On the single-orbit conjecture for uncoverings-by-bases

Robert F. Bailey*
School of Mathematics and Statistics
Carleton University
1125 Colonel By Drive
Ottawa, Ontario K1S 5B6
Canada

Peter J. Cameron†
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London E1 4NS
United Kingdom

December 3, 2007

Abstract

Let G be a permutation group acting on a finite set Ω. An *uncovering-by-bases* (or UBB) for G is a set $\mathcal{U}$ of bases for G such that any r-subset of Ω is disjoint from at least one base in $\mathcal{U}$, where $r = \lfloor \frac{d-1}{2} \rfloor$, for d the minimum degree of G. The *single-orbit conjecture* asserts that for any finite permutation group G, there exists a UBB for G contained in a single orbit of G on its irredundant bases. We prove a case of this conjecture, for when G is k-transitive and has a base of size $k+1$. Furthermore, in the more restricted case when G is primitive and has a base of size 2, we show how to construct a UBB of minimum possible size.

Keywords: permutation group, base, orbit, uncovering-by-bases.

MSC2000 classification: 20B20 (primary), 05B40, 05C25 (secondary).

*Corresponding author. E-mail robertb@math.carleton.ca
†E-mail p.j.cameron@qmul.ac.uk

1 Introduction

Let G be a permutation group acting on a finite set Ω. A *base* for G is a sequence of points $(a_1,\ldots,a_m)$ chosen from Ω whose pointwise stabiliser is trivial. A base is *irredundant* if, for each i, the stabiliser of $(a_1,\ldots,a_{i-1})$ does not fix a_i. An *uncovering-by-bases* is a set $\mathcal{U}$ of bases for G in this action such that any r-subset of Ω is disjoint from at least one base in $\mathcal{U}$, where r is defined as follows. Suppose G has minimum degree d (i.e. the least number of points moved by a non-identity element is d), then $r = \lfloor \frac{d-1}{2} \rfloor$.

Uncoverings-by-bases were introduced by the first author [1, 2] as part of a decoding algorithm for error-correcting codes based on permutation groups, where the codewords are permutations written in list form. The parameter r is called the *correction capability* of G, as it is the number of errors that can be corrected by G when viewed as a code in this way. A straightforward contradiction argument shows that an uncovering-by-bases will always exist for any finite permutation group.

Clearly, G acts on its bases, and we note that the image of an irredundant base is also irredundant. Also in [1, 2], the following conjecture is made.

Conjecture. *Let G be a finite permutation group. Then there exists an uncovering-by-bases for G contained in a single orbit of G on its irredundant bases.*

We say that G has the *single-orbit property* if it satisfies the conjecture. This property is not unmotivated; as well as being of theoretical interest, it has implications for the complexity of the decoding algorithm mentioned above (see [1, 2] for details of this).

2 The main theorem

Our main theorem is as follows.

Theorem 1. *Let G be a finite permutation group which is k-transitive and has an irredundant base $(a_1,a_2,\ldots,a_{k+1})$ of size $k+1$. Then G has an uncovering-by-bases contained within a single orbit on its irredundant bases, namely $(a_1,a_2,\ldots,a_{k+1})^G$.*

The main tool in our proof is the following result, due to Birch, Burns, Macdonald and Neumann in 1976 [3].

Theorem 2. *Let G be a permutation group acting on a set Ω. Let Δ,Γ be subsets of Ω with $|\Delta| = m$, $|\Gamma| = n$. If G has an orbit on Ω of size strictly larger than mn, then there exists $g \in G$ such that $\Delta^g \cap \Gamma = \varnothing$.*

Note that if G is transitive, then Theorem 2 implies that such an element g will exist if $|\Omega| > |\Delta|.|\Gamma|$.

Proof of Theorem 1. To show that an uncovering-by-bases exists inside the given orbit, we show that for an arbitrary r-subset of Ω, there is an orbit representative disjoint from it. Throughout, n denotes the degree of G.

We proceed by induction on k. The case $k = 1$ corresponds to transitive groups with an irredundant base of size 2. Since the stabiliser of a point is not trivial, there exist elements with fixed points, and so the minimum degree of such a group is at most $n-1$. (This bound is sharp, as it is achieved by Frobenius groups.) Consequently, the correction capability is at most $r_{\max} = \lfloor \frac{n-2}{2} \rfloor$.

