Designs, Codes and Cryptography, 32, 51–64, 2004

Constructions for Permutation Codes in Powerline Communications

WENSONG CHU wensong.chu@asu.edu
Department of Computer Science and Engineering, Arizona State University, Tempe, AZ 85287-8809, U.S.A.

CHARLES J. COLBOURN colbourn@asu.edu
Department of Computer Science and Engineering, Arizona State University, Tempe, AZ 85287-8809, U.S.A.

PETER DUKES dukes@math.toronto.edu
Department of Mathematics, University of Toronto, Toronto, Ontario, Canada M5S 1A1

Abstract. A permutation array (or code) of length n and distance d is a set Γ of permutations from some fixed set of n symbols such that the Hamming distance between each distinct $x, y \in \Gamma$ is at least d. One motivation for coding with permutations is powerline communication. After summarizing known results, it is shown here that certain families of polynomials over finite fields give rise to permutation arrays. Additionally, several new computational constructions are given, often making use of automorphism groups. Finally, a recursive construction for permutation arrays is presented, using and motivating the more general notion of codes with constant weight composition.

Keywords: permutation code, permutation array, permutation polynomial, constant composition code, heuristic search, reactive local search

1. Introduction

Permutation codes have been studied for many years. They do not enjoy the popularity of binary codes, but for certain communication channels such codes arise naturally. Consider a common electric power line, for example. While the primary function is delivery of electric power, the frequency can be modulated to produce a family of n "close" frequencies that are orthogonal. At the receiver, as the power itself is received, these small variations in frequency can be decoded as symbols (see Pavlidou et al. [11]). This information transmission function must not interfere with power transmission. For this reason, while minor variations in frequency (and commensurate minor variations in power) are acceptable, it is imperative that power output remain as constant as possible. One means to achieve this is to use block coding (fixed length codewords of length l). Select integers $r_1, \ldots, r_n$ with $\sum_{i=1}^{n} r_i = l$. If we choose each codeword to have exactly r_i occurrences of the i-th symbol (i-th frequency) then the code is a constant composition code. More importantly, the power delivered in the transmission of any codeword is a constant. When codewords

are short (i.e., when l is close to n), the power envelope remains very close to constant. In such a system, effective design of a code must address the sources of errors unique to such a channel. While white Gaussian noise does arise, it is dominated by two other sources of error. Electrical interference from equipment, or from strong magnetic fields, can produce permanent narrow band noise. This masks transmission on a small number of frequencies over a long period of time. Impulse noise has the dual effect of masking all frequencies but for a small number of time slots. Narrow band noise can be addressed by using many frequencies but not using any frequency too often, while impulse noise suggests using many time slots. A tradeoff results between these goals and the requirement for constant power envelope. Choosing $r_1 = \cdots = r_n = 1$ and $l = n$ results in each type of noise affecting a single symbol in a codeword, and in keeping the length "short". Now considering the structure of a codeword, we find that each codeword is a permutation; moreover, errors result in the loss of a single entry of the permutation. These practicalities underpin the importance of permutation codes (permutation arrays) which we introduce formally next.

Let n be a positive integer. Two distinct permutations $\sigma, \tau \in \mathscr{S}_n$ have distance d if $\sigma\tau^{-1}$ has exactly $n - d$ fixed points. A permutation array of length n and minimum distance d, denoted by $PA(n, d)$ or simply PA, is a subset Γ of $\mathscr{S}_n$ such that the distance between distinct members of Γ is at least d. Often, we view a $PA(n, d)$ of size s as an $s \times n$ array whose rows represent the image of $(1, 2, \ldots, n)$ under the s permutations in Γ.

Let $M(n, d)$ denote the maximum size of a $PA(n, d)$. The following are well-known elementary consequences of the definitions.

PROPOSITION 1.1

a. $M(n, 2) = n!$,

b. $M(n, 3) = n!/2$,

c. $M(n, n) = n$,

d. $M(n, d) \geq M(n-1, d), M(n, d+1)$,

e. $M(n, d) \leq nM(n-1, d)$,

f. $M(n, d) \leq n!/(d-1)!$.

