Frequency Permutation Arrays

Sophie Huczynska[1] and Gary L. Mullen[2]
[1]*School of Mathematics and Statistics, Mathematical Institute, North Haugh, St. Andrews, Fife KY16 9SS, United Kingdom; E-mail: sophieh@mcs.st-andrews.ac.uk*

[2]*Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, U. S. A.; E-mail: mullen@math.psu.edu*

Received June 6, 2005; revised November 3, 2005

Published online 4 January 2006 in Wiley InterScience (www.interscience.wiley.com).
DOI 10.1002/jcd.20096

Abstract: Motivated by recent interest in permutation arrays, we introduce and investigate the more general concept of frequency permutation arrays (FPAs). An FPA of length $n = m\lambda$ and distance d is a set T of multipermutations on a multiset of m symbols, each repeated with frequency λ, such that the Hamming distance between any distinct $x, y \in T$ is at least d. Such arrays have potential applications in powerline communication. In this article, we establish basic properties of FPAs, and provide direct constructions for FPAs using a range of combinatorial objects, including polynomials over finite fields, combinatorial designs, and codes. We also provide recursive constructions, and give bounds for the maximum size of such arrays. © 2006 Wiley Periodicals, Inc. J Combin Designs 14: 463–478, 2006.

Keywords: *permutation arrays*

1. INTRODUCTION

As indicated in [4] and [7], permutation arrays arise in the study of permutation codes, which in turn have a natural applicability to powerline communications. An electric power line may be used to transmit information in addition to electric power, by modulating its frequency to form a set of frequencies, and transmitting the symbols of codewords in time as the corresponding frequencies. Steps must be taken to ensure that this information transmission does not interfere with the line's primary function of power transmission, and for this reason block coding is used (codewords of fixed length). A code is a *constant composition code* if each codeword, of length n, has precisely r_i occurrences of the i-th symbol, where the r_i are positive integers

Contract grant sponsor: Royal Society Dorothy Hodgkin Fellowship.

satisfying $\sum_{i=1}^{m} r_i = n$. (Here, the i-th symbol corresponds to the i-th frequency.) Various tradeoffs must be made between the competing goals of addressing noise problems and the requirement of a constant power envelope.

One approach is to choose $r_1 = r_2 = \cdots = r_n = 1$, in which case each codeword is a permutation on n symbols. An (n, d) permutation array, usually denoted by $PA(n, d)$, is a set of permutations of n symbols with the property that the Hamming distance between any two distinct permutations in the set is at least d. Permutation arrays are important not only in powerline communications as described above; they have also been applied in the design of block ciphers; see [9].

In this article, we introduce a generalization of permutation arrays, which we call *frequency permutation arrays*. These arise from the constant composition codes when we take $r_1 = r_2 = \cdots = r_m = \lambda$, for some λ such that $n = m\lambda$. When $\lambda = 1$, this reduces to the permutation case studied in [4] and [7]. We present various results and constructions for frequency permutation arrays, many of which have well-known permutation array results as special cases. There is a strong connection with recent work on constant composition codes such as [5] and [11].

2. FREQUENCY PERMUTATION ARRAYS

Consider a multiset of size $n = m\lambda$ $(m, \lambda \in \mathbb{N})$ consisting of m elements, each occurring λ times. We define a *λ-permutation* to be a multipermutation of such a multiset. When $\lambda = 1$, the set of all λ-permutations is the symmetric group S_n of permutations on n symbols. In general, we shall take the multiset to be $\{0, \ldots, 0, 1, \ldots, 1, \ldots, m-1, \ldots, m-1\}$ or $\{1, \ldots, 1, 2, \ldots, 2, \ldots, m, \ldots, m\}$ (each element occurring λ times).

Definition 2.1. *Two distinct λ-permutations $\sigma = s_1 \ldots s_n$, $\tau = t_1 \ldots t_n$ have distance $d(\sigma, \tau) = d$ if they disagree in d entries, that is if $|\{i : s_i \neq t_i\}| = d$.*

This is the Hamming distance familiar from coding theory. In the case when $\lambda = 1$, two permutations $\sigma, \tau \in S_n$ have distance d if $\sigma\tau^{-1}$ has exactly $n - d$ fixed points.

Definition 2.2. *A permutation array of length n and minimum distance d, denoted by $PA(n, d)$, is a subset T of S_n such that the distance between any two members of T is at least d. A $PA(n, d)$ may be viewed as an $s \times n$ array whose rows are the s permutations of T in image form; taken pairwise, any two distinct rows differ in at least d positions. The maximum possible size of a $PA(n, d)$ is denoted by $M(n, d)$.*

We define a frequency permutation array as follows.

Definition 2.3. *Let $n = m\lambda$ and let S be a multiset comprising λ occurrences each of m symbols. A frequency permutation array of length n, frequency λ, and minimum distance d, denoted by $FPA_\lambda(n, d)$, is a set T of λ-permutations of the symbols of S, with the property that the distance between any two members of T is at least d. Equivalently, an $FPA_\lambda(n, d)$ is an $s \times n$ array whose s rows consist of m distinct symbols, each repeated exactly λ times, such that taken pairwise any two rows differ in at least d positions.*

Thus an $FPA_1(n,d)$ is simply a $PA(n,d)$. We let $M_\lambda(n,d)$ denote the maximum possible number of rows that can exist in any $FPA_\lambda(n,d)$; then $M_1(n,d) = M(n,d)$.

Example 2.4. An $FPA_3(6,4)$ of size 4 is given by

$$L_1 = \begin{matrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{matrix}$$

We first establish basic properties of frequency permutation arrays. Various basic results on permutation arrays (for example from [4] and [7]) appear as special cases of these results.

Theorem 2.5. *Let $n = m\lambda$. Then*

(i) $M_\lambda(n,2) = \frac{n!}{(\lambda!)^m}$;
(ii) $M_\lambda(n,n) = m$;
(iii) $M_\lambda(n,d) \geq M_\lambda(n-\lambda,d), M_\lambda(n,d+1)$;
(iv) *If $n_1 = m\lambda_1$ and $n_2 = m\lambda_2$, then*

$$M_{\lambda_1+\lambda_2}(n_1+n_2,d_1+d_2) \geq \min\{M_{\lambda_1}(\mathrm{n_1},\mathrm{d_1}),\mathrm{M}_{\lambda_2}(\mathrm{n_2},\mathrm{d_2})\}.$$

In particular, $M_{2\lambda}(2n,2d) \geq M_\lambda(n,d)$.
(v) $M_\lambda(n,d) \leq \frac{n!}{\lambda(d-1)!}$; $M_\lambda(n,d) \leq \frac{n!}{\lambda(d-1)!}$

Moreover, for any divisor l of λ, $M_\lambda(n,d) \leq \frac{l}{\lambda}M_l(n,d)$.

