Des. Codes Cryptogr. (2010) 54:109–120
DOI 10.1007/s10623-009-9312-0

Equidistant frequency permutation arrays and related constant composition codes

Sophie Huczynska

Received: 16 December 2008 / Revised: 11 June 2009 / Accepted: 11 June 2009 /
Published online: 7 July 2009

Abstract In this paper we study the special class of equidistant constant composition codes of type $CCC(n, d, \mu^m)$ (where $n = m\mu$), which correspond to equidistant frequency permutation arrays; we also consider related codes with composition "close to" μ^m. We establish various properties of these objects and give constructions for optimal families of codes.

Keywords Permutation arrays · Constant composition codes · Combinatorial designs

Mathematics Subject Classifications (2000) 05B15 · 94B25

1 Introduction

Constant composition codes (CCCs) have recently been the subject of much study (see [4,6,11]). Of particular interest are codes with composition 1^n, which correspond to permutation arrays (PAs); these have recently found application in the area of powerline communication (see for example [3]). More generally, codes with composition μ^m (where length $n = m\mu$) are of interest for similar reasons; such codes correspond to frequency PAs (FPAs) (see [10]).

The situation when these codes (correspondingly, these arrays) are equidistant is of particular interest. Equidistant PAs (EPAs) have been studied since the 1970s (e.g. [9,14]), so it is natural to consider equidistant FPAs; moreover in the setting of codes, it is known that any CCC which is of optimal size with respect to the non-recursive Johnson bound (see [11]) must be an equidistant code. In this paper, we first obtain bounds for equidistant $CCC(n, d, \mu^m)$s with small distances, then give various constructions for families of equidistant CCCs whose

Communicated by Charles J. Colbourn.

S. Huczynska (✉)
School of Mathematics and Statistics, University of St Andrews, Fife KY16 9SS, Scotland, UK
e-mail: sophieh@mcs.st-and.ac.uk

compositions are μ^m or "close to" μ^m. Wherever the non-recursive Johnson bound is applicable, we show that the constructed codes are optimal in terms of this bound.

1.1 Preliminaries

Let C be an m-ary code of length n and minimum Hamming distance d on the alphabet $\{0, 1, \ldots, m-1\}$. The code C has constant weight composition $[\mu_0, \mu_1, \ldots, \mu_{m-1}]$ if every codeword has μ_i occurrences of symbol i for $i = 0, 1, \ldots, m-1$. We refer to C as a CCC, written $CCC(n, d, [\mu_0, \mu_1, \ldots, \mu_{m-1}])$ (here $n = \sum_{i=0}^{m-1} \mu_i$). The code is said to be equidistant if the pairwise distance between any two of its codewords is precisely d. For convenience, when writing these compositions, we may use exponential notation; i.e. a composition $[a_0, \ldots, a_0, a_1, \ldots, a_1, \ldots, a_h, \ldots, a_h]$ comprising t_i occurrences of each a_i will be written as $a_0^{t_0} a_1^{t_1} \ldots a_h^{t_h}$.

In the case when $\mu_i = 1$ for all $i = 0, \ldots, m-1$, the code corresponds to a PA: a PA of length n, minimum distance d and size v, defined on the elements of an n-set S, is a $v \times n$ array such that each row is a permutation of the symbols of S and any two rows agree in at most $n - d$ columns, or precisely $n - d$ columns for an EPA. More generally, the CCCs in which $\mu_0 = \cdots = \mu_{m-1} = \mu$ for $n = m\mu$ correspond to FPAs ([10]). A FPA of length $n = m\mu$, frequency μ, distance d and size v, defined on the elements of a m-set S, is a $v \times n$ array in which each row is a multipermutation of the symbols of S each repeated μ times and any two rows agree in at most $n - d$ columns, or precisely $n - d$ columns for an equidistant FPA (EFPA).

An important equivalence exists between CCCs and a special kind of combinatorial design called packings. A design (V, B) consists of a set V of elements (called points) and a collection B of subsets of V (called blocks). The design is called an (n, λ)-packing if every pair of distinct points of V occurs in at most λ blocks, and every point occurs in precisely n blocks. A resolution of a design is a partition of its blocks into classes; a μ-parallel class is a set of blocks such that each point occurs in precisely μ blocks. Two resolutions are orthogonal if any class in one resolution intersects every class from another resolution in at most one block. In [6], *generalized doubly resolvable packings* are introduced, and their equivalence to CCCs is established. A $GDRP(n, \lambda; v)$ with type $\{\mu_0, \ldots, \mu_{m-1}\}$ is defined to be an (n, λ)-packing which admits two orthogonal resolutions, where one of the resolutions forms a partition of B into a μ_0-parallel class, a μ_1-parallel class, $\ldots$, a μ_{m-1}-parallel class, while the other is a partition of B into n 1-parallel classes. It is shown that such a GRDP exists if and only if a $CCC[n, n - \lambda, [\mu_0, \ldots, \mu_{m-1}])$ of size v exists.

In particular, when the code corresponds to an EPA, the equivalent packing may be viewed in terms of a combinatorial object called a generalized Room square (GRS). A GRS of side r and index λ defined on a v-set X is an $r \times r$ array F such that every cell of F contains a subset (possibly empty) of X; each symbol of X occurs once in each row and column of F; and any two distinct symbols occur together in exactly λ cells of F. Such a GRS is denoted by $S(r, \lambda; v)$, and it is well-known (see [5]) that an EPA of length r, distance $r - \lambda$ and size v exists if and only if an $S(r, \lambda; v)$ exists. When the code corresponds to an equidistant $CCC(n, d, [\mu_0, \ldots, \mu_{m-1}])$, we may define the concept of a generalized Room rectangle as its packing equivalent.

