Uncoverings-by-bases for base-transitive permutation groups

Robert F. Bailey
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road, London E1 4NS
United Kingdom
r.f.bailey@qmul.ac.uk

June 23, 2006

Abstract

An *uncovering-by-bases* for a group G acting on a finite set Ω 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 is a parameter dependent on G. They have applications in the decoding of permutation groups when used as error-correcting codes, and are closely related to covering designs.

We give constructions for uncoverings-by-bases for many families of base-transitive group (i.e. groups which act transitively on their irredundant bases), including a general construction which works for any base-transitive group with base size 2, and some more specific constructions for other groups. In particular, those for the groups $\mathrm{GL}(3,q)$ and $\mathrm{AGL}(2,q)$ make use of the theory of finite fields.

We also describe how the concept of uncovering-by-bases can be generalised to matroid theory, with only minor modifications, and give an example of this.

Keywords: Covering design, permutation group, bases, decoding

AMS classification: 05B40, 20B20, 94B35 (primary), 11T30, 05B30 (secondary)

1 Introduction

The concept of an *uncovering-by-bases* was introduced by the author in his Ph.D. thesis [1] (and is also explained in the author's paper [2]). The motivation for this was the use of permutation groups as error-correcting codes (where permutations written in list form are the codewords), which makes heavy use of them in a decoding algorithm. The results in sections 1 to 6 of this article are also taken from the author's Ph.D. thesis [1].

1.1 Uncoverings-by-bases

In [2] the author gives the following definition.

Definition 1.1. Let $n > k$ and $r \leq n-k$. An (n,k,r)-*uncovering* is a set $\mathcal{U}$ of k-subsets of $\Omega = \{1,\dots,n\}$ such that any r-subset of Ω is disjoint from at least one k-subset in $\mathcal{U}$.

An (n,k,r)-uncovering is equivalent to an $(n,n-k,r)$ *covering design*, which is a set of $(n-k)$-subsets, called blocks, such that any r-subset is contained in at least one block. Because of this, we call the k-subsets in an uncovering *coblocks*. Covering designs are well-studied (see, for example, the survey paper by Mills and Mullin [24]). In this article, we are interested in a particular specialisation. In order to explain this, we need some group theory.

Definition 1.2. Let G be a group acting on Ω. A *base* for G in this action is a sequence of points $(x_1,\dots,x_b)$ chosen from Ω such that the pointwise stabiliser $G_{(x_1,\dots,x_b)}$ of this sequence in G is trivial. An *irredundant* base is a base where $G_{(x_1,\dots,x_i,x_{i+1})} \neq G_{(x_1,\dots,x_i)}$ for $i = 1,\dots,b-1$.

For instance, if G is *sharply k-transitive* (i.e. given two k-tuples of distinct elements of Ω, there exists a unique $g \in G$ mapping one to the other), any k-tuple of points form an irredundant base.

Now let $r = \lfloor \frac{d-1}{2} \rfloor$, where

$$d = n - \max_{\substack{g \in G \\ g \neq 1}} |\mathrm{Fix}(g)|,$$

and $\mathrm{Fix}(g)$ denotes the set of fixed points of g. So d is the *minimum degree* of G, which is also the minimum Hamming distance of G when regarded as a code. Because of the application in coding theory, we call r the *correction capability* of G.

The specialisation we need is as follows.

Definition 1.3. Let G be a group acting on Ω. An *uncovering-by-bases* for G in this action is a set $\mathcal{U}$ of bases for G such that any r-subset of Ω is disjoint from at least one base, where r is as above.

Although not immediately obvious, it is quite easy to show that for a given action of a given group an uncovering-by-bases exists (see [2]). In the case where G is sharply k-transitive, any k-tuple of points form a base, so all that is required is an (n,k,r)-uncovering.

A general approach to the construction of uncoverings-by-bases (which we use in this article) is to first obtain an uncovering (or, equivalently, a covering design) and then to arrange the set Ω so that each coblock forms a base for the action of G on Ω.

1.2 Base-transitive groups

An obvious starting point for the construction of uncoverings-by-bases are groups where all irredundant bases have the same form.

Definition 1.4. A group G acting on Ω is said to be *base-transitive* if it acts transitively on its irredundant bases. The *rank* of a base-transitive group is the size of an irredundant base for G.

Because a base-transitive group of rank 1 is precisely a regular permutation group, we only consider groups of rank at least 2.

Example 1.5. Suppose G is sharply k-transitive of degree n. Then G is base-transitive of rank k.

Example 1.6. Let G be the general linear group $\mathrm{GL}(n,q)$ acting on $\mathbb{F}_q^n \setminus \{0\}$. Then any basis for $\mathbb{F}_q^n$ forms an irredundant base for G, and so G is base-transitive of rank n.

The *type* of a base-transitive group G encodes information about the numbers of fixed points of G.

Definition 1.7. Let G be a base-transitive group of degree n and rank k, and let $(x_1,\ldots,x_k)$ be an irredundant base for G. Then the *type* of G is the pair

$$(\{l_0,l_1,\ldots,l_{k-1}\},n),$$

where l_0 is the number of fixed points of G, and l_i is the number of fixed points of $G_{(x_1,\ldots,x_i)}$ for $1 \leq i \leq k-1$.

Since l_{k-1} is the maximum number of fixed points of a non-identity element, we can therefore obtain the correction capability of G from its type.

As base-transitive groups generalise sharply k-transitive groups, the classification of the former contains the classification of the latter. This latter classification is due to Jordan (1873) [19] for $k \geq 4$, and Zassenhaus (1936) [27, 28] for $k = 2$ and 3. A sharply k-transitive group must be one of the following.

$k \geq 6$: S_k, S_{k+1} and A_{k+2} only.

$k = 5$: S_5, S_6, A_7 and the Mathieu group M_{12}.

$k = 4$: S_4, S_5, A_6 and the Mathieu group M_{11}.

$k=3$: The group

$$\mathrm{PGL}(2,q)=\left\{\tau : x\mapsto \frac{ax+b}{cx+d}\;\middle|\; a,b,c,d\in\mathbb{F}_q, ad-bc\neq 0\right\}$$

acting on the projective line $\mathbb{F}_q\cup\{\infty\}$ (which includes $S_3\cong\mathrm{PGL}(2,2)$, $S_4\cong\mathrm{PGL}(2,3)$ and $A_5\cong\mathrm{PGL}(2,4)$), plus an additional infinite family as described by Cameron [5], page 16.

$k=2$: The group

$$\mathrm{AGL}(1,F)=\{\tau : x\mapsto ax+b \mid a,b\in F, a\neq 0\}$$

where F is a finite near-field, acting on F. In the case where $F=\mathbb{F}_q$, we use the notation $\mathrm{AGL}(1,q)$. Note that $\mathrm{AGL}(1,2)\cong S_2$, $\mathrm{AGL}(1,3)\cong S_3$ and $\mathrm{AGL}(1,4)\cong A_4$.

A *near-field* is an object which satisfies all of the axioms of a field, with the exception of the commutativity of multiplication and a left distributive law. So any field is a near-field, and there is also an additional infinite family of finite near-fields plus seven “exceptional” examples. All have prime-power order, and are described by Cameron [5], page 16. A detailed account of the proof of this classification is given by Dixon and Mortimer [14], section 7.6.

In the literature, base-transitive groups are often called *geometric groups*; see section 7 for the reason behind this alternative name.

2 Classification of base-transitive groups

In this section, we give an overview of the classification of base-transitive groups. Such a group falls into one of the following cases:

- “generic” examples for arbitrary rank;
- infinite families for ranks 2 and 3;
- “sporadic” examples of rank ≤ 5.

In order to describe the classification in detail, we require the important notion of a “blow-up”, which is as follows.

Definition 2.1. Let G be a base-transitive group of rank k and type (L,n). Then a *blow-up* of G is a base-transitive group $\hat{G}$ of rank k and type (mL,mn) (where $mL=\{ml\mid l\in L\}$), such that:

(i) $\hat{G}$ has a normal subgroup N which has n orbits of size m,

(ii) $\hat{G}/N\cong G$,

(iii) $\hat{G}$ induces the given action of G on the N-orbits.

From the third property, it follows that a base for $\hat{G}$ consists of k points chosen from k "independent" N-orbits, i.e. from orbits which form a base for the action of G induced on them.

The symmetric group S_n is something of an anomaly here, as although it has rank $n-1$ and type $(\{0,1,\ldots,n-2\},n)$, when it comes to constructing blow-ups, it behaves as if it also has an action of rank n and type $(\{0,1,\ldots,n-1\},n)$. (This is because it is both sharply $(n-1)$-transitive and sharply n-transitive.) We see this in the following example.

Example 2.2. Consider the entry (iii) in the list of "generic" base-transitive groups. Here we have $G=S_n$ and $\hat{G}=H\wr S_n$, where H is a regular group of order m. Since $H\wr S_n$ has the form $H^n\rtimes S_n$, we take $K=H^n$ (the direct product of n copies of H). So K has n orbits of size m, $\hat{G}/K\cong S_n$, and $\hat{G}$ induces the usual action of S_n on these orbits.