Proof.

(i) Since two distinct multipermutations must differ in at least two entries, $M_\lambda(n,2)$ is the number of distinct λ permutations. There are $\binom{n}{y}\cdot\binom{n-\lambda}{\lambda}\cdots\binom{n-(m-1)\lambda}{\lambda}$ choices for each λ-permutation, that is $\binom{m\lambda}{\lambda}\cdot\binom{(m-1)\lambda}{\lambda}\ldots\binom{x}{y}\binom{\lambda}{\lambda} = \frac{(m\lambda)!}{(\lambda!)^m}$ such multipermutations in total.
(ii) Since there are at most m choices for the symbol in the first position of a λ-permutation in an $FPA_\lambda(n,n)$, we have $M_\lambda(n,n) \leq m$. Take m blocks comprising λ copies of each symbol: $\{0\ldots0\}$, $\{1,\ldots,1\}$, …, $\{m-1,\ldots,m-1\}$; applying an m-cycle to these blocks yields m λ permutations, all of pairwise distance n.
(iii) Adding λ copies of some new symbol to each row of an $FPA_\lambda(n-\lambda,d)$ yields an $FPA_\lambda(n,d)$; the second observation is immediate from the definition.
(iv) Juxtaposing an $FPA_{\lambda_1}(n_1,d_1)$ and an $FPA_{\lambda_2}(n_2,d_2)$ yields an $FPA_\lambda(n,d)$ with $\lambda = \lambda_1+\lambda_2$, $n = n_1+n_2$, and $d = d_1+d_2$.
(v) This is proved in Theorem 4.1; from [4], the size of a $PA(n,d)$ is bounded above by $n!/(d-1)!$. □

For any λ-permutation σ, the sphere with centre σ and radius r is defined to be the set of all λ permutations with distance at most r from σ. We denote its volume by $V_\lambda(n,r)$.

Lemma 2.6. *Let $n = m\lambda$. Then*

$$V_\lambda(n,r) = 1 + \sum_{k=1}^{r} \sum_{P(k)} \frac{m!}{r_1! \dots r_s!(m-t)!} \binom{\lambda}{k_1}\binom{\lambda}{k_2} \dots \binom{\lambda}{k_t} (-1)^k \int_0^\infty e^{-x} \left\{ \prod_{j=1}^{t} L_{k_j}(x) \right\} dx,$$

where $L_k(x)$ is the kth Laguerre polynomial. Here the inner sum runs over $P(k) = \{(k_1, \dots, k_t; r_1, \dots, r_s)\}$, the set of all partitions $k_1 + \dots + k_t$ of $k \in \mathbb{N}$ into positive integers $1 \le k_i \le \lambda$, where the set $\{k_1, \dots, k_t\}$ consists of r_j occurrences of value k_{i_j} ($j = 1, \dots, s$), with $1 \le k_{i_j} \le \lambda$, $1 \le r_j \le t$, and $r_1 + \dots + r_s = t$.

Proof. Let σ be any λ-permutation of length n. The set of λ permutations at distance k from σ is obtained by taking each k-entry subset of σ, and deranging its entries. By a result obtained in [12], and reproved in [3], the number of derangements of a sequence composed of n_1 objects of type 1, n_2 objects of type 2,..., n_t objects of type t (i.e., permutations in which no object occupies a site originally occupied by an object of the same type) is given by

$$D(n_1, \dots, n_t) = (-1)^N \int_0^\infty e^{-x} \left\{ \prod_{j=1}^{t} L_{n_j}(x) \right\} dx,$$

where $n_1 + \dots + n_t = N$. The result follows upon applying this theorem to each k-element subset of σ. For any λ-permutation σ, and any partition $k_1 + \dots + k_t$ of $k \in \mathbb{N}$ into positive integers $1 \le k_i \le \lambda$ ($1 \le t \le m$), we count the number of k subsets comprising k_1 occurrences of symbol s_1, k_2 occurrences of symbol s_2, ..., k_t occurrences of symbol s_t. Suppose the set $\{k_1, \dots, k_t\}$ consists of r_1 occurrences of value k_{i_1}, ..., r_s occurrences of value k_{i_s}, where $r_1 + \dots + r_s = t$. There are $\binom{m}{r_1}\binom{m-r_1}{r_2} \dots \binom{m-\sum_{i=1}^{s-1} r_i}{r_s} = \frac{m!}{r_1! \dots r_s!(m-t)!}$ choices for symbols $s_1, \dots, s_t$. For each choice, there are $\binom{\lambda}{k_1}\binom{\lambda}{k_2} \dots \binom{\lambda}{k_t}$ subsets of σ in which elements occur with appropriate frequency. □

A covering argument yields the following lower bound for $M_\lambda(n,d)$, an analog of the Gilbert–Varshamov bound in coding theory, while a sphere-packing argument yields an upper bound, analogous to the Hamming bound for coding.

Theorem 2.7.

$$\frac{n!}{(\lambda!)^m V_\lambda(n, d-1)} \le M_\lambda(n,d) \le \frac{n!}{(\lambda!)^m V_\lambda(n, \lfloor \frac{d-1}{2} \rfloor)}.$$

A useful upper bound for the maximum size of general constant-composition codes (CCCs) has recently been presented in [16] and has been further developed in [11]. For a CCC in which all symbols of a codeword occur with equal frequency λ (corresponding to an FPA), this upper bound reduces to the Plotkin bound.

Proposition 2.8. (Plotkin bound). *For $\lambda > n - d$,*

$$M_\lambda(n,d) \le \frac{d}{d-n+\lambda}.$$

We observe that, since the direct constructions presented in this article have frequency less than or equal to $n-d$, the bound is of limited applicability in our setting. However, the reader is referred to [11] for a construction of CCC's which include some $FPA_\lambda(n,d)$'s with $\lambda > n-d$.

3. DIRECT CONSTRUCTIONS

It is known that permutation arrays may be constructed using latin squares (see [4] and [13]). Frequency permutation arrays are related to frequency squares as permutation arrays are to latin squares, and this connection may be exploited to obtain a construction for FPAs.