Definition 1 Let X be a set of cardinality v. Define a *generalized Room rectangle* (GRR) of size $m \times n$, frequency composition $\{\mu_0, \ldots, \mu_{m-1}\}$ (where $n = \sum_{i=0}^{m-1} \mu_i$) and index λ on X to be an $m \times n$ array F such that every cell of F contains a subset (possibly empty) of X; each symbol of X occurs once in each column of F; each symbol of X occurs μ_i times in

the ith row of F; and any two distinct symbols occur together in exactly λ cells of F. Denote such an object by $GRR(n, \{\mu_0, \ldots, \mu_{m-1}\}, \lambda; v)$.

Observe that a $GRR(n, \{\mu_0, \ldots, \mu_{m-1}\}, \lambda; v)$ is an "exact" $GDRP(n, \lambda; v)$ of type $\{\mu_0, \ldots, \mu_{m-1}\}$ where every pair of distinct points occurs in precisely λ blocks.

The following relationship is easily established (see [6,7] for a discussion of the general GDRP case):

Theorem 1 *An equidistant m-ary $CCC(n, n-\lambda, [\mu_0, \ldots, \mu_{m-1}])$ of size v exists if and only if a $GRR(n, \{\mu_0, \ldots, \mu_{m-1}\}, \lambda; v)$ exists.*

Given such a code C, list its codewords as $c_1, \ldots, c_v$; then a GRR can be formed from C as follows. Label the m rows of a $m \times n$ array by $\{0, \ldots, m-1\}$ and the n columns by $\{1, \ldots, n\}$. In the (i, j)th cell, place symbol r if codeword c_r has symbol i in position j. Performing the reverse process yields an equidistant CCC from a GRR.

Our main yardstick for optimality will be the following upper bound for the maximum size of general CCCs, which first appeared in [11]. It is called the non-recursive Johnson bound. Observe that, for a CCC in which all symbols of a codeword occur with equal frequency μ (corresponding to an FPA), this upper bound reduces to the Plotkin bound. As mentioned in the introduction, an important observation here is that any CCC which achieves equality in the non-recursive Johnson bound must in fact be equidistant.

Proposition 1 (i) *Denote by $A_m(n, d, [\mu_0, \mu_1, \ldots, \mu_{m-1}])$ the maximum possible size of an m-ary $CCC(n, d, [\mu_0, \mu_1, \ldots, \mu_{m-1}])$. Then (if the denominator is positive):*

$$A_m(n, d, [\mu_0, \mu_1, \ldots, \mu_{m-1}]) \leq \frac{nd}{nd - n^2 + (\mu_0^2 + \mu_1^2 + \cdots + \mu_{m-1}^2)}$$

(ii) *In particular, for $d > n - \mu$,*

$$A_m(n, d, \mu^m) \leq \frac{d}{d - n + \mu}$$

.

2 Preliminary bounds for equidistant $CCC(n, d, \mu^m)$s

In this section, we consider equidistant codes of the form $CCC(n, d, \mu^m)$ where $n = m\mu$, and obtain some initial bounds. We shall let $B_m(n, d)$ denote the maximum possible number of codewords that can exist in any equidistant $CCC(n, d, \mu^m)$ (i.e. the maximum number of rows in any EFPA with length n, distance d and frequency μ).

Proposition 2 *Let $n = m\mu$. Then*

(i) $B_m(n, d) = 1$ *if $m = 2$ and d is odd;*
(ii) $B_m(n, n) = m$;
(iii) $B_m(n, 2) = \mu + 1$.

Since the proof is straightforward, we omit the details.

Theorem 2 *Let $n = m\mu$. For $m > 2$, $B_m(n, 3) = \max\{3, m - 1\}$.*

Proof With $m \geq 3$, let A be an equidistant $CCC(n, 3, \mu^m)$ of largest possible size. Let ρ_1 be the "standard" μ-permutation written as $0_1 \dots 0_\mu 1_1 \dots 1_\mu \dots (m-1)_1 \dots (m-1)_\mu$ (with additional subscripts) where we refer to each $i_1 \dots i_\mu$ as a "block" in ρ_1. Let ρ_2 be the second row of A; it must be derived from ρ_1 by permuting three symbols from different blocks in a 3-cycle. Clearly, taking all three rotations of this 3-cycle yields the largest possible array such that two non-identity rows have the same set of non-fixed positions. So let ρ be any other row which does not have the same non-fixed positions as ρ_2. Then ρ_2 and ρ must share two of their non-fixed positions: of these, they must agree on one position and disagree on the other, forcing the third position of each to correspond to a different block in ρ_1 (different also from those corresponding to the two shared entries). Hence, given a non-identity row ρ_2, there are at most $m-3$ choices for the block corresponding to the third non-fixed position of any other non-identity row, giving an upper bound of $m-1$ for the size of the array (position within a block is not relevant here). Conversely, an array of size $m-1$ may be constructed by taking ρ_1 plus (say) the $m-2$ multipermutations derived from ρ_1 by applying the 3-cycle $(0_1 1_1 a_1)$, $(a = 2, \dots, m-1)$. □

