Permutation codes

Peter J. Cameron
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London E1 4NS
UK
p.j.cameron@qmul.ac.uk

Abstract

There are many analogies between subsets and permutations of a set, and in particular between sets of subsets and sets of permutations. The theories share many features, but there are also big differences. This paper is a survey of old and new results about sets (and groups) of permutations, concentrating on the analogies and on the relations to coding theory. Several open problems are described.

It is a pleasure to dedicate this paper to Michel Deza, who was a pioneer in the investigation of permutations from this point of view.

There are many analogies between sets of subsets of $\{1, \ldots, n\}$ and sets of permutations of $\{1, \ldots, n\}$.

In both cases, the objects can be represented by lists of length n (with entries $\{0, 1\}$ for subsets or $\{1, \ldots, n\}$ for permutations, where a permutation is represented in passive form).

In each case, there is a metric structure (Hamming distance) for the lists (where $d(x, y)$ is the number of positions where x and y differ) and an algebraic structure (addition mod 2 or symmetric difference for subsets, composition for permutations).

1 Algebraic substructures

The algebraic substructures are particularly interesting. For subsets, these are the *linear codes* over $\mathbb{F}_2$; for permutations, they are the *permutation groups*. If we are looking for extremal results, they are likely to be much stronger for these than for arbitrary families.

Here is a comparison of the two situations, showing corresponding concepts and parameters of a linear code C and a permutation group G.

One of the most important parameters is the *cardinality* C or G. The cardinality of a linear code is a power of 2 and is at most 2^n; any such power is possible. The order of a permutation group is a divisor of $n!$, but not all divisors occur.

1.1 Bases

A linear code C is a subspace of $\mathbb{F}_2{}^n$, and so has a *dimension* k. We have $|C| = 2^k$.

In a permutation group G, a *base* is a sequence $i_1, \ldots, i_b$ of points whose pointwise stabiliser is the identity. Bases are important in computational group theory since an element of G is uniquely determined by its effect on a base. The connection between base size and order is not as close as for codes:

Proposition 1.1 *If b is the minimum size of a base for G, then*

$$2^b \leq |G| \leq n^b.$$

Proof Let G_j denote the subgroup of G stabilising the first j points in a base. Then $|G_{i-1} : G_i|$ is the size of the orbit of G_{i-1} which contains G_i, and so $2 \leq |G_{i-1} : G_i| \leq n$. Moreover, $G_0 = G$ and $G_b = \{1\}$. $\square$

A base for G is said to be *minimal* if no proper subset is a base, that is, if no point is fixed by the stabiliser of the others. A base is *irredundant* if no point is fixed by the stabiliser of its predecessors. Clearly a base of minimum size is minimal, and a minimal base is irredundant. The argument of the preceding paragraph shows that the inequality $2^b \leq |G| \leq n^b$ holds if b is the size of any irredundant base.

The bases of a linear code satisfy the matroid basis axioms; the bases of a permutation group do not, in general. Indeed, the minimal (or irredundant) bases need not all have the same cardinality. The inequality above shows that, if b is the minimal base size, then any irredundant base has size at most $b \log_2 n$.

There is a simple algorithm to choose an irredundant base: choose points in order, none fixed by the stabiliser of its predecessors, as long as possible. Then we can find a minimal base by deleting points from an irredundant base as long as possible. However, it is NP-hard to find the minimum base size [4].

Blaha [4] devised the *greedy algorithm* for choosing an irredundant base: choose each point in an orbit of maximum size of its predecessors. He showed:

Theorem 1.2 *If a permutation group of degree n has minimum base size b, then the greedy algorithm finds a base of size at most $b \log \log n$.*

Cameron and Fon-Der-Flaass [12] showed:

Theorem 1.3 *The following conditions on a permutation group are equivalent:*

- *the irredundant bases all have the same size;*
- *the irredundant bases are preserved by re-ordering;*
- *the irredundant bases satisfy the matroid basis axioms.*

They called a permutation group satisfying this property an *IBIS group* (for Irredundant Bases of Invariant Size).

Problem Which matroids can arise in this way from IBIS groups?

