Permutations and codes:

Polynomials, bases, and covering radius

Peter J. Cameron

Queen Mary, University of London
p.j.cameron@qmw.ac.uk

International Conference on Graph Theory
Bled, 22–27 June 2003

Binary codes and sets of permutations

We will be considering sets of n-tuples over an alphabet A, in two important cases:

- $A = \{0,1\}$ (binary code);
- $A = \{1,\dots,n\}$, all entries of each word distinct (set of permutations).

We often impose *closure conditions* on these sets, as follows:

- A binary code is *linear* if it is closed under coordinatewise addition mod 2.
- A set of permutations is a *group* if it is closed under composition.

Hamming distance

Hamming distance $d(x,y)$ is the number of coordinate positions where two words differ. It is a metric on the set of words.

In the binary case,

$$d(x,y) = \mathrm{wt}(x-y),$$

so for a linear code, minimum distance equals smallest number of non-zero coordinates of a non-zero element (*minimum weight*).

In the permutation group case,

$$d(x,y) = n - \mathrm{fix}(x^{-1}y),$$

so, for a permutation group, minimum distance equals smallest number of points moved by a non-identity element (*minimal degree*).

An apology

This is not really graph theory: the distance between permutations is not a graph distance, because there do not exist two permutations at distance 1.

However, it is closely related to the distance d' in the *Cayley graph* of the symmetric group with respect to the set of transpositions: we have

$$d(g,h)/2 \le d'(g,h) \le d(g,h) - 1$$

for $g \neq h$.

Also, we will be considering the size of the smallest *dominating set* in the graph $G_{n,k}$ with vertex set S_n, two permutations joined if they agree in at least k places.

Some analogies

Linear code	Permutation group
length	degree
minimum weight	minimal degree
weight enumerator	permutation character
Tutte polynomial	cycle index
basis	base
dimension	base size
covering radius	??

Groups as codes

The idea of coding with permutations goes back to Blake, Cohen and Deza in the 1970s.

Among their suggestions was that the Mathieu group M_{12} would be a good code (comparable to a Reed–Solomon code). It has minimal degree 8, so is 3-error-correcting.

Recently, R. F. Bailey showed that it corrects about 96% of all four-error patterns.

Also, it is easy to decode, using efficient algorithms for permutation groups. Bailey's decoding algorithm uses a covering design to give a collection of 5-sets such that at least one is disjoint from each error pattern. Then find the unique element of M_{12} agreeing with the received word on that 5-set.

Bases for permutation groups

Let G be a permutation groups. A *base* is a sequence of points whose pointwise stabiliser is the identity. It is *irredundant* if no point is fixed by the stabiliser of its predecessors, and is *minimal* if no point is fixed by the stabiliser of all the others.

Note that changing the order preserves the properties of being a base and minimality, but not necessarily irredundance. However, computationally it is easy to produce an irredundant base but much harder to find a minimal base.

IBIS groups

The following are equivalent for the permutation group G:

- all irredundant bases have the same number of elements;
- the irredundant bases are preserved by reordering;
- the irredundant bases are the bases of a matroid.

A group with these properties is called an *IBIS group* (**I**rredundant **B**ases of **I**nvariant **S**ize).

Examples of IBIS groups

Any linear code C of length n gives an IBIS group with essentially the same matroid, as follows. The set of points permuted is $\{1,\ldots,n\} \times \mathrm{GF}(2)$; the group is the additive group of C; the action is

$$c : (i,x) \mapsto (i,x+c_i).$$

The matroid is just the usual matroid of the code with each element 'doubled'.

There are many other examples: symmetric and alternating groups; linear and affine groups; linear fractional groups; and many sporadic ones.

A group which permutes its irredundant bases transitively is an IBIS group. Such groups were determined by Maund (using the Classification of Finite Simple Groups).

Polynomials

A permutation group has a *cycle index* polynomial. If it is an IBIS group, it is associated with a matroid, which has a *Tutte polynomial*.

Sometimes (e.g. for the groups obtained from linear codes) the cycle index is a specialisation of the Tutte polynomial; sometimes (e.g. for base-transitive groups) it is the other way round.

It is possible to define a more general polynomial, the *Tutte cycle index*, which specialises to the cycle index and (in the case of an IBIS group) also to the Tutte polynomial. Its properties haven't been investigated systematically.

The Tutte cycle index

The Tutte cycle index of a permutation group G on Ω is

$$ZT(G) = \frac{1}{|G|} \sum_{\Delta \subseteq \Omega} u^{|G_\Delta|} v^{b(G_{(\Delta)})} Z(G[\Delta]).$$

Here G_Δ is the setwise stabiliser of Δ, $G_{(\Delta)}$ its pointwise stabiliser, $G[\Delta] \cong G_\Delta / G_{(\Delta)}$ the group induced on Δ by G_Δ, and b is the minimum base size.

