Des Codes Crypt (2006) 41:79–86
DOI 10.1007/s10623-006-0017-3

A random construction for permutation codes and the covering radius

Peter Keevash · Cheng Yeaw Ku

Received: 27 January 2006 / Revised: 8 April 2006 /
Accepted: 2 May 2006

Abstract We analyse a probabilistic argument that gives a semi-random construction for a permutation code on n symbols with distance $n-s$ and size $\Theta(s!(\log n)^{1/2})$, and a bound on the covering radius for sets of permutations in terms of a certain frequency parameter.

Keywords Permutation codes · Covering radius · Restricted intersections

AMS Classification 05D40

1 Introduction

Permutation codes arise naturally in a communication model where it is desirable to always transmit exactly the same set of symbols, distinguishing different words by the order of transmission. An example of such a model is that of power line communications (see [14]), where variations in the delivery of electric power can be used as a communication channel, but the total power output must remain constant. We work in the metric space (S_n, d), where S_n is the permutation group on $[n] = \{1, \ldots, n\}$, and d is the Hamming distance, defined for two permutations g, h as $d(g,h) = n - \mathrm{fix}(gh^{-1})$, where $\mathrm{fix}(g) = |\{x : g(x) = x\}|$ is the number of fixed points of g, considered as a bijection from $[n]$ to itself. A permutation code of distance d is a subset $C \subset S_n$, such

Communicated by C. J. Colbourn.

P. Keevash (✉) · C. Y. Ku
Department of Mathematics, Caltech,
Pasadena, CA 91125, USA
e-mail: keevash@caltech.edu

C. Y. Ku
e-mail: cyk@caltech.edu

that any two distinct elements of C are at distance at least d. For recent results on permutation codes we refer the reader to [5, 15].

Another viewpoint may be obtained by analogy with the theory of set systems with restricted intersections. Say that a family $\mathcal{A}$ of subsets of $[n]$ is L-intersecting if $|A \cap B| \in L$ for every pair $A, B \in \mathcal{A}$, where L is some set of non-negative integers. The basic question in this theory is determine the maximum size of such a family $\mathcal{A}$, either as stated above, or with the additional assumption that $\mathcal{A}$ is k-uniform, i.e. all of its sets have size k, for some k. There is a wealth of combinatorial literature on these questions, to which [2, 10] provide a good introduction. The analogue of intersection for two permutations g, h is the set of positions at which they agree, and this has size $\mathrm{fix}(gh^{-1})$. Thus we call $C \subset S_n$ L-intersecting if $\mathrm{fix}(gh^{-1}) \in L$ for any two distinct elements g, h of C. Note that a permutation code in S_n of distance d is precisely a $\leq(n-d)$-intersecting subset of S_n. (It will be convenient, whenever $*$ is an relation, such as $\leq$, to write $*s$ for the set $\{t : t * s\}$.)

Let $p(n, L)$ denote the maximum of $|C|$ where $C \subset S_n$ is L-intersecting. Deza and Frankl [6] showed that $p(n, \geq 1) = (n-1)!$. Cameron and Ku [3] showed that equality can only hold for the coset of a stabilizer of point, i.e. a set $G_{xy} = \{g \in S_n : g(x) = y\}$ for some x, y. This can be viewed as analogous to the case $s = 1$ of the following theorem of Erdős et al. [8]: if $n > n_0(k, s)$ is sufficiently large then any k-uniform $\geq s$-intersecting family $\mathcal{A}$ of subsets of $[n]$ has size at most $\binom{n-s}{k-s}$, with equality if and only if there is some $S \subset [n]$ of size s such that $S \subset A$ for every $A \in \mathcal{A}$. The permutation analogue is not known for general s, and indeed the main conjecture of Deza and Frankl in [6] is that $p(n, \geq s)$ should equal $(n-s)!$ for $n > n_0(s)$ sufficiently large.