The matroids which arise from linear codes are precisely those which are representable over $\mathbb{F}_2$. If M is such a matroid, and $2M$ denotes the matroid obtained from M by replacing each element by two parallel elements, then $2M$ is associated with an IBIS group. For if C is the linear code corresponding to M, the group $G(C)$ of permutations of $\{1, \ldots, n\} \times \mathbb{F}_2$ given by

$$G(C) = \{(i, x) \mapsto (i, x + c_i) : c = (c_1, \ldots, c_n \in C\}$$

is the required IBIS group. (This construction of IBIS groups from codes generalises to linear codes over any finite field.)

There are many other interesting examples, including affine spaces. The Mathieu group M_{24} is an IBIS group, and gives rise to an interesting rank 7 matroid which has not had much attention.

In greater generality, we could ask the following question:

Problem What are the combinatorial properties of the irredundant bases (or minimal bases, or bases of minimum cardinality, or bases chosen by the greedy algorithm) for an arbitrary permutation group?

1.2 Minimum weight and minimum degree

For both subsets and permutaitons, the *minimum distance* of the code or group (the minimum distance between distinct elements) is equal to the *minimum weight* (the minimum distance from zero or identity to another element). In the group case, the weight of G is n minus the number of fixed points of G.

The minimum weight d of a code determines its error-correction capability; it can correct up to $\lfloor (d-1)/2 \rfloor$ errors.

The minimum weight of a permutation group is usually called its *minimum degree*. This parameter has been studied since the time of Jordan.

In the final section of the paper we will look more closely at practical aspects.

1.3 Covering radius

A parameter which is in some sense dual to minimum distance is the *covering radius*, the maximum (over all words or permutations x) of the minimum distance from x to the code or group. This is also related to error correction: if more errors occur than the covering radius, then nearest-neighbour decoding will certainly be wrong!

Much is known about this parameter for codes, but comparatively little for permutation groups. Its study was recently begin by Cameron and Wanless [15]. Here are two open problems from this paper, one specific and one more general.

Let $G = \mathrm{AGL}(1,q)$ be the 1-dimensional affine group over $\mathbb{F}_q$:

$$G = \{x \mapsto ax + b : a, b \in \mathbb{F}_q, a \neq 0\}.$$

What is the covering radius of G? It is known [15] that:

Proposition 1.4 *The covering radius of* $\mathrm{AGL}(1,q)$ *is*

$$\begin{cases} q-2 & \textit{if } q \textit{ is even;} \\ q-3 & \textit{if } q \textit{ is odd and not congruent to } 1 \textit{ mod } 6\textit{;} \\ \textit{either } q-3 \textit{ or } q-4 & \textit{in the remaining case.} \end{cases}$$

Problem Remove the remaining ambiguity.

This problem has a geometric interpretation. The covering radius is $q-s$ if and only if there is a set Q of q points in the affine plane over $\mathbb{F}_q$ which meets every horizontal or vertical line in one point and any other line in at most s points, and s is the least such number. To see this, take two distinguished parallel classes ('horizontal' and 'vertical' lines) in the affine plane. Then the points of the plane are coordinatised by $\mathbb{F}_q \times \mathbb{F}_q$, and the remaining lines of the plane are the graphs of the permutations in G. A set of points the graph of a permutation if and only if it meets each horizontal and vertical line in exactly one point.

The second problem arises from the following result from [15]:

Proposition 1.5 *If the permutation group G of degree n is t-transitive, then its covering radius is at most $n-t$.*

In [15] there is a partial characterisation of the groups meeting this bound (for $t > 1$).

Problem Complete this characterisation.

The paper [15] also contains results on covering radius of sets of permutations, which have many combinatorial connections, for example to questions of Ryser and Brualdi on Latin squares. The connection with transversals of Latin squares arises from the following simple observation:

Proposition 1.6 *Let X be the set of rows of a Latin square of order n. Then the covering radius of X is $n-1$ if L possesses a transversal, and $n-2$ otherwise.*

1.4 Strength and degree of transitivity

Another parameter of a code is its *strength* (as an 'orthogonal array'), the largest number t such that, in any t coordinate positions, all possible t-tuples occur equally often as codewords.

Delsarte [17] observed that the strength of a linear code is one less than the minimum weight of the dual code.

