ARS MATHEMATICA CONTEMPORANEA

Also available at http://amc-journal.eu
ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 13 (2017) 275–291

Large circulant graphs of fixed diameter and arbitrary degree

David Bevan
University of Strathclyde, Glasgow, U.K.

Grahame Erskine , Robert Lewis
Open University, Milton Keynes, U.K.

Received 9 November 2015, accepted 24 February 2017, published online 9 March 2017

Abstract

We consider the degree-diameter problem for undirected and directed circulant graphs. To date, attempts to generate families of large circulant graphs of arbitrary degree for a given diameter have concentrated mainly on the diameter 2 case. We present a direct product construction yielding improved bounds for small diameters and introduce a new general technique for "stitching" together circulant graphs which enables us to improve the current best known asymptotic orders for every diameter. As an application, we use our constructions in the directed case to obtain upper bounds on the minimum size of a subset A of a cyclic group of order n such that the k-fold sumset kA is equal to the whole group. We also present a revised table of largest known circulant graphs of small degree and diameter.

Keywords: Degree-diameter problem, Cayley graphs, circulant graphs, sumsets.

Math. Subj. Class.: 05C25, 05C35

1 Introduction

The goal of the *degree-diameter problem* is to identify the largest possible number $n(d, k)$ of vertices in a graph having diameter k and maximum degree d. This paper considers the problem for the restricted category of circulant graphs, which we view as Cayley graphs of cyclic groups. We consider both undirected and directed versions of the problem in this paper. For a history and more complete summary of the degree-diameter problem, see the survey paper by Miller and Širáň [5].

E-mail address: david.bevan@strath.ac.uk (David Bevan), grahame.erskine@open.ac.uk (Grahame Erskine), robert.lewis@open.ac.uk (Robert Lewis)

All groups considered in this paper are Abelian (indeed cyclic) and hence we use additive notation for the group operation. With this convention we define a *Cayley graph* as follows.

Let G be an Abelian group and $S \subseteq G$ a subset such that $0 \notin S$. Then the *Cayley graph* $\mathrm{Cay}(G, S)$ has the elements of G as its vertex set and each vertex g has an edge to $g + s$ for each $s \in S$. The following properties of $\mathrm{Cay}(G, S)$ are immediate from the definition:

- $\mathrm{Cay}(G, S)$ has order $|G|$ and is a regular graph of degree $|S|$.
- $\mathrm{Cay}(G, S)$ has diameter at most k if and only if every element of G can be expressed as a sum of no more than k elements of S.
- $\mathrm{Cay}(G, S)$ is an undirected graph if $S = -S$; otherwise it is a directed graph.

A *circulant graph* is a Cayley graph of a cyclic group, and we use these terms interchangeably.

Throughout the paper we use the following notation:

- $CC(d, k)$ is the largest order of an undirected circulant graph with degree d and diameter k.
- $DCC(d, k)$ is the largest order of a directed circulant graph with degree d and diameter k.

For a given diameter k, we are interested in determining the asymptotics of $CC(d, k)$ and $DCC(d, k)$ as the degree d tends to infinity. We make use of the following limits:

- $L_C^-(k) = \liminf_{d\to\infty} CC(d, k)/d^k$; $L_C^+(k) = \limsup_{d\to\infty} CC(d, k)/d^k$.
- $L_D^-(k) = \liminf_{d\to\infty} DCC(d, k)/d^k$; $L_D^+(k) = \limsup_{d\to\infty} DCC(d, k)/d^k$.

We begin with some trivial bounds on L^- and L^+. The following asymptotic upper bound is easily obtained; see for example the survey paper [5]:

Observation 1.1 (Trivial upper bound)**.** $L_C^+(k) \le L_D^+(k) \le \frac{1}{k!}$.

For a lower bound, consider $\mathbb{Z}_{r^k}$ with generators $\{hr^\ell : |h| \le \left\lfloor \frac{r}{2} \right\rfloor, 0 \le \ell < k\}$:

Observation 1.2 (Trivial lower bound)**.** $L_D^-(k) \ge L_C^-(k) \ge \frac{1}{k^k}$.

In this paper, we present constructions which yield, for each $k \ge 2$, lower bounds on $L_C^-(k)$ and $L_D^-(k)$ that are greater than the trivial $1/k^k$ bound. No such bounds were known previously. Our results include the following (see Corollary 4.6):

- For any diameter $k \ge 2$ and any degree d large enough, $CC(d, k) > \left(1.14775\,\frac{d}{k}\right)^k$.
- For any diameter k that is a multiple of 5 or sufficiently large, and any degree d large enough, $CC(d, k) > \left(1.20431\,\frac{d}{k}\right)^k$.
- For any diameter $k \ge 2$ and any degree d large enough, $DCC(d, k) > \left(1.22474\,\frac{d}{k}\right)^k$.
- For any diameter k that is a multiple of 6 or sufficiently large, and any degree d large enough, $DCC(d, k) > \left(1.27378\,\frac{d}{k}\right)^k$.

We also deduce a result concerning sumsets covering $\mathbb{Z}_n$, and use our techniques to construct a revised table of the largest known circulant graphs of small degree and diameter.

For larger diameters, the trivial bounds become numerically small, and the ratio between the upper and lower bound becomes arbitrarily large. Therefore, in order more easily to assess the success of our constructions, we make use of the following measure which records improvement over the trivial lower bound.

Let $R_C^-(k) = kL_C^-(k)^{1/k}$, and define $R_C^+(k)$, $R_D^-(k)$ and $R_D^+(k)$ analogously. Thus, $R_C^-(k) \geq 1$, with equality if the trivial lower bound is approached asymptotically for large degrees. For each k, these R values thus provide a useful indication of the success of our constructions in exceeding the trivial lower bound. In Section 4, we show how to construct a cyclic Cayley graph from two smaller ones in such a way that the R values are preserved.

The R values are bounded above by $R_{\max}(k) = k(k!)^{-1/k}$. Using the asymptotic version of Stirling's approximation, $\log k! \sim k \log k - k$, we see that as the diameter tends to infinity,

$$1 \;\leq\; \liminf_{k\to\infty} R_C^-(k) \;\leq\; \liminf_{k\to\infty} R_C^+(k) \;\leq\; e,$$

and similarly for $R_D^-(k)$ and $R_D^+(k)$.

In the next section, we extend a result of Vetrík [7] to deduce new lower bounds for $L_C^-(2)$ and $R_C^-(2)$. In Section 3, we describe a direct product construction and use it to build large cyclic Cayley graphs of small diameter and arbitrarily large degree. We also prove that this construction is unable to yield values that exceed the trivial lower bound for large diameter. However, in Section 4, we demonstrate a method of building a circulant graph by "stitching" together two smaller ones, and show how the application of this method to the constructions from Section 3 enables us to exceed the trivial lower bound for every diameter.

Section 5 contains an application of our constructions to obtain upper bounds on the minimum size of a set $A \subseteq \mathbb{Z}_n$ such that the k-fold sumset kA is equal to $\mathbb{Z}_n$. We conclude, in Section 6, by presenting a revised table of the largest known circulant graphs of small degree and diameter, including a number of new largest orders resulting from our constructions.

2 Diameter 2 bounds for all large degrees

Much of the study of this problem to date has concentrated on the diameter 2 undirected case. In this instance, the trivial lower bound on $L_C^-(2)$ is 1/4 and the trivial upper bound on $L_C^+(2)$ is 1/2. Vetrík [7] (building on Macbeth, Šiagiová & Širáň [4]) presents a construction that proves that $L_C^+(2) \geq \frac{13}{36} \approx 0.36111$, and thus $R_C^+(2) > 1.20185$.

