circ \beta_1)$ corresponding to the Belyi pair $(\mathbb{P}^1, \beta_2 \circ \beta_1)$. This amounts to replacing each edge of $\mathcal{D}(\beta_1)$ by a copy of $\mathcal{D}(\beta_2)$. Note that the degrees of the black and white vertices are thus multiplied by mr and

nr, respectively. Analogously to μ_0 we define

$$\begin{aligned}\mu \coloneqq &(\xi^{mrd_1}\eta\xi^s\eta)(\xi^{nrd_2}\eta\xi^s\eta)\cdots(\xi^{mrd_{t-2}}\eta\xi^s\eta)(\xi^{nrd_{t-1}}\eta\xi^s\eta)\\ &\cdot(\xi^{2mrd_t}\eta\xi^s\eta)(\xi^{nrd_{t-1}}\eta\xi^s\eta)(\xi^{mrd_{t-2}}\eta\xi^s\eta)\cdots(\xi^{nrd_2}\eta\xi^s\eta)\xi^{mrd_1}\end{aligned}$$

and we verify again that μ fixes the edge $(0, v_1)$. Note also that ξ^{2s} fixes the edge $(0, \gamma\sqrt[p]{q})$. See Figure 8.

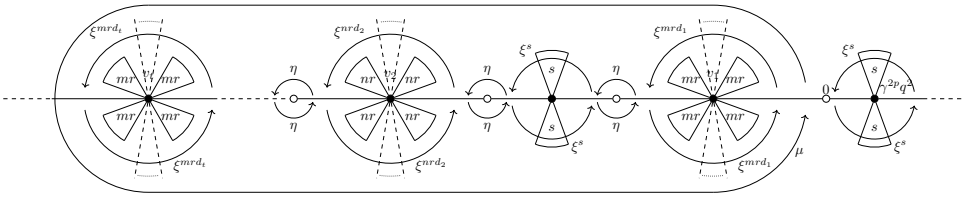


Figure 8: Dessin $\mathcal{D}(\beta_2 \circ \beta_1)$ corresponding to $(\mathbb{P}^1, \beta_2 \circ \beta_1)$.

Let $\mathcal{D}_0$ be the dessin corresponding to the Belyi pair $(\mathbb{P}^1, \beta_2 \circ \beta_1 \circ \beta_0)$. To simplify the representations of the dessins we only show the vertices 0, $\zeta_{2p}^k(1-\zeta_p)$, $1-\zeta_p^k$, and $\zeta_{2p}^k\gamma\sqrt[p]{q}$. We decorate the vertices $\zeta_{2p}^k(1-\zeta_p)$ (which map to $(1-\zeta_p)^{2p} \in \mathbb{R}_-$ by β_0) and $\zeta_{2p}^k\gamma\sqrt[p]{q}$ (which map to $\gamma^{2p}q^2 \in \mathbb{R}_+$ by β_0) respectively with the symbols $\ominus$ and $\oplus$ to distinguish them. See Figure 9.

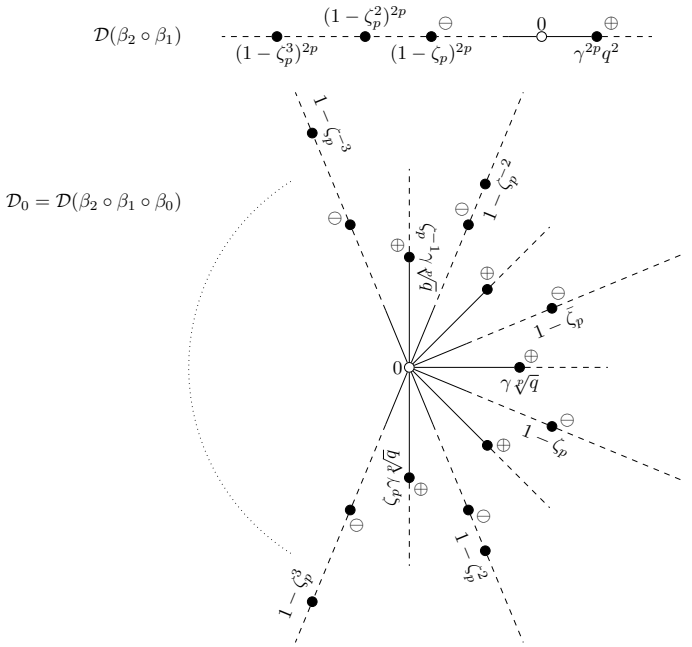
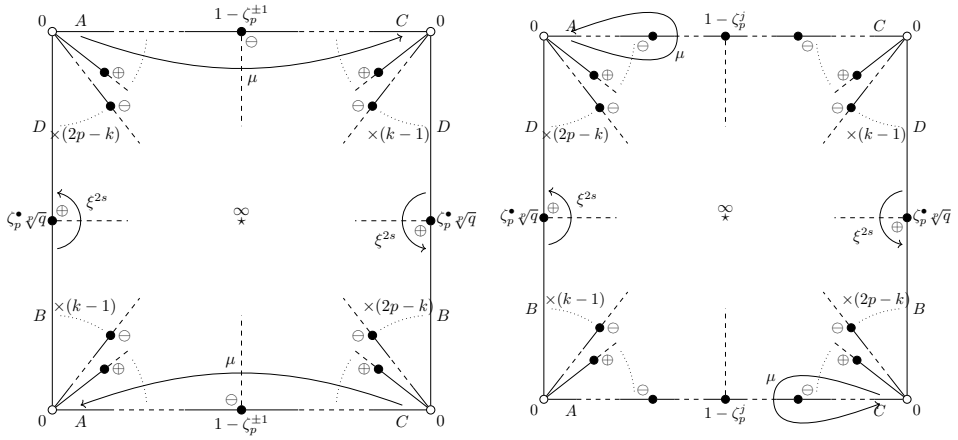


Figure 9: Dessin $\mathcal{D}_0$ corresponding to $(\mathbb{P}^1, \beta_2 \circ \beta_1 \circ \beta_0)$.

We may now draw the Galois conjugates $\mathcal{D}^\sigma$ for $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by lifting the dessin $\mathcal{D}_0$ along the projection π, by treating separately the cases $\sigma(\zeta_p) \in \{\zeta_p, \bar{\zeta_p}\}$ and $\sigma(\zeta_p) \in$

$\{\zeta_p^2, \ldots, \zeta_p^{p-2}\}$. We call the dessins respectively $\mathcal{D}_k$ and $\mathcal{D}_k^j$, see Figure 10. We identify the outermost edges on opposite sides in the representations.



(a) $\mathcal{D}_k := \mathcal{D}^\sigma$ with $\sigma(\zeta_p) = \zeta_p^{\pm 1}$.

(b) $\mathcal{D}_k^j := \mathcal{D}^\sigma$ with $\sigma(\zeta_p) = \zeta_p^j$ where $j \in \{2, \ldots, p-2\}$.

Figure 10: Dessins (a) $\mathcal{D}_k$ and (b) $\mathcal{D}_k^j$ in the Galois orbit of $\mathcal{D}$.

For all k, we have in fact $\mathcal{D}_{2k-1} = \mathcal{D}^\sigma$ where $\sigma\colon (\zeta_p, \sqrt[p]{q}) \mapsto (\zeta_p, \zeta_p^{k-1}\sqrt[p]{q})$, and $\mathcal{D}_{2k} = \mathcal{D}^\sigma$ where $\sigma\colon (\zeta_p, \sqrt[p]{q}) \mapsto (\bar{\zeta_p}, \zeta_p^k \sqrt[p]{q})$. We have similar expressions for the dessins $\mathcal{D}_k^j$.

Let k be fixed, and let us consider the dessin $\mathcal{D}_k$. Let A denote one of the two edges incident to 0 and on the path to the ramification point $1 - \zeta_p^{\pm 1}$. We also call $B := A^{\eta^{2k-1}}, C := A^{4p}, D := C^{\eta^{2k-1}}$ (See Figure 10a). Let E denote the set of edges incident to 0. The action of η induces the cyclic permutation of the edges of $E = \{A^{\eta^i}\}_{0 \le i < 8p}$. Furthermore by construction every white vertex aside from 0 has degree 1 or 2, so η^2 fixes every edge in the complement of E. We can write $E = E^\ominus \sqcup E^\oplus$ as the disjoint union of $E^\ominus := \{A^{2i}\}_{0 \le i < 4p}$ and $E^\oplus := \{B^{2i}\}_{0 \le i < 4p}$, such that η sends one to the other. The action of μ on $E^\ominus$ is the transposition (A, C), and similarly the action of ξ^{2s} on $E^\oplus$ is the transposition (B, D).

We do the same for the dessins of the form $\mathcal{D}_k^j$, with the only difference that this time the action of μ on $E^\ominus$ is trivial, including on the edges A and C (see Figure 10b).

We are almost in the same configuration as in the first example. We define analogously

$$\omega := \mu\eta\mu^{-1}\xi^{2s}\eta^{-1}\mu,$$

and we shall prove that for some choices of γ, the actions of ω and of η^2 commute only for $\mathcal{D}_1$. To reproduce the proof in the first example we need only show that for some choice of γ the actions of $\mu\eta\mu^{-1}\xi^{2s}$ and $\mu^{-1}\xi^{2s}\eta^{-1}\mu$ on the set $E^\oplus$ is the same as that of ξ^{2s}.

Note that for any edge $e \in E^\oplus$, the edge e^{ξ^i} is fixed by η if i is not a multiple of s. To that end we shall show that for some choice of γ the action of μ on $E^\oplus$ is the same as that of ξ^δ, where δ is the number of occurences of ξ in the word μ, and then that δ is not a multiple of s.

We define the words $\rho_1, \rho_1', \rho_2, \rho_2', \ldots, \rho_{2t-2}, \rho_{2t-2}' \in F_2$ to be the increasing subsequence of the prefixes ending in η of the word μ defined above, such that $\rho_1 := \xi^{mrd_1}\eta$, $\rho_1' := \rho_1\xi^s\eta$, $\rho_2 := \rho_1'\xi^{nrd_2}\eta$, $\rho_2' := \rho_2\xi^s\eta$, etc., and $\mu = \rho_{2t-2}'\xi^{mrd_1}$. We shall show by induction that for some choice of γ the action of ρ_i (resp. ρ_i') is the same as the action of ξ^{δ_i} (resp. $\xi^{\delta_i'}$), where δ_i (resp. δ_i') is the number of occurences of ξ in the word ρ_i (resp. ρ_i'). By induction it suffices to show that δ_i, δ_i' are not multiples of s. Modulo s we have $\delta_i \equiv \delta_i'$ equal to the non empty partial sum of

$$mrd_1+nrd_2+\cdots+mrd_{t-2}+nrd_{t-1}+2mrd_t+nrd_{t-1}+mrd_{t-2}+\cdots+nrd_2+mrd_1$$

consisting of the first i terms.

To proceed we shall use the following result, but let us first introduce some notations. Let $P = \sum_{i=0}^d c_i X^i \in \mathbb{Z}[X]$ and $c \in \mathbb{Z}_{>0}$ such that $\beta_1 = \frac{P}{c}$. Note that P and c do not depend on the choice of γ, and $0 < \beta_1(0) = \frac{P(0)}{c} < 1$ so $0 < c_0, c - c_0$. We define

$$\alpha := v_2(\gamma^{2p}q^2), \quad \nu := v_2(c_0) + v_2(c - c_0),$$

where v_2 denotes the 2-valuation.

Lemma 3.6. *If $\alpha > \nu$, then there exists $e \in \mathbb{Z}$ such that $em \equiv c_0 \mod 2^\alpha$ and $en \equiv c - c_0 \mod 2^\alpha$, and $v_2(s) \geq \alpha - \nu$.*

Proof. Let $a, b \in \mathbb{Z}$ coprime such that $\gamma^{2p}q^2 = \frac{a}{b}2^\alpha$.

Firstly,

$$\frac{m}{m+n} = \beta_1(\frac{a}{b}2^\alpha) = \frac{P(\frac{a}{b}2^\alpha)}{c} = \frac{\sum_{i=0}^d c_i a^i 2^{\alpha i} b^{d-i}}{b^d c},$$

so there exists $f \in \mathbb{Z}$ such that $fm = \sum_{i=0}^d c_i a^i 2^{\alpha i} b^{d-i}$ and $f(m+n) = b^d c$, so

$$em \equiv c_0 \mod 2^\alpha, \quad en \equiv c - c_0 \mod 2^\alpha$$

for $e \in \mathbb{Z}$ such that $eb^d \equiv f \mod 2^\alpha$.

Secondly,

$$\begin{aligned}\frac{r}{r+s} = B_{m,n}(\beta_1(0)) &= \frac{\beta_1(0)^m(1-\beta_1(0))^n}{\beta_1(\frac{a}{b}2^\alpha)^m(1-\beta_1(\frac{a}{b}2^\alpha))^n} \\ &= \frac{b^{d(m+n)}c_0^m(c-c_0)^n}{(b^dP(\frac{a}{b}2^\alpha))^m(b^dc - b^dP(\frac{a}{b}2^\alpha))^n},\end{aligned}$$

so there exists $g \in \mathbb{Z}$ such that $gr = b^{d(m+n)}c_0^m(c-c_0)^n$ and $g(r+s) = (b^dP(\frac{a}{b}2^\alpha))^m(b^dc - b^dP(\frac{a}{b}2^\alpha))^n$. In the expansion of $(b^dP(\frac{a}{b}2^\alpha))^m$, aside from the constant term $b^{dm}c_0^m$, every other term is a multiple of an integer of the form $c_0^i 2^{\alpha j}$ with $i \leq m-1$ and $j \geq m-i$. By hypothesis $\alpha > \nu \geq v_2(c_0)$, so those other terms are all multiples of $2^{\alpha+(m-1)v_2(c_0)}$, hence there exists $A \in \mathbb{Z}$ such that $(b^dP(\frac{a}{b}2^\alpha))^m = b^{dm}c_0^m + A2^{\alpha+(m-1)v_2(c_0)}$. Similarly there exists $B \in \mathbb{Z}$ such that $(b^dc - b^dP(\frac{a}{b}2^\alpha))^n = b^{dn}(c-c_0)^n + B2^{\alpha+(n-1)v_2(c-c_0)}$. Then $g(r+s) = b^{d(m+n)}c_0^m(c-c_0)^n + C2^{\alpha+(m-1)v_2(c_0)+(n-1)v_2(c-c_0)}$ for some $C \in \mathbb{Z}$, so $gr = b^{d(m+n)}c_0^m(c-c_0)^n$ and $gs = C2^{\alpha+(m-1)v_2(c_0)+(n-1)v_2(c-c_0)}$. The integers r and s are coprime, so after dividing gr and gs by their greatest common dividor we obtain that

$$v_2(s) \geq \alpha - \nu > 0. \qquad \square$$

Using this lemma, we know that if $\alpha > \nu$, then there exists $e \in \mathbb{Z}$ such that $em \equiv c_0 \mod 2^\alpha$ and $en \equiv c - c_0 \mod 2^\alpha$, $v_2(s) \geq \alpha - \nu$ where ν does not depend on γ, and r is coprime to s so is not a multiple of 2. Therefore there exists $e' \in \mathbb{Z}$ such that $e'mr \equiv c_0 \mod 2^\alpha$ and $e'nr \equiv c - c_0 \mod 2^\alpha$. Moreover $2^{\alpha-\nu}$ is a common divisor of 2^α and s, so by the above modulo $2^{\alpha-\nu}$ we have $e'\delta_i \equiv e'\delta_i'$ equal to the non empty partial sum $\widetilde{\delta}_i$ consisting of the first i terms of the sum

$$\begin{aligned} &c_0d_1 + (c-c_0)d_2 + \cdots + c_0d_{t-2} + (c-c_0)d_{t-1} + 2c_0d_t \\ &\quad + (c-c_0)d_{t-1} + c_0d_{t-2} + \cdots + (c-c_0)d_2 + c_0d_1. \end{aligned}$$

Similarly $e'\delta$ is equal modulo $2^{\alpha-\nu}$ to the whole sum

$$\widetilde{\delta} \coloneqq 2(c_0d_1 + (c-c_0)d_2 + \cdots + c_0d_{t-2} + (c-c_0)d_{t-1} + c_0d_t).$$

By construction $c_0, c-c_0, d_i$ are positive and do not depend on the choice of γ, so $0 < c_0d_1 \leq \widetilde{\delta}_i \leq \widetilde{\delta}$, thus for any choice of γ such that $\alpha > \nu$ and $\widetilde{\delta} < 2^{\alpha-\nu}$ (for instance $\gamma = \frac{2^u}{2^v+1}$ with $1 \ll u \ll v$), we obtain $\widetilde{\delta}_i, \widetilde{\delta} \not\equiv 0 \mod 2^{\alpha-\nu}$, and in consequence δ_i, δ_i' and δ are not multiples of s. Therefore we can now conclude by induction that the actions of ρ_i and ρ_i' are the same as that of ξ^{δ_i} and $\xi^{\delta_i'}$, respectively. Indeed, δ_1 is not a multiple of s so $\rho_1 = \xi^{\delta_1}\eta$ and ξ^{δ_1} have the same action on $E^\oplus$. If ρ_i has the same action as ξ^{δ_i} on $E^\oplus$, then $\rho_i' = \rho_i\xi^s\eta$ has the same action as $\xi^{\delta_i}\xi^s\eta = \xi^{\delta_i'}\eta$ on $E^\oplus$, and also the same action as $\xi^{\delta_i'}$ because δ_i' is not a multiple of s. Similarly, if ρ_i' has the same action as $\xi^{\delta_i'}$ on $E^\oplus$, then ρ_{i+1} has the same action as $\xi^{\delta_{i+1}}\eta$ on $E^\oplus$, and also the same action as $\xi^{\delta_{i+1}}$ because δ_{i+1} is not a multiple of s.

We have thus proved that μ has the same action as ξ^δ on $E^\oplus$, and by symmetry μ^{-1} has the same action as $\xi^{-\delta}$ on $E^\oplus$. And δ and $2s-\delta$ are not multiples of s, so $\mu\eta\mu^{-1}\xi^{2s}$ and $\mu^{-1}\xi^{2s}\eta^{-1}\mu$ have the same action as ξ^{2s} on $E^\oplus$, as announced. We shall now observe the action of $\omega = \mu\eta\mu^{-1}\xi^{2s}\eta^{-1}\mu$ on E. Let M_k and M_k^j denote the monodromy maps of the dessins $\mathcal{D}_k$ and $\mathcal{D}_k^j$.

For the dessins $\mathcal{D}_k$ for $1 \leq k \leq 2p$, the action of μ on $E^\ominus$ is the transposition (A, C), and the action of ξ^{2s} on $E^\oplus$ is the transposition (B, D), therefore the action of ω fixes the set E on which it induces the permutation

$$M_k(\omega)|_E = (A,C)(B,D) \cdot \prod_{i=0}^{4p-1} (A^{\eta^{2i}}, A^{\eta^{2i+1}}) \cdot (A,C)(B,D).$$

Hence for $k = 1$,

$$\begin{aligned} M_1(\omega)|_E &= (A, A^{\eta^{4p}})(A^\eta, A^{\eta^{4p+1}}) \cdot \prod_{i=0}^{4p-1} (A^{\eta^{2i}}, A^{\eta^{2i+1}}) \cdot (A, A^{\eta^{4p}})(A^\eta, A^{\eta^{4p+1}}) \\ &= \prod_{i=0}^{4p-1} (A^{\eta^{2i}}, A^{\eta^{2i+1}}) \end{aligned}$$

so ω and η^2 commute on E. Moreover η^2 acts trivially on the complement of E, so finally $M_1(\omega)$ and $M_1(\eta^2)$ commute.

For $k = 2$, we observe that $B^{\omega\eta^2} = D^{\eta^{-1}\eta^2} = D^{\eta}$ but $B^{\eta^2\omega} = B^{\eta^2\eta^{-1}} = B^{\eta}$. Similarly, for $3 \leq k \leq 2p$, we observe that $A^{\omega\eta^2} = C^{\eta\eta^2} = C^{\eta^3}$ but $A^{\eta^2\omega} = A^{\eta^2\eta} = A^{\eta^3}$. Therefore $M_k(\omega)$ and $M_k(\eta^2)$ do not commute for $2 \leq k \leq 2p$.

For the dessins $\mathcal{D}_k^j$ for $1 \leq k \leq 2p$ and $2 \leq j \leq \frac{p-1}{2}$, ξ^{2s} on $E^{\oplus}$ is the transposition (B, D), and μ acts trivially on $E^{\ominus}$, therefore the action of ω fixes the set E on which it induces the permutation

$$M_k^j(\omega)|_E = (B, D) \cdot \prod_{i=0}^{4p-1} (A^{\eta^{2i}}, A^{\eta^{2i+1}}) \cdot (B, D).$$

Hence we observe that $B^{\omega\eta^2} = D^{\eta^{-1}\eta^2} = D^{\eta}$ but $B^{\eta^2\omega} = B^{\eta^2\eta^{-1}} = B^{\eta}$, so $M_k^j(\omega)$ and $M_k^j(\eta^2)$ do not commute.

We have thus shown that the actions of ω and η^2 commute only for $\mathcal{D}_1$, this concludes the proof that $\widetilde{\mathcal{D}}$ is a regular dessin with moduli field $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$.

3.3 Regular dessin with moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$

Finally, let us exhibit a regular dessin with moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$ of smaller degree by choosing a Belyi map that is a rational function instead of a polynomial as was done in the previous subsections. Let

$$C\colon y^2 = x(x - (1 - \zeta_3))(x - \sqrt[3]{3}),$$
$$\beta\colon C \to \mathbb{P}^1, (x, y) \mapsto \frac{(x + 3^3)^3}{3^5(x - 3^2)^2}.$$

The function β is given by the composition of the following maps $\beta = \beta_1 \circ \beta_0 \circ \pi$.

1. $\pi\colon C \to \mathbb{P}^1$ is the projection on the coordinate x, which ramifies over $\{0, 1 - \zeta_3, \sqrt[3]{3}, \infty\}$.
2. $\beta_0 := X^6 \in \mathbb{Q}[X]$, $\mathrm{Crit}(\beta_0) = \{0\}$ so $\beta_0 \circ \pi$ ramifies over $\{0, (1 - \zeta_3)^6 = -3^3, 3^2, \infty\}$.
3. $\beta_1 := \frac{(X+3^3)^3}{3^5(X-3^2)^2}$, $\mathrm{Crit}(\beta_1) = \{0, 1\}$ so $\beta = \beta_1 \circ \beta_0 \circ \pi$ ramifies over $\{0, 1, \infty\}$.

The pair (C, β) is thus a Belyi pair, and we call $\mathcal{D}$ the dessin corresponding to (C, β). Similarly as in 3.1, $\mathcal{D}$ has moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$. We will proceed analogously to show that the regular closure $\widetilde{\mathcal{D}}$ has the same field of moduli. Let us first draw the dessin $\mathcal{D}_0$ corresponding to the Belyi pair $(\mathbb{P}^1, \beta_1 \circ \beta_0)$ (see Figure 11), and lift it to the conjugate curves C^σ to obtain the conjugate dessins $\mathcal{D}^\sigma$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{3})/\mathbb{Q})$ (see Figure 12).

As usual we identify the outermost edges on opposite sides.

We can now compute the cartographic groups of the dessins. Let M_k denote the monodromy map of $\mathcal{D}_k$. Then

$$M_k(\xi) = \begin{matrix}(1,13,14,7,25,26)(2,15,16)(3,17,18)(4,19,20)(5,21,22)\\(6,23,24)(8,27,28)(9,29,30)(10,31,32)(11,33,34)(12,35,36)\end{matrix}$$

for all $1 \leq k \leq 6$, and

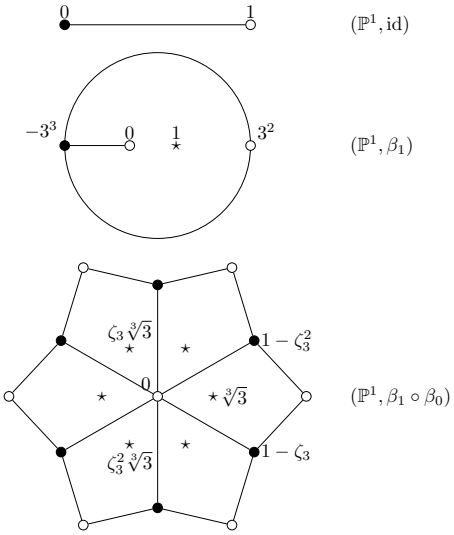
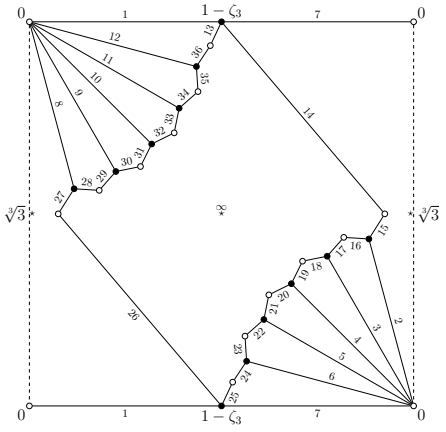
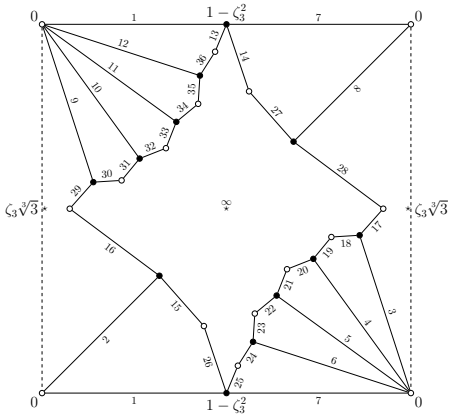


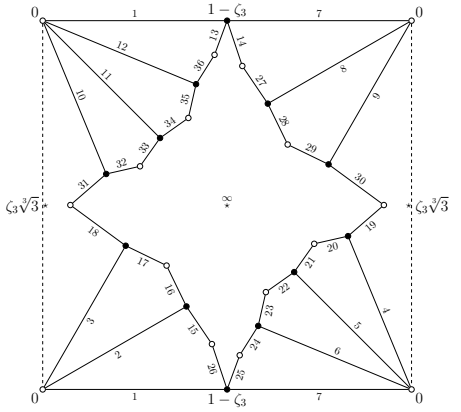
Figure 11: Construction of $\mathcal{D}_0$.



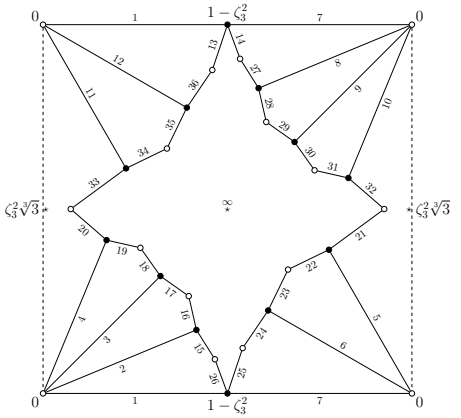
(a) $\mathcal{D}_1 \coloneqq \mathcal{D}$



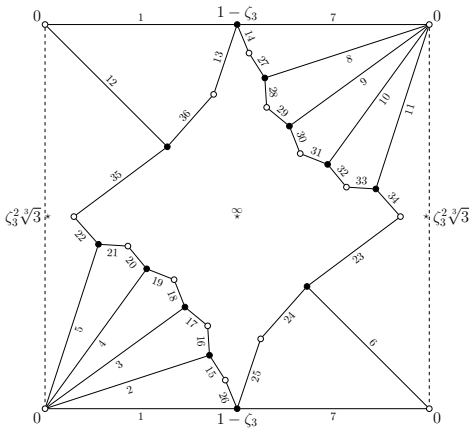
(b) $\mathcal{D}_2 \coloneqq \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3^2, \zeta_3\sqrt[3]{q})$



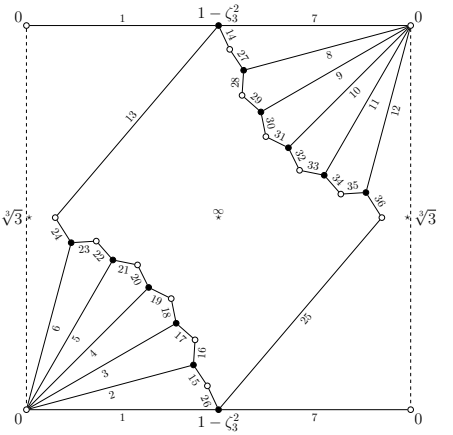
(c) $\mathcal{D}_3 := \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3, \zeta_3\sqrt[3]{q})$



(d) $\mathcal{D}_4 := \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3^2, \zeta_3^2\sqrt[3]{q})$



(e) $\mathcal{D}_5 := \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3, \zeta_3^2\sqrt[3]{q})$



(f) $\mathcal{D}_6 := \mathcal{D}^\sigma, \sigma\colon (\zeta_3, \sqrt[3]{q}) \mapsto (\zeta_3^2, \sqrt[3]{q})$

Figure 12: Dessins $\mathcal{D}_1, \ldots, \mathcal{D}_6$ in the Galois orbit of $\mathcal{D}$.

- $M_1(\eta) = \begin{matrix}(1,2,3,4,5,6,7,8,9,10,11,12)(13,36)(14,15)(16,17)(18,19)\\(20,21)(22,23)(24,25)(26,27)(28,29)(30,31)(32,33)(34,35)\end{matrix}$,
- $M_2(\eta) = \begin{matrix}(1,2,3,4,5,6,7,8,9,10,11,12)(13,36)(14,27)(15,26)(16,29)\\(17,28)(18,19)(20,21)(22,23)(24,25)(30,31)(32,33)(34,35)\end{matrix}$,
- $M_3(\eta) = \begin{matrix}(1,2,3,4,5,6,7,8,9,10,11,12)(13,36)(14,27)(15,26)(16,17)\\(18,31)(19,30)(20,21)(22,23)(24,25)(28,29)(32,33)(34,35)\end{matrix}$,
- $M_4(\eta) = \begin{matrix}(1,2,3,4,5,6,7,8,9,10,11,12)(13,36)(14,27)(15,26)(16,17)\\(18,19)(20,33)(21,32)(22,23)(24,25)(28,29)(30,31)(34,35)\end{matrix}$,
- $M_5(\eta) = \begin{matrix}(1,2,3,4,5,6,7,8,9,10,11,12)(13,36)(14,27)(15,26)(16,17)\\(18,19)(20,21)(22,35)(23,34)(24,25)(28,29)(30,31)(32,33)\end{matrix}$,
- $M_6(\eta) = \begin{matrix}(1,2,3,4,5,6,7,8,9,10,11,12)(13,24)(14,27)(15,26)(16,17)\\(18,19)(20,21)(22,23)(25,36)(28,29)(30,31)(32,33)(34,35)\end{matrix}$.

Using the computer algebra system SageMath [10], we determined that

$$|\langle M_1(\xi), M_1(\eta)\rangle| = 42467328 = 2^{19} \cdot 3^4.$$

Moreover, $M_1(\xi)$, $M_1(\eta)$ and $M_1(\xi\eta)$ respectively have orders 6, 12 and 12, so the Euler characteristic of the underlying surface of $\widetilde{\mathcal{D}_1}$ is

$$\begin{aligned}\chi &= |\langle M_1(\xi), M_1(\eta)\rangle| \cdot \left(\frac{1}{\operatorname{ord} M_1(\xi)} + \frac{1}{\operatorname{ord} M_1(\eta)} + \frac{1}{\operatorname{ord} M_1(\xi\eta)} - 1\right)\\ &= -28311552 = -2^{20} \cdot 3^3,\end{aligned}$$

and its genus is $g = 1 - \frac{\chi}{2} = 14155777$.

We will now show that $\widetilde{\mathcal{D}_1}$ is not isomorphic to $\widetilde{\mathcal{D}_2}, \ldots, \widetilde{\mathcal{D}_6}$. We claim that $\omega := [\xi^{-1}\eta^2\xi, \xi\eta] \in \ker M_1 \setminus \bigcup_{2\le k\le 6} \ker M_k$, thus concluding the proof. Indeed, we obtain:

- $M_1(\omega) = \mathrm{id}$;
- $M_2(\omega) = (13,25)(15,27)(21,33)(23,35)$;
- $M_3(\omega) = (17,29)(21,33)$;
- $M_4(\omega) = (13,25)(15,27)(19,31)(21,33)$;
- $M_5(\omega) = (13,25)(17,29)$;
- $M_6(\omega) = (13,25)(19,31)(21,33)(23,35)$.

We have thus constructed a regular dessin $\widetilde{\mathcal{D}}$ of degree $2^{19} \cdot 3^4$ and genus 14155777 with moduli field $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$.

ORCID iDs

Fumiharu Kato https://orcid.org/0009-0002-4800-0029

References

[1] M. D. E. Conder, G. A. Jones, M. Streit and J. Wolfart, Galois actions on regular dessins of small genera, *Rev. Mat. Iberoam.* **29** (2013), 163–181, doi:10.4171/rmi/717, https://doi.org/10.4171/rmi/717.

[2] E. Girondo and G. González-Diez, *Introduction to compact Riemann surfaces and dessins d'enfants*, volume 79 of *London Mathematical Society Student Texts*, Cambridge University Press, Cambridge, 2012.

[3] G. González-Diez and A. Jaikin-Zapirain, The absolute Galois group acts faithfully on regular dessins and on Beauville surfaces, *Proc. Lond. Math. Soc. (3)* **111** (2015), 775–796, doi:10.1112/plms/pdv041, https://doi.org/10.1112/plms/pdv041.

[4] A. Grothendieck, Esquisse d'un programme, in: *Geometric Galois actions, 1*, Cambridge Univ. Press, Cambridge, volume 242 of *London Math. Soc. Lecture Note Ser.*, pp. 5–48, 1997, with an English translation on pp. 243–283.

[5] P. Guillot, An elementary approach to dessins d'enfants and the Grothendieck-Teichmüller group, *Enseign. Math.* **60** (2014), 293–375, doi:10.4171/lem/60-3/4-5, https://doi.org/10.4171/lem/60-3/4-5.

[6] M. Herradón Cueto, An explicit quasiplatonic curve with non-abelian moduli field, *Rev. Mat. Complut.* **29** (2016), 725–739, doi:10.1007/s13163-016-0196-z, https://doi.org/10.1007/s13163-016-0196-z.

[7] R. A. Hidalgo and S. Quispe, Regular dessins d'enfants with field of moduli $\mathbb{Q}(\sqrt[p]{2})$, *Ars Math. Contemp.* **13** (2017), 323–330, doi:10.26493/1855-3974.1202.9c1, https://doi.org/10.26493/1855-3974.1202.9c1.

[8] G. A. Jones and J. Wolfart, *Dessins d'enfants on Riemann surfaces*, Springer Monographs in Mathematics, Springer, Cham, 2016, doi:10.1007/978-3-319-24711-3, https://doi.org/10.1007/978-3-319-24711-3.

[9] S. K. Lando and A. K. Zvonkin, *Graphs on surfaces and their applications*, volume 141 of *Encyclopaedia of Mathematical Sciences*, Springer-Verlag, Berlin, 2004, doi:10.1007/978-3-540-38361-1, with an appendix by Don B. Zagier, Low-Dimensional Topology, II, https://doi.org/10.1007/978-3-540-38361-1.

[10] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020-01-01, https://www.sagemath.org.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 24 (2024) #P2.06 / 293–315
https://doi.org/10.26493/1855-3974.2619.06c
(Also available at http://amc-journal.eu)

Generalized X-join of graphs and their automorphisms*

Javad Bagherian †, Hanieh Memarzadeh

Department of Pure Mathematics, Faculty of Mathematics and Statistics, University of Isfahan, P.O. Box: 81746-73441, Isfahan, Iran

Received 4 May 2021, accepted 6 April 2023, published online 27 September 2023

Abstract

In this paper, we first introduce a new product of finite graphs as a generalization of the X-join of graphs. We then give necessary and sufficient conditions for a graph to be isomorphic to a generalized X-join. As a main result, we give necessary and sufficient conditions under which the full automorphism group of a generalized X-join is equal to the generalized wreath product of the automorphism groups of its factors.

Keywords: Automorphism, generalized wreath product, graph, lexicographic product, permutation group, X-join.

Math. Subj. Class. (2020): 05C25, 20B25, 20E22

1 Introduction

One of the main problems in the theory of graphs, known as the König problem, asks for a concrete characterization of all automorphism groups of graphs. In particular, the problem of computing a generating set of the automorphism group is equivalent to the graph isomorphism problem [9]. The automorphism groups of many graphs can be expressed in terms of the automorphism groups of their subgraphs. For instance, in most cases the automorphism groups of the graphs which are the lexicographic product of graphs are expressed in terms of the automorphism groups of their factors. The lexicographic product of graphs is one of the important products of graphs, defined by Harary in [7]. Sabidussi in [11] showed that under some conditions the automorphism group of the lexicographic product of two graphs

*The authors are grateful to the anonymous referees, whose comprehensive reports helped to improve the quality of this paper.

†Corresponding author.
E-mail addresses: bagherian@sci.ui.ac.ir (Javad Bagherian), h.memarzadeh.762@sci.ui.ac.ir (Hanieh Memarzadeh)

Γ and Γ' can be expressed as the wreath product of the automorphism groups of Γ and Γ'. An important generalization of the lexicographic product is the X-join. It was introduced by Sabidussi as the graph formed from a given graph $\Gamma = (V, R)$ by replacing every vertex v of Γ by a graph B_v and joining the vertices of B_v with those of B_u whenever $uv \in R$ [11]. Note that the graphs B_v, $v \in V$, need not be mutually isomorphic. Hemminger in [8] gave necessary and sufficient conditions for the automorphism group of the X-join of graphs $\{B_v\}_{v\in V}$ to be the natural ones, i.e., those that are obtained by first permuting the graphs B_v, $v \in V$, according to a permutation of subscripts by an automorphism of Γ and then performing an arbitrary automorphism of each B_v. Note that Hemminger did not determine the structure of the automorphism group of the X-join of $\{B_v\}_{v\in V}$ in terms of automorphism groups of B_v, $v \in V$. It should be mentioned that the above results have been generalized to directed color graphs in [3]. If for a color digraph $C = (V, R)$ and a collection of color digraphs $\{D_c \mid c \in V\}$, each vertex c of C is replaced by a copy of D_c and all possible arcs of color k from D_c to $D_{c'}$ are included, if and only if there is an arc of color k from c to c' in C, we get the C-join of these color digraphs. The wreath product of two color digraphs C and D is the C-join of $\{D_c \mid c \in V\}$ where $D_c \cong D$ for every $c \in V$. In [3], all automorphism groups of digraphs that can be written as a wreath product have been determined.

In this paper we first give a generalization of the X-join of graphs (see Definition 2.1). This generalization, as a new operation on finite graphs, is a natural generalization of the X-join of graphs (a more algebraic way was considered by Weisfeiler [12, page 45] as the wreath product of a family of stable graphs with another stable graph). Also this new graph product generalizes the generalized wreath product of circulant digraph which defined in [2] (see Remark 2.9). It is also closely related with the wedge product of association schemes introduced and studied in [10] (see Remark 2.8). In Section 2 we give necessary and sufficient conditions under which a graph is isomorphic to a generalized X-join (see Theorem 2.4). But the main result of this paper deals with the connections between the automorphism group of a generalized X-join and the automorphism groups of its factors. For computing the automorphism group of the generalized X-join of graphs, we need a generalization of the wreath product of permutation groups. Recently, such a generalization, called the generalized wreath product, has been given in [1, 5]. We first show that under some conditions the automorphism group of the generalized X-join of graphs contains the generalized wreath product of the automorphism groups of their factors (Theorem 4.1). As a main result, we then give necessary and sufficient conditions under which the full automorphism group of the generalized X-join of graphs is equal to the generalized wreath product of the automorphism groups of their factors (Theorem 4.2). In particular, we determine the structure of the natural automorphism group of the X-join of graphs (Corollary 4.7).

Terminology and notation: Throughout this paper, by a graph $\Gamma = (V, R)$ we mean a finite undirected graph without multiple edges with the vertex set $V = V(\Gamma)$ and the edge set $R = E(\Gamma)$. We denote the complement of Γ by $\overline{\Gamma}$. If all pairs of vertices of a subgraph Γ' of Γ that are adjacent in Γ are also adjacent in Γ', then Γ' is an induced subgraph. For $X \subseteq V$ we write $\Gamma[X]$ for the subgraph of Γ induced by X and we also denote by $\Gamma(X)$ the graph with vertices X and edge set $E(\Gamma[X]) \cup \{(x, x) \mid x \in X\}$. For two graphs $\Gamma = (V, R)$ and $\Gamma' = (V', R')$, by a graph homomorphism $f\colon \Gamma \to \Gamma'$ we mean a mapping $f\colon V \to V'$ such that $(f(u), f(v)) \in R'$ whenever $(u, v) \in R$. In the case when $f\colon V \to V'$ is surjective, $f\colon \Gamma \to \Gamma'$ is called a graph epimorphism. More-

over, if $f\colon V \to V'$ is a bijection and $f^{-1}\colon \Gamma' \to \Gamma$ is also a graph homomorphism, then $f\colon \Gamma \to \Gamma'$ is called a graph isomorphism. Two graphs Γ and Γ' are called isomorphic if there exists a graph isomorphism between Γ and Γ'. In this case we write $\Gamma \simeq \Gamma'$. When $\Gamma = \Gamma'$ every graph isomorphism $f\colon \Gamma \to \Gamma$ is called a graph automorphism of Γ. The set of all graph automorphisms of Γ is denoted by $\mathrm{Aut}(\Gamma)$ and is called the automorphism group of Γ.

If Π is a partition of the vertices of a graph Γ, then the quotient graph Γ/Π is a graph with vertex set Π, for which distinct classes $X, X' \in \Pi$ are adjacent if some vertex in X is adjacent to a vertex of X'.

Let $\Gamma = (V, R)$ be a graph. The X-join of a set of graphs $\{B_x = (Y_x, E_x) \mid x \in V\}$ with Γ, denoted by $\Gamma[B_x]_{x\in V}$, is a graph $W = (Y, E)$ where $Y = \dot{\bigcup}_{x\in V} Y_x$ and

$$E = \{(y_x, y'_{x'}) \in Y_x \times Y_{x'} \mid (x, x') \in R, \text{or else } x = x' \text{ and } (y_x, y'_x) \in E_x\}.$$

If $B = (Y', E')$ and $B_x = B$ for every $x \in V$, we can identify $\dot{\bigcup}_{x\in V} Y_x$ with $Y' \times V$ and then the X-join of $\{B_x = (Y_x, E_x) \mid x \in V\}$ is the lexicographic product of Γ and B and is denoted by $\Gamma \circ B$.

We denote by K_n a complete graph with n vertices. For the graph theoretical terminology and notation that are not defined here, we refer the reader to [6].

For a finite set V, we denote by $\mathrm{Sym}(V)$ the group of all permutations of V. Every subgroup of $\mathrm{Sym}(V)$ is called a permutation group on V. For $F \leq \mathrm{Sym}(V)$ and $\Delta \subseteq V$, the setwise stabilizer of Δ in F is $F_{\{\Delta\}} = \{f \in F \mid \Delta^f = \Delta\}$ and the pointwise stabilizer of Δ in F is $F_{(\Delta)} = \{f \in F \mid \ x^f = x, \ \ \forall x \in \Delta\}$. We say that two permutation groups $F \leq \mathrm{Sym}(V)$ and $F' \leq \mathrm{Sym}(V')$ are permutation isomorphic if there exist a bijection $\lambda\colon V \to V'$ and a group isomorphism $\eta\colon F \to F'$ such that for every $f \in F$ and $v \in V$ we have $\lambda(v^f) = \lambda(v)^{\eta(f)}$.

By a system of blocks Π for a permutation group $F \leq \mathrm{Sym}(\Omega)$ we mean

(1) Π is a partition of Ω;

(2) for every $\Delta \in \Pi$ and every $f \in F$, $\Delta^f \cap \Delta = \varnothing$ or $\Delta^f = \Delta$.

If Π is a system of blocks for F and $\Delta \in \Pi$, by F^Δ we mean the group induced by the action of $F_{\{\Delta\}}$ on Δ. Then $F^\Delta/F_{(\Delta)} \leq \mathrm{Sym}(\Delta)$ is a permutation group.

2 A generalization of the X-join of graphs

In this section we first introduce a new product of graphs, called the generalized X-join of graphs. Then we give necessary and sufficient conditions under which a graph is isomorphic to a generalized X-join.

Definition 2.1. Let $\Gamma = (V, R)$ be a graph and Π be a partition of V. Suppose that for every $X \in \Pi$ we are given a graph $B_X = (Y_X, E_X)$ and a graph epimorphism $\pi_X\colon Y_X \to X$ from B_X onto $\Gamma(X)$. Put $Y = \dot{\bigcup}_{X\in\Pi} Y_X$ and $\pi = \dot{\bigcup}_{X\in\Pi} \pi_X$ where for every $y \in Y_X$, $\pi(y) := \pi_X(y)$. We define a graph W with vertex set Y and edge set E such that $(y, y') \in E$ if and only if

(1) either $(y, y') \in E_X$, for some $X \in \Pi$;

(2) or $(y, y') \in \pi_X^{-1}(x) \times \pi_{X'}^{-1}(x')$ where $X \neq X'$ and $(x, x') \in R$.

We call the graph $W = (Y, E)$ the *generalized X-join* of Γ and $\{B_X\}_{X\in\Pi}$ with respect to π, and we denote it by $\Gamma \circ_\pi \{B_X\}_{X\in\Pi}$. (See Figure 1.)

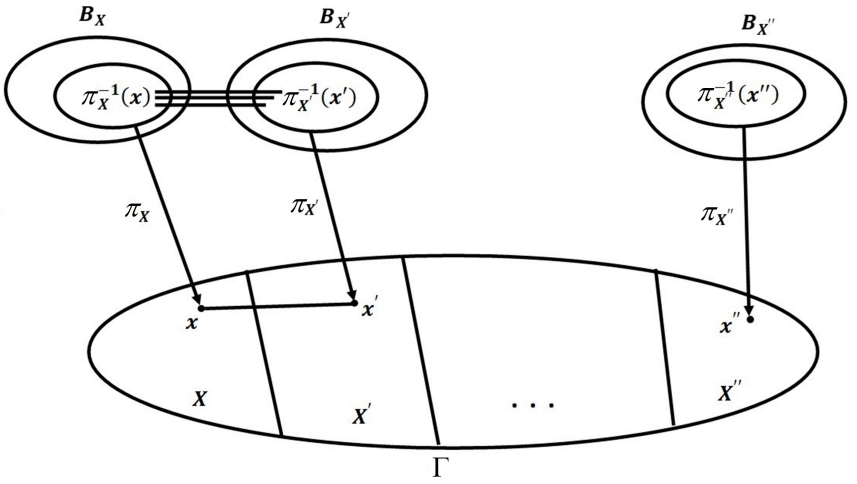


Figure 1: The generalized X-join of Γ and $\{B_X\}_{X\in\Pi}$.

In the following we show that the X-join of graphs is a special case of the generalized X-join of graphs.

Example 2.2. Let $\Gamma = (V, R)$ be a graph and Π be a partition of V such that for every $X \in \Pi$, $X = \{x\}$ for some $x \in V$. Suppose that $\{B_x = (Y_x, E_x) \mid x \in V\}$ is a set of graphs. Define a graph epimorphism $\pi_x \colon Y_x \to X$ from B_x onto $\Gamma(X)$ such that $\pi_x(y_x) = x$ for every $y_x \in Y_x$. Then the generalized X-join of Γ and $\{B_x\}_{x\in\Pi}$ with respect to $\pi = \dot{\bigcup}_{x\in V}\pi_x$ is a graph with vertices $Y = \dot{\bigcup}_{x\in V}Y_x$ and the edge set E such that $(y_x, y'_{x'}) \in E$ if and only if

(1) either $x = x'$ and $(y_x, y'_x) \in E_x$;

(2) or $x \neq x'$ and $(x, x') \in R$.

One can see that in this case $\Gamma \circ_\pi \{B_x\}_{x\in V} = \Gamma[B_x]_{x\in V}$, the X-join of graphs $\{B_x\}_{x\in V}$.