Proof. Part (a) follows because any two distinct permutations have distance at least two. For (b), let $\Gamma = A_n$. The quotient of two members of Γ is again a member of A_n, and thus cannot be a single transposition. The lower bound in (c) follows by taking Γ to be a cyclic subgroup of order n, while clearly any $n + 1$ permutations agree in at least one position. To prove (d), observe that any $PA(n, d-1)$ is also a $PA(n, d)$. Adding a new (always fixed) symbol to a $PA(n-1, d)$ produces a $PA(n, d)$. Part (e)

follows from the fact that the subarray of a $PA(n,d)$ consisting of all rows whose first entry is k, with the first column deleted, is a PA of the same distance on the symbols $\{1,\ldots,n\}\setminus\{k\}$. Finally, (f) is a result of (c) and (e). ■

A latin square of order n is a $PA(n,n)$. Two latin squares $L=(L_{ij})$ and $L'=(L'_{ij})$ are orthogonal if $\{(L_{ij},L'_{ij}):1\le i,j\le n\}=\{1,\ldots,n\}^2$. The following result was proved in Colbourn et al. [4], using techniques from Deza and Vanstone [7].

PROPOSITION 1.2 [4]. *If there are m mutually orthogonal latin squares of order n, then $M(n,n-1)\ge mn$. In particular, if q is a prime-power, then $M(q,q-1)=q(q-1)$.*

Suppose X is a set of size n which, for convenience, we may identify with $\{1,\ldots,n\}$. A group G acting on X is sharply k-transitive if, for any two k-tuples u, v of distinct points of X, there is a unique $g\in G$ such that $gu=v$. There are $n(n-1)\cdots(n-k+1)$ elements in such a group. If G is sharply k-transitive acting on X with $g,h\in G,(g\ne h)$, it follows that $g(1,2,\ldots,n)$ and $h(1,2,\ldots,n)$ can agree in at most $k-1$ positions. So the existence of a sharply k-transitive group acting on a set of size n is equivalent to a maximum $PA(n,n-k+1)$. This was first pointed out in Frankl and Deza [9].

Let q be a prime-power and $\mathbf{F}_q$ a finite field of order q. A special case of Proposition 1.2 arises from the sharply 2-transitive group $AGL(1,q)$ of linear transformations $x\mapsto ax+b$ acting on $\mathbf{F}_q$. The group $PGL(2,q)$, consisting of fractional linear transformations $x\mapsto(ax+b)/(cx+d),ad-bc=\ne 0$, is sharply 3-transitive acting on $X=F_q\cup\{\infty\}$. It is also well-known that the Mathieu groups M_{11} and M_{12} are sharply 4- and 5-transitive on sets of size 11 and 12, respectively.

PROPOSITION 1.3. Frankl and Deza [9]. *If q is a prime-power, then $M(q+1,q-1)=(q+1)q(q-1)$. Additionally, $M(11,8)=11\cdot10\cdot9\cdot8$ and $M(12,8)=12\cdot11\cdot10\cdot9\cdot8$.*

One does not need the group structure here, so that a sharply d-transitive set of permutations would serve as well. However, under the restriction that the set contain the identity and be closed under taking inverses, Bonisoli and Quattrocchi [2] have shown that the examples in Proposition 1.3 are the only ones with $d\ge4$.

A derangement of order k is an element of $\mathscr{S}_k$ with no fixed points. Let D_k be the number of derangements of order k, with the convention that $D_0=1$. The ball in $\mathscr{S}_n$ of radius r with center σ is the set of all permutations of distance $\le r$ from σ. The volume of such a ball is $V(n,r)=\sum_{k=0}^{r}\binom{n}{k}D_k$.

PROPOSITION 1.4 [9].

$$M(n,d)\ge\frac{n!}{V(n,d-1)}.$$

This bound can be marginally improved upon by stipulating that, after one permutation $\sigma \in \mathscr{S}_n$ is chosen, a second τ is chosen with distance exactly d from σ. The number of permutations at distance less than d from either σ or τ is at most $2V(n, d-1) - V_2(n, d-1)$, where $V_2(n, d-1)$ is the intersection size of two balls with radii $d-1$ and centers at distance d. In general, d permutations may be chosen with pairwise distance exactly d, ruling out fewer than $dV(n, d-1)$ permutations for future choice. Further results on sphere-packing may be of some interest in this context.

An often nontrivial upper bound on $M(n, d)$ can be similarly obtained by considering balls of radius $(d-1)/2$. For small values of n and d, still stronger upper bounds are found in Tarnanen [14] by the method of linear programming.

2. Direct Constructions

2.1. *Computational Methods*

Perhaps the first serious attempts at computer construction of permutation arrays were reported in Deza and Vanstone [7], where it was stated that $M(6, 5) = 18$ and $M(10, 9) \geq 32$. These results are of particular interest in light of Proposition 1.2.