In this section, we begin by extending this result to yield bounds for $L_C^-(2)$ and $R_C^-(2)$. This argument can also be found in Lewis [3]. We reproduce it here for completeness, since we make use of the resulting bounds below.

Vetrík's theorem applies only to values of the degree d of the form $6p-2$, where p is a prime such that $p \neq 13, p \not\equiv 1 \pmod{13}$. We extend this result to give a slightly weaker bound valid for all sufficiently large values of d. The strategy is as follows:

- Given a value of d, we select the largest prime p in the allowable congruence classes such that $6p - 2 \leq d$.
- We construct the graph of Vetrík [7] using this value of p.

- We add generators to the Vetrík construction (and hence edges to the Cayley graph) to obtain a new graph of degree d which still has diameter 2.

Note that the graphs in the Vetrík construction always have even order and hence we may obtain an odd degree d by adding the unique element of order 2 to the generator set.

Success of this method relies on being able to find a prime p sufficiently close to the optimal value so that we need only add asymptotically few edges to our graph. We use recent results of Cullinan & Hajir [1] following Ramaré & Rumely [6].

Lemma 2.1 (Cullinan & Hajir [1], Ramaré & Rumely [6]). *Let $\delta = 0.004049$. For any $x_0 \geq 10^{100}$ there exists a prime $p \equiv 2 \pmod{13}$ in the interval $[x_0, x_0 + \delta x_0]$.*

Proof. We use the method of Cullinan and Hajir [1, Theorem 1]. This method begins by using the tables of Ramaré and Rumely [6] to find a value ϵ corresponding to $k = 13, a = 2, x_0 = 10^{100}$. Following the proof of Cullinan and Hajir [1, Theorem 1], if $\delta > \frac{2\epsilon}{1-\epsilon}$ it follows that there must exist a prime $p \equiv 2 \pmod{13}$ in the interval $[x_0, x_0 + \delta x_0]$. From Table 1, Ramaré and Rumely [6] we find $\epsilon = 0.002020$ and hence $\delta = 0.004049$ will suffice. □

Our improved bound for circulant graphs of diameter 2 follows:

Theorem 2.2 (see [3, Theorem 6]). *$L_C^-(2) > 0.35820$, and hence $R_C^-(2) > 1.19700$.*

Proof. Let $\delta = 0.004049$ and let $d > 10^{101}$. We seek the largest prime $p \equiv 2 \pmod{13}$ such that $6p - 2 \leq d$. By the result of Lemma 2.1, there exists such a p with $p \geq (d + 2)/6(1 + \delta)$. Let $d' = 6p - 2$. Then by the result of Vetrík [7] we can construct a circulant graph of degree d', diameter 2 and order $n = \frac{13}{36}(d' + 2)(d' - 4)$. We can add $d - d'$ generators to this construction to obtain a graph of degree d and diameter 2, with the same order n.

Since $n = \frac{13}{36}d^2/(1 + \delta)^2 + O(d) \approx 0.358204d^2 + O(d)$ the result follows. □

3 Direct product constructions for small diameters

In this section, we construct large undirected circulant graphs of diameters $k = 3, 4, 5$ and arbitrary large degree. We also construct large directed circulant graphs of diameters $k = 2, \ldots, 9$ and arbitrary large degree. We then prove that the approach used is insufficient to yield values that exceed the trivial lower bound for large diameter.

3.1 Preliminaries

The diameter 2 constructions of Macbeth, Šiagiová & Širáň and of Vetrík both have the form $F_p^+ \times F_p^* \times \mathbb{Z}_w$ for some fixed w and variable p, where F_p^+ and F_p^* are the additive and multiplicative groups of the Galois field $GF(p)$. Thus the first two components of their constructions are very tightly coupled, and this coupling is a key to their success. However, a significant limitation of this method is that it is only applicable in the diameter 2 case.

In contrast, the constructions considered here have components that are as loosely coupled as possible. For diameter k, they have the form $\mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \ldots \times \mathbb{Z}_{r_k} \times \mathbb{Z}_w$ for some fixed w and variable pairwise coprime r_i. This gives us greater flexibility, especially in terms of the diameters we can achieve. The price for this is that we lose the inherent structure of the finite field, which consequently places limits on the bounds we can achieve.

The constructions in this section make use of the following result concerning the representation of each element of the cyclic group $\mathbb{T} = \mathbb{Z}_r \times \mathbb{Z}_s$ (r and s coprime) as the sum of a small multiple of the element $(1, 1)$ and a small multiple of another element (u, v). It can be helpful to envisage $\mathbb{T}$ as a group of vectors on the $r \times s$ discrete torus.

Lemma 3.1. *Let u, d, s and m be positive integers with $s > 1$ and coprime to md. Let $v = u + d$. Suppose $s \geq mv(u - 1)$. Then, for every element (x, y) of $\mathbb{T} = \mathbb{Z}_{s+md} \times \mathbb{Z}_s$, there exist nonnegative integers $h < s + mv$ and $\ell < s - m(u - 1)$ such that $(x, y) = h(1, 1) + \ell(u, v)$.*

Observe that the construction ensures that $(s + mv)(1, 1) = m(u, v)$. Figure 1 illustrates the case with parameters $u = 2$, $v = 5$, $s = 11$, $m = 2$.

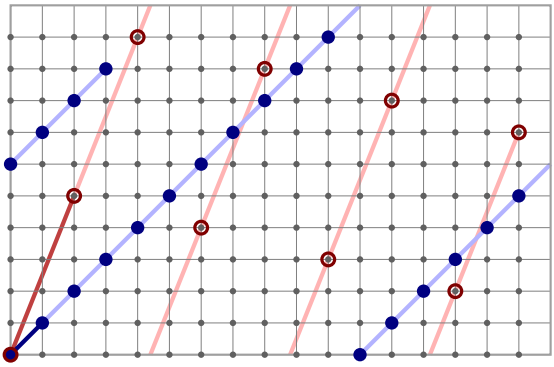

Figure 1: Every element of $\mathbb{Z}_{17} \times \mathbb{Z}_{11}$ is the sum of one of the 21 solid elements and one of the 9 circled elements.

Proof. Let $t = s - m(u - 1)$. Since s is coprime to md, $(1, 1)$ generates $\mathbb{T}$. Hence, it suffices to show that, in the list $(0, 0)$, $(1, 1)$, $(2, 2)$, ..., the gaps between members of $\{\ell(u, v) : 0 \leq \ell < t\}$ are not "too large".

Specifically, we need to show that, for each nonnegative $\ell < t$, there is some positive $h' \leq s + mv$ and nonnegative $\ell' < t$ such that $\ell(u, v) + h'(1, 1) = \ell'(u, v)$.