The classification proceedes as follows. There "generic" examples are:

(i) S_n, which has rank $n-1$ and type $(\{0,1,\ldots,n-2\},n)$;

(ii) A_n, rank $n-2$, type $(\{0,1,\ldots,n-3\},n)$;

(iii) $G=H\wr S_n$, where H is a regular group of degree m, so G has rank n and type $(\{0,m,\ldots,(n-1)m\},nm)$ (as in Example 2.2);

(iv) the semidirect product $G=X\rtimes S_n$, for $X=\{(a_1,\ldots,a_n)\in A^n \mid a_1+\cdots+a_n=0\}$ where A is an abelian, regular group of degree m (written additively), so G has rank $n-1$ and type $(\{0,m,\ldots,(n-2)m\},nm)$ (this is a blow-up of S_n in its action of rank $n-1$);

(v) $\mathrm{GL}(n,q)$ acting on $\mathbb{F}_q^n\setminus\{0\}$, which has rank n and type $(\{0,q-1,q^2-1,\ldots,q^{n-1}-1\},q^n-1)$ (i.e. the general linear group in its natural action);

(vi) the stabiliser in $\mathrm{GL}(n,q)$ of d independent vectors $v_1,\ldots,v_d$, where $0<d<n$, acting on $\mathbb{F}_q^n\setminus\langle v_1,\ldots,v_n\rangle$, which has rank $n-d$ and type $(\{0,(q-1)q^d,\ldots,(q^{n-d-1}-1)q^d\},(q^{n-d}-1)q^d)$ (this is a blow-up of $\mathrm{GL}(n-d,q)$);

(vii) $\mathrm{AGL}(n,q)$ acting on $\mathbb{F}_q^n$, which has rank $n+1$ and type $\{0,1,q,q^2,\ldots,q^{n-1}\},q^n)$ (i.e. the affine general linear group in its natural action);

(viii) the group $V\rtimes H$, where V is the additive group of $\mathbb{F}_q^n$ and H is the group in (vi), this has rank $n-d+1$ and type $(\{0,q^d,q^{d+1},\ldots,q^{n-1}\},q^n)$ (this is a blow-up of $\mathrm{AGL}(n-d,q)$).

Zil'ber [29] showed that for rank at least 7, there are only "generic" examples. The classification for ranks 2 to 6 is due to Maund [22]: we summarise her result below. In addition to the appropriate "generic" examples, we have the following groups.

–Rank 2

- The sharply 2-transitive groups, which have type $(\{0,1\},n)$ (where n is a prime power);
- $C_{(q-1)/2} \times \mathrm{PSL}(2,q)$ for $q \equiv 3 \mod 4$, of type $(\{0, \frac{q-1}{2}\}, \frac{(q^2-1)}{2})$;
- $C_{q-1} \times \mathrm{Sz}(q)$, type $(\{0,q-1\},(q-1)(q^2+1))$ (where q is an odd power of 2);
- $\mathrm{PSL}(3,2)$, type $(\{0,2\},14)$;
- $\mathrm{PSL}(3,3)$, type $(\{0,6\},78)$.

In the second and third case, the action is the Caresian product of the regular action of the cyclic factor with the natural 2-transitive action of the other factor. The fourth case arises as the point stabiliser of the degree 15 action of A_7, listed below. In the fifth case, the stabiliser of a point is the subgroup fixing a line in the projective plane of order 3 and inducing the regular Klein group on it.

–Rank 3

- $\mathrm{PGL}(2,q)$ and the other sharply 3-transitive groups, type $(\{0,1,2\},q+1)$;
- blow-ups of $\mathrm{PGL}(2,q)$, type $(\{0,q^d,2q^d\},q^d(q+1))$ (these are difficult to describe: see section 5.2);
- A_7 acting on $\mathbb{F}_2^4 \setminus \{0\}$, type $(\{0,1,3\},15)$;
- $V \rtimes K$, where V is the additive group of $\mathbb{F}_2^4$ and K is the point-stabiliser of A_7 in the above action, type $(\{0,2,4\},16)$.

–Ranks 4, 5 and 6

- $V \rtimes A_7$ (where V is as above), rank 4, type $(\{0,1,2,4\},16)$;
- M_{11}, rank 4, type $(\{0,1,2,3\},11)$;
- M_{12}, rank 5, type $(\{0,1,2,3,4\},12)$.

Unlike Zil'ber's, Maund's proof uses the classification of finite simple groups. It involves first classifying the base-transitive groups of rank 2 (by using the classification of 2-transitive groups), and then using induction to analyse the higher ranks. Unfortunately, neither Maund's nor Zil'ber's work has ever been published in a particularly accessible form: Cameron [4] contains a brief survey.

3 Infinite families of arbitrary rank

In this section, we consider some of the list of "generic" groups and construct uncoverings-by-bases. We are able to do this in general for entries (i) to (iv) (the symmetric and alternating groups, and blow-ups of S_n). The general linear group and related groups have proved more challenging, and we do not have a general construction. Rank 2 examples are, however, covered by the general construction in section 4, while the rank 3 groups $\mathrm{GL}(3,q)$ and $\mathrm{AGL}(2,q)$ are considered in detail in section 5. Constructing uncoverings-by-bases for these groups in general remains open.

3.1 Symmetric and alternating groups

The symmetric group S_n, in its usual action on n points, is both sharply n and $(n-1)$-transitive. Thus the minimum degree of S_n is $n-(n-1)+1=2$, and so its correction capability is 0. Hence it is useless as an error-correcting code, but the definition of uncovering-by-bases still holds vacuously; all we need is a single base, so any $(n-1)$-subset will do.

The alternating group, in its usual action on n points, is sharply $(n-2)$-transitive, so has minimum degree $n-(n-2)+1=3$, and hence correction capability 1. So for each n we require an $(n,n-2,1)$-uncovering.

Construction 3.1. We need a set of $(n-2)$-subsets of $\{1,\dots,n\}$ with the property that every point lies outside of one of the subsets. Alternatively, we need an $(n,2,1)$ covering design. If n is even, then we can take $\frac{1}{2}n$ disjoint pairs, and we are done. If n is odd, then we take $\frac{1}{2}(n-1)$ disjoint pairs, then a pair which contains the remaining point and any other point. Then to obtain an $(n,n-2,1)$-uncovering, we take the complement of each pair.

Example 3.2. For the alternating group A_7, we need a $(7,5,1)$-uncovering. Using the construction above, we obtain:

3	4	5	6	7
1	2	5	6	7
1	2	3	4	7
2	3	4	5	6

In section 6 we consider A_7 in another action.

3.2 Wreath products of regular groups

We now consider the entry (iii) on the list of "generic" base-transitive groups (and discussed in Example 2.2). Let H be a regular permutation group of order m, and consider $G = H \wr S_n$ in its imprimitive action on a set Ω of nm points. For convenience, we think of Ω as a rectangle of n columns each of m rows. G acts on the columns of Ω as S_n, and the kernel of this action (i.e. the group fixing all the columns) is H^n.

We call a set of n points, one chosen from each column of Ω, a *transversal* of Ω. It is clear to see that a transversal forms an irredundant base and that G acts transitively on the set of all transversals.

It is also clear that fixed points of elements of G occur in multiples of m, so the maximum number of fixed points a non-identity element can have is $(n-1)m$. This number is realised by elements of the kernel H^n which fix all points in all but one column. Consequently, the minimum degree of G is $nm-(n-1)m = m$, and so the correction capability of $G = H \wr S_n$ is $r = \lfloor \frac{m-1}{2} \rfloor$. Thus it remains to construct an uncovering-by-bases for this group, which is a straightforward task.

Proposition 3.3. *A set of $r+1$ disjoint transversals of Ω forms an uncovering-by-bases for G.*

Proof. For simplicity, we take the first $r+1$ rows of Ω to be our disjoint transversals. Now, if there are r errors, these could be spread across many columns, but can appear in at most r different rows. Thus at least one of the $r+1$ transversals must avoid the error positions. □

A similar technique is required for the related family of groups described in the next section.

3.3 Zero-sum subgroups

In this section, we consider entry (iv) on the list of "generic" groups. These are also examples of blow-ups of S_n, in its base-transitive action of rank $n-1$ and type $(\{0,1,\ldots,n-2\},n)$. Let A be a finite abelian group of order m, written additively. Define $X \leq A^n$ by $X = \{(a_1,a_2,\ldots,a_n) \mid a_1+a_2+\cdots+a_n = 0\}$, and consider the semidirect product $G = X \rtimes S_n$, where the action of S_n on X is by permuting the co-ordinates of elements of X. We refer to G as the *zero-sum subgroup* of $A \wr S_n$. As a permutation group this has degree mn, where an element $(a_1,a_2,\ldots,a_n) \in X$ acts by componentwise addition.

A set of $n-1$ points, each chosen from a different copy of A, forms an irredundant base for G; we call such a base a *partial transversal* of A^n. It can easily be shown that G acts transitively on the set of all partial transversals, so G is base-transitive. As with the group in the previous section, fixed points must occur in multiples of m. However, this time the maximum number of fixed points of a non-identity element is $(n-2)m$, as an element with $(n-1)m$ fixed points would not have the "zero-sum" property, while a transposition in S_n induces a permutation with $(n-2)m$ fixed points. Consequently the minimum degree of G is $nm-(n-2)m = 2m$, and so the correction capability is $r = \lfloor \frac{2m-1}{2} \rfloor = m-1$. Knowledge of this enables us to construct an uncovering-by-bases.

Proposition 3.4. *A set of m disjoint partial transversals forms an uncovering-by-bases for G.*

Proof. The proof is analogous to that of Proposition 3.3. For simplicity, we take the first $n-1$ entries of each of the m rows of Ω as our partial transversals. Now, if there are $r = m-1$ errors, then these can be spread across many columns, but can occur in at most $m-1$ rows. Hence there will be at least one row which contains no error positions, so there will be a partial transversal which avoids them all. □

4 Base-transitive groups of rank 2

When it comes to constructing uncoverings-by-bases, base-transitive groups of rank 2 are straightforward to deal with. This is because we have a general theorem (Theorem 4.1) which enables us to construct uncoverings-by-bases without having to consider each case separately. Throughout, G denotes a permutation group acting on Ω. For $a \in \Omega$, let G_a be the stabiliser in G of a. Also, we make the assumption that there are no points fixed by the whole group.