To get the cycle index: differentiate with respect to u, put $u = v = 1$, and replace s_i by $s_i - 1$.

To get the Tutte polynomial (if G is IBIS): put $u = 1$ and $s_i = t^i$. (The result is actually $T(M; v/t+1, t+1)$.)

The geometry of bases

We have seen that, in an IBIS group, the irredundant (or minimal) bases satisfy the matroid basis axioms.

What kind of configuration do they form in more general cases (when the two kinds may not coincide)? In particular, we may ask this question in two special cases:

- What if all minimal bases have the same cardinality?
- What if the irredundant bases have cardinalities differing by one?

The *greedy algorithm* produces an irredundant base by choosing each base point to lie in an orbit of largest size of the stabiliser of its predecessors. We can also ask whether the *greedy bases* (produced in this way) have nicer properties than arbitrary irredundant bases.

An example: S_5 on pairs

An example satisfying both conditions on the preceding slide is the symmetric group S_5 acting on the ten edges of the complete graph K_5.

A minimal base consists of the three edges of a forest with one isolated vertex and one 4-vertex tree. The minimal bases are not the bases of a matroid in this case. (For $B = \{12, 23, 34\}$ is a base; $I = \{12, 45\}$ is contained in a base, but it is not possible to add an element of B to it to form a base.) Note that the permutation group bases are *some* of the bases of the cycle matroid of K_5 truncated to rank 3.

The 4-tuple $(12, 45, 23, 34)$ is an irredundant base which is not minimal.

The greedy algorithm always produces a minimal base in this example. (This is not always the case!)

Base sizes

The largest irredundant base has size at most $\log_2 n$ times that of the smallest. Indeed, if G has an irredundant base of size b, then

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

The largest base chosen by the greedy algorithm has size at most $(\log\log n + c)$ times that of the smallest base.

It is conjectured that both these ratios are much smaller for *primitive* permutation groups; in particular, it is conjectured that a greedy base has size at most $9/8 + o(1)$ times the minimum base size in a primitive group.

There is a relation between base size $b(G)$ and minimal degree $\mu(G)$. Since any base meets the support of any non-identity element, it follows that in a transitive group G we must have

$$b(G) \cdot \mu(G) \geq n.$$

Base sizes

Imre Leader asked:

> Do the base sizes of a permutation group form an interval?

The answer is ‘no’ for minimal bases. The group C_2^3, with three orbits of size 2 and one regular orbit of size 8, has minimal bases of size 1 (a point in the regular orbit) and 3 (one point in each orbit of size 2) only.

However, it is true for irredundant bases: if a group has irredundant bases of sizes m_1 and m_2, then it has irredundant bases of all intermediate sizes.

What happens for greedy bases? (Note that the greedy algorithm is not deterministic since at some point there may be several largest orbits.)

Covering radius

Let S be a subset of a finite metric space M. The *packing radius* of S is the maximum r such that the balls of radius r with centres at points of S are pairwise disjoint; the *covering radius* is the minimum R such that the balls of radius R cover M. Under fairly weak assumptions, $r \leq R$.

The covering radius is thus

$$R = \max_{x \in M} \min_{y \in S} d(x, y).$$

We now look at covering radius of subsets (and subgroups) of the symmetric group, with the Hamming distance.

The covering bound

If

$$|S| < \frac{n!}{|B_d|},$$

where B_d is the number of permutations which move d or fewer points, then the covering radius of S is at least $d+1$: the balls of radius d don't contain all the permutations.

This bound is quite poor. For example, it doesn't even show that a set of two permutations has covering radius n, even though much more is true:

Theorem (Kézdy–Snevily) Any set of at most $\lfloor n/2 \rfloor$ permutations in S_n has covering radius n. This is best possible.

No analogous result holds for binary codes. The repetition code contains only two codewords, but its covering radius is only $\lfloor n/2 \rfloor$. The covering bound is met for odd n.

Proof

Let S be a subset of S_n, with $|S| = k$. Let A_i be the set of elements of $\{1, \ldots, n\}$ which are not the image of i under any permutation in S. Then a permutation at distance n from S is a system of distinct representatives of the sets $A_1, \ldots, A_n$; so we will apply Hall's Theorem. For $I \subseteq \{1, \ldots, n\}$, put $A(I) = \bigcap_{i \in I} A_i$.

Clearly $|A_i| \geq n-k$ for all i; so $|A(I)| \geq |I|$ if $|I| \leq n-k$.

Each element j occurs at most k times in the permutations in S, so at least $n-k$ of the sets A_i contain j. Thus, if $|I| > k$, then $j \in A(I)$, and so $|A(I)| = n$.

