Covering radius for sets of permutations

Peter J. Cameron [a,1] Ian M. Wanless [b,c]

[a] *School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK*

[b] *Christ Church, St Aldates, Oxford OX1 1DP, UK*

[c] *Department of Computer Science, Australian National University, ACT 0200, Australia*

Abstract

We study the covering radius of sets of permutations with respect to the Hamming distance. Let $f(n, s)$ be the smallest number m for which there is a set of m permutations in S_n with covering radius $r \leq n - s$. We study $f(n, s)$ in the general case and also in the case when the set of permutations forms a group.

We find $f(n, 1)$ exactly and bounds on $f(n, s)$ for $s > 1$. For $s = 2$ our bounds are linear in n. This case relates to classical conjectures by Ryser and Brualdi on transversals of Latin squares and to more recent work by Kezdy and Snevily. We discuss a flaw in Derienko's published proof of Brualdi's conjecture. We also show that every Latin square contains a set of entries which meets each row and column exactly once while using no symbol more than twice.

In the case where the permutations form a group, we give necessary and sufficient conditions for the covering radius to be exactly n. If the group is t-transitive, then its covering radius is at most $n - t$, and we give a partial determination of groups meeting this bound.

We give some results on the covering radius of specific groups. For the group $\mathrm{PGL}(2, q)$, the question can be phrased in geometric terms, concerning configurations in the Minkowski plane over $\mathrm{GF}(q)$ meeting every generator once and every conic in at most s points, where s is as small as possible. We give an exact answer except in the case where q is congruent to 1 mod 6.

The paper concludes with some remarks about the relation between packing and covering radii for permutations.

Key words: permutations, covering radius, dominating sets, multiply transitive groups, Latin squares, affine planes, Minkowski planes, Steiner triple systems

[1] Corresponding author.

1 Introduction

Let S be a subset of a finite metric space M, in which all the distances are integers. The *covering radius* $\mathrm{cr}(S)$ of S is the smallest R such that the balls of radius R with centres at the elements of S cover the whole space. Compare this with the *packing radius*, the largest r such that the balls of radius r with centres at the elements of S are pairwise disjoint. Under mild assumptions on the metric space, we have $r \le R$.

Alternatively, if we define $d(x, S) = \min_{s \in S} d(x, s)$, then the covering radius is the maximum of $d(x, S)$ over all points x in the space.

The "main problem" of coding theory is to find the largest set S with given packing radius. One question considered here is the dual problem: to find the smallest set with given covering radius. We also consider briefly (in the last section) the problem of bounding the covering radius by a function of the packing radius.

The metric space here is the *symmetric group* S_n, with *Hamming distance*: the distance between g and h is $n - \mathrm{fix}(gh^{-1})$. Note that it is invariant under left and right translation. The symmetric group has been studied as a setting for coding theory since the paper of Blake *et al.* [2]; but little attention has been given to questions about covering radius.

We write i^g for the image of $i \in \{1, \ldots, n\}$ under $g \in S_n$ (regarding g as a function). The passive form of g is the word $1^g 2^g \cdots n^g$.

There is one small complication: since no two permutations have Hamming distance 1, a ball of radius 1 consists of a single element. So, according to the definition, if S contains two permutations at distance 2, its packing radius is 1. To simplify things later, we disallow balls of radius 1 and assume that in this case the packing radius is 0.

Much more about covering radius can be found in the book [5], although the context is different.

We begin with a result of Cameron and Ku [4] and, independently, Kézdy and Snevily [14].

Theorem 1 *Let S be a set of permutations. If $|S| \le n/2$, then $\mathrm{cr}(S) = n$. This is best possible: if $k > n/2$, then there exists S with $|S| = k$ and $\mathrm{cr}(S) < n$.*

PROOF. Suppose that $|S| = k \le n/2$. To show that S has covering radius n, we must find a permutation g such that g has no agreements with any of the

permutations in S. So let

$$A_i = \{1, \ldots, n\} \setminus \{i^h : h \in S\}.$$

Then by assumption $|A_i| \geq n - k$ for all i. The required permutation will be a system of distinct representatives for $(A_1, \ldots, A_n)$; so we must verify that the hypotheses of Hall's theorem are satisfied. So, for $J \subseteq \{1, \ldots, n\}$, let $A(J) = \bigcup_{i \in J} A_i$. We must show that $|A(J)| \geq |J|$ for any set J.

This statement is clearly true if $|J| \leq n - k$, so suppose that $|J| > n - k \geq k$. An arbitrary element j occurs k times as the image of a permutation in S, so has at least $n - k$ occurrences in the sets A_i. So any given set of more than k of them must contain an occurrence of j. So $A(J) = \{1, \ldots, n\}$, and clearly the conclusion holds.

To show that this is best possible, suppose that $k \leq n < 2k$. Take a Latin square of order k, and extend each of its rows to a permutation of $\{1, \ldots, n\}$ fixing the points $k + 1, \ldots, n$. Now the sets $A_1, \ldots, A_k$ each consist of the points $k + 1, \ldots, n$; so $A(\{1, \ldots, k\}) = \{k + 1, \ldots, n\}$, and Hall's condition fails. If $k > n$, then take n permutations chosen as above; adding any $k - n$ further permutations cannot increase the covering radius. □

2 Smallest set with at least a given covering radius

2.1 The problem

Theorem 1 suggests the following problem:

Problem 2 *Given n and s, what is the smallest m such that there is a set S of permutations with $|S| = m$ and $\mathrm{cr}(S) \leq n - s$? We let $f(n, s)$ denote this minimum value m.*

Of course, it is equivalent to consider the function $g(n, s)$ defined to be the largest number m such that any set S of at most m permutations of an n-set has covering radius at least $n - s$. Clearly $f(n, s) = g(n, s - 1) + 1$. In coding theory the analogue of the function f is usually considered; but in other parts of extremal combinatorics such as Ramsey theory, the function considered is the analogue of g.

We note also that this question can be interpreted in graph-theoretic language. Define the graph $G_{n,s}$ on the vertex set S_n, with two permutations being adjacent if they agree in at least s places. Now the size of the smallest dominating

set in $G_{n,s}$ is $f(n,s)$.

Theorem 1 shows that $f(n,1) = \lfloor n/2 \rfloor + 1$. Since any two distinct permutations have distance at least 2, we see that $f(n,n-1) = n!$ for $n \geq 2$. Moreover, $f(n,s)$ is a monotonic increasing function of s (by definition).

The next case to consider is $f(n,2)$. Kézdy and Snevily [14] made the following conjecture, which we consider further in the next subsection.

Conjecture 3 *If n is even, then $f(n,2) = n$; if n is odd, then $f(n,2) > n$.*

We conclude this section by extending the argument of Theorem 1 to give a very weak lower bound for $f(n,2)$, improving by 1 the trivial $f(n,2) \geq f(n,1)$.