There are two cases. If $\ell < t - m$, then we can take $h' = s + mv$ and $\ell' = \ell + m$:

$$\begin{aligned} \ell(u, v) \ + \ (s + mv)(1, 1) &= (\ell u + s + mu + md, \ \ell v + s + mv) \\ &= (\ell u \quad + mu, \quad\quad \ell v \quad + mv) \\ &= (\ell + m)(u, v). \end{aligned}$$

If $\ell \geq t - m$, then we can take $h' = muv$ and $\ell' = \ell + m - t = \ell + mu - s$:

$$\begin{aligned} \ell(u, v) \ + \ muv(1, 1) &= (\ell u + mu^2 + mud, \quad\quad\quad\quad \ell v + muv) \\ &= (\ell u + mu^2 + mud - u(s + md), \ \ell v + muv - vs) \\ &= (\ell + mu - s)(u, v). \end{aligned}$$

The requirement that $muv \leq s + mv$ is clearly equivalent to the condition on s in the statement of the lemma. □

In our direct product constructions, we make use of Lemma 3.1 via the following crucial lemma. Our strategy is to construct a cyclic group of the form $\mathbb{T} = \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \ldots \times \mathbb{Z}_{r_k}$ such that $r_1 > r_2 > \ldots > r_k > 1$, and for each pair $\mathbb{Z}_{r_i} \times \mathbb{Z}_{r_j}$ for $i < j$ we will bring Lemma 3.1 to bear. In the notation of that lemma we will set $u = i$, $d = j - i$, $s = r_j$, $s + md = r_i$. The conditions of Lemma 3.2 below are designed to ensure that for each pair i, j we can find $m = m_{i,j}$ to make this work.

Lemma 3.2. *Let $k > 1$ and let $r_1 > r_2 > \ldots > r_k$ be pairwise coprime integers greater than 1 such that r_i is coprime to i for all $1 \leq i \leq k$. Suppose that for each i, j with $1 \leq i < j \leq k$ there exists a positive integer $m_{i,j}$ such that:*

- $r_i - r_j = m_{i,j}(j - i)$
- $r_j \geq m_{i,j}(i - 1)j$.

Let $\mathbb{T} = \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \ldots \times \mathbb{Z}_{r_k}$. Let $\mathbf{o} = (1, 1, \ldots, 1)$, $\mathbf{u} = (1, 2, \ldots, k)$ and, for each i, $\mathbf{e}_i = (0, \ldots, 1, \ldots, 0)$ be elements of $\mathbb{T}$, where only the ith coordinate of $\mathbf{e}_i$ is 1, and let the set A consist of these $k + 2$ elements.

Let $c_{\mathbf{o}} = \max_{i<j}(r_j + j\,m_{i,j})$, $c_{\mathbf{u}} = r_1$, and for each i, $c_{\mathbf{e}_i} = r_i$.

Then, for every element $\mathbf{x}$ of $\mathbb{T}$ and every k-element subset S of A, there exist nonnegative integers $h_{\mathbf{s}} < c_{\mathbf{s}}$ for each $\mathbf{s} \in S$, such that $\mathbf{x} = \sum_{\mathbf{s}} h_{\mathbf{s}}\,\mathbf{s}$.

Proof. There are four cases. If S contains neither $\mathbf{o}$ nor $\mathbf{u}$, the result follows trivially.

If S contains $\mathbf{o}$ but not $\mathbf{u}$, omitting $\mathbf{e}_i$, then we can choose $h_{\mathbf{o}}$ to be the ith coordinate of $\mathbf{x}$. Note that, as required, $c_{\mathbf{o}} \geq r_2 + 2(r_1 - r_2) = r_1 + (r_1 - r_2) > r_i$ for all i.

If S contains $\mathbf{u}$ but not $\mathbf{o}$, omitting $\mathbf{e}_i$, then, since i and r_i are coprime, we can choose $h_{\mathbf{u}}$ such that $i h_{\mathbf{u}} \pmod{r_i}$ is the ith coordinate of $\mathbf{x}$.

Finally, if S contains both $\mathbf{o}$ and $\mathbf{u}$, omitting $\mathbf{e}_i$ and $\mathbf{e}_j$, then we can choose $h_{\mathbf{o}}$ and $h_{\mathbf{u}}$ by applying Lemma 3.1 to $\mathbb{Z}_{r_i} \times \mathbb{Z}_{r_j}$ with $(u, v) = (i, j)$. □

We note that the conditions of Lemma 3.2 imply that at most one of the r_i can be even, and if $k \geq 4$ then all r_i must be odd.

3.2 Undirected constructions

We can use Lemma 3.2 to construct undirected circulant graphs of any diameter by means of the following theorem:

Theorem 3.3. *Let w and k be positive integers and suppose that there exist sets B and T of positive integers with the following properties:*

- *$B = \{b_1, \ldots, b_{k+2}\}$ has cardinality $k + 2$ and the property that every element of $\mathbb{Z}_w$ can be expressed as the sum of exactly k distinct elements of $B \cup -B$, no two of which are inverses.*
- *$T = \{r_1, r_2, \ldots, r_k\}$ has cardinality k and the properties that all its elements are coprime to w, and satisfies the requirements of Lemma 3.2, i.e. for each $i < j$:*

  (a) $r_i > r_j$

  (b) $\gcd(r_i, r_j) = 1$

  (c) $\gcd(r_i, i) = 1$

(d) There is a positive integer $m_{i,j}$ such that equalities $r_i - r_j = m_{i,j}(j-i)$ and $r_j \geq m_{i,j}(i-1)j$ hold.

Let $c_{\mathbf{o}} = \max_{i<j}(r_j + jm_{i,j})$ and $c_{\mathbf{u}} = r_1$ as in Lemma 3.2.

Then there exists an undirected circulant graph of order $w\prod_{i=1}^{k} r_i$, degree at most $2\left(\sum_{i=1}^{k} r_i + c_o + c_u\right)$ and diameter k.

Proof. Let $\mathbb{T} = \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \ldots \times \mathbb{Z}_{r_k} \times \mathbb{Z}_w$. Then $\mathbb{T}$ is a cyclic group since all its factors have coprime orders.

Let X be the generating set consisting of the following elements:

- $(x, 0, 0, \ldots, 0, \pm b_1)$, $x \in \mathbb{Z}_{r_1}$
- $(0, x, 0, \ldots, 0, \pm b_2)$, $x \in \mathbb{Z}_{r_2}$

  $\vdots$
- $(0, 0, \ldots, 0, x, \pm b_k)$, $x \in \mathbb{Z}_{r_k}$
- $\pm(x, x, \ldots, x, x, b_{k+1})$, $0 \leq x < c_{\mathbf{o}}$
- $\pm(x, 2x, \ldots, (k-1)x, kx, b_{k+2})$, $0 \leq x < c_{\mathbf{u}}$

Then by construction and by Lemma 3.2, every element of $\mathbb{T}$ is the sum of at most k elements of X. Since $|\mathbb{T}| = w\prod_{i=1}^{k} r_i$ and $|X| = 2\left(\sum_{i=1}^{k} r_i + c_o + c_u\right)$, the result follows. □

For small diameters this technique results in the following asymptotic bounds:

Theorem 3.4. *For diameters $k = 3, 4, 5$, we have the following lower bounds:*

(a) $L_C^+(3) \geq \frac{57}{1000}$ *and* $L_C^-(3) \geq \frac{7}{125}$, *so* $R_C^+(3) > 1.15455$ *and* $R_C^-(3) > 1.14775$.

(b) $L_C^+(4) \geq L_C^-(4) \geq \frac{25}{3456}$, *so* $R_C^+(4) \geq R_C^-(4) > 1.16654$.

(c) $L_C^+(5) \geq L_C^-(5) \geq \frac{109}{134456}$, *so* $R_C^+(5) \geq R_C^-(5) > 1.20431$.