Example 2.3. Let $\Gamma = (V, R)$ be the graph in Figure 2. Consider the partition $\Pi = \{X, X', X''\}$ of V where $X = \{1, 2\}, X' = \{3, 4\}$, and $X'' = \{5, 6\}$. Suppose that $B_X = (Y_X, E_X)$, $B_{X'} = (Y_{X'}, E_{X'})$, and $B_{X''} = (Y_{X''}, E_{X''})$ are the graphs in Figure 2 with vertices $Y_X = \{a, b, c\}$, $Y_{X'} = \{d, e, f\}$, and $Y_{X''} = \{g, h, i, k\}$, respectively.

Now define the graph epimorphisms $\pi_X \colon B_X \to \Gamma(X)$, $\pi_{X'} \colon B_{X'} \to \Gamma(X')$, and $\pi_{X''} \colon B_{X''} \to \Gamma(X'')$ as follows:

$$\begin{cases} \pi_X(a) = \pi_X(b) = 1 \\ \pi_X(c) = 2 \end{cases}$$

$$\begin{cases} \pi_{X'}(e) = \pi_{X'}(d) = 3 \\ \pi_{X'}(f) = 4 \end{cases}$$

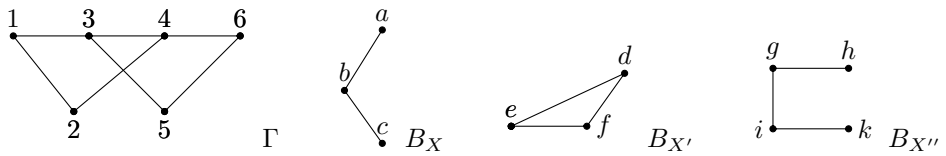


Figure 2: Graph Γ and set of graphs $\{B_X\}_{X\in\Pi}$.

$$\begin{cases}\pi_{X''}(g)=\pi_{X''}(h)=5\\ \pi_{X''}(i)=\pi_{X''}(k)=6.\end{cases}$$

Then the generalized X-join of Γ and $\{B_X, B_{X'}, B_{X''}\}$ with respect to π is the graph in Figure 3.

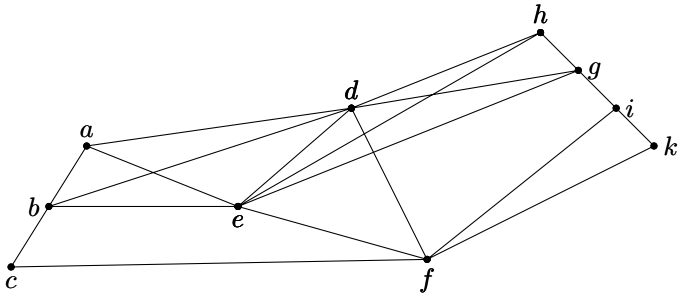


Figure 3: Graph $W = \Gamma \circ_\pi \{B_X, B_{X'}, B_{X''}\}$.

Let $\Gamma = (V, R)$ be a graph and let $A, B \subseteq V$. We say that A is *externally related* with respect to B, if every vertex $v \in B$ that is adjacent to at least one element in A is adjacent to all vertices of A. Moreover, if B is also externally related with respect to A, we say that A and B are *externally related to each other*.

Suppose that $W = (Y, E)$ is the generalized X-join of $\Gamma = (V, R)$ and $\{B_X = (Y_X, E_X) \mid X \in \Pi\}$ with respect to π. Then we can define two equivalence relations E_0 and E_1 on Y as follows:

$$(u,v)\in E_0 \quad\Leftrightarrow\quad u,v\in \pi_X^{-1}(x),\quad \text{for some } X\in\Pi \text{ and } x\in X; \tag{2.1}$$

$$(u,v)\in E_1 \quad\Leftrightarrow\quad u,v\in Y_X,\ \text{for some } X\in\Pi. \tag{2.2}$$

Clearly, $E_0 \subseteq E_1$. In the following we give a characterization of the generalized X-join of graphs in terms of the equivalence relations E_0 and E_1.

Theorem 2.4. *A graph $W = (Y, E)$ is a generalized X-join of graphs if and only if there exist two equivalence relations E_0 and E_1 on Y such that*

(i) $E_0 \subseteq E_1$;

(ii) *for every equivalence class P of E_0 which is contained in a equivalence class Q of E_1, P is externally related with respect to every equivalence class of E_0 which is not in Q.*

Proof. Suppose that $W = (Y, E)$ is the generalized X-join of Γ and $\{B_X\}_{X\in\Pi}$ with respect to π. Then as we saw above, there are two equivalence relations E_0 and E_1 on Y such that $E_0 \subseteq E_1$. Since for every $x \in X$ and $x' \in X'$ where $X \neq X'$, $\pi_X^{-1}(x)$ and $\pi_{X'}^{-1}(x')$ are externally related to each other, it follows that condition (ii) holds.

Now suppose that there exist two equivalence relations E_0 and E_1 on Y such that conditions (i) and (ii) hold. Let Y/E_0 and Y/E_1 be the sets of the equivalence classes of E_0 and E_1 on Y, respectively. Let Γ be the quotient graph W/E_0. Moreover, for every $U \in Y/E_1$, let U_0 be the equivalence classes of E_0 which are contained in U and B_{U_0} be the subgraph of W induced by U. Since $E_0 \subseteq E_1$, $\{U_0 \mid U \in Y/E_1\}$ gives a partition Π on Y/E_0. Then for every $U \in Y/E_1$ we can define a graph epimorphism π_{U_0} from the graph B_{U_0} onto $\Gamma(U_0)$. Suppose that W' is the generalized X-join of Γ and $\{B_{U_0}\}_{U_0\in\Pi}$ with respect to π. Then $V(W') = Y$ and it follows from condition (ii) that the set of edges of W and W' are the same. Thus $W = W'$ and so W is a generalized X-join of graphs. □

Remark 2.5. The following example shows that unlike the X-join of graphs, a graph can be represented as a generalized X-join of graphs, but not a unique way. This means that if W and W' are two isomorphic generalized X-join of graphs then it is not necessarily true that the factors of W and W' are isomorphic.

Example 2.6. Consider the graph $W = (Y, E)$ in Figure 4. If we consider two equivalence relations $E_0 \subseteq E_1$ such that $Y/E_0 = \{\{a\}, \{b, c\}, \{d, e, f, g\}, \{h\}\}$ and $Y/E_1 = \{\{a, b, c\}, \{d, e, f, g, h\}\}$, then one can see that conditions (i) and (ii) of Theorem 2.4 hold. So it follows from Theorem 2.4 that $W = \Gamma \circ_\pi \{B_X, B_{X'}\}$ where the graphs Γ, B_X and $B_{X'}$ are shown in Figure 5. On the other hand, consider the graphs Γ', B'_X and $B'_{X'}$ that are shown in Figure 6. Set $\Pi' = \{X = \{1, 2, 3\}, X' = \{4, 5\}\}$ and define the graph epimorphisms $\pi'_X \colon B'_X \to \Gamma'(X)$ by

$$\begin{cases} a \longrightarrow 1 \\ b, c \longrightarrow 2 \\ h \longrightarrow 3 \end{cases}$$

and $\pi'_{X'} \colon B'_{X'} \to \Gamma'(X')$ by

$$\begin{cases} d, e \longrightarrow 4 \\ f, g \longrightarrow 5 \end{cases}.$$

Then one can see that W is the generalized X-join $\Gamma' \circ_{\pi'} \{B'_X, B'_{X'}\}$ with respect to π'.

The following lemma that gives a sufficient condition under which two generalized X-join are isomorphic, is straightforward and therefore left to the reader.

Lemma 2.7. *Let $W = \Gamma \circ_\pi \{B_X\}_{X\in\Pi}$ and $W' = \Gamma' \circ_{\pi'} \{B_{X'}\}_{X'\in\Pi'}$. Suppose that the following conditions hold.*

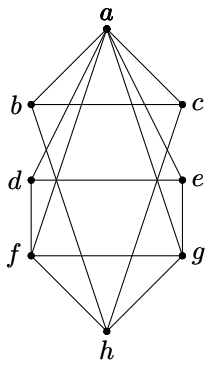


Figure 4: Graph W.

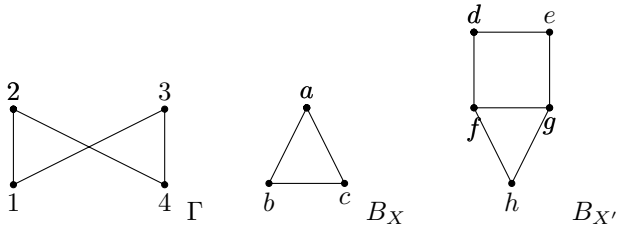


Figure 5: Graph Γ and set of graphs $\{B_X, B_{X'}\}$.

(1) *There exists a graph isomorphism* $\alpha\colon \Gamma \to \Gamma'$ *which maps every partition class* $X \in \Pi$ *onto a partition class* $X' \in \Pi'$*;*

(2) *For every* $X \in \Pi$*, there exist graph isomorphisms* $\beta_{XX'}\colon B_X \to B_{X'}$ *with* $X' = X^{\alpha}$ *such that the following diagram is commutative.*

$$\begin{array}{ccc} Y_X & \xrightarrow{\beta_{XX'}} & Y_{X'} \\ {\scriptstyle \pi_X}\downarrow & & \downarrow{\scriptstyle \pi_{X'}} \\ X & \xrightarrow{\alpha} & X' \end{array}$$

Then $\psi\colon \dot{\bigcup}_{X\in\Pi} Y_X \to \dot{\bigcup}_{X'\in\Pi'} Y_{X'}$ *defined by* $y_X \to \beta_{XX'}(y_X)$ *is a graph isomorphism between* W *and* W'*.*

Remark 2.8. The generalized X-join is closely related with the wedge product of association schemes. The wedge product of association schemes which provides a way to construct new association schemes from old ones has been given in [10]. In the following we give the relationship between the relations of a wedge product of symmetric association schemes and the generalized X-join.

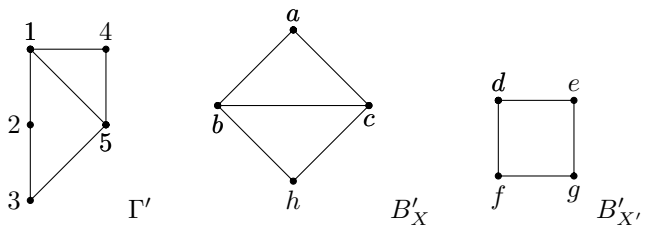


Figure 6: Graph Γ' and set of graphs $\{B'_X, B'_{X'}\}$.

Suppose (V, G) is an association scheme and E is an equivalence relation on V such that it is a union of some relations $R_0, R_1, \ldots, R_t$ of G. Put $D = \{R_0, R_1, \ldots, R_t\}$ and suppose Σ is the set of equivalence classes of E. For every $X \in \Sigma$, let $D_X = \{g_X \mid g \in D\}$ where $g_X = g \cap X \times X$. Moreover, assume that

(1) there is a set of association schemes $\{(Y_X, B_X) \mid X \in \Sigma\}$ such that all Y_X are pairwise disjoint and for every $X \in \Sigma$ there exists a scheme normal epimorphism $\pi_X \colon Y_X \cup B_X \to X \cup D_X$.

(2) for every $X, X' \in \Sigma$, there exists an algebraic isomorphism $\varphi_{XX'} \colon B_X \to B_{X'}$ such that the diagram

$$\begin{array}{ccc} B_X & \xrightarrow{\varphi_{XX'}} & B_{X'} \\ {\scriptstyle \pi_X}\downarrow & & \downarrow{\scriptstyle \pi_{X'}} \\ D_X & \xrightarrow{\varepsilon_{XX'}} & D_{X'} \end{array}$$

is commutative, where $\varepsilon_{XX'}(g_X) = g_{X'}$.

Put $Y := \dot{\bigcup}_{X\in\Sigma} Y_X$, $\pi := \dot{\bigcup}_{X\in\Sigma} \pi_X$ and for every $b \in B_X$, $\widetilde{b} = \bigcup_{X'\in\Sigma} \varphi_{XX'}(b_X)$. Moreover, for every $g \in G$ put

$$\overline{g} = \bigcup_{\substack{(x,x')\in g\cap X\times X',\\ X,X'\in\Sigma, X\neq X'}} \psi_X^{-1}(x) \times \psi_{X'}^{-1}(x').$$

Fix $Z \in \Sigma$. Put $\widetilde{B_Z} = \{\widetilde{b} \mid b \in B_Z\}$. Then it follows from [10, Theorem 2.2] that the pair $(Y, \widetilde{B_Z} \cup (\overline{G} \setminus \overline{D}))$ is an association scheme, is called the *wedge product* of $(Y_X, B_X), X \in \Sigma$, and (V, G). Now let $g \in G \setminus D$ and $b_X \in B_X$ such that $\pi_X(b_X) = g_X$. Then one can see that the graph with vertices Y and the edge set $\overline{g} \cup \widetilde{b}$ is the generalized X-join of g and $\{\varphi_{XX'}(b_X)\}_{X'\in\Sigma}$ with respect to π.

Remark 2.9. The generalized wreath product of Cayley digraphs on abelain groups was first introduced in [2] and an entire section of the recent book [4, Section 5] is devoted to their study. A Cayley digraph $Cay(G, S)$ of G with connection set S is a generalized wreath product if there are subgroups $1 < K \leq L < G$ such that $S \setminus L$ is a union of cosets of K. In the following we show that the generalized X-join generalizes the generalized wreath product. To see this, let $Cay(G, S)$ be a generalized wreath product on abelian

group G such that $1 \notin S$ and $S = S^{-1}$. Let $V = \{g_1, \ldots, g_t\}$ be a set of left coset representatives of K in G and Γ be the subgraph of G induced on V. Suppose that $\{a_0 = 1, a_1, \ldots, a_m\}$ is a set of left coset representatives of L in G. For every $0 \leq i \leq m$, let $X_i = \{g_j \in V \mid g_j \in a_i L\}$. Then $\Pi = \{X_0, X_1, \ldots, X_m\}$ is a partition of V. Put $B_0 = Cay(L, L \cap S)$ and for every $1 \leq i \leq m$, let $B_i = \phi_i(B_0)$ where $\phi_i \colon B_0 \to B_i$ is a graph isomorphism defined by $\phi_i(l) = a_i l$ for every $l \in L$. Then there is the graph epimorphism $\pi_i \colon B_i \to \Gamma(X_i)$ such that $\pi_i(g_j K) = g_j$. Now let $W = (G, E)$ be the generalized X-join of Γ and $\{B_0, B_1, \ldots, B_m\}$ with respect to π where $\pi = \dot{\bigcup}_{i=0}^{m} \pi_i$. We show that for every $x, y \in G$, $xy \in E$ if and only if $xy^{-1} \in S$. Clearly, if $x, y \in a_i L$, then $xy \in E$ if and only if $xy^{-1} \in S \cap L$. If $x \in g_r K \subseteq a_i L$ and $y \in g_s K \subseteq a_j L$ where $i \neq j$, then $xy^{-1} \in g_r g_s^{-1} K$. Then $xy \in E$ if and only if $g_r g_s^{-1} \in S \setminus L$ if and only if $g_r g_s^{-1} K \subseteq S \setminus L$, since $S \setminus L$ is a union of cosets of K. So in this case $xy \in E$ if and only if $xy^{-1} \in S \setminus L$. Thus we conclude that $W = (G, E) = Cay(G, S)$. This means that $Cay(G, S)$ is a generalized X-join.

3 Generalized wreath product, definition and construction

The generalized wreath product of permutation groups has been defined in [1, 5]. Since in the next section we need to construct the generalized wreath product of the automorphism group of graphs, here we have a look at the definition of this product which has been given in [1].

Let $\Gamma = (V, R)$ be a graph and $F = \mathrm{Aut}(\Gamma)$. Suppose that Π is a system of blocks for F. Moreover, suppose that we are given a set of graphs $\{B_X = (Y_X, E_X) \mid X \in \Pi\}$ such that the following conditions hold.

(G1) If for some $f \in F$, $X^f = X'$, then $B_X \simeq B_{X'}$,

(G2) If Δ is an orbit of F on Π, then for some $X \in \Delta$, there exists a graph epimorphism $\pi_X \colon Y_X \to X$ from B_X onto $\Gamma(X)$ and there exists an epimorphism $\eta_X \colon \mathrm{Aut}(B_X) \to F^X / F_{(X)}$ such that

$$\pi_X(y^l) = (\pi_X(y))^{\eta_X(l)}, \ \ \forall y \in Y_X, l \in \mathrm{Aut}(B_X).$$

By condition $(G1)$, if there exists $f_{XX'} \in F$ such that $X^{f_{XX'}} = X'$, we have a graph isomorphism $\phi_{XX'} \colon Y_X \to Y_{X'}$ from graph B_X onto $B_{X'}$. Then $\psi_{XX'} \colon \mathrm{Aut}(B_X) \to \mathrm{Aut}(B_{X'})$ defined by

$$\psi_{XX'}(\alpha) = \phi_{XX'} \alpha \phi_{XX'}^{-1}, \ \ \forall\, \alpha \in \mathrm{Aut}(B_X),$$

is an isomorphism from $\mathrm{Aut}(B_X)$ onto $\mathrm{Aut}(B_{X'})$.
Moreover, by condition $(G2)$, $\Lambda_X = \{\pi_X^{-1}(x) \mid x \in X\}$ is a system of blocks for $\mathrm{Aut}(B_X)$,

$$\overline{\eta_X} \colon \mathrm{Aut}(B_X)/K_X \to F^X / F_{(X)}$$

is an isomorphism, and $\mathrm{Aut}(B_X)/K_X \leq \mathrm{Sym}(\Lambda_X)$ and $F^X/F_{(X)} \leq \mathrm{Sym}(X)$ are permutation isomorphic where $K_X = \ker(\eta_X)$.

Lemma 3.1. *Let $X' \in \Delta$ with $X' \neq X$. Then*

(1) *there exists a graph epimorphism $\pi_{X'}$ from $B_{X'}$ onto $\Gamma(X')$ such that the following diagram is commutative, where $\xi_{XX'}\colon X \to X'$, given by $\xi_{XX'}(x) = x^{f_{XX'}}$ for every $x \in X$.*

$$\begin{array}{ccc} Y_X & \xrightarrow{\phi_{XX'}} & Y_{X'} \\ {\scriptstyle \pi_X}\downarrow & & \downarrow{\scriptstyle \pi_{X'}} \\ X & \xrightarrow{\xi_{XX'}} & X' \end{array}$$

(2) *there exists an epimorphism $\eta_{X'}\colon \mathrm{Aut}(B_{X'}) \to F^{X'}/F_{(X')}$ such that the following diagram is commutative, where $\rho_{XX'}\colon F^X/F_{(X)} \to F^{X'}/F_{(X')}$, defined by $\rho_{XX'}(hF_{(X)}) = f_{XX'}hf_{XX'}^{-1}F_{(X')}$ for every $hF_{(X)} \in F^X/F_{(X)}$.*

$$\begin{array}{ccc} \mathrm{Aut}(B_X) & \xrightarrow{\psi_{XX'}} & \mathrm{Aut}(B_{X'}) \\ {\scriptstyle \eta_X}\downarrow & & \downarrow{\scriptstyle \eta_{X'}} \\ F^X/F_{(X)} & \xrightarrow{\rho_{XX'}} & F^{X'}/F_{(X')} \end{array}$$

Proof. (1) If we define $\pi_{X'} = \xi_{XX'}\pi_X\phi_{XX'}^{-1}$, then $\pi_{X'}\colon Y_{X'} \to X'$ is a graph epimorphism from $B_{X'}$ onto $\Gamma(X')$ such that the diagram mentioned above is commutative.

(2) Define $\eta_{X'} = \rho_{XX'}\eta_X\psi_{XX'}^{-1}$. Then $\eta_{X'}\colon \mathrm{Aut}(B_{X'}) \to F^{X'}/F_{(X')}$ is an epimorphism such that the above diagram is commutative. □

Now suppose that a graph $\Gamma = (V, R)$ and a set of graphs $\{B_X = (Y_X, E_X) \mid X \in \Pi\}$ satisfy conditions $(G1)$ and $(G2)$. Set $Y = \dot{\bigcup}_{X\in\Pi} Y_X$. Since for every $X \in \Pi$, $K_X \leq \mathrm{Aut}(B_X)$ it follows that the action of $\prod_{X\in\Pi} K_X$ on Y defined by

$$y^k := y^{k_X}, \quad y \in Y_X,\ k = \prod_{X\in\Pi} k_X \in K$$

is faithful. Set $K = \prod_{X\in\Pi} K_X$. Then $K \leq \mathrm{Sym}(Y)$.

Moreover, every element of F can be also considered as an element of $\mathrm{Sym}(Y)$. In fact, for every $g \in F$ we can associate $\overline{g} \in \mathrm{Sym}(Y)$. To do this, let $y_X \in Y_X$ and T_X be a set of left coset representatives for K_X in $\mathrm{Aut}(B_X)$ such that $\mathrm{id}_{Y_X} \in T_X$. Let $g \in F$. We associate to g an element $\overline{g} \in \mathrm{Sym}(Y)$ as follows:

(i) if $X^g = X$, then $(y_X)^{\overline{g}} = (y_X)^t$ where $\overline{\eta_X}(tK_X) = gF_{(X)}$ for some $t \in T_X$;

(ii) if $X^g = X'$, then $(y_X)^{\overline{g}} = \phi_{XX'}((y_X)^t)$ where $\overline{\eta_X}(tK_X) = f_{XX'}^{-1}gF_{(X)}$ for some $t \in T_X$.

Set $\overline{F} = \{\overline{g} \mid g \in F\}$. Clearly, $\overline{F} \subseteq \mathrm{Sym}(Y)$ and $\langle K, \overline{F}\rangle \leq \mathrm{Sym}(Y)$. According to [1, Definition 2.1], the permutation group $\langle K, \overline{F}\rangle$, is the *generalized wreath product* of $\{\mathrm{Aut}(B_X)\}_{X\in\Pi}$ and F. We denote it by $F \circ \{\mathrm{Aut}(B_X)\}_{X\in\Pi}$.

Remark 3.2. It should be mentioned that the generalized wreath product of $\{\mathrm{Aut}(B_X)\}_{X\in\Pi}$ and F is independent of the choice of representatives T_X for every $X \in \Pi$. To see this, let $y_X \in Y_X$ and T'_X be a set of left coset representatives for K_X in $\mathrm{Aut}(B_X)$ such that

$\mathrm{id}_{Y_X} \in T'_X$ and $T'_X \neq T_X$. Let $g \in F$ and $\widehat{g}$ be an element of $\mathrm{Sym}(Y)$ associated with g by the above argument. If $X^g = X$, then $(y_X)^{\widehat{g}} = (y_X)^{t'}$ where $\overline{\eta_X}(t'K_X) = gF_{(X)}$ for some $t' \in T'_X$. Since $t' = tk_X$, for some $t \in T_X$ and $k_X \in K_X$, we have

$$(y_X)^{\widehat{g}} = (y_X)^{t'} = (y_X)^{tk_X} = (y_X)^{\overline{g}k_X}.$$

Similarly, if $X^g = X'$, then $(y_X)^{\widehat{g}} = \phi_{XX'}((y_X)^{t'})$ where $\overline{\eta_X}(t'K_X) = f^{-1}_{XX'}gF_{(X)}$ for some $t' \in T'_X$. If $t' = tk_X$ for some $t \in T_X$ and $k_X \in K_X$, then

$$(y_X)^{\widehat{g}} = \phi_{XX'}((y_X)^{t'}) = \phi_{XX'}((y_X)^{tk_X}) = \phi_{XX'}((y_X)^{\overline{g}k_X}).$$

Then we conclude that

$$< \widehat{F}, K > = < \overline{F}, K >,$$

where $\widehat{F} = \{\widehat{f} \mid f \in F\}$. This shows that $F \circ \{\mathrm{Aut}(B_X)\}_{X\in\Pi} = < \widehat{F}, K >$.

Example 3.3. Let Γ and $\{B_X, B_{X'}, B_{X''}\}$ be the graphs in Figure 7. Then

$$\mathrm{Aut}(\Gamma) = \{\mathrm{id}_V, (14)(25)(36), (23), (56), (23)(56), (2635)(14), (2536)(14), (26)(35)(14)\}$$

and

$$\Pi = \{X = \{2,3\}, X' = \{5,6\}, X'' = \{1,4\}\}$$

is a system of blocks for $F = \mathrm{Aut}(\Gamma)$. Put $f_{XX'} = (14)(25)(36)$. Since $X^{f_{XX'}} = X'$ we have the following graph isomorphism from B_X onto $B_{X'}$.

$$\begin{aligned} \phi_{XX'} \colon Y_X &\to Y_{X'} \\ a &\longrightarrow a' \\ b &\longrightarrow b' \\ c &\longrightarrow c' \\ d &\longrightarrow d' \end{aligned}$$

So condition (G1) holds, because, $\{X, X'\}$ and $\{X''\}$ are the orbits of F on Π. Moreover, there exist the graph epimorphisms $\pi_X \colon B_X \to \Gamma(X)$, $\pi_{X'} \colon B_{X'} \to \Gamma(X')$, and $\pi_{X''} \colon B_{X''} \to \Gamma(X'')$ such that $\{\pi^{-1}_X(x) \mid x \in X\} = \{\{a,c\},\{b,d\}\}$, $\{\pi^{-1}_{X'}(x) \mid x \in X'\} = \{\{a',c'\},\{b',d'\}\}$, and $\{\pi^{-1}_{X''}(x) \mid x \in X''\} = \{\{b'',c''\},\{a'',d''\}\}$. If we define the epimorphisms $\eta_X \colon \mathrm{Aut}(B_X) \to F^X/F_{(X)}$, $\eta_{X'} \colon \mathrm{Aut}(B_{X'}) \to F^{X'}/F_{(X')}$, and $\eta_{X''} \colon \mathrm{Aut}(B_{X''}) \to F^{X''}/F_{(X'')}$ by

$$\begin{cases} \eta_X(\mathrm{id}_{Y_X}) = F_{(X)} \\ \eta_X((ab)(cd)) = (23)F_{(X)} \end{cases}$$

$$\begin{cases} \eta_{X'}(\mathrm{id}_{Y_{X'}}) = F_{(X')} \\ \eta_{X'}((a'b')(c'd')) = (56)F_{(X')} \end{cases}$$

and

$$\begin{cases} \eta_{X''}(\mathrm{id}_{Y_{X''}}) = F_{(X'')} \\ \eta_{X''}((a''b'')(c''d'')) = (14)(25)(36)F_{(X'')} \end{cases}$$

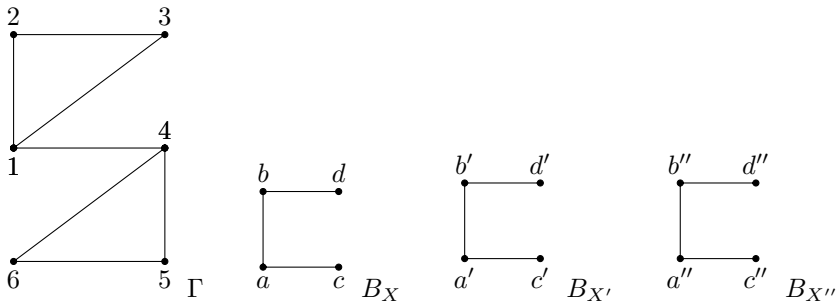


Figure 7: Graph Γ and set of graphs $\{B_X\}_{X\in\Pi}$.

then it is easy to verify that condition $(G2)$ holds.
Put $Y = \{a, b, c, d, a', b', c', d', a'', b'', c'', d''\}$. Consider element $g = (2536)(14) \in F$. Since $X = \{2, 3\}$, $X' = \{5, 6\}$, and $X'' = \{1, 4\}$ we have $X^g = X', X'^g = X$ and $X''^g = X''$. Now we associate to g, an element $\overline{g}$ such that

(i) $(y_X)^{\overline{g}} = \phi_{XX'}(y_X)$, since $\overline{\eta_X}(K_X) = f_{XX'}^{-1} g F_{(X)} = (56)F_{(X)} = F_{(X)}$;

(ii) $(y_{X'})^{\overline{g}} = \phi_{X'X}((y_{X'})^{(a'b')(c'd')})$, since $\overline{\eta_{X'}}((a'b')(c'd')K_{X'}) = f_{X'X}^{-1} g F_{(X')} = (56)F_{(X')}$;

(iii) $(y_{X''})^{\overline{g}} = (y_{X''})^{(a''b'')(c''d'')}$, since $\overline{\eta_{X''}}((a''b'')(c''d'')K_{X''}) = gF_{(X'')} = (14)(25)(36)F_{(X'')}$.

Then $\overline{g} = (aa'bb')(cc'dd')(a''b'')(c''d'')$. Similarly,

(1) if $g = (23)$ then $\overline{g} = (ab)(cd)$;

(2) if $g = (56)$ then $\overline{g} = (a'b')(c'd')$;

(3) if $g = (23)(56)$ then $\overline{g} = (ab)(cd)(a'b')(c'd')$;

(4) if $g = (2635)(14)$ then $\overline{g} = (ab'ba')(cd'dc')(a''b'')(c''d'')$;

(5) if $g = (14)(25)(36)$ then $\overline{g} = (aa')(bb')(cc')(dd')(a''b'')(c''d'')$;

(6) if $g = (14)(26)(35)$ then $\overline{g} = (ab')(ba')(cd')(dc')(a''b'')(c''d'')$.

Since K_X, $K_{X'}$ and $K_{X''}$ are trivial groups, it follows that

$$\mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_X)\}_{X\in\Pi} = \langle \mathrm{id}_Y, (ab)(cd), (a'b')(c'd'), (aa'bb')(cc'dd')(a''b'')(c''d''), (ab'ba')(cd'dc')(a''b'')(c''d''), (aa')(bb')(cc')(dd')(a''b'')(c''d''), (ab')(ba')(cd')(dc')(a''b'')(c''d'')\rangle.$$

4 Automorphism group of the generalized X-join of graphs

In this section we show that the automorphism group of some graphs which are isomorphic to a generalized X-join can be expressed in terms of the generalized wreath product of automorphism groups of its factors.

Theorem 4.1. *With the notation above, suppose that a graph* $\Gamma = (V, R)$ *and a set of graphs* $\{B_X = (Y_X, E_X) \mid X \in \Pi\}$ *satisfy the conditions* $(G1)$ *and* $(G2)$. *Then*

$$\mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_X)\}_{X\in\Pi} \leq \mathrm{Aut}(\Gamma \circ_\pi \{B_X\}_{X\in\Pi}).$$

Proof. Let $W = (Y, E)$ be the generalized X-join of Γ and $\{B_X\}_{X\in\Pi}$ with respect to π, and $H = \langle K, \overline{F}\rangle$ be the generalized wreath product of $\{\mathrm{Aut}(B_X)\}_{X\in\Pi}$ and $\mathrm{Aut}(\Gamma)$.

We show that for every $h \in H$ and $u, v \in Y$, if $(u, v) \in E$, then $(u^h, v^h) \in E$. To do this, we assume that $(u, v) \in E$ and we consider the following cases.

Case 1. Suppose that $h = \prod_{X\in\Pi} k_X \in K$.

(i) If $u, v \in Y_X$ for some $X \in \Pi$, then since for every $X \in \Pi$, $k_X \in \mathrm{Aut}(B_X)$ we have $(u, v)^h = (u^h, v^h) = (u^{k_X}, v^{k_X}) \in E_X$.

(ii) If $u \in Y_X$ and $v \in Y_{X'}$ for some X and X' in Π where $X \neq X'$, then $(x, x') = (\pi_X(u), \pi_{X'}(v)) \in R$ and since $(u^{k_X}, v^{k_{X'}}) \in \pi_X^{-1}(x)\times\pi_{X'}^{-1}(x')$ we have $(u, v)^h = (u^h, v^h) = (u^{k_X}, v^{k_{X'}}) \in E$.

Case 2. Suppose that $h = \overline{g}$ for some $g \in F$ and $u, v \in Y_X$ for some $X \in \Pi$.

(i) If $X^g = X$, then since $(u, v)^{\overline{g}} = (u^{\overline{g}}, v^{\overline{g}}) = (u^t, v^t)$ where $\overline{\eta_X}(tK_X) = gF_{(X)}$ for some $t \in \mathrm{Aut}(B_X)$, we have $(u, v)^h = (u^h, v^h) = (u^t, v^t) \in E$.

(ii) If $X^g = X'$ for some $X' \in \Pi$, then since $(u, v)^{\overline{g}} = (u^{\overline{g}}, v^{\overline{g}}) = (\phi_{XX'}(u^t), \phi_{XX'}(v^t))$ where $\overline{\eta_X}(tK_X) = f_{XX'}^{-1}gF_{(X)}$ for some $t \in \mathrm{Aut}(B_X)$ we have $(u, v)^h = (u^h, v^h) = (\phi_{XX'}(u^t), \phi_{XX'}(v^t)) \in E$.

Case 3. Let $h = \overline{g}$ for some $g \in F$, $u \in Y_X$ and $v \in Y_{X'}$ for some $X, X' \in \Pi$ where $X \neq X'$. In this case since $(x, x') = (\pi_X(u), \pi_{X'}(v)) \in R$ and $g \in \mathrm{Aut}(\Gamma)$ we have $(x^g, x'^g) \in R$. Then the following cases arise.

(i) If $X^g = X$ and $X'^g = X'$, then $(u, v)^{\overline{g}} = (u^{\overline{g}}, v^{\overline{g}}) = (u^t, v^{t'})$ where $\overline{\eta_X}(tK_X) = gF_{(X)}$ and $\overline{\eta_{X'}}(t'K_{X'}) = gF_{(X')}$. Since $\pi_X(u^t) = \pi_X(u)^{\eta_X(t)} = x^g$ and $\pi_{X'}(v^{t'}) = \pi_{X'}(v)^{\eta_{X'}(t')} = x'^g$ we have

$$(u^t, v^{t'}) \in \pi_X^{-1}(x^g) \times \pi_{X'}^{-1}(x'^g).$$

Then $(u^h, v^h) = (u^t, v^{t'}) \in E$.

(ii) If $X^g = X$ and $X'^g = X''$, then $(u, v)^{\overline{g}} = (u^{\overline{g}}, v^{\overline{g}}) = (u^t, \phi_{X'X''}(v^{t'}))$ where $\overline{\eta_X}(tK_X) = gF_{(X)}$ and $\overline{\eta_{X'}}(t'K_{X'}) = f_{X'X''}^{-1}gF_{(X')}$. Then $\pi_X(u^t) = \pi_X(u)^{\eta_X(t)} = x^g$ and by condition $(G2)$ we have

$$\begin{aligned}
\pi_{X''}(\phi_{X'X''}(v^{t'})) &= \xi_{X'X''}(\pi_{X'}(v^{t'})) \\
&= \xi_{X'X''}(\pi_{X'}(v)^{\eta_{X'}(t')}) \\
&= f_{X'X''}\overline{\eta_{X'}}(t'K_{X'})(\pi_{X'}(v)) \\
&= gF_{(X')}(\pi_{X'}(v)) \\
&= (\pi_{X'}(v))^g \\
&= x'^g.
\end{aligned}$$

So $(u^t, \phi_{X'X''}(v^{t'})) \in \pi_X^{-1}(x^g) \times \pi_{X''}^{-1}(x'^g)$ and then $(u^h, v^h) = (u^t, \phi_{X'X''}(v^{t'})) \in E$.

(iii) If $X^g = X'$ and $X'^g = X''$, then $(u, v)^{\overline{g}} = (u^{\overline{g}}, v^{\overline{g}}) = (\phi_{XX'}(u^t), \phi_{X'X''}(v^{t'}))$ where $\overline{\eta_X}(tK_X) = f_{XX'}^{-1} g F_{(X)}$ and $\overline{\eta_{X'}}(t'K_{X'}) = f_{X'X''}^{-1} g F_{(X')}$. From condition $(G2)$ we have

$$\begin{aligned}
\pi_{X'}(\phi_{XX'}(u^t)) &= \xi_{XX'}(\pi_X(u^t)) \\
&= \xi_{XX'}(\pi_X(u)^{\eta_X(t)}) \\
&= f_{XX'}\overline{\eta_X}(tK_X)(\pi_X(u)) \\
&= gF_{(X)}(\pi_X(u)) \\
&= (\pi_X(u))^g \\
&= x^g.
\end{aligned}$$

Similarly, $\pi_{X''}(\phi_{X'X''}(v^{t'})) = x'^g$. Then

$$(\phi_{XX'}(u^t), \phi_{X'X''}(v^{t'})) \in \pi_{X'}^{-1}(x^g) \times \pi_{X''}^{-1}(x'^g)$$

and so $(u^h, v^h) = (\phi_{XX'}(u^t), \phi_{X'X''}(v^{t'})) \in E$.

(iv) If $X^g = X''$ and $X'^g = X'''$, then $(u, v)^{\overline{g}} = (u^{\overline{g}}, v^{\overline{g}}) = (\phi_{XX''}(u^t), \phi_{X'X'''}(v^{t'}))$ where $\overline{\eta_X}(tK_X) = f_{XX''}^{-1} g F_{(X)}$ and $\overline{\eta_{X'}}(t'K_{X'}) = f_{X'X'''}^{-1} g F_{(X')}$. Then an argument similar to that given in (iii) shows that $\pi_{X''}(\phi_{XX''}(u^t)) = x^g$ and $\pi_{X'''}(\phi_{X'X'''}(v^{t'})) = x'^g$. So $(\phi_{XX''}(u^t), \phi_{X'X'''}(v^{t'})) \in \pi_{X''}^{-1}(x^g) \times \pi_{X'''}^{-1}(x'^g)$ and hence $(u^h, v^h) = (\phi_{XX''}(u^t), \phi_{X'X'''}(v^{t'})) \in E$.

Then we conclude that $\langle K, \overline{F} \rangle \subseteq \mathrm{Aut}(\Gamma \circ_\pi \{B_X\}_{X \in \Pi})$. Thus

$$\mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_X)\}_{X \in \Pi} \leq \mathrm{Aut}(\Gamma \circ_\pi \{B_X\}_{X \in \Pi}). \qquad \square$$

The inclusion $\mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_X)\}_{X \in \Pi} \leq \mathrm{Aut}(\Gamma \circ_\pi \{B_X\}_{X \in \Pi})$ in the above theorem may be proper. For example

$$D_8 = \mathrm{Aut}(K_2) \circ \mathrm{Aut}(K_2) < \mathrm{Aut}(K_2 \circ K_2) = S_4,$$

where S_4 is the symmetric group on 4 elements $V = \{1, 2, 3, 4\}$ and $D_8 = \{\mathrm{id}_V, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$ is the dihedral group of order 8; see [6, Chapter 10]. In the following we give necessary and sufficient conditions under which the above inclusion is proper.

Theorem 4.2. *With the notation above, suppose that the graph $\Gamma = (V, R)$ and the set of graphs $\{B_X = (Y_X, E_X) \mid X \in \Pi\}$ satisfy the conditions $(G1)$ and $(G2)$. Let $W = (Y, E)$ be the generalized X-join of Γ and $\{B_X\}_{X \in \Pi}$ with respect to π and let $E_0 \subseteq E_1$ be the equivalence relations defined in (1) and (2). Then the inclusion*

$$\mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_X)\}_{X \in \Pi} \leq \mathrm{Aut}(W)$$

is proper if and only if there exist equivalence relations $E_0' \subseteq E_1'$ on Y such that the following conditions hold.

(i) *$E'_0 \subsetneq E_0$ and $E'_1 \subsetneq E_1$, and $W = \Gamma' \circ_{\pi'} \{A_Z\}_{Z\in\Pi'}$, where the graph Γ' is the quotient graph W/E'_0, Π' is a partition of $V(\Gamma')$, $\{A_Z\}_{Z\in\Pi'}$ are the subgraphs of W induced by the equivalence classes of E'_1, $\pi' = \dot{\bigcup}_{Z\in\Pi'}\pi'_Z$, and $\{{\pi'}_Z^{-1}(x) \mid x \in V(\Gamma'), Z \in \Pi'\}$ is the set of equivalence classes of E'_0.*

(ii) *There exist $Z \neq Z' \in \Pi' - \Pi$ and a graph isomorphism $\phi\colon Y_Z \to Y_{Z'}$ from A_Z onto $A_{Z'}$, such that ϕ preserves equivalence classes of E'_0 contained in Y_Z.*

(iii) *For every equivalence class S' of E'_0 contained in Y_Z, if $W[S']$ is a union of connected components of $W[S]$ for some $S \in W/E_0$, where $S' \subsetneq S$ then $\pi'_Z(S')$ and $\pi'_{Z'}(\phi(S'))$ are nonadjacent, otherwise $\pi'_Z(S')$ and $\pi'_{Z'}(\phi(S'))$ are adjacent. In both cases $\pi'_Z(S')$ and $\pi'_{Z'}(\phi(S'))$ have the same neighbors in $V(\Gamma') \setminus Z \cup Z'$.*

(iv) *For each two distinct equivalence classes S'_1 , S'_2 of E'_0 that are contained in Y_Z, S'_1 and $\phi(S'_2)$ are adjacent if and only if $\phi(S'_1)$ and S'_2 are adjacent.*

Proof. Suppose that there exists $\phi \in \mathrm{Aut}(W) \setminus \mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_X)\}_{X\in\Pi}$. Let U be the set of all elements of Y that are moved by ϕ. Since $Y/E_1 = \{Y_X \mid X \in \Pi\}$ and $Y/E_0 = \bigcup_{X\in\Pi}\Lambda_X$, where $\Lambda_X = \{\pi_X^{-1}(x) \mid x \in X\}$, are two system of blocks for $\mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_X)\}_{X\in\Pi}$, then there exist

(1) $X \in \Pi$ such that $U_X = U \cap Y_X \neq \emptyset$;

(2) $X' \in \Pi$ such that $X \neq X'$ and $\phi(U_X) \subseteq Y_{X'}$. Note that if $X = X'$, then the restriction of ϕ to Y_X is an automorphism of B_X and $\phi(U_X) \subseteq Y_X$. But since $\phi \notin \mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_X)\}_{X\in\Pi}$ we must have at least two equivalence classes $S_1, S_2 \in E_0$ such that a part of S_1 is moved by the automorphism ϕ to a part of S_2. This contradicts the fact that $\Lambda_X = \{\pi_X^{-1}(x) \mid x \in X\}$ is a system of blocks for $\mathrm{Aut}(B_X)$.

(3) at least one equivalence class S of E_0 such that $S \cap U_X \subsetneq S$. Indeed, if $U_X = \bigcup_{i=1}^{t} S_i \subsetneq Y_X$ where every S_i is an equivalence class of E_0, then by (2), $\phi(U_X) \subseteq Y_{X'}$ for some $X' \neq X$ and $\phi(U_X)$ is a union of some equivalence classes of E_0 which are contained in $Y_{X'}$. This means that the vertices $\pi_X(S_1), \ldots, \pi_X(S_t)$ of X can be moved to the vertices $\pi_{X'}(\phi(S_1)), \ldots, \pi_{X'}(\phi(S_t))$ of X'. This contradicts the fact that Π is a system of blocks for $\mathrm{Aut}(\Gamma)$.

Put $V_{X'} = \phi(U_X)$. Let $S_1, S_2, ..., S_t$ be the equivalence classes of E_0 contained in Y_X such that for every $1 \leq i \leq t$,

$$S_i^X = S_i \cap U_X \neq \emptyset.$$

Then for at least one i, $S_i^X \subsetneq S_i$. Moreover, we have the following.

(a) The restriction of ϕ to U_X gives an isomorphism between $W[U_X]$ and $W[V_{X'}]$, the subgraphs of W induced by U_X and $V_{X'}$.

(b) For each i the vertices in $S_i^X \cup \phi(S_i^X)$ have the same neighbors in $Y \setminus (U_X \cup V_{X'})$. Indeed, suppose that $u \in S_i^X$ and w is a neighbor of u. Suppose that $T_1, \ldots, T_t$ are equivalence classes of E_0 such that $\phi(S_i^X) \cap T_i \neq \emptyset$ and $v_i \in T_i \setminus \phi(S_i^X)$. If $w \in Y \setminus (Y_X \cup Y_{X'})$, then $\phi(w)$ is adjacent to all vertices of T_i, specially v_i. So w and $\phi^{-1}(v_i) = v_i$ are adjacent. Thus w is adjacent to all vertices of $\phi(S_i^X)$.

Moreover, if $w \in Y_X \setminus U_X$, then since w is adjacent to u, $\phi(w) = w$ is adjacent to $\phi(u)$. Then w is adjacent to all vertices of $\phi(S_i^X)$. Similarly, if $w \in Y_{X'} \setminus V_{X'}$, then w is adjacent to all vertices of $\phi(S_i^X)$. Hence we conclude that $S_i^X \cup \phi(S_i^X)$ have the same neighbors in $Y \setminus (U_X \cup V_{X'})$.

(c) If $W[S_i^X]$ is a union of connected components of $W[S_i]$, then S_i^X and $\phi(S_i^X)$ are nonadjacent; otherwise by the definition of W, $S_i \setminus S_i^X$ and $\phi(S_i^X)$ are adjacent and since $\phi \in \mathrm{Aut}(W)$, S_i^X and $S_i \setminus S_i^X$ are adjacent and this contradicts the hypothesis that $W[S_i^X]$ is a union of connected components of $W[S_i]$. Also if $W[S_i^X]$ and $W[S_i \setminus S_i^X]$ are adjacent, then since $\phi \in \mathrm{Aut}(W)$, $S_i \setminus S_i^X$ and $\phi(S_i^X)$ must be adjacent and the definition of W implies that $\phi(S_i^X)$ and S_i are externally related to each other. Moreover, $S_i \setminus S_i^X$ and S_i^X are also externally related to each other.

(d) For two different equivalence classes S_1 and S_2 of E_0 with $S_1^X, S_2^X \neq \emptyset$, if S_1 and $\phi(S_2^X)$ are adjacent then from the definition of W it follows that S_1 and $\phi(S_2^X)$ are externally related to each other. Moreover, since $\phi \in \mathrm{Aut}(W)$ we must have $\phi(S_1^X)$ and S_2 are also externally related to each other. Similarly, if S_2 and $\phi(S_1^X)$ are adjacent then $\phi(S_2^X)$ and S_1 are externally related to each other.

Now we consider two equivalence relations $E_0' \subseteq E_1'$ on Y such that

$$Y/E_1' = \{U_X, V_{X'}, Y_X \setminus U_X, Y_{X'} \setminus V_{X'}, Y/E_1 \setminus \{Y_X, Y_{X'}\}\},$$

and the equivalence classes of E_0' are equal

$$S_i^X, S_i \setminus S_i^X, \phi(S_i^X), T_i \setminus \phi(S_i^X), \quad 1 \leq i \leq t,$$

and $Y/E_0 \setminus \{S_i, T_i \mid 1 \leq i \leq t\}$, where for every i, T_i is an equivalence class of E_0 such that $\phi(S_i^X) \subseteq T_i$.
From statements (b) and (c) we conclude that the condition (ii) of Theorem 2.4 holds and so $W = \Gamma' \circ_{\pi'} \{A_X\}_{X \in \Pi'}$, where Γ' is the quotient graph W/E_0', Π' is a partition of $V(\Gamma')$ induced by Y/E_1', and $\{A_X\}_{X \in \Pi'}$ are the subgraphs of W induced by the equivalence classes of E_1'. So (i) holds. If we denote by A_X and $A_{X'}$ the subgraphs of W induced by U_X and $V_{X'}$, respectively, then the restriction of ϕ to U_X gives a graph isomorphism between A_X and $A_{X'}$. Clearly, ϕ preserves the equivalence classes of E_0' contained in U_X. Thus condition (ii) of theorem holds. Moreover, (b), (c) and the definition of π' imply that condition (iii) holds. Finally, condition (iv) follows from statement (d).

Conversely, suppose that there exist equivalence relations $E_0' \subseteq E_1'$ on Y such that conditions (i) – (iv) hold. Let U_Z and $U_{Z'}$ be the vertex sets of A_Z and $A_{Z'}$, respectively. Assume that $\phi\colon U_Z \longrightarrow U_{Z'}$ is the graph isomorphism from A_Z onto $A_{Z'}$. We define a bijection $\psi\colon Y \longrightarrow Y$ as follows:

$$\psi(v) = \begin{cases} \phi(v) & \text{if } v \in U_Z, \\ \phi^{-1}(v) & \text{if } v \in U_{Z'}, \\ v & \text{if } v \notin \{U_Z, U_{Z'}\}. \end{cases}$$

We claim that $\psi \in \mathrm{Aut}(W)$. To do this, we suppose that $(u, v) \in E$ and we consider the following cases.