Certain special cases of this conjecture were proved in [6], some by means of the fundamental inequality $p(n, \geq s) \cdot p(n, < s) \leq n!$. This establishes a connection with permutation codes, as a construction of a $<s$-intersecting subset of S_n, i.e. a permutation code of distance $n - s + 1$, provides an upper bound on the function $p(n, \geq s)$. In general, when $s = o(n)$, their best bounds are obtained by sphere covering considerations, analogous to the Gilbert–Varshamov bound (see, e.g., [13]). They show that $p(n, < s) \geq n!/B(n, n-s)$, and so $p(n, \geq s) \leq B(n, n-s)$, where $B(n, r)$ denotes the number of permutations in a ball of radius r in (S_n, d). When $s \to \infty$ one can estimate $B(n, n-s) = \sum_{i=0}^{n-s} d_i \binom{n}{i} \sim n!/es!$, where $d_i \sim i!/e$ is the number of derangements of i elements, i.e. $p(n, <s) \geq (1 + o_s(1))es!$.

This existence result is inherently non-constructive, and for practical purposes one would hope for a code that can be described algorithmically. Various constructions are known for specific small values of n and s and sequences of (n, s) satisfying certain algebraic conditions (typically n being a prime-power): see [5, 7, 11]. With the following theorem we give a randomized algorithm to find a code for general n and s, which is roughly comparable in size to that guaranteed by the Deza–Frankl bound. (It is even better for $s = O(\log n)^{1/2}$, but for s so small there is a larger family that is $\{0\}$-intersecting, namely the set of all n powers of a fixed n-cycle.) The expected run time of our algorithm is quadratic in the size of the code, multiplied by a polynomial factor of n.

Theorem 1.1 *For any $\theta > 0$, $n > e^{30/\theta^2}$ and $s < n^{1-\theta}$ there is a randomized algorithm to construct a set of $m = \frac{1}{60}(\theta \log n)^{1/2}(s-1)!$ permutations in S_n that is $<s$-intersecting (i.e. a permutation code of distance $n-s+1$) in expected time $O((\theta(n/s)^3/\log n)^{1/\theta} m^2)$.*

Our methods also apply to certain questions on the covering radius of sets of permutations, which are motivated by two important conjectures on Latin squares:

Ryser's conjecture that every Latin square of odd order has a transversal, and Brualdi's conjecture that every Latin square of order n has a partial transversal of size $n-1$.[1] Given a subset G of S_n, the covering radius of G is $\mathrm{cr}(G) = \max_{h\in S_n} \min_{g\in G} d(g,h)$, i.e. the smallest r such that the balls of radius r with centres at the elements of G cover the whole space. Let $f(n,s)$ denote the smallest size of a set G with $\mathrm{cr}(G) \le n-s$. A result obtained independently by Cameron and Ku [3] and Kézdy and Snevily [12] is that $f(n,1) = \lfloor n/2 \rfloor + 1$. For the next case, $s=2$, Kézdy and Snevily [12] conjecture that $f(n,2)$ is equal to n if n is even, but is larger than n if n is odd. They observed that this conjecture would imply the conjectures of Ryser and Brualdi mentioned above. This is encapsulated in a result of Cameron and Wanless [4], that if $G \subset S_n$ consists of the rows of a Latin square, then $\mathrm{cr}(G)$ is equal to $n-1$ if G has a transversal, and equal to $n-2$ if G does not have a transversal.

Our next result gives a bound for the covering radius in terms of the following frequency parameter. For $G \subset S_n$ and $1 \le a,b \le n$ let $N_G(a,b) = |\{g \in G : g(a) = b\}|$. Note that if G is the set of rows of a Latin square then $N_G(a,b) = 1$ for all a,b.

Theorem 1.2 *Let $G \subset S_n$ be a set of permutations such that $N_G(a,b) \le k$ for any a,b in $[n]$. If $k \le \frac{(s-1)!}{s} \cdot \frac{n}{2n-s} \cdot \left(\frac{1}{e} - \frac{(n-s)!}{n!}\right)$ for some positive integer s, then there exists a permutation g which agrees with each permutation of G in at most $s-1$ positions, i.e.* $\mathrm{cr}(G) \ge n-s+1$.

An immediate consequence is the following corollary:

Corollary 1.3 *Let G be the set of rows of k Latin squares $L_1,\ldots,L_k$. Then* $\mathrm{cr}(G) \ge n-s$ *where s is the smallest positive integer such that $k \le \frac{s!}{s+1} \cdot \frac{n}{2n-s-1} \cdot \left(\frac{1}{e} - \frac{(n-s-1)!}{n!}\right)$.*

This can be compared with a lower bound of Cameron and Wanless [4] obtained by covering arguments, namely, if k is the largest integer such that $|G|B(n,k) < n!$ then $\mathrm{cr}(G) \ge k+1$. Consider, for example, three Latin squares L_1, L_2, L_3 of order $n = 1{,}000$ such that their rows are pairwise distinct and let G be the set of rows of L_1, L_2 and L_3, so that $|G| = 3{,}000$. Then, a simple calculation shows that the covering bound gives $\mathrm{cr}(G) \ge 994$, whereas Corollary 1.3 gives $\mathrm{cr}(G) \ge 995$.