Analogously we have the *degree of transitivity* of a permutation group, the largest t for which the group acts transitively on t-tuples of distinct points. This is another parameter whose study goes back to the nineteenth century.

Two differences between strength and degree of transitivity: first, there is no 'dual' permutation group, so Delsarte's result is not available; second, using the Classification of Finite Simple Groups, the degree of transitivity cannot be greater than 5 (apart from the symmetric and alternating groups).

1.5 Weight and support enumerators

The *weight enumerator* of a code is the generating function $\sum a_i x^i$ for the number a_i of words of given weight i. The analogous polynomial for a permutation group is the *support enumerator*. Often it is more natural to count fixed points instead, giving the *fixed point enumerator*, of the above form where a_i is the number of group elements fixing exactly i points.

These polynomials, suitably normalised, are the probability generating functions for the weight, or number of fixed points, of a randomly chosen element of the code or permutation group. The weight enumerator has a huge literature; the support enumerator has been less investigated (see [3]).

Nigel Boston and others [7] showed:

Proposition 1.7 *Let $P_G(x)$ be the fixed point enumerator of G, normalised by dividing by $|G|$, and let $F_G(x)$ be the exponential generating function for the number of orbits of G on i-tuples of distinct points. Then*

$$F_G(x) = P_G(x+1).$$

Note that, if G is the symmetric group S_n, then $F_G(x)$ is the exponential series, truncated to degree n. So $P_G(0) = F_G(-1)$ is the proportion of permutations which are derangements; the Proposition gives a formula for this and shows the classical result that it is close to e^{-1}.

1.6 Other polynomials

According to a theorem of Greene [19], the weight enumerator of a code C is a specialisation of the two-variable *Tutte polynomial* of the matroid whose bases are the bases for the code.

Analogously, the fixed point enumerator of a permutation group is a specialisation of the n-variable *cycle index* $Z(G)$ of the group. This is the polynomial in variables $s_1, \ldots, s_n$ in which the coefficient of a monomial $s_1^{c_1} s_2^{c_2} \cdots$ is the number of elements of G having c_1 cycles of length 1, c_2 cycles of length 2, and so on, normalised by dividing by $|G|$. Clearly, putting all s_i equal to 1 for $i > 1$ gives the normalised fixed point enumerator.

It is tempting to think that these two multivariate polynomials have a common generalisation, at least in some cases. There are some pointers in this direction. See [9], for example.

1.7 Association schemes

Another tool from algebraic combinatorics has been used in coding theory (and to a lesser extent for permutations) to find bounds, namely *association schemes*. This is not the place for an extensive discussion, but I give a brief sketch to indicate some differences between subsets and permutations.

An *association scheme* on a set X is a partition of the set X^2 into r symmetric binary relations $R_1, \ldots, R_r$, one of which is the relation of equality, so that the relation matrices span an algebra over $\mathbb{R}$. These matrices are symmetric and commute, so they are simultaneously diagonalisable; let P be the matrix whose i,j entry is the jth eigenvalue of the ith relation matrix. Then let Q be the inverse of P.

The *inner distribution* of a subset A of X is the r-tuple whose ith component is $|R_i \cap A^2|/|A|$ (the average number of points of A in the ith relation to a given point). Delsarte showed that, if a set A has inner distribution $d = (d_1, \ldots, d_r)$, then $dQ^\top \geq 0$ (that is, all entries of $dQ^\top$ are non-negative); this is the so-called *linear programming bound*.

Delsarte pointed out the importance of association schemes for coding theory. For the *Hamming scheme* $H(n, 2)$, the set X is the set of all n-tuples over the alphabet $\{0, 1\}$; the pair (x, y) belongs to the ith relation if the Hamming distance between x and y is i, for $i = 0, \ldots, n$. The P-matrix of this scheme can be written down explicitly in terms of Krautchouk polynomials. We have $Q = (1/2^n)P^\top$. If d is the inner distribution of a linear code C, then the (non-negative) entries of $dQ^\top$ (that is, of dP) have an interpretation: after normalisation, they give the inner distribution of the dual code $C^\perp$. (This is a statement of the *MacWilliams identities*.)