Proposition 4 *$f(n,2) \geq \lfloor n/2 \rfloor + 2$ for $n > 2$.*

PROOF. Assume first that n is odd, say $n = 2k+1$, and let S be a set of permutations with $|S| = k+1$. As in Theorem 1, we have $|A(J)| \geq k$ for all non-empty J, and $A(J) = \{1, \ldots, n\}$ if $|J| \geq k+2$. So the only possible failure of Hall's condition is that there could be a set J with $|J| = k+1$ and $|A(J)| = k$. Now $|A(J)| \geq |J| - 1$ for all sets J. By the 'defect form' of Hall's Theorem, there is a partial SDR of size $n-1$. This extends uniquely to a permutation, which agrees with any element of S in at most one position.

Now assume that $n = 2k$ and $|S| = k+1$. The argument using the defect form of Hall's theorem can only fail if there is a set J with $|J| = k+1$ and $|A(J)| = k-1$. Suppose without loss of generality that $J = \{1, \ldots, k+1\}$ and $A(J) = \{k+2, \ldots, 2k\}$. Then the matrix with rows S has a Latin square of order $k+1$ in the first $k+1$ columns. Choose two columns of the Latin square, and select two cells in these columns lying in distinct rows and containing distinct entries. (This choice is possible if $k+1 \geq 3$.) Now let g be any permutation with these entries in these columns, entries $k+1, \ldots, 2k$ in the remaining $k-1$ of the first $k+1$ columns, and the unused entries from $1, \ldots, k+1$ in the last $k-1$ columns. Then g agrees with two elements of S in one position and the others in no positions. □

2.2 Latin squares

The Kézdy–Snevily conjecture, described in the preceding section, has several connections with Latin squares. The rows of a Latin square of order n form a *sharply transitive set* of permutations (that is, exactly one permutation carries i to j, for any i and j); and every sharply transitive set is the set of rows of a Latin square.

A *transversal* of a Latin square of order n is a set of n cells, one in each row, one in each column, and one containing each symbol. A *partial transversal* is a set of cells with no two in the same row or column or containing the same symbol. The connection with covering radius is given by the following result:

Proposition 5 *Let S be a sharply transitive subset of S_n. Then S has covering radius at most $n-1$, with equality if and only if the corresponding Latin square has a transversal.*

PROOF. For any given position i, any permutation must agree at i with some element of S, so the covering radius cannot exceed $n-1$. If equality holds, let h be a permutation at distance $n-1$ from S; then for each i there is a unique element $s \in S$ with $i^s = i^h$. The positions of these agreements form a transversal of the Latin square, since by construction they involve different columns and symbols, and if two of them lay in the same row then that row would have distance less than $n-1$ from h. Conversely, a transversal of the Latin square gives rise to a permutation at distance $n-1$ from S. □

Corollary 6 *If there exists a Latin square of order n with no transversal, then $f(n,2) \leq n$. In particular, this holds for n even.* □

The existence of a transversal, in the case of the Cayley table of a group, is equivalent to the existence of a complete mapping, or orthomorphism, of the group. Hall and Paige [13] showed that having trivial or non-cyclic Sylow 2-subgroup is necessary and (in the case of soluble groups) sufficient for this.

In particular, if n is even, the Cayley table of the cyclic group C_n of order n has no transversal, and so $f(n,2) \leq n$. (The easy proof is as follows. Suppose that there is a transversal, and let r, c, and s be the sums (in C_n) of the row, columns, and symbols of the transversal. Since each row occurs once, $r = n(n+1)/2 = n/2$. Similarly $c = s = n/2$. But, by definition of the Cayley table, $r + c = s$, a contradiction.)

The Cayley table of C_n does possess a transversal if n is odd (the cells (i,i) form a transversal), and has a partial transversal of size $n-1$ if n is even (the cells (i,i) for $0 \leq i < n/2$, and the cells $(i,i+1)$ for $n/2 \leq i < n-1$).

It was conjectured by Ryser that a Latin square of odd order has a transversal; this is still open. (Incidentally, the fact that a Latin square of even order has an even number of transversals was proved by Balasubramanian [1]. The author was aiming to prove a strong form of the Ryser Conjecture, namely that the number of transversals of a Latin square of order n is congruent to n modulo 2. However, this conjecture and a stronger conjecture which Balasubramanian made are easily seen to be false and a number of counter-examples of order 7 can be found, for example, in [6].)

Note that the Kézdy–Snevily conjecture implies Ryser's conjecture, as Kézdy and Snevily [14] observed. This is immediate from the following result:

Proposition 7 *If S is the set of rows of a Latin square L of order n with no transversal, then S has covering radius $n-2$.*

PROOF. Let R, C, S be the sets of rows, columns and symbols (all equal to $\{1, \ldots, n\}$). We have to show that there is a permutation $h : C \to S$ such that, any given row of L contains at most two cells which, for some choice of $c \in C$, have symbol c^h in column c. By taking a conjugate of L, it is equivalent to find a permutation $h : R \to C$ such that any given symbol s occurs at most twice in cells of the form $[r, r^h]$ for some $r \in R$. We say for short that the symbols $L[r, r^h]$ are *selected* by h, and must show that there exists a permutation h which selects any symbol at most twice.

Take an arbitrary permutation $h : R \to C$. For $s \in S$, let $\mu(s)$ be the number of $r \in R$ such that $L[r, r^h] = s$ (the number of times s is selected by h). Let

$$M(h) = \sum_{s:\mu(s)>2} (\mu(s) - 2).$$

If $M(g) = 0$, we are done, so suppose that there exists $r_0 \in R$ such that $s = L[r_0, r_0^h]$ satisfies $\mu(s) \geq 3$.

Let $I = \{r \in R : \mu(L[r_0, r^h]) \geq 2\}$, and $J = \{r \in R : \mu(L[r, r_0^h]) = 0\}$. We claim that $|I| < |J|$. To see this, let $x_i = |\{s \in S : \mu(s) = i\}|$ be the number of symbols selected exactly i times, for $i \geq 0$. We have

$$\sum_{i \geq 0} x_i = n = \sum_{i \geq 0} i x_i,$$

so (since $x_i > 0$ for some $i > 2$)

$$|J| = x_0 = x_2 + 2x_3 + \cdots > x_2 + x_3 + \cdots = |I|.$$

Now choose $r_1 \in J \setminus I$; note that $r_0 \neq r_1$. Replace h by $(r_0, r_1)h$. In so doing we deselect $s = L[r_0, r_0^h]$ and $L[r_1, r_1^h]$, and replace them with $L[r_0, r_1^h]$ and $L[r_1, r_0^h]$. The effect is to decrease $\mu(s)$ by at least 1 without increasing $\mu(s')$ for any other element s' with $\mu(s') \geq 3$ or introducing any new element with this property. To see the last fact, we consider two cases:

(i) $s' = L[r_0, r_1^h] \neq L[r_1, r_0^h] = s''$. By assumption, $\mu(s') \leq 1$ (since $r_1 \notin I$), so s' is selected at most once by h, and so at most twice by $(r_0, r_1)h$. Also, s'' is not selected by h, so is selected only once by $(r_0, r_1)h$.