The rest of this paper is organized as follows. In the next section we describe our main probabilistic tool, which is the local lemma, in a more general form than is often used. The proofs of Theorems 1.2 and 1.1 appear in Sections 3 and 4, respectively. We conclude with a remark about covering radius in more general groups.

2 The local lemma

We start by citing a rather general form of the local lemma, in which the usual independence assumption is replaced by an inequality on conditional probabilities (see [1], Section 5.1 for a proof.)

Theorem 2.1 *Suppose we have events $A_1,\ldots,A_n$, subsets $D_1,\ldots,D_n$ of $[n]$ and reals $x_1,\ldots,x_n$ so that for any $S \subset [n] \setminus D_i$ we have $\mathbb{P}(A_i \mid \cap_{j\in S} \overline{A_j}) \le x_i \prod_{j\in D_i}(1-x_j)$. Then $\mathbb{P}(\cap_{i=1}^n \overline{A_i}) \ge \prod_{i=1}^n (1-x_i)$.*

[1] A Latin square is an n by n table in which there are n distinct symbols, each appearing exactly once in each row and once in each column. A transversal is a choice of n cells, in which all n symbols appear exactly once, and exactly one cell is chosen from each row and each column.

We will use the following two special cases, restated in a manner that makes them easier to apply.

Theorem 2.2 *Suppose $\mathcal{A}$ is a collection of events, and for any $A \in \mathcal{A}$ there is a subset $\mathcal{D}_A \subset \mathcal{A}$ of size at most d, such that for any subset $\mathcal{S} \subset \mathcal{A} \setminus \mathcal{D}_A$ we have $\mathbb{P}(A | \bigcap_{S \in \mathcal{S}} \overline{S}) \leq p$. If $ep(d+1) \leq 1$ then $\mathbb{P}(\bigcap_{A \in \mathcal{A}} \overline{A}) > 0$.*

Proof Label $\mathcal{A} = \{A_1, \ldots, A_n\}$ and apply Theorem 2.1 with $x_i = 1/(d+1)$ for all i (using the inequality $(1 - 1/(d+1))^d > 1/e$). □

Theorem 2.3 *Suppose $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2$ is a collection of two types of events, such that, for $i = 1, 2$, any $A \in \mathcal{A}_i$ has probability p_i, and for each $A \in \mathcal{A}$ there are subsets $\mathcal{D}^i_A \subset \mathcal{A}_i$ of size at most d_i, so that, for any subsets $\mathcal{S}_i \subset \mathcal{A}_i \setminus \mathcal{D}^i_A$, we have $\mathbb{P}(A \mid \cap_{S \in \mathcal{S}_1 \cup \mathcal{S}_2} \overline{S}) \leq \mathbb{P}(A)$. If $8p_i d_i \leq 1$ for $i = 1, 2$ then $\mathbb{P}(\cap_{A \in \mathcal{A}} \overline{A}) \geq (1 - 4p_1)^{|\mathcal{A}_1|}(1 - 4p_2)^{|\mathcal{A}_2|}$.*

Proof Label $\mathcal{A} = \{A_1, \ldots, A_n\}$ and apply Theorem 2.1 with $x_j = 4p_i$ if $A_j \in \mathcal{A}_i$ for $i = 1, 2$. This is valid, as for any $A \in \mathcal{A}_i$ we have $\prod_{A_j \in \mathcal{D}^1_A \cup \mathcal{D}^2_A} (1 - x_j) \geq (1 - 4p_1)^{d_1}$ $(1 - 4p_2)^{d_2} \geq (1/2)^2$ so that $\mathbb{P}(A) \leq x_i \prod_{A_j \in \mathcal{D}^1_A \cup \mathcal{D}^2_A} (1 - x_j)$. □

3 Covering radius for permutations

As a prelude to Theorem 1.2, we first give a lower bound for covering radius using the most basic of probabilistic methods: the counting sieve, which says that if the sum of the probabilities of events $A_1, \ldots, A_n$ is less than 1, then with positive probability none of them occur. This is just for illustrative purposes, as the bound obtained is weaker than the covering bound of Cameron and Wanless mentioned above.