(1) If $u, v \in Y \setminus U_Z \cup U_{Z'}$, then clearly $(\psi(u), \psi(v)) = (u, v) \in E$.

(2) If $u, v \in U_Z$, then since ϕ is a graph isomorphism it follows that $(\psi(u), \psi(v)) = (\phi(u), \phi(v)) \in E$. Similarly, if $u, v \in U_{Z'}$ we have $(\psi(u), \psi(v)) = (\phi^{-1}(u), \phi^{-1}(v)) \in E$.

(3) If $u \in U_Z$ and $v \in Y \setminus U_Z \cup U_{Z'}$, then since v is a neighbor of u it follows from (iii) that v is also a neighbor of $\phi(u)$. Hence $(\psi(u), \psi(v)) = (\phi(u), v) \in E$.

(4) If $u \in U_Z$ and $v \in U_{Z'}$ such that for some equivalence class S' of E'_0, $u \in S'$ and $v \in \phi(S')$, then the definition of W implies that all vertices in S' are adjacent to all vertices in $\phi(S')$ and so $(\psi(u), \psi(v)) = (\phi(u), \phi^{-1}(v)) \in E$.

(5) If $u \in U_Z$ and $v \in U_{Z'}$ such that for two equivalence classes S'_1 and S'_2 of E'_0, $u \in S'_1$ and $v \in \phi(S'_2)$, then by the definition of W, all vertices in S'_1 are adjacent to all vertices in $\phi(S'_2)$. On the other hand, it follows from (iv) that $\phi(S'_1)$ and S'_2 are adjacent. So all vertices of $\phi(S'_1)$ are adjacent to all vertices of S'_2 and thus $(\psi(u), \psi(v)) = (\phi(u), \phi^{-1}(v)) \in E$.

Hence $\psi \in \mathrm{Aut}(W)$. Since $E'_0 \subsetneq E_0$ and $Z, Z' \in \Pi' - \Pi$, and ψ preserves the equivalence classes of E'_0 we conclude that $\psi \in \mathrm{Aut}(W) \setminus \mathrm{Aut}(\Gamma) \circ \{Aut(B_X)\}_{X \in \Pi}$. □

Example 4.3. Suppose that Γ is the graph in Figure 8 with vertices $V = \{1, 2, 3, 4, 5, 6\}$. Then one can see that

$$F = \mathrm{Aut}(\Gamma) = \{\mathrm{id}_V, (12)(56)(34), (13)(24), (23)(56)(14)\}$$

and

$$\Pi = \{X = \{1, 2\}, X' = \{3, 4\}, X'' = \{5, 6\}\},$$

is a system of blocks for F. Moreover, $F^X = F^{X'} = \{\mathrm{id}_V, (12)(56)(34)\}$, $F^{X''} = F$, $F_{(X)} = F_{(X')} = \{\mathrm{id}_V\}$, and $F_{(X'')} = \{\mathrm{id}_V, (13)(24)\}$. Suppose that B_X, $B_{X'}$, and $B_{X''}$ are the graphs in Figure 8 with vertices $Y_X = \{a, b, c, d\}$, $Y_{X'} = \{a', b', c', d'\}$, $Y_{X''} = \{a'', b'', c'', d''\}$, respectively.

Now consider the graph epimorphisms $\pi_X \colon B_X \to \Gamma(X)$, $\pi_{X'} \colon B_{X'} \to \Gamma(X')$, and $\pi_{X''} \colon B_{X''} \to \Gamma(X'')$ as the following:

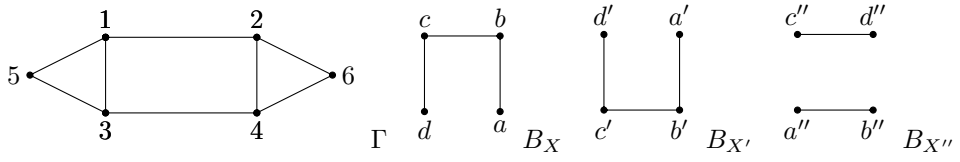


Figure 8: Graph Γ and set of graphs $\{B_X\}_{X \in \Pi}$.

$$\begin{cases} \pi_X(a) = \pi_X(b) = 1 \\ \pi_X(c) = \pi_X(d) = 2 \end{cases}$$

$$\begin{cases}\pi_{X'}(a') = \pi_{X'}(b') = 3\\ \pi_{X'}(c') = \pi_{X'}(d') = 4\end{cases}$$

and

$$\begin{cases}\pi_{X''}(a'') = \pi_{X''}(b'') = 6\\ \pi_{X''}(c'') = \pi_{X''}(d'') = 5\end{cases}.$$

Since $\mathrm{Aut}(B_X) = \{\mathrm{id}_{Y_X}, (bc)(ad)\}$, $\mathrm{Aut}(B_{X'}) = \{\mathrm{id}_{Y_{X'}}, (b'c')(a'd')\}$, and

$$\mathrm{Aut}(B_{X''}) = \{\mathrm{id}_{Y_{X''}}, (a''b''), (c''d''), (a''b'')(c''d''), (a''c''b''d''), (a''d''b''c''), (a''c'')(b''d''), (a''d'')(b''c'')\},$$

we can define epimorphisms $\eta_X \colon \mathrm{Aut}(B_X) \to F^X/F_{(X)}$, $\eta_{X'} \colon \mathrm{Aut}(B_{X'}) \to F^{X'}/F_{(X')}$, and $\eta_{X''} \colon \mathrm{Aut}(B_{X''}) \to F^{X''}/F_{(X'')}$ by

$$\begin{cases}\eta_X(\mathrm{id}_{Y_X}) = \mathrm{id}_V\\ \eta_X((bc)(ad)) = (12)(56)(34)F_{(X)}\end{cases}$$

$$\begin{cases}\eta_{X'}(\mathrm{id}_{Y_{X'}}) = \mathrm{id}_V\\ \eta_{X'}((b'c')(a'd')) = (12)(56)(34)F_{(X')}\end{cases}$$

and

$$\begin{cases}\eta_{X''}(\mathrm{id}_{Y_{X''}}) = \eta_{X''}((a''b'')) = \eta_{X''}((c''d'')) = \eta_{X''}((a''b'')(c''d'')) = \mathrm{id}_V\\ \eta_{X''}((a''c''b''d'')) = \eta_{X''}((a''d''b''c'')) = \eta_{X''}((a''c'')(b''d'')) = \eta_{X''}((a''d'')(b''c'')) =\\ (12)(56)(34)F_{(X'')}\end{cases}$$

Then K_X and $K_{X'}$ are trivial groups and

$$K_{X''} = \{\mathrm{id}_{Y_{X''}}, (a''b''), (c''d''), (a''b'')(c''d'')\}.$$

Let $T_X = \{\mathrm{id}_{Y_X}, (bc)(ad)\}$, $T_{X'} = \{\mathrm{id}_{Y_{X'}}, (b'c')(a'd')\}$, and $T_{X''} = \{\mathrm{id}_{Y_{X''}}, (a''c'')(b''d'')\}$. Put $f_{XX'} = (13)(24)$. Then the elements $(12)(56)(34), (13)(24)$ and $(23)(56)(14)$ in $\mathrm{Aut}(\Gamma)$ are associated to $(bc)(ad)(b'c')(a'd')(a''c'')(b''d'')$, $(aa')(bb')(cc')(dd')$ and $(bc')(ad')(cb')(da')(a''c'')(b''d'')$, respectively. Then we have

$$\mathrm{Aut}(\Gamma)\circ\{\mathrm{Aut}(B_X)\}_{X\in\Pi} = \langle \mathrm{id}_Y, (aa')(bb')(cc')(dd'), (bc')(ad')(cb')(da')(a''c'')(b''d''), (a''b''), (c''d''), (bc)(ad)(b'c')(a'd')(a''c'')(b''d'')\rangle.$$

Now let $W = (Y, E)$ be the generalized X-join of Γ and $\{B_X\}_{X\in\Pi}$ with respect to π. (See Figure 9.) Consider the equivalence relations E_0' and E_1' on Y with the following classes,

$$Y/E_0' = \{\{a\}, \{b\}, \{c\}, \{d\}, \{a'\}, \{b'\}, \{c'\}, \{d'\}, \{a'', b''\}, \{c'', d''\}\}$$

$$Y/E_1' = \{\{a, d\}, \{b, c\}, \{a', d'\}, \{b', c'\}, \{a'', b'', c'', d''\}\}.$$

Then one can see that

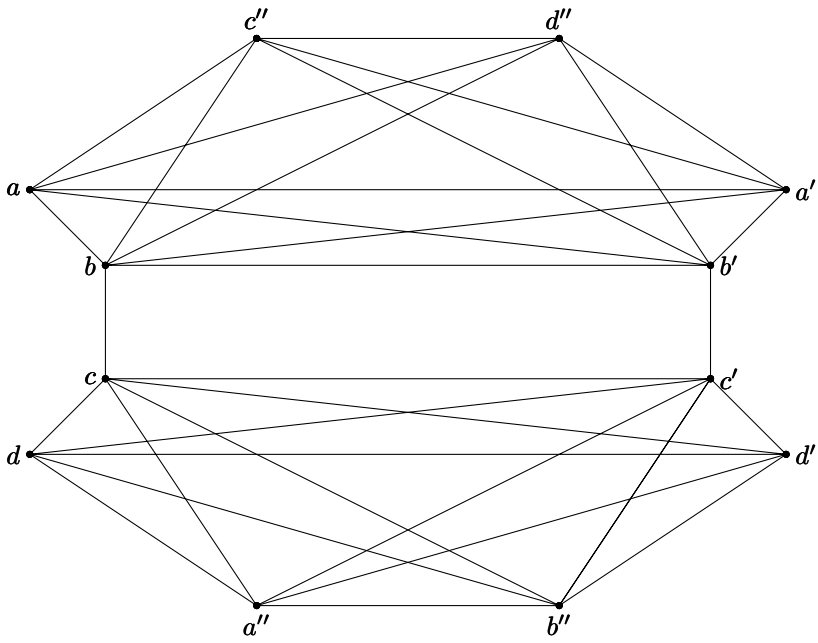


Figure 9: Graph $W = \Gamma \circ_\pi \{B_X\}_{X\in\Pi}$.

(1) $\Gamma \circ_\pi \{B_X\}_{X\in\Pi} = \Gamma' \circ_{\pi'} \{A_Z\}_{Z\in\Pi'}$, where Γ' is the quotient graph W/E_0' with vertices $V(\Gamma') = \{1, 2, \ldots, 10\}$, and $\{A_Z\}_{Z\in\Pi'}$ are the subgraphs of W induced by the equivalence classes of E_1', and $\pi' = \dot{\bigcup}_{Z\in\Pi'}\pi'_Z$ maps $\{a\}, \{b\}, \{c\}, \{d\}, \{a'\}$, $\{b'\}, \{c'\}, \{d'\}, \{c'', d''\}, \{a'', b''\}$ onto $1, 2, \ldots, 10$, respectively. (See Figure 10.)

(2) Put $Y_Z = \{b, c\}$ and $Y_{Z'} = \{b', c'\}$ and let $A_Z = W[Y_Z]$ and $A_{Z'} = W[Y_{Z'}]$. Then $\phi\colon Y_Z \to Y_{Z'}$ such that $\phi(b) = b'$ and $\phi(c) = c'$ is a graph isomorphism from A_Z onto $A_{Z'}$. Clearly, ϕ preserves the equivalence classes of E_0' contained in Y_Z.

(3) Y_Z contains two equivalence classes $S_1' = \{b\}$ and $S_2' = \{c\}$ of E_0' such that $S_1' \subseteq S_1$ and $S_2' \subseteq S_2$ where $S_1 = \{a, b\} \in Y/E_0$ and $S_2 = \{c, d\} \in Y/E_0$. Moreover, $W[S_1]$ is connected and $\pi'_Z(b)$ and $\pi'_{Z'}(\phi(b))$ are adjacent and have the same neighbors in $V(\Gamma') \setminus \{Z \cup Z'\}$, where $Z = \{\pi'_Z(b), \pi'_Z(c)\}$ and $Z' = \{\pi'_{Z'}(b'), \pi'_{Z'}(c')\}$. Similarly, $W[S_2]$ is connected and $\pi'_Z(c)$ and $\pi'_{Z'}(\phi(c))$ are adjacent and have the same neighbors in $V(\Gamma') \setminus \{Z \cup Z'\}$.

(4) The vertex b is nonadjacent to $\phi(c)$ and vertex c is nonadjacent to $\phi(b)$.

Then the conditions of Theorem 4.2 hold. So

$$\mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_X)\}_{X\in\Pi} \lneq \mathrm{Aut}(\Gamma \circ_\pi \{B_X\}_{X\in\Pi}).$$

In the following as a main result, we give necessary and sufficient conditions under which the full automorphism group of the generalized X-join of graphs is equal to the generalized wreath product of the automorphism groups of their factors.

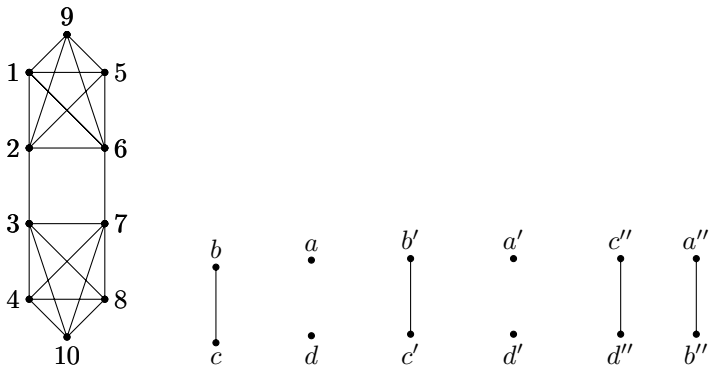


Figure 10: Graph Γ' and set of graphs $\{A_Z\}_{Z\in\Pi'}$.

Corollary 4.4. *Suppose that $W = \Gamma \circ_\pi \{B_X\}_{X\in\Pi}$ is such that the graph $\Gamma = (V, R)$ and the set of graphs $\{B_X = (Y_X, E_X) \mid X \in \Pi\}$ satisfy the conditions $(G1)$ and $(G2)$. Then $\mathrm{Aut}(\Gamma \circ_\pi \{B_X\}_{X\in\Pi}) = \mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_X)\}_{X\in\Pi}$ if and only if there are no equivalence relations $E_0' \subseteq E_1'$ on Y satisfying the conditions* (i)*,* (ii)*,* (iii)*, and* (iv) *of* Theorem 4.2.

Proof. This follows immediately from Theorem 4.2. □

Example 4.5. Let $W = (Y, E)$ be the graph in Figure 11. It is easy to see that W is the graph $\Gamma \circ_\pi \{B_X, B_{X'}, B_{X''}\}$ where Γ and $\{B_X, B_{X'}, B_{X''}\}$, and $\pi = \pi_X \cup \pi_{X'} \cup \pi_{X''}$ are given in Example 3.3. Moreover, $Y/E_0 = \{\{a, c\}, \{b, d\}, \{a', c'\}, \{b', d'\}, \{b'', c''\}, \{a'', d''\}\}$ and $Y/E_1 = \{\{a, c, b, d\}, \{a', c', b', d'\}, \{b'', c'', a'', d''\}\}$. Since there are no equivalence relations $E_0' \subseteq E_1'$ on Y that satisfy the conditions (i), (ii), (iii), and (iv) of Theorem 4.2, it follows that

$$\begin{aligned}\mathrm{Aut}(W) = \mathrm{Aut}(\Gamma)\circ\{\mathrm{Aut}(B_X)\}_{X\in\Pi} = \ & \langle \mathrm{id}_Y, (ab)(cd), (aa'bb')(cc'dd')(a''b'')(c''d''),\\ & (a'b')(c'd'), (ab'ba')(cd'dc')(a''b'')(c''d''),\\ & (aa')(bb')(cc')(dd')(a''b'')(c''d''),\\ & (ab')(ba')(cd')(dc')(a''b'')(c''d'')\rangle.\end{aligned}$$

The next corollary follows directly from Theorem 4.2.

Corollary 4.6. *Suppose that the graph $\Gamma = (V, R)$ and the set of graphs $\{B_X = (Y_X, E_X) \mid X \in \Pi\}$ satisfy the conditions $(G1)$ and $(G2)$. Let $W = (Y, E)$ be the generalized X-join of Γ and $\{B_X\}_{X\in\Pi}$ with respect to π and let $E_0 \subseteq E_1$ be the equivalence relations defined in* (1) *and* (2)*. Then*

$$\mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_X)\}_{X\in\Pi} = \mathrm{Aut}(\Gamma \circ_\pi \{B_X\}_{X\in\Pi})$$

if W is uniquely determined by E_0 and E_1.

Corollary 4.7 (See [8, Theorem 2.10])**.** *Let $\Gamma = (V, R)$ be a graph and $\{B_x \mid x \in V\}$ be a set of graphs such that $B_x \simeq B_{x'}$ whenever $x^f = x'$ for some $f \in \mathrm{Aut}(\Gamma)$. Then*

$$\mathrm{Aut}(\Gamma[B_x]_{x\in V}) = \mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_x)\}_{x\in V}$$

if and only if

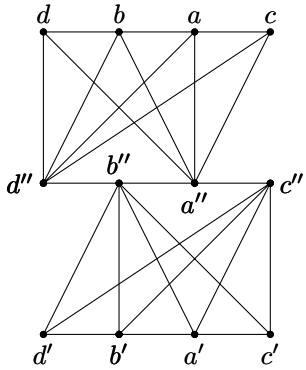


Figure 11: Graph W.

(1) *B_x is connected if there exists at least one vertex $w \in V$ such that x and w are nonadjacent and have the same neighbors in V,*

(2) *$\overline{B_x}$ is connected if there exists at least one vertex $w \in V$ such that x and w are adjacent and have the same neighbors in $V \setminus \{x, w\}$.*

Proof. By Example 2.2, $W = \Gamma[B_x]_{x\in V} = \Gamma \circ_\pi \{B_x\}_{x\in V}$ where $\Pi = \{\{x\} \mid x \in V\}$ and $\pi_x \colon Y_x \to X$ is a graph epimorphism from B_x onto $\Gamma(X)$ such that $\pi_x(y_x) = x$ for every $y_x \in Y_x$. In this case $E_0 = E_1$ and $F^X = F_{(X)}$. If we define

$$\eta_X := \mathrm{Aut}(B_X) \to F^X/F_{(X)}$$

by $\eta_X(\alpha) = 1_{F^X/F_{(X)}}$ for every $\alpha \in \mathrm{Aut}(B_X)$, then η_X is an epimorphism and condition (G2) holds. Then it follows from Corollary 4.4 that

$$\mathrm{Aut}(\Gamma[B_x]_{x\in V}) = \mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_x)\}_{x\in V}$$

if and only if there is no equivalence relation E_0' on Y satisfying the conditions (i), (ii), (iii), and (iv) of Theorem 4.2.

Now suppose that $\mathrm{Aut}(\Gamma[B_x]_{x\in V}) = \mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_x)\}_{x\in V}$ and there exist $x, w \in V$ such that x and w are nonadjacent and have the same neighbors in V. If B_x is disconnected then B_w is also disconnected and we can define an equivalence relation E_0' on Y such that the equivalence classes of E_0' are $Y_z, z \notin \{x, w\}$, together with the connected components of B_x and B_w. Since x and w are nonadjacent and have the same neighbors in V, one can see that the conditions (i), (ii), (iii), and (iv) of Theorem 4.2 hold, a contradiction. So B_x is connected. Moreover, suppose that there exist $x, w \in V$ such that x and w are adjacent and have the same neighbors in $V \setminus \{x, w\}$. If $\overline{B_x}$ is disconnected, then there exist at least two subsets $S_1, S_2 \subset Y_x$ such that all vertices of S_1 are adjacent to all vertices of S_2. Similarly, there exist subsets $S_1', S_2' \subset Y_w$ with the property that all vertices of S_1' are adjacent to all vertices of S_2'. Then we can define an equivalence relation E_0' on Y such that S_1, S_2, S_1', and S_2' together with $Y_z, z \notin \{x, w\}$ are its equivalence classes. One can see that in this case the conditions (i), (ii), (iii), and (iv) of Theorem 4.2 hold and thus again we have a contradiction.

Conversely, suppose that conditions (1) and (2) hold and suppose on the contrary that

$$\varphi \in \mathrm{Aut}(\Gamma[B_x]_{x\in V}) \setminus \mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_x)\}_{x\in V}.$$

Then there is an equivalence relation E_0' on Y satisfying the conditions (i), (ii), (iii), and (iv) of Theorem 4.2. It follows from condition (i) that $W = \Gamma' \circ_{\pi'} \{A_z\}_{z\in V(\Gamma')}$, where the graph Γ' is the quotient graph W/E_0' and $\{A_z\}_{z\in V(\Gamma')}$ are the subgraphs of W induced by the equivalence classes of E_0'. It follows from (ii) that there exist $x, w \in V$ such that the equivalence classes of E_0' contain $Y_z \subsetneq Y_x$ and $Y_{z'} = \varphi(Y_z) \subsetneq Y_w$. By (iii) if $B_x[Y_z]$ is a union of connected components of B_x, then z and z' are nonadjacent and all of their neighbors are exactly the same in $V(\Gamma')$, otherwise z and z' are adjacent and have the same neighbors in $V(\Gamma') \setminus \{z, z'\}$. This implies that if B_x is disconnected then z and z' are nonadjacent and all vertices in Y_z and all vertices in $Y_{z'}$ have the same neighbors in $Y \setminus (Y_z \cup Y_{z'})$. Since $Y_z \subsetneq Y_x$ and $Y_{z'} \subsetneq Y_w$ it follows that x and w must be nonadjacent and have the same neighbors in V, which contradicts (1). Moreover, if B_x is connected, since z and z' are adjacent and have the same neighbors in $V(\Gamma') \setminus \{z, z'\}$ it follows that all vertices in Y_z are adjacent to all vertices of $Y_{z'}$ and all vertices in Y_z and all vertices in $Y_{z'}$ have the same neighbors in $Y \setminus (Y_z \cup Y_{z'})$. Then all vertices in Y_x are adjacent to all vertices of Y_w. So x and w must be adjacent and have the same neighbors in $V \setminus \{x, w\}$. Furthermore, since all vertices in Y_z are adjacent to all vertices of $Y_x \setminus Y_z$ it follows that $\overline{B_x}$ is disconnected, which contradicts (2). Thus we have

$$\mathrm{Aut}(\Gamma[B_x]_{x\in V}) = \mathrm{Aut}(\Gamma) \circ \{\mathrm{Aut}(B_x)\}_{x\in V}. \qquad \square$$

5 Conclusion

A generalization of the X-join of graphs has been introduced and necessary and sufficient conditions under which a graph is isomorphic to a generalized X-join has been given. A generating set for the automorphism groups of a class of graphs which are isomorphic to a generalized X-join has been computed.

Since the generalized X-join of graphs is a natural generalization of the X-join of graphs, the results on the X-join or lexicographic product of graphs can be also studied for the generalized X-join of graphs.

References

[1] J. Bagherian, Schurity of the wedge product of association schemes and generalized wreath product of permutation groups, *Discrete Math.* **343** (2020), 10, doi:10.1016/j.disc.2020.112084, id/No 112084, https://doi.org/10.1016/j.disc.2020.112084.

[2] S. Bhoumik, T. Dobson and J. Morris, On the automorphism groups of almost all circulant graphs and digraphs, *Ars Math. Contemp.* **7** (2014), 499–518, doi:10.26493/1855-3974.315.868, https://doi.org/10.26493/1855-3974.315.868.

[3] E. Dobson and J. Morris, Automorphism groups of wreath product digraphs, *Electron. J. Comb.* **16** (2009), research paper r17, 30, doi:10.37236/106, https://doi.org/10.37236/106.

[4] T. Dobson, A. Malnič and D. Marušič, *Symmetry in Graphs*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2022, doi:10.1017/9781108553995, https://doi.org/10.1017/9781108553995.

[5] S. A. Evdokimov and I. N. Ponomarenko, Schurity of S-rings over a cyclic group and generalized wreath product of permutation groups, *St. Petersbg. Math. J.* **24** (2013), 431–460, doi:10.1090/S1061-0022-2013-01246-5, https://doi.org/10.1090/S1061-0022-2013-01246-5.

[6] R. Hammack, W. Imrich and S. Klavžar, *Handbook of Product of Graphs*, Discrete Mathematics and its Applications, CRC Press, Boca Raton, 2nd edition, 2011.

[7] F. Harary, On the group of the composition of two graphs, *Duke Math. J.* **26** (1959), 29–36, doi:10.1215/S0012-7094-59-02603-1, https://doi.org/10.1215/S0012-7094-59-02603-1.

[8] R. L. Hemminger, The group of an X-join of graphs, *J. Comb. Theory* **5** (1968), 408–418, doi:10.1016/S0021-9800(68)80017-1, https://doi.org/10.1016/S0021-9800(68)80017-1.

[9] R. Mathon, A note on the graph isomorphism counting problem, *Inf. Process. Lett.* **8** (1979), 131–132, doi:10.1016/0020-0190(79)90004-8, https://doi.org/10.1016/0020-0190(79)90004-8.

[10] M. Muzychuk, A wedge product of association schemes, *Eur. J. Comb.* **30** (2009), 705–715, doi:10.1016/j.ejc.2008.07.008, https://doi.org/10.1016/j.ejc.2008.07.008.

[11] G. Sabidussi, The lexicographic product of graphs, *Duke Math J.* **26** (1961), 573–578, doi:10.1215/S0012-7094-61-02857-5, https://doi.org/10.1215/S0012-7094-61-02857-5.

[12] B. Weisfeiler, *On Construction and Identifcation of Graphs*, volume 558 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin-Heidelberg-New York, 1976.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 24 (2024) #P2.07 / 317–325
https://doi.org/10.26493/1855-3974.2126.5b3
(Also available at http://amc-journal.eu)

The automorphism group of the zero-divisor digraph of matrices over an antiring

David Dolžan *
Faculty of Mathematics and Physics, University of Ljubljana, Jadranska 21, 1000 Ljubljana, Slovenia and *IMFM, Jadranska 19, 1000 Ljubljana, Slovenia*

Gabriel Verret
Department of Mathematics, University of Auckland, Private Bag 92019, Auckland 1142, New Zealand

Received 26 September 2019, accepted 29 May 2023, published online 3 October 2023

Abstract

We determine the automorphism group of the zero-divisor digraph of the semiring of matrices over an antinegative commutative semiring with a finite number of zero-divisors.

Keywords: Automorphism group of a graph, zero-divisor graph, semiring.

Math. Subj. Class. (2020): 05C60, 16Y60, 05C25

1 Introduction

In recent years, the zero-divisor graphs of various algebraic structures have received a lot of attention, since they are a useful tool for revealing the algebraic properties through their graph-theoretical properties. In 1988, Beck [3] first introduced the concept of the zero-divisor graph of a commutative ring. In 1999, Anderson and Livingston [1] made a slightly different definition of the zero-divisor graph in order to be able to investigate the zero-divisor structure of commutative rings. In 2002, Redmond [15] extended this definition to also include non-commutative rings. Different authors then further extended this concept to semigroups [6], nearrings [4] and semirings [8].

Automorphisms of graphs play an important role both in graph theory and in algebra, and finding the automorphism group of certain graphs is often very difficult. Recently, a

*Corresponding author. The author acknowledges the financial support from the Slovenian Research Agency (research core funding no. P1-0222).

E-mail addresses: david.dolzan@fmf.uni-lj.si (David Dolžan), g.verret@auckland.ac.nz (Gabriel Verret)

lot of effort has been made to determine the automorphism group of various zero-divisor graphs. In [1], Anderson and Livingston proved that $\mathrm{Aut}(\Gamma(\mathbb{Z}_n))$ is a direct product of symmetric groups for $n \geq 4$ a non-prime integer. In the non-commutative case, the case of matrix rings and semirings is especially interesting. Thus, it was shown in [10] that, when p is a prime, $\mathrm{Aut}(\Gamma(\mathrm{M}_2(\mathbb{Z}_p)))$ is isomorphic to $\mathrm{Sym}(p+1)$, the symmetric group of degree $p+1$. More generally, it was proved in [13], that $\mathrm{Aut}(\Gamma(\mathrm{M}_2(\mathbb{F}_q))) \cong \mathrm{Sym}(q+1)$. In [18], the authors determined the automorphism group of the zero-divisor graph of all rank one upper triangular matrices over a finite field, and in [16] they determined the automorphism group of the zero-divisor graph of the matrix ring of all upper triangular matrices over a finite field. Recently, the automorphism group of the zero-divisor graph of the complete matrix ring of matrices over a finite field has been found independently in [17] and [20].

In this paper, we study the zero-divisor graph of matrices over commutative semirings. The theory of semirings has many applications in optimization theory, automatic control, models of discrete event networks and graph theory (see e.g. [2, 5, 12, 19]) and the zero-divisor graphs of semirings were recently studied in [9, 7, 14]. For an extensive theory of semirings, we refer the reader to [11]. There are many natural examples of commutative semirings, for example, the set of nonnegative integers (or reals) with the usual operations of addition and multiplication. Other examples include distributive lattices, tropical semirings, dioïds, fuzzy algebras, inclines and bottleneck algebras.

The theory of matrices over semirings differs quite substantially from the one over rings, so the methods we use are necessarily distinct from those used in the ring setting. The main result of this paper is the determination of the automorphism group of the zero-divisor digraph of a semiring of matrices over an antinegative commutative semiring with a finite number of zero-divisors (see Theorem 3.12).

2 Definitions and preliminaries

2.1 Digraphs

A *digraph* Γ consists of a set $\mathrm{V}(\Gamma)$ of *vertices*, together with a binary relation $\to$ on $\mathrm{V}(\Gamma)$. An *automorphism* σ of Γ is a permutation of $\mathrm{V}(\Gamma)$ such that $u \to v \iff \sigma(u) \to \sigma(v)$. The automorphisms of Γ form its *automorphism group* $\mathrm{Aut}(\Gamma)$.

Let Γ be a digraph and let $v \in \mathrm{V}(\Gamma)$. We write $\mathrm{N}^-(v) = \{u \in \mathrm{V}(\Gamma) \colon u \to v\}$ and $\mathrm{N}^+(v) = \{u \in \mathrm{V}(\Gamma) \colon v \to u\}$. If, for $u, v \in \mathrm{V}(\Gamma)$, we have $\mathrm{N}^-(u) = \mathrm{N}^-(v)$ and $\mathrm{N}^+(u) = \mathrm{N}^+(v)$, then we say u and v are *twin* vertices. The relation $\sim$ on $\mathrm{V}(\Gamma)$, defined by $u \sim v$ if and only if u and v are twin vertices, is clearly an equivalence relation preserved by $\mathrm{Aut}(\Gamma)$. For $v \in \mathrm{V}(\Gamma)$, we shall denote by $\overline{v}$ the $\sim$-equivalence class of v. Let $\overline{\Gamma}$ be the graph with these equivalence classes as vertices and $\overline{u} \to_{\overline{\Gamma}} \overline{v}$ if and only if $u \to_\Gamma v$. For $\sigma \in \mathrm{Aut}(\Gamma)$ we denote by $\overline{\sigma}$ the induced automorphism of $\overline{\Gamma}$. An automorphism $\sigma \in \mathrm{Aut}(\Gamma)$ is called *regular* if $\overline{\sigma}$ is the identity map.

2.2 Semirings

A *semiring* is a set S equipped with binary operations $+$ and $\cdot$ such that $(S, +)$ is a commutative monoid with identity element 0, and $(S, \cdot)$ is a semigroup. Moreover, the operations $+$ and $\cdot$ are connected by distributivity and 0 annihilates S.

A semiring S is *commutative* if $ab = ba$ for all $a, b \in S$, and *antinegative* if, for all $a, b \in S$, $a + b = 0$ implies that $a = 0$ or $b = 0$. Antinegative semirings are also called

zerosum-free semirings or *antirings*. The smallest nontrivial example of an antiring is the *Boolean antiring* $\mathbb{B} = \{0, 1\}$ with addition and multiplication defined so that $1 + 1 = 1 \cdot 1 = 1$.

Let S be a semiring. For $x \in S$, we define the *left and right annihilators in* S by $\mathrm{Ann}_L(x) = \{y \in S \colon yx = 0\}$ and $\mathrm{Ann}_R(x) = \{y \in S \colon xy = 0\}$. If S is commutative, we simply write $\mathrm{Ann}(x)$ for $\mathrm{Ann}_L(x) = \mathrm{Ann}_R(x)$. We denote by $\mathrm{Z}(S)$ the set of *zero-divisors* of S, that is $\mathrm{Z}(S) = \{x \in S \colon \exists y \in S \setminus \{0\}$ such that $xy = 0$ or $yx = 0\}$. The *zero-divisor digraph* $\Gamma(S)$ of S is the digraph with vertex-set S and $u \to v$ if and only if $uv = 0$.

It is easy to see that if $n \geq 1$ and S is a semiring, then the set $\mathrm{M}_n(S)$ of $n \times n$ matrices forms a semiring with respect to matrix addition and multiplication. If S is antinegative, then so is $\mathrm{M}_n(S)$. If S has an identity 1, let $E_{ij} \in \mathrm{M}_n(S)$ with entry 1 in position (i, j), and 0 elsewhere. For $s \in S$, define $sE_{ij} \in \mathrm{M}_n(S)$ as the matrix with entry s in position (i, j), and 0 elsewhere.

3 The automorphisms of the zero-divisor digraph

The following fact will be used repeatedly.

Lemma 3.1. *Let S be a semiring. If $A, B \in S$ and $\sigma \in \mathrm{Aut}(\Gamma(S))$, then*

$$\sigma(\mathrm{Ann}_L(A)) = \mathrm{Ann}_L(\sigma(A)) \quad \textit{and} \quad \sigma(\mathrm{Ann}_R(A)) = \mathrm{Ann}_R(\sigma(A)).$$

Proof. We have

$$\begin{aligned} X \in \sigma(\mathrm{Ann}_L(A)) &\iff \sigma^{-1}(X) \in \mathrm{Ann}_L(A) \\ &\iff \sigma^{-1}(X)A = 0 \\ &\iff X\sigma(A) = 0 \\ &\iff X \in \mathrm{Ann}_L(\sigma(A)). \end{aligned}$$

The proof of the second part is analogous. □

Lemma 3.2. *Let S be an antiring and let $\Gamma = \Gamma(S)$. If $A, B \in S$ and $\sigma \in \mathrm{Aut}(\Gamma)$, then $\sigma(A + B)$ and $\sigma(A) + \sigma(B)$ are twin vertices and, in particular, $\overline{\sigma(A + B)} = \overline{\sigma(A) + \sigma(B)}$.*

Proof. Using antinegativity, we have

$$\begin{aligned} X \in \mathrm{Ann}_L(\sigma(A + B)) &\iff X\sigma(A + B) = 0 \\ &\iff \sigma^{-1}(X)(A + B) = 0 \\ &\iff \sigma^{-1}(X)A = \sigma^{-1}(X)B = 0 \\ &\iff X\sigma(A) = X\sigma(B) = 0 \\ &\iff X(\sigma(A) + \sigma(B)) = 0 \\ &\iff X \in \mathrm{Ann}_L(\sigma(A) + \sigma(B)). \end{aligned}$$

We have proved that $\mathrm{Ann}_L(\sigma(A+B)) = \mathrm{Ann}_L(\sigma(A)+\sigma(B))$. An analogous proof yields $\mathrm{Ann}_R(\sigma(A+B)) = \mathrm{Ann}_R(\sigma(A)+\sigma(B))$. This implies that $\sigma(A+B)$ and $\sigma(A)+\sigma(B)$ are twin vertices. □

Definition 3.3. Let S be a commutative semiring, let $n \in \mathbb{N}$ and let $A \in \mathrm{M}_n(S)$ with (i,j) entry a_{ij}. For every $i,j \in \{1,\dots,n\}$, we define $C_i(A) = \bigcap_{k=1}^n \mathrm{Ann}(a_{ki})$ and $R_j(A) = \bigcap_{k=1}^n \mathrm{Ann}(a_{jk})$. Let $\mathcal{A}_R(A) := (C_1(A),\dots,C_n(A)) \in \mathcal{P}(S)^n$ and $\mathcal{A}_L(A) := (R_1(A),\dots,R_n(A)) \in \mathcal{P}(S)^n$, where $\mathcal{P}(S)$ denotes the power set of S.

The next theorem characterizes the twin vertices of $\Gamma(\mathrm{M}_n(S))$.

Theorem 3.4. *Let S be a commutative antiring, let $n \in \mathbb{N}$ and let $A, B \in \mathrm{M}_n(S)$. Then A and B are twin vertices of $\Gamma(\mathrm{M}_n(S))$ if and only if $\mathcal{A}_L(A) = \mathcal{A}_L(B)$ and $\mathcal{A}_R(A) = \mathcal{A}_R(B)$.*

Proof. Let a_{ij} and b_{ij} be the (i,j) entry of A and B, respectively. Suppose first that A and B are twin vertices of $\Gamma(\mathrm{M}_n(S))$ and assume that $\mathcal{A}_R(A) \neq \mathcal{A}_R(B)$. This implies that, for some $i \in \{1,\dots,n\}$, we have $C_i(A) \neq C_i(B)$. Swapping the role of A and B if necessary, there exists $s \in S$ such that $s \in C_i(A)$ and $s \notin C_i(B)$. Therefore, there exists $k \in \{1,\dots,n\}$ such that $s \notin \mathrm{Ann}(b_{ki})$. Now, let $C = sE_{ik} \in \mathrm{M}_n(S)$ and observe that $AC = 0$ but $BC \neq 0$, so $\mathrm{N}^+(A) \neq \mathrm{N}^+(B)$, which is a contradiction with the fact that A and B are twin vertices. We have thus proved that $\mathcal{A}_R(A) = \mathcal{A}_R(B)$. A similar argument yields that $\mathcal{A}_L(A) = \mathcal{A}_L(B)$.

Conversely, assume now that $\mathcal{A}_L(A) = \mathcal{A}_L(B)$ and $\mathcal{A}_R(A) = \mathcal{A}_R(B)$. Suppose there exists $X \in \mathrm{M}_n(S)$ such that $AX = 0$. Therefore, for all $i,j \in \{1,\dots,n\}$ we have $\sum_{k=1}^n a_{ik}x_{kj} = 0$. Since S is an antiring, this further implies that $a_{ik}x_{kj} = 0$ for all $i,j,k \in \{1,\dots,n\}$. So, $x_{kj} \in \mathrm{Ann}(a_{ik})$ and therefore $x_{kj} \in C_k(A) = C_k(B)$ for all $k \in \{1,\dots,n\}$. Thus, for all $i,j,k \in \{1,\dots,n\}$, we have $x_{kj} \in \mathrm{Ann}(b_{ik})$. This yields $b_{ik}x_{kj} = 0$ for all $i,j,k \in \{1,\dots,n\}$, so $BX = 0$. Thus, we have proved that $\mathrm{N}^+(A) \subseteq \mathrm{N}^+(B)$. By swapping the roles of A in B we also get $\mathrm{N}^+(B) \subseteq \mathrm{N}^+(A)$, so $\mathrm{N}^+(A) = \mathrm{N}^+(B)$. A similar argument yields that $\mathrm{N}^-(A) = \mathrm{N}^-(B)$, thus A and B are twin vertices. □

Definition 3.5. Let S be a commutative semiring and let $\alpha \in S \setminus \mathrm{Z}(S)$. We say that $\alpha = e_1 + e_2 + \cdots + e_s$ such that $e_i \neq 0$ for all i and $e_ie_j = 0$ for all $i \neq j$ is *a decomposition of α of length s*. The *length* $\ell(\alpha)$ of α is the supremum of the length of a decomposition of α (note that $\ell(\alpha)$ can be infinite). We say that α is of *maximal length* if $\ell(\alpha) \geq \ell(\beta)$ for all $\beta \in S \setminus \mathrm{Z}(S)$.

A semiring S is *decomposable* if $S \setminus Z(S)$ contains an element of length at least 2, otherwise it is *indecomposable*.

Lemma 3.6. *Let S be a commutative antiring and let $\alpha \in S \setminus \mathrm{Z}(S)$ be of finite maximal length s with decomposition $\alpha = e_1 + e_2 + \cdots + e_s$. Then, for every $i \in \{1,\dots,s\}$, the subsemiring e_iS is indecomposable.*

Proof. Suppose that e_iS is decomposable for some $i \in \{1,\dots,s\}$, say $i = 1$ without loss of generality. By definition, there exists $e_1w \in e_1S \setminus \mathrm{Z}(e_1S)$ such that $e_1w = f_1 + f_2$, where $f_1, f_2 \in e_1S \setminus \{0\}$ and $f_1f_2 = 0$. For all $j \neq 1$, we have $e_je_1w = 0$ and thus $e_jf_1 = e_jf_2 = 0$ by antinegativity. Let $\beta = e_1w + e_2 + \cdots + e_s$.

Suppose that $\beta x = 0$ for some $x \in S$. By antinegativity, we have $(e_1w)(e_1x) = 0$ and $e_2x = \cdots = e_sx = 0$. Since e_1w is not a zero-divisor in e_1S this implies that $e_1x = 0$ and therefore also $\alpha x = 0$. However, α is not a zero-divisor, so we can conclude that $x = 0$.

This shows that $\beta = f_1 + f_2 + e_2 + \cdots + e_s$ is not a zero-divisor in S, which is a contradiction with the maximal length of α. □

We shall investigate commutative antirings with identity where 1 is an element of finite maximal length. The next lemma shows that in this case, we can study the automorphisms of the zero-divisor digraph of the matrix ring componentwise.

Lemma 3.7. *Let S be a commutative antiring and suppose $1 \in S$ is of finite maximal length s with decomposition $1 = e_1 + e_2 + \cdots + e_s$. Let $n \in \mathbb{N}$ and $\sigma \in \mathrm{Aut}(\Gamma(\mathrm{M}_n(S)))$. Then there exists $\omega \in \mathrm{Sym}(s)$ such that, for every $r \in \{1, \ldots, s\}$, we have $\sigma(e_r \mathrm{M}_n(S)) = e_{\omega(r)}\mathrm{M}_n(S)$.*

Proof. Let $r \in \{1, \ldots, s\}$, let $i, j \in \{1, \ldots, n\}$ and let $B = \sigma(e_r E_{ij})$. So, $\overline{\sigma(e_r E_{ij})} = \overline{\sum_{k=1}^{s} e_k B}$. By Lemma 3.2, we have $\overline{e_r E_{ij}} = \overline{\sum_{k=1}^{s} \sigma^{-1}(e_k B)}$. Since S is antinegative, for every $k \in \{1, \ldots, s\}$, there exists $f_k \in S$ such that $\sigma^{-1}(e_k B) = f_k E_{ij}$. Since $f_k = f_k(e_1 + e_2 + \cdots + e_s) = f_k e_r \in e_r S$, we have $\sum_{k=1}^{s} f_k = e_r z$ for $z = \sum_{k=1}^{s} f_k$. Observe that $\overline{e_r E_{ij}} = \overline{z E_{ij}}$ yields $z \in S \setminus \mathrm{Z}(S)$.

Let $k, k' \in \{1, \ldots, s\}$. We have $\mathrm{Ann}_L(f_k E_{ij}), \mathrm{Ann}_L(f_{k'} E_{ij}) \subseteq \mathrm{Ann}_L(f_k f_{k'} E_{ij})$ hence $\mathrm{Ann}_L(e_k B), \mathrm{Ann}_L(e_{k'} B) \subseteq \mathrm{Ann}_L(\sigma(f_k f_{k'} E_{ij}))$. If $k \neq k'$, then $\mathrm{M}_n(S) \subseteq \mathrm{Ann}_L(e_k B) + \mathrm{Ann}_L(e_{k'} B)$, which is possible only if $f_k f_{k'} = 0$. We have shown that $f_k f_{k'} = 0$ for every $k, k' \in \{1, \ldots, s\}$ with $k \neq k'$.

It follows that

$$z = (e_1 + e_2 + \cdots + e_s)z = \sum_{i \neq r} e_i z + \sum_{k=1}^{s} f_k$$

is a decomposition of z. Since $z \notin \mathrm{Z}(S)$, $e_i z \neq 0$ and, since $\ell(z) \leq \ell(1) = s$, it follows that all but exactly one of the f_k's are 0. This implies that all but one of the $e_k B$'s are 0 and there exists $k \in \{1, \ldots, s\}$ such that $\overline{\sigma(e_r E_{ij})} = \overline{e_k B}$. This shows the existence of a permutation $\omega \in \mathrm{Sym}(s)$ such that $\overline{\sigma(e_r E_{ij})} = \overline{e_{\omega(r)} B}$.

Let $t \in \{1, \ldots, n\}$. We have $e_r^2 = e_r \neq 0$, so $e_r E_{ij} e_r E_{jt} \neq 0$ and $\overline{(e_{\omega(r)} B)\sigma(e_r E_{jt})} \neq 0$. This implies $\overline{\sigma(e_r E_{jt})} \in \overline{e_{\omega(r)} \mathrm{M}_n(S)}$.

As this holds for all $j, t \in \{1, \ldots, n\}$ and for any $A \in \mathrm{M}_n(S)$, we have $A = (e_1 + e_2 + \cdots + e_s)A$, we have $\overline{\sigma(e_r \mathrm{M}_n(S))} \subseteq \overline{e_{\omega(r)} \mathrm{M}_n(S)}$. By the same token, we can conclude that a twin vertex to a vertex from $e_r \mathrm{M}_n(S)$ is itself in $e_r \mathrm{M}_n(S)$, therefore also $\sigma(e_r \mathrm{M}_n(S)) \subseteq e_{\omega(r)} \mathrm{M}_n(S)$. Since σ is a bijection, $\sigma(e_r \mathrm{M}_n(S)) = e_{\omega(r)} \mathrm{M}_n(S)$. □

We next focus on the automorphisms restricted to the matrices over indecomposable subsemirings.

Proposition 3.8. *Let S be a commutative antiring and suppose $1 \in S$ is of finite maximal length s with decomposition $1 = e_1 + e_2 + \cdots + e_s$. Let $u, v \in \{1, \ldots, s\}$, $S_1 = e_u S$ and $S_2 = e_v S$. Let $n \in \mathbb{N}$ and $\sigma \in \mathrm{Aut}(\Gamma(\mathrm{M}_n(S)))$ such that $\sigma(\mathrm{M}_n(S_1)) = \mathrm{M}_n(S_2)$. If $i, j \in \{1, \ldots, n\}$, then there exist $y \in S_2 \setminus \mathrm{Z}(S_2)$ and $k, \ell \in \{1, \ldots, n\}$ such that $\sigma(e_u E_{ij}) = y E_{k\ell}$.*

Proof. Write $\sigma(e_u E_{ij}) = \sum_{k,\ell} \beta_{k\ell} E_{k\ell}$. Let $A_{k\ell} = \sigma^{-1}(\beta_{k\ell} E_{k\ell})$. By Lemma 3.2, $\sigma(e_u E_{ij})$ and $\sigma\left(\sum_{k,\ell} A_{k\ell}\right)$ are twin vertices, therefore $e_u E_{ij}$ and $\sum_{k,\ell} A_{k\ell}$ are twin vertices as well. Now, twin vertices of $e_u E_{ij}$ must be of the form $z E_{ij}$, so $\sum_{k,\ell} A_{k\ell} = z E_{ij}$ for some $z \in S$. Since $z = z(e_1 + e_2 + \cdots + e_s)$, we conclude that $z \in S_1$. Note also

that z is not a zero-divisor in S_1, since e_uE_{ij} and zE_{ij} are twin vertices. Since S is antinegative, we can conclude that, for all $k, \ell \in \{1, \dots, n\}$, there exist $\alpha_{k\ell} \in S_1$ such that $A_{k\ell} = \alpha_{k\ell}E_{ij}$ and $\sum_{k,\ell} \alpha_{k\ell} = z$.