(ii) $s' = L[r_0, r_1^h] = L[r_1, r_0^h]$. Then s' is not selected by h, so is selected twice by $(r_0, r_1)h$.

Hence, after iterating this process a finite number of times, we must reduce $M(h)$ to zero, and we are done. □

Brualdi (see [7]) conjectured that every Latin square of order n contains a partial transversal of size $n-1$ (see also Keedwell's article on complete mappings in the *Handbook of Combinatorial Design* [6], and the article by Erdős *et al.* [10]). Derienko [8] claimed to have proved this conjecture; but the proof contains an error. In Section 2.4 we discuss this further. The following result is due to Kézdy and Snevily [14].

Theorem 8 *The Kézdy–Snevily conjecture implies Brualdi's conjecture.*

PROOF. Suppose that there is an $n \times n$ Latin square L with no near transversal. Viewing the rows of L as permutations of $\{1, 2, \ldots, n\}$ we see that any $h \in S_n$ must either intersect at least one row in three places or intersect two rows (say row j and row k) each in at least two places.

Append the symbol $n+1$ to the end of each of the rows of L to give a set $S' \subseteq S_{n+1}$. We argue that any permutation in S_{n+1} agrees at least twice with one of this set; this shows that $f(n+1, 2) \leq n$, in contradiction to the Kézdy–Snevily conjecture.

Let $g \in S_{n+1}$. If $(n+1)^g = n+1$, we are done. So suppose not; let $(n+1)^g = p$. For the moment let p and $n+1$ switch places, then drop the $n+1$. Call this new permutation $g' \in S_n$. If g' intersects some row of L in three or more places then g intersects that same row in two or more places and we are done. So g' must intersect row j in two places and it also must intersect row k in two places. Since L is a Latin square the symbol p can be involved in only one of these intersections (say with row j); this implies that g and row k must intersect in two places. □

In Corollary 6 we used Latin squares to find an upper bound for $f(n, 2)$ when n is even. For odd n we can also find upper bounds based on Latin squares. The idea is to choose a Latin square with few transversals, or whose transversals have a particular structure, and add a small set of permutations meeting each transversal twice. For $n = 5, 7, 9$, one can find a Latin square for which a single permutation suffices, showing that $f(n, 2) \leq n+1$ in these cases. The sets are

as follows:

1	2	3	4	5
2	1	4	5	3
3	5	1	2	4
4	3	5	1	2
5	4	2	3	1
1	3	4	2	5

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

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

In general, we have the following:

Theorem 9 *(a) If $n = 4k + 1$, then $f(n, 2) \leq 5k + 2$.*
(b) If k is an even integer such that $n/3 < k \leq n/2$ then $f(n, 2) \leq n + k$.

The theorem shows that $f(n, 2) \leq 4n/3 + O(1)$ for all n.

PROOF. (a) We have to construct a set of $5k + 2$ permutations which have at least two agreements with every permutation in S_n. Take a Latin square L of order n with a subsquare of order $2k$. Say it has block structure

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

where A is the subsquare, which contains the 'low' symbols $1, \ldots, 2k$. Then D contains exactly one 'high' symbol, ie one of $(2k + 1), \ldots, n$, per row and column. Call these cells D^*.

We take as our set the rows of L, plus $k + 1$ further permutations each of which consists of a different row of A followed by the symbols from D^*. This gives $5k + 2$ permutations in all.

Suppose that we have a transversal of L which includes a entries from A, $2k-a$ entries from each of B and C, d^* entries from D^* and $a + 1 - d^*$ entries from the rest of D.

In order to have the right number of low symbols we must have $2a+1-d^* = 2k$, which means that d^* must be odd. But if $d^* > 1$ then the transversal hits each of the supplementary rows in our dominating set at least twice and we need not worry. Hence we can assume $d^* = 1$ in which case $a = k$.

Finally note that since we have chosen $k + 1$ of the $2k$ rows of A we must

hit the transversal (which is choosing k of the rows) at least once with one of them, and since $d^* = 1$ this provides the second hit.

(b) Take the rows of a Latin square L with a subsquare of order k, such that the subsquare has no transversal. Say L has the same block structure as in part (a), where again A is the subsquare. For $i = 1, 2, \ldots k$ we add to our collection a permutation which is the i^{th} row of A followed by the $(i+1)^{\text{th}}$ row of B (taking row numbers modulo k). We now have $n + k$ permutations, and we claim that it agrees twice with each permutation. Again we only have to worry about transversals of L. Such a transversal T has to satisfy one of the following:

(i) T hits A but avoids B. This is ruled out by the fact that A has no transversal.
(ii) T hits B but avoids A. In this case T must hit k cells in C as well as the k in B. But $k > n/3$ means that $2k > n - k$ so there are not enough symbols in the square to allow this.
(iii) T hits both A and B. In this case there must be some i such that T hits the i^{th} row of A but the $(i+1)^{\text{th}}$ row of B, and hence will score two hits on the i^{th} auxiliary row. □

2.3 Further results

We can give lower bounds for $f(n, s)$ for large n by using the covering bound. Let $B(n, k)$ be the number of permutations in the ball of radius k about the identity in S_n (the set of permutations with at least $n - k$ fixed points). We have

$$B(n, k) = \sum_{i=0}^{k} \binom{n}{i} d(i),$$

where $d(i)$ is the number of derangements in S_i. Clearly, if $mB(n, d) < n!$, then any set of m permutations has covering radius at least $d + 1$. Hence:

Proposition 10 $f(n, s) \geq \left\lfloor \dfrac{n! - 1}{B(n, n - s)} \right\rfloor + 1.$ □

For example, the lower bound for $f(5, 3)$ given by this formula is $\lfloor 119/11 \rfloor + 1 = 11$; this can be improved by one as follows. Take any set S of eleven permutations in S_5. By the Pigeonhole Principle, at least six of them have the same parity; say there are $11 - m$ such, with $m \leq 5$. Then the m permutations of the opposite parity differ by transpositions from at most $10m$ further permutations of the given parity. If S has covering radius 2, then all 60 permutations of this parity are accounted for, which implies that $11 - m + 10m \geq 60$, con-

tradicting $m \leq 5$. So S has covering radius at least 3. Thus $f(5,3) \geq 12$. (This result was also proved by Quistorff [15]. We are grateful to the referee for this information.)

However, sometimes this bound gives weaker results than those we already know. For example, $B(n, n-1)$ is approximately $n!(1-1/\mathrm{e})$, so the lower bound for $f(n,1)$ is only 2 (the true value being $\lfloor n/2 \rfloor + 1$). More generally, the lower bound for $f(n,s)$ depends only on s for large enough n. For example, $f(n,3) \geq 13$ for $n \geq 6$.