Proposition 3.1 *Let $G \subset S_n$ such that $|G| < s!$. Then $\mathrm{cr}(G) \geq n - s + 1$.*

Proof Let $G = \{g_1, \ldots, g_m\}$. Pick a permutation g uniformly at random. Given an index $i \in \{1, \cdots, m\}$ and a set $S \subset [n]$ of size s, we define $A_{i,S}$ to be the event that g and g_i agree on S, that is $g(x) = g_i(x)$ for all $x \in S$. Clearly, $\mathbb{P}(A_{i,S}) = \frac{(n-s)!}{n!}$. It follows that $\sum_{i,S} \mathbb{P}(A_{i,S}) = m\binom{n}{s}\frac{(n-s)!}{n!} < 1$. So, with positive probability, there exists a permutation which agrees with every element of G in at most $s - 1$ positions, that is $\mathrm{cr}(G) \geq n - s + 1$. □

Proof of Theorem 1.2 Let g be a permutation, chosen uniformly at random. We shall prove that with positive probability g agrees with each permutation of G in at most $s - 1$ positions.

Let $G = \{g_1, \ldots, g_m\}$. Given an index i and a subset $S \subset [n]$ of size s, we define $A_{i,S}$ as before to be the event that g and g_i have the same restriction to S, i.e. $g(x) = g_i(x)$ for all $x \in S$. Set $p = \mathbb{P}(A_{i,S}) = (n - s)!/n!$. Let $\mathcal{A}$ denote the set of all the events $A_{i,S}$. We also let $X_{i,S}$ be the collection of all pairs (i', S') such that at least one of $S \cap S'$ and $g_i(S) \cap g_{i'}(S')$ is non-empty.[2]

Let $\mathcal{D}_{i,S}$ consist of the events $A_{i',S'}$ such that $(i', S') \in X_{i,S}$. Let us now count the number of events $A_{i',S'} \in \mathcal{D}_{i,S}$. First, we choose two elements x, y of $[n]$ so that at least

[2] For a function f and a subset S of its domain we are using the notation $f(S) = \{f(s) : s \in S\}$.

one of $x \in S$ or $y \in g_i(S)$ holds: there are $2sn - s^2$ choices. Next, we choose i' such that $g_{i'}(x) = y$, for which we have at most k choices (using the assumption $N_G(a,b) \le k$ for any a, b in $[n]$). Finally, we can choose the rest of S' in at most $\binom{n-1}{s-1}$ ways. Therefore $|\mathcal{D}_{i,S}| \le d = ks(2n-s)\binom{n-1}{s-1}$.

To apply Theorem 2.2 we need to verify that $\mathbb{P}(A_{i,S}|E) \le p$, with an event $E = \bigcap_{A_{i',S'} \in \mathcal{S}} \overline{A_{i',S'}}$ for any subset $\mathcal{S} \subset \mathcal{A} \setminus \mathcal{D}_{i,S}$. Our method mirrors that used by Erdős and Spencer [9] to find Latin transversals (see also [1], Section 5.6).

For any injection $f : S \to [n]$ let B_f be the event that g restricts to f on S. We claim that $\mathbb{P}(A_{i,S}|E) \le \mathbb{P}(B_f|E)$. To see this, we exhibit an injective map, from the set of permutations g such that $E \cap A_{i,S}$ holds, to the set of permutations such that $E \cap B_f$ holds. This map is to replace the permutation g by g_f, which is defined as follows. Let $T = \{x \in [n] \setminus S : g(x) \in f(S)\}$. Define $g_f(x) = f(x)$ for $x \in S$, $g_f(x) = g(f^{-1}(g(x)))$ for $x \in T$, and $g_f(x) = g(x)$ otherwise. It is not hard to see that the map $g \mapsto g_f$ is injective, and that $E \cap B_f$ holds for g_f (using the definition of $X_{i,S}$ to see that none of the events in E is affected by the map).