Proof. Given a diameter k, the strategy is to find an optimal value of w which admits a set B satisfying the conditions of Theorem 3.3. We then seek an infinite family of positive integers q and a set $\Delta = \{\delta_1, \delta_2, \ldots, \delta_{k-1}\}$ such that for each of our values of q, the set $T = \{q, q-\delta_1, \ldots, q-\delta_{k-1}\}$ satisfies the conditions of the theorem. We illustrate for $k = 3$.

To prove *(a)* we take $w = 57$ and $B = \{1, 2, 7, 8, 27\}$. It is easily checked that every element of $\mathbb{Z}_{57}$ is the sum of three distinct elements of $B \cup -B$, no two of which are inverses. Now we let $\Delta = \{4, 6\}$. For any $q \geq 17, q \equiv 5 \pmod 6, q \not\equiv 0, 4, 6 \pmod{19}$ it is straightforward to verify that the set $T = \{q, q-4, q-6\}$ satisfies the conditions of Theorem 3.3. In the notation of Lemma 3.2, we have $c_{\mathbf{o}} = q + 4$.

Taking a generating set X as defined in Theorem 3.3 we may construct a circulant graph of diameter 3, degree $d = |X| = 10q - 12$ and order $57q(q-4)(q-6) = \frac{57}{1000}(d+12)(d-28)(d-48)$.

We can do this for an infinite number of values of q, and hence for an infinite number of values of $d = 10q - 12$ we have

$$CC(d, 3) \geq \frac{57}{1000}(d+12)(d-28)(d-48).$$

This yields $L_C^+(3) \geq \frac{57}{1000}$. Now we need to consider $L_C^-(3)$. The strategy will be to try to add "few" edges to our graphs to cover all possible degrees. Observe that we can use this construction for any $q \equiv 17 \pmod{114}$ and hence for any $d \equiv 158 \pmod{1140}$. Given any arbitrary *even* degree d, we can therefore find some d' no smaller than $d - 1140$ for which the construction works. We can then add $d - d'$ generators to our graph to obtain a graph of the same order, degree d and diameter 3.

However our graphs always have odd order, and so we are unable to obtain an odd degree graph by this method. To get round this problem we may use $w = 56$, $B = \{1, 2, 7, 14, 15\}$, $\Delta = \{2, 4\}$ and $c_{\mathbf{o}} = q + 2$. Again it is easy to check that the relevant conditions are satisfied for any $q \geq 15$ such that $q \equiv 3, 5 \pmod{6}$ and $q \equiv 1, 3, 5, 6 \pmod{7}$. Then for $d = 10q-8$ we can construct a graph of order $\frac{7}{25}(d+8)(d-12)(d-32)$, degree d and diameter 3. We can do this for any $q \equiv 15 \pmod{42}$ and hence for any $d \equiv 142 \pmod{420}$. So given any arbitrary degree d, we can therefore find some d' no smaller than $d - 420$ for which the construction works, and then add $d - d'$ generators to our graph to obtain a graph of the same order and diameter 3. (Since our graphs now have even order it is possible to add an odd number of generators.) Since the number of added generators is bounded above (by 419), the order of the graph is $\frac{7}{125}d^3 + O(d^2)$. Result *(a)* for $L_C^-(3)$ follows.

For *(b)* and *(c)* we adopt a similar method, except that in both cases the graphs used have even order and so our bounds on L^+ and L^- are equal. For brevity we show only the relevant sets in the construction, summarised as follows:

(b) ($k = 4$) – Take $w = 150$, $B = \{1, 7, 16, 26, 41, 61\}$ and $\Delta = \{6, 8, 12\}$ so $c_{\mathbf{o}} = q + 6$. Then for $q \geq 49$, $q \equiv 19 \pmod{30}$ and $d = 12q - 40$, we have

$$CC(d, 4) \geq \frac{25}{3456}(d + 40)(d - 32)(d - 56)(d - 104).$$

(c) ($k = 5$) – Take $w = 436$, $B = \{1, 15, 43, 48, 77, 109, 152\}$ and $\Delta = \{0, 4, 10, 12, 16\}$ so $c_{\mathbf{o}} = q + 8$. Then for $q \geq 77$, $q \equiv 5 \pmod{6}$, $q \not\equiv 0, 1 \pmod{5}$, $q \not\equiv 0, 4, 10, 12, 16 \pmod{109}$ and $d = 14q - 68$, we have

$$CC(d, 5) \geq \frac{109}{134456}(d + 68)(d + 12)(d - 72)(d - 100)(d - 156).$$

□

3.3 Directed constructions

An analogous method yields directed circulant graphs via the following theorem:

Theorem 3.5. *Let w and k be positive integers and suppose that there exist sets B and T of non-negative integers with the following properties:*

- *$B = \{0, b_2, \ldots, b_{k+2}\}$ has cardinality $k + 2$ and the property that every element of $\mathbb{Z}_w$ can be expressed as the sum of exactly k distinct elements of B.*
- *$T = \{r_1, r_2, \ldots, r_k\}$ has cardinality k and the properties that all its elements are coprime to w, and it satisfies the requirements of Lemma 3.2, i.e. for each $i < j$:*

  (a) $r_i > r_j$

(b) $\gcd(r_i, r_j) = 1$

(c) $\gcd(r_i, i) = 1$

(d) There is a positive integer $m_{i,j}$ *such that equalities* $r_i - r_j = m_{i,j}(j - i)$ *and* $r_j \geq m_{i,j}(i-1)j$ *hold.*

Let $c_{\mathbf{o}} = \max_{i<j}(r_j + jm_{i,j})$ *and* $c_{\mathbf{u}} = r_1$ *as in Lemma 3.2.*

Then we may construct a directed circulant graph of order $w\prod_{i=1}^{k} r_i$*, degree at most* $\sum_{i=1}^{k} r_i + c_o + c_u - 1$ *and diameter* k*.*

Proof. Let $\mathbb{T} = \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \ldots \times \mathbb{Z}_{r_k} \times \mathbb{Z}_w$. Then $\mathbb{T}$ is a cyclic group since all its factors have coprime orders.

Let X be the generating set consisting of the following elements:

- $(x, 0, 0, \ldots, 0, 0)$, $x \in \mathbb{Z}_{r_1} \setminus \{0\}$
- $(0, x, 0, \ldots, 0, b_2)$, $x \in \mathbb{Z}_{r_2}$

  $\vdots$
- $(0, 0, \ldots, 0, x, b_k)$, $x \in \mathbb{Z}_{r_k}$
- $(x, x, \ldots, x, x, b_{k+1})$, $0 \leq x < c_{\mathbf{o}}$
- $(x, 2x, \ldots, (k-1)x, kx, b_{k+2})$, $0 \leq x < c_{\mathbf{u}}$

Then by construction and by Lemma 3.2, every element of $\mathbb{T}$ is the sum of at most k elements of X. Since $|\mathbb{T}| = w\prod_{i=1}^{k} r_i$ and $|X| = \sum_{i=1}^{k} r_i + c_o + c_u - 1$, the result follows. □

For small diameters this technique results in the following asymptotic bounds:

Theorem 3.6. *For diameters* $k = 2, \ldots, 9$*, we have the following lower bounds on* $L_D^-(k)$ *and* $R_D^-(k)$*:*