Let $k, k', \ell, \ell' \in \{1, \dots, n\}$ with $(k, \ell) \neq (k', \ell')$. Now, we either have $k \neq k'$ or $\ell \neq \ell'$. Suppose first that $k \neq k'$. Since S is commutative, we have $\mathrm{Ann}_L(A_{k\ell}) = \mathrm{Ann}_L(\alpha_{k\ell}E_{ij}) \subseteq \mathrm{Ann}_L(\alpha_{k\ell}\alpha_{k'\ell'}E_{ij})$. By Lemma 3.1, this implies $\mathrm{Ann}_L(\beta_{k\ell}E_{k\ell}) \subseteq \mathrm{Ann}_L(\sigma(\alpha_{k\ell}\alpha_{k'\ell'}E_{ij}))$. Similarly, we have $\mathrm{Ann}_L(\beta_{k'\ell'}E_{k'\ell'}) \subseteq \mathrm{Ann}_L(\sigma(\alpha_{k\ell}\alpha_{k'\ell'}E_{ij}))$. Since $k \neq k'$, $\mathrm{M}_n(S) = \mathrm{Ann}_L(\beta_{k\ell}E_{k\ell}) + \mathrm{Ann}_L(\beta_{k'\ell'}E_{k'\ell'}) \subseteq \mathrm{Ann}_L(\sigma(\alpha_{k\ell}\alpha_{k'\ell'}E_{ij}))$, which implies $\sigma(\alpha_{k\ell}\alpha_{k'\ell'}E_{ij}) = 0$ and thus $\alpha_{k\ell}\alpha_{k'\ell'} = 0$. If $\ell \neq \ell'$, we arrive at the same conclusion by using right annihilators, namely that distinct $\alpha_{k\ell}$'s annihilate each other. Since S_1 is indecomposable by Lemma 3.6, the sum $\sum_{k,\ell} \alpha_{k\ell} = z$ has at most one non-zero summand. It follows that there is at most one non-zero $A_{k\ell}$ and at most one non-zero $\beta_{k\ell}E_{k\ell}$. This concludes the proof of the first part, with $y = \beta_{k\ell}$.

It remains to show that $y \notin \mathrm{Z}(S_2)$. Suppose, on the contrary, that $y \in \mathrm{Z}(S_2)$. By the first part of the result, there exist $y' \in S_1$ and $i', j' \in \{1, \dots, n\}$ such that $\sigma^{-1}(e_vE_{k\ell}) = y'E_{i'j'}$. Since $y \in \mathrm{Z}(S_2)$, we have $\mathrm{Ann}_L(e_vE_{k\ell}) \subsetneq \mathrm{Ann}_L(yE_{k\ell})$ and $\mathrm{Ann}_R(e_vE_{k\ell}) \subsetneq \mathrm{Ann}_R(yE_{k\ell})$. By Lemma 3.1, it follows that $\mathrm{Ann}_L(y'E_{i'j'}) \subsetneq \mathrm{Ann}_L(e_uE_{ij})$ and of course also $\mathrm{Ann}_R(y'E_{i'j'}) \subsetneq \mathrm{Ann}_R(e_uE_{ij})$. This is only possible if $i = i'$ and $j = j'$ which implies $\mathrm{Ann}_L(y'E_{ij}) \subsetneq \mathrm{Ann}_L(e_uE_{ij})$, a contradiction. □

Lemma 3.9. *Let S be a commutative antiring and suppose $1 \in S$ is of finite maximal length s with decomposition $1 = e_1 + e_2 + \cdots + e_s$. Let $u, v \in \{1, \dots, s\}$, $S_1 = e_uS$ and $S_2 = e_vS$. Let $n \in \mathbb{N}$ and $\sigma \in \mathrm{Aut}(\Gamma(\mathrm{M}_n(S)))$ such that $\sigma(\mathrm{M}_n(S_1)) = \mathrm{M}_n(S_2)$. If $x \in \mathrm{Z}(S_1)$ and $i, j \in \{1, \dots, n\}$, then there exist $z \in \mathrm{Z}(S_2)$ and $k, \ell \in \{1, \dots, n\}$ such that $\sigma(xE_{ij}) = zE_{k\ell}$.*

Proof. By Proposition 3.8, we know that $\sigma(e_uE_{ij}) = yE_{k\ell}$ for some $y \notin \mathrm{Z}(S_2)$ and $k, \ell \in \{1, \dots, n\}$. Since $x \in \mathrm{Z}(S_1)$, we have $\mathrm{Ann}_L(e_uE_{ij}) \subsetneq \mathrm{Ann}_L(xE_{ij})$ and $\mathrm{Ann}_R(e_uE_{ij}) \subsetneq \mathrm{Ann}_R(xE_{ij})$. By Lemma 3.1, it follows that $\mathrm{Ann}_L(yE_{k\ell}) \subsetneq \mathrm{Ann}_L(\sigma(xE_{ij}))$ and also $\mathrm{Ann}_R(yE_{k\ell}) \subsetneq \mathrm{Ann}_R(\sigma(xE_{ij}))$. This implies that all entries of $\sigma(xE_{ij})$ are zeros except entry (k, ℓ), so $\sigma(xE_{ij}) = zE_{k\ell}$ for some $z \in S_2$. Because $\mathrm{Ann}_L(yE_{k\ell}) \neq \mathrm{Ann}_L(\sigma(xE_{ij})) = \mathrm{Ann}_L(zE_{k\ell})$ and $\mathrm{Ann}_R(yE_{k\ell}) \neq \mathrm{Ann}_R(\sigma(xE_{ij})) = \mathrm{Ann}_R(zE_{k\ell})$, we must have $z \in \mathrm{Z}(S_2)$. □

Lemma 3.10. *Let S be a commutative antiring and suppose $1 \in S$ is of finite maximal length s with decomposition $1 = e_1 + e_2 + \cdots + e_s$. Let $u, v \in \{1, \dots, s\}$, $S_1 = e_uS$ and $S_2 = e_vS$. Let $n \in \mathbb{N}$ and $\sigma \in \mathrm{Aut}(\Gamma(\mathrm{M}_n(S)))$ such that $\sigma(\mathrm{M}_n(S_1)) = \mathrm{M}_n(S_2)$. Then there exists $\pi \in \mathrm{Sym}(n)$ such that $\overline{\sigma(e_uE_{ij})} = \overline{e_vE_{\pi(i)\pi(j)}}$ for all $i, j \in \{1, \dots, n\}$.*

Proof. Let $i, j, j' \in \{1, \dots, n\}$ with $j \neq j'$. By Proposition 3.8, there exist $k, k', \ell, \ell' \in \{1, \dots, n\}$ such that $\overline{\sigma(e_uE_{ij})} = \overline{e_vE_{k\ell}}$ and $\overline{\sigma(e_uE_{ij'})} = \overline{e_vE_{k'\ell'}}$. For all $r, s \in \{1, \dots, n\}$ with $s \neq i$, we have $e_uE_{rs}(e_uE_{ij} + e_uE_{ij'}) = 0$. By Lemma 3.2, this implies that $\overline{\sigma(e_uE_{rs})(e_uE_{k\ell} + e_uE_{k'\ell'})} = 0$ and thus $\overline{\left(\sum_{r,s\neq i} \sigma(e_uE_{rs})\right)(e_uE_{k\ell} + e_uE_{k'\ell'})} = 0$. By Proposition 3.8, $\overline{\sigma(e_uE_{rs})} = \overline{e_vE_{r's'}}$ for some $r', s' \in \{1, \dots, n\}$. Since σ is a permutation, $\sum_{r,s\neq i} \sigma(e_uE_{rs})$ is a matrix with exactly n entries equal to 0. It follows that $k = k'$.

By the paragraph above, there exists $\pi \in \mathrm{Sym}(n)$ such that $\overline{\sigma(e_uE_{ab})} = \overline{e_vE_{\pi(a)c}}$, for some c. A similar argument yields that there exists a permutation such that $\overline{\sigma(e_uE_{ab})} =$

$\overline{e_v E_{c\pi'(b)}}$, for some c. However, for every $j,k \in \{1,\dots,n\}$ with $j \neq k$, we have $E_{jj}E_{kk} = 0$ and thus $E_{\pi(j)\pi'(j)}E_{\pi(k)\pi'(k)} = 0$. This implies that $\pi(k) \neq \pi'(j)$ for every $k \neq j$, so $\pi(j) = \pi'(j)$. Therefore $\pi' = \pi$. □

For $\pi \in \mathrm{Sym}(n)$ and $A \in \mathrm{M}_n(S)$, let $\theta_\pi(A)$ be the matrix obtained from A by applying the permutation π to its rows and columns. Note that θ_π induces a permutation of $\mathrm{M}_n(S)$.

Corollary 3.11. *Let S be a commutative antiring and suppose $1 \in S$ is of finite maximal length s with decomposition $1 = e_1+e_2+\cdots+e_s$. Let $u,v \in \{1,2,\dots,s\}$, $S_1 = e_uS$ and $S_2 = e_vS$. Let $n \in \mathbb{N}$ and $\sigma \in \mathrm{Aut}(\Gamma(\mathrm{M}_n(S)))$ such that $\sigma(\mathrm{M}_n(S_1)) = \mathrm{M}_n(S_2)$. Then there exist $\pi \in \mathrm{Sym}(n)$ and τ an isomorphism from $\Gamma(S_1)$ to $\Gamma(S_2)$ such that, if we extend τ entry-wise to a mapping $\mathrm{M}_n(S_1) \to \mathrm{M}_n(S_2)$ and restrict σ to $\mathrm{M}_n(S_1)$, then $\overline{\sigma} = \overline{\theta_\pi \circ \tau}$.*

Proof. By Lemma 3.10, there exists $\pi \in \mathrm{Sym}(n)$ such that $\overline{\sigma(e_uE_{ij})} = \overline{\theta_\pi(e_vE_{ij})}$ for all $i,j \in \{1,\dots,n\}$. Let $\rho = \theta_\pi^{-1} \circ \sigma$ and note that $\rho \in \mathrm{Aut}(\Gamma(\mathrm{M}_n(S)))$ and we have $\overline{\rho(e_uE_{ij})} = \overline{e_vE_{ij}}$ for all $i,j \in \{1,\dots,n\}$.

Let $x \in \mathrm{Z}(S_1)$ and $i,j,j' \in \{1,\dots,n\}$. Clearly, $\rho(\mathrm{M}_n(S_1)) = \mathrm{M}_n(S_2)$ so, by Lemma 3.9, there exist $z,z' \in \mathrm{Z}(S_2)$ such that $\rho(xE_{ij}) = zE_{ij}$ and $\rho(xE_{ij'}) = z'E_{ij'}$.

Let $X = \{s \in S_2; sz = 0\}$. We show that $X \subseteq \mathrm{Ann}(z')$. Let $a \in S_2$ such that $az = 0$. Note that $(aE_{ii})(zE_{ij}) = 0$. Since $a \in \mathrm{Z}(S_2)$, Lemma 3.9 implies that there exists $b \in \mathrm{Z}(S_1)$ such that $aE_{ii} = \rho(bE_{ii})$, hence $\rho(bE_{ii})\rho(xE_{ij}) = 0$ and therefore also $(bE_{ii})(xE_{ij}) = 0$ which implies $bx = 0$. It follows that $(bE_{ii})(xE_{ij'}) = 0$, $\rho(bE_{ii})\rho(xE_{ij'}) = 0$ and $(aE_{ii})(z'E_{ij'}) = 0$ which yields $az' = 0$.

We have shown that $X \subseteq \mathrm{Ann}(z')$. A symmetrical argument yields $\mathrm{Ann}(z') \subseteq X$ hence $X = \mathrm{Ann}(z')$ which implies that $\overline{\rho(xE_{ij'})} = \overline{z'E_{ij'}} = \overline{zE_{ij'}}$ (where for $A \in \mathrm{M}_n(S_2)$, by a slight abuse of notation, $\overline{A}$ now refers to the image in $\overline{\Gamma}(\mathrm{M}_n(S_2))$ and not in $\overline{\Gamma}(\mathrm{M}_n(S))$). A similar argument shows that $\overline{\rho(xE_{i'j})} = \overline{zE_{i'j}}$ for all $i' \in \{1,\dots,n\}$. This implies that $\overline{\rho(xE_{k\ell})} = \overline{zE_{k\ell}}$ for all $k,\ell \in \{1,\dots,n\}$.

Let τ denote the mapping $S_1 \to S_2$ that satisfies $\rho(xE_{11}) = \tau(x)E_{11}$. Since ρ is a bijection from $\mathrm{M}_n(S_1)$ to $\mathrm{M}_n(S_2)$, τ is a bijection from S_1 to S_2. If $x,y \in S_1$, then $xy = 0$ if and only if $(xE_{11})(yE_{11}) = 0$ if and only if $\tau(x)\tau(y) = 0$, therefore τ is an isomorphism from $\Gamma(S_1)$ to $\Gamma(S_2)$. Now, extend τ to an entry-wise mapping $\mathrm{M}_n(S_1) \to \mathrm{M}_n(S_2)$. Let $A = [a_{ij}], B = [b_{ij}] \in \mathrm{M}_n(S_1)$. Note that $AB = 0$ if and only if $\sum_{k=1}^n a_{ik}b_{kj} = 0$ for every $1 \leq i,j \leq n$ if and only if $a_{ik}b_{kj} = 0$ for every $1 \leq i,j,k \leq n$, so τ induces an isomorphism from $\Gamma(\mathrm{M}_n(S_1))$ to $\Gamma(\mathrm{M}_n(S_2))$. Observe that, restricted to $\mathrm{V}(\Gamma(\mathrm{M}_n(S_1)))$, we have $\overline{\rho} = \overline{\tau}$. As $\sigma = \theta_\pi \circ \rho$, this concludes the proof. □

We can now join these findings into the following theorem.

Theorem 3.12. *Let S be a commutative antiring and suppose $1 \in S$ is of finite maximal length s with decomposition $1 = e_1 + e_2 + \cdots + e_s$. Let $n \in \mathbb{N}$ and $\sigma \in \mathrm{Aut}(\Gamma(\mathrm{M}_n(S)))$. Then there exist $\omega \in \mathrm{Sym}(s)$ and, for every $i \in \{1,\dots,s\}$, there exist $\pi_i \in \mathrm{Sym}(n)$ and an isomorphism $\tau_i \colon \Gamma(e_iS) \to \Gamma(e_{\omega(i)}S)$ such that, if we extend τ_i entry-wise to a mapping $\mathrm{M}_n(e_iS) \to \mathrm{M}_n(e_{\omega(i)}S)$, then*

$$\overline{\sigma(A)} = \overline{\left(\sum_{i=1}^{s} (\theta_{\pi_i} \circ \tau_i)(e_iA)\right)} \text{ for all } A \in \mathrm{M}_n(S).$$

Conversely, if $\omega \in \mathrm{Sym}(s)$ has the property that, for every $i \in \{1, \dots, s\}$, we have $\Gamma(e_i S) \cong \Gamma(e_{\omega(i)} S)$, τ_i is an isomorphism from $\Gamma(e_i S)$ to $\Gamma(e_{\omega(i)} S)$ and $\pi_i \in \mathrm{Sym}(n)$, then σ defined with $\sigma(A) = \sum_{i=1}^{s} (\theta_{\pi_i} \circ \tau_i)(e_i A)$ is an automorphism of $\Gamma(\mathrm{M}_n(S))$.

Proof. By Lemma 3.7, there exists $\omega \in \mathrm{Sym}(s)$ such that, for every $i \in \{1, \dots, s\}$, we have $\sigma(e_i \mathrm{M}_n(S)) = e_{\omega(i)} \mathrm{M}_n(S)$.

By Corollary 3.11, there exist $\pi_i \in \mathrm{Sym}(n)$ and τ_i an isomorphism from $\Gamma(e_i S)$ to $\Gamma(e_{\omega(i)} S)$ such that, if we extend τ_i entry-wise to a mapping $\mathrm{M}_n(e_i S) \to \mathrm{M}_n(e_{\omega(i)} S)$ and restrict σ to $\mathrm{M}_n(e_i S)$, then $\overline{\sigma} = \overline{\theta_{\pi_i} \circ \tau_i}$.

Now, let $A \in \mathrm{M}_n(S)$. We have $\overline{A} = \overline{e_1 A + e_2 A + \cdots + e_s A}$ and the result follows by Lemma 3.2. □

Remark 3.13. Throughout the paper, we restricted ourselves to studying semirings with the property that no non-zero-divisor element can be written as a sum of infinitely many mutually orthogonal zero-divisors. Obviously, any semiring with a finite set of zero-divisors satisfies this condition.

ORCID iDs

David Dolžan https://orcid.org/0000-0001-6548-3945
Gabriel Verret https://orcid.org/0000-0003-1766-4834

References

[1] D. F. Anderson and P. S. Livingston, The zero-divisor graph of a commutative ring, *J. Algebra* **217** (1999), 434–447, doi:10.1006/jabr.1998.7840, https://doi.org/10.1006/jabr.1998.7840.

[2] F. Baccelli and J. Mairesse, Ergodic theorems for stochastic operators and discrete event networks, in: *Idempotency*, Cambridge University Press, Cambridge, pp. 171–208, 1998.

[3] I. Beck, Coloring of commutative rings, *J. Algebra* **116** (1988), 208–226, doi:10.1016/0021-8693(88)90202-5, https://doi.org/10.1016/0021-8693(88)90202-5.

[4] G. A. Cannon, K. M. Neuerburg and S. P. Redmond, Zero-divisor graphs of nearrings and semigroups, in: H. Kiechle, A. Kreuzer and M. Thomsen (eds.), *Nearrings and Nearfields*, Springer, Dordrecht, pp. 189–200, 2005.

[5] R. Cuninghame-Green, *Minimax Algebra*, volume 166, Springer Science & Business Media, 2012.

[6] F. R. DeMeyer, T. McKenzie and K. Schneider, The zero-divisor graph of a commutative semigroup, *Semigroup Forum* **65** (2002), 206–214, doi:10.1007/s002330010128, https://doi.org/10.1007/s002330010128.

[7] D. Dolžan and P. Oblak, The zero-divisor graphs of rings and semirings, *Int. J. Algebra Comput.* **22** (2012), 1250033, 20, doi:10.1142/s0218196712500336, https://doi.org/10.1142/s0218196712500336.

[8] S. Ebrahimi Atani, The zero-divisor graph with respect to ideals of a commutative semiring., *Glas. Mat., III. Ser.* **43** (2008), 309–320, doi:10.3336/gm.43.2.06, https://doi.org/10.3336/gm.43.2.06.

[9] S. Ebrahimi Atani, An ideal based zero-divisor graph of a commutative semiring., *Glas. Mat., III. Ser.* **44** (2009), 141–153, doi:10.3336/gm.44.1.07, https://doi.org/10.3336/gm.44.1.07.

[10] J. Han, The zero-divisor graph under group actions in a noncommutative ring, *J. Korean Math. Soc.* **45** (2008), 1647–1659, doi:10.4134/jkms.2008.45.6.1647, https://doi.org/10.4134/jkms.2008.45.6.1647.

[11] U. Hebisch and H. J. Weinert, *Semirings: Algebraic theory and Applications in Computer Science*, volume 5 of *Ser. Algebra*, World Scientific Publishing, Singapore, 1998.

[12] P. Li, A heuristic method to compute the approximate postinverses of a fuzzy matrix, *IEEE Trans. Fuzzy Syst.* **22** (2014), 1347–1351, doi:10.1109/tfuzz.2013.2282231, https://doi.org/10.1109/tfuzz.2013.2282231.

[13] S. Park and J. Han, The group of graph automorphisms over a matrix ring, *J. Korean Math. Soc.* **48** (2011), 301–309, doi:10.4134/jkms.2011.48.2.301, https://doi.org/10.4134/jkms.2011.48.2.301.

[14] A. Patil, B. N. Waphare and V. Joshi, Perfect zero-divisor graphs, *Discrete Math.* **340** (2017), 740–745, doi:10.1016/j.disc.2016.11.027, https://doi.org/10.1016/j.disc.2016.11.027.

[15] S. P. Redmond, The zero-divisor graph of a non-commutative ring, *Int. J. Commut. Rings* **1** (2002), 203–211.

[16] L. Wang, A note on automorphisms of the zero-divisor graph of upper triangular matrices., *Linear Algebra Appl.* **465** (2015), 214–220, doi:10.1016/j.laa.2014.09.035, https://doi.org/10.1016/j.laa.2014.09.035.

[17] L. Wang, Automorphisms of the zero-divisor graph of the ring of all $n \times n$ matrices over a finite field, *Discrete Math.* **339** (2016), 2036–2041, doi:10.1016/j.disc.2016.02.021, https://doi.org/10.1016/j.disc.2016.02.021.

[18] D. Wong, X. Ma and J. Zhou, The group of automorphisms of a zero-divisor graph based on rank one upper triangular matrices, *Linear Algebra Appl.* **460** (2014), 242–258, doi:10.1016/j.laa.2014.07.041, https://doi.org/10.1016/j.laa.2014.07.041.

[19] S. Zhao and X.-p. Wang, Invertible matrices and semilinear spaces over commutative semirings, *Inf. Sci.* **180** (2010), 5115–5124, doi:10.1016/j.ins.2010.08.033, https://doi.org/10.1016/j.ins.2010.08.033.

[20] J. Zhou, D. Wong and X. Ma, Automorphisms of the zero-divisor graph of the full matrix ring, *Linear Multilinear Algebra* **65** (2017), 991–1002, doi:10.1080/03081087.2016.1219302, https://doi.org/10.1080/03081087.2016.1219302.

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 24 (2024) #P2.08 / 327–346
https://doi.org/10.26493/1855-3974.2947.cd6
(Also available at http://amc-journal.eu)

Quotients of skew morphisms of cyclic groups

Martin Bachratý *

Faculty of Civil Engineering, Slovak University of Technology, Bratislava, Slovakia

Received 25 August 2022, accepted 19 April 2023, published online 4 October 2023

Abstract

A skew morphism of a finite group B is a permutation φ of B that preserves the identity element of B and has the property that for every $a \in B$ there exists a positive integer i_a such that $\varphi(ab) = \varphi(a)\varphi^{i_a}(b)$ for all $b \in B$. The problem of classifying skew morphisms for all finite cyclic groups is notoriously hard, with no such classification available up to date. Each skew morphism φ of $\mathbb{Z}_n$ is closely related to a specific skew morphism of $\mathbb{Z}_{|\langle\varphi\rangle|}$, called the quotient of φ. In this paper, we use this relationship and other observations to prove new theorems about skew morphisms of finite cyclic groups. In particular, we classify skew morphisms for all cyclic groups of order $2^e m$ with $e \in \{0, 1, 2, 3, 4\}$ and m odd and square-free. We also develop an algorithm for finding skew morphisms of cyclic groups, and implement this algorithm in MAGMA to obtain a census of all skew morphisms for cyclic groups of order up to 161.

During the preparation of this paper we noticed a few flaws in Section 5 of the paper Cyclic complements and skew morphisms of groups from 2016. We propose and prove weaker versions of the problematic original assertions (namely Lemma 5.3(b), Theorem 5.6 and Corollary 5.7), and show that our modifications can be used to fix all consequent proofs (in the aforementioned paper) that use at least one of those problematic assertions.

Keywords: Skew morphism, cyclic group, coset-preserving, quotient, square-free.

Math. Subj. Class. (2020): 20B25, 05C25, 05E18

1 Introduction

A skew morphism of a finite group B is a permutation φ of B that preserves the identity element of B and has the property that for every $a \in B$ there exists a positive integer i_a such that $\varphi(ab) = \varphi(a)\varphi^{i_a}(b)$ for all $b \in B$. The *order* of a skew morphism, denoted by

*The author acknowledges the use of the MAGMA system [7] to find examples of skew morphisms relevant to this paper. The author also acknowledges support from the APVV Research Grants 17-0428 and 19-0308, and the VEGA Research Grants 1/0206/20 and 1/0567/22.

E-mail address: martin.bachraty@stuba.sk (Martin Bachratý)

$\mathrm{ord}(\varphi)$, is defined as the order of the cyclic group $\langle\varphi\rangle$. Note that for each $a \in B$ there is a unique choice for i_a such that $i_a \in \{1, 2, \ldots, \mathrm{ord}(\varphi) - 1\}$ (unless φ is the identity permutation). The function π that maps each element $a \in B$ to this integer i_a is called the *power function* of φ, and it satisfies $\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b)$ for all $a, b \in B$. In the case when φ is the identity permutation of B, we define $\pi(a) = 1$ for all $a \in B$.

Skew morphisms were first introduced by Jajcay and Širáň in [18], with primary interest in their connection to the regular Cayley maps. Skew morphisms are also intriguing from a purely group-theoretical point of view, mainly due to their close relationship with group automorphisms, with which they share a number of important features. The problem of classifying all skew morphisms for given families of finite groups has gained much attention in the last two decades; see [8, 10, 23, 24] for example. Recently, in [4], skew morphisms were classified for all finite simple groups, and we understand that a classification for dihedral groups is imminent; see [19]. On the other hand, the problem of finding all skew morphisms for finite cyclic groups remains open, despite recent positive progress, which we discuss next.

Automorphisms of a finite group B are special cases of skew morphisms (with $\pi(a) = 1$ for all $a \in B$), and as such can be viewed as an important family of skew morphisms. There are also other intriguing families of skew morphisms, for example, *coset-preserving* (sometimes also called *smooth*) skew morphisms, which are defined as skew morphisms satisfying $\pi(a) = \pi(\varphi(a))$ for all $a \in B$. Coset-preserving skew morphisms have been fully classified for all finite cyclic groups in [6]. Another interesting family of skew morphisms that is fully understood for finite cyclic groups consists of all skew morphisms φ such that φ^2 is an automorphism of the same group; see [16].

While there is no classification of skew morphisms of finite cyclic groups available to date, skew morphisms have been fully classified for some specific (infinite) families of finite cyclic groups. Most notably, this was done for cases where the order of a cyclic group is a prime [18] (in this case, all skew morphisms are automorphisms), a product of two distinct primes [20], and any power of an odd prime [21]. Some partial progress for cyclic 2-groups can be found in [14].

Another approach for studying skew morphisms of finite cyclic groups is to find a connection between skew morphisms of a given cyclic group B and skew morphisms of cyclic groups of smaller orders. Presumably the strongest finding to date made in this direction is the observation of Kovács and Nedela proved in [20] which states that if $\gcd(m, n) = \gcd(m, \phi(n)) = \gcd(\phi(m), n) = 1$, then the skew morphisms of $\mathbb{Z}_{mn}$ are exactly the direct products of skew morphisms of $\mathbb{Z}_m$ and $\mathbb{Z}_n$. There is also a useful connection between general skew morphisms and coset-preserving skew morphisms for finite cyclic groups. Namely, for each skew morphism φ of a finite cyclic group B there exists an exponent e such that φ^e is a non-trivial coset-preserving skew morphism of B; see [5].

In this paper, we combine a number of known facts about skew morphisms (which we summarise in Sections 2 and 3) with new observations presented in Section 4, to prove a number of theorems about skew morphisms of cyclic groups. Namely, in Section 5 we develop a new method for finding skew morphisms of cyclic groups, and implement it to obtain a census of all skew morphisms of cyclic groups of order up to 161. (Up to the time of writing this paper, and apart from some specific orders, skew morphisms of cyclic groups were known only up to order 60; see [9].) Further, in Section 6 we show that all skew morphisms of $\mathbb{Z}_n$ are coset-preserving if and only if $n = 2^e m$ for some $e \in \{0, 1, 2, 3, 4\}$

and m odd and square-free. As a consequence, we obtain a complete classification of skew morphisms for all cyclic groups of order expressible in this form, significantly expanding the list of finite cyclic groups for which such classification is available. During the review process, it was communicated to us that Kan Hu, István Kovács and Young Soo Kwon has recently submitted a paper devoted to similar ideas to those we investigated in Section 6 of this paper.

2 Preliminaries

In this section, we recall some definitions from group theory and provide some background from the theory of skew morphisms. All groups considered in this paper are assumed to be finite. For the cyclic group of order n we use the additive notation $\mathbb{Z}_n$, and so the elements of $\mathbb{Z}_n$ may be viewed as integers in the interval $[0, n-1]$. We also let $\mathrm{Sym}(G)$ denote the symmetric group on (the underlying set of) a group G.

The *core* of a subgroup H in a group G is the largest normal subgroup of H contained in G. We say that H is *core-free* in G if the core of H in G is trivial. A *complement* for H in G is a subgroup K of G such that $G = HK$ and $H \cap K = \{1\}$. The following theorem proved by Lucchini in [22] will be helpful.

Theorem 2.1 ([22])**.** *Let C be a cyclic proper subgroup of a group G. If C is core-free in G, then $|C| < |G : C|$.*

Next, let φ be a skew morphism of a group B, and identify B with the subgroup of $\mathrm{Sym}(B)$ which acts by left multiplication. Then it can be easily checked that $B\langle\varphi\rangle$ is a subgroup of $\mathrm{Sym}(B)$ (see [20] for example). Moreover, $B\langle\varphi\rangle$ is a complementary factorisation and $\langle\varphi\rangle$ is core-free in $B\langle\varphi\rangle$ (see [12, Lemma 4.1]). A group G containing B which has a cyclic core-free complement C for B is called a *skew product group* for a group B, and we say that C is a *skew complement* (for B in G). The skew product group $B\langle\varphi\rangle$ (for B) with skew complement $\langle\varphi\rangle$ described in this paragraph is said to be *induced* by φ.

Conversely, let G be a skew product group for a group B, and let c be a generator of a skew complement for B in G. Note that every element $g \in G$ is uniquely expressible in a form $g = ac'$ with $a \in B$ and $c' \in C$. Then for every $a \in B$ there exists a unique $a' \in B$ and a unique exponent $j \in \{1, 2, \ldots, |C| - 1\}$ such that $ca = a'c^j$, and this induces a bijection $\varphi\colon B \to B$ and a function $\pi\colon B \to \mathbb{N}$, defined by $\varphi(a) = a'$ and $\pi(a) = j$. It can be easily checked that φ is a skew morphism of B with power function π. We say that φ is *induced* by the pair (B, c).

Recall that if φ is a skew morphism of B with power function π, then we have $\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b)$ for all $a, b \in B$. (Hence, if $B = \mathbb{Z}_n$, then $\varphi(a+b) = \varphi(a) + \varphi^{\pi(a)}(b)$ for all $a, b \in \mathbb{Z}_n$.) Also recall that an automorphism of B is a skew morphism with $\pi(a) = 1$ for all $a \in B$. In what follows, it will be often convenient to distinguish between general skew morphisms and skew morphisms that are not automorphisms, and so we will refer to the latter as *proper* skew morphisms. We say that φ is *trivial* if it is the identity permutation of B. The *kernel* of φ, denoted by $\ker\varphi$, is the subset $\{a \in B \mid \pi(a) = 1\}$ of B. By definition, φ is an automorphism of B if and only if $\ker\varphi = B$. In the case of proper skew morphisms $\ker\varphi$ is not equal to B, but it is always a subgroup of B; see [18, Lemma 4].

Since $\ker\varphi$ is a subgroup of B and also $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in \ker\varphi$, it follows that φ restricts to a group isomorphism from the kernel to its image. In particular, if $\ker\varphi$ is preserved by φ set-wise, then φ restricts to an automorphism of $\ker\varphi$. In [11] this was shown to always be true for abelian groups. We also have the following.

Lemma 2.2 ([18]). *Let φ be a skew morphism of a group B with power function π. Then two elements $a, b \in B$ belong to the same right coset of the subgroup $\ker\varphi$ in B if and only if $\pi(a) = \pi(b)$.*

Theorem 2.3 ([12]). *Every skew morphism of a non-trivial group has non-trivial kernel.*

An immediate consequence of Theorem 2.3 is that every skew morphism of a group of prime order is an automorphism. The following facts about kernels of skew morphisms will be useful, too.

Lemma 2.4 ([12]). *Let G be a skew product group for a group B with skew complement C, and let c be a generator of C. If φ is the skew morphism induced by (B, c), then $\ker\varphi$ is the largest subgroup H of B for which $cHc^{-1} \subseteq B$. In particular, φ is an automorphism of B if and only if B is normal in G.*

Proposition 2.5 ([12]). *Let φ be a skew morphism of a group B, and let N be a subgroup of $\ker\varphi$ that is normal in B and preserved by φ. Then the mapping $\varphi_N^* : B/N \to B/N$ given by $\varphi_N^*(x) = N\varphi(x)$ is a well-defined skew morphism of B/N.*

Lemma 2.6 ([12]). *Let φ be a skew morphism of a finite abelian group A with power function π. Also suppose that N is any non-trivial subgroup of $\ker\varphi$ preserved by φ, let i be the exponent of N, and let φ_N^* be the skew morphism of A/N induced by φ. If a is an element of A such that Na lies in the kernel of φ_N^*, then $i\pi(a) \equiv i \pmod{\mathrm{ord}(\varphi)}$ and, in particular, if $\gcd(i, \mathrm{ord}(\varphi)) = 1$, then $a \in \ker\varphi$.*

Note that if φ is a skew morphism of $\mathbb{Z}_n$, then $\ker\varphi$ is normal in $\mathbb{Z}_n$ and φ restricts to an automorphism of $\ker\varphi$. Moreover, since $\mathbb{Z}_n$ is cyclic, so is (its subgroup) $\ker\varphi$. Noting that every automorphism of a cyclic group preserves all of its subgroups, we deduce that φ preserves all subgroups of $\ker\varphi$. Hence it follows from Proposition 2.5 that φ_N^* is a well defined skew morphism of $\mathbb{Z}_n/N$ for each subgroup N of $\ker\varphi$. In the case when $N = \ker\varphi$, we will write simply φ^* instead of φ_N^*.

We proceed with some useful facts about orders of skew morphisms.

Proposition 2.7 ([20]). *Let φ be a skew morphism of a group B, and let T be an orbit of $\langle\varphi\rangle$. If $\langle T\rangle = B$, then $\mathrm{ord}(\varphi) = |T|$.*

Theorem 2.8 ([12]). *The order of a skew morphism of a non-trivial group B is less than the order of B.*

Theorem 2.9 ([20]). *If φ is a skew morphism of a group $\mathbb{Z}_n$, then $\mathrm{ord}(\varphi)$ is a divisor of $n\phi(n)$. Moreover, if $\gcd(\mathrm{ord}(\varphi), n) = 1$, then φ is an automorphism of $\mathbb{Z}_n$.*

The *periodicity* of a skew morphism φ of a group B, denoted by p_φ, is the smallest positive integer such that $\pi(a) = \pi(\varphi^{p_\varphi}(a))$ for all $a \in B$. Similarly, the *periodicity* of $a \in B$ (with respect to φ) is the smallest positive integer p_a such that $\pi(a) = \pi(\varphi^{p_a}(a))$. Note that if $\ker\varphi$ is preserved by φ (which is always true if B is abelian), then the periodicity of φ can be defined equivalently as the order of φ^*.

Recall that φ is coset-preserving if $\pi(a) = \pi(\varphi(a))$ for all $a \in B$. Equivalently, coset-preserving skew morphisms can be viewed as skew morphism that preserves all right cosets of $\ker\varphi$ in B, or as skew morphisms with the periodicity equal to 1. The following theorem about periodicities underlines the importance of coset-preserving skew morphisms in the study of skew morphisms of abelian (and, in particular, cyclic) groups.

Theorem 2.10 ([5]). *If φ is a skew morphism of an abelian group A, then φ^{p_φ} is a coset-preserving skew morphism of A. Moreover, if A is cyclic, b is a generator of A, and φ is non-trivial, then $p_\varphi = p_b$ and $p_\varphi < \mathrm{ord}(\varphi)$.*

The following fact will be helpful too.

Lemma 2.11 ([12]). *Let φ be any skew morphism of a finite group G, and let H be any finite group. Then φ can be extended to a skew morphism θ of $G \times H$, such that $\theta \restriction_G = \varphi$ and $\ker\theta = \ker\varphi \times H$.*

We conclude this section with two well-known facts about skew morphisms that are easy exercises, but we include their proofs for completeness.

Lemma 2.12. *Let φ be a skew morphism of an abelian group A. If $\varphi(a) = a$ for some $a \in A$, then $a \in \ker\varphi$.*

Proof. Let a' be any element of A. Since a is fixed by φ, we have $\varphi(aa') = a\varphi^{\pi(a)}(a')$. On the other hand, we have $\varphi(aa') = \varphi(a'a) = \varphi(a')\varphi^{\pi(a')}(a) = \varphi(a')a$, and hence $\varphi(a') = \varphi^{\pi(a)}(a')$ for all $a' \in A$. It follows that $\pi(a) = 1$, and therefore $a \in \ker\varphi$. □

Lemma 2.13. *Let φ be a skew morphism of a group B with power function π, and let $a \in B$. Then:*

$$\varphi(a^i) = \varphi(a)\varphi^{\pi(a)}(a)\varphi^{\pi(a^2)}(a)\dots\varphi^{\pi(a^{i-1})}(a) \text{ for all } i \in \mathbb{N}.$$

Proof. The assertion is trivially true for $i = 1$. Next, if it holds for some positive integer j, then $\varphi(a^{j+1}) = \varphi(a^j a) = \varphi(a^j)\varphi^{\pi(a^j)}(a) = \varphi(a)\varphi^{\pi(a)}(a)\dots\varphi^{\pi(a^{j-1})}(a)\varphi^{\pi(a^j)}(a)$, and so it is also true for $j+1$. Hence the proof follows by induction. □

3 Skew morphisms of abelian groups

Several useful facts about skew morphisms of abelian groups (which we also apply in this paper) were proved in [12]. During the preparation of this paper, however, we noticed that three assertions in [12] do not hold. In this section, we list the incorrect findings and provide a counterexample for each of them. We also propose and prove weaker versions of the original statements. Finally, we discuss all proofs in [12] that use at least one of the flawed statements, and show that in all cases it is sufficient to replace the flawed statements by our modifications. For the rest of the section, we let φ be a skew morphism of an abelian group A with power function π. Also, to distinguish between references to this paper and references to [12], we put an asterisk after each numbered reference in the latter case.

The first flawed assertion in [12] is part (b) of Lemma 5.3*. It states that if N is a non-trivial subgroup of $\ker\varphi$ preserved by φ, and φ is not an automorphism of A, then $\mathrm{ord}(\varphi)$ has a non-trivial divisor in common with the exponent of N. To show that this is not true, note that according to [9] the cyclic group of order 12 admits a proper skew morphism ψ of order 3 with kernel (which is preserved by ψ) of order 6. Since $\ker\psi$ is cyclic and preserved by ψ, so is its unique subgroup of order 2. But the exponent of this subgroup, which is 2, does not have a non-trivial divisor in common with $\mathrm{ord}(\psi)$. We propose the following modification:

Lemma 3.1. *If φ is a proper skew morphism of an abelian group A, then $\mathrm{ord}(\varphi)$ has a non-trivial divisor in common with the exponent of $\ker\varphi$.*

Proof. Let $K = \ker\varphi$, let e be the exponent of K, and let L/K be the kernel of the skew morphism φ^* of A/K induced by φ. Since φ is proper we know that A/K is a non-trivial group, and by Theorem 2.3 it follows that L/K is non-trivial. In particular, there exists an element a of A such that $a \notin K$ and $a \in L$. It follows that $\pi(a) \not\equiv 1 \pmod{\mathrm{ord}(\varphi)}$, by Lemma 2.6 we have $e\pi(a) \equiv e \pmod{\mathrm{ord}(\varphi)}$, and the rest follows. □

Part (b) of Lemma 5.3* is used in the proofs of six theorems presented in [12]. Proofs of Theorem 5.4*, Theorem 5.10*, Theorem 6.2* and Theorem 6.4* are all easily fixable, since in each case Lemma 5.3(b)* is applied for $N = K$, and hence it is sufficient to replace it with Lemma 3.1. The proof of Theorem 6.1* can also be corrected. Here Lemma 5.3(b)* is used to show that if φ is proper and $A \cong \mathbb{Z}_n$, then $\gcd(\mathrm{ord}(\varphi), n) \neq 1$. Since A is cyclic, the exponent of $\ker\varphi$ is equal to the order of $\ker\varphi$ (which necessarily divides n), so this is an easy consequence of Lemma 3.1. Finally, since Theorem 7.3* was already proved previously in [20], there is no need to fix its alternative proof presented in [12]; although we believe that it is possible.

Another flawed assertion in [12] is Theorem 5.6*. It states that if $L/(\ker\varphi)$ is the kernel of the skew morphism φ^* of $A/(\ker\varphi)$ induced by φ, and p is a prime that divides $|L|$ but not $|\ker\varphi|$, then $p < q$ for every prime divisor q of $|\ker\varphi|$. Again, we provide a counterexample that shows that this is not true. According to [9] the cyclic group of order 42 admits a proper skew morphism ρ of order 7 with kernel of order 14. Since $\mathbb{Z}_{42}/(\ker\rho)$ is isomorphic to $\mathbb{Z}_3$ and $\mathbb{Z}_3$ does not admit any proper skew morphism, it follows that the kernel $L/(\ker\rho)$ (of the skew morphism of $\mathbb{Z}_{42}/(\ker\rho)$ induced by ρ) is equal to $\mathbb{Z}_{42}/(\ker\rho)$. Therefore, $|L| = |\mathbb{Z}_{42}|$ and, in particular, 3 divides $|L|$. But 3 is greater than 2, and 2 is a prime divisor of $|\ker\rho|$. We propose the following modification:

Theorem 3.2. *Let φ be a skew morphism of the finite abelian group A, let $K = \ker\varphi$, and let q be any prime divisor of $|K|$. Also let N be a subgroup of K consisting of the identity and all elements of order q, and let L/N be the kernel of the skew morphism φ_N^* of A/N induced by φ. If p is a prime that divides $|L|$ but not $|K|$, then $p < q$.*

Proof. Suppose that such a prime p exists. Since K is abelian, we know that N is a subgroup of K of exponent q that is invariant under φ. Next, let a be any element of order p in L, let $m = \mathrm{ord}(\varphi)$, and let π be the power function of φ. Since L/N is the kernel of φ_N^*, we know by Lemma 2.6 that $q(\pi(a) - 1) \equiv 0 \pmod{m}$. If q is relatively prime to m, then $\pi(a) \equiv 1 \pmod{m}$ and so $a \in K$, which is impossible since K has no element of order p. Thus q divides m and $\pi(a) - 1 \equiv 0 \pmod{m/q}$. In particular, $\pi(a) = 1 + i(m/q)$ where $1 \leq i \leq q - 1$, so there are at most $q - 1$ possibilities for $\pi(a)$.

The same holds for every non-trivial power of a. So now if $p > q$, then by the pigeonhole principle two different powers of a will have the same value under π, in which case they lie in the same coset of N. But that cannot happen since $K \cap \langle a\rangle$ is trivial. Thus $p < q$. □

The only application of the flawed original version of Theorem 5.6* is Corollary 5.7*. This final problematic assertion in [12] states that every prime divisor of $|\ker\varphi|$ is greater than every prime that divides $|A|$ but not $|\ker\varphi|$. To see that this is not true, take the skew morphism ρ of $\mathbb{Z}_{42}$ with kernel of order 14 discussed earlier. Since 2 divides $|\ker\rho|$ and 3 divides $|\mathbb{Z}_{42}|$ but not $|\ker\rho|$, the statement is clearly not true. The following, however, still holds.

Corollary 3.3. *Let A be a non-trivial finite abelian group, and let p be the largest prime divisor of $|A|$. Then the order of the kernel of every skew morphism of A is divisible by p when p is odd, or by 4 when $p = 2$.*

Proof. Let φ be any skew morphism of A, let $K = \ker \varphi$, and suppose to the contrary that p does not divide $|K|$. Also let q be any prime divisor of $|K|$, let N be a subgroup of K consisting of the identity and all elements of order q, and let L/N be the kernel of the skew morphism φ_N^* of A/N induced by φ. If p divides $|L/N|$, then by Theorem 3.2 we know that p is smaller than q, so this cannot happen. It follows that p does not divide $|L/N|$, so we can repeat the same argument for the skew morphism φ_N^* of A/N with kernel L/N. (Note that p divides $|A/N|$.) Since A is finite, this will eventually terminate for some groups A', N' and L' with $|L'/N'| = 1$. Then since the kernel L'/N' is trivial, it follows by Theorem 2.3 that A'/N' is a trivial group, and hence $|A'| = |N'|$. But this is impossible, since p divides $|A'|$ but not $|N'|$. The second part for $p = 2$ follows from the original proof of [12, Corollary 5.7]. □

Both applications of Corollary 5.7*, namely the proofs of Theorem 6.2* and Theorem 9.1*, only use the fact that the order of $\ker \varphi$ is divisible by the largest prime divisor of $|A|$. Since this follows by Corollary 3.3, both theorems still hold, and their proofs can be corrected by minor changes in their wording.

4 Quotients and their properties

In this section, we will show that if BC is a complementary product of two cyclic groups with C core-free in BC, then not only C corresponds to some skew morphism of B (of order $|C|$), but also B corresponds to some skew morphism of C (of order smaller than $|B|$). Let φ be a skew morphism of a cyclic group B, let $G = B\langle\varphi\rangle$, and let $C = \langle\varphi\rangle$. Also let b be a generator of B. To distinguish between φ as a permutation of B and φ as a generator of the cyclic group C, we use c in the latter case. Since C is core-free in G, by Theorem 2.1 we have

$$|G : B| = |C| < |G : C| = |B|\,,$$

so (again by Theorem 2.1) we find that B has a non-trivial core in G. Let K denote the core of B in G, and for every $X \leq G$ let $\overline{X}$ denote XK/K ($\cong X/(X \cap K)$). Next, let H be a subgroup of B such that $cHc^{-1} \subseteq B$. Then, since B is cyclic, H is the unique subgroup of B of order $|H|$, and so $cHc^{-1} = H$. It follows that H is normal in G, and so it is contained in K. Moreover, since K is the core of B in G, we have $cKc^{-1} = K \subseteq B$, and hence by Lemma 2.4 we find that $K = \ker \varphi$.

Now we look closely at the product $\overline{G} = \overline{B}\,\overline{C}$. First, noting that $K \cap C = \{1\}$ we have $C \cong \overline{C}$ (and so $\overline{C}$ is cyclic, and hence abelian) and $\overline{B} \cap \overline{C} = \{1\}$. Since B is cyclic, so is its quotient $\overline{B}$, and by the definition of K we deduce that $\overline{B}$ is core-free in $\overline{G}$. Now it is straightforward to check that the bijection that maps every element $\overline{d} \in \overline{C}$ to the unique element $\overline{d'} \in \overline{C}$ such that $\overline{d}\,\overline{b} = \overline{b}^j\overline{d'}$ defines a skew morphism of $\overline{C}$, with power function $\overline{\pi}$ given by $\overline{\pi}(\overline{d}) = j$. (We choose $\overline{b}$ to be the image of $b \in B$ under the natural homomorphism from B to $\overline{B}$; since b is a generator of B, it follows that $\overline{b}$ is a generator of $\overline{B}$.)

A skew morphism of C ($\cong \overline{C}$) constructed in the way described in the previous paragraph is called the *quotient* of φ (with respect to b), and will be denoted by $\overline{\varphi}$. Since a cyclic group $\overline{B}$ can be generated by different elements, φ can have more than one quotient.

(In fact, by [4, Remark 5.1] this is always true unless B has a unique generator.) In the case of additive notation $B = \mathbb{Z}_n$, and unless otherwise specified, by the quotient of φ we understand the quotient with respect to 1.

The above construction (proposed in the author's PhD thesis [3]) was also introduced independently in [15], where it was noted that if φ is a skew morphism of $\mathbb{Z}_n$ and $\overline{\varphi}$ is a quotient of φ, then $(\varphi, \overline{\varphi})$ is an $(\mathrm{ord}(\varphi), n)$-reciprocal pair of skew morphisms. A pair (φ, ρ) of skew morphisms of $\mathbb{Z}_n$ and $\mathbb{Z}_m$ with power functions π and τ is called (m, n)-*reciprocal* if $\mathrm{ord}(\varphi)$ divides m, $\mathrm{ord}(\rho)$ divides n, and the congruences $\pi(i) \equiv \rho^i(1) \pmod{\mathrm{ord}(\varphi)}$ and $\tau(j) \equiv \varphi^j(1) \pmod{\mathrm{ord}(\rho)}$ hold for each $i \in \mathbb{Z}_n$ and $j \in \mathbb{Z}_m$. We note that while every pair $(\varphi, \overline{\varphi})$ gives an $(\mathrm{ord}(\varphi), n)$-reciprocal pair of skew morphisms, not every reciprocal pair arises in this way. For example, there exist (m, n)-reciprocal pairs of skew morphisms with $m = n$, but by Theorem 2.8 we know that $\mathrm{ord}(\varphi)$ is always strictly smaller than n.