We deduce that $\mathbb{P}(A_{i,S}|E) \le \frac{(n-s)!}{n!} \sum_f \mathbb{P}(B_f|E) = (n-s)!/n! = p$. Now, our assumption $k \le \frac{(s-1)!}{s} \cdot \frac{n}{2n-s} \cdot \left(\frac{1}{e} - \frac{(n-s)!}{n!}\right)$ implies that $ep(d+1) \le 1$, so by Theorem 2.2 there is a permutation g for which no event $A_{i,S}$ occurs, as required. □

4 A semi-random construction of a permutation code

In this section we prove Theorem 1.1, which states that for any $\theta > 0$, $n > e^{30/\theta^2}$ and $s < n^{1-\theta}$ there is a randomized algorithm to construct a set of $m = \frac{1}{60}(\theta \log n)^{1/2}(s-1)!$ permutations in S_n that is $<s$-intersecting in expected time $O((\theta(n/s)^3/\log n)^{1/\theta} m^2)$.

We apply the following semi-random algorithm. Set $r = 3/\theta$ and $m_0 = \theta^{-1/2} s (\log n)^{1/2}$. Suppose at time t we have a set of $<s$-intersecting permutations $g_1, \ldots, g_{tm_0}$ in S_n such that for every $a, b \in [n]$ we have

$$N^t_{a,b} = |\{i : g_i(a) = b, 1 \le i \le tm_0\}| \le tr.$$

Now we pick m_0 random permutations $g_{tm_0+1}, \ldots, g_{(t+1)m_0}$ and show that with positive probability the set $g_1, \ldots, g_{(t+1)m_0}$ is $<s$-intersecting and satisfies $N^{t+1}_{a,b} \le r(t+1)$. Then we fix such a set and continue the algorithm. We will show that the algorithm can proceed while $t < t^* = (s-1)!/20rs$, so at the end we have a $<s$-intersecting set of size $t^* m_0 = m$, as required.

To verify the claim for probabilities we consider the following events. Let B be the event that $N^{t+1}_{a,b} > r(t+1)$ for some a, b. Note that $N^{t+1}_{a,b} = N^t_{a,b} + X^{t+1}_{a,b}$ where $X^{t+1}_{a,b}$ is a binomial random variable $B(m_0, 1/n)$, so $\mathbb{P}(B) \le \binom{n}{2}\mathbb{P}(B(m_0, 1/n) > r)$. Now

$$\begin{aligned}
\mathbb{P}(B(m_0, 1/n) > r) &= \sum_{i \ge r+1} \binom{m_0}{i} (1/n)^i (1-1/n)^{m_0 - i} \\
&\le (m_0/n)^{r+1} \frac{1}{(r+1)!} \sum_{i \ge 0} (m_0/n)^i \\
&< (m_0/n)^{r+1}.
\end{aligned}$$

Here we have used the inequality $m_0 < (\theta^{-1}\log n)^{1/2}n^{1-\theta} < n/2$, which follows from the calculation $(\log n)^{-1/2}n^{\theta} > (30/\theta^2)^{-1/2}e^{30/\theta} > (30/\theta^2)^{-1/2}\cdot\frac{1}{2}(30/\theta)^2 > 2\theta^{-1/2}$. We deduce that

$$\mathbb{P}(B) < m_0^{r+1}/2n^{r-1}. \tag{1}$$

Given indices i,j, a set $S\subset[n]$ of size s and an injection $f: S\to[n]$ we define $A_{i,j,S,f}$ to be the event that g_i and g_j both restrict to f on S. We divide these A-events into two types: $\mathcal{A}_1$ consists of those events with $i\le tm_0$ and $tm_0+1\le j\le(t+1)m_0$, $\mathcal{A}_2$ is those with $tm_0+1\le i<j\le(t+1)m_0$. Let $\mathcal{A}=\mathcal{A}_1\cup\mathcal{A}_2$. If $A\in\mathcal{A}_1$ then $\mathbb{P}(A)=p=(n-s)!/n!$ and if $A\in\mathcal{A}_2$ then $\mathbb{P}(A)=p^2=((n-s)!/n!)^2$. There are $n_1=tm_0^2\binom{n}{s}$ events of type 1 and $n_2=\binom{m_0}{2}\binom{n}{s}n!/(n-s)!$ events of type 2.