For permutation groups, the relevant association scheme is the *conjugacy class scheme* of the symmetric group. Recall that a conjugacy class of S_n consists of all elements with given cycle structure. Now we take $X = S_n$, and let $C_1, \ldots, C_m$ be the conjugacy classes, where $m = p(n)$ (the number of partitions of n). For $i = 1, \ldots, m$, the pair (g, h) belongs to relation R_i if $gh^{-1} \in C_i$.

The *character table* of a group G is the matrix whose columns are indexed by the conjugacy classes and whose rows are indexed by the irreducible complex representations of the group; the entry corresponding to a representation P_i and class C_j is the character of P_i on an element of C_j (that is, $\mathrm{Tr}(P_i(g))$, for $g \in C_j$). Now the P-matrix of the association scheme is obtained by multiplying each column by the size of the conjugacy class indexing it and dividing each row by the degree of the representation indexing it, and then taking the transpose.

Patrick Solé pointed out to me that the cycle index polynomial of a permutation group is (apart from a normalising factor) precisely the inner distribution of the group as a subset of the conjugacy class scheme of S_n.

So there is a linear programming bound for sets of permutations. This can be effective in small cases. Tarnanen [24] has given a number of examples of its use for $n \leq 10$. But there are several reasons why this is more complicated than the coding theory case. First, the number of classes of the association scheme is $p(n)$, which is very much larger than n (though still small compared to $n!$). Second, the association scheme is not 'self-dual', that is, $Q \neq (1/|X|)P^\top$. Third, the character table of S_n can be worked out for particular values of n but no general formula is known. Finally, since we do not have duality in this situation, there is no interpretation of the vector $dQ^\top$ in terms of anything resembling a MacWilliams transform.

1.8 Permutation geometries

There is a natural partial order on the subsets of $\{1, \ldots, n\}$: they form the *Boolean lattice*. Is there anything similar for permutations?

There are two approaches here. One is the *Bruhat order*. This depends on an ordering of the set $\{1, \ldots, n\}$. It can be extended to arbitrary Coxeter groups (see [20]).

A completely different answer, and one which is purely combinatorial (and does not depend on ordering the underlying set) was introduced by Deza (see [10]). We enlarge the set of permutations to the set of *subpermutations* or *partial permutations*, the bijections between subsets of $\{1, \ldots, n\}$. The set of subpermutations has two natural structures:

- a partial order, given by inclusion (regarding a subpermutation f as the set $\{(i, i^f) : i \in \mathrm{dom}(f)\}$ of ordered pairs);

- a composition, given by

$$f \circ g = \{(i, j) : (\exists k)((i, k) \in f \text{ and } (k, j) \in g)\}.$$

The partial order is a meet-semilattice but not a lattice: two subpermutations f, g may not have a join since there may be a point i such that i^f and i^g are both defined but are unequal. The operation gives the set of subpermutations the structure of an *inverse semigroup* (the so-called *symmetric inverse semigroup* on $\{1, \ldots, n\}$).

By analogy with the notion of matroid or 'combinatorial geometry', Deza (see [10]) defined a *permutation geometry*. If G is a permutation group which permutes its irredundant bases transitively (a *base-transitive group*), then G is an IBIS group; the restrictions of the elements of G to the flats of the corresponding matroid form a permutation geometry. These structures are the analogues for permutation geometries of the *perfect matroid designs* (see [11]).

Note that the base-transitive groups have been determined by Maund [23], using the Classification of Finite Simple Groups. This result has been used in several places. Zil'ber [25] gave a proof of the determination for base size at least 7 which was heavily geometric but did not use the Classification, for an application in model theory; there is also an application in universal algebra [14].

2 Extremal permutation theory

This theory, much of it due to Michel Deza and his co-authors, takes results of extremal set theory and finds analogues for permutations.

For a simple example, the distances between distinct permutations lie in the set $\{2, 3, \ldots, n\}$. If A is a subset of this set, we let $F_A(n)$ be the maximum cardinality of a set of permutations such that all distances lie in the set A. We denote by $F_A^\circ(n)$ the maximum cardinality of a subgroup of the symmetric group all of whose distances lie in A (equivalently, all of whose weights lie in A).

The metric space admits a transitive group of isometries: both left and right translation by arbitrary permutations are isometries.

The following elementary result relates the values of $F_A(n)$ for various sets n.