Theorem 3 *Let $n = m\mu$. For $n \geq 4$, $B_m(n, 4) \geq \lfloor \frac{n}{2} \rfloor$.*

Proof An equidistant $CCC(n, 4, \mu^m)$ of size $\lfloor \frac{n}{2} \rfloor$ can be constructed as follows. Let ρ_1 be the "standard" μ-permutation $0_1 \dots 0_\mu 1_1 \dots 1_\mu \dots (m-1)_1 \dots (m-1)_\mu$. Let A be the set of all "pairs of transpositions" of the form $\{(0_1 1_1)(a_i b_j)\}$ where the set $\{(a_i, b_j)\}$ comprises $\lfloor \frac{n-2}{2} \rfloor$ pairs from the set of positions $\{0_2, \dots, 0_\mu, 1_2, \dots, 1_\mu, 2_1, \dots, 2_\mu, \dots, (m-1)_1, \dots, (m-1)_\mu\}$ such that all pairs are disjoint and in each pair, a and b are distinct symbols from the alphabet. Then $\rho_1 \cup A$ is the desired CCC. We show that it is always possible to obtain $\lfloor \frac{n-2}{2} \rfloor$ such pairs.

- For m even, form $(\mu - 1)$ pairs $(0_2, 1_2), \dots, (0_\mu, 1_\mu)$, then (if $m > 2$) form $\frac{(m-2)\mu}{2}$ pairs $(2_1, 3_1), \dots, ((m-2)_\mu, (m-1)_\mu)$.
- For m odd and μ even, form
  - $\frac{\mu}{2}$ pairs $(0_i, 2_j)$ $(2 \leq i \leq \frac{\mu}{2} + 1$ and $1 \leq j \leq \frac{\mu}{2})$,
  - $\frac{\mu}{2}$ pairs $(1_i, 2_j)$ $(2 \leq i \leq \frac{\mu}{2} + 1$ and $\frac{\mu}{2} + 1 \leq j \leq \frac{\mu}{2})$,
  - $\frac{\mu}{2} - 1$ pairs $(0_j, 1_j)$ $(\frac{\mu}{2} + 2 \leq j \leq \mu)$,
  - If $m > 3$, form $\frac{(m-3)\mu}{2}$ pairs $(2_1, 3_1), \dots, ((m-2)_\mu, (m-1)_\mu)$.
- For m odd and μ odd, the construction is analogous to the previous construction except that there are $\lceil \frac{\mu}{2} \rceil$ pairs of the form $(0_i, 2_j)$, $\lfloor \frac{\mu}{2} \rfloor$ pairs of the form $(1_i, 2_j)$, and $\lfloor \frac{\mu}{2} \rfloor - 1$ pairs of the form $(0_i, 1_j)$. □

Example 1 An equidistant $CCC(12, 4, 3^4)$ of size 6 arising from the above construction is

$$\begin{array}{l}
\rho_0\ 0\ 0\ 0\ 1\ 1\ 1\ 2\ 2\ 2\ 3\ 3\ 3 \\
\rho_1\ 1\ 1\ 0\ 0\ 0\ 1\ 2\ 2\ 2\ 3\ 3\ 3 \\
\rho_2\ 1\ 0\ 1\ 0\ 1\ 0\ 2\ 2\ 2\ 3\ 3\ 3 \\
\rho_3\ 1\ 0\ 0\ 0\ 1\ 1\ 3\ 2\ 2\ 2\ 3\ 3 \\
\rho_4\ 1\ 0\ 0\ 0\ 1\ 1\ 2\ 3\ 2\ 3\ 2\ 3 \\
\rho_5\ 1\ 0\ 0\ 0\ 1\ 1\ 2\ 2\ 3\ 3\ 3\ 2
\end{array}$$

For small values of n, it is possible to construct equidistant $CCC(n, 4, \mu^m)$s of size larger than $\lfloor \frac{n}{2} \rfloor$; for example $B_m(n, 4) \geq 7$ for $\mu \geq 4$ and $m \geq 2$, since an equidistant $CCC(8, 4, 4^2)$ of size 7 may be built from a Hadamard matrix. However, we make the following conjecture:

Conjecture 1 Let $n = m\mu$. For $n \geq 14$, $B_m(n, 4) = \lfloor \frac{n}{2} \rfloor$.

Observe that the preceding results generalize those known for EPAs. It is known (see [5]) that $B_n(n, 2) = 2$; for $n > 3$, $B_n(n, 3) = n - 1$ and for $n > 9$, $B_n(n, 4) = \lfloor \frac{n}{2} \rfloor$.

We conclude this section by summarizing a few basic ways in which new codes can be obtained from old.