Recall that a *latin square of order n* is an $n \times n$ array in which n distinct symbols are arranged so that each symbol occurs once in each row and column. Two latin squares L_1 and L_2 of the same order n are said to be *orthogonal* if, when superimposed, each of the possible n^2 ordered pairs occurs exactly once. A set $\{L_1, L_2, \ldots, L_t\}$ of $t \geq 2$ latin squares is said to be *mutually orthogonal* (a set of MOLS) if the squares in the set are pairwise orthogonal. Latin squares have been generalized to allow repetitions of elements in each row and column.

Definition 3.1. *Let $n = m\lambda$. An $F(n;\lambda)$ frequency square is an $n \times n$ array in which each of m distinct symbols occur exactly λ times in each row and column. Moreover two such squares are orthogonal if when superimposed, each of the m^2 possible ordered pairs occurs λ^2 times.*

The following result in fact contains Proposition 1.2 of [4] as a special case.

Theorem 3.2. *If there are E mutually orthogonal frequency squares of type $F(n;\lambda)$ where $n = m\lambda$, then $M_\lambda(n\lambda, n\lambda - \lambda^2) \geq mE$. In particular, if q is a prime power and $i \geq 1$ is a positive integer, then*

$$M_{q^{i-1}}(q^{2i-1}, q^{2i-1} - q^{2i-2}) \geq q(q^i - 1)^2/(q-1).$$

Further if $i = 1$, $M_1(q, q-1) = q(q-1)$.

Proof. Label the rows and columns of each $n \times n$ frequency square by the elements $0, 1, , n-1$. Then from each of the frequency squares, form a set of $n\lambda$-tuples as follows. For each symbol $i = 0, 1, , m-1$, form an $n\lambda$-tuple by listing the cell locations (k, l) where i occurs in the given square, proceeding row-by-row as k runs from 0 to $n-1$. Viewed as m blocks, each of size $n\lambda$, of an affine resolvable design, these form a parallel class of size m. In total from the E squares, Em such $n\lambda$ tuples are obtained, corresponding to E parallel classes. The entries of each $n\lambda$-tuple are ordered pairs; form new $n\lambda$ tuples by disregarding the first coordinate of each ordered pair. The resulting $n\lambda$ tuples form the rows of an $FPA_\lambda(n\lambda, n\lambda - \lambda^2)$. For, since each symbol occurs λ times in each column of a frequency square, each row of the array comprises λ copies of each of the n column headings. Any two rows of the FPA arising from the same parallel class will have distance $n\lambda$. Any two rows derived from different classes will, due to the orthogonality of the corresponding frequency squares, agree in at most λ^2 positions, since agreement in p positions implies that some ordered pair occurs p times when the MOFS are juxtaposed. Hence the array has minimum distance $n\lambda - \lambda^2$. □

For $n = m\lambda$, it is known that the maximum number of mutually orthogonal frequency squares (MOFS) of the form $F(n;\lambda)$ is bounded above by $(n-1)^2/(m-1)$. Further, if q is any prime power and $i \geq 1$ is a positive integer, then using linear polynomials in $2i$ variables over the finite field F_q, a complete set of $F(q^i;q^{i-1})$ MOFS can be constructed. Specifically, take the polynomials $a_1x_1 + \cdots + a_{2i}x_{2i}$ where neither $(a_1,\ldots,a_i)$ nor $(a_{i+1},\ldots,a_{2i})$ is the zero vector $(0,\ldots,0)$ and no two of the vectors are nonzero F_q multiples of each other, that is $(a_1',\ldots,a_{2i}') \neq e(a_1,\ldots,a_{2i})$ for any nonzero $e \in F_q$. Further details may be found in Chapter 4 of [14].

We remark in passing that, while the array obtained from Theorem 3.2 is optimal in size when $i = 1$, it is not necessarily optimal for $i > 1$. This is in some sense expected because, in using these complete sets of mutually orthogonal frequency squares to construct error-correcting codes, the resulting codes are maximal distance separable only in the case when $i = 1$; see [10]. For example in the case $q = i = 2$, Theorem 4.6 yields an $FPA_2(8,4)$ with more than 18 rows (see Example 4.7).

Another way to build frequency permutation arrays utilises finite fields, and may be considered as extending the approach of Theorem 2.4 of [4].

Theorem 3.3. *Let $L(x) = \sum_{s=0}^{i-1} \alpha_s x^{q^s} \in F_{q^i}[x]$. Denote by q^l the degree of $L(x)$, and by r the rank of the matrix*

$$A(L) = \begin{pmatrix} \alpha_0 & \alpha_{i-1}^q & \alpha_{i-2}^{q^2} & \ldots & \alpha_1^{q^{i-1}} \\ \alpha_1 & \alpha_0^q & \alpha_{i-1}^{q^2} & \ldots & \alpha_2^{q^{i-1}} \\ \alpha_2 & \alpha_1^q & \alpha_0^{q^2} & \ldots & \alpha_3^{q^{i-1}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{i-1} & \alpha_{i-2}^q & \alpha_{i-3}^{q^2} & \ldots & \alpha_0^{q^{i-1}} \end{pmatrix},$$

so that $1 \leq r \leq i$. Let $0 < d < q^{i-l}$. Then

$$M_{q^{i-r}}(q^i, q^i - dq^l) \geq \sum_{j=1}^{d} \frac{N_j(q^i)}{q^{i-r}},$$

where $N_j(q^i)$ denotes the number of permutation polynomials over F_{q^i} of degree j.

Proof. It is a well-known result (see p 361 of [15]) that the linearized polynomial $L(x)$ is a permutation polynomial of F_{q^i} if and only if the determinant of the matrix $A(L)$ is non-zero. More generally, the value set of L has cardinality q^r, where r is the rank of $A(L)$. So the linear transformation on F_{q^i} defined by the polynomial $L(x)$ has image of cardinality q^r and kernel of cardinality q^{i-r}. Note that $q^{i-r} \leq q^l$.

Form an array as follows: for each permutation polynomial $f(x)$ over F_{q^i}, form a row by taking the images of the function $L(f(x))$ as x runs through the elements of the field F_{q^i}. Each row is a λ-permutation of length q^i on $m = q^r$ symbols, each occurring with frequency $\lambda = q^{i-r}$. If $f(x)$ and $g(x)$ are permutation polynomials over F_{q^i} of degrees at most d, then the polynomial $L(f(x)) - L(g(x))$ has degree at most dq^l.