Here, a variety of computational methods have been employed to determine lower bounds on $M(n, d)$ for certain small values of n and d.

Clique search

This technique involves simply building a graph $G(n, d)$ whose vertex set is all $n!$ permutations of order n, with an edge between two vertices if the distance between their associated permutations is at least d. A reactive local search, such as the one found in Battiti and Protasi [1], is then used to find a large clique in $G(n, d)$. Due to size constraints on $G(n, d)$, this method is currently only practical for $n \leq 7$. One example of its use provides:

PROPOSITION 2.1. $M(7, 4) \geq 349$.

Greedy algorithm

In this method, we begin with an empty array, run through all permutations, and add a permutation if it has distance at least d from every member of the current PA. Of course, the order in which all permutations are considered is of great importance. A reasonable ordering seems to be the rank order on permutations σ of order n, defined recursively by

$$\text{rank}(\sigma) = (\sigma(1) - 1)(n-1)! + \text{rank}(\sigma'),$$

where the entries of the smaller permutation $\sigma' = (\sigma(2), \ldots, \sigma(n))$ are, if necessary, relabeled to act on $1, 2, \ldots$ in the same order. Due to the length of time required to process all $n!$ permutations, this method is currently only practical for $n \leq 10$ or 11, of course with faster results for larger d.

While none of the best lower bounds were found with the greedy algorithm alone, an easy modification often yields some interesting results. Consider several sequential runs through all permutations, with a small fixed number, say e, of the permutations in the current array deleted after every run is complete. To prevent the same e permutations from being re-added in a subsequent run, we start each run at a randomly chosen rank r, and end at $r - 1 \pmod{n!}$. If desired, a monotonically increasing array is forced with the stipulation that adding less than the previously deleted e permutations causes the array to revert to the old array, with a new random start rank chosen. This method of repeated applications of the greedy algorithm offered an improvement often around 15% of the size of an array from one greedy run. An example of its application provides:

PROPOSITION 2.2. $M(10, 9) \geq 35$.

0251467938	0387125649	0732894561	0976531824	1450923867
1569847302	2063759841	2139065784	2591384670	2648173905
3126974058	3295806147	3701245896	3967082415	4512076839
4603592178	4835720916	5017634982	5249781063	5674028391
5783916204	6182507493	6329410875	6418795320	6540239718
7230618459	7802961345	7914350268	8046312597	8175649230
8794563012	9072483156	9364271580	9406158732	9857346021

Automorphisms

A $PA\Gamma$ has $H \leq \mathscr{S}_n$ as a (left) automorphism group if $h\Gamma = \Gamma$ for all $h \in H$. In this case, Γ can be completely specified by $|\Gamma|/|H|$ orbits under H. Stipulating a certain automorphism group for a PA can significantly reduce computation time. The methods discussed earlier are easily modified by using a search space of $n!/|H|$ orbit representatives and distance function reporting the minimum between two orbits. Standard groups with which we have had success are the cyclic group, dihedral group, linear group, and fractional-linear group.

LEMMA 2.3. *The following lower bounds on $M(n, d)$ (Table 1) arise by direct computation using the automorphism groups and methods indicated.*

Proof. Some small examples are presented below and in the proof of Lemma 3.2. Interested readers are asked to contact the authors for larger ones. ■

(7, 5): Develop with $x \mapsto x + a \pmod 7$, $a \in Z_7$.

0125643	0143256	0263541	0246315	0324516	0362154
0412635	0456123	0531462	0654231	0615324	

(9, 6): Represent $[f] \in Z_2/\langle x^3 + x^2 + 1\rangle$ by the integer $f(2) \pmod 8$. Develop under $PGL(2, 8)$.

Table 1.

(n,d)	Automorphism Group	Method	$M(n,d) \geq$
$(7,5)$	$\mathbb{Z}_7$	clique	11×7
$(8,4)$	$PGL(2,7)$	clique	8×336
$(9,4)$	$PGL(2,8)$	clique	36×504
$(9,5)$	$AGL(1,9)$	greedy	27×72
$(9,6)$	$PGL(2,8)$	clique	3×504
$(10,5)$	$PGL(2,9)$	greedy	19×720
$(10,6)$	$PGL(2,9)$	greedy	6×720
$(11,9)$	$\mathbb{Z}_{11}$	greedy	14×11
$(12,5)$	$PGL(2,11)$	greedy	554×1320
$(12,6)$	$PGL(2,11)$	greedy	89×1320
$(13,9)$	$AGL(1,13)$	greedy	23×156
$(14,10)$	$PGL(2,13)$	greedy	3×2184

$$\infty 01327456 \quad \infty 01547263 \quad \infty 01674235$$

$(10,\ 6)$: Represent $[f] \in Z_3/\langle x^2 + x + 2\rangle$ by the integer $f(3)$ (mod 9). Develop under $PGL(2,9)$.