We are given an irredundant base (a_1, a_2) for G. We observe that (a_2, a_1) is also an irredundant base (as G is not regular), so we can regard the base as a set, $\{a_1, a_2\}$. We want our uncovering-by-bases to be contained in the orbit on this base. Let R be an arbitrary $r_{\max}$-subset of Ω. We want to find an element $g \in G$ such that $R \cap \{a_1, a_2\}^g = \varnothing$. Because R has size $\lfloor \frac{n-2}{2} \rfloor$, $\{a_1, a_2\}$ size 2, and $2\lfloor \frac{n-2}{2} \rfloor < n$, since G is transitive we can appeal to Theorem 2 to show that a suitable element $g \in G$ exists.

Now, for the induction hypothesis we assume $k \geq 2$ and that a $(k-1)$-transitive group of degree m with a base of size k satisfies the conditions of the theorem.

Let G (of degree n) be k-transitive and have an irredundant base of size $(k+1)$. Let $(a_1, \ldots, a_{k+1})$ be such a base, and choose an arbitrary r-subset $S \subseteq \Omega$, where r is the correction capability of G. If our chosen base is already disjoint from S, then we are done. So suppose not. Without loss of generality, we may assume $a_{k+1} \in S$. Since G is transitive, there exists an element $h_1 \in G$ such that $a_{k+1}^{h_1} = b_{k+1} \in \Omega \setminus S$. We obtain a new base $(b_1, \ldots, b_{k+1}) = (a_1, \ldots, a_{k+1})^{h_1}$. Now consider $H = G_{b_{k+1}}$ acting on $\Omega \setminus \{b_{k+1}\}$. Clearly, H is $(k-1)$-transitive, has degree $n-1$ and an irredundant base of size k, namely $(b_1, \ldots, b_k)$.

As the degree and maximum number of fixed points of H are both one less than those of G, their minimum degrees (and hence their correction capabilities) are equal. So, by the induction hypothesis, there exists $h_2 \in H$ such that $S \cap \{b_1, \ldots, b_k\}^{h_2} = \varnothing$. Thus $S \cap (a_1, \ldots, a_{k+1})^{h_1 h_2} = \varnothing$, and so by taking $g = h_1 h_2$ we have the element $g \in G$ we require.

Hence, by induction, the result holds for all k. □

3 Constructing optimal uncoverings-by-bases

In the case where G is primitive and has an irredundant base of size 2, then we can prove a stronger result, in that not only can we show that such an uncovering-by-bases exists but that we can construct one of optimal size.

Clearly, the smallest possible size of an uncovering-by-bases for G is $r+1$, as otherwise we could have an r-set which meets every base. This can be achieved if there are $r+1$ disjoint bases for G. If G has degree n, then since $r+1 \leq \lfloor \frac{n-2}{2} \rfloor + 1 = \lfloor \frac{n}{2} \rfloor$, this is feasible. In Theorem 4, we give a construction to show that if G is primitive then this is possible.

Our construction uses graph-theoretic techniques. Recall that a *matching* in a

graph Γ is a set of disjoint edges of Γ, and that a *perfect matching* (or 1-*factor*) is a matching that covers every vertex of Γ. Clearly, a perfect matching requires the number of vertices to be even; if the number of vertices is odd, we define a *near-perfect matching* to be a matching which covers all but one vertex. Recall also that Γ is *vertex-transitive* if its automorphism group acts transitively on its vertices.

The following result can be found in Godsil and Royle [8], Section 3.5.

Lemma 3. *Let $\Gamma = (V,E)$ be a connected, vertex-transitive graph. Then Γ has either a perfect matching or a near-perfect matching, depending on the parity of $|V|$.*

We now have the tools necessary to prove the following:

Theorem 4. *Let G be a finite, primitive permutation group acting on a set Ω of size n, with an irredundant base of size 2 and correction capability r. Then G has an uncovering-by-bases of size $r+1$ contained within a single orbit on its irredundant bases.*

Proof. We want to show that there exist $r+1$ disjoint bases for G, contained in a single orbit. Choose a base (a_1,a_2) for G, and let $A = \{(a_1^g, a_2^g) : g \in G\}$ be the orbit containing (a_1,a_2). Now, form a graph Γ whose vertex set is Ω and $\{u,v\}$ is an edge if and only if $(u,v) \in A$. (Note that $(u,v) \in A$ if and only if $(v,u) \in A$ since G is not regular, so this defines an undirected graph.) Clearly $G \leq \mathrm{Aut}(\Gamma)$, and by construction G acts vertex-transitively on Γ. Since Γ is an special case of an orbital graph for G, we call Γ a *base-orbital graph* for G.