We will apply Theorem 2.3 to show that $\mathbb{P}(\cap_{i,j,S,f}\overline{A_{i,j,S,f}})>m_0^{r+1}/n^{r-1}$. Then inequality (1) will imply that with probability at least $m_0^{r+1}/2n^{r-1}$ our random choice of $g_{tm_0+1},\dots,g_{(t+1)m_0}$ is *successful*, in that neither B nor any of the $A_{i,j,S,f}$ occur. For a randomized algorithm we simply repeat the random choice until we are successful. The number of trials is a geometric random variable with expectation less than $2n^{r-1}/m_0^{r+1}$. On each trial it takes time $O(m_0n^2)$ to check if B occurs and time $O(tm_0^2n)$ to check if any event $A_{i,j,S,f}$ occurs (for each i,j we only need to find $\mathrm{fix}(g_ig_j^{-1})$ and compare it to s, and this takes time $O(n)$). Therefore the expected run time of the algorithm is $O(n^rm^2/m_0^{r+1})<O((\theta(n/s)^3/\log n)^{1/\theta}m^2)$.

Given a set $S\subset[n]$ of size s and an injection $f:S\to[n]$ we let $X_{S,f}$ be the collection of all pairs (S',f') such that $S'\subset[n]$ has size s, $f':S'\to[n]$ is injective, and at least one of $S\cap S'$ and $f(S)\cap f'(S')$ is non-empty. Given indices i,j we let $Y_{i,j}$ be the collection of all pairs $\{i',j'\}$ such that $\{i,j\}\cap\{i',j'\}\cap\{tm_0+1,\dots,(t+1)m_0\}$ is non-empty. For an event $A_{i,j,S,f}$ and $k=1,2$ we let $\mathcal{D}^k_{i,j,S,f}$ consist of those events $A_{i',j',S',f'}$ in $\mathcal{A}_k$ such that $(S',f')\in X_{S,f}$ and $\{i',j'\}\in Y_{i,j}$.

To estimate $|\mathcal{D}^2_{i,j,S,f}|$ we note that $|X_{S,f}|\le 2sn\binom{n-1}{s-1}(n-1)!/(n-s)!$ for any S,f. Also, the number of choices of $tm_0+1\le i'<j'\le(t+1)m_0$ such that $\{i,j\}\cap\{i',j'\}\cap\{tm_0+1,\dots,(t+1)m_0\}$ is non-empty is at most $2m_0$. Therefore $|\mathcal{D}^2_{i,j,S,f}|\le d_2=4snm_0\binom{n-1}{s-1}(n-1)!/(n-s)!$. Next, we count the number of events $A_{i',j',S',f'}\in\mathcal{D}^1_{i,j,S,f}$. First we choose $x\in S'$ and $y=f'(x)$ so that either $x\in S$ or $y\in f(S)$, for which we have at most $2sn$ choices. Now we choose $1\le i'\le tm_0$ so that $g_{i'}(x)=y$, for which we have at most rt choices. Then we can choose the rest of S' in at most $\binom{n-1}{s-1}$ ways. The rest of f' is determined by $g_{i'}$ and j' is determined by the condition that $\{i,j\}\cap\{i',j'\}\cap\{tm_0+1,\dots,(t+1)m_0\}$ is non-empty. Therefore $|\mathcal{D}^2_{i,j,S,f}|\le d_1=2snrt\binom{n-1}{s-1}$.

Next we have to verify that $\mathbb{P}(A_{i,j,S,f}|E)\le\mathbb{P}(A_{i,j,S,f})$, where $E=\cap_{A_{i',j',S',f'}\in\mathcal{S}_1\cup\mathcal{S}_2}\overline{A_{i',j',S',f'}}$ for some subsets $\mathcal{S}_k\subset\mathcal{A}_k\setminus\mathcal{D}^k_{i,j,S,f}$.

When $1\le i\le tm_0$ and $tm_0+1\le j\le(t+1)m_0$, i.e. $A_{i,j,S,f}\in\mathcal{A}_1$, the argument is rather similar to that given in Theorem 1.2, so we will omit it, and just give the argument for $tm_0+1\le i<j\le(t+1)m_0$, i.e. $A_{i,j,S,f}\in\mathcal{A}_2$. For any injections $f_i:S\to[n]$ and $f_j:S\to[n]$ we let A_{i,j,S,f_i,f_j} be the event that g_i restricts to f_i and g_j restricts to f_j on S. We claim that $\mathbb{P}(A_{i,j,S,f}\mid E)\le\mathbb{P}(A_{i,j,S,f_i,f_j}\mid E)$. To see this, we exhibit an injective map, from the set of permutations $g_{tm_0+1},\cdots,g_{(t+1)m_0}$ such that $E\cap A_{i,j,S,f}$ holds, to the set of permutations such that $E\cap A_{i,j,S,f_i,f_k}$ holds. This map is to replace g_i by g_i^* and g_j by g_j^*, which are defined in a similar manner to the proof of Theorem 1.2. For

