dMFA

ARS MATHEMATICA CONTEMPORANEA

Also available at http://amc.imfm.si
ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 4 (2011) 63–72

Motion and distinguishing number two*

Marston Conder †
Department of Mathematics, University of Auckland,
Private Bag 92019, Auckland 1142, New Zealand

Thomas Tucker
Mathematics Department, Colgate University, Hamilton, NY 13346, USA

Received 10 July 2010, accepted 27 September 2010, published online 7 March 2011

Abstract

A group A acting faithfully on a finite set X is said to have distinguishing number two if there is a proper subset Y whose (setwise) stabilizer is trivial. The motion of A acting on X is defined as the largest integer k such that all non-trivial elements of A move at least k elements of X. The Motion Lemma of Russell and Sundaram states that if the motion is at least $2\log_2|A|$, then the action has distinguishing number two. When X is a vector space, group, or map, the Motion Lemma and elementary estimates of the motion together show that in all but finitely many cases, the action of $\mathrm{Aut}(X)$ on X has distinguishing number two. A new lower bound for the motion of any transitive action gives similar results for transitive actions with restricted point-stabilizers. As an instance of what can happen with intransitive actions, it is shown that if X is a set of points on a closed surface of genus g, and $|X|$ is sufficiently large with respect to g, then any action on X by a finite group of surface homeomorphisms has distinguishing number two.

Keywords: Distinguishing number, group action, stabilizer, motion.

Math. Subj. Class.: 05E18, 05C10, 20B05

1 Introduction

Let A be a group acting faithfully on a set X. The *distinguishing number* for this action, denoted by $D(A, X)$, is the smallest natural number k such that the elements of X can be colored with k colors so that any color-preserving element of A fixes all $x \in X$. In particular, if the action is faithful, then the only element of A preserving colors is the identity. This terminology was introduced by Albertson and Collins [2] in the situation where

*In memory of Michael Albertson.

†Supported in part by the N.Z. Marsden Fund (grant no. UOA0721).

E-mail addresses: m.conder@auckland.ac.nz (Marston Conder), ttucker@mail.colgate.edu (Thomas Tucker)

$A = \mathrm{Aut}(G)$ and $X = \mathrm{V}(G)$ for a graph G. This was later generalized to arbitrary group actions by Tymoczko [21]. On the other hand, the special case of distinguishing number two had been considered previously for permutation groups. For example, a theorem by Gluck [13] states that $D(A, X) = 2$ whenever $|A|$ is odd, and this preceded [2] by ten years. Albertson and Collins were motivated by a long-standing recreational mathematics question on coloring beads on a necklace (or keys on a key chain) so as to destroy the dihedral symmetry: two colors suffice if the number of beads is at least 6 and one of the colors is used on only three beads.

The theme of this paper is that having distinguishing number two is a generic property. Gluck's Theorem is a good example. If one takes a Cartesian product of enough copies of the same graph, then the distinguishing number is two (see [1, 15]). For all maps with more than 10 vertices, the action of the automorphism group on the vertices has distinguishing number two (see [20]). All primitive permutation groups of degree $n > 32$ other than S_n or A_n have distinguishing number two (see [19, 4]).

Given an action of A on X, the *motion* of the action is defined by Russell and Sundaram [18] as the smallest integer k such that some non-trivial element of A moves exactly k elements of X. This number, denoted by $m(A, X)$, or simply $m(A)$ when the context is clear, is more commonly known as the *minimal degree* of the permutation group induced by A on X. The survey paper [4] provides a number of examples of other recent concepts in graph theory that have had previous lives, under different names, in the theory of permutation groups.

Russell and Sundaram's 'Motion Lemma' [18] shows that the distinguishing number of a group action is two if the motion is large enough with respect to the order of the group:

Lemma 1.1. *If the group A acts faithfully on the set X with $m(A, X) > 2\log_2 |A|$, then $D(A, X) = 2$.*

The proof is short and elementary; see [18] or [20].