Hence (unless it is the zero polynomial) it has at most dq^l roots in F_{q^i}, and so appropriately chosen $f(x)$ and $g(x)$ yield distinct rows of distance at least $q^i - dq^l$. We must now ensure that $L(f-g)$ is not the zero polynomial. This happens if and only if the value set of the polynomial $f-g$ lies wholly within the kernel of L, which has cardinality q^{i-r}. Suppose first that $f-g$ is non-constant. Now, $f-g$ has degree at most $d<q^{i-l}$ and, since a polynomial of degree d cannot have more than d roots in a field, its value set has cardinality at least $\lfloor\frac{q^i-1}{d}\rfloor + 1 > q^l \geq q^{i-r}$. So the value set of $f-g$ cannot be contained entirely within the set of q^{i-r} values mapped by L to zero, and hence $L(f-g)$ is not the zero polynomial. For the constant case note that, for any permutation polynomial $f(x)$, all $f(x)+c$ with $c \in F_{q^i}$ are also permutation polynomials. For $f(x)+c$ to yield distinct rows, c must run through precisely one representative for each coset of the kernel of L; there are q^r of these. Taking q^r/q^i of the total number of permutation polynomials yields the desired number of rows. □

Observe that, in Theorem 3.3, if we take L to be the permutation polynomial $x^{q^{i-1}}$, we have maximal rank $r=i$ and degree $q^l = q^{i-1}$, so we obtain a $PA(q^i, q^i - dq^{i-1})$ of size $\sum_{j=1}^{d} N_j(q^i)$.

To build an FPA with desired parameters, appropriate linearized polynomials may be chosen, as illustrated in the following corollaries.

Corollary 3.4. *Let q be a prime power and let i and n be positive integers such that $n(<i)$ divides i. Let $0<d<q^{i-n}$. Then*

$$M_{q^n}(q^i, q^i - dq^n) \geq \sum_{j=1}^{d} \frac{N_j(q^i)}{q^n},$$

where $N_j(q^i)$ denotes the number of permutation polynomials over F_{q^i} of degree j.

Proof. Let $L(x) = x^{q^n} - x$ in Theorem 3.3; its roots are precisely the elements of F_{q^n}. The polynomial L defines a linear transformation on F_{q^i} whose kernel is the subfield F_{q^n} and whose value set has cardinality q^{i-n}. For permutation polynomials f, g of degree at most $d<^{i-n}$, non-constant $f-g$ has value set of cardinality at least $\lfloor\frac{q^i-1}{d}\rfloor + 1 > q^n$ and so identical rows can arise only in the case when $g(x) = f(x)+c$ with $c \in F_{q^n}$. □

Recall that the trace function $TR: F_{q^i} \to F_q$ is defined for $\alpha \in F_{q^i}$ by $TR(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + +\alpha^{q^{i-1}}$. More generally, letting $i = gh$ and setting $E = F_{q^i}$ and $F = F_{q^h}$, the trace function $TR_{E/F}: E \to F$ is defined for $\alpha \in E$ by

$$TR_{E/F}(\alpha) = \alpha + \alpha^{q^h} + \alpha^{q^{2h}} + \ldots + \alpha^{q^{(g-1)h}}.$$

Corollary 3.5. *Let q be a prime power and let i and h be positive integers such that h divides i. Let $0<d<q^h$. Then*

$$M_{q^{i-h}}(q^i, q^i - dq^{i-h}) \geq \sum_{j=1}^{d} \frac{N_j(q^i)}{q^{i-h}}.$$

Proof. Let $i = gh$, let $E = F_{q^i}$ and $F = F_{q^h}$. Take L to be the generalized trace function $TR_{E/F}$ defined above; its kernel has cardinality q^{i-h} and its value set has cardinality q^h. For any two permutation polynomials f, g over F_{q^i} of degree at most $d <^h$, the value set of (non-constant) $f - g$ has cardinality at least $\lfloor \frac{q^i-1}{d} \rfloor + 1 > q^{i-h}$ and so $TR(f - g)$ is not the zero polynomial. As in the proof of Theorem 3.3 dividing by q^{i-h} deals with the case when $f - g$ is constant. □

In the next section, we consider how a PA may be converted into an FPA by appropriate substitutions on its symbols. If q is a prime power, a natural choice might be to apply the trace function to the rows of a $PA(q^i, d)$. However if, for example, there are two rows in the $PA(q^i, d)$ which differ by a constant $a \in F_{q^i}$ with $TR(a) = 0$, then the resulting two rows in the FPA will be identical and so the rows will have distance 0. Thus applying the trace function to the elements of an arbitrary PA does not appear to be a good method to apply in a general setting.

We refer to [8] for a method for computing the value of $N_j(q^i)$ for any prime power q and positive integers i and j. Note, however, that the result of [8] requires considerable computation to compute, and that the corresponding permutation polynomials which arise from solutions to the system of equations in [8] must be constructed before the FPA can be built. In the case when $d = 1$ however, it is clear that $N_1(q^i) = (q^i - 1)q^i$, the number of linear polynomials over F_{q^i}. So, $M_{q^{i-h}}(q^i, q^i - q^{i-h}) \geq q^h(q^i - 1)$. For example, $M_3(9, 6) \geq 24$, $M_4(8, 4) \geq 14$, and $M_2(4, 2) \geq 6$. All of these are optimal: the first by known results for ternary codes (17]), the second by Theorem 5.2 since a Hadamard matrix of order 8 exists, and the third (trivially) by Theorem 2.5. An alternative construction for an $FPA_4(8, 4)$ of size 14 is given in the last section.

Affine resolvable designs can be used to construct FPAs. A *balanced incomplete block design* consists of a finite set V of v points, and a collection B of equally sized subsets of V called blocks, each of size k, such that every pair of distinct points of V occurs in exactly λ blocks. A *resolvable* design has the additional property that the collection B of blocks can be partitioned into *parallel classes* (or resolution classes), such that every point of V occurs exactly once in each parallel class. An *affine resolvable design* (ARD) is a resolvable design with the further property that any two non-parallel blocks intersect in precisely μ points, where $\mu = \frac{k^2}{v} \in \mathbb{N}$. When $\mu = 1$, the ARD is an affine plane of order k^2.

Proposition 3.6.