Here are some techniques to give upper bounds for $f(n,s)$. First, we have the following recursive bound:

Proposition 11 *For $s > 0$, we have*

$$f(n,s) \leq n f(n-1, s-1).$$

PROOF. Let S_0 be a set of $f(n-1,s-1)$ permutations of $\{1,\ldots,n-1\}$ having covering radius at most $n-s$ (with the permutations written in passive form). Let S_i be obtained from S_0 by using the symbols $\{1,\ldots,n\} \setminus \{i\}$ in place of $\{1,\ldots,n-1\}$. Precede each permutation in S_i by the symbol i, and let S be the union of all these sets. Clearly $|S| = n|S_0|$. Now let h be any permutation. Let $1^h = i$. By assumption, h (with the first symbol deleted) agrees with some element of S_i in at least $s-1$ places; so it agrees with the corresponding element of S in at least s places. Thus $\mathrm{cr}(S) \leq n-s$, proving the result. □

This gives an upper bound of about $n^2/2$ for $f(n,2)$, far worse than Theorem 9.

The covering bound, combined with a probabilistic argument, gives an $O(n \log n)$ upper bound for $f(n,s)$, for any fixed s.

Proposition 12 $f(n,s) \leq \mathrm{e}(s+1)!\, n \log n$ *provided* $n \geq 2s+3$.

PROOF. The complement of the ball of radius $n-s-1$ in S_n has cardinality $n!\,q$, where q is a function of n and s (although the dependence on n is asymptotically negligible). Specifically, with $d(n)$ the number of derangements of an n-set, we have:

$$q = \frac{1}{n!} \sum_{i=0}^{s} \binom{n}{i} d(n-i) = \sum_{i=0}^{s} \frac{1}{i!} \frac{d(n-i)}{(n-i)!}$$

$$
\begin{aligned}
&< \sum_{i=0}^{s} \frac{1}{i!}\Big(\frac{1}{\mathrm{e}} + \frac{1}{(n-s+1)!}\Big) \\
&< \Big(\mathrm{e} - \frac{1}{(s+1)!} - \frac{1}{(s+2)!}\Big)\Big(\frac{1}{\mathrm{e}} + \frac{1}{(n-s+1)!}\Big) \\
&< 1 - \frac{1}{\mathrm{e}(s+1)!} + \frac{\mathrm{e}}{(n-s+1)!} - \frac{1}{\mathrm{e}(s+2)!} \\
&< 1 - \frac{1}{\mathrm{e}(s+1)!}. \qquad (1)
\end{aligned}
$$

The last inequality relies on the assumption that $n \geq 2s+3$.

Choose a fixed permutation $h \in S_n$. If x is a random permutation, the probability that h is not within distance $n-s-1$ of x is thus q. Hence, if $x_1, \ldots, x_m$ are independent random permutations, the probability that h is not within distance $n-s-1$ of any of them is q^m. So the expected number of permutations uncovered by m balls of radius $n-s-1$ with random centres is $n!\,q^m$. If this is less than 1, then there is a set of points of cardinality m with covering radius at least $n-s$, and so $f(n,s) \leq m$. Taking $m = \mathrm{e}(s+1)!\,n\log n$ we find from (1) that $m \log q < -n \log n$ and hence $n!\,q^m < 1$ as required. □

Another technique depends on the following observation due to C. Y. Ku (personal communication). A set S of permutations is ($\leq k$)-*intersecting* if any two distinct permutations in the set agree in at most k positions.

Proposition 13 *Let S be a maximal ($\leq k$)-intersecting subset of S_n. Then S has covering radius at most $n-k-1$. Hence $f(n,k+1) \leq |S|$.*

PROOF. Let $g \in S_n \setminus S$. If g and h agree in at most k positions for all $h \in S$, then $S \cup \{g\}$ is ($\leq k$)-intersecting, contradicting the assumed maximality. So there exists $h \in S$ with $d(g,h) \leq n-k-1$. Since g was arbitrary, the covering radius of S is at most $n-k-1$. The last sentence is now clear. □

Most research to date on ($\leq k$)-intersecting sets (for example, [9]) has concentrated on the largest such sets. However, to get the best from Proposition 13, we want to know the size of the *smallest* maximal ($\leq k$)-intersecting set of permutations. Let $m(n,k)$ be this number: then we have $f(n,k+1) \leq m(n,k)$.

This bound is not always attained. For example, $m(n,0) = n$. (The upper bound is obvious; the lower bound comes from the fact that any set of fewer than n mutually disjoint permutations can be extended to a set of n such, by Hall's theorem.) However, as we have seen, $f(n,1) = \lfloor n/2 \rfloor + 1$.

A computation using GAP [11] shows that $m(5,1) = 7$, giving $f(5,2) \leq 7$. (By contrast, the largest ($\leq$1)-intersecting subset of S_5 has size 20. We use the GAP share package GRAPE [16] to find all cliques in the graph $\overline{G_{5,2}}$, up to automorphisms of the graph.) The correct value of $f(5,2)$ is 6. The lower bound is found by brute force, and the upper bound comes from the example in the preceding subsection.

The following table gives some values of the function $f(n,s)$ for small arguments.

s	$n=3$	$n=4$	$n=5$
1	2	3	3
2	6	4	6
3	6	24	12..20
4		24	120
5			120

The values for $s = 1$ and $s \geq n-1$ follow from our earlier remarks, while $f(4,2) = 4$ comes from Proposition 4 and Corollary 6. The entry 12..20 means that the value of $f(5,3)$ is in the range 12 to 20. The lower bound was proved above, and the upper bound follows from the fact that the group AGL$(1,5)$ of order 20 has covering radius 2 (shown in the next section), or from the bound of Proposition 11.

2.4 On a paper of Derienko

Derienko [8] claimed to have proved Brualdi's conjecture, but unfortunately the proof contains an error. We now describe Derienko's method and give an example which shows that it fails.

Suppose that B is an order k submatrix of some Latin square L. Let R be the set of rows of B and C be the set of its columns. A permutation $\phi : R \mapsto C$ selects (in the sense of Proposition 7) k entries of B. We say that the number of different symbols selected by ϕ is the weight of ϕ, denoted $w(\phi)$.

Derienko claims to prove the following lemma. For every L, k and B for which there exists a permutation $\phi : R \mapsto C$ with $w(\phi) = k-2$, there exists another permutation $\phi' : R \mapsto C$ with $w(\phi') > k-2$.

An easy corollary of this lemma would be that for every Latin square L of

order n there is a permutation ϕ mapping the rows of L to its columns such that $w(\phi) > n-2$; a statement clearly equivalent to the Brualdi conjecture.

Derienko's approach starts with a $\phi = \phi_0$ of weight $k-2$ and applies successive perturbations to create a sequence of permutations $\phi_1, \phi_2, \ldots$. The perturbations are chosen so that they never decrease the weight. Hence if they ever succeed in increasing the weight we have the desired ϕ'.

The assumption is that $w(\phi_i) = k-2$ at the i-th stage of the process, so that we can partition R into sets T_i and D_i, of respectively cardinalities $k-2$ and 2, in such a way that ϕ restricted to T_i selects $k-2$ distinct symbols. There is one row, which we label r, which will be in D_i for all i. The other row in D_i will be denoted by r_i. For a given ϕ_0 we have several choices for T_0, D_0 and r but these initial choices determine all subsequent T_i's, D_i's, r_i's and, most importantly, ϕ_i's.