In this paper, we show how motion can be used to prove that for various types of actions, the distinguishing number is two in all but finitely many cases. In other words, having distinguishing number two is generic to many situations. The contexts we will study in this paper include these: $\mathrm{Aut}(X)$ on X where X is a finite vector space, a group, or a map; general transitive actions where $|X| > 4(\log_2 |A|)^2$; general transitive group actions with restricted point-stabilizers; and intransitive actions on a finite subset of a surface. Along the way, we also give a general lower bound on the motion (or equivalently, the minimal degree) of any transitive permutation group. Although it can be derived from an exercise in [10], we have been unable to find this bound in the literature.

Given an action of A on X, we denote by A_x the stabilizer of a point $x \in X$, and given a subset $Y \subseteq X$, we denote by A_Y the pointwise stabilizer of Y, namely the subgroup of all $a \in A$ that fix every point of Y, and by $A_{\{Y\}}$ the setwise stabilizer of Y, which is the subgroup of all $a \in A$ that preserve Y. We sometimes use $m(a)$ for the number of points of X moved by an element $a \in A$ (that is, the size of the *support* of a), so that $m(A) = \min(\{m(a) : a \in A \setminus \{1\}\})$. We also sometimes denote the action of A on X simply by the pair (A, X). Note that $D(A, X) = 2$ if and only if A has a regular orbit on the subsets of X — that is, an 'orbital' on which A acts (transitively) with trivial point-stabilizer.

2 Vector spaces and groups

We apply the Motion Lemma here to two cases: one where X is a finite-dimensional vector space over a finite field K, and one where X is a group. The first was considered by Chan [8], and then answered completely by Klavžar, Wong and Zhu [16].

Theorem 2.1. *Let X be a vector space of dimension n over the finite field $GF(q)$ and let $A = \mathrm{Aut}(X) = GL(n,q)$. Then $D(A,X) = 2$ in all cases except possibly those where $q = 4$ and $n = 2$, or $q = 3$ and $n \leq 3$, or $q = 2$ and $n \leq 7$.*

Proof. Since the vectors fixed by any $a \in A$ form a subspace of X of dimension at most $n-1$, we have $m(A) \geq q^n - q^{n-1}$. Also there are q^{n^2} matrices of size $n \times n$ over $GF(q)$ so $|A| < q^{n^2}$. Hence by the Motion Lemma, $D(A,X) = 2$ whenever

$$q^n - q^{n-1} \geq 2n^2 \log_2 q.$$

It is easily verified that this inequality holds for all $q \geq 5$ when $n = 2$, and also holds when $(q,n) = (4,3)$, $(3,4)$, or $(2,8)$. Also for fixed q, the left side of this inequality increases with n more rapidly than the right side, and so the result follows. □

With considerably more work, it is shown in [16] that $D(A,X) = 2$ for all the other cases except those where $(q,n) = (3,2)$, or $q = 2$ and $n \leq 4$. It is also shown in [16] that $D(A,X) = 3$ in all these remaining cases except $(q,n) = (2,3)$, when $D(A,X) = 4$. It should be noted that motion is not used in either [8] or [16], and that the remaining cases can be handled by computer.

Next, we consider the case where X is a group G, and A is the group of all automorphisms of G.

Theorem 2.2. *Let G be a finite group with order $|G| \geq 256$, and let $A = \mathrm{Aut}(G)$. Then $D(A,G) = 2$.*

Proof. Let $n = |G|$. Since the elements of G fixed by a given $a \in A$ form a proper subgroup of G, we have $m(A) \geq n/2$. To obtain an upper bound on $|A|$, let r be the rank of G (namely the smallest size of a generating set for G). Then $|A| < n^r$, since any automorphism is determined by what it does on a generating set, and each non-trivial generator has at most $n-1$ possible images under the automorphism. Also r is at most equal to the sum of the exponents in the prime-power factorization of n, since one may construct a generating set from generating sets for the Sylow subgroups of G. In particular, we have $r < \log_2 n$, so $\log_2 |A| < r \log_2 n < (\log_2 n)^2$. Now for $n \geq 256 = 2^8$ we have $n \geq 4(\log_2 n)^2$, and hence by the Motion Lemma, $D(A,G) = 2$. □