(i) *Given an affine resolvable* (v, k, λ) *design with* r *parallel classes, an* $FPA_k(v, v - k)$ *may be constructed of size* r.
(ii) *If there exist* m *MOLS of order* n, *then an* $FPA_n(n^2, n^2 - n)$ *may be constructed of size* $m + 2$. *In particular, if* q *is a prime power, an* $FPA_q(q^2, q^2 - q)$ *may be constructed of size* $q + 1$.

More details of this approach, including a proof of Prop. 3.6(i), may be found in [5]. In the MOLS case, a standard construction may be used to build $m + 2$ parallel classes of an affine plane from the m MOLS, and these classes then used in part (i) to form an $FPA_n(n^2, n^2 - n)$. Equivalently, this FPA may be constructed directly by writing the rows of each of the $m + 2$ latin and index squares side-by-side to form new rows of length n^2.

Example 3.7. *Using the following* 2 *MOLS of order* 3

$$L_1 = \begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix}, \quad L_2 = \begin{matrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{matrix}$$

yields the following $FPA_3(9, 6)$*:*

$$\begin{matrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0. \end{matrix}$$

Frequency permutation arrays can also be constructed from MDS codes. Recall that a q-ary (n, k) code is said to be maximal distance separable (MDS) if it satisfies the Singleton bound with equality, that is if $d = n - k + 1$.

Theorem 3.8. *Given an* $[n, k, d]$ *MDS linear code* C *over* F_q, *the array formed by taking the codewords of* C *as columns is an* $FPA_{q^{k-1}}(q^k, q^k - q^{k-1})$.

Proof. Let C be an $[n, k, d]$ MDS linear code over F_q. Let G be a $k \times n$ generator matrix for the code C, and write $G = [C_1 C_2 \ldots C_n]$, where the C_i are the columns of G. Form an $n \times q^k$ array A by taking the codewords of C as the columns of A. These are given by $G^T x^T = C^T$ as x runs through F_q^k; the rows ${C_1}^T, \ldots, {C_n}^T$ of G^T can be viewed as generating the rows of A.

Each element of F_q occurs in each row of A with frequency q^{k-1}, that is occurs q^{k-1} times as the ith coordinate of the codewords of C. Let $g_1, ..., g_k$ be the elements in the i-th column C_i of G, and consider the equation $a_1 g_1 + ... + a_k g_k = b$, where $b, a_1, \ldots, a_k \in F_q$. Since C_i has at least one non-zero value, say in the j-th row, we can isolate the term $a_j g_j = b - \sum_{l \neq j} a_l g_l$. Then we can arbitrarily assign q values to each of $k - 1$ remaining a's, and uniquely solve the equation for a_j since $g_j \neq 0$. Thus there are q^{k-1} solutions for each value of b in the i-th coordinate.

Consider the distance between the two rows of the FPA corresponding to ${C_i}^T$ and ${C_j}^T$. We have the system of equations ${C_i}^T \cdot (x_1, \ldots, x_k) = \alpha$ and ${C_j}^T \cdot (x_1, \ldots, x_k) = \beta$ $(\alpha, \beta \in F_q)$. For an MDS code, any k columns (in particular, any two columns) of the generator matrix are linearly independent. Since ${C_i}^T$ and ${C_j}^T$ are linearly independent, this system of two linear equations in k variables will have rank 2, and thus q^{k-2} solutions. This means that every ordered pair (α, β) occurs q^{k-2} times. Thus, in particular, the q ordered pairs $(\alpha, \alpha), \alpha \in F_q$ are obtained q^{k-2} times, so A is an FPA with distance $q^k - qq^{k-2} = q^k - q^{k-1}$. □

Note that Example 3.7 may alternatively be obtained by the MDS construction using the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Definition 3.9. *An orthogonal array of size* v, *with* r *constraints,* s *levels, and strength* t, *denoted* $OA[v, r, s, t]$, *is an* $r \times v$ *array with entries from a set of* $s \geq 2$

symbols, having the property that in every $t \times v$ submatrix, every $t \times 1$ column vector appears the same number v/s^t of times.

The frequency permutation arrays constructed in Proposition 3.6 and Theorem 3.8 are in fact orthogonal arrays. This gives rise to the following observation.

Proposition 3.10. *Every orthogonal array $OA[v, r, s, 2]$ of strength 2 is an $FPA_{\frac{v}{s}}(v, v - \frac{v}{s})$ of size r.*

Proof. In any row, each of the s symbols occurs with frequency v/s. For any pair of rows, each of the s^2 pairs (i,j) of elements occurs v/s^2 times. In particular, each of the s pairs (i, i) occurs v/s^2 times, and hence two rows agree pairwise in precisely v/s positions. □

Note that the FPAs obtained in this way are equidistant, in the sense that any two rows have distance precisely $v - \frac{v}{s}$. For construction of orthogonal arrays, see for example [6]; their connection with affine resolvable designs is explored in [1].

4. CONSTRUCTING NEW FPAS FROM OLD

In this section, we explore how one or more FPAs may be used as ingredients in the construction of new FPAs.

Theorem 4.1.

(i) *Given an $FPA_\lambda(n, d)$ of size N, a $PA(n, d)$ may be constructed of size λN. In particular, $M_\lambda(n, d) \le \frac{M(n,d)}{\lambda}$.*
(ii) *Let l divide λ. Given an $FPA_\lambda(n, d)$ of size N, an $FPA_l(n, d)$ may be constructed, of size $\frac{\lambda}{l}N$. In particular, $M_\lambda(n, d) \le \frac{l}{\lambda} M_l(n, d)$.*

Proof.

(i) Denote the $FPA_\lambda(n, d)$ by A; let the symbol set of A be $\{0, 1, \ldots, m-1\}$. Using appropriate substitutions, A can be converted to a $PA(n, d)$, A', of size N. For a row R of A, moving from left to right, replace the λ occurrences of a given symbol s by the sequence $s\lambda + 1, s\lambda + 2, \ldots, (s+1)\lambda$ $(0 \le s \le m-1)$. The new row R' is a permutation of $1, 2, \ldots, n$. Since agreement between any two rows of A' can occur only at positions of agreement between the corresponding rows of A, the PA A' has minimal distance d. Now perform a cyclic shift on the entries of each substitution set $\{s\lambda + 1, s\lambda + 2, \ldots, (s+1)\lambda\}$ $(0 \le s \le m-1)$. This process can be repeated λ times, to obtain λ different substitutions for R; all have pairwise distance n. Apply this process to each row of A; the distance between new rows corresponding to different rows of A is at least d. Hence we have a $PA(n, d)$ of size λN.
(ii) The proof is analogous to that of part (i). In this case, the substitution set for a given symbol s of the $FPA_\lambda(n, d)$ comprises l copies each of $\frac{\lambda}{l}$ symbols.