(a) $L_D^-(2) \geq \frac{3}{8}$*, so* $R_D^-(2) > 1.22474$*.*

(b) $L_D^-(3) \geq \frac{9}{125}$*, so* $R_D^-(3) > 1.24805$*.*

(c) $L_D^-(4) \geq \frac{13}{1296}$*, so* $R_D^-(4) > 1.26588$*.*

(d) $L_D^-(5) \geq \frac{17}{16807}$*, so* $R_D^-(5) > 1.25881$*.*

(e) $L_D^-(6) \geq \frac{3}{32768}$*, so* $R_D^-(6) > 1.27378$*.*

(f) $L_D^-(7) \geq \frac{10}{1594323}$*, so* $R_D^-(7) > 1.26436$*.*

(g) $L_D^-(8) \geq \frac{9}{25000000}$*, so* $R_D^-(8) > 1.25206$*.*

(h) $L_D^-(9) \geq \frac{42}{2357947691}$*, so* $R_D^-(9) > 1.23939$*.*

Proof. The method is exactly the same as the proof of Theorem 3.4 and we summarise as follows:

(a) $(k = 2)$ – Take $w = 6$, $B = \{0, 1, 2, 4\}$ and $\Delta = \{2\}$ so $c_{\mathbf{o}} = q + 2$. Then for $q \geq 7$, $q \equiv 1 \pmod 6$ and $d = 4q - 1$, we have

$$DCC(d, 2) \geq \frac{3}{8}(d + 1)(d - 7).$$

(b) $(k = 3)$ – Take $w = 9$, $B = \{0, 1, 2, 3, 6\}$ and $\Delta = \{4, 6\}$ so $c_{\mathbf{o}} = q + 4$. Then for $q \geq 17$, $q \equiv 5 \pmod 6$ and $d = 5q - 7$, we have

$$DCC(d, 3) \geq \frac{9}{125}(d + 7)(d - 13)(d - 23).$$

(c) $(k = 4)$ – Take $w = 13$, $B = \{0, 1, 3, 5, 7, 8\}$ and $\Delta = \{2, 4, 6\}$ so $c_{\mathbf{o}} = q + 2$. Then for $q \geq 23$, $q \equiv 5 \pmod 6$, $q \not\equiv 0, 2, 4, 6 \pmod{13}$ and $d = 6q - 11$, we have

$$DCC(d, 4) \geq \frac{13}{1296}(d + 11)(d - 1)(d - 13)(d - 25).$$

(d) $(k = 5)$ – Take $w = 17$, $B = \{0, 1, 2, 3, 4, 8, 13\}$ and $\Delta = \{4, 10, 12, 16\}$ so $c_{\mathbf{o}} = q + 8$. Then for $q \geq 77$, $q \equiv 5 \pmod 6$, $q \not\equiv 0, 1 \pmod 5$, $q \not\equiv 0, 4, 10, 12, 16 \pmod{17}$ and $d = 7q - 35$, we have

$$DCC(d, 5) \geq \frac{17}{16807}(d + 35)(d + 7)(d - 35)(d - 49)(d - 77).$$

(e) $(k = 6)$ – Take $w = 24$, $B = \{0, 1, 2, 4, 8, 13, 18, 22\}$ and $\Delta = \{6, 12, 18, 24, 30\}$ so $c_{\mathbf{o}} = q + 6$. Then for $q \geq 181$, $q \equiv 1, 5 \pmod 6$, $q \not\equiv 0, 4 \pmod 5$ and $d = 8q - 85$, we have

$$DCC(d, 6) \geq \frac{3}{32768}(d + 85)(d + 37)(d - 11)(d - 59)(d - 107)(d - 155).$$

(f) $(k = 7)$ – Take $w = 30$, $B = \{0, 1, 2, 6, 9, 12, 16, 17, 18\}$ and $\Delta = \{0, 2, 6, 18, 20, 30, 42\}$ so $c_{\mathbf{o}} = q + 42$. Then for $q \geq 529$, $q \equiv 1 \pmod 6$, $q \equiv 4 \pmod 5$, $q \not\equiv 0, 2, 6 \pmod 7$, $q \not\equiv 9 \pmod{11}$ and $d = 9q - 77$, we have

$$DCC(d, 7) \geq \frac{10}{1594323}(d+77)(d+59)(d+23)(d-85)(d-103)(d-193)(d-301).$$

(g) $(k = 8)$ – Take $w = 36$, $B = \{0, 1, 2, 3, 6, 12, 19, 20, 27, 33\}$ and $\Delta = \{0, 6, 12, 18, 24, 30, 36, 42\}$ so $c_{\mathbf{o}} = q + 6$. Then for $q \geq 353$, $q \equiv 1, 5 \pmod 6$, $q \equiv 3 \pmod 5$, $q \not\equiv 0, 1 \pmod 7$ and $d = 10q - 163$, we have

$$\begin{aligned} DCC(d, 8) \geq \frac{9}{25000000}&(d + 163)(d + 103)(d + 43)(d - 17) \\ &(d - 77)(d - 137)(d - 197)(d - 257). \end{aligned}$$

(h) $(k = 9)$ – Take $w = 42$, $B = \{0, 1, 2, 3, 4, 9, 16, 20, 26, 30, 37\}$ and $\Delta = \{0, 2, 6, 12, 20, 30, 42, 56, 72\}$ so $c_{\mathbf{o}} = q + 72$. Then for $q \geq 1093$, $q \equiv 1 \pmod 6$, $q \equiv 3, 4 \pmod 5$, $q \equiv 1, 3, 4 \pmod 7$, $q \not\equiv 1, 6, 9 \pmod{11}$, $q \not\equiv 4, 7 \pmod{13}$ and $d = 11q - 169$, we have

$$\begin{aligned} DCC(d, 9) \geq \frac{42}{2357947691}&(d + 169)(d + 147)(d + 103)(d + 37)(d - 51) \\ &(d - 161)(d - 293)(d - 447)(d - 623). \end{aligned}$$

□

3.4 Limitations

In [3], Lewis showed that an analogous class of constructions using finite fields to create graphs of diameter 2 is limited by the bound $L_C^-(2) \leq \frac{3}{8}$. The constructions in this section have a similar limitation:

Observation 3.7. *Let k be a positive integer. The direct product constructions of Theorems 3.3 and 3.5 can never yield a lower bound on $L_C^-(k)$ or $L_D^-(k)$ that exceeds $\frac{k+1}{2(k+2)^{k-1}}$.*

Proof. First we consider the undirected case. Suppose the requirements of Theorem 3.3 hold and for each $i = 1, \ldots, k$, we have $r_i = q - a_i$, where $a_1 < a_2 < \ldots < a_k$. Let $\mathbb{T} = \mathbb{Z}_{q-a_1} \times \ldots \times \mathbb{Z}_{q-a_k} \times \mathbb{Z}_w$ and X be its generating set as in the proof of Theorem 3.3.

Since every element of $\mathbb{Z}_w$ is a sum of k distinct elements of B, no pair of which are inverses, we must have $w \leq \binom{k+2}{k} 2^k = (k+1)(k+2)2^{k-1}$.

By the requirements of Lemma 3.2, for any $i < j$, we have $m_{i,j} \leq r_i - r_j$ and $c_{\mathbf{o}} = \max_{i<j}(r_j + jm_{i,j})$. Hence, since $r_i = q - a_i$, we have $m_{i,j} \leq a_k - a_1$, and so $c_{\mathbf{o}} \leq q + ka_k$.

Thus X is the generating set for a Cayley graph on $\mathbb{T}$ with diameter k, degree d no greater than $2(k+2)q - 2\sum_{i=1}^{k} a_i + 2ka_k - 2a_1$, and order $n = w(q-a_1)(q-a_2)\ldots(q-a_k)$.