It is not difficult to reduce the given lower bound on $n = |G|$ in the above theorem. For example, if $n \geq 4r \log_2 n$, then $m(A) \geq n/2 \geq 2r \log_2 n > 2 \log_2 |A|$ and so $D(A,G) = 2$. In particular, this occurs when $r \leq 4$ and $n \geq 128$. Hence in the range $128 \leq |G| < 256$ we need only consider groups G rank 5 or more, implying that n has at most one prime factor larger than 3. Arguments like this can be used to show that $D(A,G) = 2$ whenever $|G| > 128$. On the other hand, use of the computer systems GAP [12] or MAGMA [5] is helpful to consider the cases $|G| \leq 128$, and hence to obtain the following:

Theorem 2.3. *For groups, $D(\mathrm{Aut}(G), G) \neq 2$ if and only if G is isomorphic to one of the four elementary abelian groups ${C_2}^2, {C_2}^3, {C_3}^2$ and ${C_2}^4$ (of orders 4, 8, 9 and 16) or the quaternion group Q_8.*

It is interesting to note that the five groups given in the theorem are precisely those shown by Babai [3] to have no *directed graphical representation (DRR)*. The latter is defined as follows. Given a generating set Y for the group G, the Cayley digraph $C(G, Y)$ has vertex set G and a directed edge from g to gy for all $g \in G$ and $y \in Y$. A DRR for the group G is a Cayley digraph for G whose (directed) automorphism group is isomorphic to G.

We observed this some time after obtaining the above theorem, but there is a simple explanation. Suppose $D(\mathrm{Aut}(G), G) \neq 2$. Then given any generating set Y for G, there must be a non-trivial automorphism leaving Y invariant. Such an automorphism induces an automorphism of the directed graph $C(G, Y)$ leaving the identity vertex fixed, and so $C(G, Y)$ cannot be a DRR for G. Since Y is arbitrary, that means G has no DRR, and therefore is one of Babai's five groups. Unfortunately, there is no obvious implication the other way. For suppose that G has no DRR. Then for any generating set Y, the Cayley digraph $C(G, Y)$ has an automorphism leaving the identity vertex fixed. It is not the case, however, that this digraph automorphism must induce a group automorphism of G; see [11] for a counter-example.

3 Transitive group actions

It is easy to see that if the action of the group A on the set X is *regular* (that is, transitive with trivial point-stabilizers) then $D(A, X) = 2$. For more general transitive actions we have the following:

Theorem 3.1. *Suppose that the finite group A acts faithfully and transitively on the set X (or in other words, A is a transitive permutation group on X). Then either A is regular on X (in which case $m(A) = |X|$), or otherwise*

$$|X| \leq 2\, m(A) \lfloor \log_2 |A_x| \rfloor \quad \textit{for all } x \in X.$$

Proof. Let $n = |X|$ and $s = |A_x|$ (for any $x \in X$). Suppose that $s > 1$ but

$$2m(a) \lfloor \log_2 s \rfloor < n$$

for some non-trivial $a \in A$. Then $m(a) < n/(2\lfloor \log_2 s \rfloor) < n$, so that a has fixed points on X. Without loss of generality, we may suppose that a fixes x. Next let $[a] = \{g^{-1}ag : g \in A\}$ be the conjugacy class of a in A, and let B be the subgroup of A generated by $[a] \cap A_x$. This subgroup contains a and hence is non-trivial. We will show that B is normal in A, and obtain a contradiction.

First observe that B can be generated by a subset C of $[a] \cap A_x$ of size at most $\lfloor \log_2 s \rfloor$: simply begin with the empty set and adjoin elements of $[a] \cap A_x$ one at a time, at each stage at least doubling the size of the subgroup generated. Now all elements of C are conjugate to a and so have motion $m(a)$. Hence the total number of points $y \in X$ moved by at least one element of C is at most $|C| m(a) \leq \lfloor \log_2 s \rfloor m(a) < n/2$, so the subset Y of points of X fixed by all elements of C has size $|Y| > n/2$. In particular, this subset Y is the fixed point set of $B = \langle C \rangle$.