Theorem 4.1. *Let G be a finite base-transitive group of rank 2 acting on a set Ω. Then there is a system of imprimitivity on Ω such that two points drawn from distinct imprimitivity blocks form a base for G.*

Proof. We define a G-invariant equivalence relation on Ω and show that the ensuing block system has the property we require. Define $\sim$ on Ω by $a \sim b \Leftrightarrow G_a = G_b$. Clearly this is an equivalence relation. We need to check that it is G-invariant. Suppose $a \sim b$. Since $G_{a^g} = g^{-1}G_a g$, we have $G_{a^g} = g^{-1}G_a g = g^{-1}G_b g = G_{b^g}$, i.e. that $a^g \sim b^g$.

The next step is to determine the equivalence classes. Let $[a] = \{b : b \sim a\}$, and let $\mathrm{Fix}(H)$ denote the set of points fixed by all elements of $H \leq G$. We claim that $[a] = \mathrm{Fix}(G_a)$.

First, suppose $b \in [a]$, i.e. that $G_b = G_a$. By definition, $b \in \mathrm{Fix}(G_b) = \mathrm{Fix}(G_a)$. Conversely, suppose $b \notin [a]$, i.e. that $G_a \neq G_b$. Now, since G is base-transitive and therefore transitive, $|G_a| = |G_b|$, so there exists some $g \in G_a$ with $b^g \neq b$. Thus $b \notin \mathrm{Fix}(G_a)$, and the claim is proved.

Finally, we explain the base structure of G. Since G is base-transitive of rank 2, a base consists of a pair of points whose pointwise stabiliser is trivial. The choice of the first point is arbitrary, so let this be some point a. Now, for $\{a,b\}$ to be a base for G, we require that b is not fixed by G_a, and so must therefore lie outside the block $[a] = \mathrm{Fix}(G_a)$. Consequently, we can choose b to be any point from the remaining blocks. □

We remark that this block system is trivial (i.e. the blocks all have size 1) if and only if G is sharply 2-transitive: this follows easily from the proof above. If G is sharply 2-transitive, then $G_a \neq G_b$ for $a \neq b$, so $a \sim b$ means $a = b$. Conversely, if the equivalence relation $\sim$ is equality, because G is base-transitive G_a is transitive on $\Omega \setminus \mathrm{Fix}(G_a) = \Omega \setminus [a] = \Omega \setminus \{a\}$. Thus G is 2-transitive, and must therefore be sharply 2-transitive. This corresponds to our knowledge that any pair of points forms a base for a sharply 2-transitive group.

Another useful fact is a general formula for the maximum number of fixed points of a non-identity element.

Proposition 4.2. *Let G acting on Ω be a finite base-transitive group of rank 2. Then the number of fixed points of a non-identity element of G is either* 0 *or m, where $m = |\mathrm{Fix}(G_a)|$ for some $a \in \Omega$.*

Proof. We need to show that if $g \neq 1$ has a fixed point, say a, then it has exactly $m = |\mathrm{Fix}(G_a)|$ fixed points. (We note that the size of $\mathrm{Fix}(G_a)$ is not dependent on the choice of a.)

Since G is base-transitive of rank 2, G_a acts regularly on $\Omega \setminus \mathrm{Fix}(G_a)$ (because any point in here, along with a, forms a base for G, by Theorem 4.1). Consequently, if an element of G_a fixes a point in $\Omega \setminus \mathrm{Fix}(G_a)$, it fixes all these points, and therefore must be the identity.

Suppose g fixes a. Clearly, g belongs to G_a, so g (when acting on Ω) fixes all points in $\mathrm{Fix}(G_a)$ and no others. Hence g has $|\mathrm{Fix}(G_a)|$ fixed points. □

By an earlier remark, the minimum degree of G is given by

$$|\Omega| - \max_{\substack{g \in G \\ g \neq 1}} |\mathrm{Fix}(g)| \, .$$

Here, Ω is partitioned into blocks of the form $\mathrm{Fix}(G_a)$, each of which has size m. Thus $|\Omega| = km$ for some k. By Proposition 4.2, the maximum number of fixed points of a non-identity element is m. Hence the minimum degree of G is $km - m = (k-1)m$. Consequently, the correction capability of a base-transitive group of rank 2 is $r = \left\lfloor \frac{(k-1)m-1}{2} \right\rfloor$.

We construct an uncovering-by-bases by taking a suitable $(km, 2, r)$-uncovering and ensuring each pair of points is a base. One can easily construct a general $(v, 2, t)$-uncovering, by taking $t+1$ disjoint pairs of elements from our v-set; clearly this forms an uncovering, as no t-set can intersect non-trivially with all pairs. Obviously this will only work if $t \leq \frac{1}{2}v - 1$. In the case we are interested in, we have $v = km$ and $t = r$ (where r is as above); one can easily verify that $r = \left\lfloor \frac{(k-1)m-1}{2} \right\rfloor \leq \frac{1}{2}km - 1$ for all $m \geq 1$. So we can use this to construct an uncovering-by-bases, provided we can allocate the disjoint pairs so that each forms a base for G (i.e. that each pair is chosen from distinct blocks).

Recall that there are k blocks, and that we require $r+1$ disjoint bases.

Construction 4.3. First, suppose k is even. Partition the set of blocks into $\frac{1}{2}k$ pairs of blocks. Let $\{A, B\}$ be a pair of blocks, where $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_m\}$. Then we can have m disjoint bases of the form $\{a_i, b_i\}$ (for $i = 1, \ldots, m$). Doing this for each pair of blocks gives $\frac{1}{2}km$ bases in total. As shown above, we know that $r + 1 \leq \frac{1}{2}km$, so this is sufficient.

Now suppose k is odd. Perform the same trick to $k-1$ of the blocks, giving $\frac{1}{2}(k-1)m$ disjoint bases. However, since k is odd, we know that $r+1 = \left\lfloor \frac{(k-1)m-1}{2} \right\rfloor + 1 = \frac{1}{2}(k-1)m$. Hence we have exactly the right number of bases.

It is worth remarking that if G is sharply 2-transitive, the blocks all have size 1, so therefore this construction reduces to merely taking disjoint pairs of points to form an uncovering.

Example 4.4. Let G be the general linear group $\mathrm{GL}(2,q)$ acting on $\mathbb{F}_q^2 \setminus \{0\}$. Now, using elementary linear algebra, an element fixing a point v fixes its linear span, $\langle v \rangle$, i.e. a line through the origin. So each line (with 0 removed) forms an equivalence class of size $q-1$, and there are $q+1$ classes. The minimum degree is $(q^2-1)-(q-1) = q^2-q$. To construct an uncovering-by-bases, we arrange the lines into pairs of lines, and take $q-1$ pairs of points to give $q-1$ bases. This gives us a total of $\lfloor \frac{q+1}{2} \rfloor (q-1)$ disjoint bases.

5 Base-transitive groups of rank 3

In this section we construct uncoverings-by-bases for various families of base-transitive groups of rank 3. These are the sharply 3-transitive groups, the blow-ups of $\mathrm{PGL}(2,q)$, the general linear group $\mathrm{GL}(3,q)$ and the affine general linear group $\mathrm{AGL}(2,q)$. The two exceptional groups of rank 3 are considered in section 6. The rank 3 cases of the "generic" families (vi) and (viii) remain open.

We begin by giving constructions for $(2m,3,m-1)$- and $(2m-1,3,m-2)$-uncoverings, then showing how to convert these into suitable uncoverings-by-bases for the groups we consider.

5.1 An uncovering

The construction we present first gives a $(2m,3,m-1)$-uncovering, so this can be used when the number of points is even. As the coblocks have size three, we refer to them as *triples*.

Theorem 5.1. *Let $\mathcal{A}_{2m}$ denote the set of all $2m$ triples of the form $\{i-1,i,i+m\}$, for $i \in \mathbb{Z}_{2m}$ and with addition modulo $2m$. Then $\mathcal{A}_{2m}$ forms a $(2m,3,m-1)$-uncovering.*

Proof. Let X denote an arbitrary $(m-1)$-subset of $\mathbb{Z}_{2m}$, and let Y denote its complement, so $|Y| = m+1$. We assign colours to the $2m$ points as follows: red if the point lies in X, green if it lies in Y.

We partition $\mathbb{Z}_{2m}$ as the union of the m "antipodal" pairs, i.e. the set of pairs of the form $\{i,i+m\}$. Now, with the colouring described above, the pairs are as follows:

- *green* pairs (i.e. both points are coloured green);

- *red* pairs (both points red);
- *bichromatic* pairs (one point of each colour).

Let $\mathcal{G}$ denote the set of green pairs, $\mathcal{R}$ the set of red pairs and $\mathcal{B}$ the set of bichromatic pairs.

We need to show that there exists a green pair that can be extended to a triple of the form $\{i-1, i, i+m\}$ that is disjoint from X, i.e. all three points are coloured green. This will only fail if every green pair is preceded by a red pair (i.e. both $i-1$ and $i+m-1$ are coloured red), which would require $|\mathcal{G}| \leq |\mathcal{R}|$.

Counting the total number of red points gives $|X| = m-1 = 2|\mathcal{R}| + |\mathcal{B}|$. From this and the fact that $|\mathcal{R}| + |\mathcal{G}| + |\mathcal{B}| = m$, it follows that $|\mathcal{G}| = |\mathcal{R}| + 1$ and we cannot possibly fail. □

Example 5.2. Consider the case $m = 5$. In each row, the framed elements form a coblock in the $(10, 3, 4)$-uncovering $\mathcal{A}_{10}$, while the remaining elements form a block in the corresponding covering design.