The perturbation employed by Derienko is simply the transposition (r, r_i), so $\phi_{i+1} = (r, r_i)\phi_i$. It is immediate from the definitions that $w(\phi_{i+1}) \geq w(\phi)$. If strict inequality holds then we set $\phi' = \phi_{i+1}$ and we are done. So assume that $w(\phi_{i+1}) = w(\phi)$, in which case we can define r_{i+1} to be the unique element of T_i satisfying $r_{i+1}\phi = r_i\phi_{i+1}$. We then define $D_{i+1} = \{r, r_{i+1}\}$ and $T_{i+1} = R \setminus D_{i+1}$ and we are ready to make the next perturbation.

Since we are working with finite sets, the only way we could fail to find the desired ϕ' is if there exists distinct i and j for which $\phi_i = \phi_j$, in which case the process will fall into an endless loop. Derienko's proof relies on showing that this cannot happen, which he shows in Property 8. Unfortunately it seems that step (24) of that proof is not justified.

Moreover, the following example shows that it is possible to cycle indefinitely with a constant weight of $k-2$.

Consider the partial Latin square of order 15 shown in Fig. 1, which we take to be B (entries not specified can be chosen arbitrarily and will be irrelevant to what follows).

We start with $r = 8$, $r_0 = 9$ and $\phi = \phi_0$ being the identity permutation. Note that $w(\phi) = 13$, because 1 and 2 are each selected twice.

Following through the perturbation process we find that $r_1 = 10$, $\phi_1 = (8\,9)$, $r_2 = 12$, $\phi_1 = (8\,10)(8\,9)$ and so on. Eventually, we find that $\phi_{48} = \phi_0$ is again the identity permutation, so that this example disproves Derienko's result.

The intuition behind this construction is that it is nearly symmetric between the numerical symbols in the bottom right and the alphabetic symbols in the top left. The first 12 steps of Derienko's process manouvre in the bottom right

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	b														
2		g		f		d									
3		e	f												
4				e	f	g									
5			c		d		g								
6			d	g		c	e								
7							2	c							
8		c	e	b	g	f	d	1	4	6	7	2	5	3	
9								3	2						
10									5	3		7	4		
11									7		4		3		
12										7	6	5			
13													6	5	
14										4		6		7	
15															1

Fig. 1. Counter-example to Derienko's method

of B. After that we make the equivalent steps among the alphabetic symbols. After 12 more steps we are back in the bottom right, undoing the steps we first made there. Finally, we go back to the top left and undo the steps we made there. So, after four lots of 12 perturbations we are back to where we started.

3 Covering radius of permutation groups

Can we say more if $S = G$ is a group? In this case we have $d(g, G) = d(1, Gg^{-1})$ for any $g \in S_n$. So G has covering radius at least $n - s$ if and only if there is a right coset of G in S_n consisting of elements with s or fewer fixed points.

Unexplained notation for permutation groups is mostly in [3]. One exception is that, if X is a linear or semilinear group (a subgroup of $\mathrm{GL}(d, q)$ or $\Gamma\mathrm{L}(d, q)$), then $\mathrm{A}X$ denotes the corresponding affine group (the semidirect product of the additive group of the vector space by X).

We begin by characterising those groups which have maximum covering radius.

Theorem 14 *Let G be a subgroup of S_n. Then $\mathrm{cr}(G) = n$ if and only if G has no orbit of size greater than $n/2$.*

PROOF. Suppose first that X is an orbit of G with $|X| > n/2$. Let g be any permutation in S_n. Then $X \cap X^{g^{-1}} \neq \emptyset$. Choose a point x in this intersection. Then $x \in X$ and $y = x^g \in X$, so there exists $h \in G$ with $y = x^h$. Then $d(g,h) \leq n-1$, so $d(g,G) \leq n-1$. Since g was arbitrary, $\mathrm{cr}(G) \leq n-1$.

Conversely, suppose that all G-orbits have size at most $n/2$. We first show the following statement:

> Let π be a partition of X. Suppose that all parts of π have size at most $|X|/2$. Then there is a partition ρ of X whose parts have size at least 2, such that $|Y \cap Z| \leq 1$ for all $Y \in \pi$, $Z \in \rho$.

The proof is by induction on $|X|$. The induction begins with the trivial case $X = \emptyset$. For $X \neq \emptyset$, it is enough to find a set Z meeting every part of π in at most one point, such that the induced partition of $X \setminus Z$ satisfies the hypothesis. If π has d parts of maximum size, with $d > 1$, then let Z contain one point from each of these parts. If there is a unique part of maximal size, let Z contain one point from this part and one other point.

Now apply this result with π the orbit partition of G. Let g be a permutation whose cycle partition is ρ. For every point $x \in \{1,\ldots,n\}$, x and x^g lie in different G-orbits, so no element of G can agree with g on x. Thus $d(g,G) = n$, and so $\mathrm{cr}(G) = n$. $\square$

The first part of the proof gives further information which is useful to us.

Proposition 15 *Let G be a subgroup of S_n having an orbit X of size greater than $n/2$. Let x be a point of X, and H the stabiliser of x (acting on the remaining $n-1$ points). Then $\mathrm{cr}(G) \leq \mathrm{cr}(H) \leq n-1$. In particular, this holds if G is transitive.*

PROOF. Take any permutation $g \in S_n$. As in Theorem 14, there exists $y \in X$ and $h \in G$ with $y^g = y^h$. There is no loss of generality in assuming that $y = x$, so that gh^{-1} fixes x. Since distance is translation-invariant, we have

$$d(g,G) = d(gh^{-1},G) \leq d(gh^{-1},H) \leq \mathrm{cr}(H).$$

Since g was arbitrary, we have $\mathrm{cr}(G) \leq \mathrm{cr}(H)$. $\square$

This immediately extends to groups with higher degrees of transitivity:

Proposition 16 *If G is t-transitive, then* $\mathrm{cr}(G) \leq n - t$. $\square$

The idea behind Proposition 16 can be extended beyond t-transitive groups. Let G be a permutation group on $X = \{1, \ldots, n\}$. Define sets Y_i as follows:

- $Y_0 = \emptyset$;
- Let G_i be the pointwise stabiliser of Y_i. If G_i has an orbit of size larger than $(n - i)/2$, choose a point y_{i+1} in this orbit and let $Y_{i+1} = Y_i \cup \{y_{i+1}\}$.

By Proposition 15, $\mathrm{cr}(G_{i+1}) \leq \mathrm{cr}(G_i)$. So, if r is the value of i when the condition is no longer satisfied, we have $\mathrm{cr}(G) \leq \mathrm{cr}(G_r) \leq n - r$.