Now let T be a transversal (set of distinct coset representatives) for A_x in A, of size n. Note that over half of the elements of T take x to some point of Y. In particular, if $t \in T$ takes x to $y \in Y$, then for all $c \in C$ we find that $x^t = y = y^c = x^{tc}$, which implies that $tct^{-1} \in A_x$, but also $tct^{-1} \in [a]$ (since $c \in C \subseteq [a]$), therefore $tct^{-1} \in [a] \cap A_x \subseteq B$. Since $\langle C \rangle = B$, it follows that B is normalized by each such t. Thus $B = \langle [a] \cap A_x \rangle$ is normalized by A_x and over half of the elements of the transversal T, so B must be normal in A. Thus A_x contains a non-trivial normal subgroup of A, so the action of A on X is not faithful, contradiction. □

It is important to note that the factor $\lfloor \log_2 s \rfloor$ in the above theorem comes from a very loose bound on the rank of a certain subgroup of A_x. This bound can be improved significantly in some situations, for example as follows.

Corollary 3.2. *Suppose that the group A acts faithfully and transitively on the set X with cyclic point-stabilizers. Then $m(A) \geq |X|/2$.*

Proof. In the proof of Theorem 3.1, the element a generates the subgroup B, when A_x is cyclic. Thus we can replace the factor $\log_2 s$ by 1 in the statement of Theorem 3.1. □

Corollary 3.3. *Suppose that the group A acts faithfully and transitively on the set X with cyclic point-stabilizers. If $|X| > 43$, then $D(A, X) = 2$.*

Proof. Let $n = |X|$. By the previous corollary and the Motion Lemma, we know that $D(A, X) = 2$ whenever $n > 4 \log_2 |A|$. It remains to get a good bound on $|A|$, or equivalently on $|A_x|$. An easy upper bound on the order of a permutation on n symbols is of order $n^{\sqrt{2n}}$ (any such permutation has at most $\sqrt{2n}$ disjoint cycles of different lengths, and each cycle has order at most n). This suffices to show all but finitely many of these actions have distinguishing number two. On the other hand, Lucchini [17] has shown that if the point-stabilizer A_x is cyclic, then $|A_x| \leq n-1$, so $|A| \leq n(n-1) < n^2$. Using this bound, we find that $D(A, X) = 2$ whenever $n > 4 \log_2(n^2) = 8 \log_2 n$. It is easily verified that this is true for all $n \geq 44$ but not for $n \leq 43$. □

One special case is the action of the group of orientation-preserving automorphisms of an orientable map (a 2-cell embedding of a connected graph on an orientable surface). This acts on the vertex set X of the map with cyclic vertex-stabilizers, and in that context, the bound $|X| > 43$ can be replaced by $|X| > 8$; see [20].

Also we have the following general consequence of Theorem 3.1:

Corollary 3.4. *If the group A acts faithfully and transitively on the set X, then $D(A, X) = 2$ whenever the action is regular or $|X| \geq 4 \log_2 |A| \log_2(|A|/|X|)$.*

Proof. Since $|A_x| = |A|/|X|$ for all $x \in X$, the result follows from the proof of Theorem 3.1 and the Motion Lemma. □

Corollary 3.5. *Suppose the group A acts faithfully and transitively on the set X of size n, and $|A| < 2^{\sqrt{n}/2}$. Then $D(A, X) = 2$.*

Proof. Here $\log_2 |A| < \sqrt{n}/2$, so $n > 4(\log_2 |A|)^2 > 4 \log_2 |A| \log_2(|A|/|X|)$. □

In any collection of group actions where the group orders are polynomial in the set orders, all but finitely many of the actions have distinguishing number two:

Corollary 3.6. *For any $r > 0$, let $\mathcal{A}$ be any collection of faithful transitive actions (A, X) with the property that $|A| < |X|^r$ for all but finitely many $(A, X) \in \mathcal{A}$. Then $D(A, X) = 2$ for all but finitely many $(A, X) \in \mathcal{A}$.*

Proof. This follows from the previous corollary since $n^r < \sqrt{2}^{\sqrt{n}}$ for all sufficiently large n. □

Corollary 3.7. *A faithful transitive action of the symmetric group S_n on a set X has distinguishing number two whenever $|X| > 4(n \log_2 n)^2$.*

Proof. Apply Corollary 3.4 with $\log_2 |S_n| = \log_2(n!) \leq \log_2(n^n) = n \log_2 n$. □

A *base* for a group A acting on a set X is a subset Y of X having trivial pointwise stabilizer A_Y. A base Y has the property that the permutation induced by each element of A on X is uniquely determined by its effect on the elements of Y. The *base size* of the action (A, X) is the minimum size of a base for the action.