Hence, $n = \frac{w}{(2(k+2))^k} d^k + O(d^{k-1}) \leq \frac{(k+1)(k+2)2^{k-1}}{(2(k+2))^k} d^k + O(d^{k-1}) = \frac{k+1}{2(k+2)^{k-1}} d^k + O(d^{k-1})$, as required.

The directed case is analogous. We follow Theorem 3.5 and its proof. In this case, every element of $\mathbb{Z}_w$ is the sum of k distinct elements of B, so $w \leq \binom{k+2}{k} = (k+1)(k+2)/2$, and X is the generating set for a Cayley graph on $\mathbb{T}$ with diameter k, degree $d \leq (k+2)q - \sum_{i=1}^{k} a_i + ka_k - a_1 - 1$, and order $n = w(q-a_1)(q-a_2)\ldots(q-a_k)$.

Hence, $n = \frac{w}{(k+2)^k} d^k + O(d^{k-1}) \leq \frac{(k+1)(k+2)}{2(k+2)^k} d^k + O(d^{k-1}) = \frac{k+1}{2(k+2)^{k-1}} d^k + O(d^{k-1})$. □

Observe that, in the limit,

$$\lim_{k\to\infty} k \left(\frac{k+1}{2(k+2)^{k-1}} \right)^{1/k} = 1.$$

As a consequence, these direct product constructions themselves can never yield an improvement on the trivial lower bound for the limiting value of $R_C^-(k)$ or $R_D^-(k)$. However, it is possible to combine graphs of small diameter to produce larger graphs in such a way that we can improve on the trivial lower bound in the limit as the diameter increases. The next section introduces this idea.

4 A general graph product construction

The following theorem gives a simple way to combine two cyclic Cayley graphs to obtain a third cyclic Cayley graph. It is valid in both the directed and undirected cases.

Theorem 4.1. *Let G_1 and G_2 be two cyclic Cayley graphs of diameters k_1 and k_2, orders n_1 and n_2, and degrees d_1 and d_2 respectively. In the case of undirected graphs where d_1 and d_2 are both odd let $\delta = 1$, otherwise $\delta = 0$. In the directed case let $\delta = 0$ always. Then there exists a cyclic Cayley graph with diameter $k_1 + k_2$, degree at most $d_1 + d_2 + \delta$, and order $n_1 n_2$.*

Proof. Let S_1 be the connection set of G_1 so that $|S_1| = d_1$ and similarly for G_2. For convenience we consider each S_i to consist of elements within the interval $(-n_i/2, n_i/2]$. Let G be the cyclic group $\mathbb{Z}_{n_1 n_2}$ and consider the connection set $S' = n_2 S_1 \cup S_2$. Then $|S'| \leq n_1 + n_2$.

We now construct a connection set S for the group G such that the Cayley graph $\mathrm{Cay}(G, S)$ has diameter $k_1 + k_2$. In the directed case we may simply take $S = S'$. In the undirected case we need to ensure that $S = -S$. If at least one of d_1, d_2 is even we may assume without loss of generality that d_2 is even and then we may again let $S = S'$ and $S = -S$ by construction.

It remains to consider the undirected case when d_1 and d_2 are both odd (the case $\delta = 1$). In that case we know $n_2/2 \in S_2 \subset S'$ and we let $S = S' \cup \{-n/2\}$ so that $S = -S$.

It is then clear that the Cayley graph $\mathrm{Cay}(G, S)$ has degree at most $d_1 + d_2 + \delta$, diameter $k_1 + k_2$ and order $n_1 n_2$. □

We can use this "stitching" construction to obtain lower bounds on our L and R values for large diameters, given values for smaller diameters.

Corollary 4.2. *If $L(k)$ is one of $L_C^-(k)$, $L_C^+(k)$, $L_D^-(k)$ or $L_D^+(k)$ and $R(k)$ is one of $R_C^-(k)$, $R_C^+(k)$, $R_D^-(k)$ or $R_D^+(k)$, then*

(a) $L(k_1 + k_2) \geq \dfrac{L(k_1) L(k_2) k_1^{k_1} k_2^{k_2}}{(k_1 + k_2)^{k_1 + k_2}}$,

(b) $R(k_1 + k_2) \geq \left(R(k_1)^{k_1} R(k_2)^{k_2}\right)^{\frac{1}{k_1 + k_2}}$.

Proof. (a) Let $d > 1$. For $i = 1, 2$ we may construct graphs Γ_i of diameter k_i, degree $k_i d$ and order $L(k_i)(k_i d)^{k_i} + o(d^{k_i})$. Theorem 4.1 yields a product graph of diameter $k_1 + k_2$, degree at most $(k_1 + k_2)d + 1$ and order $L(k_1)L(k_2)k_1^{k_1} k_2^{k_2} d^{k_1 + k_2} + o(d^{k_1 + k_2})$.

Part *(b)* follows by straightforward algebraic manipulation. □

In particular, we note that the stitching construction of Theorem 4.1 preserves lower bounds on the R values: $R(mk) \geq R(k)$ for every positive integer m.

We may use this idea to obtain better bounds for some particular diameters; for example we may improve on the undirected diameter 4 construction in Theorem 3.4:

Corollary 4.3.

(a) $L_C^+(4) \geq \frac{169}{20736} \approx 0.0081501$, *and hence* $R_C^+(4) > 1.20185$.

(b) $L_C^-(4) > 0.0080194$, *and hence* $R_C^-(4) > 1.19700$.

Proof. For statement *(a)* we note $R_C^+(2) \geq \frac{13}{36}$ from Vetrík [7] and apply Corollary 4.2 with $k_1 = k_2 = 2$. For *(b)* we use the same method starting with Theorem 2.2. □

The stitching process of Theorem 4.1 can be iterated to produce a construction for any desired diameter, and Corollary 4.2 then gives us a lower bound for the R values for that diameter. We illustrate the results for small diameter k in Table 1. As an indicator of progress we show also the largest possible value of R for a particular k, given by $R_{\max}(k) = k(k!)^{-1/k}$.

It is worth noting that the method of Corollary 4.2 may be used to produce values of R which are larger than those achievable from the direct product constructions of Section 3.

Table 1: The best R values for diameter $k \leq 9$.

	Diameter (k)							
	2	3	4	5	6	7	8	9
$R_{\max}(k) \approx$	1.41421	1.65096	1.80720	1.91926	2.00415	2.07100	2.12520	2.17016
$R_C^+(k) >$	1.20185^a	1.15455^d	1.20185^c	1.20431^d	1.20185^f	1.20360^f	1.20185^f	1.20321^f
$R_C^-(k) >$	1.19700^b	1.14775^d	1.19700^c	1.20431^d	1.19700^f	1.20222^f	1.19700^f	1.20105^f
$R_D^-(k) >$	1.22474^e	1.24805^e	1.26588^e	1.25881^e	1.27378^e	1.26436^e	1.26588^f	1.26514^f

a. Vetrík [7]; b. Theorem 2.2; c. Corollary 4.3; d. Theorem 3.4; e. Theorem 3.6; f. Corollary 4.2

For example, the limitations noted in Observation 3.7 show that the maximum possible value of $R_D^-(10)$ we could achieve using Theorem 3.5 is approximately 1.26699. However, combining the results for diameters 4 and 6 in Table 1 yields $R_D^-(10) > 1.27061$.

Next we use our previous results to show that R is well-behaved in the limit.