The following observation is an easy consequence of the fact that a skew morphism (of a cyclic group) and its quotient always give a reciprocal pair of skew morphisms.

Lemma 4.1. *Let φ be a skew morphism of $\mathbb{Z}_n$ with power function π, and let $\overline{\varphi}$ be the quotient of φ with power function $\overline{\pi}$. Then for every $i \in \mathbb{N}$:*

(a) $\pi(i) = \overline{\varphi}^i(1)$, *so in particular* $\mathrm{ord}(\overline{\varphi}) = n/|\ker\varphi|$; *and*

(b) $\varphi^i(1) \equiv \overline{\pi}(i) \pmod{n/|\ker\varphi|}$.

Proof. First, since $(\varphi, \overline{\varphi})$ is an $(\mathrm{ord}(\varphi), n)$-reciprocal pair of skew morphisms, we have $\pi(i) \equiv \overline{\varphi}^i(1) \pmod{\mathrm{ord}(\varphi)}$. Hence, since both π and $\overline{\varphi}$ are mappings into $\mathbb{Z}_{\mathrm{ord}(\varphi)}$, it follows that $\pi(i) = \overline{\varphi}^i(1)$. The second part of (a) follows from the fact that $n/|\ker\varphi|$ is the smallest non-zero integer in $\ker\varphi$. Finally, (b) follows easily as $\overline{\pi}(i) \equiv \varphi^i(1) \pmod{\mathrm{ord}(\overline{\varphi})}$ and $\mathrm{ord}(\overline{\varphi}) = n/|\ker\varphi|$. □

Next we provide a lemma which shows that quotients can be used to check whether a skew morphism of a cyclic group is an automorphism or a coset-preserving skew morphism.

Lemma 4.2. *A skew morphism φ of $\mathbb{Z}_n$ is coset-preserving if and only if the quotient $\overline{\varphi}$ of φ is an automorphism. Moreover, φ is proper if and only if $\overline{\varphi}$ is non-trivial.*

Proof. Let φ be a coset-preserving skew morphism of $\mathbb{Z}_n$. This is equivalent with $\varphi(1) \equiv 1 \pmod{n/|\ker\varphi|}$, which by Lemma 4.1(b) happens if and only if $\overline{\pi}(1) = 1$. This proves the first part. The second part follows easily by Lemma 4.1(a) as $\varphi \in \mathrm{Aut}(\mathbb{Z}_n)$ if and only if $\pi(1) = 1$, and $\overline{\varphi}$ is trivial if and only if $\overline{\varphi}(1) = 1$. □

We note that a part of the Lemma 4.2 was proved in [17], where it was shown that if $\overline{\varphi}$ is an automorphism, then φ is coset-preserving, but not the other way around. Also note that since the only skew morphism of $\mathbb{Z}_2$ is the identity mapping, it follows immediately from Lemma 4.2 that if a skew morphism of a cyclic group has order 2, then it must be an automorphism. (This is also an easy consequence of Lemma 2.4.) Another consequence of Lemma 4.2 is the fact that a proper skew morphism of $\mathbb{Z}_n$ is coset-preserving if and only if the quotient of its quotient is the identity mapping. Somewhat interestingly, Lemma 4.2 also implies that by taking quotients every skew morphism of a cyclic group can be reduced to a non-trivial automorphism of the same group.

5 Using quotients to generate skew morphisms

In this section, we describe an algorithm for finding recursively skew morphisms of cyclic groups based on various observations about the quotients of skew morphisms.

5.1 Skew morphisms with a given quotient

First, we explain how to find all skew morphisms of a cyclic group with a given quotient. The following observation about quotients of skew morphisms of cyclic groups will be useful.

Proposition 5.1. *Let φ be a skew morphism of $\mathbb{Z}_n$ with power function π, and let $\overline{\varphi}$ be the quotient of φ with power function $\overline{\pi}$. Then:*

(a) *the periodicity p_φ of φ is the smallest generator of $\ker\overline{\varphi}$;*

(b) $\mathrm{ord}(\varphi) = |\ker\overline{\varphi}|p_\varphi$*; and*

(c) *the orbit T of $\langle\varphi\rangle$ that contains 1 is expressible in the form*

$$T = (x_1, \ldots, x_{p_\varphi}, \psi(x_1), \ldots, \psi(x_{p_\varphi}), \ldots, \psi^{\mathrm{ord}(\psi)-1}(x_1), \ldots, \psi^{\mathrm{ord}(\psi)-1}(x_{p_\varphi})), \tag{5.1}$$

for some coset-preserving skew morphism ψ of $\mathbb{Z}_n$ such that $\mathrm{ord}(\psi) = \mathrm{ord}(\varphi)/p_\varphi$ and $\psi(1) \equiv 1 \pmod{n/|\ker\varphi|}$, and with $x_1 = 1$ and $x_i \equiv \overline{\pi}(i-1) \pmod{n/|\ker\varphi|}$ for each $i \in \{2, \ldots, p_\varphi\}$.

Proof. First, by Theorem 2.10 we have $p_\varphi = p_1$. Then, since the values taken by π at any two elements of $\mathbb{Z}_n$ are equal if and only if they belong to the same right coset of $\ker\varphi$ in $\mathbb{Z}_n$, it follows that p_1 is the smallest positive integer such that $1 \equiv \varphi^{p_1}(1) \pmod{n/|\ker\varphi|}$, which by Lemma 4.1(b) is equivalent with $1 \equiv \overline{\pi}(p_1) \pmod{n/|\ker\varphi|}$. Noting that $n/|\ker\varphi| = \mathrm{ord}(\overline{\varphi})$, we deduce that p_1 is the smallest positive integer such that $\overline{\pi}(p_1) = 1$, and (a) follows. Moreover, since p_φ is the smallest non-trivial element of $\ker\overline{\varphi}$, which is a subgroup of $\mathbb{Z}_{\mathrm{ord}(\varphi)}$, it follows that $\mathrm{ord}(\varphi) = |\ker\overline{\varphi}|p_\varphi$, which proves (b).

To prove the final assertion, let T denote the orbit of $\langle\varphi\rangle$ that contains 1, and let $\psi = \varphi^{p_1}$. By Theorem 2.10 we know that ψ is a coset-preserving skew morphism of $\mathbb{Z}_n$, and by the definition of the periodicity we have $\psi(1) \equiv 1 \pmod{n/|\ker\varphi|}$. By Proposition 2.7 we know that the size of T is equal to $\mathrm{ord}(\varphi)$. Moreover, p_1 divides $|T|$ (see [6, Lemma 3.1]), and hence $\mathrm{ord}(\psi) = \mathrm{ord}(\varphi^{p_1}) = \mathrm{ord}(\varphi)/p_1$, and the effect of ψ on T induces p_1 cycles, each of length $\mathrm{ord}(\varphi)/p_1$. Finally, by Lemma 4.1(b) we have $x_i = \varphi^{i-1}(1) \equiv \overline{\pi}(i-1) \pmod{n/|\ker\varphi|}$ and the rest follows. □

Let ρ be a skew morphism of a cyclic group $\mathbb{Z}_m$. We will provide a detail explanation of the method for finding all skew morphisms φ of $\mathbb{Z}_n$ with quotient ρ.[1]

First, we find the smallest positive integer j such that $j \in \ker\rho$. Then by Proposition 5.1(a) we have $p_1 = p_\varphi = j$. Next, since ρ is a quotient of φ, it follows by

[1] It is important to emphasise here that this method finds all skew morphisms with a particular quotient only for a given cyclic group. If we do not restrict ourselves to a specific group, then in some cases we can find infinitely many skew morphisms with a given quotient. For example, using the classification of skew morphisms for cyclic p-groups of odd order (presented in [21]) it can be shown that each cyclic 3-group of order at least 9 admits a skew morphism whose quotient is the skew morphism $(1, 3, 5)$ of $\mathbb{Z}_6$.

Lemma 4.1(a) that $\mathrm{ord}(\rho) = n/|\ker\varphi|$, and hence $\ker\varphi$ is the unique subgroup of $\mathbb{Z}_n$ of order $n/\mathrm{ord}(\rho)$. As a next step we find all coset-preserving skew morphisms ψ of $\mathbb{Z}_n$ satisfying $\mathrm{ord}(\psi) = m/p_\varphi$ and $\psi(1) \equiv 1 \pmod{n/|\ker\varphi|}$ (note here that $m = |\mathbb{Z}_m| = \mathrm{ord}(\varphi)$). This allows us to identify all possible candidates for the orbit T of $\langle\varphi\rangle$ that contains 1, using (5.1). (For each choice of ψ, we have at most $|\ker\varphi|^{p_1-1} = (n/\mathrm{ord}(\rho))^{p_1-1}$ candidates; the number of candidates could be smaller since sometimes (5.1) does not define a cycle on B.)

Next, suppose that φ is a skew morphism, and let φ_1 be the cyclic permutation of T induced by φ. Then by Lemma 4.1(a) we have $\pi(i) = \rho^i(1)$, and hence by Lemma 2.13 we find that

$$\varphi(i) = \varphi_1(1) + \varphi_1^{\rho(1)}(1) + \varphi_1^{\rho^2(1)}(1) + \cdots + \varphi_1^{\rho^{i-1}(1)}(1) \text{ for all } i \in \mathbb{N}. \tag{5.2}$$

As a final step, for each candidate for φ_1 we use (5.2) to define a function $\varphi\colon \mathbb{Z}_n \to \mathbb{Z}_n$, and then check whether φ is a skew morphism of $\mathbb{Z}_n$, and T an orbit of $\langle\varphi\rangle$. It can be easily verified that if this is true, then ρ is the quotient of φ.

Remark 5.2. Note that to use (5.2), we do not need to know the complete orbit T, but only the elements $\varphi_1^{\rho^i(1)}(1)$ for each $i \in \{0, 1, \ldots, \mathrm{ord}(\rho)\}$. In fact, since for every positive integer j we have $\varphi_1^{j+p_1}(1) = \psi(\varphi_1^j(1))$, only elements of the form $\varphi_1^e(1)$ with $e \equiv \rho^i(1) \pmod{p_1}$ are needed to define φ. In some cases, this significantly reduces the number of possible candidates for φ_1.

5.2 Algorithm for finding all skew morphisms of a cyclic group

We are ready to describe our algorithm for finding all skew morphisms of cyclic groups up to any order. This algorithm is recursive in the sense that it takes the sets of all skew morphisms of the groups $\mathbb{Z}_m$ for $m \in \{2, 3, \ldots, n-1\}$ as input and outputs all skew morphisms of $\mathbb{Z}_n$. Since the only skew morphism of $\mathbb{Z}_2$ is the identity permutation, the algorithm can be easily initialised.

As the first step, we use the method presented in [6] to find all coset-preserving skew morphisms of $\mathbb{Z}_n$. Further details on this method are available in Section 6.3. Next, let φ be a skew morphism of $\mathbb{Z}_n$ that is not coset-preserving, and let $\overline{\varphi}$ be the quotient of φ. Then by Lemma 4.2 we know that $\overline{\varphi}$ is a proper skew morphism of $\mathbb{Z}_{\mathrm{ord}(\varphi)}$. Moreover, by Theorem 2.8 and Theorem 2.9 we find that $\mathrm{ord}(\varphi) < n$, and that $\mathrm{ord}(\varphi)$ divides $n\phi(n)$, and $\gcd(\mathrm{ord}(\varphi), n) \neq 1$. Since we know all skew morphisms of $\mathbb{Z}_m$ for each $m < n$, and we also know all coset-preserving skew morphisms of $\mathbb{Z}_n$, it follows that we can simply apply the method explained in the previous subsection to find all skew morphisms of $\mathbb{Z}_n$ that are not coset-preserving. Together with the coset-preserving skew morphisms of $\mathbb{Z}_n$ (which include all automorphisms and were found earlier), this gives all skew morphisms of $\mathbb{Z}_n$.

A MAGMA [7] implementation of the described algorithm succeeded in finding all skew morphisms of cyclic groups of order up to 161. (The file listing all of these skew morphisms is available at [2].) This significantly improves the previous largest complete list [9] which goes up to the order 60. In Table 1 we summarise the information obtained about skew morphisms of cyclic groups $\mathbb{Z}_n$ for $n \leq 161$. We include a group in the table if and only if it admits a proper skew morphism. Moreover, if a listed group admits a proper skew morphism that is not coset-preserving, then the order of the group is preceded by

n	Skew	Classes	n	Skew	Classes	n	Skew	Classes
6	**2** + 2	**1**	58	**28** + 28	**1**	114	**148** + 36	**7**
8	**2** + 4	**1**	60	**80** + 16	**17**	116	**112** + 56	**3**
*9	**4** + 6	**2**	62	**30** + 30	**1**	*117	**88** + 72	**11**
10	**4** + 4	**1**	*63	**44** + 36	**7**	118	**58** + 58	**1**
12	**4** + 4	**2**	*64	**268** + 32	**42**	120	**208** + 32	**43**
14	**6** + 6	**1**	66	**60** + 20	**13**	*121	**900** + 110	**90**
16	**12** + 8	**4**	68	**64** + 32	**3**	122	**60** + 60	**1**
*18	**24** + 6	**6**	70	**72** + 24	**11**	124	**60** + 60	**2**
20	**16** + 8	**3**	*72	**156** + 24	**36**	*125	**1568** + 100	**152**
21	**12** + 12	**1**	74	**36** + 36	**1**	*126	**348** + 36	**34**
22	**10** + 10	**1**	*75	**96** + 40	**24**	*128	**1132** + 64	**114**
24	**16** + 8	**7**	76	**36** + 36	**2**	129	**84** + 84	**1**
*25	**48** + 20	**12**	78	**104** + 24	**9**	130	**144** + 48	**17**
26	**12** + 12	**1**	80	**152** + 32	**26**	132	**120** + 40	**26**
*27	**64** + 18	**20**	*81	**676** + 54	**110**	134	**66** + 66	**1**
28	**12** + 12	**2**	82	**40** + 40	**1**	*135	**256** + 72	**80**
30	**24** + 8	**7**	84	**104** + 24	**14**	136	**228** + 64	**10**
*32	**60** + 16	**14**	86	**42** + 42	**1**	138	**132** + 44	**25**
34	**16** + 16	**1**	88	**80** + 40	**15**	140	**240** + 48	**29**
*36	**48** + 12	**12**	*90	**216** + 24	**36**	142	**70** + 70	**1**
38	**18** + 18	**1**	92	**44** + 44	**2**	*144	**552** + 48	**96**
39	**24** + 24	**1**	93	**60** + 60	**1**	146	**72** + 72	**1**
40	**44** + 16	**9**	94	**46** + 46	**1**	*147	**960** + 84	**68**
42	**52** + 12	**7**	*96	**272** + 32	**58**	148	**144** + 72	**3**
44	**20** + 20	**2**	*98	**480** + 42	**38**	*150	**648** + 40	**74**
*45	**16** + 24	**8**	*99	**40** + 60	**20**	152	**144** + 72	**23**
46	**22** + 22	**1**	*100	**512** + 40	**42**	*153	**64** + 96	**32**
48	**64** + 16	**20**	102	**96** + 32	**19**	154	**180** + 60	**17**
*49	**180** + 42	**30**	104	**132** + 48	**13**	155	**120** + 120	**1**
*50	**152** + 20	**18**	105	**48** + 48	**4**	156	**352** + 48	**22**
52	**48** + 24	**3**	106	**52** + 52	**1**	158	**78** + 78	**1**
*54	**246** + 18	**33**	*108	**492** + 36	**66**	*160	**616** + 64	**84**
55	**40** + 40	**1**	110	**168** + 40	**9**			
56	**48** + 24	**11**	111	**72** + 72	**1**			
57	**36** + 36	**1**	112	**192** + 48	**36**			

Table 1: Skew morphisms of cyclic groups of order n.

the asterisk character (*). All included groups are listed by their orders, and for each of them we provide the total number of skew morphisms (written as the sum of the numbers of proper skew morphisms and automorphisms), and the number of conjugacy classes of proper skew morphisms in $\mathrm{Aut}(\mathbb{Z}_n)$. Note that the automorphism group of a cyclic group $\mathbb{Z}_n$ is always abelian, and hence the conjugation action of $\mathrm{Aut}(\mathbb{Z}_n)$ on itself is trivial. It follows that the number of conjugacy classes of $\mathrm{Aut}(\mathbb{Z}_n)$ is equal to $|\mathrm{Aut}(\mathbb{Z}_n)|$. For this reason, we list the number of conjugacy classes only for proper skew morphisms. We also note that the numbers of skew morphisms in Table 1 for $n \leq 60$ coincide with the numbers of skew morphisms in [9].

5.3 Remarks concerning Table 1

An inspection of Table 1 suggests various interesting questions regarding skew morphisms of cyclic groups. Possibly the most natural question to ask here is which values n actually appear in Table 1 or, equivalently, which cyclic groups admit a proper skew morphism.

This was answered in [20] for cyclic groups, and later in [12] for all other abelian groups. Specifically, if an abelian group A does not admit any proper skew morphism, then A is cyclic of order n where $n = 4$ or $\gcd(n, \phi(n)) = 1$, or A is an elementary abelian 2-group.

Next, we look at values n such that $\mathbb{Z}_n$ admits (up to conjugacy in $\mathrm{Aut}(\mathbb{Z}_n)$) only one proper skew morphism. In [20] this was shown to be true for all cases where n is a product of two distinct primes and $\gcd(n, \phi(n)) > 1$. The only other value n that appears in Table 1 and has this property is $n = 8$. An interesting question raised in this context is whether this covers all such values n, or if there are others.

We are also interested in those cyclic groups that admit only coset-preserving skew morphisms. Unlike general skew morphisms, coset-preserving skew morphisms are well understood for cyclic groups, and, in particular, we can list all coset-preserving skew morphisms of $\mathbb{Z}_n$ in polynomial time; see [6]. Thus, if for some n we can show that all skew morphisms of $\mathbb{Z}_n$ are coset-preserving, then we can find all skew morphisms of $\mathbb{Z}_n$ much faster than by using the algorithm explained in Section 5.2. In the following section we completely solve this problem by characterising all cyclic groups that admit only coset-preserving skew morphisms.

6 Cyclic groups that admit only coset-preserving skew morphisms

In this section we focus on cyclic groups admitting only coset-preserving skew morphisms. Our main theorem is the following:

Theorem 6.1. *All skew morphisms of $\mathbb{Z}_n$ are coset-preserving if and only if $n = 2^e m$ with $e \in \{0, 1, 2, 3, 4\}$ and m odd and square-free.*

Note that Theorem 6.1 include all groups $\mathbb{Z}_n$ that does not admit any proper skew morphism, as in that case either $n = 4$, or $(n, \phi(n)) = 1$, which forces n to be square-free (for if some prime square p^2 divides n, then p is a common factor of n and $\phi(n)$). In what follows, we will say that the positive integer n is *resolvable* if it is expressible in the form $n = 2^e m$ with $e \in \{0, 1, 2, 3, 4\}$ and m odd and square-free. The proof of Theorem 6.1 is split into two parts; in Section 6.1 we show that if n is not resolvable, then $\mathbb{Z}_n$ admits a non-coset-preserving skew morphism, and in Section 6.2 we show that if n is resolvable, then $\mathbb{Z}_n$ does not admit a non-coset-preserving skew morphism. Then in Section 6.3 we use Theorem 6.1 (and further facts about coset-preserving skew morphisms of cyclic groups) to enumerate all skew morphisms for many finite cyclic groups for which no such enumeration was available to date. Finally, in Section 6.4 we give an example that demonstrates how Theorem 6.1 can be applied to find a precise formula for the number of skew morphisms of $\mathbb{Z}_n$ in the case when n is resolvable and has a relatively small number of prime factors.

6.1 Cyclic groups admitting non-coset-preserving skew morphisms

Here we show that if the order of a cyclic group is divisible by 32 or by the square of an odd prime, then this group admits a skew morphism that does not preserve the cosets of its kernel. To do this, we will use some facts about skew morphisms of $\mathbb{Z}_n$ that give rise to a regular Cayley map. First, we have the following:

Proposition 6.2 ([18])**.** *A skew morphism φ of a finite group B gives rise to a regular Cayley map for B if and only if the set of elements of some orbit of $\langle\varphi\rangle$ is closed under taking inverses and generates B.*

We say that a skew morphism φ of a group B is *t-balanced* if its kernel has index 2 in B. The value t is given by $t = \pi(a)$, where a is any element of B not contained in $\ker\varphi$. In the special case when $t = \mathrm{ord}(\varphi) - 1$ we say that φ is anti-balanced. For further information on t-balanced skew morphisms we refer the reader to [11]. The following observation shows that every coset-preserving skew morphism of $\mathbb{Z}_n$ that gives rise to a regular Cayley map is either an automorphism of $\mathbb{Z}_n$, or a t-balanced skew morphism of $\mathbb{Z}_n$.

Lemma 6.3. *If φ is a coset-preserving skew morphism of $\mathbb{Z}_n$ that gives rise to a regular Cayley map, then the index of $\ker\varphi$ in $\mathbb{Z}_n$ is at most two. In particular, if n is odd, then $\ker\varphi = \mathbb{Z}_n$ and φ is an automorphism of $\mathbb{Z}_n$.*

Proof. Since φ gives rise to a regular Cayley map, by Proposition 6.2 there exists some orbit T of $\langle\varphi\rangle$ that is closed under taking inverses and generates $\mathbb{Z}_n$. Further, by [20, Corollary 3.3] we know that T contains some element t such that $\langle t\rangle = \mathbb{Z}_n$, and since $T = -T$, we also have $-t \in T$. Next, from the fact that φ is coset-preserving we deduce that t and $-t$ are both in the same coset of $\ker\varphi$ in $\mathbb{Z}_n$. It follows that $2t \in \ker\varphi$, and noting that t is a generator of $\mathbb{Z}_n$, we also have $\gcd(n, t) = 1$. Hence $2 \in \ker\varphi$, and the rest follows. □

Throughout the proof of the following proposition we repeatedly refer to the classification of regular Cayley maps for cyclic groups given in [13].

Proposition 6.4. *If a positive integer n is divisible by 32 or p^2 for some odd prime p, then $\mathbb{Z}_n$ admits a skew morphism that is not coset-preserving.*

Proof. First, assume that n is odd and divisible by p^2 for some odd prime p. Then there exists a regular Cayley map for $\mathbb{Z}_n$ with non-balanced representation (see [13, Section 8]), and hence there exists a proper skew morphism φ of $\mathbb{Z}_n$ that gives rise to this Cayley map. Since φ is proper and n is odd, by Lemma 6.3 we deduce that φ is not coset-preserving.

Next, if n is even and divisible by p^2 for some odd prime p, then we have $\mathbb{Z}_n = \mathbb{Z}_\ell \times \mathbb{Z}_{2^e}$ with ℓ odd. Since ℓ is clearly divisible by p^2, from the previous paragraph we know that $\mathbb{Z}_\ell$ admits a skew morphism φ that is not coset-preserving. By Lemma 2.11 there exists a skew morphism θ of $\mathbb{Z}_n$ such that $\theta\restriction_{\mathbb{Z}_\ell} = \varphi$ and $\ker\theta = \ker\varphi \times \mathbb{Z}_{2^e}$. Now it can be easily seen that since φ does not preserve the cosets of $\ker\varphi$ in $\mathbb{Z}_\ell$, the same is true for θ and cosets of $\ker\theta$ in $\mathbb{Z}_n$.

Finally, let n be even and divisible by 32, and consider the factorisation $\mathbb{Z}_n = \mathbb{Z}_{2^e} \times \mathbb{Z}_\ell$ with ℓ odd. Note that to show that $\mathbb{Z}_n$ admits a non-coset-preserving skew morphism, it is sufficient to prove this for $\mathbb{Z}_{2^e}$ (and the rest will follow by Lemma 2.11). Let $M(2m, r)$ be the regular Cayley map for $\mathbb{Z}_{2m}$ given by [13, Definition 3.6]. This map is defined for every unit r modulo m such that if b is the largest divisor of m that is relatively prime to $r - 1$, then either $b = 1$, or r is a root of -1 modulo b of multiplicative order $2k$ where k is relatively prime to m/b. Let $m = 2^{e-1}$, $r = 2^{e-3} + 1$, and $M = M(2m, r)$. Note that the largest divisor of m relatively prime to $r - 1$ is 1, and hence $b = 1$. Also note that r is not a root of -1 modulo m, and since $e \geq 5$ we have $r^2 \not\equiv 1 \pmod m$. It follows that M has no balanced, no t-balanced, and no anti-balanced representation; see [13, Section 8]. Since every automorphism of $\mathbb{Z}_{2^e}$ gives rise to a skew morphism with a balanced representation, and every skew morphism of $\mathbb{Z}_{2^e}$ with kernel of index 2 in $\mathbb{Z}_{2^e}$ gives rise to a skew morphism with either t-balanced or anti-balanced representation, we

deduce that a skew morphism φ of $\mathbb{Z}_{2^e}$ that gives rise to M has kernel of index greater than two in $\mathbb{Z}_{2^e}$. Hence by Lemma 6.3 we find that φ is not coset-preserving. □

6.2 Cyclic groups admitting only coset-preserving skew morphisms

Next we show that if the positive integer n is resolvable, then all skew morphisms of $\mathbb{Z}_n$ are coset-preserving. We start with the following technical lemma.

Lemma 6.5. *Let φ be a skew morphism of a cyclic group $\mathbb{Z}_n$, let N be any non-trivial subgroup of $\ker\varphi$, let φ_N^* be the skew morphism of $\mathbb{Z}_n/N$ induced by φ, and let L/N be the kernel of φ_N^*. Also let s be a prime factor of $n/|\ker\varphi|$, let k_s denote the largest power of s that divides $|(\ker\varphi)/N|$, and let $a = n/(s|\ker\varphi|)$ be an element of $\mathbb{Z}_n$. If sk_s divides $|L/N|$, then $a \notin \ker\varphi$ and $a \in L$.*

Proof. First, since $a|\ker\varphi| = n/s < n$, we have $a \notin \ker\varphi$. (Note that this part is true regardless of whether sk_s divides $|L/N|$.) Next, let $K = \ker\varphi$, and let m be an integer such that $|K/N| = mk_s$. (Observe that m and k_s are relatively prime.) Then since K/N is a subgroup of L/N, we know that mk_s divides $|L/N|$. But $|L/N|$ is also divisible by sk_s, and since $\gcd(m, k_s) = 1$, it follows that $|L/N|$ must be divisible by msk_s. Hence $|L|$ is divisible by $s|K|$, and therefore $a \in L$. □

We are now ready to prove the key part of the proof of Theorem 6.1.

Proposition 6.6. *Let $n = 2^e m$ with $e \in \{0, 1, 2, 3, 4\}$ and m odd and square-free. Then every skew morphism of $\mathbb{Z}_n$ is coset-preserving.*

Proof. Suppose to the contrary that the assertion is not true, and let n be the smallest resolvable integer such that $\mathbb{Z}_n$ admits a skew morphism φ that is not coset-preserving. Also let $K = \ker\varphi$, let φ^* denote the skew morphism of $\mathbb{Z}_n/K$ induced by φ, and let $\overline{\varphi}$ be a quotient of φ. Since the only skew morphism of the trivial group is clearly coset-preserving, we have $n > 1$. Recalling that every skew morphism of a non-trivial group has a non-trivial kernel, it follows that $|K| \geq 2$. In particular, it follows that $|K|$ has at least one prime factor. We proceed by considering the two following cases:

Case (a): $|K|$ is a prime power

Let p be the largest prime divisor of n. Then by Corollary 3.3 we know that p divides $|K|$. If $p = 2$, then $n = 2$, 4, 8, or 16, in which case $\mathbb{Z}_n$ does not admit a skew morphism that is not coset-preserving; see [9]. Hence p is odd and $|K| = p$, and thus $|\mathbb{Z}_n/K| = n/p$. Then since p is the largest prime divisor of n, we know that p does not divide $|\mathbb{Z}_n/K|\phi(|\mathbb{Z}_n/K|)$, and it follows from Theorem 2.9 that p does not divide the order of φ^*. Further, by Lemma 3.1 we know that p divides $\mathrm{ord}(\varphi)$, and since $\mathrm{ord}(\varphi^*) = p_\varphi$, we deduce that p divides $\mathrm{ord}(\varphi^{p_\varphi})$. On the other hand, noting that φ^{p_φ} preserves the cosets of K in $\mathbb{Z}_n$, we have $\mathrm{ord}(\varphi^{p_\varphi}) \leq |K| = p$, and hence $\mathrm{ord}(\varphi^{p_\varphi}) = p$. Therefore $\mathrm{ord}(\varphi) = pp_\varphi$, and then by Proposition 5.1(b) we have $|\ker\overline{\varphi}| = p$. But p does not divide (n/p), which (by Lemma 4.1(a)) is the order of $\overline{\varphi}$, and so by Lemma 3.1 we find that $\overline{\varphi}$ is a group automorphism. Hence by Lemma 4.2 we deduce that φ is coset-preserving, contradiction.

Case (b): $|K|$ has at least two distinct prime factors

Let $k = |K|$, and let d denote the integer satisfying $n = kd$. (Note that the elements of K are exactly the multiples of d modulo n.) Also let $d = r_1 \dots r_\ell$ be a factorisation such that each factor is either an odd prime or the maximum possible power of two. Since φ does not preserve the cosets of K in $\mathbb{Z}_n$, we know that $\varphi(1) \not\equiv 1 \pmod{d}$. Hence, noting that all factors r_i for $i \in \{1, \dots, \ell\}$ are pairwise relatively prime, it follows from the Chinese Remainder Theorem that there exists $r \in \{r_1, \dots, r_\ell\}$ such that $\varphi(1) \not\equiv 1 \pmod{r}$. We will show that this cannot happen.

First, assume that r is odd. It follows that r is a prime, and also that n is not divisible by r^2. (And so, in particular, r does not divide $|K|$.) Let p be any prime factor of $|K|$, let N be the unique subgroup of K of order p, and let φ_N^* be the skew morphism of $\mathbb{Z}_n/N$ induced by φ. Also let L/N be the kernel of φ_N^*, and suppose that $|L/N|$ is not divisible by r. Since the order of the cyclic group $\mathbb{Z}_n/N$ is clearly resolvable, by the assumption of minimality of n we know that φ_N^* is coset-preserving. Then since r divides $\mathbb{Z}_n/N$ but not L/N, we have $\varphi(1) \equiv \varphi_N^*(1) \equiv 1 \pmod{r}$. But this contradicts the fact that $\varphi(1) \not\equiv 1 \pmod{r}$, and hence we deduce that r divides $|L/N|$. Now, since r does not divide $|K|$, it follows that r does not divide $|K/N|$, and thus we may use Lemma 6.5 (with $s = r$ and $k_s = 1$). Hence we deduce that the element $a = d/r$ of $\mathbb{Z}_n$ is not contained in K, but also $a \in L$, and by Lemma 2.6 it follows that $p\pi(a) \equiv p \pmod{\mathrm{ord}(\varphi)}$. Since p was an arbitrary prime factor of $|K|$, the same is true also for some other prime factor q of $|K|$. (Here we use the assumption that the order of K has at least two distinct prime factors.) Hence we have

$$p\pi(a) \equiv p \pmod{\mathrm{ord}(\varphi)},$$
$$q\pi(a) \equiv q \pmod{\mathrm{ord}(\varphi)},$$

for a pair of distinct primes p and q. Then since $\gcd(p, q) = 1$, we deduce that $\pi(a) \equiv 1 \pmod{\mathrm{ord}(\varphi)}$, and consequently $a \in K$, contradiction.

Next, assume that r is even. Again let p denote a prime factor of $|K|$, and define N, φ_N^*, and L/N same as in the case when r was odd. Also let k_2 denote the largest power of 2 that divides $|K/N|$, and suppose that $|L/N|$ is not divisible by $2k_2$. Noting that K/N is a subgroup of L/N, it follows that the largest power of 2 that divides $|L/N|$ must be k_2. Then since φ_N^* must be coset-preserving (due to the minimality of n) and the largest power of 2 that divides $|\mathbb{Z}_n/N|$ is equal to rk_2, we deduce that $\varphi(1) \equiv \varphi_N^*(1) \equiv 1 \pmod{r}$, contradicting the fact that $\varphi(1) \not\equiv 1 \pmod{r}$. Hence it follows that $2k_2$ divides $|L/N|$, and Lemma 6.5 (in this case we take $s = 2$ and $k_s = k_2$) implies that the element $a = d/2$ of $\mathbb{Z}_n$ satisfies $a \notin K$ and $a \in L$. Using the same argument as for r odd this again leads to a contradiction. □

Theorem 6.1 now follows directly from Propositions 6.4 and 6.6.

6.3 Enumeration

In [6] it was shown that each coset-preserving skew morphism φ of $\mathbb{Z}_n$ is uniquely determined by the following four parameters: the smallest non-zero element d of $\ker\varphi$; the element h of $\mathbb{Z}_n$ such that $\varphi(1) = 1+h$; the smallest positive integer s such that $\varphi(d) = sd$; and the positive integer $e = \pi(1)$. (Note that s always exists since $d \in \ker\varphi$ and φ restricts to an automorphism of $\ker\varphi$.) Using various properties of coset-preserving skew morphisms it can be checked that if φ is non-trivial, then the parameters d, h, s and e must satisfy the following properties (see [6, Section 4] for details):

(i) all four parameters are positive integers;

(ii) d is a proper divisor of n;

(iii) $s < n/d$ and $\gcd(s, n/d) = 1$;

(iv) h is a multiple of d strictly smaller than n;

(v) if r is the smallest positive integer such that $h\sum_{i=0}^{r-1} s^i \equiv 0 \pmod{n}$, then e is a (multiplicative) unit modulo r of order d and $e < r$;

(vi) $sd \equiv \sum_{j=0}^{d-1}(1 + h\sum_{i=0}^{\ell_j} s^i) \pmod{n}$, where $\ell_j = e^j - 1 \bmod r$; and

(vii) $s^{e-1} \equiv 1 \pmod{n/d}$.

On the other hand, for each set of parameters (d, h, s, e) satisfying all of the above properties there exists a unique non-trivial coset-preserving skew morphism of $\mathbb{Z}_n$ (which can be constructed in a straightforward way) with this parameter set; see [6, Section 5]. This gives a one-to-one correspondence between non-trivial coset-preserving skew morphisms of $\mathbb{Z}_n$ and the sets of parameters (d, h, s, e), and this correspondence can be used to find all coset-preserving skew morphisms of a given cyclic group in a polynomial time (in the cardinality of the group). Hence, by Theorem 6.1 we can quickly find all skew morphisms of $\mathbb{Z}_n$, where n is resolvable. Using the above observations, we developed an algorithm that can enumerate all skew morphisms for any given cyclic group of any resolvable order. A C++ implementation of this algorithm succeeded in enumerating all skew morphisms for cyclic groups of resolvable orders smaller than 10000 within a second, even without parallelisation. In comparison, the best available method to date for finding all skew morphisms for cyclic groups of general order (described in Section 5.2) is computationally feasible only up to order 161. In our enumeration, which is available at [1], we provide the total number of skew morphisms of $\mathbb{Z}_n$, and also the total number of automorphisms and their proportion among all skew morphisms.

6.4 Skew morphisms of $\mathbb{Z}_{4p}$

Although coset-preserving skew morphisms can be generated efficiently, there is no known explicit formula for the number of coset-preserving skew morphisms of $\mathbb{Z}_n$ for general n. Such a formula would be useful, and in the case when n is resolvable it would give the number of all skew morphisms of $\mathbb{Z}_n$. Resolvable integers n with the simplest structure (with respect to their prime factorisation) are primes, in which case all skew morphisms of $\mathbb{Z}_n$ are automorphisms of $\mathbb{Z}_n$. The situation is also completely understood in the case when n is a product of two distinct primes p and q, in which case the number of skew morphisms of $\mathbb{Z}_{pq}$ is $(p-1)(q-1)$ if $\gcd(p, q-1) = \gcd(p-1, q) = 1$, and $2(p-1)(q-1)$ otherwise; see [20] for example. Here we go one step further and find a formula for the number of skew morphisms of $\mathbb{Z}_{4p}$, where p is an odd prime. We will use the following fact:

Proposition 6.7. *Let p be an odd prime. If φ is a proper skew morphism of $\mathbb{Z}_{4p}$, then the action of φ on its kernel is trivial.*

Proof. Let π and K denote the power function and the kernel of φ, and let φ^* be the skew morphism of $\mathbb{Z}_n/K$ induced by φ. Note that by Theorem 6.1 we know that φ is coset-preserving, and so φ^* must be trivial. Further, by Corollary 3.3 we know that p divides $|K|$, and since φ is proper it follows that the order of K is either p or $2p$. We proceed by considering these two cases. In each case, we let T be the orbit of $\langle\varphi\rangle$ that contains 1. Note that by Proposition 2.7 we have $|T| = \mathrm{ord}(\varphi)$.

Case (a): $|K| = p$

Since φ is coset-preserving, we know that the cosets of K in $\mathbb{Z}_n$ are preserved set-wise by φ. Note that only one element of the coset $1 + K$ does not generate $\mathbb{Z}_n$ (either p or $3p$, depending on whether $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$), and since by Lemma 2.12 no elements outside of K are fixed by φ, it follows that each orbit of $\langle\varphi\rangle$ on $1 + K$ generates $\mathbb{Z}_n$. Hence by Proposition 2.7 we know that all of these orbits have size $\mathrm{ord}(\varphi)$, and since $|1 + K| = |K| = p$, we see that $\mathrm{ord}(\varphi) = p$. Since φ restricts to an automorphism of K, and $\mathrm{ord}(\varphi) = |K| = p$, we deduce that the action of φ on K is trivial.

Case (b): $|K| = 2p$

In this case, since φ is proper, by Theorem 2.9 we have $\gcd(\mathrm{ord}(\varphi), 4p) > 1$. If the order of φ is odd, then we have $\mathrm{ord}(\varphi) = p$ or $\mathrm{ord}(\varphi) = 3p$, but the latter case can be easily excluded since φ must preserve both cosets of K in $\mathbb{Z}_n$ of size $2p$.

Next we deal with the case when $\mathrm{ord}(\varphi)$ is even. Note that by Lemma 4.1(a) we have $\pi(1) = \overline{\varphi}(1)$, and since $\overline{\varphi}$ is an automorphism of the cyclic group $\mathbb{Z}_{\mathrm{ord}(\varphi)}$ of even order, we deduce that $\pi(1)$ is odd. We will use this observation to show that both p and $3p$ are contained in some orbits of $\langle\varphi\rangle$ that generate $\mathbb{Z}_n$. Suppose to the contrary that this is not true. Since every element of $1 + K$ other than p and $3p$ generates $\mathbb{Z}_n$ and no element of $1 + K$ is fixed by φ, we must have $\varphi(p) = 3p$ and $\varphi(3p) = p$. Then since $\pi(1)$ is odd, we have $\varphi^{\pi(1)}(p) = 3p$, and therefore $\varphi(1+p) = \varphi(1) + \varphi^{\pi(1)}(p) = \varphi(1) + 3p$. On the other hand, we have $\varphi(p + 1) = \varphi(p) + \varphi^{\pi(p)}(1) = 3p + \varphi^{\pi(p)}(1)$. But then $\varphi(1) = \varphi^{\pi(p)}(1)$, and since $|T| = \mathrm{ord}(\varphi)$ we find that $\pi(p) = 1$. This forces $p \in K$, contradicting the fact that the order of K is $2p$. Hence we deduce that all orbits of $\langle\varphi\rangle$ on $1 + K$ generate $\mathbb{Z}_n$. In particular, $\mathrm{ord}(\varphi)$ divides $2p$, and it follows that $\mathrm{ord}(\varphi) = 2p$.

We have shown that if $|K| = 2p$, then $\mathrm{ord}(\varphi)$ is equal to p or $2p$. Hence by order considerations it can be easily seen that φ acts on K either trivially, or by the inversion. To exclude the latter, first note that 1 and $\varphi(1)$ are in the same coset of K in $\mathbb{Z}_{4p}$, and hence $\varphi(1) - 1 \in K$. If we let $h = \varphi(1) - 1$, then we have $\varphi^2(1) = \varphi(h + 1) = \varphi(h) + \varphi(1) = -h + h + 1 = 1$, but then by Proposition 2.7 we have $\mathrm{ord}(\varphi) = 2$, which is impossible. Hence we again conclude that the action of φ on K is trivial. □

Using Theorem 6.1 and Proposition 6.7 we can now easily enumerate all proper skew morphisms of $\mathbb{Z}_{4p}$.

Theorem 6.8. *If p is an odd prime, then the number of skew morphisms of $\mathbb{Z}_{4p}$ is*

$$\begin{cases} 6p - 6 & \text{if } p \equiv 1 \pmod 4 \\ 4p - 4 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. Throughout this proof we refer to the properties (i) to (vii) and the parameters d, h, s and e of coset-preserving skew morphisms for cyclic groups explained in Section 6.3.

We know that $|\mathrm{Aut}(\mathbb{Z}_{4p})| = 2p-2$, so we proceed by counting proper skew morphisms of $\mathbb{Z}_{4p}$. Let φ be a proper skew morphism of $\mathbb{Z}_{4p}$, and recall that by Theorem 6.1 it is coset-preserving. Let d, h, s and e be the four defining parameters of φ, and note that by Proposition 6.7 we have $s = 1$. Since p is the largest prime divisor of $4p$, by Corollary 3.3 we know that p divides $|\ker\varphi|$, and it follows that $d = 2$ or $d = 4$. (The case $d = 1$ can be excluded as φ is proper.)

First let $d = 2$, and let h be any positive multiple of 2 strictly smaller than $4p$. If 4 divides h, then by (v) we find that $r = p$ and $e = p-1$. Since $s = 1$, both (iii) and (vii) are trivially true, and (vi) holds as $(1+h)+(1+h(p-1)) \equiv 2+hp \equiv 2 \pmod{4p}$. If 4 does not divide h and $h \neq 2p$, then by (v) we have $r = 2p$ and $e = 2p-1$. Again both (iii) and (vii) hold trivially, and (vi) is also true since $(1+h)+(1+h(2p-1) \equiv 2+2hp \equiv 2 \pmod{4p}$. If $h = 2p$, then it can be easily verified that $\mathrm{ord}(\varphi) = r = 2$, contradicting the fact that φ is proper. Since for all but one choice of h we obtain exactly one coset-preserving skew morphism, it follows that in this case we have exactly $2p-2$ skew morphism of $\mathbb{Z}_{4p}$.

Next let $d = 4$, and let h be any positive multiple of 4 strictly smaller than $4p$. Then by (v) we deduce that $r = p$, and e must be a fourth root of unity modulo p. It follows that necessarily $p \equiv 1 \pmod 4$, in which case there are two possible candidates for e. Note that for either candidate we have $e^2 \equiv -1 \pmod p$ and $e^3 \equiv -e \pmod p$. Again (iii) and (vii) hold trivially, and (vi) holds as well since $(1+h)+(1+he)+(1+h(p-1))+(1+h(p-e)) \equiv 4+2hp \equiv 4 \pmod{4p}$. Hence, if $p \equiv 1 \pmod 4$, then every choice of h gives two coset-preserving skew morphisms (one for each choice of e), which gives a total of $2p-2$ skew morphisms of $\mathbb{Z}_{4p}$. □

ORCID iDs

Martin Bachratý https://orcid.org/0000-0002-4300-7507

References

[1] M. Bachratý, Enumeration of skew morphisms of cyclic groups admitting only coset-preserving skew morphisms up to order 100000, https://drive.google.com/file/d/1HpumLCS-hJW-LCdWbYsUJ-PCj3pVes4g.

[2] M. Bachratý, List of skew-morphisms of cyclic groups up to order 161, https://drive.google.com/file/d/1rpFTIa961JkxHY5yuyN2gm2fUovQSuar.

[3] M. Bachratý, *Skew morphisms and skew product groups of finite groups*, Ph.D. thesis, University of Auckland, 2020, https://researchspace.auckland.ac.nz/bitstream/handle/2292/53164/Bachraty-2020-thesis.pdf.

[4] M. Bachratý, M. Conder and G. Verret, Skew product groups for monolithic groups, *Algebr. Comb.* **5** (2022), 785–802, doi:10.5802/alco.206, https://doi.org/10.5802/alco.206.

[5] M. Bachratý and R. Jajcay, Powers of skew-morphisms, *Symmetries in Graphs, Maps, and Polytopes* (2016), 1–25, doi:10.1007/978-3-319-30451-9_1, https://doi.org/10.1007/978-3-319-30451-9_1.

[6] M. Bachratý and R. Jajcay, Classification of coset-preserving skew-morphisms of finite cyclic groups, *Australas. J. Comb.* **67** (2017), 259–280, https://ajc.maths.uq.edu.au/pdf/67/ajc_v67_p259.pdf.

[7] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265, doi:10.1006/jsco.1996.0125, https://doi.org/10.1006/jsco.1996.0125.

[8] J. Chen, S. Du and C. H. Li, Skew-morphisms of nonabelian characteristically simple groups, *J. Comb. Theory Ser. A* **185** (2022), 105539, doi:10.1016/j.jcta.2021.105539, https://doi.org/10.1016/j.jcta.2021.105539.

[9] M. Conder, List of skew-morphisms for small cyclic groups, https://www.math.auckland.ac.nz/~conder/SkewMorphisms-SmallCyclicGroups-60.txt.

[10] M. Conder, R. Jajcay and T. W. Tucker, Regular Cayley maps for finite abelian groups, *J. Algebr. Comb.* **25** (2007), 343–364, doi:10.1007/s10801-006-0037-0, https://doi.org/10.1007/s10801-006-0037-0.

[11] M. Conder, R. Jajcay and T. W. Tucker, Regular t-balanced Cayley maps, *J. Comb. Theory Ser. B* **97** (2007), 453–473, doi:10.1016/j.jctb.2006.07.008, https://doi.org/10.1016/j.jctb.2006.07.008.

[12] M. Conder, R. Jajcay and T. W. Tucker, Cyclic complements and skew morphisms of groups, *J. Algebra* **453** (2016), 68–100, doi:10.1016/j.jalgebra.2015.12.024, https://doi.org/10.1016/j.jalgebra.2015.12.024.

[13] M. Conder and T. W. Tucker, Regular Cayley maps for cyclic groups, *Trans. Amer. Math. Soc.* **336** (2014), 3585–3609, doi:10.1090/s0002-9947-2014-05933-3, https://doi.org/10.1090/s0002-9947-2014-05933-3.

[14] S. Du, K. Hu. and A. Lucchini, Skew-morphisms of cyclic 2-groups, *J. Group Theory* **22** (2019), 617–635, doi:10.1515/jgth-2019-2046, https://doi.org/10.1515/jgth-2019-2046.

[15] Y.-Q. Feng, K. Hu, R. Nedela, M. Škoviera and N.-E. Wang, Complete regular dessins and skew-morphisms of cyclic groups, *Ars Math. Contemp.* **18** (2020), 289–307, doi:10.26493/1855-3974.1748.ebd, https://doi.org/10.26493/1855-3974.1748.ebd.

[16] K. Hu, Y. S. Kwon and J.-Y. Zhang, Classification of skew morphisms of cyclic groups which are square roots of automorphisms, *Ars Math. Contemp.* **21** (2021), 2–01, 23 pp., doi:10.26493/1855-3974.2129.ac1, https://doi.org/10.26493/1855-3974.2129.ac1.

[17] K. Hu, R. Nedela, N.-E. Wang and K. Yuan, Reciprocal skew morphisms of cyclic groups, *Acta Math. Univ. Comenian.* **88** (2019), 305–318, http://www.iam.fmph.uniba.sk/amuc/ojs/index.php/amuc/article/view/1006.

[18] R. Jajcay and J. Širáň, Skew-morphisms of regular Cayley maps, *Discrete Math.* **244** (2002), 167–179, doi:10.1016/S0012-365X(01)00081-4, https://doi.org/10.1016/S0012-365X(01)00081-4.

[19] I. Kovács and Y. S. Kwon, Regular Cayley maps for dihedral groups, *J. Comb. Theory Ser. B* **148** (2021), 84–124, doi:10.1016/j.jctb.2020.12.002, https://doi.org/10.1016/j.jctb.2020.12.002.