Corollary 3.8. *For any given positive integer k, all but finitely many faithful transitive group actions with base size k have distinguishing number 2.*

Proof. Suppose that (X, A) has a base Y of size k. Then $|A| \leq |X|^k$, since any element $a \in A$ is determined by the $|X|$ choices for the images y^a of points $y \in Y$. By Corollary 3.6, all but finitely many such actions have distinguishing number 2. □

We note that the results of [20] for maps can also be interpreted in terms of minimum base size: since the vertices forming a corner of a map have trivial pointwise stabilizer, map groups have minimum base size 3.

After obtaining Theorem 3.1, we discovered the following fact, which is given as an exercise in [10, 3.3.7]:

Lemma 3.9. *If A is a transitive permutation group with minimum base size k and minimal degree (motion) $m = m(A)$, then $|X| \leq km$.*

Proof. Let $n = |X|$, and let Y be a base for A of size k. Also let a be any non-trivial element of A, and let U be the support of a (that is, the set of points moved by a). Now count the number of pairs $(b, x) \in A \times U$ such that $x \in Y^b$. For any $b \in A$, we know that Y^b is a base for A, so a moves at least one point in Y^b, and hence the number of such pairs is at least $|A|$. On the other hand, for any $x \in U$, there are exactly $|A_x|$ elements of A taking x to any given point of X, so the number of $b \in A$ for which $x^{b^{-1}} \in Y$ is $|Y||A_x| = k|A|/n$, and hence the number of pairs is $|U|k|A|/n$. Thus $|U|k|A|/n \geq |A|$, which gives $|U| \geq n/k$, and therefore $m = m(A) \geq n/k$. □

We now obtain the following (with thanks to Peter Neumann for suggesting the use of the number-theoretic function λ):

Theorem 3.10. *If A is a transitive permutation group on the finite set X, then*

$$|X| \leq m(A)\,(1 + \lambda(|A|/|X|))$$

where $\lambda(N)$ is the number of prime divisors of N (counted with their multiplicities). In particular,

$$|X| \leq m(A)\,(1 + \log_2(|A|/|X|)).$$

Proof. Let $Y = \{y_1, y_2, \ldots, y_k\}$ be a minimal base for the action, and let $B_i = A_{y_1 \ldots y_i}$ be the subgroup fixing $(y_1, \ldots, y_i)$, for $1 \leq i \leq k$. Then $|B_1| = |A_{y_1}| = |A|/|X|$, and since B_{i+1} is strictly contained in B_i (by the minimality of the base), each index $|B_i : B_{i+1}|$ is a non-trivial divisor of $|B_1| = |A_{y_1}| = |A|/|X|$, so $k - 1 \leq \lambda(|A|/|X|))$. The first bound on $|X|$ now follows from Lemma 3.9, and the second from the fact that $2^{\lambda(N)} \leq N$ for all N. □

This theorem gives stronger inequalities than Theorem 3.1, which has an extra factor of 2. For example, in Corollary 3.5, we can replace the hypothesis $|A| < 2^{\sqrt{n}/2}$ by $|A| < 2^{\sqrt{n/2}}$. Similarly, in Corollary 3.8, we can replace $|X| > 4k^2(\log_2 n)^2$ by $|A| > 2k^2 \log_2 n$. On the other hand, the effective dependence of the proofs of Theorems 3.1 and 3.10 on a generating set for the point-stabilizer allows greater precision in special cases, such as that where A_x is cyclic (see Corollary 3.2). Note also that in Theorem 3.1 we can replace $\lfloor \log_2 |A|/|X| \rfloor$ by $\lambda(|A|/|X|)$, by the same reasoning.

Another approach to 2-distinguishability for transitive actions is via primitivity. It has been shown by Cameron, Neumann and Saxl [7, 6] that all but finitely many primitive permutation groups other than A_n or S_n (in their standard actions) have distinguishing number 2, and the exceptions have been classified by Seress [19]; see also [4]. For imprimitive actions, Chan [9] gives examples of wreath products of groups with large distinguishing numbers; see also [22]. These actions have analogues for graphs that are lexicographic products of a transitive graph G with d independent vertices; the example given at the end of [20] is the case $d = 2$ with G an n-cycle.