The generalization of the λ cyclic shifts applied to the substitution sets, is the set of λ/l permutations comprising an $FPA_l(\lambda, \lambda)$, described in part (ii) of Theorem 2.5. □

Example 4.2. *An* $FPA_6(12, 6)$ *is constructed in Example* 5.3. *By Theorem* 4.1, *this FPA can be converted first to an* $FPA_3(12, 6)$ *and then to a* $PA(12, 6)$. *We illustrate the use of the substitutions (without the cyclic shifts) on four sample rows.*

The first four rows of the $FPA_6(12, 6)$ are

$$\begin{array}{cccccccccccc} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{array}$$

After substitutions, four rows of the $FPA_3(12, 6)$ are

$$\begin{array}{cccccccccccc} 3 & 1 & 3 & 1 & 3 & 4 & 4 & 1 & 2 & 2 & 4 & 2 \\ 3 & 1 & 1 & 3 & 1 & 3 & 4 & 4 & 2 & 2 & 2 & 4 \\ 3 & 3 & 1 & 1 & 3 & 1 & 4 & 4 & 4 & 2 & 2 & 2 \\ 3 & 1 & 3 & 1 & 1 & 3 & 2 & 4 & 4 & 4 & 2 & 2 \end{array}$$

After substitutions, four rows of the $FPA_6(12, 6)$ are

$$\begin{array}{cccccccccccc} 7 & 1 & 8 & 2 & 9 & 10 & 11 & 3 & 4 & 5 & 12 & 6 \\ 7 & 1 & 2 & 8 & 3 & 9 & 10 & 11 & 4 & 5 & 6 & 12 \\ 7 & 8 & 1 & 2 & 9 & 3 & 10 & 11 & 12 & 4 & 5 & 6 \\ 7 & 1 & 8 & 2 & 3 & 9 & 4 & 10 & 11 & 12 & 5 & 6 \end{array}$$

Converting a PA to an FPA by substitution is less straightforward in general. The next result applies, for example, to an FPA arising from an orthogonal array.

Proposition 4.3. *Let* $n = m\lambda$. *Let A be an* $FPA_\lambda(n, d)$ *such that, between any two rows, each of the* m^2 *pairs* (i, j) *occurs precisely t times. Then A may be converted, by reduction mod r (where* $r|m$*) to an* $FPA_{\frac{n}{r}}(n, n - \frac{tm^2}{r})$.

Proof. Reduce the entries of A mod r. Each row of the new array is a λ-permutation on r symbols with frequency n/r. For any two rows in the new FPA, the pair of entries $(i \bmod r, j \bmod r)$ agree, for each of the m/r values of j in the congruence class of i. This yields tm/r pairs for a given value of i, yielding tm^2/r such pairs in total, that is a minimal distance of $n - \frac{tm^2}{r}$. □

The substitution technique may also be used on permutation arrays which have been constructed from latin squares. For example, given a PA obtained from Theorem 3.2 using a set of $q^i - 1$ MOLS of order q^i, applying the $(q^i - 1)/(q - 1)$ substitutions from Theorem 9.20 of [14] to its entries, yields an FPA as described in the second part of Theorem 3.2. This approach allows the FPA to be built without constructing the corresponding sets of MOFS.

A useful tool in building new arrays from old is the direct product.

Proposition 4.4. *Let X_1 be an $FPA_\lambda(n_1, a)$ of size N_1 and let X_2 be an $FPA_\lambda(n_2, b)$ of size N_2. Then an $FPA_\lambda(n_1 + n_2, \min(a, b))$ may be constructed of size N_1N_2.*

In particular, for even n, given two $FPA_\lambda(n, \frac{n}{2})$, of sizes N_1 and N_2, respectively an $FPA_\lambda(2n, \frac{n}{2})$ may be constructed of size N_1N_2, so that

$$M_\lambda\left(2n, \frac{n}{2}\right) \geq M_\lambda\left(n, \frac{n}{2}\right)^2.$$

Proof. Relabelling if necessary, construct X_1 and X_2 on disjoint symbol sets, giving $n_1 + n_2/\lambda$ symbols in total. Take the direct product of X_1 and X_2, that is $Y = \{(u, v) : u \in X_1, v \in X_2\}$, where an ordered pair of codewords is interpreted as their concatenation. Now, Y is a set of λ permutations of length $n_1 + n_2$, with frequency λ. Any pair of λ permutations in Y differ in at least $\min(a, b)$ positions, hence Y is an $FPA_\lambda(n_1 + n_2, \min(a, b))$. □

In [7], a permutation array is defined to be *r-separable* if it is a disjoint union of r $PA(n, n)$'s of size n. We constructed an example of such a PA in part (i) of Theorem 4.1. We use this notion of a separable PA, that is a PA which is a disjoint union of other PA's, in the next result.

Theorem 4.5.

(i) *Given a separable $PA(n, d)$ which is the disjoint union of r $PA(n, \delta)$'s, each of size N, where $2d \geq \delta$, an $FPA_2(2n, \delta)$ of size rN^2 may be constructed.*
(ii) *Given r MOLS of order n, an $FPA_2(2n, n)$ of size rn^2 may be constructed. If n is a prime power, an $FPA_2(2n, n)$ of size $(n-1)n^2$ is obtained.*

Proof. Denote the r $PA(n, \delta)$'s by $\Gamma_1, \ldots, \Gamma_r$. For each $i = 1, \ldots, r$, form the direct product of Γ_i with itself, that is $Z_i = \{(u, v) : u, v \in \Gamma_i\}$. Then Z_i is a set of N^2 λ permutations of length $2n$, on n symbols, with frequency $\lambda = 2$, and minimum distance δ. Take the union $Z = Z_1 \cup \ldots \cup Z_r$. The λ permutations from different Z_i have pairwise distance $2d \geq \delta$, and hence Z is an $FPA_2(2n, \delta)$ of size rN^2.