$\boxed{1}$	$\boxed{2}$	3	4	5	6	$\boxed{7}$	8	9	10
1	$\boxed{2}$	$\boxed{3}$	4	5	6	7	$\boxed{8}$	9	10
1	2	$\boxed{3}$	$\boxed{4}$	5	6	7	8	$\boxed{9}$	10
1	2	3	$\boxed{4}$	$\boxed{5}$	6	7	8	9	$\boxed{10}$
$\boxed{1}$	2	3	4	$\boxed{5}$	$\boxed{6}$	7	8	9	10
1	$\boxed{2}$	3	4	5	$\boxed{6}$	$\boxed{7}$	8	9	10
1	2	$\boxed{3}$	4	5	6	$\boxed{7}$	$\boxed{8}$	9	10
1	2	3	$\boxed{4}$	5	6	7	$\boxed{8}$	$\boxed{9}$	10
1	2	3	4	$\boxed{5}$	6	7	8	$\boxed{9}$	$\boxed{10}$
$\boxed{1}$	2	3	4	5	$\boxed{6}$	7	8	9	$\boxed{10}$

Note: Examples of these uncoverings (or rather the corresponding covering designs) appear in the database of covering designs maintained by Gordon [16], as "cyclic coverings found by search program". No reference for a general construction is given.

We remark that this construction is within a constant factor of the least possible size. Thanks to a result of W. H. Mills (which is too complicated to state in full generality here, but can be found in [23], Theorem 2.3), a $(2m, 3, m-1)$-uncovering (or, equivalently, a $(2m, 2m-3, m-1)$ covering design) must have size at least $\frac{5}{3}m$. Our construction gives an uncovering of size $2m$, so this is within a factor of at most $\frac{6}{5}$ of the optimal size.

From the construction in Theorem 5.1, we can obtain uncoverings for where there are an odd number of points, thanks to the following lemma. This is a special case, rephrased in terms of uncoverings rather than covering designs, of the "induced construction" due to Gordon, Kuperberg and Patashnik [17], in section 4 of their paper.

Lemma 5.3. *Let $\mathcal{U}$ be a (v,k,t)-uncovering with point set $\{1,\dots,v\}$, and let $\mathcal{W}$ be the subset of $\mathcal{U}$ obtained by removing all coblocks containing the point v. Then $\mathcal{W}$ is a $(v-1,k,t-1)$-uncovering.*

Proof. Let E be an $(t-1)$-subset of $\{1,2,\dots,v-1\}$. As $\mathcal{U}$ is a (v,k,t)-uncovering, there exists a coblock $T \in \mathcal{U}$ disjoint from the t-set $E \cup \{v\}$. Now, clearly T cannot be one of the m-sets containing v. Thus $T \in \mathcal{W}$, and is disjoint from E. Hence $\mathcal{W}$ is a $(v-1,k,t-1)$-uncovering. □

Thus we can apply Lemma 5.3 to the construction from Theorem 5.1 to obtain a $(2m-1,3,m-2)$-uncovering.

Corollary 5.4. *Let $\mathcal{B}_{2m-1}$ be the subset of $\mathcal{A}_{2m}$ obtained by removing all triples containing the point $2m$. Then $\mathcal{B}_{2m-1}$ is a $(2m-1,3,m-2)$-uncovering, of size $2m-3$.*

Example 5.5. The $(9,3,3)$-uncovering $\mathcal{B}_9$, obtained from $\mathcal{A}_{10}$ (see Example 5.2), is given below:

1	2	7
2	3	8
3	4	9
1	5	6
2	6	7
3	7	8
4	8	9

For sharply 3-transitive groups, any triple of points forms a base, so the above constructions $\mathcal{A}_{2m}$ and $\mathcal{B}_{2m-1}$ can be used immediately as uncoverings-by-bases for these groups. From the list of rank 3 groups in section 2, we see that a sharply 3-transitive group of degree n has minimum degree $n-2$ and hence correction capability $r = \lfloor \frac{n-3}{2} \rfloor$. If n is even, say $n = 2m$, we have $r = m-2$; if n is odd, say $n = 2m-1$, again we have $r = m-2$. So in fact when n is even, we actually have a better uncovering than we need.

Example 5.6. $\mathrm{PGL}(2,q)$ is sharply 3-transitive of degree $q+1$, and exists for all prime powers q. So, for instance, $\mathcal{A}_{10}$ (Example 5.2) can be used for $\mathrm{PGL}(2,9)$ and $\mathcal{B}_9$ (Example 5.5) used for $\mathrm{PGL}(2,8)$.

5.2 Blow-ups of $\mathrm{PGL}(2,q)$

The family of groups described by Maund [22] as blow-ups of $\mathrm{PGL}(2,q)$ are quite hard to define from scratch. However, as they are blow-ups (see Definition 2.1) their base structure is relatively uncomplicated. For our purposes, this is all that is required: one does not need to know the precise details of the action of the group in order to construct an uncovering-by-bases. The following theorem is taken from Maund's D.Phil. thesis [22].

Theorem 5.7. *Let G be a blow-up of $\mathrm{PGL}(2,q)$. Then G has degree $q^d(q+1)$, and has $q+1$ blocks of imprimitivity, each of size q^d. An irredundant base for G consists of three points lying in distinct blocks; moreover, every such triple is an irredundant base and G acts transitively on them.*

We think of the blocks as $(q+1)$ columns each containing q^d points. The base structure follows from the fact that the action on the $q+1$ columns is the usual action of $\mathrm{PGL}(2,q)$ on $q+1$ points, which is sharply 3-transitive, so a base for G consists of three points, each drawn from different columns.

Proposition 5.8. *Let G be a blow-up of $\mathrm{PGL}(2,q)$. Then the correction capability of G is $r = \frac{1}{2}q^d(q-1)-1$.*

Proof. According to Maund [22], the maximum number of fixed points of a non-identity element is $2q^d$. Hence the minimum degree is $q^d(q+1)-2q^d = q^d(q-1)$ and so the correction capability is $r = \left\lfloor \frac{1}{2}(q^d(q-1)-1) \right\rfloor = \frac{1}{2}q^d(q-1)-1$. □

Observe that $q^d(q+1)$ is always even, so we only need the $(2m,3,m-1)$-uncovering $\mathcal{A}_{2m}$ (Theorem 5.1). We notice that this is actually better than we really need, since the correction capability r is actually less than $m-1 = \frac{1}{2}q^d(q+1)-1$.

In order to convert $\mathcal{A}_{2m}$ into an uncovering-by-bases for G, we must ensure that each triple forms a base. So we arrange the $2m = q^d(q+1)$ points into a rectangle of q^d rows of length $q+1$, such that in each triple in $\mathcal{A}_{2m}$ the three points come from different columns. As will become evident, we must consider q odd and q even separately.

Construction 5.9. Suppose that the set of points is $\{1,2,\ldots,2m\}$. Arrange them into a rectangle by placing $1,2,\ldots,q+1$ into the first row, $q+2,q+3,\ldots,2(q+1)$ into the second row, and so on. Thus column j contains all points congruent to j (mod $q+1$). For example, with $q=3$ and $d=1$ we have 12 points arranged as follows.

1	2	3	4
5	6	7	8
9	10	11	12

Theorem 5.10. *Let G be a blow-up of $\mathrm{PGL}(2,q)$, where q is odd, and let $2m = q^d(q+1)$. Suppose the points $\{1,2,\ldots,2m\}$ are arranged in a rectangle as in Construction 5.9. Then $\mathcal{A}_{2m}$ forms an uncovering-by-bases for G.*

Proof. Recall that $\mathcal{A}_{2m}$ contains all triples of the form $\{i-1, i, i+m\}$, where $1 \leq i \leq 2m$ and addition is modulo $2m$. (In particular, this means that $i+m = i-m$.) We wish to avoid situations where any two of the three points lie in the same column. First, as q is an odd prime power we have $q+1 \geq 4$, so clearly the points $i-1$ and i are always in different columns. Second, i and $i+m$ are in the same column if and only if $m \equiv 0 \pmod{q+1}$. Since $m = \frac{1}{2}q^d(q+1)$, this happens if and only if q is even, contrary to assumption. Finally, $i-1$ and $i+m$ are in the same column if and only if $m+1 \equiv 0 \pmod{q+1}$. If this happens, then as both $m+1$ and $2m$ are multiples of $q+1$, we have that $(q+1) \mid 2(m+1) - 2m = 2$. But this is impossible, as $q+1 \geq 4$. □

So Construction 5.9 definitely works when q is odd. For example, with $q = 3$ and $d = 1$ we have the 12 triples listed below.

Example 5.11. By comparing these with the arrangement above, we see that each of the 12 triples is spread across three columns.

12	1	7	6	7	1
1	2	8	7	8	2
2	3	9	8	9	3
3	4	10	9	10	4
4	5	11	10	11	5
5	6	12	11	12	6

However, the case where q is even is still to be resolved. As the proof of Theorem 5.10 shows, the same method won't work, so we need to modify it. First we observe that since q is even, we now have an even number of rows, so we can split these into a "top half" (first $\frac{q^d}{2}$ rows) and a "bottom half" (last $\frac{q^d}{2}$ rows). Furthermore, we observe that, in Construction 5.9 above, when $i-1$ and i lie in the top half, $i+m$ must lie in the bottom half (with the exception of the "boundary cases", when $i = 1$ or $i = m+1$). So we perform the following "trick".

Construction 5.12. Arrange the points $\{1, \ldots, 2m\}$ into a rectangle as in Construction 5.9, except with all rows in the bottom half "cycled" two places to the right. For instance, with $q = 4$, $d = 1$ we have the following:

1	2	3	4	5
6	7	8	9	10
14	15	11	12	13
19	20	16	17	18

We need to demonstrate that this trick works in general.