If $k \leq n/2$, then these two possibilities cover all cases.

An extremal problem

Let $f(n,s)$ be the largest number m with the property that any set of at most m permutations in S_n has covering radius $n-s$ or greater.

The result of Kézdy and Snevily shows that

$$f(n,0) = \lfloor n/2 \rfloor.$$

Apart from this and the trivial values $f(n,n) = n!$, $f(n,n-2) = n! - 1$, very few exact results are known.

Kézdy and Snevily have made the following conjecture:

Conjecture If n is even, then $f(n,1) = n-1$; if n is odd, then $f(n,1) \geq n$.

Latin squares

The rows of a Latin square form a *sharply transitive set* of permutations, and every sharply transitive set arises in this way.

The covering radius of a sharply transitive set in S_n is at most $n-1$, with equality if and only if the Latin square has a transversal.

It is known that, for every even n, there is a Latin square (the Cayley table of the cyclic group) which has no transversal. Ryser conjectured that every Latin square of odd order has a transversal. Some random search, using the Jacobson–Matthews Markov chain for random Latin squares and Leonard Soicher's DESIGN package to search for transversals, has failed to find a counterexample to Ryser's conjecture. Note that the Kézdy–Snevily conjecture implies Ryser's.

Examples

The first Latin square has a transversal, and a permutation at distance $n-1$ from its rows is shown. The second Latin square has a partial transversal of size $n-1$, and a permutation at distance $n-2$ from its rows is shown.

$\boxed{1}$	2	3	4	5
2	$\boxed{3}$	4	5	1
3	4	$\boxed{5}$	1	2
4	5	1	$\boxed{2}$	3
5	1	2	3	$\boxed{4}$
1	3	5	2	4

$\boxed{1}$	2	3	4	5	6
2	$\boxed{3}$	4	5	6	1
3	4	$\boxed{5}$	6	1	2
4	5	6	1	2	3
5	6	1	$\boxed{2}$	3	4
6	1	2	3	$\boxed{4}$	5
1	3	5	2	4	6

Brualdi's conjecture and covering radius

Brualdi conjectured that every Latin square has a partial transversal of size at least $n-1$. Derienko claimed a proof of this conjecture. However, Wanless has found a mistake in the proof. The best known lower bound is $n-\sqrt{n}$ by Woolbright.

The Kézdy–Snevily conjecture implies Brualdi's conjecture.

If there is a transversal, then the covering radius is $n-1$; otherwise it is $n-2$ (Cameron and Wanless, in preparation). This assertion is weaker than Brualdi's conjecture.

Latin squares and $f(n,1)$

In any case, we have the following:

Proposition If there is a Latin square of order n with no transversal (in particular, if n is even), then $f(n,1) \leq n-1$.

The best lower bound I know for $f(n,1)$ is $\lfloor n/2 \rfloor + 1$.

Ian Wanless has shown that $f(n,1) = n$ for $n = 5,7,9$; that $f(4k+1,1) \leq 5k+1$; and that, if k is even and $n/3 < k \leq n/2$, then $f(n,1) \leq n+k-1$. The method is to take a Latin square with 'few' transversals and add some permutations meeting each transversal twice.

Thus, for odd n, we have $f(n,1) \leq \frac{4}{3}n + O(1)$, with better results in some cases.

Permutation groups

More is known about the covering radius of permutation groups. For example:

Theorem A subgroup of S_n has covering radius n if and only if all its orbits have size at most $n/2$.

Corollary The covering radius of a transitive permutation group is at most $n-1$.

For regular permutation groups, the bound $n-1$ is attained if and only if the Cayley table of the group has a transversal. This is equivalent to the existence of a *complete mapping* of the group. A criterion for all transitive groups is not known.

Corollary The covering radius of a t-transitive permutation group is at most $n-t$.

Groups attaining the bound

Problem Which t-transitive permutation groups have covering radius exactly $n-t$?

For $t \geq 2$, the answer is not completely known, but such groups are restricted to fairly short lists of possibilities for $t=2$ and $t=3$, as well as the alternating groups ($t=n-2$) and symmetric groups ($t=n$).

For some of the groups on these lists, the covering radius is known to be $n-t$; in other cases this has not been determined.

A curiosity: Of the 49 multiply-transitive groups of degree at most 12, all have even covering radius except two (these are $\mathrm{A\Gamma L}(1,8)$ and $\mathrm{AGL}(2,3)$, both with covering radius 5).

The cases $t=2,3$

For $t=2$, groups meeting the bound are among the list

- $G \leq \mathrm{A\Gamma L}(1,q)$, where q is a power of 2;
- $\mathrm{ASL}(2,q) \leq G \leq \mathrm{A\Gamma L}(2,q)$, where q is a power of 2;
- G has a normal subgroup $\mathrm{PSL}(2,q)$ or $\mathrm{PSU}(3,q)$ (for q an odd prime power) or a Ree group ${}^2G_2(q)$ (for q an odd power of 3).