$$\begin{array}{lll} \infty 014728356 & \infty 017824563 & \infty 018427635 \\ \infty 013625487 & \infty 015326748 & \infty 016523874 \end{array}$$

$(11,\ 9)$: Develop under $x \mapsto \pm x + a$ (mod 11), $a \in Z_{11}$.

$$\begin{array}{ll} (0,5,9,4,7,6,8,1,10,3,2) & (0,3,1,4,2,10,5,6,8,9,7) \\ (0,4,3,9,10,8,5,7,1,6,2) & (0,2,1,8,4,7,9,3,6,10,5) \\ (0,4,9,1,6,2,10,8,7,5,3) & (0,5,2,3,8,10,6,9,7,4,1) \\ (0,1,4,5,8,2,7,10,3,9,6) & \end{array}$$

2.2. Permutation Polynomials Over Finite Fields

Let $\mathbf{F}_q$ be a finite field of order q. A polynomial f over $\mathbf{F}_q$ is a permutation polynomial if the mapping it defines is one-to-one. It is well known that any mapping $g : \mathbf{F}_q \to \mathbf{F}_q$ arises from the unique polynomial p_g of degree less than q, where

$$p_g(x) = \sum_{c \in \mathbf{F}_q} g(c)(1 - (x - c)^{q-1}).$$

In this section, we are interested in the enumeration of permutation polynomials over $\mathbf{F}_q$ of given degree $d \geq 1$. We use $N_d(q)$ to denote the number of such permutation polynomials. By the remarks above, we have $\sum_{d \leq q-2} N_d(q) = q!$. In addition, $N_d(q) = 0$ if $d \mid (q-1)$. For a complete treatment of permutation polynomials, refer to Lidl and Niederreiter [10].

A direct construction of PAs results from permutation polynomials.

THEOREM 2.4. *Let n be a prime power. Then*

$$M(n, n-d) \geq \sum_{l=1}^{d} N_l(n).$$

Proof. Suppose $f(x)$ and $g(x)$ are two permutation polynomials with degree no more than $n-d$. Then $f(x)-g(x)=0$ has at most $n-d$ solutions because the equation is over a field. Therefore, the distance between corresponding permutations is at least d. ■

Unfortunately, not much is known about permutation polynomials. While their classification and enumeration are far from complete, everything is known for $d<6$. A permutation polynomial $f(x)$ is in normalized form if f is monic, $f(0)=0$ and, when the degree of f is not divisible by the field characteristic, the coefficient of x^{n-1} is 0. Note that if $f(x)$ is a normalized permutation polynomial over $\mathbf{F}_q$, and $b, c, d \in \mathbf{F}_q$ with $c \neq 0$, then $f_1(x) = cf(x+b)+d$ is also a permutation polynomial of equal degree. For a given normalized permutation polynomial, the number of distinct such f_1 is either $q^2(q-1)$ or $q(q-1)$, depending on whether $(q,t)=1$ for some $t>1$ such that there is a nonzero coefficient of x^t.

LEMMA 2.5. [10]. *All normalized permutation polynomials with degree $d \leq 5$, together with the total produced by each class, are given in Table 2.*

Proof. The classification of normalized permutation polynomials appears in Lidl and Niederreiter [10]. For the count in each class, we prove the entries marked with *. The others are similar or routine.

Table 2.