The Motion Lemma partly explains such constructions, since having block-size d often implies that the motion is at most d. Hence if one wants to limit such actions, one might bound the number of blocks. For example, one could take blocks of minimal size, so that the action on an individual block is primitive. Then for given r, there are only finitely many wreath products $H \wr K$ where $|K| \leq r$ and H is primitive but $H \neq A_n$ or S_n, with distinguishing number greater than 2. For further discussion of minimum base size and distinguishing number for wreath products, see [4].

4 Intransitive group actions

It is clear that the distinguishing number can be affected by local behavior. For example, given any graph G, if we simply add n vertices all joined to the same vertex of G, then the resulting graph has distinguishing number at least n, no matter what the distinguishing number is for G. Hence for intransitive group actions, we cannot expect the same kind of phenomena that we have for transitive actions.

The following example from [22] illustrates the problem.

Example 4.1. For given positive integers n and k, let $X = \{1, 2, \ldots, n + 2k\}$, and choose any pairing of the $2k$ points $n + 1, n + 2, \ldots, n + 2k$. Define an action of S_n on $X = \{1, 2, \ldots n + 2k\}$ by taking the standard action on $\{1, 2 \ldots, n\}$, and letting all even elements of S_n fix the k given pairs pointwise, and all odd elements of S_n interchange the two points of each pair. This action has distinguishing number n, for all k.

Hence S_n can act (intransitively) on arbitrarily large sets with distinguishing number n. Note that one can always do this by adding singleton orbits, but in the given example, every point is moved by some permutation. The motion of this action is 3, given by a single

3-cycle in S_n (as a single transposition in S_n moves $2 + 2k$ points). Also for any k, the action has the same base size as S_n, namely $n - 1$.

This example can be modified as follows. Let $X \subset \mathbb{R}^3$ consist of the vertices of an equilateral triangle in the xy-plane centered at the origin, together with points $(0, 0, \pm j)$ for integers j in the range $0 < j \leq k$. Let A be the group of Euclidean isometries of $\mathbb{R}^3$ that take X to X. Then $A \cong D_3 \times C_2$, and $D(A, X) = 3$ since A contains a standard D_3 acting on the triangle and leaving the z-axis fixed. Thus there are arbitrarily large finite subsets X in Euclidean 3-space such that $D(A, X) = 3$, where A is the group of Euclidean isometries leaving X invariant. In the Euclidean plane, a regular pentagon together with its center gives a set X of size 6 such that $D(A, X) = 3$ for any group A of isometries leaving X invariant. But this is the largest such set:

Theorem 4.2. *Let X be any finite subset of the Euclidean plane $\mathbb{R}^2$ with $|X| > 6$, and let A be the group of isometries of $\mathbb{R}^2$ leaving X invariant. Then $D(A, X) = 2$.*

Proof. Recall that every isometry is a reflection, rotation, translation, or glide reflection. Since X is finite, all elements of A must be rotations or reflections. If A has 3 reflections in lines not through the same point, then A contains a triangle group with elements of infinite order. If it has rotations a and b around different points, then $aba^{-1}b^{-1}$ is a translation, so A is either a cyclic group generated by a single rotation or a dihedral group D_n generated by a pair of reflections. If A is generated by a rotation about z, then for any $x \in X$ such that $x \neq z$, we find that A_x is trivial, so $D(A, X) = 2$.

Suppose instead that A is isomorphic to D_n and leaves invariant n lines, all of which pass through a central point z. If $x \in X$ does not lie on any of those lines, then A_x is trivial and $D(A, X) = 2$. Hence all points in X lie on those lines. If $n > 6$, then $D(A, X) = 2$ by the original necklace problem, so suppose instead that $n \leq 5$. Since $|X| > 6$, some line L contains two points $x, y \in X$ other than z. If $w \in X$ does not lie on L, then the pointwise stabilizer A_{xyw} is trivial. If instead $X \subset L$ and $x \neq z$, then the only nontrivial element of A_x is the reflection in the line L, which fixes all of X, and again $D(A, X) = 2$. □