For $t=3$, they satisfy

$$\mathrm{PGL}(2,q) \leq G \leq \mathrm{P\Gamma L}(2,q),$$

where q is a power of 2.

We note that groups meeting the bound do have even covering radius! A direct proof would be nice.

An example: Suzuki groups

As an example, I outline the proof that the 2-transitive Suzuki groups do not have covering radius $n-2$.

In a transitive group G, the average distance of the elements from an arbitrary permutation is $n-1$ (this is an analogue of the Orbit-Counting Lemma). So, if the covering radius is $n-1$ and $d(g,G)=n-1$, then $d(g,h)=n-1$ for all $h \in G$.

It follows that, if G is 2-transitive and $d(g,G)=n-2$, then $d(g,h)=n-2$ or n for all $h \in G$, with half the elements taking each value. The same holds for any uniformly transitive subset of G.

If $G=Sz(q)$, then the involutions in G form a uniformly transitive subset of odd cardinality, so this is not possible.

Covering radius of $\mathrm{PGL}(2,q)$

The covering radius of the group $\mathrm{PGL}(2,q)$ of linear fractional transformations over $\mathrm{GF(q)}$ is

$$\begin{cases} q-2 & \text{if } q \text{ is a power of } 2,\\ q-3 & \text{if } q \equiv 3 \text{ or } 5 \bmod 6,\\ q-3, q-4 & \text{if } q \equiv 1 \bmod 6.\\ \quad \text{or } q-5 & \end{cases}$$

The upper bounds follow from arguments like those above. For the lower bounds, consider first q even. Then $x \mapsto x^2$ is a permutation, and it is easily shown that it agrees with any linear fractional transformation in at most 3 points (the equation $x^2=(ax+b)/(cx+d)$ is a cubic). Similarly, if q is not congruent to 1 mod 6, we use the permutation $x \mapsto x^3$.

Question What is the covering radius of $\mathrm{PGL}(2,q)$ for $q \equiv 1$ mod 6? (It is known to be $q-3$ for $q=7,13$, and either 15 or 16 for $q=19$.)

A geometric formulation

Consider the *Minkowski plane* or ruled quadric over $\mathrm{GF}(q)$ Let S be a set of $q+1$ points which contains one point on each generator. What is the smallest value of s for which such a set exists with at most s points on each conic?

The covering radius of $\mathrm{PGL}(2,q)$ is $q+1-s$, where s is the above minimal value. Hence the answer is $s=3$ for q even, $s=4$ for q odd and not congruent to 1 mod 6, and $4 \le s \le 6$ in the remaining cases.

Packing and covering

We noted that the packing radius r and covering radius R satisfy $r \le R$ under mild conditions. Is R bounded above by a function of r?

No such bound can hold in general, and we are led to restrict the question to *primitive* permutation groups.

In this case, the existence of such a bound was proved by Jordan in the nineteenth century. (Jordan actually showed that the degree of a primitive group is bounded by a function of its minimal degree.)

However, a construction based on Steiner triple systems shows that no *linear* bound can hold in general.

Analogues of extremal set theory

Let $A \subseteq \{0,\ldots,n-2\}$. A subset S of S_n is A-*intersecting* if $\mathrm{fix}(gh^{-1}) \in A$ for all $g,h \in S$ (that is, all Hamming distances in S are of the form $n-a$ for $a \in A$).

We write $F(n,A)$ for the cardinality of the largest A-intersecting set of permutations of $\{1,\ldots,n\}$. Moreover, we write for short $F(n, \le s)$ and $F(n, \ge s)$ with the obvious meaning.

Clearly,

$$F(n,\le s) \le n(n-1)\cdots(n-s+1),$$

with equality if and only if a sharply s-transitive set exists. Such sets are equivalent to Latin squares for $s=1$, but are quite rare for $s>1$. For example, a sharply 2-transitive set is ‘equivalent’ to a projective plane of order n; examples are known only for prime powers n.

Intersecting sets of permutations

Deza and Frankl showed that

$$F(n, \ge 1) = (n-1)!.$$

Very recently, Cameron and Ku showed that an intersecting set of permutations which attains this bound must be a coset of the stabiliser of a point in the symmetric group.

In view of this, it is natural to conjecture that, for $n \ge n_0(s)$, we have

$$F(n, \ge s) = (n-s)!,$$

and that a set meeting the bound is a coset of an s-point stabiliser. However, even the bound has only been proved in very special cases (for example, $s=2$, n a prime power, using the existence of sharply 2-transitive sets in this case).