[20] I. Kovács and R. Nedela, Decomposition of skew-morphisms of cyclic groups, *Ars Math. Contemp.* **4** (2011), 329–349, doi:10.26493/1855-3974.157.fc1, https://doi.org/10.26493/1855-3974.157.fc1.

[21] I. Kovács and R. Nedela, Skew-morphisms of cyclic p-groups, *J. Group Theory* **20** (2017), 1135–1154, doi:10.1515/jgth-2017-0015, https://doi.org/10.1515/jgth-2017-0015.

[22] A. Lucchini, On the order of transitive permutation groups with cyclic point-stabilizer, *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.* **9** (1998), 241–243.

[23] N.-E. Wang, K. Hu, K. Yuan and J.-Y. Zhang, Smooth skew morphisms of the dihedral groups, *Ars Math. Contemp.* **16** (2019), 527–547, doi:10.26493/1855-3974.1475.3d3, https://doi.org/10.26493/1855-3974.1475.3d3.

[24] J.-Y. Zhang and S. Du, On the skew-morphisms of dihedral groups, *J. Group Theory* **19** (2016), 993–1016, doi:10.1515/jgth-2016-0027, https://doi.org/10.1515/jgth-2016-0027.

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 24 (2024) #P2.09 / 347–354
https://doi.org/10.26493/1855-3974.2751.81f
(Also available at http://amc-journal.eu)

Finite simple groups on triple systems*

Xiaoqin Zhan, Xuan Pang, Suyun Ding †
School of Science, East China JiaoTong University,
Nanchang, 330013, People's Republic of China

Received 3 December 2021, accepted 14 May 2023, published online 22 November 2023

Abstract

Let $\mathcal{D}$ be a triple system, and let G be a finite simple group. In this paper we almost determine all possibilities of $\mathcal{D}$ admitting G as its flag-transitive automorphism group.

Keywords: Triple system, flag-transitivity, finite simple group.

Math. Subj. Class. (2020): 05B07, 20B25, 05B25

1 Introduction

A 2-(v, k, λ) design is a pair $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ where $\mathcal{P}$ is a set of v points and $\mathcal{B}$ is a collection of b k-subsets (blocks) of $\mathcal{P}$ with the property that every 2-subset of $\mathcal{P}$ occurs in λ blocks of $\mathcal{B}$. If no blocks are identical, then $\mathcal{D}$ is called simple.

An *automorphism* of a design $\mathcal{D}$ is a permutation of $\mathcal{P}$ which leaves $\mathcal{B}$ invariant. The full automorphism group of $\mathcal{D}$, denoted by $\mathrm{Aut}(\mathcal{D})$, is the group consisting of all automorphisms of $\mathcal{D}$. A $flag$ of $\mathcal{D}$ is a point-block pair (α, B) such that $\alpha \in B$. For $G \leq \mathrm{Aut}(\mathcal{D})$, G or $\mathcal{D}$ is called *flag-transitive* if G acts transitively on the set of flags, and *point-primitive* if G acts primitively on $\mathcal{P}$. A set of blocks of $\mathcal{D}$ is called a set of *base blocks* with respect to an automorphism group G of $\mathcal{D}$ if it contains exactly one block from each G-orbit on the block set. In particular, if G is a flag-transitive automorphism group of $\mathcal{D}$, then any block B is a base block of $\mathcal{D}$.

*The authors would like to express their gratitude to the referee who made very helpful comments and suggestions that improved our paper. This work is supported by the National Natural Science Foundation of China (Grant Nos. 12361004 and 11961026) and the Natural Science Foundation of Jiangxi Province (Grant Nos. 20224BAB211005 and 20224BAB201005).

†Corresponding author.
E-mail addresses: zhanxiaoqinshuai@126.com (Xiaoqin Zhan), p1443202623@163.com (Xuan Pang), dingsy2017@163.com (Suyun Ding)

In this paper, we focus on simple 2-$(v, 3, \lambda)$ designs also known as simple triple systems, which can be denoted by $TS(v, \lambda)$. One possibility is to take all possible 3-subsets of $\mathcal{P}$ however such designs are called *complete* and will be ignored. A triple system is a *Steiner triple system*, or $STS(v)$, when $\lambda = 1$.

Let r be the number of the blocks through a given point. For a $TS(v, \lambda)$, it is well known that a necessary and sufficient condition for the existence of a $TS(v, \lambda)$ is $v \neq 2$ and $\lambda \equiv 0 \pmod{(v-2, 6)}$, and

$$3b = vr; \tag{1.1}$$

$$r = \frac{\lambda(v-1)}{2}; \tag{1.2}$$

$$b = \frac{\lambda v(v-1)}{6}; \tag{1.3}$$

$$b \geq v. \tag{1.4}$$

A 2-$(v, k, 1)$ design is also called a finite linear space. A classic result is that of Higman and McLaughlin [8] who proved that for a finite linear space, flag-transitivity implies point-primitivity. Then Buekenhout, Delandtsheer and Doyen in [1] proved that if G acts flag-transitively on a linear space, then G is of affine or almost simple type. In 1990, the six-person team [2] classified all flag-transitive linear spaces apart from those with an one-dimensional affine automorphism group.

For 2-$(v, k, 1)$ designs with small values of k, one of the first classifications was for Steiner triple systems in [4], which considered what happens when the action was block-transitive but not 2-transitive on points. It is described in [11] what happens when the action on points is 2-transitive. This result depends on the classification of all finite simple groups and is subsumed into the general results proved by Kantor in [10].

Let G be a flag-transitive automorphism group of a $TS(v, \lambda)$. It is shown in [6, 2.3.7(c), (e)] that G is point-primitive. Moreover, we can easily prove that G is 2-homogeneous (see Lemma 2.2 below). This result makes it possible to classify all flag-transitive triple systems using the classification of the finite 2-transitive permutation groups. Our main purpose is to give a classification of all triple systems admitting a simple flag-transitive automorphism group.

We now state the main result of this paper:

Theorem 1.1. *Let $\mathcal{D}$ be a triple system, and let G be a finite simple group. If G acts flag-transitively on $\mathcal{D}$, then one of the following* LINES *of* Table 1 *holds.*

Remark 1.2.

- All but the triple systems listed in LINES 20 and 21 exist.
- If $G = PSU(3, q)$ with $q = 5$, then there are only two flag-transitive triple systems corresponding to LINES 19 and 20.
- The existence of triple systems with $3 \nmid q$ and $q \neq 5$ corresponding to LINES 20 and 21 is in doubt.

Table 1: G and corresponding triple systems.

LINE	G	$\mathcal{D}$	Notes
1	A_7	$TS(15,1)$	
2		$TS(15,12)$	
3	$PSL(2,11)$	$TS(11,3)$	
4		$TS(11,6)$	
5	HS	$TS(176,12)$	
6		$TS(176,72)$	
7		$TS(176,90)$	
8	Co_3	$TS(276,112)$	
9		$TS(276,162)$	
10	$PSp(2d,2)$	$TS(2^{d-1}(2^d+1), 2^{2d-2})$	$d \geq 3$
11		$TS(2^{d-1}(2^d+1), 2(2^{d-1}-1)(2^{d-2}+1))$	
12	$PSp(2d,2)$	$TS(2^{d-1}(2^d-1), 2^{2d-2})$	$d \geq 3$
13		$TS(2^{d-1}(2^d-1), 2(2^{d-1}+1)(2^{d-2}-1))$	
14	$PSL(d,q)$	$TS(\frac{q^d-1}{q-1}, q-1)$	$d \geq 3$
15		$TS(\frac{q^d-1}{q-1}, \frac{q^d-1}{q-1}-q-1)$	
16	$PSL(2,q)$	$TS(q+1, \frac{q-1}{2})$	$q \equiv 1 (\mathrm{mod}\, 4)$
17	$Ree(q)$	$TS(q^3+1, 2(q-1))$	$q = 3^{2e+1} > 3$
18		$TS(q^3+1, q-1)$	
19	$PSU(3,q)$	$TS(q^3+1, q-1)$	$q \geq 3$
20		$TS(q^3+1, \frac{q^2-1}{(3,q+1)})$	
21		$TS(q^3+1, \frac{2(q^2-1)}{(3,q+1)})$	

2 Useful lemmas

The notation and terminology used is standard and can be found in [5, 6] for design theory and in [7, 9] for group theory. In particular, if G is a permutation group on a set Ω, and $\{\alpha, \beta\} \subseteq \Delta \subseteq \Omega$, then G_α denotes the stabilizer of a point α in G, and $G_{\alpha\beta}$ denotes the pointwise stabilizer of two points α and β in G, and G_Δ denotes the setwise stabilizer of Δ in G.

The following result about flag-transitive 2-designs is well-known.

Lemma 2.1. *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a 2-(v,k,λ) design, and let G be an automorphism group of $\mathcal{D}$. For any $\alpha \in \mathcal{P}$ and $B \in \mathcal{B}$, G is flag-transitive if and only if G is point-transitive and G_α is transitive on the pencil $P(\alpha)$ (the set of blocks through α), if and only if G is block-transitive and G_B is transitive on the points of B.*

Lemma 2.2. *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a triple system, and let G be a flag-transitive automorphism group of $\mathcal{D}$. If G is a simple group, then G acts 2-transitively on $\mathcal{P}$.*

Proof. Let $\{\alpha, \beta\}$ and $\{\gamma, \delta\}$ be arbitrary two unordered pairs of $\mathcal{P}$. By the definition of a triple system, there are two points ε and θ such that $B_1 = \{\alpha, \beta, \varepsilon\}$ and $B_2 = \{\gamma, \delta, \theta\}$ are two blocks of $\mathcal{D}$. The flag-transitivity of G implies that there is a $g \in G$ such that

$$(\varepsilon, B_1)^g = (\varepsilon^g, B_1^g) = (\theta, B_2),$$

and so $\{\alpha, \beta\}^g = \{\gamma, \delta\}$. Thus G is 2-homogeneous. If G is a simple group, then G acts 2-transitively on $\mathcal{P}$ by [7, Theorem 9.4B]. □

Lemma 2.3. *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a triple system, and let $G \leq \mathrm{Aut}(\mathcal{D})$ be a 2-transitive group on $\mathcal{P}$. Then the following conditions are equivalent:*

(i) *G acts flag-transitively on $\mathcal{D}$.*

(ii) *If $B = \{\alpha, \beta, \gamma\} \in \mathcal{B}$, then $\{\{\alpha, \beta, \gamma_i\} \mid \gamma_i \in \gamma^{G_{\{\alpha,\beta\}}}\}$ is the set of all blocks through points α and β.*

Proof. (i) $\Rightarrow$ (ii): Let $B(\alpha, \beta) = \{B_1, B_2, \ldots, B_\lambda\}$ be the set of blocks through points α and β, where $B_i = \{\alpha, \beta, \gamma_i\}$, $\gamma_i \in \mathcal{P} \setminus \{\alpha, \beta\}$. Clearly, $B(\alpha, \beta)^{G_{\{\alpha,\beta\}}} = B(\alpha, \beta)$. If G acts flag-transitively on $\mathcal{D}$, then for any two flags (γ_i, B_i) and (γ_j, B_j), there is a $g \in G$ such that $(\gamma_i, B_i)^g = (\gamma_j, B_j)$, so $\gamma_i^g = \gamma_j$ and $g \in G_{\{\alpha,\beta\}}$. Thus $G_{\{\alpha,\beta\}}$ acts transitively on $B(\alpha, \beta)$ and hence $\{\gamma_1, \ldots, \gamma_\lambda\} = \gamma_i^{G_{\{\alpha,\beta\}}}$.

(ii) $\Rightarrow$ (i): Let (γ, B) and (ϵ, C) be two flags of $\mathcal{D}$ with $B = \{\alpha, \beta, \gamma\}$, $C = \{\delta, \eta, \epsilon\}$. By the 2-transitivity of G, there exists $g_1 \in G$ such that $\{\alpha, \beta\}^{g_1} = \{\delta, \eta\}$, thus $B^{g_1} = \{\delta, \eta, \gamma^{g_1}\}$ is a block containing δ and η. Since $\{\{\delta, \eta, \epsilon_i\} \mid \epsilon_i \in \epsilon^{G_{\{\delta,\eta\}}}\}$ is the set of all blocks through δ and η, there exists $g_2 \in G_{\{\delta,\eta\}}$ such that $\gamma^{g_1 g_2} = \epsilon$, and then $(\gamma, B)^{g_1 g_2} = (\epsilon, C)$. Therefore, G acts flag-transitively on $\mathcal{D}$. □

Corollary 2.4. *Let G be a 2-transitive group on a point set $\mathcal{P}$ with $|\mathcal{P}| = v$, and let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be all sizes of orbits of $G_{\alpha\beta}$ on $\mathcal{P} \setminus \{\alpha, \beta\}$. If $\lambda_i \neq \lambda_j$ for $i \neq j$, then there exist k different flag-transitive $TS(v, \lambda_i)$.*

Proof. Without loss of generality, let $\Delta = \gamma^{G_{\alpha\beta}}$ with $|\Delta| = \lambda_1$, where $\gamma \in \mathcal{P} \setminus \{\alpha, \beta\}$. Since $G_{\alpha\beta} \trianglelefteq G_{\{\alpha,\beta\}}$, the group $G_{\alpha\beta}$ acts $\frac{1}{2}$-transitively on $\gamma^{G_{\{\alpha,\beta\}}}$, that is, $G_{\alpha\beta}$-orbits on $\gamma^{G_{\{\alpha,\beta\}}}$ have the same length. The uniqueness of the $G_{\alpha\beta}$-orbit with size λ_1 implies that $\gamma^{G_{\alpha\beta}} = \gamma^{G_{\{\alpha,\beta\}}}$. Thus $G_{\{\alpha,\beta\}}$ has a unique orbit with size λ_1. Let $B = \{\alpha, \beta, \gamma\}$ and $\mathcal{B} = B^G$. We shall prove below that $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a $TS(v, \lambda_1)$ admitting G as its flag-transitive automorphism group.

Since G is 2-transitive, for any pair $\{\delta, \eta\}$, there exists $g \in G$ such that $\{\alpha, \beta\}^g = \{\delta, \eta\}$. So $G_{\{\delta,\eta\}}$ has a unique orbit $\Delta^g = (\gamma^g)^{G_{\{\delta,\eta\}}}$ with $|\Delta^g| = |\Delta| = \lambda_1$. Let $B(\delta, \eta)$ be the set of elements of $\mathcal{B}$ containing δ, η with $|B(\delta, \eta)| = \lambda$. It is easy to see that $\Lambda = \{\{\delta, \eta, \epsilon\} \mid \epsilon \in \Delta^g\} \subseteq \mathcal{B}$, so we have $\lambda \geq \lambda_1$. On the other hand, for $C = \{\delta, \eta, \theta\} \in B(\delta, \eta)$, there exists $h \in G$ such that $C = B^h$. As $|\gamma^{G_{\alpha\beta}}| = |\alpha^{G_{\gamma\beta}}| = |\beta^{G_{\alpha\gamma}}| = \lambda_1$, we may assume that $\theta = \gamma^h$. Then $|\theta^{G_{\{\delta,\eta\}}}| = |\gamma^{hG_{\{\delta,\eta\}}}| = |\gamma^{G_{\{\alpha,\beta\}h}}| = |\Delta^h| = \lambda_1$, it implies $\lambda_1 \geq \lambda$. Thus, $\lambda = \lambda_1$ and $B(\delta, \eta) = \Lambda$. Hence $\mathcal{D}$ is a $TS(v, \lambda_1)$, and G is a flag-transitive automorphism group of $\mathcal{D}$ by Lemma 2.3(ii). □

Lemma 2.5. *Let G be a 2-transitive group on a point set $\mathcal{P}$ with $|\mathcal{P}| = v$, and let $\Delta = \{\alpha, \beta, \gamma\}$ be a 3-subset of $\mathcal{P}$. If $G_{\alpha\beta}$ is a cyclic group of order λ and $|\gamma^{G_{\alpha\beta}}| = \lambda$, then*

(i) *$\mathcal{D} = (\mathcal{P}, \Delta^G)$ is a flag-transitive $TS(v, \lambda)$ if and only if $G_\Delta^\Delta \cong S_3$, or*

(ii) *$\mathcal{D} = (\mathcal{P}, \Delta^G)$ is a flag-transitive $TS(v, 2\lambda)$ if and only if $G_\Delta^\Delta \cong \mathbb{Z}_3$.*

Proof. Here we only prove case (i), and case (ii) can be proved by same procedure. Since $G_{\alpha\beta}$ is a cyclic group for any points α and β, we have that $G_\Delta = G_\Delta^\Delta$. Let $\mathcal{D} = (\mathcal{P}, \Delta^G)$. If $\mathcal{D}$ is a flag-transitive $TS(v, \lambda)$, then using Lemma 2.1 and Equation (1.3), we have that

$$b = \frac{\lambda v(v-1)}{6} = |\Delta^G| = [G : G_\Delta] = [G : G_{\alpha\beta}][G_{\alpha\beta} : G_\Delta].$$

By 2-transitivity of G and $|G_{\alpha\beta}| = \lambda$, we obtain $|G_\Delta| = 6$. The flag-transitivity of G implies that G_Δ acts transitively on the points of Δ by Lemma 2.1. Thus $G_\Delta \cong S_3$.

If $G_\Delta \cong S_3$, then $G_{\{\alpha,\beta\}\gamma} \cong \mathbb{Z}_2$ and $|\Delta^G| = [G : G_{\alpha\beta}][G_{\alpha\beta} : G_\Delta] = \frac{\lambda v(v-1)}{6}$. Thus, $\mathcal{D}$ is a $TS(v,\lambda)$ as G acts 2-transitively on $\mathcal{P}$. Clearly,

$$|\gamma^{G_{\{\alpha,\beta\}}}| = [G_{\{\alpha,\beta\}} : G_{\{\alpha,\beta\}\gamma}] = \lambda,$$

where $G_{\{\alpha,\beta\}\gamma} = G_{\{\alpha,\beta\}} \cap G_\gamma$. Therefore, G acts flag-transitively on $\mathcal{D}$ by Corollary 2.4. □

Lemma 2.6. *Let $G = Ree(q)$ act 2-transitively on Ω, where $|\Omega| = q^3+1$ and $q = 3^{2e+1} > 3$. Then there exist subsets Δ, Σ of size 3 such that*

$$G_\Delta^\Delta = \mathbb{Z}_3, \;\; G_\Sigma^\Sigma = S_3.$$

Proof. Let Q be a Sylow 3-subgroup of G. Then $|Q| = q^3$, and there exists $\alpha \in \Omega$ such that Q is regular on $\Omega \setminus \{\alpha\}$. Thus each subgroup of Q is semiregular on $\Omega \setminus \{\alpha\}$. Let $x, y \in Q$ such $|x| = |y| = 3$, $x \notin \mathbf{Z}(Q)$ and $y \in \mathbf{Z}(Q)$, where the centre $\mathbf{Z}(Q)$ is elementary abelian of order q.

Let Δ be an orbit of $\langle x\rangle$. Then $|\Delta| = 3$ and $G_\Delta^\Delta = \mathbb{Z}_3$ or S_3. Further, since x is not conjugate to x^{-1} in G (reference [12]), we have $G_\Delta^\Delta \cong \langle x\rangle \cong \mathbb{Z}_3$.

Consider y acting on $\Omega \setminus \{\alpha\}$. Since y is in the centre $\mathbf{Z}(Q)$, there is an involution $z \in G_\alpha$ such that $y^z = y^{-1}$, and the subgroup $H = \langle y, z\rangle \cong S_3$. Since $\langle y\rangle$ is semiregular on $\Omega \setminus \{\alpha\}$, the set $\Omega \setminus \{\alpha\}$ is divided into $\frac{1}{3}q^3$ orbits of $\langle y\rangle$:

$$\Delta_1, \Delta_2, \ldots, \Delta_m,$$

where $m = \frac{1}{3}q^3$ is odd. Since each H-orbit Σ contains a $\langle y\rangle$-orbit, the cardinality $|\Sigma| = 3$ or 6. As the number $\frac{1}{3}q^3$ of $\langle y\rangle$-orbits is odd, it follows that there is at least one H-orbit Σ on $\Omega \setminus \{\alpha\}$ has length 3. Therefore, $G_\Sigma^\Sigma = H_\Sigma^\Sigma = S_3$ with $|\Sigma| = 3$. □

3 Proof of Theorem 1.1

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a $TS(v,\lambda)$, and let G be a simple group acting flag-transitively on $\mathcal{D}$. Then G acts 2-transitively on $\mathcal{P}$ by Lemma 2.2. Since we neglect the case $\mathcal{D}$ is complete, we may assume that G is not 3-homogeneous group on $\mathcal{P}$. Thus, all such groups are known and we can find a classification in [3] and we have that G must be one of the following Table 2.

We will prove Theorem 1.1 by analyzing the 11 cases in Table 2 one by one.

Proof of Theorem 1.1. Let α and β be two points of $\mathcal{P}$. For Cases 1 – 7, we have the following facts by the proof of [10, Theorem 1]:

If $G = A_7$ and $v = 15$, then $G_{\alpha\beta}$ has orbit-lengths 1 and 12 on $\mathcal{P} \setminus \{\alpha, \beta\}$.

If $G = PSL(2, 11)$ and $v = 11$, then $G_{\alpha\beta}$ has orbit-lengths 3 and 6 on $\mathcal{P} \setminus \{\alpha, \beta\}$.

If $G = HS$ and $v = 176$, then $G_{\alpha\beta}$ has orbit-lengths 12, 72 and 90 on $\mathcal{P} \setminus \{\alpha, \beta\}$.

If $G = Co_3$ and $v = 276$, then $G_{\alpha\beta}$ has orbit-lengths 112 and 162 on $\mathcal{P} \setminus \{\alpha, \beta\}$.

If $G = PSp(2d, 2)$ and $v = 2^{2d-1} + 2^{d-1}$, then $G_{\alpha\beta}$ has orbit-lengths $2(2^{d-1} - 1)(2^{d-2} + 1)$ and 2^{2d-2} on $\mathcal{P} \setminus \{\alpha, \beta\}$.

Table 2: 2-transitive, not 3-homogeneous simple groups.

Case	Group	Degree	Notes
1	A_7	15	
2	$PSL(2,11)$	11	
3	HS	176	
4	Co_3	276	
5	$PSp(2d,2)$	$2^{2d-1}+2^{d-1}$	$d \geq 3$
6	$PSp(2d,2)$	$2^{2d-1}-2^{d-1}$	$d \geq 3$
7	$PSL(d,q)$	$(q^d-1)/(q-1)$	$d \geq 3$
8	$PSL(2,q)$	$q+1$	$q \equiv 1 \pmod 4$
9	$Suz(q)$	q^2+1	$q = 2^{2e+1} > 2$
10	$Ree(q)$	q^3+1	$q = 3^{2e+1} > 3$
11	$PSU(3,q)$	q^3+1	$q \geq 3$

If $G = PSp(2d,2)$ and $v = 2^{2d-1}-2^{d-1}$, then $G_{\alpha\beta}$ has orbit-lengths $2(2^{d-1}+1)(2^{d-2}-1)$ and 2^{2d-2} on $\mathcal{P} \setminus \{\alpha,\beta\}$.

If $G = PSL(d,q)$ with $d \geq 3$ and $v = \frac{q^d-1}{q-1}$, $G_{\alpha\beta}$ has orbit-lengths $q-1$ and $\frac{q^d-1}{q-1}-q-1$ on $\mathcal{P} \setminus \{\alpha,\beta\}$.

It follows from Corollary 2.4 that $\mathcal{D}$ is one of triple systems corresponding LINES 1-15 in Table 1.

Case 8: $G = PSL(2,q)$ with $q \equiv 1 \pmod 4$ and $v = q+1$. In this case, there are exactly two G-orbits on 3-subsets of $q+1$ points with size $\frac{q(q^2-1)}{12}$. Also, $G_{\alpha\beta} \cong Z_{\frac{q-1}{2}}$ has two orbits with length $\frac{q-1}{2}$ on $\mathcal{P} \setminus \{\alpha,\beta\}$, denoted by Γ_1 and Γ_2. Suppose that $\Gamma_1 = \{\alpha_1,\alpha_2,\ldots,\alpha_{\frac{q-1}{2}}\}$, $\Gamma_2 = \{\beta_1,\beta_2,\ldots,\beta_{\frac{q-1}{2}}\}$. For $i \in \{1,2\}$, let $\mathcal{D}_i = (\mathcal{P},\Delta_i^G)$ where $\Delta_i = \{\alpha,\beta,\gamma_i\}$ and $\gamma_i \in \Gamma_i$. It is easy to calculate that $|G_{\Delta_i}| = 6$, and hence $G_{\Delta_i} \cong S_3$. By Lemma 2.5(i), both $\mathcal{D}_1$ and $\mathcal{D}_2$ are $TS(q+1,\frac{q-1}{2})$. Let

$$g = (\alpha,\beta)(\alpha_1,\beta_1)\cdots(\alpha_{\frac{q-1}{2}},\beta_{\frac{q-1}{2}}).$$

Clearly, g is an isomorphism from $\mathcal{D}_1$ to $\mathcal{D}_2$, that is $\mathcal{D}_1 \cong \mathcal{D}_2$. Thus, $\mathcal{D}$ is a $TS(q+1,\frac{q-1}{2})$.

Case 9: $G = Sz(q)$ and $v = q^2+1$. Since G acts flag-transitively on $\mathcal{D}$, then $3 \mid |G|$ by Lemma 2.1. But this contracts the fact that $3 \nmid |G|$ (see [9, Theorem 3.6]). Therefore, there is no triple system admitting $Sz(q)$ as its flag-transitive automorphism group.

Case 10: $G = Ree(q)$ and $v = q^3+1$ with $q = 3^{2e+1} > 3$. From Lemmas 2.5 and 2.6, we have that $\mathcal{D}$ is one of triple systems corresponding LINES 17 and 18 in Table 1.

Case 11: $G = PSU(3,q)$ and $v = q^3+1$. Since $G_{\alpha\beta} \cong Z_{\frac{q^2-1}{(3,q+1)}}$ has a unique orbit O with size $q-1$ and $q(3,q+1)$ orbits with size $\frac{q^2-1}{(3,q+1)}$. Similar to proof of Lemma 2.4, we can prove that there exists a unique $TS(q^3+1,q-1)$ admitting G as its flag-transitive automorphism group.

If $q = 3^e \geq 3$, there exist subsets Δ, Σ of size 3 such that $G_\Delta^\Delta = \mathbb{Z}_3$, $G_\Sigma^\Sigma = S_3$ by the same proof as Lemma 2.6. In this case, $\mathcal{D}$ is one of triple systems corresponding LINES 20 and 21 in Table 1 from Lemma 2.5.

If $q = 5$ then $\mathcal{D}$ can only be a flag-transitive $TS(126, 8)$ in addition to $TS(126, 4)$ by a simple calculation. This means that there is no flag-transitive $TS(126, 16)$ in this case.

Unfortunately, we don't know whether Lemma 2.6 holds when $3 \nmid q$. Thus the existence of $TS(q^3 + 1, \frac{q^2-1}{(3,q+1)})$ (or $TS(q^3 + 1, \frac{2(q^2-1)}{(3,q+1)})$) with $3 \nmid q$ and $q \neq 5$ is in doubt.

This completes the proof of Theorem 1.1. □

Conjecture 3.1. *Let $\mathcal{D}$ be a triple system $TS(q^3 + 1, \lambda)$, and let $G = PSU(3, q)$ act flag-transitively on $\mathcal{D}$ with $3 \nmid q$ and $q \neq 5$. If $\lambda \neq q - 1$ then one of following holds:*

(i) *If q is even, then $\lambda = \frac{2(q^2-1)}{(3,q+1)}$.*

(ii) *If q is odd, then $\lambda = \frac{q^2-1}{(3,q+1)}$ or $\frac{2(q^2-1)}{(3,q+1)}$.*

In fact, using MAGMA, we have already proved that the conjecture holds when $q \leq 100$.

ORCID iDs

Xiaoqin Zhan https://orcid.org/0000-0003-0669-6419
Xuan Pang https://orcid.org/0000-0003-2500-9741
Suyun Ding https://orcid.org/0000-0002-6564-4427

References

[1] F. Buekenhout, A. Delandtsheer and J. Doyen, Finite linear spaces with flag-transitive groups, *J. Comb. Theory, Ser. A* **49** (1988), 268–293, doi:10.1016/0097-3165(88)90056-8, https://doi.org/10.1016/0097-3165(88)90056-8.

[2] F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck and J. Saxl, Linear spaces with flag-transitive automorphism groups, *Geom. Dedicata* **36** (1990), 89–94, doi:10.1007/bf00181466, https://doi.org/10.1007/bf00181466.

[3] P. J. Cameron, Finite permutation groups and finite simple groups, *Bull. Lond. Math. Soc.* **13** (1981), 1–22, doi:10.1112/blms/13.1.1, https://doi.org/10.1112/blms/13.1.1.

[4] P. C. Clapham, Steiner triple systems with block-transitive automorphism groups, *Discrete Math.* **14** (1976), 121–131, doi:10.1016/0012-365x(76)90055-8, https://doi.org/10.1016/0012-365x(76)90055-8.

[5] C. J. Colbourn and J. H. Dinitz (eds.), *The CRC Handbook of Combinatorial Designs*, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2nd edition, 2007, doi:10.2307/3618812, https://doi.org/10.2307/3618812.

[6] P. Dembowski, *Finite Geometries*, Classics in Mathematics, Springer-Verlag, New York, 1968, doi:10.1007/978-3-642-62012-6, https://doi.org/10.1007/978-3-642-62012-6.

[7] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1996, doi:10.1007/978-1-4612-0731-3, https://doi.org/10.1007/978-1-4612-0731-3.

[8] D. G. Higman and J. E. McLaughlin, Geometric ABA-groups, *Ill. J. Math.* **5** (1961), 382–397, doi:10.1215/ijm/1255630883, https://doi.org/10.1215/ijm/1255630883.

[9] B. Huppert and N. Blackburn, *Finite Groups II*, Springer-Verlag, New York, 1982, doi:10.1007/978-3-642-67994-0, https://doi.org/10.1007/978-3-642-67994-0.

[10] W. M. Kantor, Homogeneous designs and geometric lattices, *J. Comb. Theory, Ser. A* **38** (1985), 66–74, doi:10.1016/0097-3165(85)90022-6, https://doi.org/10.1016/0097-3165(85)90022-6.

[11] J. Key and E. Shult, Steiner triple systems with doubly transitive automorphism groups: A corollary to the classification theorem for finite simple groups, *J. Comb. Theory Ser. A.* **36** (1984), 105–110, doi:10.1016/0097-3165(84)90082-7, https://doi.org/10.1016/0097-3165(84)90082-7.

[12] H. N. Ward, On Ree's series of simple groups, *Bull. Am. Math. Soc.* **69** (1963), 113–114, doi:10.1090/S0002-9904-1963-10885-X, https://doi.org/10.1090/S0002-9904-1963-10885-X.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 24 (2024) #P2.10 / 355–383
https://doi.org/10.26493/1855-3974.2763.1e6
(Also available at http://amc-journal.eu)

There is a unique crossing-minimal rectilinear drawing of K_{18}*

Bernardo M. Ábrego, Silvia Fernández–Merchant

Departament of Mathematics, California State University at Northridge, CA, United States

Oswin Aichholzer

Institute for Software Technology, University of Technology, Graz, Austria

Jesús Leaños †

Academic Unit of Mathematics, Autonomous University of Zacatecas, Mexico

Gelasio Salazar

Institute of Physics, Autonomous University of San Luis Potosi, Mexico

Received 8 December 2021, accepted 15 June 2023, published online 14 February 2024

Abstract

We show that, up to order type isomorphism, there is a unique crossing-minimal rectilinear drawing of K_{18}. It is easily verified that this drawing does not contain any crossing-minimal drawing of K_{17}. Therefore this settles, in the negative, the following question from Aichholzer and Krasser: is it true that, for every integer $n \geq 4$, there exists a crossing-minimal drawing of K_n that contains a crossing-minimal drawing of K_{n-1}?

Keywords: Rectilinear crossing number, complete graphs, k-edges.

Math. Subj. Class. (2020): 05C10, 05C60

*We thank an anonymous referee for carefully reading an earlier version of this paper, and providing several insightful comments, corrections, and suggestions.

†Corresponding author.

E-mail addresses: bernardo.abrego@csun.edu (Bernardo M. Ábrego), silvia.fernandez@csun.edu (Silvia Fernández–Merchant), oaich@ist.tugraz.at (Oswin Aichholzer), jleanos@uaz.edu.mx (Jesús Leaños), gsalazar@ifisica.uaslp.mx (Gelasio Salazar)

1 Introduction

The *rectilinear crossing number* $\overline{\mathrm{cr}}(G)$ of a graph G is the minimum number of edge crossings in a *rectilinear* drawing of G in the plane, i.e., a drawing of G in the plane where the vertices are points in general position and the edges are straight line segments. A drawing of G with exactly $\overline{\mathrm{cr}}(G)$ crossings is *crossing-minimal*.

Determining the rectilinear crossing number $\overline{\mathrm{cr}}(K_n)$ of the complete graph K_n is a well-known open problem in combinatorial geometry (see for instance [5, 11]). In [9] Aichholzer et al. determined the exact values of $\overline{\mathrm{cr}}(K_n)$ for $13 \leq n \leq 17$. In that paper also the following question was raised.

Question 1.1. Is it true that, for every integer $n \geq 4$, there exists a crossing-minimal drawing of K_n that contains a crossing-minimal drawing of K_{n-1}?

The exact value of $\overline{\mathrm{cr}}(K_n)$ is known for $n \leq 27$ and $n = 30$ (see [3, 7, 8, 9, 10]). The value of $\overline{\mathrm{cr}}(K_{18}) = 1029$ was established in [8]. Crossing-minimal rectilinear drawings of K_n for this range of values of n can be found in [2] and [6]. In particular, from [6], we know that there are at least 37269 non-isomorphic crossing-minimal drawings of K_{17}.

Let θ denote the counterclockwise rotation of $2\pi/3$ around the origin, and let $W := \{(-51, 113), (6, 834), (16, 989), (18, 644), (18, 1068), (22, 211)\}$. From [2], we know that the 18-point set $W \cup \theta(W) \cup \theta^2(W)$ induces a crossing-minimal drawing of K_{18}. See Figure 1 for an illustration of such a point set.

Our main result is the following.

Theorem 1.2. *Up to order type isomorphism, there is a unique* 18*-point set whose induced rectilinear drawing of* K_{18} *has* $\overline{\mathrm{cr}}(K_{18})$ *crossings.*

Let $\mathcal{D}$ be the (unique, in view of Theorem 1.2) crossing-minimal rectilinear drawing of K_{18}. It is easily verified that every subdrawing of $\mathcal{D}$ with 17 points has more than $\overline{\mathrm{cr}}(K_{17}) = 798$ crossings. This settles Question 1.1 in the negative.

In the next section, we introduce the necessary notation and additional concepts required for the proof of Theorem 1.2. In Section 4 we prove Theorem 1.2.

2 k-edges, $(\leq k)$-edges, and 3-decomposability

Throughout this section, Q is a set of $n \geq 3$ points in general position in the plane. If p and q are distinct points of Q, then we denote by pq the directed line spanned by p and q, directed from p towards q. Furthermore, pq^+ and pq^- denote the set of points in Q on the right and left, respectively, of pq. Thus $Q = pq^- \cup \{p, q\} \cup pq^+$ for all $p, q \in Q$ with $p \neq q$.

Let $k \in \{0, 1, \ldots, \lfloor n/2 \rfloor - 1\}$. A *$k$-edge* of Q is a directed line spanned by two distinct points of Q, which leaves exactly k points of Q on one side. A *$(\leq k)$-edge* (respectively, a *$(> k)$-edge*) is an i-edge of Q with $0 \leq i \leq k$ (respectively, $k < i \leq \lfloor n/2 \rfloor - 1$). Let $E_k(Q), E_{\leq k}(Q)$, and $E_{>k}(Q)$ denote, respectively, the set of k-edges, $(\leq k)$-edges and $(> k)$-edges of Q. We use $e_k(Q)$, $e_{\leq k}(Q)$, and $e_{>k}(Q)$ to denote, respectively, the number of elements in $E_k(Q)$, $E_{\leq k}(Q)$, and $E_{>k}(Q)$. Then $e_{\leq k}(Q) = \sum_{j=0}^{k} e_j(Q)$ and $e_{>k}(Q) = \binom{n}{2} - e_{\leq k}(Q)$.

The vector $\mathbf{E}_{\leq k}(Q) := (e_{\leq 0}(Q), e_{\leq 1}(Q), \ldots, e_{\leq \lfloor n/2 \rfloor - 1}(Q))$ is the *$(\leq k)$-edges vector* of Q. Finally, $e_{\leq k}(n)$ denotes the minimum of $e_{\leq k}(P)$ taken over all n-point sets P

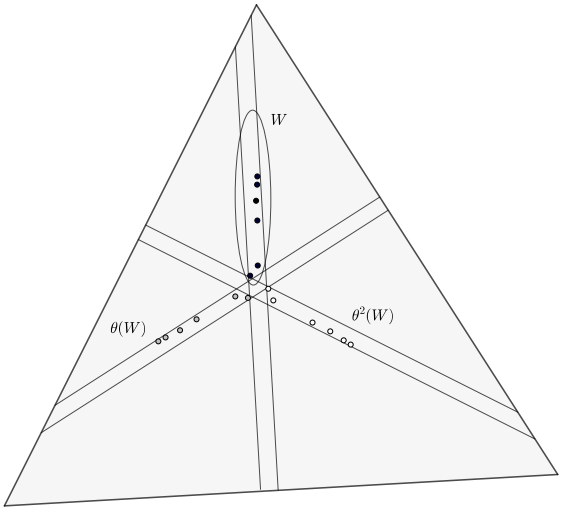


Figure 1: This is the 18-point set produced by the union of $W = \{(-51, 113), (6, 834), (16, 989), (18, 644), (18, 1068), (22, 211)\}$, $\theta(W)$ and $\theta^2(W)$. It is not difficult to see that P produces a crossing-minimal rectilinear drawing of K_{18}. The triangle and the six straight line segments show that P is 3-decomposable.

in the plane in general position. The exact determination of $e_{\leq k}(n)$ is another well known open problem in combinatorial geometry (see for instance [3, 4, 7, 8]).

The number of crossings in a rectilinear drawing of K_n and the number of k- and $(\leq k)$-edges in its underlying n-point set P are closely related by the following equality, independently proved in [4] and [12]:

$$\overline{\mathrm{cr}}(P) = \sum_{k=0}^{\lfloor n/2 \rfloor - 2} (n - 2k - 3)\, e_{\leq k}(P) - \frac{3}{4}\binom{n}{3} + \left(1 + (-1)^{n+1}\right)\frac{1}{8}\binom{n}{2}. \qquad (2.1)$$

This equality allows us to fully determine the $(\leq k)$-edges vector of any 18-point set whose induced drawing attains the rectilinear crossing number of K_{18}.

Proposition 2.1. *If P is an 18-point set such that $\overline{\mathrm{cr}}(P) = \overline{\mathrm{cr}}(K_{18})$, then $\mathbf{E}_{\leq k}(P) = (3, 9, 18, 30, 45, 63, 87, 120, 153)$.*

Proof. Let Q be an 18-point set in the plane in general position. It is known (see [3] or [7]) that $\mathbf{E}_{\leq k}(Q) = (e_{\leq 0}(Q), e_{\leq 1}(Q), \ldots, e_{\leq 8}(Q))$ is bounded below entry-wise by $(3, 9, 18, 30, 45, 63, 87, 120, 153)$. On the other hand, from (2.1) we know that

$$\overline{\mathrm{cr}}(Q) = -612 + 15 \cdot e_{\leq 0}(Q) + 13 \cdot e_{\leq 1}(Q) + \cdots + 1 \cdot e_{\leq 7}(Q).$$

From the coefficients of this equation and the fact that $e_{\leq 8}(Q) = 153$, it follows that if $e_{\leq k}(Q)$ is greater than the k-th component in the vector $(3, 9, 18, 30, 45, 63, 87, 120, 153)$, then $\overline{\mathrm{cr}}(Q) > 1029$. □

Finally, we introduce a concept that captures a property shared by all known crossing-minimal rectilinear drawings of K_n, for n a multiple of 3. A point set Q is 3-*decomposable* if it can be partitioned into three equal-size sets A, B and C, such that (i) there exists a triangle T enclosing the point set Q; and (ii) the orthogonal projection of Q onto the three sides of T shows A between B and C on one side, B between C and A on the second side, and C between A and B on the third side. In such a case, we say that $\{A, B, C\}$ is a 3-*decomposition* of Q. For instance, $\{W, \theta(W), \theta^2(W)\}$ is a 3-decomposition of the 18-point set shown in Figure 1.

As in [2], if $\{A, B, C\}$ is a 3-decomposition of Q, we define two types of edges. Let p and q be distinct points of Q. If $p, q \in A$, $p, q \in B$ or $p, q \in C$ then we call pq *monochromatic*; otherwise, pq is *bichromatic*. Let $E_k^{\text{mon}}(Q)$ and $E_k^{\text{bi}}(Q)$ denote the set of monochromatic and bichromatic k-edges of Q, respectively. As before, we use $e_k^{\text{mon}}(Q)$ and $e_k^{\text{bi}}(Q)$ to denote $|E_k^{\text{mon}}(Q)|$ and $|E_k^{\text{bi}}(Q)|$, respectively. Note that $e_k(Q) = e_k^{\text{mon}}(Q) + e_k^{\text{bi}}(Q)$. Now we partition the monochromatic edges of Q into three types. If $p, q \in A$, then we say that pq is an edge *of type* aa. Similarly, we define the edges of types bb and cc. For $x \in \{a, b, c\}$, we denote the number of monochromatic k-edges of type xx by $e_k^{xx}(Q)$. Then $e_k^{\text{mon}}(Q) = e_k^{aa}(Q) + e_k^{bb}(Q) + e_k^{cc}(Q)$.

3 Overview of the proof of Theorem 1.2

For the rest of this paper, P is an 18-point set in the plane in general position where the rectilinear crossing number of K_{18} is attained. That is, $\overline{\text{cr}}(P) = \overline{\text{cr}}(K_{18})$.

The first step in the proof, carried out in Section 4.1, consists of giving an algorithm that yields a canonical, unambiguous labelling of the points in P. The 18 points in P get labelled $x_0, x_1, \ldots, x_5, y_0, y_1, \ldots, y_5, z_0, z_1, \ldots, z_5$. Thus P gets naturally partitioned into three sets $X = \{x_0, x_1, x_2, x_3, x_4, x_5\}, Y = \{y_0, y_1, y_2, y_3, y_4, y_5\}$, and $Z := \{z_0, z_1, z_2, z_3, z_4, z_5\}$. As we shall prove shortly afterwards, $\{X, Y, Z\}$ happens to be a 3-decomposition of P.

Once we have laid out the foundation by giving a canonical labelling of the points of P, the rest of the proof consists of showing the following:

Lemma 3.1 (Implies Theorem 1.2)**.** *For each pair of distinct points $p, q \in P$, the set pq^+ is uniquely determined.*

Clearly Lemma 3.1 implies Theorem 1.2: if the lemma holds, then the unambiguity of the labelling of the points in P implies that P is unique up to order type isomorphism.

First we establish the lemma for the case in which pq is a (≤ 5)-edge. This is actually done in Section 4.1, where we give the algorithm to label the points in P. Indeed, the unambiguity in the labelling of the points in P is established in Proposition 4.3(1), and in order to prove this we need to prove simultaneously Proposition 4.3(2), which in particular implies Lemma 3.1 for the case in which pq is a (≤ 5)-edge.

We then move on to proving Lemma 3.1 for the case in which pq is a (>5)-edge, that is, when pq is either a 6-edge, or a 7-edge, or an 8-edge. As we shall see, even if this follows from elementary observations, the investigation of these cases is remarkably more involved than the case in which pq is a (≤ 5)-edge.

The first step towards the investigation of (>5)-edges is given in Section 4.2, where we prove that $\{X, Y, Z\}$ is a 3-decomposition of P. This allows us to classify each edge of P as either monochromatic or bichromatic, as we explained at the end of Section 2. Also

in Section 4.2 we show that for each $k \in \{6, 7, 8\}$ it is easy to determine the number of bichromatic k-edges and the number of monochromatic k-edges.

After proving these elementary properties of P we move on to Section 4.3. This is the most technical and long part of the paper, and its purpose is to establish a collection of structural properties of P. On a first read it may be advisable to skip this section, and only come back to it whenever its main results are invoked in Sections 4.4 and 4.5.

Finally, in Section 4.4 (respectively, Section 4.5) we prove Lemma 3.1 for the case in which pq is a monochromatic (respectively, bichromatic) 6-edge, 7-edge, or 8-edge. As we shall see, using the structural results from Section 4.3 these tasks are reduced to a relatively straightforward case analysis.

For completeness, the conclusion of the proof is presented in Section 4.6.

4 Proof of Theorem 1.2

We recall that throughout this paper, P is an 18-point set in the plane in general position such that $\overline{\mathrm{cr}}(P) = \overline{\mathrm{cr}}(K_{18})$.

4.1 The algorithm to label the 18 points in P, and proof of Lemma 3.1 when pq is a (≤ 5)-edge

It follows from Proposition 2.1 that the convex hull of P has exactly 3 vertices. Without loss of generality (the whole set P may be rotated, if necessary) we may assume that all three vertices have distinct x-coordinates. Let x_0 denote the vertex with the smallest x-coordinate. As we travel counterclockwise along the convex hull starting from x_0, let y_0 be the first vertex we find, and let z_0 be the other vertex. See Figure 2.

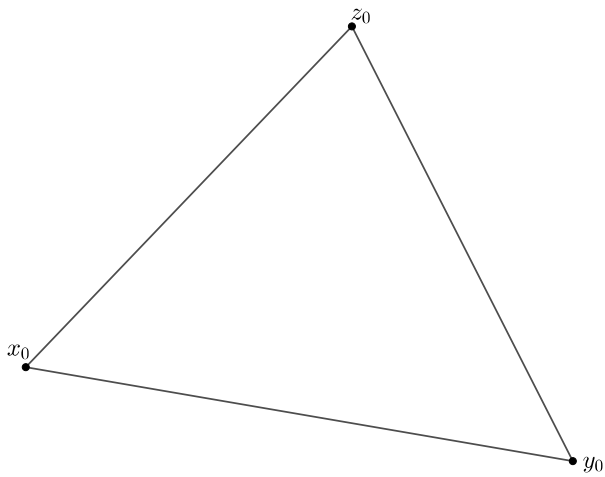


Figure 2: The convex hull of P.

Observation 4.1. $E_0(P) = \{x_0y_0, y_0z_0, x_0z_0\}$. □

We have already unambiguously determined a labelling for the three convex hull vertices of P. It remains to unambiguously determine a labelling for the remaining 15 points of P.

For $j \in \{0, \ldots, 5\}$, let $x_j^{\curvearrowright}$ denote the j-th point in P that we find as we rotate the line y_0x_0 clockwise around y_0 (we consider x_0 to be the 0-th point in P hit by the rotating line, so that $x_0^{\curvearrowright} = x_0$). We define $y_j^{\curvearrowright}$ and $z_j^{\curvearrowright}$ similarly, using z_0y_0 and x_0z_0 as the clockwise rotating lines, around z_0 and x_0, respectively. See Figure 3(a).

In an analogous manner, we let $x_j^{\curvearrowleft}$ denote the j-th point in P that we find as we rotate the line z_0x_0 counterclockwise around z_0 (again, we consider x_0 to be the 0-th point in P hit by the rotating line, so that $x_0^{\curvearrowleft} = x_0$). We define $y_j^{\curvearrowleft}$ and $z_j^{\curvearrowleft}$ similarly, using x_0y_0 and y_0z_0 as the counterclockwise rotating lines, around x_0 and y_0, respectively. See Figure 3(b).