example, to define g_i^*, let $T = \{x \in [n] \setminus S : g_i(x) \in f_i(S)\}$, define $g_i^*(x) = f_i(x)$ for $x \in S$, $g_i^*(x) = g_i(f_i^{-1}(g_i(x)))$ for $x \in T$, and $g_i^*(x) = g_i(x)$ otherwise. Now we have a similar calculation as before: $\mathbb{P}(A_{i,j,S,f} \mid E) \leq \left(\frac{(n-s)!}{n!}\right)^2 \sum_{f_i,f_j} \mathbb{P}(A_{i,j,S,f_i,f_j} \mid E) = ((n-s)!/n!)^2 = p^2 = \mathbb{P}(A_{i,j,S,f})$, as required.

The rest of the proof is calculation. We have $8pd_1 = 8 \cdot (n-s)!/n! \cdot 2snrt\binom{n-1}{s-1} = 16srt/(s-1)! < 1$ provided that $t < t^* = (s-1)!/20rs$, and

$$8p^2d_2 = 8 \cdot ((n-s)!/n!)^2 \cdot 4snm_0\binom{n-1}{s-1}(n-1)!/(n-s)! = 32sm_0/n(s-1)!$$
$$< 200\theta^{-1/2}(\log n)^{1/2}/n < 1,$$

since $n > e^{30/\theta^2}$, so we can apply Theorem 2.3 to obtain $\mathbb{P}(\cap_{i,j,S,f}\overline{A_{i,j,S,f}}) \geq (1-4p)^{n_1}(1-4p^2)^{n_2}$. From the estimate $1 - x \geq e^{-2x}$ for $0 < x < 1/2$ and noting that $pn_1 = tm_0^2/s!$ and $p^2n_2 = \binom{m_0}{2}/s!$ we have $\mathbb{P}(\cap_{i,j,S,f}\overline{A_{i,j,S,f}}) > e^{-9tm_0^2/s!}$.

We claim that this is at least m_0^{r+1}/n^{r-1}, or equivalently, we need to show that $(r+1)\log m_0 + 9tm_0^2/s! < (r-1)\log n$ for $t < t^*$. Recalling that $r = 3/\theta$ and $m_0 = \theta^{-1/2}s(\log n)^{1/2}$ we have $9tm_0^2/s! < \frac{1}{6}\log n$ and $\log m_0 = \log s + \frac{1}{2}\log\log n + \frac{1}{2}\log\theta^{-1} < (1-\theta)\log n + \log\log n$ since $n > e^{30/\theta^2}$, so

$$(r-1)\log n - (r+1)\log m_0 - 9tm_0^2/s! > \left(\frac{3}{\theta} - 1 - \left(\frac{3}{\theta}+1\right)(1-\theta) - 1/6\right)$$
$$\log n - \left(\frac{3}{\theta}+1\right)\log\log n > \frac{1}{2}\log n - \left(\frac{3}{\theta}+1\right)\log\log n > 0.$$

For the final estimate we use the inequalities $\frac{\log n}{2\log\log n} > \frac{15\theta^{-2}}{\log 30 + 2\log\theta^{-1}} > \frac{15\theta^{-2}}{3/2+2\theta^{-1}} > 3\theta^{-1} + 1$. We deduce that the probability $\mathbb{P}(\cap_{i,j,S,f}\overline{A_{i,j,S,f}} \cap \overline{B})$ of success in a step of our algorithm is at least $m_0^{r+1}/2n^{r-1}$, as required. □