It is straightforward to show that the connected components of Γ form a system of imprimitivity for G. However, since G is primitive and by construction Γ has non-empty edge set, Γ must have only one connected component.

Now, if n is even we have $r+1 \leq \frac{n}{2}$, while if n is odd, we have $r+1 \leq \frac{n-1}{2}$. So the existence of $r+1$ disjoint bases in A is implied by the existence of a (near-) perfect matching in Γ. By Lemma 3, since Γ is connected and vertex-transitive, one exists, and so we are done. □

If we were to change the hypothesis so as to consider imprimitive groups (with an irredundant base of size 2), the situation is less clear. However, all we need to replicate the proof of Theorem 4 is for there to be a base-orbital graph which has a (near-) perfect matching. One way that this can be achieved is if each connected component has an even number of vertices, as each component will have a perfect matching and so the whole graph does. If the degree of G is a power of 2, then this is guaranteed.

For other degrees, the situation is more complicated. First, depending on the choice of base, the graph may or may not be connected. For instance, consider the dihedral group of order 12, acting on the vertices of a hexagon: any two non-antipodal vertices form a base, but the only base-orbital graph which is connected is that formed from the orbit on adjacent vertices.

However, we only need *one* base-orbital graph to be connected in order to find a (near-) perfect matching. An infinite family of imprimitive groups for which such a graph exists is given by the following result.

Proposition 5. *For the group* $\mathrm{SL}(2,q)$ *acting on the non-zero vectors of* $\mathbb{F}_q^2$*, the base-orbital graph containing the standard basis* $\{(1,0),(0,1)\}$ *is connected.*

Proof. We show that an arbitrary non-zero vector $(i,j) \in \mathbb{F}_q^2$ is connected by a path to the vector $(1,1)$. Starting from (i,j), we construct a path, where each edge $\{u,v\}$ is the image of $\{(1,0),(0,1)\}$ under the unimodular transformation given by the matrix M.

For $i \neq 0$, we have the following matrices:

$$\begin{aligned}
\{(i,j),(0,i^{-1})\}: &\quad M = \begin{pmatrix} i & 0 \\ j & i^{-1} \end{pmatrix} \\
\{(0,i^{-1}),(i,i+1)\}: &\quad M = \begin{pmatrix} i & 0 \\ i+1 & i^{-1} \end{pmatrix} \\
\{(i,i+1),(1,1)\}: &\quad M = \begin{pmatrix} 1 & i \\ 1 & i+1 \end{pmatrix},
\end{aligned}$$

while for $i = 0$, we have:

$$\begin{aligned}
\{(0,j),(j^{-1},j^{-1}+1)\}: &\quad M = \begin{pmatrix} j^{-1} & 0 \\ j^{-1}+1 & j \end{pmatrix} \\
\{(j^{-1},j^{-1}+1),(1,1)\}: &\quad M = \begin{pmatrix} 1 & j^{-1} \\ 1 & j^{-1}+1 \end{pmatrix}.
\end{aligned}$$

□

In some other cases, we are not so lucky: there are also instances of groups for which none of the base-orbital graphs are connected.

Proposition 6. *For the Frobenius group* $G = q^2 : q-1$ *acting on* q^2 *points, no base-orbital graph is connected.*

Proof. Although the base-2 action of this group arises from the fact that it is a subgroup of the sharply 2-transitive group $\mathrm{AGL}(1,q^2)$, it is easier to understand this action by viewing it as a subgroup of $\mathrm{AGL}(2,q)$, acting on the vector space $\mathbb{F}_q^2$. Now, as G is a Frobenius group, any two points form a base, and so any orbital graph is a base-orbital graph. Also, the structure of G is as follows:

$$G = \left\{ \mathbf{x} \mapsto a\mathbf{x} + \mathbf{b} \,:\, a \in \mathbb{F}_q^*, \mathbf{b} \in \mathbb{F}_q^2 \right\}.$$