Theorem 4.4. *Let $L(k)$ be one of $L_C^-(k)$, $L_C^+(k)$, $L_D^-(k)$ or $L_D^+(k)$, and let $R(k) = kL(k)^{1/k}$. The limit $R = \lim_{k\to\infty} R(k)$ exists and is equal to $\sup R(k)$.*

Proof. $R(k)$ is bounded above (by e), so $s = \sup R(k)$ is finite. Hence, given $\varepsilon > 0$, we can choose k so that $s - R(k) < \varepsilon/2$. By Corollary 4.2 (b), $R(mk) \geq R(k)$ for every positive integer m. Moreover, for any fixed $j < k$, since $R(j) \geq 1$, we have $R(mk+j) \geq R(k)^{mk/(mk+j)} \geq R(k)^{m/(m+1)}$, which, by choosing m large enough, can be made to differ from $R(k)$ by no more than $\varepsilon/2$. □

Corollary 4.5.

(a) $\lim_{k\to\infty} R_C^-(k) \geq \dfrac{5 \times 109^{1/5}}{7 \times 2^{3/5}} > 1.20431$

(b) $\lim_{k\to\infty} R_D^-(k) \geq \dfrac{3^{7/6}}{2^{3/2}} > 1.27378$

Proof. We choose the largest entry in the relevant row in Table 1. For *(a)* we know from Theorem 3.4 that $L_C^-(5) \geq \frac{109}{2^3 \times 7^5}$. For *(b)* we know from Theorem 3.6 that $L_D^-(6) \geq \frac{3}{2^{15}}$. □

We conclude this section by using the foregoing to derive new lower bounds for the maximum possible orders of circulant graphs of given diameter and sufficiently large degree.

Corollary 4.6.

(a) For any diameter $k \geq 2$ and any degree d large enough, $CC(d,k) > \left(1.14775\,\frac{d}{k}\right)^k$.

(b) For any diameter k that is a multiple of 5 or sufficiently large, and any degree d large enough, $CC(d,k) > \left(1.20431\,\frac{d}{k}\right)^k$.

(c) For any diameter $k \geq 2$ and any degree d large enough, $DCC(d,k) > \left(1.22474\,\frac{d}{k}\right)^k$.

(d) For any diameter k that is a multiple of 6 or sufficiently large, and any degree d large enough, $DCC(d,k) > \left(1.27378\,\frac{d}{k}\right)^k$.

Proof.

(a) From Theorem 4.4 and Corollary 4.2, we know that $R_C^-(k)$ always exceeds the smallest value in the R_C^- row of Table 1, which is 1.14775.

(b) For k a multiple of 5, we know from Theorem 3.4 and Corollary 4.2 that $R_C^-(k) > 1.20431$. The result for sufficiently large k follows from Corollary 4.5.

(c) and (d) follow by using similar logic in the directed case.

□

These represent significant improvements over the trivial bound of $\left(\frac{d}{k}\right)^k$.

5 Sumsets covering $\mathbb{Z}_n$

Our constructions of directed circulant graphs can be used to obtain an upper bound on the minimum size, $SS(n,k)$, of a set $A \subset \mathbb{Z}_n$ for which the sumset

$$kA = \underbrace{A + A + \ldots + A}_{k} = \mathbb{Z}_n.$$

The trivial bound is $SS(n,k) \leq kn^{1/k}$ which follows in the same way as the trivial lower bound for the directed circulant graph (see Observation 1.2). Improvements to this trivial bound do not appear to have been investigated in the literature.

The idea is that, given $S \subseteq \mathbb{Z}_n$ such that $\mathrm{Cay}(\mathbb{Z}_n, S)$ has diameter k, if we let $A = S \cup \{0\}$ then $kA = \mathbb{Z}_n$. Our constructions thus enable us to bound $SS(n,k)$ for fixed k and infinitely many values of n. For example, if we let $L_S^-(k) = \liminf_{n\to\infty} SS(n,k)/n^{1/k}$, then the following new result for $k = 2$ follows from Theorem 3.6 (a):

Corollary 5.1. $L_S^-(2) \leq \sqrt{\frac{8}{3}} \approx 1.63299$.

More generally, Corollary 4.5 shows that for large enough k and infinitely many values of n, $SS(n,k)$ is at least 21 percent smaller than the trivial bound:

Corollary 5.2. $\lim_{k\to\infty} k^{-1} L_S^-(k) \leq \frac{2^{3/2}}{3^{7/6}} \approx 0.78506$.

6 Largest graphs of small degree and diameter

We can use the construction of Theorem 4.1 to obtain large undirected circulant graphs for small degrees and diameters. Recently in [2], Feria-Puron, Pérez-Rosés and Ryan published a table of largest known circulant graphs with degree up to 16 and diameter up to 10. Their method uses a construction based on graph Cartesian products which is somewhat similar to ours. In contrast, however, Theorem 4.1 does not in general result in a graph isomorphic to the Cartesian product of the constituents. Furthermore, our construction does not require the constituent graph orders to be coprime, which allows more graphs to be constructed.

Using Theorem 4.1 allowed us to improve many of the entries in the published table. However, at the same time we developed a computer search which allows us to find circulant graphs of given degree, diameter and order. It turns out that this search is able to find

larger graphs (at least in the range $d \leq 16, k \leq 10$) than the Theorem 4.1 method. We therefore present a much improved table of largest known circulant graphs based on the outputs of this search.

In Table 2, we show the largest known circulant graphs of degree $d \leq 16$ and diameter $k \leq 10$. In Table 3 we give a reduced generating set for each new record largest graph found by the search. The computer search has been completed as an exhaustive search in the diameter 2 case up to degree 23, and these results are included in Table 3 for completeness.

Table 2: Largest known circulant graphs of degree $d \leq 16$ and diameter $k \leq 10$.

$d \setminus k$	1	2	3	4	5	6	7	8	9	10
2	3	5	7	9	11	13	15	17	19	21
3	4	8	12	16	20	24	28	32	36	40
4	5	13	25	41	61	85	113	145	181	221
5	6	16	36	64	100	144	196	256	324	400
6	7	21	55	117	203	333	515	737	1027	1393
7	8	26	76	160	308	536	828	1232	1764	2392
8	9	35	104	248	528	984	1712	2768	4280	6320
9	10	42	130	320	700	1416	2548	4304	6804	10320
10	11	51	177	457	1099	2380†	4551†	8288†	14099†	22805†
11	12	56	210	576	1428†	3200†	6652†	12416†	21572†	35880†
12	13	67	275	819†	2040†	4283†	8828†	16439†	29308†	51154†
13	14	80	312	970†	2548†	5598†	12176†	22198†	40720†	72608†
14	15	90	381	1229†	3244†	7815†	17389†	35929†	71748†	126109†
15	16	96	448	1420†	3980†	9860†	22584†	48408†	93804†	177302†
16	17	112	518†	1717†	5024†	13380†	32731†	71731†	148385†	298105†

† new record largest value

Table 3: Largest circulant graphs of small degree d and diameter k found by computer search.

d	k	Order	Generators
6	2	21*	$1, 2, 8$
6	3	55*	$1, 5, 21$
6	4	117*	$1, 16, 22$
6	5	203*	$1, 7, 57$
6	6	333*	$1, 9, 73$
6	7	515*	$1, 46, 56$
6	8	737*	$1, 11, 133$
6	9	1027*	$1, 13, 157$
6	10	1393*	$1, 92, 106$
7	2	26*	$1, 2, 8$
7	3	76*	$1, 27, 31$
7	4	160*	$1, 5, 31$
7	5	308*	$1, 7, 43$
7	6	536*	$1, 231, 239$
7	7	828*	$1, 9, 91$
7	8	1232*	$1, 11, 111$
7	9	1764*	$1, 803, 815$
7	10	2392*	$1, 13, 183$