Proposition 3 (i) *Let $n = m\mu$. Then $B_m(n, d) \geq B_{m-1}(n - \mu, d)$.*

(ii) *Let $n_1 = m\mu_1$ and $n_2 = m\mu_2$. Then $B_m(n_1 + n_2, d_1 + d_2) \geq \min\{B_m(n_1, d_1), B_m(n_2, d_2)\}$.*

(iii) *If there exists an equidistant $CCC(n, n - \lambda, [\mu_0, \ldots, \mu_{m-1}])$ of size v, then for any $k \in \mathbb{N}$ there exists an equidistant $CCC(kn, k(n - \lambda), [k\mu_0, \ldots, k\mu_{m-1}])$ of size v. Moreover, if the original $CCC(n, n-\lambda, [\mu_0, \ldots, \mu_{m-1}])$ is of optimal size (i.e. satisfies the upper bound of Proposition 1) then the $CCC(kn, k(n-\lambda), [k\mu_0, \ldots, k\mu_{m-1}])$ is also of optimal size.*

(iv) *Let M be the maximum size of an equidistant binary code with length n and distance d. Then $B_2(2n, 2d) \geq M$.*

Proof Part (i) follows by adjoining columns, part (ii) is immediate by juxtaposition and part (iii) follows by "inflating" or self-concatenating the words of the original code by a factor of k. For (iv), let C be an equidistant binary code of size M with length n and distance d. The required $CCC(2n, 2d, n^2)$ may be constructed by changing 0's to 1's and 1's to 0's in C, then juxtaposing the resulting array with the original array. □

3 Codes constructed via GRRs

In this section, we present some constructions for EFPAs and related CCCs via their associated GRRs. In each case, we demonstrate the optimality of either the $CCC(n, d, \mu^m)$ itself or (if its parameters do not allow the non-recursive Johnson bound to be applied) of a closely-related CCC derived from the same construction.

3.1 EFPAs from resolvable BIBDs

We give a construction for producing optimal $CCC(n, d, \mu^m)$s from any balanced incomplete block design (BIBD) which possesses the property of being resolvable. This yields various infinite families of optimal $CCC(n, d, \mu^m)$s. The construction of equidistant q-ary codes using resolvable BIBDs dates back to the 1960s (see [13]); our construction is a variation on this approach.

A balanced incomplete block design (BIBD) is a pair (V, B) where V is a v-set and B is a collection of b k-subsets (blocks) of V, such that each element of V is contained in exactly r blocks and any 2-subset of V is contained in exactly λ blocks. Here $r = \frac{\lambda(v-1)}{k-1}$ and $b = \frac{vr}{k}$. A parallel class is a set of blocks of a BIBD that partition the point set, and a resolvable BIBD is one whose blocks can be partitioned into parallel classes. Necessary conditions for the existence of a (v, k, λ)-RBIBD are $(k - 1)|\lambda(v - 1)$ and $k|v$. Properties and construction methods of resolvable BIBDs have been extensively studied; we refer the reader to [5] for information and further references. Known results on families of RBIBDs may be combined with Theorem 4 to yield infinite families of optimal $CCC(n, d, \mu^m)$s. We note that in [7], a construction method is given for a family of optimal $CCC(n, d, \mu^m)$s, using RBIBDs in combination with difference matrices.

Theorem 4 *If there exists a resolvable* (v, k, λ)*BIBD, then there exists an optimal (equidistant)* $CCC(b, \frac{(r-\lambda)v}{k}, r^{\frac{v}{k}})$ *of size* v.

Proof Denote the design by D. Then D has r parallel classes, each containing $\frac{v}{k}$ blocks. Label these parallel classes as $\pi_1, \ldots, \pi_r$, where each π_i comprises $\frac{v}{k}$ k-sets, which we list as $\pi_i(1), \ldots, \pi_i(\frac{v}{k})$ (the order of the k-sets does not matter here).

Form $\frac{v}{k}$ arrays of cells $A_1, \ldots, A_{\frac{v}{k}}$, as follows: each A_i is a $1 \times r$ array of cells, where the $(1, j)$th cell of A_i contains the k-set $\pi_j(i)$ $(1 \leq i \leq \frac{v}{k}, 1 \leq j \leq r)$. Now take a latin square of order $\frac{v}{k}$ on the symbols $\{1, \ldots, \frac{v}{k}\}$, and create an $\frac{v}{k} \times b$ array of cells by arranging the arrays $A_1, \ldots, A_{\frac{v}{k}}$ according to the latin square.

Then every column comprises some parallel class π_i for some $1 \leq i \leq r$, and every row comprises all the blocks of the design, arranged one per cell. Altogether, the array contains each block of the design precisely $\frac{v}{k}$ times. So the array is a $GRR(b, r^{\frac{v}{k}}, \frac{\lambda v}{k}; v)$, and hence corresponds to an equidistant $CCC(b, \frac{(r-\lambda)v}{k}, r^{\frac{v}{k}})$ of size v. Since this meets the Plotkin bound (here the expression for the maximum possible size simplifies to $\frac{\lambda(v-k)}{k-1} \cdot \frac{v(k-1)}{\lambda(v-k)} = v$), the CCC so constructed is optimal. □

Corollary 1 *For any* $k, n \in \mathbb{N}$ *with* $k|n$*, an optimal (equidistant)* $CCC\left(\binom{n}{k}, \frac{n-k}{n-1}\binom{n}{k}, \binom{n-1}{k-1}^{n/k}\right)$ *of size* n *can be constructed using the set of* k*-sets of* $\{1, \ldots, n\}$.

Proof It is clear that the collection of k-sets of an n-set satisfy the conditions of a BIBD. Moreover, by Baranyai's Theorem ([2]), if $k|n$, then there exists a partition π of the set of k-subsets of $\{1, 2, \ldots, n\}$ into parallel classes, each of which is a partition of $\{1, 2, \ldots, n\}$. Hence we have a resolvable BIBD, and so Theorem 4 may be applied. □

The case when $k = 2$ in Corollary 1 can be used as input to obtain another infinite family of optimal codes corresponding to EFPAs.