Thus the orbit of G on a base $\{\mathbf{x},\mathbf{y}\}$ is the set

$$\left\{ \{a\mathbf{x}+\mathbf{b}, a\mathbf{y}+\mathbf{b}\} \,:\, a \in \mathbb{F}_q^*, \mathbf{b} \in \mathbb{F}_q^2 \right\},$$

i.e. the line l spanned by $\mathbf{x}$ and $\mathbf{y}$ together with all its cosets. Thus, in the corresponding orbital graph, a vertex (i.e. vector) $\mathbf{v}$ is adjacent to the $q-1$ other vectors on the line through $\mathbf{v}$ parallel to l, and no others. Consequently, the orbital graph consists of q disjoint copies of a complete graph K_q, and is not connected. □

4 Discussion

We conclude by discussing which families of groups our theorems can be applied to.

The class of groups where we can apply Theorem 1 includes the following. An *IBIS group* is a group where all of the irredundant bases have the same size (see Cameron and Fon-Der-Flaass [6]); the *rank* of an IBIS group is the size of an irredundant base. (The acronym is short for *Irredundant Bases of Invariant Size*.) The IBIS groups of rank $k > 1$ for which *any* k-tuple forms an irredundant base were determined in [6]: these are the Frobenius groups (rank 2), Zassenhaus groups (rank 3), a family of rank 4 groups determined by Gorenstein and Hughes [9], and then only the sharply k-transitive groups for higher ranks. All of these groups are $(k-1)$-transitive and have an irredundant base of size k, so are covered by our result.

In addition to these IBIS groups, for base sizes larger than 2 there are very few other examples. We can appeal to the classification of 2-transitive groups (which follows from the classification of finite simple groups) which is quite restrictive. However, this class of groups does contain some interesting examples, such as the action of the Mathieu group M_{11} on 12 points (which is 3-transitive and has a base of size 4), and its point stabiliser $\mathrm{L}_2(11)$ acting on 11 points (2-transitive with a base of size 3).

Theorem 4 is obviously much more specific, referring to groups which are primitive and have a base of size 2. However, recent work of Burness, Guralnick and Saxl [4], Burness, O'Brien and Wilson [5], and James [10, 11], suggests that, in a meaningful sense, "most" almost simple primitive permutation groups admit a base of size two. This study was initiated by Kantor and the second author [7], who considered actions of symmetric and alternating groups. They showed that if G is such a group with socle A_m for some m, and if the point-stabiliser G_α acts primitively on $\{1,\ldots,m\}$, then G has a base of size two if m is sufficiently large. This is extended in [4], where it is shown that $m > 12$ suffices. Consequently, our construction can be applied to a fairly wide range of groups.

References

[1] R. F. Bailey, Permutation groups, error-correcting codes and uncoverings, Ph.D. thesis, University of London, 2006.

[2] R. F. Bailey, Error-correcting codes from permutation groups, submitted.

[3] B. J. Birch, R. G. Burns, S. Oates Macdonald and P. M. Neumann, On the orbit-sizes of permutation groups containing elements separating finite subsets, *Bull. Austral. Math. Soc.* **14** (1976), 7–10.

[4] T. C. Burness, R. M. Guralnick and J. Saxl, Base sizes for simple groups, in preparation.

[5] T. C. Burness, E. A. O'Brien and R. A. Wilson, Base sizes for sporadic groups, submitted.

[6] P. J. Cameron and D. G. Fon-Der-Flaass, Bases for permutation groups and matroids, *Europ. J. Combin.* **16** (1995), 537–544.

[7] P. J. Cameron and W. M. Kantor, Random permutations: Some group-theoretic aspects, *Combin. Probab. Comput.* **2** (1993), 257–262.

[8] C. D. Godsil and G. F. Royle, *Algebraic Graph Theory*, Graduate Texts in Mathematics (207), Springer-Verlag, New York, 2001.

[9] D. Gorenstein and D. R. Hughes, Triply transitive groups in which only the identity fixes four letters, *Illinois J. Math* **5** (1961), 486–491.

[10] J. P. James, Two point stabilisers of partition actions of linear groups, *J. Algebra* **297** (2006), 453–469.

[11] J. P. James, Partition actions of symmetric groups and regular bipartite graphs, *Bull. London Math. Soc.* **38** (2006), 224–232.