This result applies in particular to the class of *Jordan groups* (see [3, Section 6.8] for discussion of these). A *Jordan set* for a permutation group G on X is a set Y (not a singleton) such that the pointwise stabiliser of the complement of Y is transitive on Y. Marggraff showed that, if G is primitive but not symmetric or alternating, then any Jordan set Y satisfies $|Y| \geq |X|/2$. Moreover, the complements of Jordan sets in such a group are the flats of a matroid. Hence we obtain the following result:

Proposition 17 *Let G be a primitive Jordan group of degree n whose associated matroid has rank r. Then* $\mathrm{cr}(G) \leq n - r$. $\square$

Sometimes this bound can be further improved. For example, $G = \mathrm{PGL}(r, q)$ is a Jordan group whose associated matroid is the projective space $\mathrm{PG}(r-1, q)$ of rank r. So $\mathrm{cr}(G) \leq n - r$, where $n = (q^r - 1)/(q - 1)$. The stabiliser of a basis has an orbit of size $(q - 1)^{r-1}$ on the points in general position with respect to the basis. So, if $(q - 1)^{r-1} > (n - r)/2$, then the covering radius of G is at most $n - r - 1$. For any r, the inequality holds for all sufficiently large q. For example, when $r = 3$, it holds for $q > 4$.

3.2 Maximum covering radius

In this section, we give a partial determination of the t-transitive groups of degree n which have covering radius $n-t$ for $t \geq 2$ (that is, those which attain the bound of Proposition 16).

First, consider the case $t = 2$. It follows from Theorem 14 and Proposition 15 that the orbits of the 2-point stabiliser have size at most $(n-2)/2$. Using this and the list of 2-transitive groups (see [3]), we see that the minimal normal

subgroup of G is regular elementary abelian or is isomorphic to $\mathrm{PSL}(2,q)$ (where q is an odd prime power), $\mathrm{PSU}(3,q)$, or a Suzuki or Ree group.

We require the following generalisation of the Orbit-Counting Lemma. A set S of permutations of $\{1,\ldots,n\}$ is said to be *uniformly transitive* if, for any points x, y, the number of permutations $g \in S$ with $x^g = y$ is constant. Clearly the constant value is $|S|/n$. (The case where the constant is 1 corresponds to a sharply transitive set as described in the last section.) Clearly a transitive permutation group is uniformly transitive; so taking S to be a group and $g = 1$ in the following result gives the Orbit-Counting Lemma.

Proposition 18 *Let S be a uniformly transitive set of permutations and g an arbitrary permutation. Then the average number of points at which an element of S agrees with g is 1.*

PROOF. Count pairs (x,h) with $h \in S$ and $x^h = x^g$. For each x, the number of h is $|S|/n$, where n is the degree. So the number of such pairs is equal to $|S|$, and the average over S is 1 as claimed. □

Lemma 19 *Let G be a 2-transitive permutation group of degree n with covering radius $n-2$. Suppose that S is a uniformly transitive subset of G. Then $|S|$ is even.*

PROOF. If H is transitive and has covering radius $n-1$, choose a permutation g at distance $n-1$ from H. Then the maximum number of points where an element of H agrees with g is 1; so we have $d(g,h) = n-1$ for all $h \in H$.

Now suppose that G is 2-transitive and has covering radius $n-2$. Applying the preceding paragraph to the point stabiliser, we see that if $d(g,G) = n-2$, then any permutation $h \in G$ agrees with g in 0 or 2 points.

Finally let S be a uniformly transitive subset of G. Then any element of S agrees with g in 0 or 2 points, and the average number of agreements is 1 by Proposition 18; so half the elements of S agree with g in no points, and half in 2 points. Thus $|S|$ is even. □

A regular normal subgroup of G is a uniformly transitive subset of cardinality n. So, if such a subgroup is a p-group, then $p = 2$. Consulting the list of 2-transitive groups, and using the fact that the orbits of the 2-point stabiliser have size at most $(n-2)/2$, we find that $G \leq \mathrm{A\Gamma L}(1,q)$ or $\mathrm{ASL}(2,q) \leq G \leq \mathrm{A\Gamma L}(2,q)$ in this case, where q is a power of 2. (In the latter case, some subgroups are excluded; for example, if G contains $\mathrm{AGL}(2,q)$, then it is a Jordan group of rank 3.)

We can deal with unitary groups in even characteristic and Suzuki groups using the following result.

Lemma 20 *Let G be a 2-transitive permutation group of degree n, where n is odd. Suppose that there is an involution u in the centre of a Sylow 2-subgroup of G which has exactly one fixed point. Then the covering radius of G is at most $n-3$.*

PROOF. Since u lies in the centre of a Sylow 2-subgroup of G, the conjugacy class $C = u^G$ containing u has odd cardinality. We claim that C is uniformly transitive.

- Count pairs (x, g) with $g \in C$ and $x^g = x$. For each element $g \in C$ there is exactly one such point x, by assumption. So there are $|C|$ such pairs. Now each point x occurs equally often in such a pair, by the transitivity of G. So there are $|C|/n$ elements of C fixing x.
- Count triples (x, y, g) with $x \neq y$, $g \in C$ and $x^g = y$. For each element $g \in C$ there are $n-1$ choices for x moved by g, then y is determined as x^g. So there are $|C|(n-1)$ such triples. Now each distinct pair (x, y) occurs equally often in such a triple, by the 2-transitivity of G. So the number of elements of C mapping x to y is $(n-1)|C|/n(n-1) = |C|/n$.

Now C is a uniformly transitive subset of G of odd cardinality. So the covering radius of G cannot be $n-2$, by Lemma 19. □

Now the unitary groups $\mathrm{PSU}(3, q)$ with q even and the Suzuki groups have involutions of the type required in this lemma, since the Sylow 2-subgroup of such a group fixes a point and is regular on the remaining points. So these cannot have covering radius $n-2$, and neither can any of their overgroups. We have proved the first part of the following result.

Theorem 21 *Let G be a t-transitive permutation group of degree n with covering radius $n-t$.*

(1) If $t = 2$, then one of the following occurs:
- *$G \leq \mathrm{A\Gamma L}(1, q)$, 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).*

(2) If $t > 2$, then one of the following occurs:
- *$t = 3$, $\mathrm{PGL}(2, q) \leq G \leq \mathrm{P\Gamma L}(2, q)$, where q is a power of 2;*
- *$t = n-2$, $G = A_n$;*
- *$t = n$, $G = S_n$.*

PROOF. The case $t = 2$ was proved above, so suppose that $t > 2$. Then G is a $(t-2)$-fold transitive extension of one of the groups with $t = 2$. Inspection of the list of multiply transitive groups show that only the cases listed can occur. □

The theorem does not assert that all of the groups listed actually have covering radius $n - t$. This holds trivially for symmetric and alternating groups; we will investigate groups containing $\mathrm{PSL}(2, q)$ in the next section. The covering radius of $\mathrm{A\Gamma L}(1, 8)$ is equal to 5 rather than 6. We have been unable to decide whether $\mathrm{ASL}(2, q)$ and the unitary or Ree groups have covering radius $n - 2$.