Theorem 5 *For any even* $h \neq 2, 6 \in \mathbb{N}$*, an optimal (equidistant)* $CCC(2h^2 - h, 2h^2 - 2h, (2h-1)^h)$ *of size* $2h$ *can be constructed.*

Proof Let A be a $GRR\left(\binom{h}{2}, (h-1)^{\frac{h}{2}}, \frac{h}{2}; h\right)$ constructed using Corollary 1 with $k = 2$, and let $\mathbf{a}$ and $\mathbf{b}$ denote symbol sets $\{1, \ldots, h\}$ and $\{h+1, \ldots, 2h\}$ respectively. Denote by $A(\mathbf{a})$ a copy of A taken on symbol set $\mathbf{a}$ (similarly for $A(\mathbf{b})$). Denote by $LS(\mathbf{a}, \mathbf{b})$ the $h \times h$ array formed by taking a pair of mutually orthogonal latin squares of order h, one on symbol set $\mathbf{a}$ and the other on $\mathbf{b}$, and superimposing them. Then a GRR corresponding to an equidistant $CCC(2h^2 - h, 2h^2 - 2h, (2h-1)^h)$ of size $2h$ is obtained by forming the $h \times h(h-1)$ array $C(\mathbf{a}, \mathbf{b})$ as follows

$A(\mathbf{a})$	$A(\mathbf{b})$
$A(\mathbf{b})$	$A(\mathbf{a})$

then juxtaposing $C(\mathbf{a}, \mathbf{b})$ with h copies of $LS(\mathbf{a}, \mathbf{b})$ to form: $C(\mathbf{a}, \mathbf{b})|LS(\mathbf{a}, \mathbf{b})|\cdots|LS(\mathbf{a}, \mathbf{b})$. This creates an $h \times (2h^2 - h)$ array in which each symbol of $\mathbf{a} \cup \mathbf{b}$ occurs once per column and $2h - 1$ times per row; each pair of distinct elements from a symbol set occurs together h times in $C(\mathbf{a}, \mathbf{b})$ while each pair (i, j) with i and j in different symbol sets occurs together h times in the h copies of $LS(\mathbf{a}, \mathbf{b})$. Optimality follows as the corresponding CCC meets the bound of Proposition 1 with equality. □

Example 2 An optimal $CCC(28, 24, 7^4)$ of size 8 from Theorem 5. Take array $C(\mathbf{a}, \mathbf{b})$ as

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

and take $LS(\mathbf{a}, \mathbf{b})$ to be (using two MOLS of order 4 from [5]):

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

Then a $GRR(28, \{7, 7, 7, 7\}, 4; 8)$ is given by the juxtaposition: $C(\mathbf{a}, \mathbf{b})|LS(\mathbf{a}, \mathbf{b})|LS(\mathbf{a}, \mathbf{b})|LS(\mathbf{a}, \mathbf{b})|LS(\mathbf{a}, \mathbf{b})$.

3.2 EFPAs from odd balanced tournament designs

An odd balanced tournament design, $OBTD(k)$, defined on a $2k+1$-set V, is an arrangement of the $\binom{2k+1}{2}$ distinct unordered pairs of the elements of V into a $k \times (2k+1)$ array such that each column of the array contains $2k$ distinct elements of V, and each element of V occurs precisely twice in each row. It is known that an $OBTD(k)$ exists for every positive integer k. Moreover, by appropriate choice of construction methods, it can be ensured that no two columns of the array are missing the same element of $\{1, \ldots, 2k+1\}$.

Theorem 6 *For any $k \in \mathbb{N}$,*

(i) *an optimal (equidistant) $CCC(2k+1, 2k, 2^k 1^1)$ of size $2k+1$ can be constructed;*
(ii) *an equidistant $CCC(2k+2, 2k, 2^{k+1})$ of size $2k+1$ can be constructed.*

Proof Let A be an $OBTD(k)$; from the remark preceding the theorem, we may assume that no two columns of the array are missing the same element of $\{1, \ldots, 2k+1\}$. Adding an extra row to A, whose ith cell contains the single symbol not occurring in the ith column of A, yields a GRR for part (i). Optimal size follows as it satisfies the bound of Proposition 1. Adjoining an additional column whose cells are empty apart from the cell in row $k+1$, which contains a copy of each symbol, yields a GRR equivalent to the desired code for part (ii). □

Our next construction uses OBTDs to give an infinite family of EFPAs; the same construction also yields an infinite family of equidistant CCCs with non-uniform composition. While the optimality of the first cannot be judged by the bound of Proposition 1 (which here would have negative denominator), the second is of maximum possible size.