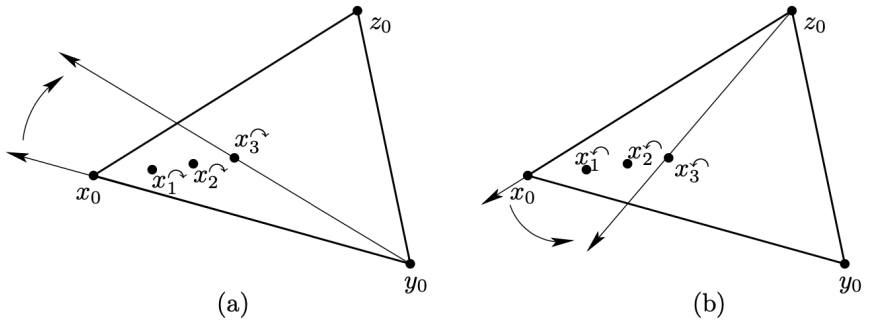


Figure 3: (a) As we rotate the line y_0x_0 clockwise around y_0, the third point in P we find is labelled $x_3^{\curvearrowright}$. The points $x_1^{\curvearrowright}$ and $x_2^{\curvearrowright}$ are also indicated. (b) As we rotate the line z_0x_0 counterclockwise around z_0, the third point in P we find is labelled $x_3^{\curvearrowleft}$. The points $x_1^{\curvearrowleft}$ and $x_2^{\curvearrowleft}$ are also indicated. By definition $x_0^{\curvearrowright} = x_0^{\curvearrowleft} = x_0$. Note that in this example $x_i^{\curvearrowright} = x_i^{\curvearrowleft}$ for $i = 0, 1, 2, 3$.

Observation 4.2. For each $j \in \{0, \ldots, 5\}$, $y_0x_j^{\curvearrowright}$, $z_0x_j^{\curvearrowleft}$, $z_0y_j^{\curvearrowright}$, $x_0y_j^{\curvearrowleft}$, $x_0z_j^{\curvearrowright}$, and $y_0z_j^{\curvearrowleft}$ are all j-edges. □

The next statement is our first major result on the structure of P. In particular, it yields a labelling of all the points of P. As it happens, this proposition simultaneously establishes Lemma 3.1 for the case in which pq is a (≤ 5)-edge.

Proposition 4.3. *Let $j \in \{0, \ldots, 5\}$. Then:*

(1) *For $u \in \{x, y, z\}$, $u_j^{\curvearrowright}$ and $u_j^{\curvearrowleft}$ are the same point, which will be denoted u_j;*

(2) *For all nonnegative integers m, n such that $m + n = j$, we have that*

(a) *$E_j(P) = \{u_mv_n \mid m+n = j$ and $uv \in \{xy, yz, zx\}\}$. Moreover, for such values of m, n, and j the following holds:*

(b) $u_m v_n^+ = \{u_i \,|\, i < m\} \cup \{v_i \,|\, i < n\}$ *for any* $uv \in \{xy, yz, zx\}$.

Proof. We prove (1) and (2) by induction on j. Since $x_0^{\curvearrowright} = x_0^{\curvearrowleft} = x_0$, $y_0^{\curvearrowright} = y_0^{\curvearrowleft} = y_0$, and $z_0^{\curvearrowright} = z_0^{\curvearrowleft} = z_0$, it follows from Observations 4.1 and 4.2 that (1) and (2) are true for $j = 0$. Now we let $t \in \{0, 1, 2, 3, 4\}$ be an integer such that (1) and (2) hold for every j such that $0 \leq j \leq t$ (in particular, the points x_j, y_j, z_j are already defined for $0 \leq j \leq t$). We complete the proof by showing that then (1) and (2) hold for $j = t + 1$.

Let $X_t := \{x_0, \ldots, x_t\}$, $Y_t := \{y_0, \ldots, y_t\}$, $Z_t := \{z_0, \ldots, z_t\}$, and $P_t := X_t \cup Y_t \cup Z_t$. From the definitions involved, it follows that $|P_t| = 3(t + 1)$. First we establish an injection $\psi\colon P_t \to E_{t+1}(P)$.

Consider any point $x_i \in X_t$. It follows from the induction hypothesis that $x_i y_{t-i}$ is a t-edge, and that $x_i y_{t-i}^+ = \{x_r \,|\, r < i\} \cup \{y_r \,|\, r < t - i\}$.

Let $\overline{x}_i$ be the first point that we find as we rotate the line $x_i y_{t-i}$ counterclockwise around x_i. It is easy to see that the induction hypothesis implies that the rotating line hits $\overline{x}_i$ with its head, and so $x_i \overline{x}_i^+ = \{x_r \,|\, r < i\} \cup \{y_r \,|\, r < t-i+1\}$. We define $\psi(x_i) = x_i \overline{x}_i$. In an analogous manner we define $\psi(y_i)$ and $\psi(z_i)$ for all $y_i \in Y_t$ and $z_i \in Z_t$. Since ψ defines a one-to-one relation and $|P_t| = 3(t + 1)$, it follows that $|\psi(P_t)| = 3(t + 1)$.

Let $E' := \{x_0 z_{t+1}^{\curvearrowleft}, y_0 x_{t+1}^{\curvearrowleft}, z_0 y_{t+1}^{\curvearrowleft}\}$. Observation 4.2 implies that $E' \subset E_{t+1}(P)$. We note that $\psi(x_0) = x_0 y_{t+1}^{\curvearrowleft}$, $\psi(y_0) = y_0 z_{t+1}^{\curvearrowleft}$, and $\psi(z_0) = z_0 x_{t+1}^{\curvearrowleft}$. Using these observations and that $\{x_{t+1}^{\curvearrowleft}, y_{t+1}^{\curvearrowleft}, z_{t+1}^{\curvearrowleft}\} \cap P_t = \emptyset$, it follows that $E' \cap \psi(P_t) = \emptyset$. On the other hand, from Proposition 2.1 it follows that $|E_{t+1}(P)| = 3(t + 2)$. Thus $E_{t+1}(P)$ is the disjoint union of $\psi(P_t)$ and E'.

By way of contradiction, suppose that $x_{t+1}^{\curvearrowright} \neq x_{t+1}^{\curvearrowleft}$. Then each point of $\{x_1, \ldots, x_t\}$ is contained in the interior of the quadrilateral bounded by $y_0 x_{t+1}^{\curvearrowright}$, $z_0 x_{t+1}^{\curvearrowleft}$, $z_0 x_0$, and $x_0 y_0$ (see Figure 4). From the induction hypothesis it follows that $x_{t+1}^{\curvearrowright} x_{t+1}^{\curvearrowleft} \notin E_{\leq t}(P)$. This and the fact that $x_{t+1}^{\curvearrowright} x_{t+1}^{\curvearrowleft} \notin \psi(P_t) \cup E'$ imply that $|x_{t+1}^{\curvearrowright} x_{t+1}^{\curvearrowleft\,-}| \geq t+2$. Then the interior of the triangle T bounded by $y_0 x_{t+1}^{\curvearrowright}$, $z_0 x_{t+1}^{\curvearrowleft}$, and $x_{t+1}^{\curvearrowright} x_{t+1}^{\curvearrowleft}$ is nonempty, and, moreover, it contains every element of $Q := x_{t+1}^{\curvearrowright} x_{t+1}^{\curvearrowleft\,-} \setminus \{x_0, x_1, \ldots, x_t\}$. Let p be the first point of Q that $z_0 x_{t+1}^{\curvearrowleft}$ finds as it is rotated counterclockwise around $x_{t+1}^{\curvearrowleft}$. Then $x_{t+1}^{\curvearrowleft} p$ must be a $(t + 1)$-edge of P. On the other hand, it is immediately seen that $x_{t+1}^{\curvearrowleft} p \notin \psi(P_t) \cup E'$, contradicting that $E_{t+1} = \psi(P_t) \cup E'$.

This contradiction shows that $x_{t+1}^{\curvearrowright}$ and $x_{t+1}^{\curvearrowleft}$ are the same point. Analogous arguments show that $y_{t+1}^{\curvearrowright}$ and $y_{t+1}^{\curvearrowleft}$ are the same point, and that $z_{t+1}^{\curvearrowright}$ and $z_{t+1}^{\curvearrowleft}$ are the same point. This proves (1) for $j = t + 1$.

Now we show that (2) holds for $j = t + 1$. Note that at this point $x_{t+1}, y_{t+1}, z_{t+1}$ are all well-defined. For each $m \in \{0, 1, \ldots, t + 1\}$, we let $X_m := \{x_i \,|\, i \leq m\}$, $Y_m := \{y_i \,|\, i \leq m\}$, and $Z_m := \{z_i \,|\, i \leq m\}$.

Let $m \in \{0, 1, 2, \ldots, t + 1\}$. We shall show that

(i) $x_m y_{t+1-m}$ is in $E_{t+1}(P)$; and

(ii) $x_m y_{t+1-m}^+ = X_{m-1} \cup Y_{t-m}$.

By symmetry, analogous arguments show that: (i') $y_m z_{t+1-m}$ is in $E_{t+1}(P)$; (ii') $y_m z_{t+1-m}^+ = Y_{m-1} \cup Z_{t-m}$; (i") $z_m x_{t+1-m}$ is in $E_{t+1}(P)$; and (ii") $z_m x_{t+1-m}^+ = Z_{m-1} \cup X_{t-m}$. Note that these six assertions, together with the fact that $|E_{t+1}(P)| = 3(t + 2)$, imply (2).

Thus we complete the proof by showing (i) and (ii).

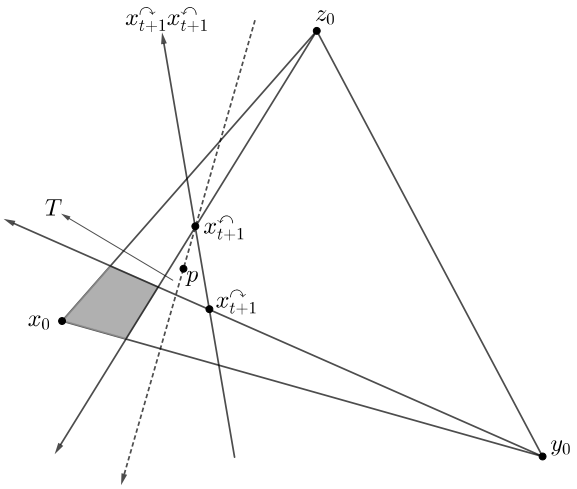


Figure 4: If $x^{\curvearrowright}_{t+1} \neq x^{\curvearrowleft}_{t+1}$, then the triangle T contains a point p such that $x^{\curvearrowleft}_{t+1}p$ is a $(t+1)$-edge of P.

Since $x_{t+1} = x^{\curvearrowleft}_{t+1} = x^{\curvearrowright}_{t+1}$, $y_{t+1} = y^{\curvearrowleft}_{t+1} = y^{\curvearrowright}_{t+1}$, and $z_{t+1} = z^{\curvearrowleft}_{t+1} = z^{\curvearrowright}_{t+1}$, it follows that (i) and (ii) hold whenever m is in $\{0, t+1\}$. Thus it suffices to prove (i) and (ii) for $1 \leq m \leq t$.

From the induction hypothesis we have that $x_{m-1}y^{+}_{t+1-m} = X_{m-2} \cup Y_{t-m}$ and $x_m y^{+}_{t-m} = X_{m-1} \cup Y_{t-m-1}$. Also note that $X_{m-1} \cup Y_{t-m} \subseteq x_m y^{+}_{t+1-m}$.

Let B denote the triangle bounded by the lines $x_{m-1}y_{t+1-m}$, $x_m y_{t-m}$, and $x_m y_{t+1-m}$ (see Figure 5). Let P_B be the set of points of P contained in the interior of B.

We claim that $P_B = \emptyset$. By way of contradiction, suppose this is not the case. Let $L = p_1 p_2 \cdots p_k$ be the lower chain of the convex hull of $P_B \cup \{x_m, y_{t+1-m}\}$. Then $p_1 = x_m$ and $p_k = y_{t+1-m}$, where (since $B \neq \emptyset$) $k \geq 3$. We note that $p_i p^{+}_{i+1} = X_{m-1} \cup Y_{t-m}$ for all $i = 1, 2, \ldots, k-1$. Thus each edge of L is a $(t+1)$-edge. We recall that $E_{t+1}(P) = \psi(P_t) \cup E'$. It is readily seen that no edge of L is in E', and so every edge of L is in $\psi(P_t)$. In particular, the line p_2p_3 is in $\psi(P_t)$.

Recall that every edge in $\psi(P_t)$ is obtained by starting with a line $v_i w_{t-i}$ (for $v, w \in \{x, y, z\}, v \neq w$), counterclockwise rotating it around v_i, and recording the first point p in P hit by the rotating line: $\psi(v_i)$ is then the line $v_i p$. Thus, in particular p_2p_3 is obtained in this way. Now if we reverse the process and clockwise rotate p_2p_3 around p_2, the first point hit by the rotating line must be y_{t-m}. This implies that $p_2 = x_m$, contradicting that $p_1 = x_m$. We therefore conclude that $P_B = \emptyset$. Finally, note that $P_B = \emptyset$ immediately implies that $\psi(x_m) = x_m y_{t+1-m}$. Thus $x_m y_{t+1-m}$ is a $(t+1)$-edge. This proves (i). Moreover, as we observed above, $X_{m-1} \cup Y_{t-m} \subseteq x_m y^{+}_{t+1-m}$. Since $|X_{m-1} \cup Y_{t-m}| = t+1$, then $X_{m-1} \cup Y_{t-m} = x_m y^{+}_{t+1-m}$. Thus (ii) follows. □

In view of Proposition 4.3(1), we have achieved our goal to unambiguously identify

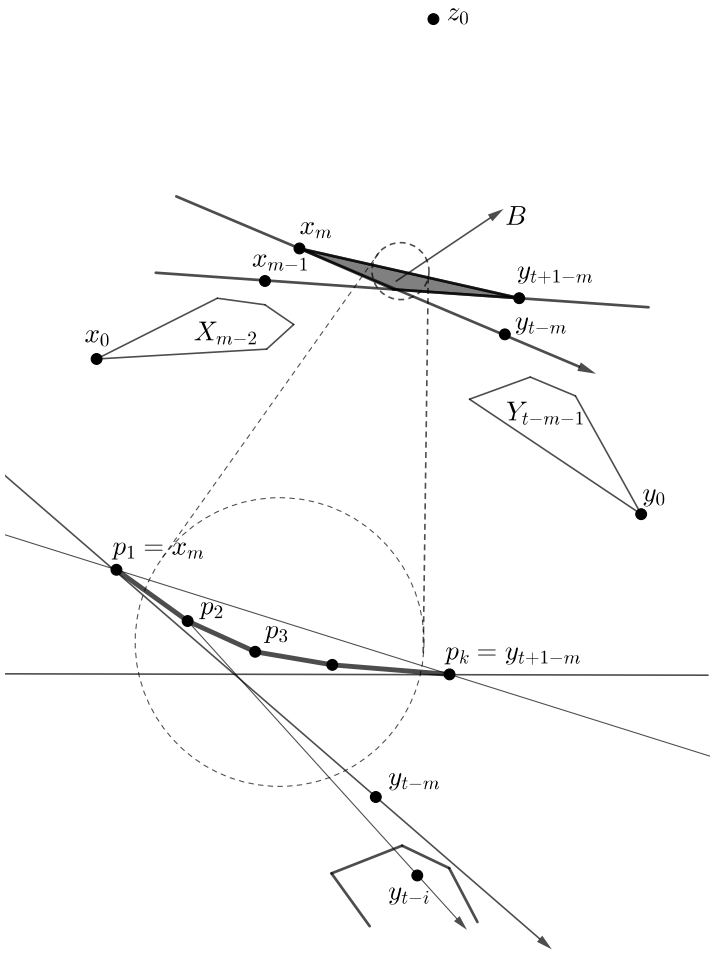


Figure 5: If the interior of the triangle B is nonempty, then every edge of the convex chain $p_1, p_2, \ldots, p_k$ is a $(t+1)$-edge.

(and label) all 18 points of P. For the rest of the paper, we let $X := \{x_0, x_1, \ldots, x_5\}$, $Y := \{y_0, y_1, \ldots, y_5\}$, and $Z := \{z_0, z_1, \ldots, z_5\}$, where x_j, y_j, and z_j are as in Proposition 4.3, for $j = 0, 1, \ldots, 5$.

4.2 $\{X, Y, Z\}$ is a 3-decomposition of P

If we rotate the line x_0z_0 clockwise along x_0, then for $j = 1, 2, \ldots, 5$, the j-th point hit by the rotating line is z_j. If we rotate the line x_0y_0 counterclockwise along x_0, then for $j = 1, 2, \ldots, 5$, the j-th point hit by the rotating line is y_j. It follows that the sixth point hit by the clockwise rotating line ℓ_x is in X, and the sixth point hit by the counterclockwise rotation line ℓ'_x is also in X (see Figure 6). These two points in X are obviously distinct (since $|X| > 2$), and so they define an infinite cone C_X with vertex x_0 (here by *cone with vertex* p we mean a pair of distinct directed rays, both with startpoint p). Note that C_X is the smallest infinite cone with vertex x_0 that contains X. See Figure 6.

We similarly find infinite cones C_Y (with vertex y_0) and C_Z (with vertex z_0).

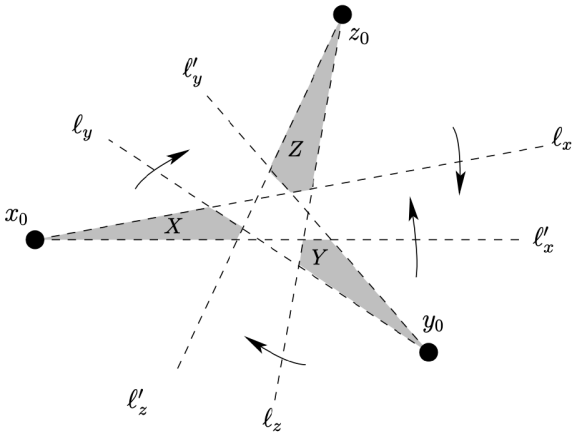


Figure 6: The sets X, Y, and Z are contained in the indicated (closed) shaded regions. The shaded region containing X is $\Delta_{X,Y} \cap \Delta_{X,Z}$.

Now $C_X \cup C_Y$ divide the plane into several regions, three of which are bounded. Two of these bounded regions are triangles: one triangle $\Delta_{X,Y}$ with x_0 as a vertex and another triangle $\Delta_{Y,X}$ with y_0 as a vertex; the other one is a quadrilateral. The entire set X is contained in $\Delta_{X,Y}$, and the entire set Y is contained in $\Delta_{Y,X}$. By considering the pair C_X, C_Z (respectively, C_Y, C_Z), we obtain triangles $\Delta_{X,Z}$ and $\Delta_{Z,X}$ (respectively, $\Delta_{Y,Z}$ and $\Delta_{Z,Y}$). Thus $X \subseteq \Delta_{X,Y} \cap \Delta_{X,Z}$, $Y \subseteq \Delta_{Y,X} \cap \Delta_{Y,Z}$, and $Z \subseteq \Delta_{Z,X} \cap \Delta_{Z,Y}$. Hence the situation is as illustrated in Figure 6. In this figure, each of $\Delta_{X,Y} \cap \Delta_{X,Z}$, $\Delta_{Y,X} \cap \Delta_{Y,Z}$, and $\Delta_{Z,X} \cap \Delta_{Z,Y}$ is a quadrilateral, although it is easy to see that any (or all) of them may be a triangle.

In view of this, it follows immediately that there is a triangle that witnesses the following:

Proposition 4.4. *P is 3-decomposable, with 3-decomposition $\{X, Y, Z\}$.* □

As we mentioned in Section 2, knowing that $\{X, Y, Z\}$ is a 3-decomposition of P

allows us to classify each edge of P as either monochromatic or bichromatic: for $p, q \in P$, the edge pq is *monochromatic* if p and q belong to the same set of the 3-decomposition $\{X, Y, Z\}$. Otherwise, pq is *bichromatic*.

We close this section by noting that using the 3-decomposability of P it is easy to determine the number of bichromatic and monochromatic k-edges in P, for each $k \in \{0, \ldots, 8\}$.

Indeed, since P is 3-decomposable it follows from [2, Claim 1] that $e^{\mathrm{bi}}_{\leq k}(P) = 3\binom{k+2}{2}$ for $k \in \{0, \ldots, 5\}$, $e^{\mathrm{bi}}_{\leq 6}(P) = 81$, and $e^{\mathrm{bi}}_{\leq 7}(P) = 99$. Also note that $e^{\mathrm{bi}}_{\leq 8}(P)$ is the total number of bichromatic edges of P, namely $3 \cdot 6 \cdot 6 = 108$. Using that $e^{\mathrm{bi}}_{j}(P) = e^{\mathrm{bi}}_{\leq j}(P) - e^{\mathrm{bi}}_{\leq j-1}(P)$ for $j \in \{1, \ldots, 8\}$, we obtain the following.

Proposition 4.5. $e^{\mathrm{bi}}_{k}(P) = 3(k+1)$ *for* $k \in \{0, \ldots, 5\}$, $e^{\mathrm{bi}}_{6}(P) = 18$, $e^{\mathrm{bi}}_{7}(P) = 18$, *and* $e^{\mathrm{bi}}_{8}(P) = 9$.

To obtain $e^{\mathrm{mon}}_{6}(P), e^{\mathrm{mon}}_{7}(P)$ and $e^{\mathrm{mon}}_{8}(P)$, we note that Proposition 2.1 implies that $e_6(P) = 24, e_7(P) = 33$, and $e_8(P) = 33$. Since $e_j(P) = e^{\mathrm{bi}}_{j}(P) + e^{\mathrm{mon}}_{j}(P)$ for $j = 0, \ldots, 8$, Proposition 4.5 implies the following.

Corollary 4.6. $e^{\mathrm{mon}}_{k}(P) = 0$ *for* $k \in \{0, \ldots, 5\}$, $e^{\mathrm{mon}}_{6}(P) = 6$, $e^{\mathrm{mon}}_{7}(P) = 15$, *and* $e^{\mathrm{mon}}_{8}(P) = 24$.

4.3 Structural properties of P

4.3.1 Determination of $e^{uu}_{k}(P)$ for any $u \in \{x, y, z\}$ and any $k \in \{0, \ldots, 8\}$

Let $u \in \{x, y, z\}$, $i \in \{1, 2, \ldots, 5\}$, and ℓ_u, ℓ'_u be the directed rays forming the cone C_U with vertex u_0 mentioned in the arguments leading to Proposition 4.4. See Figure 6. From now on, we shall use u^i_0 to denote the i-th point of P that ℓ_u finds when it is rotated clockwise around of u_0 until it reaches ℓ'_u. Clearly, $\{u^1_0, u^2_0, \ldots, u^5_0\} = \{u_1, u_2, \ldots, u_5\}$.

Our next observation is evident, but useful.

Observation 4.7. Let v_1, v_2, and v_3 be three distinct points in P, and let $\ell := v_1v_2$ and $\ell' := v_1v_3$. Let $P_1 := \ell^- \cap \ell'^+$, $P_2 := \ell^+ \cap \ell'^+$, and $P_3 := \ell^- \cap \ell'^-$. Then P_1, P_2, and P_3 are pairwise disjoint subsets of P. See Figure 7. For $i = 1, 2, 3$, let r_i be the number of points in P_i. If $P \setminus \{v_1, v_2, v_3\}$ is the disjoint union of P_1, P_2, and P_3, and p_i is the i-th point of P_1 that ℓ finds when it is rotated counterclockwise around v_1 until it reaches ℓ', then v_1p_i is a j-edge of P for $j = \min\{r_2 + i, 16 - (r_2 + i)\}$.

The next observation is immediate from the definition of u^i_0 and Observation 4.7.

Observation 4.8. Let $u \in \{x, y, z\}$. Then

(1) $u_0u^1_0$ and $u_0u^5_0$ are both 6-edges,

(2) $u_0u^2_0$ and $u_0u^4_0$ are 7-edges and they are the only 7-edges of the type u_0u, and

(3) $u_0u^3_0$ is an 8-edge.

Claim 4 in [2] implies that $e^{uu}_{8}(P) \leq 8$ for each $u \in \{x, y, z\}$. Using this, together with Observation 4.8 and Corollary 4.6, we obtain the following.

Proposition 4.9. *Let* $u \in \{x, y, z\}$. *Then* $e^{uu}_{k}(P) = 0$ *for* $k \in \{0, \ldots, 5\}$, $e^{uu}_{6}(P) = 2$, $e^{uu}_{7}(P) = 5$, *and* $e^{uu}_{8}(P) = 8$.

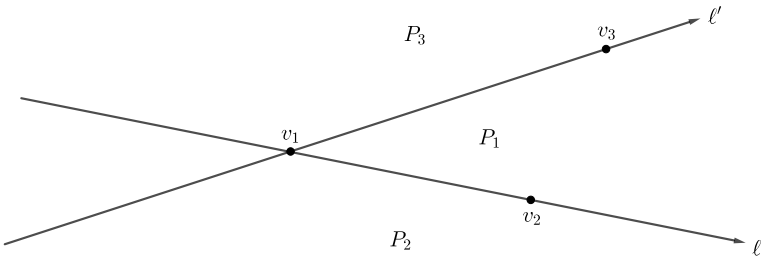


Figure 7: The i-th point of $P_1 := \ell^- \cap \ell'^+$ that ℓ finds when it is rotated counterclockwise around v_1 is a j-edge for $j = \min\{r_2 + i, 16 - (r_2 + i)\}$, where r_2 denotes the number of points of $P_2 := \ell^+ \cap \ell'^+$.

The next corollary follows immediately from Observation 4.8(1) and Proposition 4.9.

Corollary 4.10. $E_6^{\mathrm{mon}}(P) = \{x_0x_0^1, x_0x_0^5, y_0y_0^1, y_0y_0^5, z_0z_0^1, z_0z_0^5\}$. *Moreover, any other monochromatic edge must belong to* $E_7^{\mathrm{mon}}(P) \cup E_8^{\mathrm{mon}}(P)$.

4.3.2 Determination of the convex hull of U for $U \in \{X, Y, Z\}$ and related facts

Let u be any element of $\{x, y, z\}$. One of the main goals in this subsection is to show that the triangle formed by u_0, u_4 and u_5 contains in its interior the remaining u's, namely, u_1, u_2 and u_3. We also prove other statements about the relative position of the elements of U. Almost all these assertions will be used in the subsequent steps later on.

Proposition 4.11. *Let* $u \in \{x, y, z\}$. *If* $u_1 \in \{u_0^2, u_0^4\}$, *then there are at least three* 7*-edges of type* uu *involving* u_1 *but not* u_0.

Proof. We prove the proposition for the case $u = x$. The cases $u = y$ and $u = z$ are handled in a totally analogous manner.

Suppose that $x_1 = x_0^4$. Then $\ell := x_0x_1$ leaves x_0^1, x_0^2 and x_0^3 on its left halfplane (and x_0^5 on its right halfplane). Let z' be the first z that ℓ finds when it is rotated counterclockwise around x_1, and let $\ell' = x_1z'$. See Figure 8. By Corollary 4.10, we know that $\{x_1x_0^1, x_1x_0^2, x_1x_0^3\} \subset E_7^{\mathrm{mon}}(P) \cup E_8^{\mathrm{mon}}(P)$. Then ℓ finds each of x_0^1, x_0^2 and x_0^3 before it reaches z'. This and Observation 4.7 imply that at most one of $x_1x_0^1, x_1x_0^2, x_1x_0^3$ is an 8-edge and, by Corollary 4.10, the other two must be 7-edges.

From the way in that the x's were labelled it follows that x_0^5 is the first x that ℓ finds when it is rotated clockwise around x_1, and so $x_1x_0^5$ is a (≤ 7)-edge. This and Corollary 4.10 imply that $x_1x_0^5$ is the third required 7-edge. The case $x_1 = x_0^2$ can be handled in an analogous manner (y's play the role of z's). □

Proposition 4.12. *Let* $u \in \{x, y, z\}$ *and* $\{p, q\} = \{x, y, z\} \setminus \{u\}$. *Suppose that* $\{q_0, \ldots, q_5\} \subset u_0u_0^{3-}$ *and that* $\{p_0, \ldots, p_5\} \subset u_0u_0^{3+}$. *Then:*

(A1) $u_1 \notin \{u_0^1, u_0^5\}$;

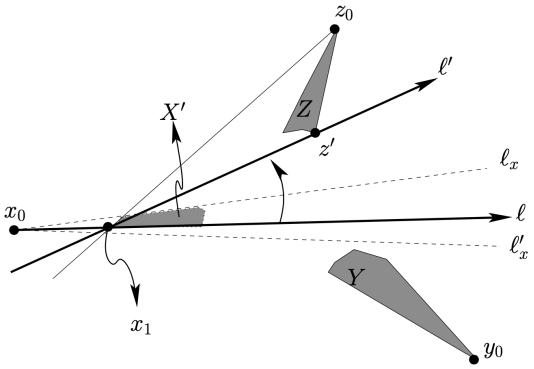


Figure 8: Here x_0x_1 is a 7-edge.

(A2) *there are at least two* 7*-edges of type* uu *involving* u_1 *but not* u_0*;*

(A3) $u_2 \notin \{u_0^1, u_0^5\}$*;*

(A4) *each of* u_3u_4, u_3u_5 *and* u_4u_5 *is an* 8*-edge;*

(A5) $\{u_0^1, u_0^5\} = \{u_4, u_5\}$*;*

(A6) *the triangle formed by* u_0, u_4 *and* u_5 *is the convex hull of* U*; and*

(A7) *if* $u_5 \in u_0u_4^+$*, then* $u_0u_4^- = \{q_0, \ldots, q_5\}$ *and* $u_0u_5^+ = \{p_0, \ldots, p_5\}$*. Otherwise,* $u_0u_4^+ = \{p_0, \ldots, p_5\}$ *and* $u_0u_5^- = \{q_0, \ldots, q_5\}$ *.*

Proof. By rotating P if necessary, and exchanging appropriately the labels x, y, and z, we can assume, without any loss of generality, that $u = x, p = y, q = z$ and that X, Y and Z are placed as in Figure 9.

(A1): Seeking a contradiction, suppose that $x_0^1 = x_1$. Let v be the first point that x_0x_1 finds when it is rotated clockwise around x_1 as shown in Figure 9(a). Note that $v \in Y$, as otherwise $v \in \{x_2, x_3, x_4, x_5\}$ and $x_1v^- = Z$. Then x_1v is a 6-edge, contradicting Corollary 4.10. Let x' be the last element of $\{x_2, x_3, x_4, x_5\}$ that x_1v finds when it is rotated clockwise around x_1. Since $v \in Y$, then x_1x' must be a (≤ 6)-edge, contradicting Proposition 4.9. The case $x_0^5 = x_1$ can be handled in an analogous manner (with the roles of Z and Y interchanged).

(A2): From (A1) we know that x_0x_1 leaves at least one x in each side. By definition of x_1, the points x_2, x_3, x_4 and x_5 must be contained in $X' := X \cap x_1z_0^+ \cap x_1y_0^-$, see Figure 9(b). Let x' be the last element of $\{x_2, x_3, x_4, x_5\}$ that x_0x_1 finds when it is rotated clockwise around x_1 as shown in Figure 9(b). Note that x_1x' must be a (≤ 7)-edge. Since $x' \neq x_0$, then Proposition 4.9 implies that x_1x' must be a 7-edge. Similarly, if we rotate x_0x_1 in the other direction, then we can find the other 7-edge involving x_1 but not x_0.

(A3): Seeking a contradiction, suppose that $x_2 = x_0^1$. Then x_0x_2 is a 6-edge, and x_3, x_4 and x_5 are contained in $X'' := X \cap x_0^1y_0^-$. See Figure 10(b). From Observation 4.7, we know that at most one of x_2x_3, x_2x_4, x_2x_5 is an 8-edge. This and Corollary 4.10 imply

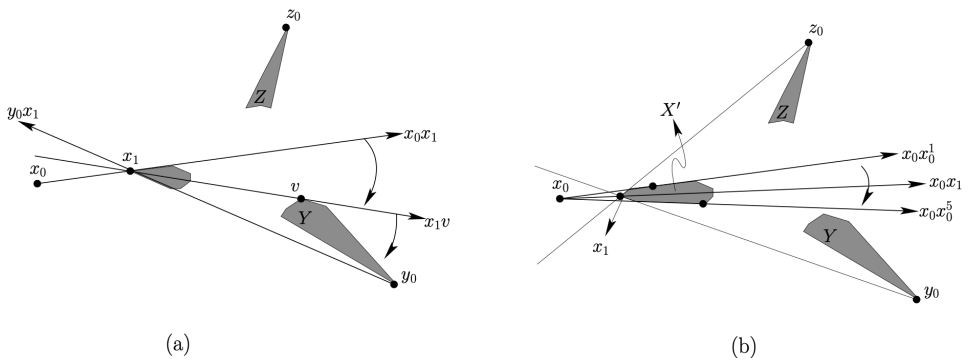


Figure 9: (a) x_0x_1 cannot be a 6-edge. (b) There are at least two 7-edges of type xx involving x_1 but not x_0.

that at least two of x_2x_3, x_2x_4, x_2x_5 are 7-edges. This together with Observation 4.8(2) and (A2) imply that $e_7^{xx}(P) \geq 6$, which contradicts Proposition 4.9. The case $x_2 = x_0^5$ can be handled in an analogous manner.

(A4): From Corollary 4.10, Observation 4.8(1), and (A1), we know that x_0x_1 is a 7-edge or an 8-edge. First suppose that x_0x_1 is a 7-edge. Then $x_1 \in \{x_0^2, x_0^4\}$. This together with Propositions 4.9 and 4.11 and Observation 4.8(2) imply that each element of $E_7^{xx}(P)$ contains at least one of x_0 or x_1. This fact and Proposition 4.9 imply that x_3x_4, x_3x_5 and x_4x_5 are 8-edges, as required.

Now, we suppose that x_0x_1 is an 8-edge. Then $x_2 \in x_0x_1^-$ or $x_2 \in x_0x_1^+$. We only analyze the case $x_2 \in x_0x_1^-$ (the other case is symmetric). Then we must have that $X' := X \cap x_0x_1^+ \cap x_2y_0^-$ contains exactly two elements x', x'' of $\{x_3, x_4, x_5\}$, see Figure 10(a). Now we rotate x_2y_0 clockwise around x_2 until it be parallel to x_0x_1. See Figure 10(a). From Observation 4.7 and Corollary 4.10, we know that at least one of x_2x', x_2x'' is a 7-edge. Such a 7-edge plus the four 7-edges provided by Observation 4.8(2) and (A2) give us, 5, the total number of 7-edges of P. This and Proposition 4.9 imply that x_3x_4, x_3x_5, x_4x_5 are 8-edges, as required.

(A5): Seeking a contradiction, suppose that $\{x_0^1, x_0^5\} \neq \{x_4, x_5\}$. Then (A1) and (A3) imply that $x_3 = x_0^1$ or $x_3 = x_0^5$. Again, by symmetry it is enough to analyze the case $x_3 = x_0^1$. Clearly, both x_1 and x_2 are contained in the triangle formed by $x_0x_3, x_0x_0^5$ and x_3y_0; and x_4, x_5 are contained in $X'' := X \cap x_0^1y_0^-$, see Figure 10(b).

Now we rotate x_0x_3 clockwise around x_3 until it reaches x_3y_0, and note that such a rotation hits x_4 and x_5. From Observation 4.7 we know that at most one of x_3x_4 or x_3x_5 is 8-edge, contradicting (A4).

(A6): This follow directly from (A5) and the way in that the x's were labelled.

(A7): Suppose that $x_5 \in x_0x_4^+$. Then (A5) implies that $x_0^1 = x_4$ and $x_0^5 = x_5$. The required equalities follow from the definition of x_0^1 and x_0^5 and the hypotheses $Z \subset x_0x_0^{3-}$ and $Y \subset x_0x_0^{3+}$. Similarly, we can deduce that $x_0x_5^- = Z$ and $x_0x_4^+ = Y$ whenever $x_5 \in x_0x_4^-$. □

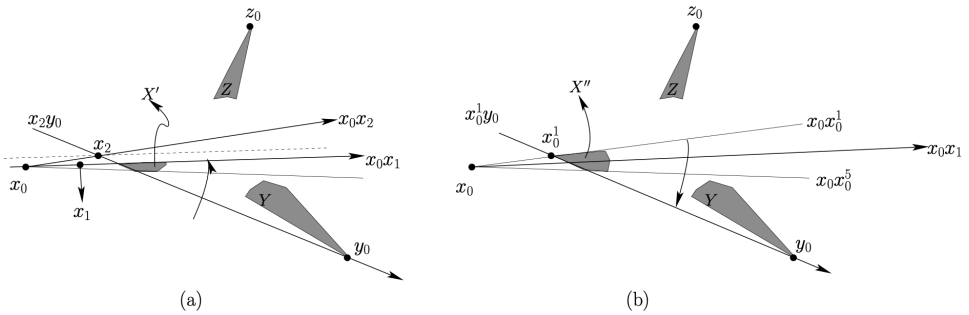


Figure 10: (a) x_3x_4, x_3x_5, x_4x_5 are 8-edges. The dotted straight line containing x_2 is parellel to x_0x_1. (b) $\{x_0^1, x_0^5\} = \{x_4, x_5\}$, and hence x_0x_4 and x_0x_5 are 6-edges.

4.3.3 Determination of the position of u_5 with respect to u_0u_4 for each $u \in \{x, y, z\}$

Our main goal in this subsection is to show that $u_5 \in u_0u_4^+$ for each $u \in \{x, y, z\}$. In order to prove this, we need to establish some auxiliary statements that will also be used later on.

Let $u, v \in \{x, y, z\}$ with $u \neq v$. We will say that u_4u_5 *splits* the v's to mean that u_4u_5 separates $\{u_0, \ldots, u_3\} \cup \{v_0, \ldots, v_3\}$ from the rest of the points of $P \setminus \{u_4, u_5\}$.

Proposition 4.13. *Let $\{u, v, w\} = \{x, y, z\}$, and suppose that u_0u_5 separates u_4 from the v's. Then u_4u_5 splits the v's.*

Proof. By rotating and/or reflecting P along u_0u_4, if necessary, we can assume that $u = x, v = y, w = z$ and that X, Y and Z are placed as in Figure 6.

Since x_0x_5 separates x_4 from the y's, then $x_5 \in x_0x_4^+$. From Proposition 4.3 we know that $x_4y_0^+ = \{x_0, x_1, x_2, x_3\}$. Then (A6) implies that $x_4y_0^+ \subseteq x_4x_5^+$. If we rotate x_4y_0 counterclockwise around x_4 until it reaches x_0x_4, then $x_5 \in x_0x_4^+$, (A6), and Observation 4.7 together imply that at most one element of $\{x_4x_5\} \cup \{x_4y \big| y \in Y\}$ is an 8-edge. This and (A4) imply that such an 8-edge must be x_4x_5. Then (A6) implies that x_4x_5 leaves exactly four y's on its right. Moreover, from Proposition 4.3 it is easy to see that y_0 and y_1 are in $x_4x_5^+$. Let y_i and y_j be two elements of Y in $x_4x_5^-$. Without loss of generality, we can assume that $i < j$. Then $2 \leq i < j \leq 5$.

From (A6) we know that the triangle formed by y_0, y_4, and y_5 is the convex hull of Y. This implies that $j \in \{4, 5\}$. Seeking a contradiction, suppose that $i \in \{2, 3\}$.

Let T be the triangle formed by x_0x_5, x_0y_i and x_4x_5. See Figure 11(b). By the way y's were labelled, we know that if $y_r \in T$ then $r \in \{i+1, \ldots, 5\} \setminus \{j\}$. Let y' be the first point in $Y \cap T$ that y_ix_0 finds when it is rotated clockwise around y_i. See Figure 11(b). Then y_iy' is a $(\leq i + 4)$-edge because the points of P lying in the left side of y_iy' is a subset of $\{x_0, \ldots, x_3, y_0, \ldots, y_{i-1}\}$. If $i = 2$, then y_iy' is a (≤ 6)-edge which does not involve y_0, contradicting Corollary 4.10. Finally, if $i = 3$, then y_iy' is a (≤ 7)-edge, contradicting (A4). □

Observation 4.14. From Proposition 4.13 we know that if $\{u, v, w\} = \{x, y, z\}$, then u_4u_5 splits the v's or the w's.

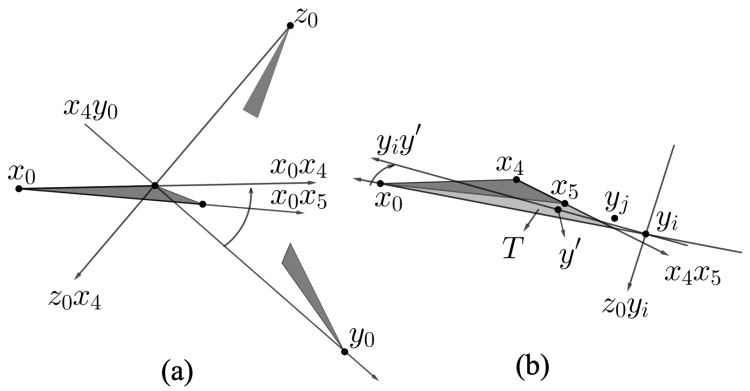


Figure 11: (a) If $x_4 \in x_0x_5^-$, then x_4x_5 splits Y. (b) There are exactly two y's, namely y_i and y_j, in $x_4x_5^-$.

Proposition 4.15. *Let u and v be two distinct elements of $\{x, y, z\}$. If u_4u_5 splits the v's, and v_3v_5 leaves u_0 and v_2 on the same side, then v_4v_5 splits the u's.*

Proof. By rotating P if necessary and exchanging appropriately the labels x, y and z, we can assume that $u = x$ and that X, Y and Z are placed as in Figure 6.

CASE 1: Suppose that x_4x_5 splits the y's. Then we need to show that if y_3y_5 leaves x_0 and y_2 on the same side, then y_4y_5 splits the x's.

From (A4), we know that y_4y_5 is an 8-edge, and from (A6), that y_4y_5 is in the convex hull of Y.

First, we show that $y_5 \in y_0y_4^-$. By way of contradiction, suppose this is not the case. Then $y_5 \in y_0y_4^+$ and the triangle formed by y_0, y_4 and y_5 looks like in Figure 12(a). Since x_4x_5 splits the y's, then x_4x_5 separates y_3 from y_4 and y_5, and so all the x's are on the left side of both y_3y_4 and y_3y_5. In particular, $x_0 \in y_3y_5^-$, and hence $y_2 \in y_3y_5^-$. Then $y_2 \in y_3y_5^- \cap z_0y_3^-$, and so y_2 is contained in the triangle Q formed by y_0y_4, z_0y_3, y_3y_5. See Figure 12(b). Since y_3y_4 is an 8-edge by (A4), and y_3y_4 leaves $\{y_0, y_2, x_0, \ldots, x_5\}$ on its left, then it leaves y_1, y_5 on its right. This and the fact that $y_1 \in z_0y_3^-$ imply that y_1 is contained in the triangle R formed by z_0y_3, y_3y_4, y_0y_5. See Figure 12(b). Then y_2y_4 and y_0y_1 are 7-edges. This, together with Observation 4.8(2) and Proposition 4.11, implies $e_7^{yy}(P) \geq 6$, the required contradiction. Thus, we can conclude that y_0y_4 leaves the x's and y_5 on the same side, and the desired result follows from Proposition 4.13.

CASE 2: x_4x_5 splits the z's. Follow the same argument as in CASE 1 with left, right, $y, z, -$ and $+$ in place of right, left, $z, y, +$ and $-$, respectively. □

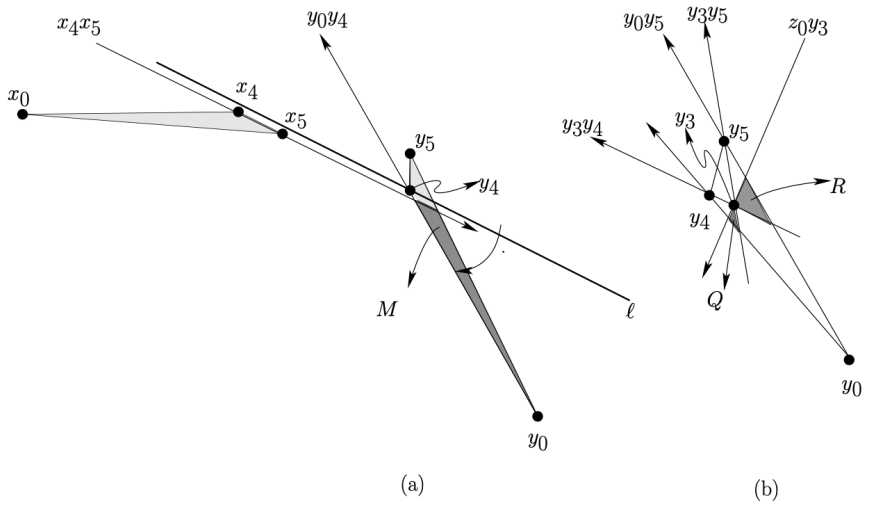


Figure 12: (a) $y_5 \in y_0y_4^+$. (b) y_2 is in Q and y_1 is in R.

Proposition 4.16. *If $u \in \{x, y, z\}$, then u_3u_5 leaves u_0 and u_1 on the same side.*

Proof. As in Proposition 4.15, we can assume that $u = x$ and that X, Y and Z are placed as in Figure 6. From (A4), we know that x_3x_5 is an 8-edge. Seeking a contradiction, suppose that x_3x_5 separates x_0 from x_1.

First, suppose that x_4x_5 splits the y's. Since P is placed as in Figure 6, then $x_0 \in x_3x_5^+$, and hence, $x_1 \in x_3x_5^-$. Then $x_3x_5^+ = \{x_0, x_2\} \cup Y$, or equivalently, $x_3x_5^- = \{x_1, x_4\} \cup Z$. This fact has two immediate consequences. The first one is that $x_1 = x_0^2$. This fact and Proposition 4.11 imply that there are at least three 7-edges of type xx involving x_1 but not x_0. The second consequence is that x_2 is in the triangle X' (see Figure 13) formed by x_1y_0, x_3x_5 and x_0x_5, and hence x_2x_5 must be a 7-edge too. The existence of these four 7-edges together with those in Observation 4.8(2) imply $e_7^{xx}(P) \geq 6$, contradicting Proposition 4.9.

Now suppose that x_4x_5 splits the z's. Again, since P is placed as in Figure 6, then $x_0 \in x_3x_5^-$ and $x_1 \in x_3x_5^+$. By similar arguments as above, we can deduce that $x_1 = x_0^4$ and that x_2x_5 is a 7-edge. As before, $x_1 = x_0^4$ and Proposition 4.11 imply that there are at least three 7-edges of type xx involving x_1 but not x_0. The existence of these four 7-edges together with those in Observation 4.8(2) imply $e_7^{xx}(P) \geq 6$, contradicting Proposition 4.9. □

Proposition 4.17. *There is a $u \in \{x, y, z\}$ such that u_3u_5 separates u_4 from the other u's.*

Proof. From Proposition 4.16 we know that u_3u_5 leaves u_0 and u_1 on the same side for each $u \in \{x, y, z\}$. Seeking a contradiction, we suppose that u_3u_5 separates $\{u_0, u_1\}$ from $\{u_2, u_4\}$ for each $u \in \{x, y, z\}$.

By rotating and/or reflecting P if necessary, and exchanging appropriately the labels x, y and z, we can assume that X, Y and Z are placed as in Figure 11(a), and that x_4x_5 splits the y's. An immediate consequence of these assumptions and our hypothesis is that (i) x_3x_5 leaves to z_0 and x_2 on its left side.

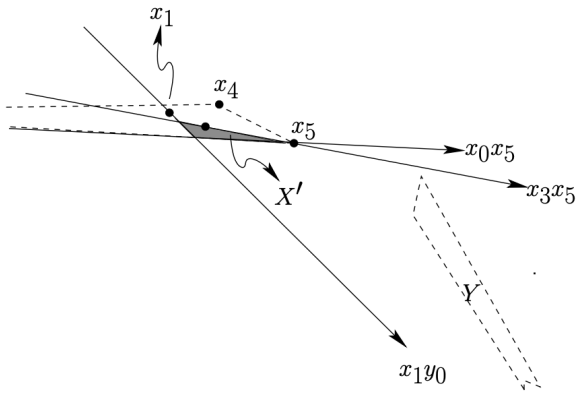


Figure 13: Here $x_1 \in x_3x_5^-$.