Normalized Permutation Polynomials	q restriction	Total
x	any q	$q(q-1)$
x^2	$q \equiv 0 \bmod 2$	$q(q-1)^*$
x^3	$q \not\equiv 1 \bmod 3$	$q^2(q-1)$ or $q(q-1)$
$x^3 - ax$ (a not a square)	$q \equiv 0 \bmod 3$	$q(q-1)^2/2$
$x^4 \pm 3x$	$q=7$	$2q^2(q-1)$
$x^4 + a_1x^2 + a_2x$ (if only root in $\mathbf{F}_q$ is 0)	$q \equiv 0 \bmod 2$	$\frac{1}{3}q(q-1)(q^2+2)^*$
x^5	$q \not\equiv 1 \bmod 5$	$q^2(q-1)$ or $q(q-1)$
$x^5 - ax$ (a not a fourth power)	$q \equiv 0 \bmod 5$	$\frac{3}{4}q(q-1)^2_*$
$x^5 + ax(a^2=2)$	$q=9$	$2q^2(q-1)$
$x^5 \pm 2x^2$	$q=7$	$2q^2(q-1)$
$x^5 + ax^3 \pm x^2 + 3a^2x$ (a not a square)	$q=7$	$q^2(q-1)^2$
$x^5 + ax^3 + 5^{-1}a^2x$ (a arbitrary)	$q \equiv \pm 2 \bmod 5$	$q^3(q-1)$
$x^5 + ax^3 + 3a^2x$ (a not a square)	$q=13$	$\frac{1}{2}q^2(q-1)^2$
$x^5 - 2ax^3 + a^2x$ (a not a square)	$q \equiv 0 \bmod 5$	$\frac{1}{2}q^2(q-1)^2*$

1. After unnormalizing x^2, we have $f_1(x) = c(x+b)^2 + d = c(x^2+b^2) + d$, which allows for any nonzero leading coefficient and any constant coefficient, a total of $q(q-1)$ possibilities.
2. By considering the linear and constant terms, we have $q(q-1)$ distinct permutation polynomials for each $x^3 + a_1x + a_2 \in \mathbf{F}_q[x]$. The number of irreducible polynomials of degree 3 over $\mathbf{F}_q$ with trace equal to 0 is

$$\frac{1}{3}(q^3 - q) - (q-1)\frac{1}{3q}(q^3 - q) = \frac{1}{3}(q^2 - 1)$$

   according to Theorem 1.1 in Ruskey et al. [12]. Setting $a_1 = a_2 = 0$ yields an additional $q(q-1)$ distinct polynomials.
3. Each normalized $x^5 - ax$ corresponds to $q(q-1)$ distinct permutation polynomials when q is a power of five. In this case, exactly one quarter of all elements of $\mathbf{F}_q^*$ are fourth powers. So the count for this class is $\frac{3}{4}q(q-1)^2$.
4. Since the polynomials $x^5 - 2ax^3 + a^2x$ have a nonzero coefficient of x^3, and since $(3, q) = 1$, we have $q^2(q-1)$ possible permutation polynomials for each choice of a. There are $(1/2)(q-1)$ possible nonsquares a. Each gives a disjoint collection of permutation polynomials, again by analyzing the linear portion. ■

The case $n = 2^k$ with d close to n appears to be of interest for applications. When $n-1$ has few divisors, some particularly robust lower bounds result from Theorem 2.4. For instance:

COROLLARY 2.6. *Let $n = 2^k$. If $n \not\equiv 1 \bmod 3$, then*

$$M(n, n-3) \geq (n+2)n(n-1) \qquad \text{and} \quad M(n, n-4) \geq n(n-1)\frac{n^2+3n+8}{3}.$$

By evaluating the totals from Lemma 2.5 for $7 \leq q \leq 23$, we get the following (Table 3) for $N_d(q)$. For some values, careful checking for overlap in normalized polynomial families is required.

Table 3.

$q \setminus d$	1	2	3	4	5
7	42	0	0	588	4410
8	56	56	448	1848	3584
9	72	0	360	0	648
11	110	0	1210	0	0
13	156	0	0	0	38,532
16	240	240	0	20,640	0
17	272	0	4624	0	78,608
19	342	0	0	0	6498
23	506	0	11,638	0	279,312

Although an arbitrary collection of permutation polynomials of degree greater than d in general fails to produce a PA with minimum distance $n-d$, it appears that such polynomials of degree slightly more than d lead to a favorable restriction on the search space for $PA(n, n-d)$. For example, there is a $PA(7,5)$ of size 77, as in the last section, such that all corresponding polynomials are of degree 1 or 4. This is noteworthy because, from the table above, only 630 of all 5040 permutations have degree 1 or 4. No larger array has been obtained by adding the remaining (degree 5) polynomials. A simple result of similar flavor is presented next.

THEOREM 2.7. *Suppose $n = q$ is a prime-power and that there are E monic permutation polynomials over $\mathbf{F}_q$ of degree less than or equal to $d+1$. Then $M(n, n-d) \geq E$.*

Proof. The difference between a pair of such polynomials has degree at most d. ■

COROLLARY 2.8. *If n is a prime-power, $n \not\equiv 2 \bmod 3$, then $M(n, n-2) \geq n^2$.*

In general, obtaining $N_d(q)$ is a finite (albeit sometimes complex) problem.