3.3 Some specific groups

The remainder of the paper gives information about the covering radius of certain groups. It follows from our remarks about Cayley tables in Subsection 2.2 that, if C_n denotes the cyclic group of order n, acting regularly, then

$$\mathrm{cr}(C_n) = \begin{cases} n-1 & \text{if } n \text{ is odd,} \\ n-2 & \text{if } n \text{ is even.} \end{cases}$$

In the following result, the groups $\mathrm{PSL}(2, q)$ and $\mathrm{PGL}(2, q)$ have their usual actions on the $n = q + 1$ points of the projective line. Recall that $\mathrm{PSL}(2, q) = \mathrm{PGL}(2, q)$ if (and only if) q is a power of 2.

Theorem 22 *(a)* $\mathrm{cr}(\mathrm{PSL}(2, q)) = \begin{cases} q-1 & \textit{if } q \textit{ is odd,} \\ q-2 & \textit{if } q \textit{ is even.} \end{cases}$

(b) If q is odd, then $q - 5 \leq \mathrm{cr}(\mathrm{PGL}(2, q)) \leq q - 3$; and if $q \not\equiv 1 \pmod 6$, then $\mathrm{cr}(\mathrm{PGL}(2, q)) = q - 3$.

PROOF. (a) Since $\mathrm{PSL}(2, q)$ is 2-transitive for q odd and 3-transitive for q even, we see that the right-hand side is an upper bound for the covering radius; it is enough to show that there is a permutation attaining the bound.

For q odd, an element $g \in \mathrm{PGL}(2, q) \setminus \mathrm{PSL}(2, q)$ agrees with any element of $\mathrm{PSL}(2, q)$ in at most two points. For if $h \in \mathrm{PSL}(2, q)$, then the points where g and h agree are the fixed points of gh^{-1}, and $gh^{-1} \in \mathrm{PGL}(2, q)$.

Now suppose that q is even. If $q = 2$, then $\mathrm{PSL}(2, q) = S_3$ has covering radius 0, so suppose that $q > 2$.

Let g be the Frobenius automorphism in $\mathrm{P\Gamma L}(2, q)$ (the map $x \mapsto x^2$, fixing ∞). Take any element $h \in \mathrm{PSL}(2, q)$, say $h : x \mapsto (ax + b)/(cx + d)$. If $c = 0$,

this permutation agrees with g on ∞, and (assuming without loss that $d = 1$) its other points of agreement satisfy $ax+b = x^2$; this quadratic has at most two solutions. If $c \neq 0$, then g and h do not agree on ∞; their points of agreement satisfy $ax + b = x^2(cx + d)$, and this cubic has at most three solutions.

(b) Since the 2-point stabiliser is cyclic of even order $q-1$, its covering radius is $q - 3$. Hence by Proposition 15, we have $\mathrm{cr}(\mathrm{PGL}(2, q)) \leq q - 3$.

Suppose first that $q \not\equiv 1 \pmod 6$. Consider the function $g : x \mapsto x^3$ (fixing ∞). This is a permutation since, by assumption, $\gcd(3, q - 1) = 1$. We claim that this permutation agrees in at most four points with any element of $\mathrm{PGL}(2, q)$. The proof is almost identical to that given in case (a) for q even. So the covering radius is $q - 3$.

Now let q be an arbitrary odd prime power. Let g be a permutation fixing ∞ and 0 and satisfying $\{x, -x\}^g = \{x^2, \alpha x^2\}$, where α is a fixed non-square in $\mathrm{GF}(q)$. Arguing as before, we see that, if $h \in \mathrm{PGL}(2, q)$ fixes ∞, then the remaining points where g and h agree satisfy $ax + b = x^g$, that is, either $ax + b = x^2$ or $ax + b = \alpha x^2$, and so there are at most four of them; if h does not fix ∞, then the points of agreement satisfy $ax + b = x(cx + d)x^g$, that is, either $ax + b = (cx + d)x^2$ or $ax + b = \alpha(cx + d)x^2$, so there are at most six of them. So the distance from g to the group is at least $q - 5$. □

Using this, we can compute the covering radius of the group $\mathrm{AGL}(1, q)$ (the stabiliser of a point in $\mathrm{PGL}(2, q)$) in many cases. Since the point stabiliser in $\mathrm{AGL}(1, q)$ is the cyclic group C_{q-1} acting regularly, we have

$$\mathrm{cr}(\mathrm{PGL}(2, q)) \leq \mathrm{cr}(\mathrm{AGL}(1, q)) \leq \mathrm{cr}(C_{q-1}) \leq \begin{cases} q-2 & \text{if } q \text{ is even,} \\ q-3 & \text{if } q \text{ is odd.} \end{cases}$$

Combining this with Theorem 22 gives the following. (The lower bound in (b) is $q-4$ rather than $q-5$ since, in the last part of the argument, we only have to consider equations of the form $ax + b = x^2$ and $ax + b = \alpha x^2$.)

Proposition 23 *(a) If q is even, then* $\mathrm{cr}(\mathrm{AGL}(1, q)) = q - 2$.
(b) If q is odd, then $q - 4 \leq \mathrm{cr}(\mathrm{AGL}(1, q)) \leq q - 3$; and if $q \not\equiv 1 \pmod 6$, then $\mathrm{cr}(\mathrm{AGL}(1, q)) = q - 3$. □

In particular, the group $G = \mathrm{AGL}(1, 5)$ of order 20 has covering radius 2, justifying the earlier observation that $f(5, 3) \leq 20$.

An obvious conjecture is that $\mathrm{cr}(\mathrm{PGL}(2, q)) = q - 3$ holds for all odd prime powers q. Computation shows that this is true for $q = 7$ and $q = 13$; the first value in doubt is $q = 19$. Choosing $\alpha = 2$ in the argument in Theorem 22, we find that, of the 2^9 permutations $g \in S_{20}$ for which $\{x, -x\}^g = \{x^2, 2x^2\}$,

exactly 180 satisfy $d(g, \mathrm{PGL}(2,19)) = 15$ (the rest have distance 14). So the covering radius is at least 15. This improves by 1 the lower bound from Theorem 22. No other value of α does better. Random search found no permutation at distance 16 from the group; the problem is rather large for an exhaustive search. Also, the covering radius of $\mathrm{AGL}(1,19)$ is 16; a permutation realising distance 16 is $(2,3)(4,5)(6,7)(8,10)(9,13)(11,15)(12,17)(14,16)$.

The covering radius of $\mathrm{AGL}(1,q)$ has a geometric interpretation. We have $\mathrm{cr}(\mathrm{AGL}(1,q)) \geq q - s$ if and only if there is a set S of q points in the affine plane over $\mathrm{GF}(q)$ which meets every horizontal or vertical line in one point and any other line in at most s points. If q is even, such a set with $s = 2$ is obtained from a hyperoval with two points on the line at infinity. For q odd, our results show that such a set exists with $s = 4$ in general, and with $s = 3$ for $q \not\equiv 1 \bmod 6$ and for $q = 7, 13, 19$. There is a similar interpretation for $\mathrm{PGL}(2,q)$ in the *Minkowski plane* or ruled quadric: a set of $q+1$ points meeting every generator in one point and every conic in at most s points, where we require the least possible value of s.