Theorem 5.13. *Let G be a blow-up of $\mathrm{PGL}(2,q)$, where q is even and $q > 2$, and let $2m = q^d(q+1)$. Suppose the points $\{1,2,\ldots,2m\}$ are arranged as in Construction 5.12. Then $\mathcal{A}_{2m}$ forms an uncovering-by-bases for G.*

Proof. Recall that our triples are of the form $\{i-1, i, i+m\}$. First, we deal with the case when $i-1$ and i are both in the top half, and lie in columns $j-1$ and j (mod $q+1$). Now, before the shift is applied, by the same arguments as in the previous proof, $i+m$ will also lie in column j. But after the shift, it will now lie in column $j+2$.

Second, we deal with the case when both $i-1$ and i are both in the bottom half. Because of the shift applied, these will lie in columns $j+1$ and $j+2$ while $i+m$, which will be in the top half, lies in column j.

Then there are the two "boundary" cases. First, if $i = 1$, then clearly i lies in the column 1. However, before the shift, $i-1$ will be in the last column of the last row (and thus is in the bottom half), so after the shift will lie in column 2. Also, $i+m$ will be in column 1 before the shift, and so is in column 3 afterwards.

Second, if $i = m+1$, then i will be in the first row of the bottom half, and in the first column before the shift. Thus after the shift it will lie in column 3. $i-1$ will be in the last column of the last row of the top half, i.e. in column $q+1$. Finally, $i+m$ will be in the first row and the first column, i.e. column 1.

We see that in all of these cases the three entries are in distinct columns. □

We conclude by remarking that this does not work if $q = 2$, as we will have three columns and, for instance, $j-1 \equiv j+2$ (mod 3). Thus for $q = 2$, an entirely different approach is required. But since $\mathrm{PGL}(2,2) \cong S_3$, we have already dealt with blow-ups of this group (in section 3).

5.3 $\mathrm{GL}(3,q)$

To construct an uncovering-by-bases for the group $\mathrm{GL}(3,q)$ acting on $\mathbb{F}_q^3 \setminus \{0\}$, we will not work in the vector space, but instead we move the problem into the extension field $\mathbb{F}_{q^3}$. Since they are isomorphic as vector spaces over $\mathbb{F}_q$, we are able to make use of the additional structure that finite fields have. We obtain a collection of bases for $\mathbb{F}_{q^3}$, and then apply the isomorphism to obtain bases for $\mathbb{F}_q^3$.

The background material on finite fields that we require is the following. For basic definitions and terminology, we refer the reader to the *Encyclopædia of Mathematics* volume on finite fields by Lidl and Niederreiter [21]. Let $K = \mathbb{F}_q$ be the finite field of order q and $F = \mathbb{F}_{q^n}$ be its degree n extension field. Because the multiplicative group of a finite field is cyclic, it can be generated by a single element; we call such an element a *primitive element*.

Definition 5.14. For $\alpha \in F$, the *trace* of α over K, $\mathrm{Tr}_{F/K}(\alpha)$, is defined as

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}},$$

i.e. the sum of the conjugates of α.

The conjugates of α are the roots of the minimum polynomial, say $f(x)$, of α over K. If α does not lie in a proper subfield of F, then all of its conjugates are distinct, and so we have that $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ factorises as $f(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})$. We observe that, when multiplying out the second form of $f(x)$, the coefficient of x^{n-1} is $-\mathrm{Tr}_{F/K}(\alpha)$, i.e. we have:

Proposition 5.15. $\mathrm{Tr}_{F/K}(\alpha) = -a_{n-1}$.

The following definition relates conjugates to bases.

Definition 5.16. A *normal basis* for F over K is a basis consisting of the conjugates $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ of some element $\alpha \in F$. Such an element α is called a *free element*.

Free elements have the following useful property.

Lemma 5.17. *A free element* $\alpha \in F$ *satisfies* $\mathrm{Tr}_{F/K}(\alpha) \neq 0$.

Proof. Suppose not. Then we would have $\alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}} = 0$, i.e. the conjugates would be linearly dependent and do not form a basis, i.e. α is not free. □

The *Normal Basis Theorem* (described in [21], Theorem 2.35) states that for any prime power q and $n > 1$, there exists a free element α, i.e. that there exists a normal basis. A more specific type of basis is a *primitive normal basis*, which is a normal basis but with the extra condition that the free element α is also a primitive element. The following theorem is important here.

Theorem 5.18. The Primitive Normal Basis Theorem (Carlitz; Davenport; Lenstra and Schoof; Cohen and Huczynska). *For any prime power q and $n > 1$, there exists a primitive normal basis of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$.

The theorem was originally proved by Carlitz [8, 9] in 1952 for "sufficiently large" q and n and in 1968 by Davenport [13] for any n in the case where q is prime. Later (1987), Lenstra and Schoof [20] completed the proof, but with the aid of a computer; more recently (2003) Cohen and Huczynska [11] gave a non-computational proof. The result we will need in the next section is the following corollary.

Corollary 5.19. *For any prime power q and $n > 1$, there exists a primitive element* $\alpha \in F = \mathbb{F}_{q^n}$ *such that* $\mathrm{Tr}_{F/K}(\alpha) \neq 0$ *(where $K = \mathbb{F}_q$).*

Proof. By the Primitive Normal Basis Theorem, a primitive, free element α exists. By Lemma 5.17, free elements have non-zero trace. □

We remark that the Primitive Normal Basis Theorem is a much stronger result than we actually need, and that there are other results that we could use in its place. For instance, a result of Cohen [10] shows that with one non-trivial exception, $\mathbb{F}_{q^n}$

contains a primitive element of arbitrary trace over $\mathbb{F}_q$.

We now have the necessary background, so we return to the subject of $\mathrm{GL}(3,q)$. As happened with $\mathrm{GL}(2,q)$ (see Example 4.4), the largest possible set of fixed points consists of a subspace of codimension 1, so this has size q^2-1. Hence the minimum degree is q^3-q^2 and so the correction capability is $r=\frac{1}{2}(q^3-q^2)-1$. Note that $\mathrm{GL}(3,q)$ can have even or odd degree (depending on the parity of q), so we will consider q odd and even separately, and convert $\mathcal{A}_{2m}$ and $\mathcal{B}_{2m-1}$ into uncoverings-by-bases.

As was the case with the groups in the previous subsection, the uncoverings $\mathcal{A}_{2m}$ and $\mathcal{B}_{2m-1}$ are actually capable of uncovering more points than the correction capability r. When q is odd we have $2m=q^3-1$, so $m-1=\frac{1}{2}(q^3-1)-1$, while when q is even we have $2m-1=q^3-1$, so $m-2=\frac{1}{2}q^3-2$. In both cases we have more than r points.

Now we proceed with the constructions. First, we suppose q is odd, so therefore q^3-1 is even, say $q^3-1=2m$. If α is a primitive element of $\mathbb{F}_{q^3}$, then the non-zero elements of $\mathbb{F}_{q^3}$ are the powers of α, i.e. $\mathbb{F}_{q^3}=\{1,\alpha,\alpha^2,\ldots,\alpha^{2m-1}\}$. Note that $\alpha^{2m}=1$, and also that $(\alpha^m)^2=\alpha^{2m}=1$, so $\alpha^m=-1$.

Suppose we attempt to convert $\mathcal{A}_{2m}$ into an uncovering-by-bases, using the bijection $\psi_\alpha:\mathbb{Z}_{2m}\to\mathbb{F}_{q^3}^*$ where $i\mapsto\alpha^i$. Unfortunately, this will not work, as each triple of field elements will have the form $\{\alpha^{i-1},\alpha^i,\alpha^{i+m}\}$. This will be a basis if and only if $\{1,\alpha,\alpha^{m+1}\}$ is a basis. However, since $\alpha^m=-1$, we have the triple $\{1,\alpha,-\alpha\}$, which is clearly not a basis.

All is not lost, however. Instead of ordering the field elements as above, we modify it as follows. Define the bijection $\varphi_\alpha:\mathbb{Z}_{2m}\to\mathbb{F}_{q^3}^*$ where $i\mapsto\varphi_\alpha(i)$ as follows:

i	0	1	2	$\cdots$	$m-1$	m	$m+1$	$\cdots$	$2m-3$	$2m-2$	$2m-1$
$\varphi_\alpha(i)$	1	α	α^2	$\cdots$	α^{m-1}	α^{m+2}	α^{m+3}	$\cdots$	α^{2m-1}	α^m	α^{m+1}

That is, the first half remain as they were under ψ_α, and the second half are moved two places to the left, with the remaining two elements replaced at the end.

Theorem 5.20. *Suppose q is odd, and that α is a primitive element of $\mathbb{F}_{q^3}$ with non-zero trace over $\mathbb{F}_q$. Then the set of triples of the form*

$$\{\varphi_\alpha(i-1),\varphi_\alpha(i),\varphi_\alpha(i+m)\},$$

for $i\in\mathbb{Z}_{2m}$ forms an uncovering-by-bases for $\mathrm{GL}(3,q)$ acting on $\mathbb{F}_{q^3}$.

Proof. First, by Theorem 5.1, we know that these triples form an uncovering, so we only need verify that each triple is a basis. Second, we have that Corollary 5.19 guarantees the existence of a suitable primitive element. Also, this choice of α ensures that both $\{1,\alpha,\alpha^2\}$ and $\{1,\alpha,\alpha^3\}$ are linearly independent over $\mathbb{F}_q$. (If not, we would have that α was a root of $x^3+ax+b=0$ (for $a,b\in\mathbb{F}_q$), but this cubic would then have to be the minimum polynomial of α, implying α had trace 0.)