Although no analogous result holds in Euclidean 3-space, we might hope that it holds for closed surfaces. On the other hand, it is not difficult to put a set X like that from our 3-space example above, with $n = 3$ and any $k > 1$, onto a surface S of genus $2(k - 1)$ having 3-fold symmetry about the z-axis in such a way that X is invariant under an action of $A = S_3 \times C_2$ on S. Hence there is no single bound for group actions on closed surfaces. Instead, we have the following:

Theorem 4.3. *Let S be closed surface of genus g. There is a number $n(g)$ such that if X is any finite subset of S with $|X| \geq n(g)$ then $D(A, X) = 2$ for any finite group of homeomorphisms of S leaving X invariant.*

Proof. We need only one fact about a closed orientable surface S: the number of fixed points of a non-trivial orientation-preserving automorphism a of finite order is at most $2g + 2$. This follows from elementary consideration of the Riemann-Hurwitz equation [14] applied to the branched covering associated with the cyclic group generated by a. In particular, if a fixes more than $2g+2$ points, then a reverses orientation, and then, since a^2 is orientation-preserving and fixes more than $2g+2$ points, a^2 must be the identity. Moreover, a is a reflection: that is, S is the union of two connected surfaces with boundaries S_1 and

S_2, such that ${S_1}^a = S_2$, and $S_1 \cap S_2$ is a set of disjoint simple closed curves left invariant by a, with at least one of these closed curves fixed by a (see [14]). Elementary calculations with the Euler characteristic show that the number of those simple closed curves is at most $g+1$.

So suppose we are given a set X in a surface S of genus g together with a finite group A of homeomorphisms of S leaving X invariant such that $D(A,X) > 2$. By the Motion Lemma, we must have $m(A) \leq 2\log_2 |A|$. We claim that if $|X|$ is sufficiently large, then some $a \in A$ has motion at most $|X|/4$ and so fixes at least $3/4$ of X. For $g > 1$, we have that $|X| > 8\log_2(168(g-1))$ suffices, since $|A| \leq 168(g-1)$ by the Hurwitz bound; see [14, 6.3.5]. For $g = 1$, point stabilizers of A have order at most 12 by the classification of toroidal groups [14]; thus $|A| \leq 12|X|$, so $|X| > 8\log_2(12|X|)$ suffices. For $g = 0$ (the sphere), we use the classification of spherical groups, which says the only possibilities for A are the subgroups of the automorphism groups of the five Platonic solids and the n-prisms. For the platonic solids, we have $|A| \leq 120$, so $|X| > 8\log_2 120$ suffices. For the prisms, the length of the orbit of any point other than centers of the top or bottom face of the prism is at least $|A|/4$, so $|A| \leq 4|X|$ when $|X| > 2$. In that case, $|X| > 8\log_2(4|X|)$ suffices.

Thus, if $|X|$ is large enough, there is some $a \in A$ with fixed-point set $Y \subseteq X$ such that $|Y| \geq 3|X|/4$.

Let us suppose that $|X| > 8g+8$, so that $|Y| \geq 6g+6$. We claim that $ab = ba$ for every $b \in A$. To see this, consider $Z = Y \cap Y^b$, which is fixed by both a and $b^{-1}ab$. Now $a^{-1}(b^{-1}ab)$ is orientation-preserving and fixes Z. Since $|Y| \geq 3|X|/4$, we have $|Z| \geq |X|/2 \geq 4g+4$, so $a^{-1}b^{-1}ab = 1$ since it fixes more than $2g+2$ points. It then follows for any $b \in A$ and any point $u \in S$ fixed by a that $u^{ba} = u^{ab} = u^b$, so u^b is also fixed by a. In particular, $Y^b = Y$; and moreover, b leaves invariant the set of all points fixed by a on the surface S, not just $Y \subseteq X$.