Continues on next page

Table 3 – continued from previous page

d	k	Order	Generators
8	2	35*	1, 6, 7, 10
8	3	104*	1, 16, 20, 27
8	4	248*	1, 61, 72, 76
8	5	528*	1, 89, 156, 162
8	6	984*	1, 163, 348, 354
8	7	1712*	1, 215, 608, 616
8	8	2768	1, 345, 1072, 1080
8	9	4280	1, 429, 1660, 1670
8	10	6320	1, 631, 2580, 2590
9	2	42*	1, 5, 14, 17
9	3	130*	1, 8, 14, 47
9	4	320*	1, 15, 25, 83
9	5	700*	1, 5, 197, 223
9	6	1416	1, 7, 575, 611
9	7	2548	1, 7, 521, 571
9	8	4304	1, 9, 1855, 1919
9	9	6804	1, 9, 1849, 1931
9	10	10320	1, 11, 4599, 4699
10	2	51*	1, 2, 10, 16, 23
10	3	177*	1, 12, 19, 27, 87
10	4	457*	1, 20, 130, 147, 191
10	5	1099*	1, 53, 207, 272, 536
10	6	2380	1, 555, 860, 951, 970
10	7	4551	1, 739, 1178, 1295, 1301
10	8	8288	1, 987, 2367, 2534, 3528
10	9	14099	1, 1440, 3660, 3668, 6247
10	10	22805	1, 218, 1970, 6819, 6827
11	2	56*	1, 2, 10, 15, 22
11	3	210*	1, 49, 59, 84, 89
11	4	576*	1, 9, 75, 155, 179
11	5	1428	1, 169, 285, 289, 387
11	6	3200	1, 259, 325, 329, 1229
11	7	6652	1, 107, 647, 2235, 2769
11	8	12416	1, 145, 863, 4163, 5177
11	9	21572	1, 663, 6257, 10003, 10011
11	10	35880	1, 2209, 5127, 5135, 12537
12	2	67*	1, 2, 3, 13, 21, 30
12	3	275*	1, 16, 19, 29, 86, 110
12	4	819	7, 26, 119, 143, 377, 385
12	5	2040	1, 20, 24, 152, 511, 628
12	6	4283	1, 19, 100, 431, 874, 1028
12	7	8828	1, 29, 420, 741, 2727, 3185
12	8	16439	1, 151, 840, 1278, 2182, 2913
12	9	29308	1, 219, 1011, 1509, 6948, 8506
12	10	51154	1, 39, 1378, 3775, 5447, 24629
13	2	80*	1, 3, 9, 20, 25, 33
13	3	312*	1, 14, 74, 77, 130, 138
13	4	970	1, 23, 40, 76, 172, 395
13	5	2548	1, 117, 121, 391, 481, 1101
13	6	5598	1, 12, 216, 450, 1204, 2708
13	7	12176	1, 45, 454, 1120, 1632, 1899
13	8	22198	1, 156, 1166, 2362, 5999, 9756
13	9	40720	1, 242, 3091, 4615, 5162, 13571
13	10	72608	1, 259, 4815, 8501, 8623, 23023
14	2	90*	1, 4, 10, 17, 26, 29, 41
14	3	381*	1, 11, 103, 120, 155, 161, 187
14	4	1229	1, 8, 105, 148, 160, 379, 502

Continues on next page

Table 3 – continued from previous page

d	k	Order	Generators
14	5	3244	1, 108, 244, 506, 709, 920, 1252
14	6	7815	1, 197, 460, 696, 975, 2164, 3032
14	7	17389	1, 123, 955, 1683, 1772, 2399, 8362
14	8	35929	1, 796, 1088, 3082, 3814, 13947, 14721
14	9	71748	1, 1223, 3156, 4147, 5439, 11841, 25120
14	10	126109	1, 503, 4548, 7762, 9210, 9234, 49414
15	2	96*	1, 2, 3, 14, 21, 31, 39
15	3	448*	1, 10, 127, 150, 176, 189, 217
15	4	1420	1, 20, 111, 196, 264, 340, 343
15	5	3980	1, 264, 300, 382, 668, 774, 1437
15	6	9860	1, 438, 805, 1131, 1255, 3041, 3254
15	7	22584	1, 1396, 2226, 2309, 2329, 4582, 9436
15	8	48408	1, 472, 2421, 3827, 4885, 5114, 12628
15	9	93804	1, 3304, 4679, 9140, 10144, 10160, 13845
15	10	177302	1, 2193, 8578, 18202, 23704, 23716, 54925
16	2	112*	1, 4, 10, 17, 29, 36, 45, 52
16	3	518	1, 8, 36, 46, 75, 133, 183, 247
16	4	1717	1, 46, 144, 272, 297, 480, 582, 601
16	5	5024	1, 380, 451, 811, 1093, 1202, 1492, 1677
16	6	13380	1, 395, 567, 1238, 1420, 1544, 2526, 4580
16	7	32731	1, 316, 1150, 1797, 2909, 4460, 4836, 16047
16	8	71731	1, 749, 4314, 7798, 10918, 11338, 11471, 25094
16	9	148385	1, 6094, 6964, 10683, 11704, 14274, 14332, 54076
16	10	298105	1, 5860, 11313, 15833, 21207, 26491, 26722, 99924
17	2	130*	1, 7, 26, 37, 47, 49, 52, 61
18	2	138*	1, 9, 12, 15, 22, 42, 27, 51, 68
19	2	156*	1, 15, 21, 23, 26, 33, 52, 61, 65
20	2	171*	1, 11, 31, 36, 37, 50, 54, 47, 65, 81
21	2	192*	1, 3, 15, 23, 32, 51, 57, 64, 85, 91
22	2	210*	2, 7, 12, 18, 32, 35, 63, 70, 78, 91, 92
23	2	216*	1, 3, 5, 17, 27, 36, 43, 57, 72, 83, 95

* proven extremal

References

[1] J. Cullinan and F. Hajir, Primes of prescribed congruence class in short intervals, *Integers* **12** (2012), #A56, http://www.integers-ejcnt.org/vol12.html.

[2] R. Feria-Puron, H. Perez-Roses and J. Ryan, Searching for large circulant graphs, 2015, arXiv:1503.07357 [math.CO].

[3] R. R. Lewis, Improved upper bounds for the order of some classes of Abelian Cayley and circulant graphs of diameter two, 2015, arXiv:1506.02844 [math.CO].

[4] H. Macbeth, J. Šiagiová and J. Širáň, Cayley graphs of given degree and diameter for cyclic, Abelian, and metacyclic groups, *Discrete Math.* **312** (2012), 94–99, doi:10.1016/j.disc.2011.03.038.

[5] M. Miller and J. Širáň, Moore graphs and beyond: a survey of the degree/diameter problem, *Electron. J. Comb.* (2013), #DS14v2, http://www.combinatorics.org/ojs/index.php/eljc/article/view/DS14.

[6] O. Ramaré and R. Rumely, Primes in arithmetic progressions, *Math. Comp.* **65** (1996), 397–425, doi:10.1090/S0025-5718-96-00669-2.

[7] T. Vetrík, Abelian Cayley graphs of given degree and diameter 2 and 3, *Graphs Combin.* **30** (2014), 1587–1591, doi:10.1007/s00373-013-1361-5.