THEOREM 2.9 [5]. *Let E be the number of distinct solutions of the following system of linear equations over $\mathbf{F}_q$ (with primitive element ω), where $x_i \neq 0$ and $x_i \neq x_j$ for any $i \neq j$. Then $N_d(q) = (q-1)E$.*

$$
\begin{aligned}
&x_1 + \omega^{(q-d-1)}x_2 + \omega^{2(q-d-1)}x_3 + \cdots + \omega^{(q-2)(q-d-1)}x_{q-1} = 1\\
&x_1 + \omega^{(q-d-2)}x_2 + \omega^{2(q-d-2)}x_3 + \cdots + \omega^{(q-2)(q-d-2)}x_{q-1} = 0\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \cdots\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \cdots\\
&x_1 + \omega x_2 + \omega^2 x_3 + \cdots + \omega^{(q-2)}x_{q-1} = 0.
\end{aligned}
$$

This gives us a possible computational method to get certain values of $N_d(q)$ with $d \geq 6$. For example, we have found that

$$N_6(11) = 29{,}040, \quad N_7(11) = 272{,}250, \quad \text{and} \quad N_7(13) = 233{,}220.$$

A standard implementation can consist of two parts. First, a list of all solutions for the system of linear equations is generated, and then second part checks each solution against the conditions in the theorem. Unfortunately, checking q^d possible solutions is very time consuming when d is large.

3. Recursive Constructions

3.1 Disjoint Arrays

For later reference, we give two results on disjoint permutation arrays.

LEMMA 3.1. *There are six disjoint* $PA(n,4)$ *of size* $M(n,4)$.

Proof. Consider the images of applying a $PA(3,2)$ to the last three columns of a $PA(n,4)$. Any two permutations resulting from this either differ because of the $PA(3,2)$, or because of the first $n-3$ positions. ■

LEMMA 3.2. *The group* $\mathscr{S}_7$ *can be partitioned into* 15 $PA(7,4)$ *of size* 336. *The group* $\mathscr{S}_8$ *can be partitioned into* 15 $PA(8,4)$ *of size* 2688.

Proof. Consider the fractional linear group $G = PGL(2,7)$. Each column of permutations below, when developed under G, forms a $PA(8,4)$ of size $8 \cdot 8 \cdot 7 \cdot 6 = 2688 = 8!/15$. Fifteen disjoint PA with these parameters are obtained by applying a 5-cycle on the last five positions in each of the three PAs.

∞0163254	∞0165423	∞0163425
∞0164532	∞0162345	∞0164253
∞0152634	∞0156243	∞0152463
∞0136452	∞0134625	∞0136245
∞0146235	∞0143265	∞0146523
∞0142356	∞0142653	∞0142635
∞0125436	∞0126435	∞0125643
∞0124653	∞0124563	∞0124365

Delete ∞ and consider the group $AGL(1,7)$ for the $\mathscr{S}_7$ partition. It is a tedious exercise to verify the partitions. ■

3.2. Main Result

Let C be a k-ary code of length n and distance d, say on the alphabet $\{1,\ldots,k\}$. It is said that C has constant weight composition $(n_1,\ldots,n_k)$ if every codeword has n_i occurrences of i for $i = 1,\ldots,k$. A $PA(n,d)$ can be viewed as such a code with $k = n$ and constant composition $(1,1,\ldots,1)$.

Suppose X is a set partitioned into subsets X_i, where $|X_i| = g_i$ for $i = 1,\ldots,k$. A transversal packing of distance δ and type $g_1 g_2 \cdots g_k$ is a collection T of k-subsets of X with $|A \cap X_i| = 1$ for each i and $A \in T$ and such that $|A \cap B| \leq k - \delta$ for every $A, B \in T$. When $\delta = k$, it is, of course, optimum to take $|T| = \min_i \{g_i\}$ disjoint k-subsets of X. Most of the current literature on transversal packings concerns $\delta = k - 1$. However, there is a well-known construction for arbitrary distance δ with

each $g_i \geq q$ for q a prime power such that $\delta \leq k \leq q$. Indeed, suppose $X = (\mathbf{F}_q)^q$ and $\mathfrak{F} \subset \mathbf{F}_q[x]$ is the set of all degree $k - \delta$ polynomials. The images of $\mathbf{F}_q$ under each $f \in \mathfrak{F}$ are identified with q-subsets of X, and no two of these can intersect in more than $k - \delta$ points.