Since $|Y| \geq 6g+6$, the element a is a reflection, and there is a simple closed curve C left fixed by a and containing at least 6 points of Y. By the previous remarks, any element b stabilizing $C \cap Y$ setwise must leave C invariant. Since $|Y \cap C| \geq 6$, by the original necklace problem there are three points $x, y, z \in C \cap Y$ such that any element b in the setwise stabilizer $A_{\{x,y,z\}}$ fixes C and hence must be a reflection. But then ab preserves orientation and also fixes C, so $ab = 1$. Therefore the only non-identity element of $A_{\{x,y,z\}}$ is a. If w is any point of X not fixed by a, then the setwise stabilizer $A_{\{x,y,z,w\}}$ is trivial, since each of its elements leaves the subset $\{x,y,z\}$ of fixed points of a invariant, so lies in $\langle a \rangle$, but $w^a \neq w$. If instead all points of X are fixed by a, then the only non-identity element of $A_{\{x,y,z\}}$ is a, which fixes all points of X, so $A_{\{x,y,z\}}$ acts trivially on X. In either case, $D(A,X) = 2$. □

The size needed for X is $O(g)$, since for $g > 1$, we have $|A| \leq 168(g-1)$. In the proof, for sufficiently large g we used $|X| > 8(g+1)$. We conjecture that the number is exactly $g+3$, for sufficiently large g; that is, for sufficiently large g there is a set X of $g+3$ points on the surface of genus g with $D(A,X) > 2$, but $D(A,X) = 2$ for all larger sets. The actual number for the sphere or torus should also be possible to calculate.

References

[1] M. Albertson, Distinguishing cartesian powers of graphs, *Electron. J. Combin.* **12** (2005), R#17.

[2] M. Albertson and K. Collins, Symmetry breaking in graphs, *Electron. J. Combin.* **3** (1996), R#18.

[3] L. Babai, Finite digraphs with given regular automorphism groups, *Period. Math. Hungar.* **11** (1980), 257–270.

[4] R. Bailey and P. Cameron, Base size, metric dimension and other invariants of groups and graphs, preprint.

[5] W. Bosma, J. Cannon and C. Playoust, The MAGMA Algebra System I: The User Language, *J. Symbolic Computation* **24** (1997), 235–265.

[6] P. J. Cameron, Regular orbits of permutation groups on the power set, *Discrete Math.* **62** (1986), 307–309.

[7] P. J. Cameron, P. M. Neumann and J. Saxl, On groups with no regular orbits on the set of subsets, *Arch. Math. (Basel)* **43** (1984), 295–296.

[8] M. Chan, The maximum distinguishing number of a group, *Electron. J. Combin.* **13** (2006), R#70.

[9] M. Chan, The distinguishing number of the direct product and wreath product actions, *J. Algebraic Comb.* **24** (2006), 331–345.

[10] J. Dixon and B. Mortimer, *Permutation Groups*, Springer-Verlag, New York, 1996.

[11] B. Elspas and J. Turner, Graphs with circulant adjacency matrices, *J. Combinatorial Theory* **9** (1970), 297–307.

[12] The GAP Group, GAP – Groups, Algorithms and Programming, Version 4.3, 2002, http://www.gap-system.org.

[13] D. Gluck, Trivial set-stabilizers in finite permutation groups, *Canad. J. Math* **35** (1983), 59–67.

[14] J. L. Gross and T. W. Tucker, *Topological Graph Theory*, Wiley-Interscience, New York, 1987, (Dover paperback 2001).

[15] M. Imrich and S. Klavžar, Distinguishing cartesian powers of graphs, *J. Graph Theory* **53** (2006), 250–260.

[16] S. Klavžar, T.-L. Wong and X. Zhu, Distinguishing labelings of group action on vector spaces and graphs, *J. Algebra* **303** (2006), 626–641.

[17] A. Lucchini, On the order of transitive permutation groups with cyclic point-stabilizer, *Rend. Mat. Acc. Lincei* **9** (1998), 241–243.

[18] A. Russell and R. Sundaram, A note on the asymptotics and computational complexity of graph distinguishability, *Electron. J. Combin.* **5** (1998), R#23.

[19] A. Seress, Primitive permutation groups with no regular orbits on the set of subsets, *Bull. London Math. Soc.* **29** (1997), 697–709.

[20] T. W. Tucker, Distinguishing maps, *Electron. J. Combin.*, to appear.

[21] J. Tymoczko, Distinguishing numbers for graphs and groups, *Electron. J. Combin.* **11** (2004), R#63.

[22] T.-L. Wong and X. Zhu, Distinguishing labeling of group actions, *Discrete Math.* **309** (2009), 1760–1765.