By a result established in [7] and reproved constructively in [13], r MOLS of order n may be used to construct an r-separable $PA(n, n-1)$. When used in the above construction, this yields an FPA with $\delta = n$ and $2d = 2n - 2$ ($> n$ for $n > 2$), that is an $FPA_2(2n, n)$ of size rn^2. The last part follows by noting that, for a prime power n, a complete set of $n - 1$ MOLS of order n is obtainable. □

Example 4.6. *By the construction from part* (ii) *of Theorem* 4.6, *an* $FPA_2(8, 4)$ *of size* 48 *may be obtained from* 3 *MOLS of order 4. For example, the MOLS*

$$L_1 = \begin{matrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{matrix}, L_2 = \begin{matrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{matrix}, L_3 = \begin{matrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{matrix}$$

yield an FPA whose first 8 *rows are listed below.*

$$\begin{array}{cccccccc}
0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\
0 & 1 & 2 & 3 & 1 & 0 & 3 & 2 \\
0 & 1 & 2 & 3 & 2 & 3 & 0 & 1 \\
0 & 1 & 2 & 3 & 3 & 2 & 1 & 0 \\
1 & 0 & 3 & 2 & 0 & 1 & 2 & 3 \\
1 & 0 & 3 & 2 & 1 & 0 & 3 & 2 \\
1 & 0 & 3 & 2 & 2 & 3 & 0 & 1 \\
1 & 0 & 3 & 2 & 3 & 2 & 1 & 0
\end{array}$$

The next two results generalize the direct product construction of Theorem 4.6. A similar approach is explored in [5], in the context of constant composition codes; the reader is referred to [5] for more details, and for proofs of Theorem 4.8 and Theorem 4.9.

Theorem 4.7. *For* $i = 1, \ldots, b$, *let* X_i *be a separable* $FPA_\lambda(n, d_i)$ *which is a disjoint union of* r_i $FPA_\lambda(n, \delta_i)$'s, ${\Gamma^i}_1, \ldots, {\Gamma^i}_{r_i}$, with $\sum d_i \geq \min\{\delta_i\}$. *Denote* $\min\{\delta_i\}$ *by* δ, and $\min\{r_i\}$ *by* r. *Then an* $FPA_{b\lambda}(bn, \delta)$ *may be constructed, of size* $\sum_{j=1}^{r}(\prod_{i=1}^{b} |{\Gamma_j}^i|)$.

The direct product construction in Theorem 4.6 and Theorem 4.8 may be adapted by choosing some subset of the direct product which has special properties. In [4], a recursive construction of PA's is given, which uses transversal packings; the next result indicates one way in which transversal packings may be used to construct an FPA from separable PAs. This construction may be applied to a set of disjoint separable PA's such as those obtainable from the MOLS construction of [13], or to a single such PA with its subarrays permuted appropriately.

Theorem 4.8. *Let* $X_1, \ldots, X_k$ *be* k *separable PA's, such that each* $X_i = PA(n, d_i)$ *is a disjoint union of* r $PA(n, d_i')$*'s,* ${\Gamma_i}^{(1)}, \ldots, {\Gamma_i}^{(r)}$, *and the* ${\Gamma_i}^{(j)}$*'s may be ordered such that* ${\Gamma_1}^{(j)}, \ldots, {\Gamma_k}^{(j)}$ *are disjoint for each* j. *Suppose there exist transversal packings* $T_1, \ldots, T_r$ *, where each* T_j *has distance* δ *and type* $|{\Gamma_1}^{(j)}| \ldots |{\Gamma_k}^{(j)}|$. *Denote* $d_1 + \cdots + d_k$ *by* D, *and denote the smallest sum of any* δ *of the* d_i' *by* t. *Then an* $FPA_k(kn, d)$ *may be constructed, of size* $\sum_{j=1}^{r} |T_j|$, *where* $d = \min(t, D)$.

Theorem 3.2 of [4] may also be generalized to construct an $FPA_\lambda(n, d)$ from k separable $FPA_\lambda(n_i, d_i)$'s ($1 \leq i \leq k$). Replacing the $PA(n_i, d_i)$'s by the equivalent FPA's in this result, an immediate generalization for $\lambda > 1$ is obtained.

In the proof of Theorem 4.1, a pairwise distance of n is imposed on the set of new rows derived from any given original row. Relaxing this condition to minimum distance d, the λ-cycle (or its frequency analogue) may be replaced by an appropriate (frequency) permutation array. This observation underlies our final recursive result.

Theorem 4.9. *Let* $n = m\lambda$, *and let* $F_1, \ldots, F_b$ *be* b $FPA_\lambda(n, d)$*'s* (*not necessarily different*). *Let* C *be an* $FPA_n(bn, c)$ *of size* N, *where* $c \geq bd$. *Then an* $FPA_\lambda(bn, bd)$ *may be constructed, of size* $N \min_{1 \leq i \leq b} |F_i|$.

Proof. Relabelling if necessary, construct $F_1, \dots, F_b$ on disjoint symbol sets, so there are bn symbols in total. For each row in C, use the entries of the row as column headings, and place the n columns of each F_i under the n occurrences of the symbol i. The resulting array is an $FPA_\lambda(bn, bd)$, of size $\min_{1\leq i\leq b}|F_i|$. Take the union of the arrays arising from each row of C to obtain an FPA of size $N\min_{1\leq i\leq b}|F_i|$. Agreement between rows of this FPA corresponding to different rows of C can occur only at positions where the rows of C agree, since the symbol sets are disjoint. There are at most c such positions, so any two rows of the new FPA have distance at least $c \geq bd$, and the array is an $FPA_\lambda(bn, bd)$. □

Applying this theorem with F_1, F_2 as $FPA_2(4,2)$'s of size 6 and C as the $F_4(8,4)$ of size 14 from Corollary 3.5, yields an $FPA_2(8,4)$ of size 84.

5. SPECIAL CASES

An $FPA_\lambda(n,d)$, where $n = m\lambda$, may be viewed as an m-ary code with constant weight composition $(\lambda, \dots, \lambda)$. In certain special cases, known results for constant weight codes provide bounds and constructions of relevance to FPAs.

Proposition 5.1. *If $n = 2\lambda$, then an $FPA_\lambda(n,d)$ of size M is a binary code (n, M, d) of length n, minimum (Hammimg) distance d and constant weight λ.*

In [2], constructions and bounds are given for $A(n,d,w)$, the maximum possible number of binary vectors of length n, Hamming distance at least d, and constant weight w, for values of n up to 28. Observe that $A(n,d,\frac{n}{2}) = M_{\frac{n}{2}}(n,d)$. The exact value of $A(n,d,w)$, and corresponding constructions, is known for all lengths $n \leq 11$. If d is odd, then $M_{\frac{n}{2}}(n,d) = M_{\frac{n}{2}}(n,d+1)$, so only even distances need be considered. The following FPAs may be directly constructed, by use of Hadamard matrices and Steiner systems ([2]).