THEOREM 3.3. *Let C be a k-ary code of length n, distance d, and constant weight composition $(n_1, \ldots, n_k)$. Suppose that for each $i = 1, \ldots, k, \Gamma_i$ is a $PA(n_i, d_i)$ which can be written as a disjoint union $\Gamma_i = \cup_j \Gamma_i^{(j)}$ of $PA(n_i, d_i')$. Suppose there are transversal packings T_j of distance δ and type $|\Gamma_1^{(j)}| \cdots |\Gamma_k^{(j)}|$ for each j. Let $d \leq d_1 + \cdots + d_k$ and suppose that the sum of any δ of the d_i' is at least d. Then there is a $PA(n, d)$ of size*

$$|C| \sum_{j \geq 1} |T_j|.$$

Proof. Construct the Γ_i on disjoint sets of symbols, so the total number of symbols is n. Now fix j and consider the $\Gamma_i^{(j)}$ as a partition for the transversal packing T_j. Form concatenations of rows of $\Gamma_i^{(j)}$ according to the members of T_j. By the condition on δ-wise sums of the d_i', it follows that the minimum distance within this sub-array is at least d. By the fact that $d \leq d_1 + \cdots + d_k$, concatenations from different indices j have distance at least d. For each word of C, we form a $PA(n, d)$ in this manner by placing the symbols of Γ_i on the positions indexed by symbol i. Since the minimum distance in C is d, the same is true for the union of all resulting PAs. ■

Theorem 3.3 can be stated still more generally as a recursive construction for codes with constant weight composition. We do not here make an exhaustive exploration of even the possible PA constructions by this method. However, some special cases of interest are now mentioned.

COROLLARY 3.4. *Suppose there are disjoint $PA(n_1, 4)$ of sizes $s_1, \ldots, s_p$ and disjoint $PA(n_2, 4)$ of sizes $t_1, \ldots, t_p$. If c is the size of a binary code of length $n = n_1 + n_2$, distance 4, and constant weight n_1, then there is a $PA(n, 4)$ of size $c \sum_{j=1}^{p} s_j t_j$.*

Proof. In Theorem 3.3, take $k = 2, d = d_i' = 4, d_i = 2$, and each T_j to be the complete set of $s_j t_j$ pairs, which is trivially a distance 1 transversal packing. ■

Applying Corollary 3.4 to $10 \leq n \leq 16$, and $n_1 = \lfloor n/2 \rfloor$ produces the following lower bounds on $M(n, 4)$ (Table 4). The partitions are given by Lemmas 3.1 and 3.2, while the codes are found in Brouwer et al. [3].

For comparison, the above bound for $M(16, 4)$ is over 7.5 times the bound from Proposition 1.4. For $n/2 > 8$, a reasonable partition into disjoint PAs can be found via a greedy coloring algorithm. For instance, this approach for $n = 18$ gives a partition of $\mathscr{S}_9$ into $58 PA(9, 4)$ with the sum of squares of part sizes equal to 3110271800. The resulting bound on $M(18, 4)$ is about 1.1×10^{13}.

Table 4.

n	c	$\sum s_j t_j$	$M(n,4) \geq$
10	36	6 $(20)^2$	86,400
11	66	6 (20)(120)	950,400
12	132	6 $(120)^2$	11,404,800
13	166	6 (120)(349)	41,712,480
14	325	15$(336)^2$	550,368,000
15	585	15(336)(2688)	7,925,299,200
16	1170	15$(2688)^2$	126,804,787,200

COROLLARY 3.5. *If $n = q + q'$ is a sum of two prime powers with $0 \leq q' - q \leq 2$, then $M(n, n-2) \geq 2q(q-1)$.*

Proof. In the theorem, take $k = \delta = 2, d_1 = d_1' = q - 1$ and $d_2 = d_2' = q' - 1$. We use the two-word binary code C of length n, weight q, and distance $d = n - (q' - q)$. ■

EXAMPLE 3.6. *A quaternary code with composition $(4,4,4,4)$ and $d = 9$ of size 403 can be found by running a greedy algorithm similar to that in Section 2. In Theorem 3.3, take $\delta = 3, d_i = d_i' = 3$ for all i to get $M(16,9) \geq 403(12)^2 = 58{,}032$. This is exceeded by the trivial lower bound $M(16,9) \geq 97{,}569$. However, it should be mentioned that the latter is not constructive, while the recursive method offers more structure for the resulting* PA.

Although the best use of Theorem 3.3 is often with binary codes, it is hoped that further study of constant composition codes with $k > 2$ may furnish nice examples of permutation arrays.