Divide consideration of the triples into seven cases: (1) $1 \leq i \leq m-3$, (2) $m-2 \leq i \leq m-1$, (3) $i = m$, (4) $m+1 \leq i \leq 2m-3$, (5) $i = 2m-2$, (6) $i = 2m-1$ and (7) $i = 2m$. We will describe the argument in two cases, (1) and (4); the other cases work similarly. In case (1), each triple is a basis if and only if $\{1, \alpha, \alpha^{m+3}\}$ is. Since $\alpha^m = -\alpha$, this is a basis if and only if $\{1, \alpha, -\alpha^3\}$ is, so if and only if $\{1, \alpha, \alpha^3\}$ is. In case (4), each triple is a basis if and only if $\{\alpha^{m+2}, \alpha^{m+3}, \alpha\}$ is, i.e. if and only if $\{-\alpha^2, -\alpha^3, \alpha\}$ is, so if and only if $\{1, \alpha, \alpha^2\}$ is.

In all seven cases, showing that each type of triple is a basis reduces to checking that either $\{1, \alpha, \alpha^2\}$ or $\{1, \alpha, \alpha^3\}$ is, so we are done. □

In order to obtain an uncovering-by-bases for the action of $\mathrm{GL}(3,q)$ on $\mathbb{F}_q^3$, we must exhibit an isomorphism between the vector space $\mathbb{F}_q^3$ and the extension field $\mathbb{F}_{q^3}$. The smallest example for this is still quite large: $\mathrm{GL}(3,3)$ acting on the 26 non-zero vectors in $\mathbb{F}_3^3$.

Example 5.21. The isomorphism between the vector space $\mathbb{F}_3^3$ and the extension field $\mathbb{F}_{27}$ is found from the minimum polynomial of the primitive element α. From Table F in Lidl and Niederreiter [21], the polynomial $x^3 + 2x^2 + 1$ is irreducible and has a primitive element as a root. Clearly this polynomial has non-zero trace, so it satisfies our requirements, although it can be verified that the primitive element obtained is also a free element.

Thus the isomorphism $\mathbb{F}_27 \to F_3^3$ is given by $a\alpha^2 + b\alpha + c \mapsto (a,b,c)$, for $a,b,c \in \mathbb{F}_3$. For example, $\alpha^4 = \alpha^2 + 2\alpha + 2 \mapsto (1,2,2)$. Finding the image of α^i for each i enables us to write each of the triples as bases for $\mathbb{F}_3^3$ over $\mathbb{F}_3$; for instance, the first triple $\{1, \alpha, \alpha^{16}\}$ corresponds to $\{(0,0,1), (0,1,0), (2,0,1)\}$. The same approach gives us all 26 triples.

We now deal with the case where q is even, say $q = 2^s$. Consider $\mathbb{F}_q \subset \mathbb{F}_{q^3}$, i.e. $\mathbb{F}_{2^s} \subset \mathbb{F}_{2^{3s}} = F$. This time, as there are an odd number, $2m-1 = 2^{3s}-1$, of elements in F^*, we want to convert $\mathcal{B}_{2m-1}$ into an uncovering-by-bases. To do so we introduce an additional element, ∞, construct an uncovering of $S = F^* \cup \{\infty\}$, then remove the triples containing ∞. Let α be a primitive element of F. We have $S = \{1, \alpha, \alpha^2, \ldots, \alpha^{2m-2}, \infty\}$ so $|S| = 2m = 2^{3s}$, say. We construct a bijection

$$\begin{array}{rcll} \chi_\alpha : \mathbb{Z}_{2m} & \to & S & \\ i & \mapsto & \alpha^i & \text{for } 0 \leq i \leq 2m-2 \\ i & \mapsto & \infty & \text{for } i = 2m-1. \end{array}$$

Theorem 5.22. *Suppose q is even, and that α is a primitive element of $\mathbb{F}_{q^3}$ whose inverse has non-zero trace over $\mathbb{F}_q$. Then the set of triples of the form*

$$\{\chi_\alpha(i-1), \chi_\alpha(i), \chi_\alpha(i+m)\},$$

for $i \in \mathbb{Z}_{2m}$, excluding those containing ∞, forms an uncovering-by-bases for $\mathrm{GL}(3,q)$ acting on $\mathbb{F}_{q^3}$.

Proof. First, by Corollary 5.4, we know that these triples will form an uncovering, so we need to verify that each triple forms a basis. Second, we have that Corollary 5.19 guarantees the existence of a suitable primitive element.

Divide consideration of the triples into two cases: (1) $1 \leq i \leq m-2$, and (2) $m \leq i \leq 2m-2$ (other values of i give triples containing ∞). In case (1), each triple is a basis if and only if $\{1, \alpha, \alpha^{m+1}\}$ is. In case (2), each triple is a basis if and only if $\{1, \alpha^{m-1}, \alpha^m\}$ is.

Observe that $\{1, \alpha, \alpha^{m+1}\}$ fails to be a basis if and only if α is a root of $f(x) = x^{m+1} + ax + b$ (for some $a, b \in \mathbb{F}_q$) and thus also of $f(x)^2 = x^3 + a^2x^2 + b^2$. This happens if and only if α^{-1} is a root of $h(x) = x^3 + \frac{a^2}{b^2}x + \frac{1}{b^2}$, i.e. if α^{-1} has trace 0. Thus, by our choice of α, $\{1, \alpha, \alpha^{m+1}\}$ must be a basis. Using a similar argument, we can show that $\{1, \alpha^{m-1}, \alpha^m\}$ is also a basis.

Thus in both cases, the triples are bases, and we are done. □

5.4 AGL$(2,q)$

As with GL$(3,q)$, we convert our earlier constructions of uncoverings $\mathcal{A}_{2m}$ and $\mathcal{B}_{2m-1}$ into uncoverings-by-bases. We apply similar techniques to those we used for GL$(3,q)$, except now we are working in a 2-dimensional vector space, and must consider affine independence rather than linear independence. To determine the minimum degree, using elementary affine geometry (see, for instance, Neumann, Stoy and Thompson [25]) we note that the largest possible set of fixed points consists of an affine subspace of codimension 1 (i.e. a coset of a linear subspace of codimension 1), which in this case has size q. Hence the minimum degree is $q^2 - q$, and therefore the correction capability of AGL$(2,q)$ is $r = \frac{1}{2}(q^2 - q) - 1$.

Once more, we remark that the uncoverings constructed are more powerful than we need. For q odd, we have an even number of non-zero field elements, so use the $(2m, 3, m-1)$-uncovering with $2m = q^2 - 1$, so $m - 1 = \frac{1}{2}(q^2 - 1) - 1$. For q even, we use the $(2m-1, 3, m-2)$-uncovering with $2m - 1 = q^2 - 1$, so $m - 2 = \frac{1}{2}q^2 - 2$. In both cases, we have something larger than r.

As with GL$(3,q)$, to construct our uncovering-by-bases we consider q odd and even separately. In the case where q is odd, we have an even number of non-zero field elements, $1, \alpha, \alpha^2, \ldots, \alpha^{2m-1}$ (where $2m = q^2 - 1$). This case is relatively straightforward.

Theorem 5.23. *Suppose q is odd. Then the set of triples $\{\alpha^{i-1}, \alpha^i, \alpha^{i+m}\}$, for $i \in \mathbb{Z}_{2m}$, forms an uncovering-by-bases for* AGL$(2,q)$ *acting on* $\mathbb{F}_{q^2}$.

Proof. By Theorem 5.1, we know that this set is an uncovering, so therefore we need to verify that each triple is a base for AGL$(2,q)$. It suffices to show that the triple $\{1, \alpha, \alpha^{m+1}\}$ (and hence each multiple of it by powers of α) is a base, i.e. that it is affine-independent. This is equivalent to the pair $\{\alpha - 1, \alpha^{m+1} - 1\}$ being linearly independent. Since $\alpha^m = -1$, this pair is actually $\{\alpha - 1, -\alpha - 1\}$, which is clearly linearly independent.

Thus $\{1, \alpha, \alpha^{m+1}\}$ is affine-independent, and it follows that each multiple of it is also. Therefore the given set of triples forms an uncovering-by-bases. □

The case where q is even is considerably more complicated. First we mention that we do not need to consider the case $q = 2$, since $\mathrm{AGL}(2,2) \cong S_4$ has correction capability 0. We require some preliminary lemmata, the first two of which are number-theoretic in nature. Henceforth, ϕ denotes Euler's totient function.

Lemma 5.24. *For any positive integer n,*

$$\phi(n) \geq \frac{n}{\log_2(n)}.$$

Proof. Let $p_1, p_2, \ldots, p_r$ be the prime divisors of n. So $n \geq p_1 p_2 \cdots p_r \geq 2^r$, and therefore $r \leq \log_2(n)$. Also,

$$\begin{aligned} \frac{\phi(n)}{n} &= \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \\ &\geq \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\cdots\left(1 - \frac{1}{r}\right) \\ &= \frac{1}{r} \\ &\geq \frac{1}{\log_2(n)} \end{aligned}$$

and the result follows. □

Lemma 5.25. *Where $q = 2^s$ (for $s > 1$), $\phi(q^2 - 1) > 2(q - 1)$.*

Proof. Suppose not, i.e. suppose $\phi(q^2 - 1) \leq 2(q - 1)$. By Lemma 5.24 above, we have

$$\begin{aligned} \phi(q^2 - 1) &\geq \frac{q^2 - 1}{\log_2(q^2 - 1)} \\ &> \frac{q^2 - 1}{\log_2(q^2)} \\ &= \frac{q^2 - 1}{2s}. \end{aligned}$$

By assumption, we have

$$\frac{q^2 - 1}{2s} < 2(q - 1)$$

i.e. $2^s + 1 < 4s$, which fails for $s \geq 4$.