Proposition 2.1 *Let G be a transitive permutation group on a set X of cardinality n. Suppose that A and B are subsets of X which satisfy $|A^g \cap B| \leq m$ for all $g \in G$. Then*

$$|A| \cdot |B| \leq |X| \cdot m.$$

Proof Count in two ways the pairs (a, g), with $a \in A$, $g \in G$, and $a^g \in B$. On the one hand there are $|A| \cdot |B|$ choices of (a, b) with $a \in A$ and $b \in B$, and $|G|/|X|$ choices of $g \in G$ with $a^g = b$ (by the Orbit-Stabiliser Theorem). On the other, there are $|G|$ elements of G, and at most m choices of $a \in A$ with $a^g \in B$. $\square$

Corollary 2.2 *If A and B are subsets of $\{2, \ldots, n\}$, then*

$$F_A(n) \cdot F_B(n) \leq n! \cdot F_{A \cap B}(n).$$

In particular, if also $A \cap B = \emptyset$ then $F_A(n)F_B(n) \leq n!$; and equality implies that any sets X_1 and X_2 with distances in A and B respectively which attain the bound satisfy $|X_1 \cap X_2| = 1$.

2.1 General results

For an arbitrary set A, the following holds. This shows clearly that we can expect stronger results for groups than for arbitrary sets! The first part of this result is from [8].

Theorem 2.3 *Suppose that A is a subset of $\{2, \ldots, n\}$ with $|a| = S$.*

(a) $F_A(n) \leq c_1(s)n^{2s}$ for some $c_1(s)$. In the other direction, for suitable sets A, we have $F_A(n) \geq c_0(s)n^{2s}$ for $c_0(s) \neq 0$.

(b) $F_A^\circ(n)$ divides $\prod_{a \in A} a$. In particular, $F_A^\circ(n) \leq n^s$.

It would be interesting to reduce the gap between $c_0(s)$ and $c_1(s)$ in part (a). The ratio of the currently-best bounds is exponential in s. Note too that the sets A in part (b) are arithmetic progressions; does a stronger upper bound hold if A is nothing like an arithmetic progression?

The result of (b) is an old theorem of Blichfeldt [6], rediscovered by Kiyota [22]. He called a permutation group *sharp* if it attains the bound. Various special types of sharp group have been determined by Kiyota and others (for example, [21]).

Problem Classify the sharp permutation groups.

The association scheme method mentioned earlier is potentially relevant to the problem of determining $F_A(n)$: see Tarnanen [24] for some examples of its application.

2.2 The coding problem

Let $F_{\geq d}(n)$ denote the maximum number of permutations which are pairwise at distance at least d. An analogue of the *Singleton bound* from coding theory holds:

$$F_{\geq n-t+1}(n) \leq n(n-1)\cdots(n-t+1).$$

Equality holds if and only if there is a *sharply t-transitive* set of permutations (any t-tuple of distinct points can be carried to any other by a unique permutation in the set).

The existence of sharply t-transitive sets of permutations for $t = 1, 2, 3$ is equivalent to that of certain geometric objects: Latin squares, affine planes, inversive planes respectively. So they always exist, and in great profusion, for $t = 1$; but for $t = 2$ it is a very hard problem!

Better results are known for groups. A sharply 1-transitive group is just an arbitrary group acting in its regular representation. For $t > 1$, all sharply t-transitive groups were determined (by Jordan for $t \geq 4$ and by Zassenhaus for $t = 2$ and for $t = 3$).

2.3 Analogue of Erdős–Ko–Rado

Let $F_{\leq d}(n)$ denote the maximum number of permutations which are pairwise at distance at most d, i.e. any two agreeing in at least $n - d$ points. The following conjecture for the value of this function is due to Deza and Frankl [18], and would be an exact analogue for permutations of the famous Erdős–Ko–Rado theorem for subsets.

Problem Show that, if $n \geq n_0(t)$, then $F_{\leq n-t}(n) \leq (n-t)!$. Show further that any set which attains this bound is a coset of the stabiliser of t points in the symmetric group.