4. Conclusions

Table 5 and the list below summarize some various old and new lower bounds on $M(n,d)$. The subscript c represents values obtained from direct computer construction in Section 2.1; p represents values obtained from permutation polynomials in Section 2.2; and r represents values obtained from the recursive method in Section 3. A subscript d denotes that this value is obtained from lower entries by part (e) of Proposition 1.1. Bold entries in Table 5 are exact.

$$M(14,4) \geq 550368000_r \qquad M(14,10) \geq 6552_c$$
$$M(15,13) \geq 2(42) = 84_r \qquad M(16,12) \geq 21120_p$$
$$M(17,12) \geq 83504_p \qquad M(22,20) \geq 2(110) = 220_r$$
$$M(23,18) \geq 291456_p \qquad M(32,28) \geq 372992_p$$

Table 5.

n	4	5	6	7	8	9	10	11	12	13
4	**4**									
5	**20**	**5**								
6	**120**	**18**	**6**							
7	349_c	77_c	**42**	**7**						
8	2688_c	560_p	**336**	**56**	**8**					
9	18144_c	1944_c	1512_c	**504**	**72**	**9**				
10	86400_r	13680_c	4320_c		**720**	35_c	**10**			
11	950400_r	60940_d	9790_d		**7920**	154_c	**110**	**11**		
12	11404800_r	731280_c	117480_c		**95040**		**1320**	60	**12**	
13	41742480_r	878778	271908_p			3588_c		**156**		**13**

Acknowledgments

The authors thank Manish Gupta and Alan C. H. Ling for fruitful conversations on this topic. The authors research is supported by the Army Research Office under grant number DAAD 19-01-1-0406.

References

1. R. Battiti and M. Protasi, Reactive local search for the maximum clique problem, *Algorithmica*, Vol. 29 (2001) pp. 610–637.
2. A. Bonisoli and P. Quattrocchi, Each invertible sharply d-transitive finite permutation set with $d \geq 4$ is a group, *J. Algebraic Combin.*, Vol. 12 (2000) pp. 241–250.
3. A. E. Brouwer, James B. Shearer, N. J. A. Sloane and Warren D. Smith, A new table of constant weight codes, *IEEE Trans. Inform. Theory*, Vol. 36 (1990) pp. 1334–1380.
4. C. J. Colbourn, T. Kløve and A. C. H. Ling, Permutation arrays for powerline communication and mutually orthogonal Latin squares, *IEEE Trans. Information Theory* (to appear).
5. P. Das, The number of permutation polynomials of a given degree over a finite field, *Finite Fields and Their Applications*, Vol. 8 (2002) pp. 478–490.
6. D. R. de la Torre, C. J. Colbourn and A. C. H. Ling, An application of permutation arrays to block ciphers. *Proceedings of the Thirty-first Southeastern International Conference on Combinatorics, Graph Theory and Computing* (Boca Raton, FL, 2000). *Congr. Numer.*, Vol. 145 (2000) pp. 5–7.
7. M. Deza and S. A. Vanstone, Bounds for permutation arrays, *J. Statist. Plann. Inference*, Vol. 2 (1978) pp. 197–209.
8. H. C. Ferreira and A. J. H. Vinck, Interference cancellation with permutation trellis codes, *Proc. IEEE Vehicular Technology Conference*, Vol. 5 (2000) pp. 2401–2407.
9. P. Frankl and M. Deza, On the maximum number of permutations with given maximal or minimal distance, *J. Combin. Theory Ser. A*, Vol. 22 (1977) pp. 352–360.
10. R. Lidl and H. Niederreiter, *Finite Fields*, second edition, Cambridge University Press (1997).
11. N. Pavlidou, A. J. H. Vinck, J. Yazdani and B. Honary, Power line communications: State of the art and future trends, *IEEE Communications Magazine*, (2003) pp. 34–40.
12. F. Ruskey, C. R. Miers and J. Sawada, The number of irreducible polynomials and Lyndon words with given trace, *SIAM J. Discrete Math.*, Vol. 14 (2001) pp. 240–245.

13. M. Svanström, P. R. J. Östergard and G. T. Rumelova, Bounds and constructions for ternary constant-composition codes, *IEEE Trans. Inform. Theory*, Vol. 48 (2002) pp. 101–111.
14. H. Tarnanen, Upper bounds on permutation codes via linear programming, *European J. Combin.*, Vol. 20 (1999) pp. 101–114.