Theorem 7 *For any $k \in \mathbb{N}$,*

(i) *an equidistant $CCC(8k+8, 8k+2, 4^{2k+2})$ of size $4k+2$ can be constructed;*
(ii) *an optimal (equidistant) $CCC(8k+4, 8k+2, 4^{2k}3^1 1^1)$ of size $4k+2$ can be constructed.*

Proof We construct GRRs corresponding to the required codes. Let O be an $OBTD(k)$, constructed so that no two columns are missing the same element of the symbol set, and let $\mathbf{a}$ and $\mathbf{b}$ denote symbol sets $\{1, \ldots, 2k+1\}$ and $\{2k+2, \ldots, 4k+2\}$ respectively. Denote by

$O(\mathbf{a})$ a copy of O taken on symbol set $\mathbf{a}$ (similarly for $O(\mathbf{b})$); note this is a $2k+1 \times k$ array. Denote by $LS(\mathbf{a}, \mathbf{b})$ the $2k+1 \times 2k+1$ array formed by taking a pair of mutually orthogonal latin squares of order $2k+1$, one on symbol set $\mathbf{a}$ and the other on $\mathbf{b}$, and superimposing them. Then a GRR corresponding to an equidistant $CCC(8k+8, 8k+2, [4, 4, \ldots, 4])$ of size $4k+2$ is obtained as follows. Form the $2k+2 \times 4k+4$ array $A(\mathbf{a}, \mathbf{b})$ by:

$O(\mathbf{a})$		$O(\mathbf{b})$	
$\mathbf{a}$	all	$\mathbf{b}$	
$O(\mathbf{b})$		$O(\mathbf{a})$	
$\mathbf{b}$		$\mathbf{a}$	all

where $\mathbf{a}$ represents the $1 \times 2k+1$ row described in Theorem 6 which converts $O(\mathbf{a})$ into a $GRR(2k+1, \{2, \ldots, 2, 1\}, 1; 2k+1)$, and "all" denotes a single cell containing a copy of each symbol in $\mathbf{a} \cup \mathbf{b}$. Form the array $B(\mathbf{a}, \mathbf{b})$ by:

$LS(\mathbf{a}, \mathbf{b})$		$LS(\mathbf{a}, \mathbf{b})$	
	all		all

Then the juxtaposition $A(\mathbf{a}, \mathbf{b})|B(\mathbf{a}, \mathbf{b})$ is a $2k+2 \times 8k+8$ array of cells which forms a $GRR(8k+8, \{4, \ldots, 4\}, 6; 4k+2)$. Clearly each symbol in $\mathbf{a} \cup \mathbf{b}$ occurs once per column and 4 times per row; each pair of different elements from a given symbol set occurs together twice in the copies of $O(\mathbf{a})$ or $O(\mathbf{b})$, while each pair of elements $\{a, b\}$ with $a \in \mathbf{a}$ and $b \in \mathbf{b}$ occurs together twice in the copies of $LS(\mathbf{a}, \mathbf{b})$. To construct a $GRR(8k+4, \{4, \ldots, 4, 3, 1\}, 2; 4k+2)$, take the above construction and convert the cells labelled "all" into empty cells (then delete the four resulting empty columns). For the former code, the bound of Theorem 1 is not applicable. However for the second code, the upper bound evaluates to $\frac{(8k+4)(8k+2)}{2(8k+1)}$, and so $4k+2$ is the largest integer satisfying this bound. □

Example 3 We apply Theorem 7 with $k = 3$. First use an $OBTD(3)$ to construct A:

3, 6	4, 7	5, 1	6, 2	7, 3	1, 4	2, 5		10, 13	11, 14	12, 8	13, 9	14, 10	8, 11	9, 12	
2, 7	3, 1	4, 2	5, 3	6, 4	7, 5	1, 6		9, 14	10, 8	11, 9	12, 10	13, 11	14, 12	8, 13	
4, 5	5, 6	6, 7	7, 1	1, 2	2, 3	3, 4		11, 12	12, 13	13, 14	14, 8	8, 9	9, 10	10, 11	
1	2	3	4	5	6	7	*all*	8	9	10	11	12	13	14	
10, 13	11, 14	12, 8	13, 9	14, 10	8, 11	9, 12		3, 6	4, 7	5, 1	6, 2	7, 3	1, 4	2, 5	
9, 14	10, 8	11, 9	12, 10	13, 11	14, 12	8, 13		2, 7	3, 1	4, 2	5, 3	6, 4	7, 5	1, 6	
11, 12	12, 13	13, 14	14, 8	8, 9	9, 10	10, 11		4, 5	5, 6	6, 7	7, 1	1, 2	2, 3	3, 4	
8	9	10	11	12	13	14		1	2	3	4	5	6	7	*all*

then take B to be (using two MOLS of order 7 from [5]):

1, 8	2, 9	3, 10	4, 11	5, 12	6, 13	7, 14		1, 8	2, 9	3, 10	4, 11	5, 12,	6, 13	7, 14	
2, 10	3, 11	4, 12	5, 13	6, 14	7, 8	1, 9		2, 10	3, 11	4, 12	5, 13	6, 14	7, 8	1, 9	
3, 12	4, 13	5, 14	6, 8	7, 9	1, 10	2, 11		3, 12	4, 13	5, 14	6, 8	7, 9	1, 10	2, 11	
4, 14	5, 8	6, 9	7, 10	1, 11	2, 12	3, 13		4, 14	5, 8	6, 9	7, 10	1, 11	2, 12	3, 13	
5, 9	6, 10	7, 11	1, 12	2, 13	3, 14	4, 8		5, 9	6, 10	7, 11	1, 12	2, 13	3, 14	4, 8	
6, 11	7, 12	1, 13	2, 14	3, 8	4, 9	5, 10		6, 11	7, 12	1, 13	2, 14	3, 8	4, 9	5, 10	
7, 13	1, 14	2, 8	3, 9	4, 10	5, 11	6, 12		7, 13	1, 14	2, 8	3, 9	4, 10	5, 11	6, 12	
							all								*all*

4 Direct constructions of EFPAS and related CCCs

In this section, we present constructions which do not involve the use of GRRs. As above, we demonstrate the optimality of the $CCC(n, d, \mu^m)$ wherever possible, and if the non-recursive Johnson bound is not applicable, we demonstrate the optimality of a closely-related CCC.