Recall that a *Hadamard matrix* is a square matrix with entries $+1$, -1 whose rows are mutually orthogonal. Hadamard matrices of order n can only exist for $n = 1, 2$ and $n = 4k$; it is conjectured that they exist for each $n = 4k$. Hadamard matrix constructions and properties may be found in Section IV.24 of [6].

Theorem 5.2. (Theorem 10, [2]). $M_{\frac{n}{2}}(n,\frac{n}{2}) = 2n - 2$ *if and only if a Hadamard matrix H_n of order $n \geq 1$ exists.*

An (optimal) $FPA_{\frac{n}{2}}(n,\frac{n}{2})$ may be constructed from the Hadamard matrix H_n as follows. First convert the entries of the 'half-frame' of $+1$'s bordering H_n into -1's. Now take the non-initial rows of H_n and $-H_n$, and convert the entries $+1$ to 0 and -1 to 1 in every row.

Example 5.3. *Using the Hadamard matrix of order* 12 (*unique up to isomorphism*) *gives an* $FPA_6(12,6)$ *of size* 22. *We list the first few rows.*

$$\begin{matrix} 1&0&1&0&1&1&1&0&0&0&1&0\\ 1&0&0&1&0&1&1&1&0&0&0&1\\ 1&1&0&0&1&0&1&1&1&0&0&0\\ 1&0&1&0&0&1&0&1&1&1&0&0 \end{matrix}$$

Combining Theorem 5.2 with Proposition 4.5 we see that, if n is an even number such that a Hadamard matrix of order n exists, then $M_{\frac{n}{2}}(2n, \frac{n}{2}) \geq (2n-2)^2$. For example, $M_6(24, 6) > 484$.

A *Steiner system* $S(t, k, v)$ is a $t-(v, k, 1)$ design, that is, a collection of k-subsets (called blocks) of a v-set such that each t-tuple of elements of this v-set is contained in a unique block. When $t = 3$ and $k = 4$, this called a *Steiner quadruple system.*

Example 5.4. *Using the Steiner quadruple system* $S(3, 4, 8)$*, an* $FPA_4(8, 4)$ *of size* 14 *may be constructed. The extended cyclic code* $\{(1011000)1, (0100111)0\}$ *is one example; the code is constructed by taking cyclic developments of the vectors in parenthesis.*

We conclude by remarking that, in the study of $PA(n, d)$ arrays, one builds the rows of the array by using permutations on n symbols, and in $FPA_\lambda(n, d)$ arrays, one builds rows by using m distinct symbols, each repeated exactly λ times. However, there is in fact no need for such uniformity of frequency, and one could consider the following, very general, setting.

Let $n = \lambda_1 + \cdots + \lambda_r$ be a partition of n. Then one could consider constructing arrays with the property that in each row, for $i = 1, \ldots, r$, the symbol i occurs exactly λ_i times. From papers such as [4], there is motivation for studying such a general setting; in fact the corresponding constant composition codes have been widely studied; see [2]. Sets of $F(n; \lambda_1, \ldots, \lambda_r)$ orthogonal frequency squares have been studied (see Chapter 4 in [14]). However, we do not consider frequency permutation arrays with an arbitrary frequency vector $n = \lambda_1 + \cdots + \lambda_r$ here.

ACKNOWLEDGMENT

The first author is supported by a Royal Society Dorothy Hodgkin Fellowship. The authors wish to thank the anonymous referees for their comments and suggestions.

REFERENCES

[1] R. A. Bailey, H. Monod, J. P. Morgan, Construction and optimality of affine-resolvable designs, Biometrika 82 (1995), 187–200.

[2] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, A new table of constant weight codes, IEEE Trans Infor Thy 36 (1990), 1334–1380.

[3] L. Carlitz, The number of derangements of a sequence with given specification, Fibonacci Quart 16 (1978), 255–258.

[4] W. Chu, C. J. Colbourn, and P. Dukes, Constructions for permutation codes in powerline communications, Designs, Codes Cryptography 32 (2004), 51–64.

[5] W. Chu, C. J. Colbourn, and P. Dukes, On constant composition codes, Discrete Applied Math, to appear.

[6] C. J. Colbourn and J. H. Dinitz (editors), The CRC handbook of combinatorial designs, CRC Press, Boca Raton, FL, 1996.

[7] C. J. Colbourn, T. Kløve, and A. C. H. Ling, Permutation arrays for powerline communication and mutually orthogonal latin squares, IEEE Trans Infor Thy 50 (2004), 1289–1291.

[8] P. Das, The number of permutation polynomials of a given degree over a finite field, Finite Fields Appl 8 (2002), 478–490.

[9] D. R. de la Torre, C. J. Colbourn, and A. C. H. Ling, An application of permutation arrays to block ciphers, Cong Numer 145 (2000), 5–7.

[10] J. Dénes, G. L. Mullen, and S. J. Suchower, Another generalized Golomb-Posner code, IEEE Trans Infor Thy 36 (1990), 737–748.

[11] C. Ding and J. Yin, Combinatorial constructions of constant composition codes, IEEE Trans Infor Thy 51 (2005), 3671–3674.

[12] S. Even and J. Gillis, Derangements and Laguerre polynomials, Math Proc Cambridge Philos Soc 79 (1976) 135–143.

[13] S. Huczynska and G. L. Mullen, Constructing permutation arrays using affine resolvable designs, Preprint.

[14] C .F. Laywine and G. L. Mullen, Discrete mathematics using latin squares, Wiley, New York, 1998.

[15] R. Lidl and H. Niederreiter, Finite fields, 2nd edition, Cambridge University Press, Cambridge, 1997.

[16] Y. Luo, F.- W. Fu, A. J Han Vinck, W. Chen, On constant-composition codes over $\mathbb{Z}_q$, IEEE Trans Infor Thy 49 (2003), 3010–3016.

[17] M. Svanström, P. R. J. Östergard, and G. T. Bogdanova, Bounds and constructions for ternary composition codes, IEEE Trans Infor Thy 48 (2002), 101–111.