This is true for $t = 1$ [18, 13]. The bound comes immediately from Corollary 2.2 and the fact that $F_{\{n\}}(n) = n$. Moreover, the Corollary also shows that a set attaining the bound contains one row of every Latin square. The structure theorem for such sets uses the fact that Latin squares exist in profusion.

This method will not easily generalise, as Deza and Frankl observed.

For $t = 2$, we know that $F_{\leq n-2}(n) = (n-2)!$ if there exists a projective plane of order n. Of course, the only known orders of projective planes are prime powers; in other words, we only know that $F_{\leq n-2}(n) = (n-2)!$ if n is a prime power. New methods are needed!

This problem concerns the value of $F_{\leq s}(n)$ when s is close to n. At the other end of the range, when s is small, the exact value is known.

If s is even, then the ball of radius $s/2$ about any permutation has all distances at most s, and has cardinality

$$|B_{s/2}(g)| = \sum_{i=0}^{s/2} \binom{n}{i} d(i) \sim c(s)n^{s/2},$$

where $d(i)$ is the number of derangements of an i-set. There is a similar construction for s odd.

Deza and Frankl showed that, if $n \geq n_1(s)$, then these sets have maximum size, and are the only sets which do so.

Problem What happens in the middle of the range, where both s and $n-s$ are large?

3 Permutation groups as codes

To conclude I would like to discuss some recent work by Robert Bailey on another topic introduced by Michel Deza and others [5], concerning the possibility of using a permutation group as an error-correcting code. Whether or not this is ever used in practice, it raises some interesting questions about permutation groups.

Let G be a permutation group of degree n which has minimal degree m. We have seen that G can correct up to e errors, where $e = \lfloor (m-1)/2 \rfloor$.

Suppose that we use G as a code over the alphabet $\{1, \ldots, n\}$. Let $(i_1, \ldots, i_b)$ be a base. An element of G is uniquely determined by its values on $i_1, \ldots, i_b$. So, if we knew that the entries in the received word in these positions were correct, then we could calculate the transmitted word uniquely using techniques of computational group theory.

Of course, we don't know this, so we need more than one base. A set $\mathcal{B}$ of bases for G is said to be an *uncovering by bases* (or *UBB*) if, for every set E of points of cardinality $e = \lfloor (m-1)/2 \rfloor$, there is a base $B \in \mathcal{B}$ such that $E \cap B = \emptyset$.

Thus, if we have an uncovering by bases, then we can decode: check bases in turn until we find one yielding a transmitted word distant at most e from the received word.

A UBB resembles a covering design, with two differences. First, we uncover rather than cover; so we have to take the complements of the blocks of a covering design. Second, we insist that all these uncovering sets should be bases.

An easy argument (given later) shows that, for any permutation group G, there is a UBB for G. Two features which would make the decoding algorithm more efficient are: a small UBB; and a UBB whose bases belong to a single G-orbit.

Problem Let G be a permutation group of degree n. Show that there is a UBB for G such that

- its size is bounded by a low-degree polynomial in n;
- it is contained in a single orbit of G on bases.

Bailey conjectures that such a UBB always exists. The second part is his 'single-orbit conjecture'. Both parts have been proved for a variety of permutation groups, by a variety of group-theoretic and combinatorial techniques; see [1, 2].

Usually, error patterns with a small number of errors are most likely. So we can improve the average run-time of the decoding algorithm if we can find a UBB $\mathcal{B} = \mathcal{B}_e$ containing a chain of subsets

$$\mathcal{B}_1 \subseteq \mathcal{B}_2 \subseteq \ldots \subseteq \mathcal{B}_e$$

such that

- $\mathcal{B}_i$ is a UBB for sets of size i;
- $|\mathcal{B}_i|$ is (close to) optimal for such a design.

Problem Do UBBs with this property exist?

This is an interesting question even with no reference to bases (i.e. for general covering designs).

The single-orbit conjecture can be quantified, to define a new parameter of a permutation group G. Define $\kappa(G)$ to be the largest number k for which the following holds:

> There is a base B for G such that, for every k-set A, there exists $g \in G$ with $A \cap B^g = \emptyset$.

In other words, $\kappa(G)$ is the largest cardinality of sets which can be 'uncovered' by bases from a single orbit.