5 Concluding remarks

- We were rather cavalier in our estimates in the proof of Theorem 1.1, preferring to give a general bound on n for all situations rather than optimize the constants. The bound $n > e^{30/\theta^2}$ can certainly be improved if one tailors the choice of parameters to a given value of s and tightens up some inequalities in the proof. For example, one can verify that our argument will work with the parameters $n = 1{,}500$, $s = 10$, $m_0 = 10$, $r = 2$, $t^* = 1{,}134$, and the resulting code has size $m = t^*m_0 = 11{,}340$. This compares poorly with the Deza–Frankl bound (which is roughly 10^7), but the expected number of operations to find it is at most $(2n/m_0^3)\left(mn^2 + \binom{m}{2}n\right) < 4 \times 10^{11}$, which is feasible on a typical desktop computer. On the other hand, the number of operations needed to find any code in S_{1500} by an exhaustive search method is of order $1{,}500! \approx 10^{4115}$.
- Our arguments can apply to more general groups, and we will briefly indicate an example here. For any permutation group $G \leq S_n$ one can define the covering radius relative to G of a subset $H \subset G$ by $\mathrm{cr}_G(H) = \max_{g\in G}\min_{h\in H} d(g,h)$. For example, if $G = A_n$ is the alternating group, and we assume a bound on $N_H(a,b)$ very close to that in Theorem 1.2, then we can obtain a bound $\mathrm{cr}_G(H) \geq n - s + 1$.

The only difference in the proof is that, with the same notation as before, we now show $\mathbb{P}(A_{i,S}|E) \leq \mathbb{P}(B_f|E)$ under the additional assumption that f belongs to the set $P_i \subset S_n$ of permutations f such that $\{x \in S : f(x) \neq g_i(x)\}$ does not have size 1. Under the assumption $f \in P_i$, we can give an injective map, from the set of *even* permutations g such that $E \cap A_{i,S}$ holds, to the set of *even* permutations such that $E \cap B_f$ holds: simply map g to g_f, as defined earlier, and apply an additional transposition to the first two elements of $g(S) \setminus f(S)$ to correct the sign of the permutation, if necessary. Since $|P_i| = n!/(n-s)! - s(n-s+1)$ we deduce that $\mathbb{P}(A_{i,S}|E) \leq (n!/(n-s)! - s(n-s+1))^{-1} \sum_{f \in P_i} \mathbb{P}(B_f|E) \leq (n!/(n-s)! - s(n-s+1))^{-1}$. Now taking this estimate as the parameter p in Theorem 2.2, one can calculate an estimate for $N_H(a,b)$ which is very close to that given in Theorem 1.2.

Acknowledgments We would like to thank the anonymous referees for their comments that helped us make several improvements to this paper.

References

1. Alon N, Spencer J (2000) The probabilistic method, 2nd edn. Wiley-Interscience [John Wiley & Sons], New York
2. Babai L, Frankl P (1992) Linear algebra methods in combinatorics. Department of Computer Science, University of Chicago, Preliminary version
3. Cameron PJ, Ku CY (2003) Intersecting families of permutations. Euro J Combin 24:881–890
4. Cameron PJ, Wanless IM (2005) Covering radius for sets of permutations. Disc Math 293:91–109
5. Chu W, Colbourn CJ, Dukes P (2004) Constructions for permutation codes in powerline communications. Des Codes Cryptogr 32:51–64
6. Deza M, Mrankl P (1977) On the maximum number of permutations with given maximal or minimal distance. J Combin Theory Ser A 22:352–360
7. Ding C, Fu F-W, Klve T, Wei VK-W (2002) Constructions of permutation arrays. IEEE Trans Inform Theory 48:977–980
8. Erdős P, Ko C, Rado R (1961) Intersection theorems for systems of finite sets. Quart J Math Oxford Ser 12:313–320
9. Erdős, P, Spencer J (1991) Lopsided Lovász local lemma and Latin transversals. Disc Appl Math 30:151–154
10. Frankl P (1995) Extremal set systems. In: Graham RL, Grotschel M, Lovasz L (eds) Handbook of combinatorics. Elsevier, Amsterdam, pp 1293–1329
11. Fu F-W, Kløve T (2004) Two constructions of permutation arrays. IEEE Trans Inform Theory 50:881–883
12. Kézdy AE, Snevily HS, unpublished manuscript
13. MacWilliams FJ, Sloane NJA (1977) The theory of error-correcting codes. North-Holland, Amsterdam
14. Pavlidou N, Vinck AJH, Yazdani J, Honary B (2003) Power line communications: state of the art and future trends. IEEE Commun Mag 41 (issue 4):34–40
15. Tarnanen H (1999) Upper bounds on permutation codes via linear programming. Euro J Combin 20:101–114