Checking small cases by hand, we have:

$$\begin{aligned} s = 1: \quad & \phi(3) = 2, & 2(q-1) = 2 \\ s = 2: \quad & \phi(15) = 8, & 2(q-1) = 6 \\ s = 3: \quad & \phi(63) = 36, & 2(q-1) = 14 \end{aligned}$$

so the proposition holds for $s > 1$. □

As we will see shortly, we will be restricted in our choice of primitive element in this case. The next lemma guarantees the existence of the specific kind of primitive element we will require.

Lemma 5.26. *Let $q = 2^s$ (for $s > 1$) and consider $\mathbb{F}_q \subset \mathbb{F}_{q^2}$. Then there exists a primitive element α of $\mathbb{F}_{q^2}$ which satisfies no polynomial of the form $x^2 + x + a$, where $a \in \mathbb{F}_q$ and $a \neq 0$.*

Proof. There are exactly $q-1$ such polynomials, which have a total of at most $2(q-1)$ roots, which are not necessarily primitive. So there are at most $2(q-1)$ primitive elements which satisfy such polynomials. However, there are a total of $\phi(q^2-1)$ primitive elements altogether, and by Lemma 5.25 above, $\phi(q^2-1) > 2(q-1)$. Therefore a primitive element satisfying no such polynomial must exist. □

In this case, instead of using $\mathcal{B}_{2m-1}$, we will use a new uncovering $\mathcal{B}'_{2m-1}$, which has triples of the form $\{i, i+1, i+m\}$, rather than what we have used previously. (The set of all such triples for $0 \leq i \leq 2m-1$ forms a $(2m, 3, m-1)$-uncovering, simply by replacing $i-1$ with $i+1$ in the proof of Theorem 5.1.) Then we apply the induced construction in Lemma 5.3, to obtain a $(2m-1, 3, m-1)$-uncovering.

As we did in Theorem 5.22, we introduce an additional point ∞, produce an uncovering on $S = \{1, \alpha, \alpha^2, \ldots, \alpha^{2m-2}, \infty\}$, then remove each triple which contains ∞. Define a bijection

$$\begin{array}{rcll} \theta_\alpha : \mathbb{Z}_{2m} & \to & S & \\ i & \mapsto & \alpha^i & \text{for } 0 \leq i \leq 2m-2 \\ i & \mapsto & \infty & \text{for } i = 2m-1. \end{array}$$

Note that $2m = q^2$ here.

Theorem 5.27. *Suppose q is even and $q > 2$. Let α be a primitive element of $\mathbb{F}_{q^2}$ such that $\alpha^2 + \alpha \notin \mathbb{F}_q$. Then the set of triples of the form*

$$\{\theta_\alpha(i), \theta_\alpha(i+1), \theta_\alpha(i+m)\},$$

for $i \in \mathbb{Z}_{2m}$, excluding those containing ∞, forms an uncovering-by-bases for $\mathrm{AGL}(2,q)$ acting on $\mathbb{F}_{q^2}$.

Proof. First, by the above we have that these triples form an uncovering, so we only need to verify that each triple is affine-independent over $\mathbb{F}_q$. Second, we observe that Lemma 5.26 guarantees the existence of a suitable primitive element.

Now, there are two cases to consider: (1) $0 \leq i \leq m-2$ and (2) $m \leq i \leq 2m-3$ (other values of i give triples containing ∞). Case (1) reduces to showing that

$\{1,\alpha,\alpha^m\}$ is affine-independent, while case (2) reduces to showing $\{1,\alpha,\alpha^{m-1}\}$ is affine-independent.

In case (1), we note that the triple $\{1,\alpha,\alpha^m\}$ is affine-independent if and only if the pair $\{\alpha+1,\alpha^m+1\}$ is linearly independent. Now, because the characteristic of this field is 2, and because m is a power of 2, we have that $\alpha^m+1=(\alpha+1)^m$, so in particular $\alpha+1$ divides α^m+1, with quotient $(\alpha+1)^{m-1}$. Thus $\{\alpha+1,\alpha^m+1\}$ will be linearly independent if and only if $(\alpha+1)^{m-1}\notin\mathbb{F}_q^*$.

So suppose not, i.e. suppose $(\alpha+1)^{m-1}\in\mathbb{F}_q^*$, and consider the quotient group $H=\mathbb{F}_{q^2}^*/\mathbb{F}_q^*$, which is cyclic and has order $q+1$. Also, consider the natural projection map $\pi:\mathbb{F}_{q^2}^*\twoheadrightarrow H$. Let $\beta=\pi(\alpha+1)$, so therefore $\beta^{m-1}=1$. Thus the order of β divides both $m-1$ and $q+1$, so divides

$$\begin{aligned}\gcd(q+1,\tfrac{1}{2}q^2-1) &= \gcd(q+1,q^2-2)\\ &= \gcd(q+1,(q+1)(q-1)-1)\\ &= 1.\end{aligned}$$

Hence β has order 1, i.e. $\beta=1$. But then this means $\alpha+1\in\mathrm{Ker}(\pi)=\mathbb{F}_q^*$, which is impossible since α is a primitive element of $\mathbb{F}_{q^2}$. Therefore $(\alpha+1)^{m-1}\notin\mathbb{F}_q^*$, so we have that $\{\alpha+1,\alpha^m+1\}$ is linearly independent, and that $\{1,\alpha,\alpha^m\}$ is affine-independent.

Case (2) requires the lemmata we proved above. Clearly, $\{1,\alpha,\alpha^{m-1}\}$ is affine-independent if and only if $\{\alpha+1,\alpha^{m-1}+1\}$ is linearly independent. Now, $\alpha+1$ divides $\alpha^{m-1}+1$, with quotient $C=1+\alpha+\alpha^2+\cdots+\alpha^{m-2}$. Since the elements of $\mathbb{F}_{q^2}$ sum to zero, we have $\sum_{i=0}^{2m-2}\alpha^i=0$, so $1+C\alpha+C\alpha^m=0$. Squaring (and remembering we have characteristic 2) gives $1+C^2\alpha+C^2\alpha^2=0$, thus $\alpha^2+\alpha=\frac{1}{C^2}$. Our choice of α ensures that $C\notin\mathbb{F}_q$, so $\{\alpha+1,\alpha^{m-1}+1\}$ is linearly independent and thus $\{1,\alpha^m,\alpha^{m+1}\}$ is affine-independent.

Hence in both cases the triples are bases for $\mathrm{AGL}(2,q)$, and we are done. □

6 Exceptional base-transitive groups

In this section we consider the "exceptional" base-transitive groups of ranks 3, 4 and 5. For each group, we first find an uncovering by taking the complements of the blocks of a suitable covering design from the internet database maintained by Gordon [16]. Then, if necessary, we relabel the points to ensure the coblocks are all bases. The uncoverings-by-bases obtained are given explicitly in the author's Ph.D. thesis [1].

Gordon's database contains covering designs with small parameters, most of which have been found using various computational search techniques. We will not discuss this here, as how the design was found does not concern us directly. It is believed that the designs in the database are the smallest-known for each set of parameters, but it is not clear from the database which have been proved to be minimal. See [16] for full details.

6.1 A_7 and two related groups

Because of the exceptional isomorphism between the A_8 and $\mathrm{GL}(4,2)$ (see the $\mathbb{ATLAS}$ [12], page 22), the alternating group A_7 has an action on $\mathbb{F}_2^4 \setminus \{0\}$. The irredundant bases for A_7 in this action are the linearly independent triples of vectors in $\mathbb{F}_2^4$, and A_7 acts transitively on these. Thus, in this action, A_7 is a base-transitive group of rank 3 and degree 15. From Maund [22] (or by direct computation), the maximum number of fixed points of a non-identity element is 3, so therefore the minimum degree is 12 and correction capability is 5.

We obtain a presentation for this action of A_7 using the computer algebra system GAP [15]. Its libraries of transitive groups contain a suitable presentation, which is given (in disjoint cycle form) by

$$\begin{aligned} &(1\ 9\ 10\ 3\ 14)(2\ 15\ 7\ 12\ 6)(4\ 5\ 11\ 13\ 8) \\ \text{and}\quad &(1\ 2\ 3)(5\ 6\ 7)(8\ 10\ 9)(12\ 14\ 13). \end{aligned}$$

A $(15,3,5)$-uncovering of size 9 can be obtained from the $(15,12,5)$ covering design in Gordon's database [16]. Checking each of these in GAP, we find that each coblock happens to be a base for A_7 in this action, so the set of coblocks does indeed form an uncovering-by-bases, which is given in [1].

There are two other groups related to A_7 which are base-transitive. The first is the affine extension of the action of A_7 on $\mathbb{F}_2^4 \setminus \{0\}$ described above, i.e. the group $G = V \rtimes A_7$ (where V is the additive group of $\mathbb{F}_2^4$). This action of G has degree 16 and is base-transitive of rank 4; the bases are affine-independent 4-tuples of vectors in $\mathbb{F}_2^4$. As with A_7, we can find this action in the GAP libraries. This group G is generated by

$$\begin{aligned} &(1\ 6\ 5\ 7\ 2\ 4\ 16)(8\ 9\ 14\ 13\ 15\ 10\ 12) \\ \text{and}\quad &(1\ 9\ 3\ 14\ 12\ 11\ 4)(2\ 13\ 8\ 16\ 10\ 7\ 5). \end{aligned}$$

From Maund [22], the maximum number of fixed points of an non-identity element of G is 4, so the minimum degree is 12, and thus the correction capability is 5. Thus we require a $(16,4,5)$-uncovering, where each 4-set is a base for G. Once more, we can obtain an uncovering from [16], as the complements of the blocks of a $(16,12,5)$ covering design. We then have to relabel the points to ensure that each coblock is a base in order to obtain an uncovering-by-bases, which has size 12 (see [1]).