Without the single-orbit requirement, the value of this parameter would be known:

Proposition 3.1 *Let G be a permutation group.*

(a) The largest number k for which, given a k-set, there is a base for G disjoint from it, is one less than the minimum degree $\mu(G)$ of G.

(b) We have $\kappa(G) \leq \mu(G) - 1$; equality holds if G permutes its minimal bases transitively.

Proof The first part is immediate from the fact that, given a set A, there is a base for G disjoint from A if and only if there is no non-identity element of G whose support is contained in A. The second follows from this. $\square$

With this notation, the single-orbit conjecture is the assertion that $\kappa(G) \geq \lfloor (\mu(G) - 1)/2 \rfloor$.

References

[1] R. F. Bailey, Uncoverings-by-bases for base-transitive permutation groups, *Designs, Codes and Cryptography* **41** (2006), 153–176.

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

[3] R. F. Bailey and J. P. Dixon, Distance enumerators for permutation groups, *Communications in Algebra*, to appear.

[4] K. D. Blaha, Minimal bases for permutation groups: the greedy approximation, *Journal of Algorithms* **13** (1992), 297–306.

[5] I. F. Blake, G. Cohen and M. Deza, Coding with permutations, *Information and Control* **43** (1979), 1–19.

[6] H. F. Blichfeldt, A theorem concerning the invariants of linear homogeneous groups, with some applications to substitution groups, *Trans Amer. Math. Soc.* **5** (1904), 461–466.

[7] N. Boston, W. Dabrowski, T. Foguel, P. J. Gies, J. Leavitt, D. T. Ose and D. A. Jackson, The proportion of fixed-point-free elements of a transitive permutation group, *Communications in Algebra* **21** (1993), 3259–3275.

[8] P. J. Cameron, Metric and geometric properties of sets of permutations, pp. 39–53 in *Algebraic, Extremal and Metric Combinatorics* (M.-M. Deza, P. Frankl & I. G. Rosenberg, eds.), London Math. Soc. Lecture Notes **131**, Cambridge University Press, Cambridge, 1988.

[9] P. J. Cameron, Cycle index, weight enumerator and Tutte polynomial, *Electronic J. Combinatorics* **9** (2002), #N2 (10pp), available from `http://www.combinatorics.org`

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

[11] P. J. Cameron and M. Deza, Designs and Matroids, in *Handbook of Combinatorial Designs*, 2nd edition (ed. C. J. Colbourn and J. Dinitz), Discrete Mathematics and its Applications **42**, Chapman & Hall/CRC, 2006, Chapter VII.10 (pp.847–851).

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

[13] P. J. Cameron and C. Y. Ku, Intersecting families of permutations, *European J. Combinatorics* **24** (2003), 881–890.

[14] P. J. Cameron and C. Szabó, Independence algebras, *J. London Math. Soc.* (2) **61** (2000), 321–334.

[15] P. J. Cameron and I. M. Wanless, Covering radius for sets of permutations, *Discrete Math.* **293** (2005), 91–109.

[16] Ph. Delsarte, The association schemes of coding theory, *Philips Res. Repts. Suppl.* **10** (1973).

[17] Ph. Delsarte, Four fundamental parameters of a code and their combinatorial significance, *Information and Control* **23** (1973), 407–438.

[18] M. Deza and P. Frankl, On the maximum number of permutations with given maximal or minimal distance, *J. Combinatorial Theory*, (A) **22** (1977), 352–360.

[19] C. Greene, Weight enumeration and the geometry of linear codes, *Studies in Applied Math.* **55** (1976), 119–128.

[20] J. E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge University Press, Cambridge, 1990.

[21] T. Ito and M. Kiyota, Sharp permutation groups, *J. Math. Soc. Japan* **33** (1981), 435–444.

[22] M. Kiyota, An inequality for finite permutation groups, *J. Combinatorial Theory* (A) **27** (1979), 119.

[23] T. Maund, *Bases for Permutation Groups*, D. Phil. thesis, Oxford University, 1989.

[24] H. Tarnanen, Upper bounds on permutation codes via linear programming, *Europ. J. Combinatorics* **20** (1999), 101–114.

[25] B. Zil'ber, The structure of models of uncountably categorical theories, pp. 359–368 in *Proc. Internat. Congr. Math.* (Warsaw 1983).