4.1 EFPAs from orthogonal arrays

An orthogonal array $OA(k, s)$ is a $k \times s^2$ array with entries from an s-set S such that in any two rows, each (ordered) pair of symbols from S occurs exactly once. It is clear that any orthogonal array $OA(k, s)$ is an example of an equidistant $CCC(s^2, s^2 - s, s^s)$. We can improve upon a basic orthogonal array.

Proposition 4 *Given an $OA(k, s)$ with M rows, an equidistant $CCC(s^2, s^2 - s, s^s)$ of size $(s - 1)M$ can be constructed. In particular, for $s = q$ (a prime power),*

(i) *an equidistant $CCC(q^2, q^2 - q, q^q)$ of size $q^2 - 1$ can be constructed*
(ii) *an optimal (equidistant) $CCC(q^2 - 1, q^2 - q, q^{q-1}(q - 1)^1)$ of size $q^2 - 1$ can be constructed.*

Proof Given an $OA(k, s)$ A on symbol set $S = \{1, \ldots, s\}$, we fix one symbol (say 1) and perform $s - 1$ substitutions on the others to obtain a new array B, in which each row of A yields $s - 1$ rows of B. More precisely, let $\pi \in S_s$ be the permutation $(2 \ldots s)$. Then for each row $\rho_i = a_{i,1}a_{i,2} \ldots a_{i,s^2}$ of A $(1 \leq i \leq M)$, and for each $1 \leq j \leq s - 1$, replace ρ_i by ${\rho_i}^j = (\pi^j(a_{i,1})\pi^j(a_{i,2}) \ldots \pi^j(a_{i,s^2}))$ to obtain array B of size $(s - 1)M$. It is clear that each row of B has the appropriate number and type of symbols; we check that the pairwise distance between rows is $s^2 - s$. Let α and β be different rows of B. If α and β arise from the same row of A under different substitutions, i.e. $\alpha = {r_i}^j$ and $\beta = {r_i}^k$ for some $1 \leq i \leq M$ and $1 \leq j \neq k \leq s - 1$, then they agree on the s copies of symbol 1 and disagree in all other positions. If α and β are two distinct rows of A under the same substitution, i.e. $\alpha = {r_h}^j$ and $\beta = {r_i}^j$ for some $1 \leq j \leq s-1$ and $1 \leq h \neq i \leq M$, then all agreements are as in the original rows. Now let α and β be different rows of A under different substitutions, i.e. $\alpha = {r_i}^k$ and $\beta = {r_j}^l$, some $1 \leq i \neq j \leq M$ and $1 \leq k \neq l \leq s-1$. Then it is still the case that each ordered pair in $S \times S$ occurs precisely once in these two rows, and hence pairwise distance is still $s^2 - s$.

For the second part, use a set of mutually orthogonal latin squares on symbols $\{1, \ldots, s\}$ to form the orthogonal array (with the squares in standard form so that the first column of the orthogonal array is an all-1 column). Perform substitutions as described above; to obtain the CCC from the resulting array, delete the first (all-1) column. Its optimality follows as it achieves the bound of Proposition 1. □

Example 4 An equidistant $CCC(9, 6, 3^3)$ of size 8 arising from a set of MOLS plus substitutions with $\pi = (23)$ is given by

1 1 1 2 2 2 3 3 3
1 1 1 3 3 3 2 2 2
1 2 3 1 2 3 1 2 3
1 3 2 1 3 2 1 3 2
1 2 3 2 3 1 3 1 2
1 3 2 3 2 1 2 1 3
1 2 3 3 1 2 2 3 1
1 3 2 2 1 3 3 2 1

Observe that deleting the first column yields a $CCC(8, 6, 3^2 2^1)$ of optimal size 8.

We observe that, while it is not possible in general to convert one EFPA to another with a smaller or larger symbol set by simple maps on the symbols, it can be done in the case where the EFPA possesses an extra property, which is possessed for example by orthogonal arrays. (The following result appeared in [10] for general FPAs.)

Proposition 5 *Let $n = m\mu$. Let A be an equidistant $CCC(n, d, \mu^m)$ such that, between any two rows of the corresponding FPA, each of the m^2 pairs (i, j) occurs precisely t times. Then A may be converted, by reduction modulo r (where $r|n$) to an equidistant $CCC(n, n-\frac{tm^2}{r}, (\frac{n}{r})^r)$.*

4.2 Arrays from Skolem sequences

Skolem sequences may be used to construct equidistant CCCs with compositions of the form 2^m or "close to" 2^m. A Skolem sequence of order n is a sequence $S = (s_1, s_2, \ldots, s_{2n})$ of $2n$ integers such that: for every $k \in \{1, 2, \ldots, n\}$ there exist exactly two elements $s_i, s_j \in S$ such that $s_i = s_j = k$, and if $s_i = s_j = k$ with $i < j$ then $j - i = k$. An extended Skolem sequence of order n is a sequence $ES = (s_1, s_2, \ldots, s_{2n+1})$ of $2n + 1$ integers satisfying the two conditions above plus a third condition: there is exactly one $s_i \in ES$ such that $s_i = 0$. An extended Skolem sequence of order n exists for any n ([1]); some small sequences are given by (1, 1, 0), (1, 1, 2, 0, 2), (3, 1, 1, 3, 2, 0, 2), (3, 1, 1, 3, 4, 2, 0, 2, 4).