The second group related to A_7 is constructed similarly. Let K denote the stabiliser of a point in the action of A_7 on 15 points described above; this group is in fact $\mathrm{PSL}(3,2)$, in its base-transitive action of rank 2 (see section 2). Then we can construct the affine extension H of this group, $H = V \rtimes K$, where V is as above.

This group also has degree 16, and is base-transitive of rank 3; the bases here are the affine-independent triples of vectors in $\mathbb{F}_2^4$. Again, we use the GAP library to find this group, which has generators

$$\begin{aligned} & (1\ 11\ 10\ 13\ 5\ 4\ 8\ 2\ 12\ 9\ 14\ 6\ 3\ 7)(15\ 16) \\ \text{and}\quad & (1\ 9\ 15\ 7)(2\ 10\ 16\ 8)(3\ 12\ 5\ 14)(4\ 11\ 6\ 13). \end{aligned}$$

From [22], the maximum number of fixed points of a non-identity element of H is 4, so the minimum degree is 12 and therefore, as a code, this group can also correct 5 errors. As before, we consult the database [16] to find a suitable uncovering; here the required parameters are $(16,3,5)$, and we find one of size 8. Once again, we need to relabel the points before it becomes an uncovering-by-bases (see [1]).

Full details of the GAP computations are given in [1].

6.2 Two Mathieu groups

The Mathieu groups M_{11} and M_{12} are sharply 4- and 5-transitive respectively. Thus to obtain uncoverings-by-bases it suffices to obtain suitable uncoverings. M_{11} has degree 11 and correction capability 3, so requires an $(11,4,3)$-uncovering, while M_{12} has degree 12 and correction capability 3, so requires a $(12,5,3)$-uncovering. Suitable uncoverings were both obtained from the covering designs in Gordon's database [16]. As an example, the $(12,5,3)$-uncovering needed for M_{12} (which has size 11) is given in Table 1 below; the uncovering needed for M_{11} (which has size 8) is given in [1].

1	2	3	4	5
1	2	6	11	12
1	3	7	8	9
1	4	6	7	10
1	5	8	9	11
2	4	8	9	12
2	5	7	10	11
3	4	7	11	12
3	5	6	10	12
3	6	8	9	11
6	7	8	9	10

Table 1: $(12,5,3)$-uncovering for M_{12}

Some further coding properties of M_{12} are investigated by Bray and the author in [3].

7 Uncoverings-by-bases for matroids?

With only minor modifications, the definition of uncovering-by-bases can be transferred from the context of base-transitive groups to that of matroid theory. The following definition is due to Cameron and Fon-Der-Flaass [7].

Definition 7.1. A permutation group in a given action is called an *IBIS group* if all irredundant bases have the same size.

The acronym stands for "irredundant bases of invariant size". In their 1995 paper [7], Cameron and Fon-Der-Flaass proved the following theorem.

Theorem 7.2. *The following statements are equivalent:*

1. *G acting on Ω is an IBIS group;*
2. *the irredundant bases of G are preserved by re-ordering;*
3. *the irredundant bases of G form the bases of a matroid on Ω.*

For matroid terminology, the reader is referred to Oxley's book [26]. Clearly, base-transitive groups are IBIS groups, and the associated matroids are *permutation geometries*, as studied by Cameron and Deza [6]; for this reason, they gave base-transitive groups the name *geometric groups*. The rank of an IBIS group is exactly the rank of the corresponding matroid.

The *flats* of a matroid are analogous to the subspaces of a vector space. In particular, when the matroid M is that corresponding to a base-transitive group G, the flats are precisely the fixed point sets of elements of G (see [6]). (For instance, where $G = \mathrm{GL}(n,q)$, the fixed point sets are precisely the subspaces of $V = \mathbb{F}_q^n$, which are precisely the flats of the corresponding vector matroid $V(n,q)$). In fact, for IBIS groups, all fixed point sets are flats (although there may be other flats), and every maximal proper flat is a fixed point set. Thus the maximum number of fixed points of a non-identity element of an IBIS group is the size of the largest proper flat of M. Consequently, we can define a parameter s for an arbitrary matroid, which is analogous to the correction capability of a permutation group (although it is not entirely clear what this parameter represents in terms of matroid theory). Let $M = (\Omega, \mathfrak{I})$ be a matroid, with $|\Omega| = n$, whose maximal proper flats have size f. Then we define

$$s = \left\lfloor \frac{n-f-1}{2} \right\rfloor.$$

Now we make the following definition.

Definition 7.3. A *t-uncovering-by-bases* for a matroid $M = (\Omega, \mathfrak{I})$ is a set $\mathcal{U}$ of bases for M such that any t-subset of Ω is disjoint from at least one base in $\mathcal{U}$.

If we take t to be equal to the parameter s given above, then in the case where M is the matroid corresponding to a base-transitive group G, then this is precisely an uncovering-by-bases for G, as defined earlier.

Example 7.4. Consider the *uniform matroid* $U_{m,n}$, i.e. the matroid on $\Omega = \{1, \ldots, n\}$ which has every m-subset of Ω as a base. Thus a t-uncovering-by-bases for $U_{m,n}$ is just an (n, m, t)-uncovering.

Since every $(m-1)$-subset is a maximal proper flat, we have $s = \lfloor \frac{n-m}{2} \rfloor$ here.

Note that the matroid corresponding to a sharply k-transitive group G of degree n is the uniform matroid $U_{k,n}$, so an s-uncovering-by-bases for $U_{k,n}$ is exactly an uncovering-by-bases for the group G. In fact, the IBIS groups corresponding to uniform matroids were determined by Cameron and Fon-Der-Flaass [7]: in addition to the sharply k-transitive groups, there are only the Frobenius groups (rank 2), Zassenhaus groups (rank 3) and some rank 4 groups classified by Gorenstein and Hughes [18]. So, by an earlier remark, we can deduce that for all these groups an (n, k, s)-uncovering will form an uncovering-by-bases for the group.

Acknowledgements

The author would like to thank his supervisor, P. J. Cameron, for numerous helpful comments and suggestions, S. Huczynska for a useful discussion about finite fields, and the two anonymous referees for their suggestions for how to improve the paper.

This research was funded by an EPSRC CASE studentship, sponsored by the UK Government Communications Headquarters (GCHQ).

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 to *Discrete Math.* Preprint available from `http://www.maths.qmul.ac.uk/~rfb/papers/`.

[3] R. F. Bailey and J. N. Bray, Decoding the Mathieu group M_{12}, in preparation.

[4] P. J. Cameron, Some multiply transitive permutation groups, in *Coding Theory, Design Theory, Group Theory: Proceedings of the Marshall Hall Conference*, (eds D. Jungnickel and S. A. Vanstone), John Wiley & Sons, New York, 1993.

[5] P. J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts (45), Cambridge University Press, Cambridge, 1999.

[6] P. J. Cameron and M. Deza, On permutation geometries, *J. London Math. Soc.* (2) **20** (1979), 373–386.

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

[8] L. Carlitz, Primitive roots in a finite field, *Trans. Amer. Math. Soc.* **73** (1952), 373–382.

[9] L. Carlitz, Some problems involving primitive roots in a finite field, *Proc. Nat. Acad. Sci. USA* **38** (1952), 314–318, 618.

[10] S. D. Cohen, Primitive elements and polynomials with arbitrary trace, *Discrete Math.* **83** (1990), 1–7.

[11] S. D. Cohen and S. Huczynska, The primitive normal basis theorem – without a computer, *J. London Math. Soc.* (2) **67** (2003), 41–56.

[12] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, $\mathbb{ATLAS}$ *of Finite Groups*, Oxford University Press, Oxford, 1985.

[13] H. Davenport, Bases for finite fields, *J. London Math. Soc.* **43** (1968), 21–39; **44** (1969), 378.

[14] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics (163), Springer-Verlag, New York, 1996.

[15] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2004, (http://www.gap-system.org).

[16] D. M. Gordon, *La Jolla Covering Repository*, http://www.ccrwest.org/cover.html.

[17] D. M. Gordon, G. Kuperberg and O. Patashnik, New constructions for covering designs, *J. Comb. Des.* **3** (1995), 269–284.

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

[19] C. Jordan, Sur la limite de transitivité des groupes non-alternées, *Bull. Soc. Math. France* **1** (1873), 40–71.

[20] H. W. Lenstra Jr. and R. J. Schoof, Primitive normal bases for finite fields, *Math. Comp.* **48** (1987), 217–231.

[21] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopædia of Mathematics and its Applications (20), 2nd edition, Cambridge University Press, Cambridge, 1997.

[22] T. Maund, *Bases for permutation groups*, D.Phil. thesis, University of Oxford, 1989.

[23] W. H. Mills, Covering designs. I. Coverings by a small number of subsets, *Ars Combin.* **8** (1979), 199–315.

[24] W. H. Mills and R. C. Mullin, Coverings and packings, in *Contemporary Design Theory: A collection of surveys*, (eds J. H. Dinitz and D. R. Stinson), John Wiley & Sons, New York, 1992.

[25] P. M. Neumann, G. A. Stoy and E. C. Thompson, *Groups and Geometry*, Oxford University Press, Oxford, 1994.

[26] J. G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, 1992.

[27] H. Zassenhaus, Kennzeichnung endlicher linearer als Permutationsgruppen, *Abh. Math. Sem. Hamburg* **11** (1936), 17–40.

[28] H. Zassenhaus, Über endliche Fastkörper, *Abh. Math. Sem. Hamburg* **11** (1936), 187–220.

[29] B. Zil'ber, Finite homogeneous geometries, *Seminarber., Humboldt-Univ. Berlin, Sekt. Math.* **98** (1988), 186–208.