A GAP computation shows that, for $G = M_n$, $n = 9, 10, 11, 12$, the covering radius of G is equal to 6 (one less than the upper bound from Theorem 16). Since distance is invariant under left and right translation, if G is a group then $d(g,G)$ is constant over the double cosets GxG for $x \in S_n$, and it is only necessary to check a set of double coset representatives. There are eight double cosets of M_{12} in S_{12}, one of which realises distance 6. Computation also shows that the covering radii of $\mathrm{PGL}(3,2)$ and $\mathrm{AGL}(3,2)$ are 4 (attaining the bound of Proposition 17).

Another speculation suggested by these results is that there is a tendency for a multiply-transitive group to have even covering radius. This holds for any group which attains the bound in Proposition 16 (though we have no direct proof of this). Computation shows that all of the 49 multiply-transitive groups of degree at most 12 have even covering radius except for $\mathrm{A\Gamma L}(1,8)$ and $\mathrm{AGL}(2,3)$ (both with covering radius 5).

3.4 Packing and covering

As we noted earlier, $\mathrm{pr}(S) \leq \mathrm{cr}(S)$ for any set of permutations. Is there a bound for $\mathrm{cr}(S)$ as a function of $\mathrm{pr}(S)$?

We restrict attention to the case where $S = G$ is a group. In general the answer is 'no': if G is generated by one transposition, then $\mathrm{pr}(G) = 0$ but $\mathrm{cr}(G) = n$ if $n \geq 4$. Even if we assume that G is transitive, there is no bound; if G consists of all permutations fixing a partition of $\{1, \ldots, n\}$ into two parts of size $n/2$, where n is a multiple of 4, then $\mathrm{pr}(G) = 0$ but $\mathrm{cr}(G) = n/2$. (Take

a partition into four parts of size $n/4$ refining the given one. Now there is a permutation fixing two parts and interchanging the other two which agrees with any element of G in at most $n/2$ places.)

What if we assume that G is primitive? This looks more hopeful. We have $\mathrm{pr}(G) = \lfloor(\mu(G)-1)/2\rfloor$, where $\mu(G)$ is the *minimal degree* of G, the smallest number of points moved by a non-trivial element of G. (This is the analogue of minimum weight for a linear code). Now good bounds are known for the minimal degrees of primitive groups. A well known theorem of Jordan asserts that the degree of a primitive group is bounded by a function of its minimal degree; so certainly there is a function F such that $\mathrm{cr}(G) \leq F(\mathrm{pr}(G))$ for any primitive group G. In particular, if $\mathrm{pr}(G) = 0$, then G contains a transposition and $G = S_n$ with $\mathrm{cr}(G) = 0$; and if $\mathrm{pr}(G) = 1$, then G contains a 3-cycle or double transposition and $G = A_n$ (for $n > 8$), whence $\mathrm{cr}(G) = 2$.

The best current result on minimal degree is the theorem of Guralnick and Magaard [12], according to which a primitive group of degree n with minimal degree at most $n/2$ is 'known'. This suggests the possibility that there might be a linear bound. (If G is not one of these exceptions, then we have $\mathrm{cr}(G) \leq n-1 \leq 2\mu(G)-2 \leq 4\,\mathrm{pr}(G)+2$.) But no such bound can exist, as the following example shows.

Let G be the symmetric group of degree m in its induced action on the set of 2-subsets of $\{1,\ldots,m\}$, with degree $n = \binom{m}{2}$. This group is primitive for $m \geq 5$. The minimal degree of G is $2(m-2)$, achieved by a transposition on $\{1,\ldots,m\}$.

We assume that $m \equiv 1$ or 3 mod 6, so that there is a Steiner triple system of order m. Take such a system, and orient each block arbitrarily. Then let g be the permutation of the set of 2-subsets of $\{1,\ldots,m\}$ in which $\{i,j\} \to \{j,k\}$ if (i,j,k) is an oriented triple of the system.

Let $h \in G$. If $\{i,j\}^h = \{i,j\}^g = \{j,k\}$, then there are two possibilities:

(a) $j^h = j$, $i^h = k$;
(b) $i^h = j$, $j^h = k$.

There are at most m choices of $\{i,j\}$ for which (b) holds, since j is determined by i. Suppose that (a) holds. Then i is a point moved by h, and j the unique third point on the triple containing i and i^h; so there are at most m choices for i and j in this case also. Thus g agrees with any element of G in at most $2m$ points, and so $\mathrm{cr}(G) \geq \binom{m}{2} - 2m$, a quadratic function of m.

Acknowledgements

Thanks to C. Y. Ku, M. A. Ollis, A. E. Kézdy and H. S. Snevily for contributions acknowledged in the text and other helpful comments. Also thanks to S. Velani for suggesting the problem discussed in the last subsection, to N. Knarr for suggesting the Minkowski plane interpretation of $\mathrm{cr}(\mathrm{PGL}(2,q))$, and to a referee for information about the paper of Quistorff.

References

[1] K. Balasubramanian, On transversals in Latin squares, *Linear Algebra Appl.* **131** (1990), 125–129.

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

[3] P. J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts **45**, Cambridge University Press, Cambridge, 1999.

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

[5] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland, Amsterdam, 1997.

[6] C. J. Colbourn and J. H. Dinitz (editors), *CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1999.

[7] J. Dénes and A. D. Keedwell, *Latin Squares and their Applications*, Akademiai Kiado, Budapest, 1974.

[8] I. I. Derienko, On the Brualdi hypothesis (Russian), *Matematicheskie Issledovaniya* **102** (1988), 53–65.

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

[10] P. Erdős, D. R. Hickerson, D. A. Norton and S. K. Stein, Has every Latin square of order n a partial Latin transversal of size $n-1$? *Amer. Math. Monthly* **95** (1988), 428–430.

[11] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.3; Aachen, St Andrews, 2002. (`http://www-gap.dcs.st-and.ac.uk/~gap`)

[12] R. Guralnick and K. Magaard, On the minimal degree of a primitive permutation group, *J. Algebra* **207** (1998), 127–145.

[13] M. Hall Jr. and L. J. Paige, Complete mappings of finite groups, *Pacific J. Math.* **5** (1955), 541–549.

[14] A. E. Kézdy and H. S. Snevily, unpublished manuscript.

[15] J. Quistorff, Improved sphere bounds in finite metric spaces, preprint.

[16] L. H. Soicher, `GRAPE`: A system for computing with graphs and groups, in *Groups and Computation* (L. Finkelstein and W. M. Kantor, eds.), DIMACS Series in Discrete Mathematics and Theoretical Computer Science **11**, American Mathematical Society, Providence, RI, 1993, pp. 287–291.