Now suppose that $y_5 \in y_0y_4^+$. Then y_0y_5 separates y_4 from the z's, and from Proposition 4.13 we know that y_4y_5 splits the z's. In particular, the triangle formed by y_0, y_4 and y_5 must be as in Figure 12(a) and $y_0 \in y_3y_5^+$. By supposition, y_3y_5 separates y_0 from y_2, and so y_3y_5 leaves to x_0 and y_2 on its left side. This last and Proposition 4.15 imply that y_4y_5 splits the x's too, which is impossible. Thus we conclude that $y_5 \in y_0y_4^-$. This and Proposition 4.13 imply that y_4y_5 splits the x's. This fact and our supposition imply that (ii) y_3y_5 leaves to z_0 and y_2 on its right side.

If z_4z_5 splits the x's, then (i) and Proposition 4.15 imply that x_4x_5 splits the z's, which contradicts that x_4x_5 splits the y's. Similarly, if z_4z_5 splits the y's, then (ii) and Proposition 4.15 imply that y_4y_5 splits the z's, again contradicting that y_4y_5 splits the x's. □

Proposition 4.18. *Let u be an element in $\{x, y, z\}$ that satisfies the property in* Proposition 4.17*, and suppose that u_4u_5 splits the v's, where $v \in \{x, y, z\} \setminus \{u\}$. Then the following hold:*

(B1) *u_3u_5 separates v_5 from the other v's;*

(B2) *v_4v_5 splits the w's, where $\{w\} = \{x, y, z\} \setminus \{u, v\}$;*

(B3) *v_1v_4 and v_2v_4 are both 7-edges; and*

(B4) *v_3v_5 separates v_4 from the other v's.*

Proof. Without loss of generality, we can assume that $u = x, v = y$, and X, Y and Z are placed according to Figure 11. Indeed, we can get such requirements by rotating and/or reflecting P, and by exchanging appropriately the labels x, y and z.

(B1): From our assumptions and the hypothesis we know that x_4 is the only x in $x_3x_5^-$. Since x_3x_5 is an 8-edge, then exactly one element y^* of Y is in $x_3x_5^-$. From (A6), we know that such a y^* is one of y_4 or y_5. If $y^* = y_4$, then, by the way $y_0, \ldots, y_5$ were labelled, we have that y_5 must be contained in the triangle S of Figure 14. Then y_4y_5 leaves x_3, x_4, x_5 and all the z's on its right side. This implies that y_4y_5 cannot be an 8-edge, contradicting (A4). This contradiction implies that (B1) holds.

(B2): From (B1), we know that $y^* = y_5$ is the only element of Y in $x_3x_5^-$. If $y_5 \in y_0y_4^-$, then y_4 must be contained in the region R of Figure 14. This implies that each element in $(X \cup Y) \setminus \{x_4, y_4, y_5\}$ lies in $y_4y_5^-$, contradicting (A4) that $y_4y^* = y_4y_5$ is an 8-edge. Thus we have that $y_5 \in y_0y_4^+$. This fact and Proposition 4.13 imply that y_4y_5 splits the z's, as required.

In view of (B2) and our previous assumptions, for the rest of the proof, we may assume that the two triangles defined by $\{x_0, x_4, x_5\}$ and $\{y_0, y_4, y_5\}$ are as shown in Figure 12(a).

(B3): Let ℓ be the line through y_4 which is parallel to x_4x_5 and let M be the interior of the triangle formed by y_0y_5, y_0y_4 and x_4x_5. See Figure 12(a). Since y_4 and y_5 are the only y's in $x_4x_5^-$, then $M \cap Y = \{y_1, y_2, y_3\}$. If we rotate ℓ in clockwise order around y_4 until it reaches y_4y_0, then by Observation 4.7 we have that exactly one of $\{y_1y_4, y_2y_4, y_3y_4\}$ is 8-edge and the other two are 7-edges. The desired assertion follows from (A4).

(B4): Seeking a contradiction, suppose that y_3y_5 does not separate y_4 from the other y's. Then Proposition 4.16 implies that y_3y_5 separates $\{y_0, y_1\}$ from $\{y_2, y_4\}$. On the other hand, since y_3y_4 is an 8-edge and x_4x_5 separates y_3 from y_4, then $y_3y_4^- = X \cup \{y_0, y_2\}$. Thus y_1 must be contained in the triangle R formed by z_0y_3, y_3y_4, y_0y_5. See Figure 12(b). This implies that $y_0^4 = y_1$. Then Proposition 4.11, Observation 4.8(2) and (B3) imply, $e_7^{yy}(P) \geq 6$, a contradiction. □

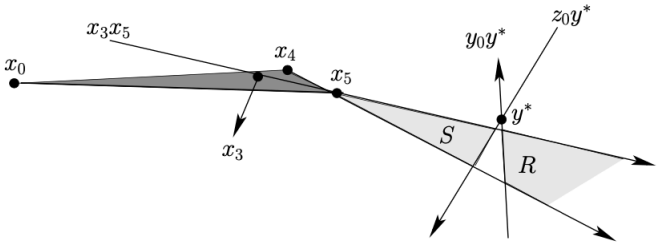


Figure 14: Here x_3x_5 separates y^* from the other y's.

Remark 4.19. From now on, without loss of generality, we assume that the $u \in \{x, y, z\}$ satisfying Proposition 4.17 is x, and that $x_5 \in x_0x_4^+$. Indeed, it is not hard to see that we can get such requirements by rotating and/or reflecting P along x_0x_4, and by appropriately exchanging the labels x, y and z. In particular, we assume that X, Y, Z, x_0, x_4 and x_5 are placed as in Figure 11.

Note that (B4) appears as hypothesis in Propositions 4.17 and 4.18. The following corollary is an immediate consequence of this fact.

Corollary 4.20. *Let $\sigma(x) = y, \sigma(y) = z$ and $\sigma(z) = x$. The following hold for each $u \in \{x, y, z\}$:*

(C1) *u_3u_5 separates $\sigma(u)_5$ from the other $\sigma(u)$'s;*

(C2) *$\sigma(u)_4\sigma(u)_5$ splits the $\sigma(\sigma(u))$'s;*

(C3) $\sigma(u)_1\sigma(u)_4$ *and* $\sigma(u)_2\sigma(u)_4$ *are both* 7*-edges;*

(C4) $\sigma(u)_3\sigma(u)_5$ *separates* $\sigma(u)_4$ *from the other* $\sigma(u)$*'s; and*

(C5) $u_5 \in u_0u_4^+$.

Proof. In view of Remark 4.19, we may assume that x_4x_5 splits the y's, x_3x_5 separates x_4 from the other x's, and X, Y, Z, x_0, x_4 and x_5 are placed as in Figure 11.

First, we show that (C1) – (C4) hold. Proposition 4.18 states exactly (C1) – (C4) for $u = x$ and $v = \sigma(x) = y$. In particular, (C2) and (C4) tell us that y_4y_5 splits the z's and that y_3y_5 separates y_4 from the other y's, respectively. By applying Proposition 4.18 to the last two conclusions on y's we have that (C1) – (C4) also hold for $u = y$ and $v = \sigma(y) = z$. Similarly, we can conclude that (C1) – (C4) also hold for $u = z$ and $v = \sigma(z) = x$.

Now, we show (C5). For $u = x$ the assertion holds by Remark 4.19. We first analyze the case $u = y$. From (A6) and Remark 4.19, we know that $\{x_0, \ldots, x_5\}$ lies on the left side of both y_0y_4 and y_0y_5. Seeking a contradiction, suppose that $y_5 \in y_0y_4^-$. Then, from (A6) and the last two facts, it is easy to verify that $x_0 \in y_3y_5^-$. Similarly, from $y_5 \in y_0y_4^-$ and (C4), we can deduce that $y_2 \in y_3y_5^-$. Thus $x_0, y_2 \in y_3y_5^-$, and so Proposition 4.15 implies that y_4y_5 splits the x's, contradicting (C2). An analogous argument shows that (C5) also holds for $u = z$. □

From Remark 4.19 and Corollary 4.20, we have that the points of P with indices $0, 3, 4$ and 5 are placed as in Figure 15.

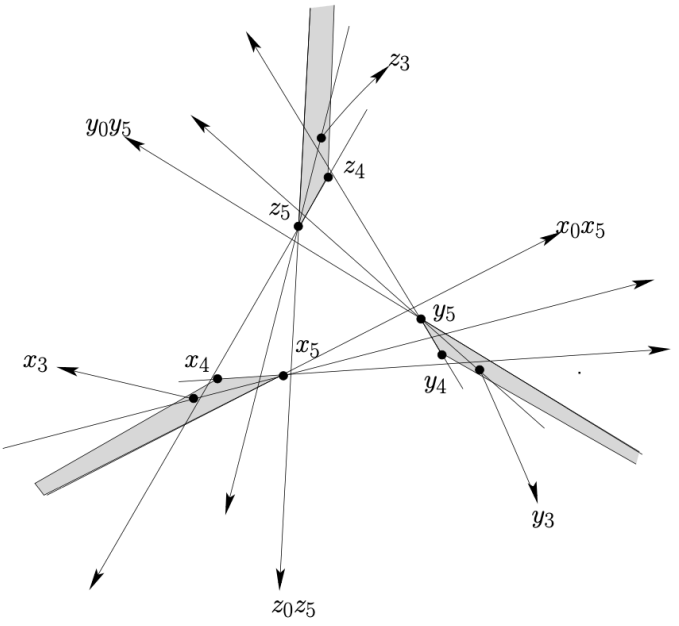


Figure 15: The relative position of the points of P with indices $0, 3, 4$ and 5.

4.4 Determination of pq^+ when pq is a monochromatic edge.

Lemma 3.1 for the case in which pq is a monochromatic edge will follow from Propositions 4.21 and 4.22 below. Regarding the statements of these propositions, we recall from Remark 4.19 and Corollary 4.20 that x_4x_5 splits the ys, y_4y_5 splits the zs, and z_4z_5 splits the xs.

Proposition 4.21. *Let $u \in \{x, y, z\}$, and let v be the element in $\{x, y, z\} \setminus \{u\}$ such that u_4u_5 splits the vs. Then the following hold:*

(D1) $u_0u_5^+ = \{v_0, \dots, v_5\}$;

(D2) $u_0u_4^+ = \{u_1, u_2, u_3, u_5\} \cup \{v_0, \dots, v_5\}$;

(D3) $u_4u_5^+ = \{u_0, u_1, u_2, u_3\} \cup \{v_0, v_1, v_2, v_3\}$; *and*

(D4) $u_3u_5^+ = \{u_0, u_1, u_2\} \cup \{v_0, v_1, v_2, v_3, v_4\}$.

Proof. (D1): From (A7), we know that u_0u_5 separates the v's from the w's. Moreover, because u_0u_5 is an edge of the convex hull of U, then u_0u_5 leaves the other u's on the same side. This and (C5) imply that $\{u_1, u_2, u_3, u_4\} \subset u_0u_5^-$. Again, from (C5) and Proposition 4.13 we have that $\{v_0, v_1, v_2, v_3\} \subset u_4u_5^+$, and hence $\{v_0, v_1, v_2, v_3\} \subset u_0u_5^+$. This and the fact that u_0u_5 separates the v's from the w's imply that $\{v_0, \dots, v_5\} \subseteq u_0u_5^+$. We finally note that Observation 4.8(1) implies that $u_0u_5^+ = \{v_0, \dots, v_5\}$, as required.

(D2): From (C5), (D1), and the way in that the points of P were labelled we have that $\{v_0, \dots, v_5\} = u_0u_5^+ \subset u_0u_4^+$. On the other hand, since u_0u_4 is an edge of the convex hull of U, then u_0u_4 leaves the other u's on the same side. This and (C5) imply that $\{u_1, u_2, u_3, u_5\} \subset u_0u_4^+$. Thus $\{u_1, u_2, u_3, u_5\} \cup \{v_0, \dots, v_5\} \subset u_0u_4^+$. Again, Observation 4.8(1) implies that $u_0u_4^+ = \{u_1, u_2, u_3, u_5\} \cup \{v_0, \dots, v_5\}$, as required.

(D3): It follows immediately from (C5) and Proposition 4.13.

(D4): Clearly, $\{v_0, \dots, v_5\} \cap u_4u_5^+ \subset \{v_0, \dots, v_5\} \cap u_3u_5^+$. This fact, together with (C1) and (D3), implies that $\{v_0, v_1, v_2, v_3, v_4\} \subset u_3u_5^+$. On the other hand, from (C4) is easy to verify that $\{u_0, \dots, u_5\} \cap u_3u_5^+ = \{u_0, u_1, u_2\}$. Then $\{u_0, u_1, u_2\} \cup \{v_0, v_1, v_2, v_3, v_4\} \subset u_3u_5^+$. We finally note that (A4) implies that $u_3u_5^+ = \{u_0, u_1, u_2\} \cup \{v_0, v_1, v_2, v_3, v_4\}$, as required. □

Proposition 4.22. *Let $u \in \{x, y, z\}$, and let v be the element in $\{x, y, z\} \setminus \{u\}$ such that u_4u_5 splits the vs. Then the following hold:*

(E1) u_0u_1 *is an* 8*-edge;*

(E2) u_0u_2 *and* u_0u_3 *are* 7*-edges;*

(E3) u_2u_3 *and* u_2u_5 *are* 8*-edges;*

(E4) $u_2u_4^+ = \{u_5\} \cup \{v_0, \dots, v_5\}$;

(E5) $u_1u_4^+ = \{u_2, u_3, u_5\} \cup \{v_0, \dots, v_5\}$ *and* $u_3u_4^+ = \{u_2, u_5\} \cup \{v_0, \dots, v_5\}$;

(E6) $u_0u_2^+ = \{u_5\} \cup \{v_0, \dots, v_5\}$;

(E7) $u_0u_1^+ = \{u_2, u_5\} \cup \{v_0, \dots, v_5\}$ *and* $u_0u_3^+ = \{u_1, u_2, u_5\} \cup \{v_0, \dots, v_5\}$;

(E8) $u_1u_5^+ = \{u_0\} \cup \{v_0, \ldots, v_5\}$;

(E9) u_1u_2 *and* u_1u_3 *are* 8*-edges;*

(E10) $u_1u_3^+ = \{u_2, u_5\} \cup \{v_0, \ldots, v_5\}$;

(E11) $u_1u_2^+ = \{u_0, u_5\} \cup \{v_0, \ldots, v_5\}$;

(E12) $u_2u_5^+ = \{u_0, u_1\} \cup \{v_0, \ldots, v_5\}$; *and*

(E13) $u_2u_3^+ = \{u_4, u_5\} \cup \{v_0, \ldots, v_5\}$.

Proof. (E1): From Proposition 4.9, Corollary 4.10, and (A5), we know that x_0x_1 is a 7- or an 8-edge. If x_0x_1 is a 7-edge, then $x_1 \in \{x_0^2, x_0^4\}$ and by Proposition 4.11, there are at least three 7-edges of type xx involving x_1 but not x_0. This, Observation 4.8(2), and (C3) imply that $e_7^{xx}(P) \geq 6$, a contradiction. Thus x_0x_1 must be an 8-edge.

(E2): From Observation 4.8(2), we know that there are exactly two 7-edges of the type x_0x. Since (E1) and (A6) imply that none of x_0x_1, x_0x_4, x_0x_5 is a 7-edge, then both x_0x_2 and x_0x_3 are 7-edges, as desired.

(E3): By Corollary 4.10 and (A5), each of x_2x_3 and x_2x_5 is a 7- or an 8-edge. From (C3) and (E2), we know that each of $x_1x_4, x_2x_4, x_0x_2, x_0x_3$ is a 7-edge. Since (A2) guarantees the existence of an additional 7-edge involving x_1 and $e_7^{xx}(P) = 5$, then x_2x_3 and x_2x_5 are 8-edges, as required.

Observation 4.23. Since z_4z_5 separates $\{x_4, x_5\}$ from the other x's (see Figure 15), then x_ix_4 leaves Z on its left for any $i \in \{0, 1, 2, 3\}$.

(E4): From (C3), we know that x_1x_4 and x_2x_4 are 7-edges. This and Observation 4.23 imply that x_2x_4 leaves exactly 1 or exactly 3 points of X on its left.

Suppose first that $x_1 \in x_2x_4^+$. Since $x_0 \in x_2x_4^-$, then $x_2x_4^+ = \{x_1, x_3, x_5\} \cup Y$. Again, Observation 4.23 implies that when we rotate x_2x_4 counterclockwise around x_4, the first two points that such line finds (with the tail) are x_1 and x_3. Since x_1x_4 is a 7-edge and x_3x_4 is an 8-edge, then the first point that such a rotation finds must be x_3, and hence $x_1 \in x_3x_4^+$. This and the way in which the x's were labelled imply that $x_0^4 = x_1$. But then x_0x_1 is a 7-edge, contradicting (E1). Then $x_0, x_1 \in x_2x_4^-$ and hence x_2x_4 leaves exactly three points of X on its left, namely x_0, x_1 and x_3. The desired equality follows from the last conclusion, Observation 4.23, and (C3).

(E5): From (A4), we know that x_3x_4 is an 8-edge, and from (C3) that x_1x_4 is a 7-edge. Since $x_1, x_3 \in x_2x_4^-$, by (E4), then when we rotate x_2x_4 clockwise around x_4, the first two points that such line finds (with the tail) are precisely x_1 and x_3. Since x_1x_4 is a 7-edge and x_3x_4 is an 8-edge, then such a rotation finds first x_3 and then x_1. The desired conclusions are immediate from this fact and (E4).

(E6): From (E4) and the way the x's were labelled, we know that when we rotate x_2x_4 clockwise around x_2, the first point that such line finds (with the tail) is one of x_0 or x_1. Since x_0x_2 is a 7-edge, by (E2), then such a point must be x_0 and the desired result follows from (E4).

(E7): From (E6), we know that the first two points that we find when we rotate x_0x_2 counterclockwise around x_0 are x_1 and x_3. Since x_0x_1 is an 8-edge, by (E1), then we

have that such a rotation finds x_1 and then x_3. These together with (E6) imply the desired results.

(E8): (D4) implies that $x_3 \in x_1x_5^-$. If $x_2 \in x_1x_5^+$, then $\{x_1, x_3, x_4\} \cup Z \subset x_2x_5^-$. This would imply that x_2x_5 is not an 8-edge, contradicting (E3). Then we can assume that $x_2 \in x_1x_5^-$. Thus, x_0 is the only x on the right side of x_1x_5 and hence x_1x_5 is a (≤ 7)-edge. From Proposition 4.9 and Corollary 4.10, we have that x_1x_5 must be a 7-edge. This implies that $Y \subset x_1x_5^+$, and hence (E8) holds.

(E9): (E4), (E5), (E6), (E7), and (E8) imply, respectively, that $x_2x_4, x_1x_4, x_0x_2, x_0x_3$ and x_1x_5 are 7-edges. Then Proposition 4.9 implies that these five are all the monochromatic edges of type xx. This and Corollary 4.10 imply that x_1x_2 and x_1x_3 must be 8-edges.

(E10): The first assertion of (E7) implies that $x_3, x_4 \in x_0x_1^-$ and $x_2, x_5 \in x_0x_1^+$. From the first assertion of (E5) we know that $x_2, x_3 \in x_1x_5^+$. Then when we rotate x_0x_1 counterclockwise around x_1, the first point that such line finds must be x_3, and so the desired result follows immediately from this and the first assertion of (E5).

(E11): From the first assertion of (E7), we have that $x_3, x_4 \in x_0x_1^-$ and $x_2, x_5 \in x_0x_1^+$. From (E8), we know that $x_2, x_3 \in x_1x_4^-$. Then when we rotate x_0x_1 clockwise around x_1, the first point that we find is x_2, and so the desired result follows from the first assertion of (E7).

(E12): (E8) implies $\{x_2, x_3, x_4\} \cup Z = x_1x_5^-$. From (D4) and the second assertion of (E3), we know that when we rotate x_1x_5 clockwise around x_5, the first point that we find must be x_2, and so the desired result follows from (E8).

(E13): (E4) implies that $Z \cup \{x_0, x_1, x_3\} = x_2x_4^-$. From (E10), we know that $x_2 \in x_1x_3^+$. This and the first assertion of (E3) imply that when we rotate x_2x_4 counterclockwise around x_2, the first point that we find must be x_3, and so the desired result follows from (E4). □

4.5 Determination of pq^+ when pq is a bichromatic (>5)-edge.

We are finally ready to prove Lemma 3.1 for the remaining case, namely when pq is a bichromatic (> 5)-edge. This is achieved in the next statement. We recall from Remark 4.19 and Corollary 4.20 that x_4x_5 splits the ys, y_4y_5 splits the zs, and z_4z_5 splits the xs.

Proposition 4.24. *Let $u \in \{x, y, z\}$, and let v be the element in $\{x, y, z\} \setminus \{u\}$ such that u_4u_5 splits the vs. Then the following hold:*

(F1) $u_5v_4^+ = \{u_0, u_1, u_2, u_3\} \cup \{v_0, v_1, v_2, v_3\}$;

(F2) $u_5v_5^+ = \{u_0, u_1, u_2\} \cup \{v_0, v_1, v_2, v_3, v_4\}$;

(F3) $u_5v_3^+ = \{u_0, u_1, u_2, u_3, u_4\} \cup \{v_0, v_1, v_2\}$;

(F4) $u_5v_2^+ = \{u_0, u_1, u_2, u_3, u_4\} \cup \{v_0, v_1\}$;

(F5) $u_5v_1^+ = \{u_0, u_1, u_2, u_3, u_4\} \cup \{v_0\}$;

(F6) $u_4v_4^+ = \{u_0, u_1, u_2, u_3, u_5\} \cup \{v_0, v_1, v_2, v_3\}$;

(F7) $u_4v_5^+ = \{u_0, u_1, u_2, u_3, u_5\} \cup \{v_0, v_1, v_2, v_3, v_4\}$;

(F8) $u_4v_3^+ = \{u_0, u_1, u_2, u_3\} \cup \{v_0, v_1, v_2\}$;

(F9) $u_4v_2^+ = \{u_0, u_1, u_2, u_3\} \cup \{v_0, v_1\}$;

(F10) $u_3v_5^+ = \{u_0, u_1, u_2, u_5\} \cup \{v_0, v_1, v_2, v_3, v_4\}$;

(F11) $u_3v_4^+ = \{u_0, u_1, u_2\} \cup \{v_0, v_1, v_2, v_3\}$;

(F12) $u_3v_3^+ = \{u_0, u_1, u_2\} \cup \{v_0, v_1, v_2\}$;

(F13) $u_2v_5^+ = \{u_0, u_1\} \cup \{v_0, v_1, v_2, v_3, v_4\}$;

(F14) $u_2v_4^+ = \{u_0, u_1\} \cup \{v_0, v_1, v_2, v_3\}$;

(F15) $u_1v_5^+ = \{u_0\} \cup \{v_0, v_1, v_2, v_3, v_4\}$.

Proof. In view of Remark 4.19 and Corollary 4.20, we may assume that the points of P are placed as in Figure 15. Moreover, by symmetry, we only need to verify the case $u = x$ and $v = y$. For brevity, for $m \in \{0, \dots, 5\}$, we let $X_m := \{x_i | i \le m\}$ and $Y_m := \{y_i | i \le m\}$.

(F1): From (D3), we know that $x_4x_5^+ = X_3 \cup Y_3$. We claim that the first point $p \in P$ that x_4x_5 finds when it is rotated counterclockwise around x_5 is y_4. From (D4), we know that $x_3x_5^+ = X_2 \cup Y_4$. Then $p = y_4$, and so $x_5y_4^+ = X_3 \cup Y_3$, as required.

(F2): We know that $x_3x_5^+ = X_2 \cup Y_4$ by (D4). We claim that the first point $p \in P$ that x_3x_5 finds when it is rotated counterclockwise around x_5 is y_5. Indeed, from (D1), (E8), and (E12), we know that $y_5 \in x_jx_5^+$ for $j = 0, 1, 2$, respectively. These imply that $p \notin X_2$, and so $p = y_5$. Then $x_5y_5^+ = X_2 \cup Y_4$, as required.

(F3): We know that $x_4x_5^+ = X_3 \cup Y_3$ by (D3). We claim that the first point $p \in P$ that x_4x_5 finds when it is rotated clockwise around x_5 is y_3. Indeed, by applying (E7), (E10), and (E13) to $j = 0, 1$ and $j = 2$ (with $u = y$ and $v = z$), respectively, we have that $X \subset y_jy_3^-$, and so $x_5 \in y_jy_3^-$. These imply that $p \notin Y_2$. This and the fact that $x_5y_0^+ = X_4$ imply that $p = y_3$. Then $x_5y_3^+ = X_4 \cup Y_2$, as required.

(F4): We know that $x_5y_3^+ = X_4 \cup Y_2$ by (F3). We claim that the first point $p \in P$ that x_5y_3 finds when it is rotated clockwise around x_5 is y_2. Indeed, by applying (E6) and (E11) to $j = 0$ and $j = 1$ (with $u = y$ and $v = z$), respectively, we have that $X \subset y_jy_2^-$, and so $x_5 \in y_jy_2^-$. These imply that $p \notin Y_1$. This and the fact that $x_5y_0^+ = X_4$ imply that $p = y_2$. Then $x_5y_2^+ = X_4 \cup Y_1$, as required.

(F5): We know that $x_5y_2^+ = X_4 \cup Y_1$ by (F4). We claim that the first point $p \in P$ that x_5y_2 finds when it is rotated clockwise around x_5 is y_1. Indeed, by taking $u = y$ in (E7), we have that $x_5 \in y_0y_1^-$, and so $p \neq y_0$. This and the fact that $x_5y_0^+ = X_4$ imply that $p = y_1$. Then $x_5y_1^+ = X_4 \cup Y_0$, as required.

(F6): We know that $x_4x_5^+ = X_3 \cup Y_3$ by (D3). We claim that the first point $p \in P$ that x_4x_5 finds when it is rotated counterclockwise around x_4 is y_4. Indeed, by taking $u = y$ and $v = z$ in D3) we get $x_4 \in y_4y_5^-$, and so $p \neq y_5$. This and the fact that $x_0x_4^+ = \{x_1, x_2, x_3, x_5\} \cup Y$ imply that $p = y_4$. Then $x_4y_4^+ = X_3 \cup Y_3 \cup \{x_5\}$, as required.

(F7): We know that $x_4y_4^+ = X_3 \cup Y_3 \cup \{x_5\}$ by (F6). We claim that the first point $p \in P$ that x_4y_4 finds when it is rotated counterclockwise around x_4 is y_5. Indeed, from (D2), we know that $x_0x_4^+ = \{x_1, x_2, x_3, x_5\} \cup Y$. These imply that $p \notin X$, and so $p = y_5$. Then $x_4y_5^+ = X_3 \cup Y_4 \cup \{x_5\}$, as required.

(F8): We know that $x_4x_5^+ = X_3 \cup Y_3$ by (D3). We claim that the first point $p \in P$ that x_4x_5 finds when it is rotated clockwise around x_4 is y_3. Indeed, by applying E7), E10), and E13) to $j = 0, 1$ and $j = 2$ (with $u = y$ and $v = z$), respectively, we have that $X \subset y_jy_3^-$, and so $x_4 \in y_jy_3^-$. These imply that $p \notin Y_2$. From Proposition 4.3(2), we know that $X_3 \subset x_4y_1^+$, and so $p \notin X_3$. All these facts imply that $p = y_3$, and so $x_4y_3^+ = X_3 \cup Y_2$, as required.

(F9): We know that $x_4y_3^+ = X_3 \cup Y_2$ by (F8). We claim that the first point $p \in P$ that x_4y_3 finds when it is rotated clockwise around x_4 is y_2. Indeed, by applying (E6) and (E11) to $j = 0$ and $j = 1$ (with $u = y$ and $v = z$), respectively, we have that $X \subset y_jy_2^-$, and so $x_4 \in y_jy_2^-$. These imply that $p \notin Y_1$. From this and (D3) it follows that $p = y_2$, and so $x_4y_2^+ = X_3 \cup Y_1$, as required.

(F10): We know that $x_3x_5^+ = X_2 \cup Y_4$ by (D4). We claim that the first point $p \in P$ that x_3x_5 finds when it is rotated counterclockwise around x_3 is y_5. Indeed, by applying (E7), (E10), and (E13) to $j = 0, 1$ and $j = 2$ (with $u = x$ and $v = y$), respectively, we have that $Y \subset x_jx_3^+$, and so $y_5 \in x_jx_3^+$. These imply that $p \notin X_2$. From this and E5) it follows that $p = y_5$, and so $x_3y_5^+ = X_2 \cup Y_4 \cup \{x_5\}$, as required.

(F11): We know that $x_3x_5^+ = X_2 \cup Y_4$ by D4). We claim that the first point $p \in P$ that x_3x_5 finds when it is rotated clockwise around x_3 is y_4. Indeed, by applying (D2), (E5), (E4), and (E5) to $j = 0, 1, 2$ and $j = 3$ (with $u = y$ and $v = z$), respectively, we have that $X \subset y_jy_4^-$, and so $x_3 \in y_jy_4^-$. These imply that $p \notin Y_3$. From Proposition 4.3(2), we know that $x_4 \in x_3y_2^-$, and so $p \neq x_4$. All these facts imply that $p = y_4$, and so $x_3y_4^+ = X_2 \cup Y_3$, as required.

(F12): We know that $x_3y_4^+ = X_2 \cup Y_3$ by (F11). We claim that the first point $p \in P$ that x_3y_4 finds when it is rotated clockwise around x_3 is y_3. Indeed, by applying (E7), (E10), and (E13) to $j = 0, 1$ and $j = 2$ (with $u = y$ and $v = z$), respectively, we have that $X \subset y_jy_3^-$, and so $x_3 \in y_jy_3^-$. These imply that $p \notin Y_2$. By taking $u = x$ in (E5) and (D4), we have that $y_4 \in x_3x_4^+$ and $y_4 \in x_3x_5^+$, respectively. These imply that $p \notin \{x_4, x_5\}$. All these facts imply that $p = y_3$, and so $x_3y_3^+ = X_2 \cup Y_2$, as required.

(F13): From Proposition 4.3(2), we know that $x_2y_3^+ = X_1 \cup Y_2$. We claim that the first point $p \in P$ that x_2y_3 finds when it is rotated counterclockwise around x_2 is y_4. Indeed, by applying (E6) and (E11) to $j = 0$ and $j = 1$ (with $u = x$ and $v = y$), respectively, we have that $Y \subset x_jx_2^+$, and so $p \notin \{x_0, x_1\}$. Finally, by applying (E4), (E12), and (E13) to $j = 4, 5$ and $j = 3$ (with $u = x$ and $v = y$), we have that $p \neq x_4, p \neq x_5$ and $p \neq x_3$, respectively. All these facts imply that $p = y_4$, and so $x_2y_4^+ = X_1 \cup Y_3$, as required.

(F14): We know that $x_2y_4^+ = X_1 \cup Y_3$ by (F13). We claim that the first point $p \in P$ that x_2y_4 finds when it is rotated counterclockwise around x_2 is y_5. As in (F13) we can deduce from (E6) and (E11) that $p \notin \{x_0, x_1\}$. Again, as in (F13) we can deduce from (E4), (E12), and (E13) that $p \neq x_4, p \neq x_5$ and $p \neq x_3$, respectively. All these facts imply that $p = y_5$, and so $x_2y_5^+ = X_1 \cup Y_4$, as required.

(F15): We know that $x_2y_5^+ = X_1 \cup Y_4$ by F14). We claim that the first point $p \in P$ that x_2y_5 finds when it is rotated counterclockwise around y_5 is x_1. Indeed, from Proposition 4.3(2), we know that $y_5z_0^+ = Y_4$. From the last two equations we have that $p \in X_1 = \{x_0, x_1\}$. Again, from Proposition 4.3(2), we know that $x_0y_5^+ = Y_4$, and so $p = x_1$. Then $x_1y_5^+ = X_0 \cup Y_4$, as required. □

4.6 Conclusion of the proof of Lemma 3.1

In Tables 1 and 2 we give a summary of the results in Propositions 4.3(2)(b), 4.21, 4.22, and 4.24. These tables assume that $u \in \{x, y, z\}$ and $v = \sigma(u)$, where σ is the automorphism of $\{x, y, z\}$ defined in Corollary 4.20, namely $x \overset{\sigma}{\mapsto} y, y \overset{\sigma}{\mapsto} z$, and $z \overset{\sigma}{\mapsto} x$.

In particular, for each $u \in \{x, y, z\}$ and $m, n \in \{0, \ldots, 5\}$ with $m < n$, the set $u_m u_n^+$ is given in Table 1. This also determines the set $u_n u_m^+$, since $u_n u_m^+ = u_m u_n^-$, and $u_m u_n^-$ is evidently determined from $u_m u_n^+$. Thus the information in Table 1 suffices to determine pq^+ whenever pq is a monochromatic edge of P.

Now for each $u \in \{x, y, z\}$ and each $m, n \in \{0, \ldots, 5\}$, the set $u_m v_n^+$ is given in Table 2. This also determines the set $v_n u_m^+$, since $v_n u_m^+ = u_m v_n^-$, and $u_m v_n^-$ is evidently determined from $u_m v_n^+$. Thus the information in Table 2 suffices to determine pq^+ whenever pq is a bichromatic edge of P. □

$u_i u_j^+$ for each $u_i u_j \in E_k^{\mathrm{mon}}(P)$	Classification of $u_i u_j$	Equality stated in
$u_0 u_5^+ = \{v_0, \ldots, v_5\}$	6-edge	(D1)
$u_0 u_4^+ = \{u_1, u_2, u_3, u_5\} \cup \{v_0, \ldots, v_5\}$	6-edge	(D2)
$u_0 u_3^+ = \{u_1, u_2, u_5\} \cup \{v_0, \ldots, v_5\}$	7-edge	(E7)
$u_0 u_2^+ = \{u_5\} \cup \{v_0, \ldots, v_5\}$	7-edge	(E6)
$u_0 u_1^+ = \{u_2, u_5\} \cup \{v_0, \ldots, v_5\}$	8-edge	(E7)
$u_1 u_5^+ = \{u_0\} \cup \{v_0, \ldots, v_5\}$	7-edge	(E8)
$u_1 u_4^+ = \{u_2, u_3, u_5\} \cup \{v_0, \ldots, v_5\}$	7-edge	(E5)
$u_1 u_3^+ = \{u_2, u_5\} \cup \{v_0, \ldots, v_5\}$	8-edge	(E10)
$u_1 u_2^+ = \{u_0, u_5\} \cup \{v_0, \ldots, v_5\}$	8-edge	(E11)
$u_2 u_5^+ = \{u_0, u_1\} \cup \{v_0, \ldots, v_5\}$	8-edge	(E12)
$u_2 u_4^+ = \{u_5\} \cup \{v_0, \ldots, v_5\}$	7-edge	(E4)
$u_2 u_3^+ = \{u_4, u_5\} \cup \{v_0, \ldots, v_5\}$	8-edge	(E13)
$u_3 u_5^+ = \{u_0, u_1, u_2\} \cup \{v_0, \ldots, v_4\}$	8-edge	(D4)
$u_3 u_4^+ = \{u_2, u_5\} \cup \{v_0, \ldots, v_5\}$	8-edge	(E5)
$u_4 u_5^+ = \{u_0, \ldots, u_3\} \cup \{v_0, \ldots, v_3\}$	8-edge	(D3)

Table 1: All the monochromatic edges of P.

5 Concluding remarks

In this work we finally have given the full proof of Theorem 1.2, which was announced at the EuroComb'11 conference [1].

As we mentioned in the Introduction, the exact rectilinear crossing number of K_n is known only for $n \leq 27$ and $n = 30$ [3, 7, 8, 9, 10]. In [2] and [6] we can find non-isomorphic crossing-minimal rectilinear drawings of K_n for both $n = 24$ and $n = 30$. On the other hand, from [6] and the main result of this work, now we know that there is a unique (up to order type isomorphism) crossing-minimal rectilinear drawing of K_n, for $n = 6, 12, 18$. Thus, a plausible conjecture is that K_{6m} has several crossing-minimal rectilinear drawings for each integer $m \geq 4$.

We close this paper with a discussion on a question raised by an anonymous reviewer of an earlier version of this paper: to what degree would it be possible to get a computer-assisted proof of Theorem 1.2?

uv^+ for each $uv \in E_k^{\mathrm{bi}}(P)$	Classification of uv	Equality stated in
$u_0v_5^+ = \{v_0, \ldots, v_4\}$	5-edge	Proposition 4.3(2)
$u_0v_4^+ = \{v_0, v_1, v_2, v_3\}$	4-edge	Proposition 4.3(2)
$u_0v_3^+ = \{v_0, v_1, v_2\}$	3-edge	Proposition 4.3(2)
$u_0v_2^+ = \{v_0, v_1\}$	2-edge	Proposition 4.3(2)
$u_0v_1^+ = \{v_0\}$	1-edge	Proposition 4.3(2)
$u_0v_0^+ = \emptyset$	0-edge	Proposition 4.3(2)
$u_1v_5^+ = \{u_0\} \cup \{v_0, \ldots, v_4\}$	6-edge	(F15)
$u_1v_4^+ = \{u_0\} \cup \{v_0, v_1, v_2, v_3\}$	5-edge	Proposition 4.3(2)
$u_1v_3^+ = \{u_0\} \cup \{v_0, v_1, v_2\}$	4-edge	Proposition 4.3(2)
$u_1v_2^+ = \{u_0\} \cup \{v_0, v_1\}$	3-edge	Proposition 4.3(2)
$u_1v_1^+ = \{u_0\} \cup \{v_0\}$	2-edge	Proposition 4.3(2)
$u_1v_0^+ = \{u_0\}$	1-edge	Proposition 4.3(2)
$u_2v_5^+ = \{u_0, u_1\} \cup \{v_0, \ldots, v_4\}$	7-edge	(F14)
$u_2v_4^+ = \{u_0, u_1\} \cup \{v_0, v_1, v_2, v_3\}$	6-edge	(F13)
$u_2v_3^+ = \{u_0, u_1\} \cup \{v_0, v_1, v_2\}$	5-edge	Proposition 4.3(2)
$u_2v_2^+ = \{u_0, u_1\} \cup \{v_0, v_1\}$	4-edge	Proposition 4.3(2)
$u_2v_1^+ = \{u_0, u_1\} \cup \{v_0\}$	3-edge	Proposition 4.3(2)
$u_2v_0^+ = \{u_0, u_1\}$	2-edge	Proposition 4.3(2)
$u_3v_5^+ = \{u_0, u_1, u_2, u_5\} \cup \{v_0, \ldots, v_4\}$	7-edge	(F10)
$u_3v_4^+ = \{u_0, u_1, u_2\} \cup \{v_0, v_1, v_2, v_3\}$	7-edge	(F11)
$u_3v_3^+ = \{u_0, u_1, u_2\} \cup \{v_0, v_1, v_2\}$	6-edge	(F12)
$u_3v_2^+ = \{u_0, u_1, u_2\} \cup \{v_0, v_1\}$	5-edge	Proposition 4.3(2)
$u_3v_1^+ = \{u_0, u_1, u_2\} \cup \{v_0\}$	4-edge	Proposition 4.3(2)
$u_3v_0^+ = \{u_0, u_1, u_2\}$	3-edge	Proposition 4.3(2)
$u_4v_5^+ = \{u_0, u_1, u_2, u_3, u_5\} \cup \{v_0, \ldots, v_4\}$	6-edge	(F7)
$u_4v_4^+ = \{u_0, u_1, u_2, u_3, u_5\} \cup \{v_0, \ldots, v_3\}$	7-edge	(F6)
$u_4v_3^+ = \{u_0, u_1, u_2, u_3\} \cup \{v_0, v_1, v_2\}$	7-edge	(F8)
$u_4v_2^+ = \{u_0, u_1, u_2, u_3\} \cup \{v_0, v_1\}$	6-edge	(F9)
$u_4v_1^+ = \{u_0, u_1, u_2, u_3\} \cup \{v_0\}$	5-edge	Proposition 4.3(2)
$u_4v_0^+ = \{u_0, u_1, u_2, u_3\}$	4-edge	Proposition 4.3(2)
$u_5v_5^+ = \{u_0, u_1, u_2\} \cup \{v_0, \ldots, v_4\}$	8-edge	(F2)
$u_5v_4^+ = \{u_0, \ldots, u_3\} \cup \{v_0, \ldots, v_3\}$	8-edge	(F1)
$u_5v_3^+ = \{u_0, \ldots, u_4\} \cup \{v_0, v_1, v_2\}$	8-edge	(F3)
$u_5v_2^+ = \{u_0, \ldots, u_4\} \cup \{v_0, v_1\}$	7-edge	(F4)
$u_5v_1^+ = \{u_0, \ldots, u_4\} \cup \{v_0\}$	6-edge	(F5)
$u_5v_0^+ = \{u_0, u_1, u_2, u_3, u_4\}$	5-edge	Proposition 4.3(2)

Table 2: All the bichromatic edges of P.

At the beginning of this project we asked ourselves the same question, but we are convinced that a traditional proof might be easier to verify. It is worth mentioning that a heavily computer-assisted proof seems to be out of reach, most likely involving several hundred million CPU hours. On the other hand, we believe that a partially computer-assisted proof would be more difficult to follow and perhaps also less reliable. Using computer-assisted proofs needs a very careful preparation and description of what is done, and proofs of the correctness of the results. The code must be explained in full detail, as well as how the program can be executed (including the operating system, compiler versions, etc.). We believe that in this particular case the task of verifying all this information would end up being more taxing on the reader than the current purely theoretical proof.

ORCID iDs

Bernardo M. Ábrego https://orcid.org/0000-0003-4695-5454
Silvia Fernández–Merchant https://orcid.org/0000-0003-2080-106X
Oswin Aichholzer https://orcid.org/0000-0002-2364-0583
Jesús Leaños https://orcid.org/0000-0002-3441-8136
Gelasio Salazar https://orcid.org/0000-0002-8458-3930

References

[1] B. M. Ábrego, O. Aichholzer, S. Fernández-Merchant, J. Leaños and G. Salazar, There is a unique crossing-minimal rectilinear drawing of K_{18}, in: *Extended abstracts of the sixth European conference on combinatorics, graph theory and applications, EuroComb 2011, Budapest, Hungary, August 29 – September 2, 2011*, Elsevier, Amsterdam, pp. 547–552, 2011, doi: 10.1016/j.endm.2011.09.089, https://doi.org/10.1016/j.endm.2011.09.089.

[2] B. M. Ábrego, M. Cetina, S. Fernández-Merchant, J. Leaños and G. Salazar, 3-symmetric and 3-decomposable geometric drawings of K_n, *Discrete Appl. Math.* **158** (2010), 1240–1258, doi: 10.1016/j.dam.2009.09.020, https://doi.org/10.1016/j.dam.2009.09.020.

[3] B. M. Ábrego, M. Cetina, S. Fernández-Merchant, J. L. nos and G. Salazar, On $\leq k$-edges, crossings, and halving lines of geometric drawings of k_n, *Discrete Comput. Geom.* **48** (2012), 192–215, doi:10.1007/s00454-012-9403-y, https://doi.org/10.1007/s00454-012-9403-y.

[4] B. M. Ábrego and S. Fernández-Merchant, A lower bound for the rectilinear crossing number, *Graphs Comb.* **21** (2005), 293–300, doi:10.1007/s00373-005-0612-5, https://doi.org/10.1007/s00373-005-0612-5.

[5] B. M. Ábrego, S. Fernández-Merchant and G. Salazar, The rectilinear crossing number of K_n: closing in (or are we?), in: *Thirty Essays on Geometric Graph Theory*, Springer, Berlin, pp. 5–18, 2013, doi:10.1007/978-1-4614-0110-0_2, https://doi.org/10.1007/978-1-4614-0110-0_2.

[6] O. Aichholzer, http://www.ist.tugraz.at/aichholzer/research/rp/triangulations/crossing/.

[7] O. Aichholzer, J. Garcia, D. Orden and P. Ramos, New lower bounds for the number of $(\leq k)$-edges and the rectilinear crossing number of K_n, *Discrete Comput. Geom.* **38** (2007), 1–14, doi: 10.1007/s00454-007-1325-8, https://doi.org/10.1007/s00454-007-1325-8.

[8] O. Aichholzer, J. García, D. Orden and P. Ramos, New results on lower bounds for the number of $(\leqslant k)$-facets, in: *Proceedings of the 4th European conference on combinatorics, graph*

theory and applications, EuroComb'07, Seville, Spain, September 11–15, 2007, Elsevier, Amsterdam, pp. 189–193, 2007, doi:10.1016/j.endm.2007.07.033, https://doi.org/10.1016/j.endm.2007.07.033.

[9] O. Aichholzer and H. Krasser, Abstract order type extension and new results on the rectilinear crossing number, *Comput. Geom.* **36** (2007), 2–15, doi:10.1016/j.comgeo.2005.07.005, https://doi.org/10.1016/j.comgeo.2005.07.005.

[10] M. Cetina, C. Hernández-Vélez, J. Leaños and C. Villalobos, Point sets that minimize $(\leq k)$-edges, 3-decomposable drawings, and the rectilinear crossing number of K_{30}, *Discrete Math.* **311** (2011), 1646–1657, doi:10.1016/j.disc.2011.03.030, https://doi.org/10.1016/j.disc.2011.03.030.

[11] R. K. Guy, A combinatorial problem, *(Nabla) Bull. Malays. Math. Sci. Soc.* **7** (1960), 68–72.

[12] L. Lovász, K. Vesztergombi, U. Wagner and E. Welzl, Convex quadrilaterals and k-sets, in: *Towards a Theory of Geometric Graphs*, American Mathematical Society (AMS), Providence, RI, pp. 139–148, 2004.

Author Guidelines

Before submission

Papers should be written in English, prepared in LaTeX, and must be submitted as a PDF file. The title page of the submissions must contain:

- *Title*. The title must be concise and informative.
- *Author names and affiliations*. For each author add his/her affiliation which should include the full postal address and the country name. If avilable, specify the e-mail address of each author. Clearly indicate who is the corresponding author of the paper.
- *Abstract*. A concise abstract is required. The abstract should state the problem studied and the principal results proven.
- *Keywords*. Please specify 2 to 6 keywords separated by commas.
- *Mathematics Subject Classification*. Include one or more Math. Subj. Class. (2020) codes – see https://mathscinet.ams.org/mathscinet/msc/msc2020.html.

After acceptance

Articles which are accepted for publication must be prepared in LaTeX using class file amcjoucc.cls and the bst file amcjoucc.bst (if you use BibTeX). If you don't use BibTeX, please make sure that all your references are carefully formatted following the examples provided in the sample file. All files can be found on-line at:

https://amc-journal.eu/index.php/amc/about/submissions/#authorGuidelines

Abstracts: Be concise. As much as possible, please use plain text in your abstract and avoid complicated formulas. Do not include citations in your abstract. All abstracts will be posted on the website in fairly basic HTML, and HTML can't handle complicated formulas. It can barely handle subscripts and greek letters.
Cross-referencing: All numbering of theorems, sections, figures etc. that are referenced later in the paper should be generated using standard LaTeX \label{...} and \ref{...} commands. See the sample file for examples.
Theorems and proofs: The class file has pre-defined environments for theorem-like statements; please use them rather than coding your own. Please use the standard \begin{proof} ... \end{proof} environment for your proofs.
Spacing and page formatting: Please do not modify the page formatting and do not use \medbreak, \bigbreak, \pagebreak etc. commands to force spacing. In general, please let LaTeX do all of the space formatting via the class file. The layout editors will modify the formatting and spacing as needed for publication.
Figures: Any illustrations included in the paper must be provided in PDF format, or via LaTeX packages which produce embedded graphics, such as TikZ, that compile with PdfLaTeX. (Note, however, that PSTricks is problematic.) Make sure that you use uniform lettering and sizing of the text. If you use other methods to generate your graphics, please provide .pdf versions of the images (or negotiate with the layout editor assigned to your article).

Subscription

Yearly subscription: 150 EUR

Any author or editor that subscribes to the printed edition will receive a complimentary copy of *Ars Mathematica Contemporanea*.

Subscription Order Form

Name: .....
E-mail: .....
Postal Address: .....
.....
.....
.....

I would like to subscribe to receive ..... copies of each issue of *Ars Mathematica Contemporanea* in the year 2024.

I want to renew the order for each subsequent year if not cancelled by e-mail:

☐ Yes ☐ No

Signature: .....

Please send the order by mail, by fax or by e-mail.

By mail: Ars Mathematica Contemporanea
UP FAMNIT
Glagoljaška 8
SI-6000 Koper
Slovenia

By fax: +386 5 611 75 71

By e-mail: info@famnit.upr.si

Printed in Slovenia by *IME TISKARNE*