Theorem 8 *For any $n \in \mathbb{N}$,*

(i) *an optimal (equidistant) $CCC(2n + 1, 2n, 2^n 1^1)$ of size $2n + 1$ can be constructed;*
(ii) *an equidistant $CCC(2n + 2, 2n, 2^{n+1})$ of size $2n + 1$ can be constructed.*

Proof For part (i), we will prove: given an extended Skolem sequence S of order n (length $2n + 1$), the array formed by taking as rows S and all its cyclic shifts is a code of the required type. For part (ii), we simply take the array from (i) and add a column consisting entirely of 0's.

Let $S = (s_1, s_2, \ldots, s_{2n+1})$, and let A be the $(2n + 1) \times (2n + 1)$ array whose rows are S and all its cyclic shifts. Denote the rows of A by ρ_j $(0 \le j \le 2n)$ where $\rho_0(i) = s_i$ $(1 \le i \le 2n+1)$ and ρ_j is the rightward shift of ρ_0 by j positions; more precisely $\rho_k(i) = s_{i-k}$ if $k < i \le 2n + 1$ and $\rho_k(i) = s_{2n+1+i-k}$ if $1 \le i \le k$.

Let ρ_j and ρ_k be any two rows of A $(j < k)$. There are three cases for a position i, $1 \le i \le 2n + 1$:

Case 1: $i > k$, i.e. $j < i \le 2n + 1$ and $k < i \le 2n + 1$. Then $\rho_j(i) = \rho_k(i) \Rightarrow s_{i-j} = s_{i-k} = x$ for some symbol $x \Rightarrow x = (i - j) - (i - k) = k - j$. Since $1 \le x \le n$, this case occurs only if $k - j \le n$.

Case 2: $j < i \le k$, i.e. $j < i \le 2n + 1$ and $1 \le i \le k$. Then $\rho_j(i) = \rho_k(i) \Rightarrow s_{i-j} = s_{2n+1+i-k} = x$ for some symbol $x \Rightarrow x = (2n + 1 + i - k) - (i - j) = 2n + 1 + j - k$. Since $1 \le x \le n$, this case occurs only if $k - j \ge n + 1$.

Case 3: $i \le j$, i.e. $1 \le i \le j$ and $1 \le i \le k$. Then $\rho_j(i) = \rho_k(i) \Rightarrow s_{2n+1+i-j} = s_{2n+1+i-k} = x$ for some symbol $x \Rightarrow x = (2n + 1 + i - j) - (2n + 1 + i - k) = k - j$. Since $1 \le x \le n$, this case occurs only if $k - j \le n$.

So, if $1 \le k - j \le n$, rows ρ_j and ρ_k can agree only in the symbol $k - j$, while if $n \le k - j \le 2n$, rows ρ_j and ρ_k can agree only in the symbol $2n + 1 + j - k$. In both cases, any agreement position must contain a symbol uniquely defined by j and k, giving Hamming distance at least $2n - 1$. Arguing as above, it can then be shown (we omit the details) that in fact ρ_j and ρ_k have precisely one position of agreement, i.e. distance $2n$ as claimed. □

Corollary 2 *For $n \in \mathbb{N}$, an optimal $CCC(2n+1, 2n, 2^n 1^1)$ of size $2n+1$ is given by: $(r, r-2, \ldots, 3, 1, 1, 3, \ldots, r-2, r, s, s-2, \ldots, 2, 0, 2, \ldots, s-2, s)$ where $r = n$ and $s = n-1$ if n is odd, and $r = n-1$ and $s = n$ if n is even, and the elements within the brackets are cyclically shifted. An equidistant $CCC(2n+2, 2n, 2^{n+1})$ of size $2n+1$ is given by $(r, r-2, \ldots, 3, 1, 1, 3, \ldots, r-2, r, s, s-2, \ldots, 2, 0, 2, \ldots, s-2, s)0$.*

Proof It is clear that the elements in the brackets form an extended Skolem sequence of order n. □

Example 5 An equidistant $CCC(10, 8, 2^5)$ of size 9 arising from the extended Skolem sequence $S = (3, 1, 1, 3, 4, 2, 0, 2, 4)$ is given by

$$\begin{array}{ll}
\rho_0 & 3\ 1\ 1\ 3\ 4\ 2\ 0\ 2\ 4\ 0 \\
\rho_1 & 4\ 3\ 1\ 1\ 3\ 4\ 2\ 0\ 2\ 0 \\
\rho_2 & 2\ 4\ 3\ 1\ 1\ 3\ 4\ 2\ 0\ 0 \\
\rho_3 & 0\ 2\ 4\ 3\ 1\ 1\ 3\ 4\ 2\ 0 \\
\rho_4 & 2\ 0\ 2\ 4\ 3\ 1\ 1\ 3\ 4\ 0 \\
\rho_5 & 4\ 2\ 0\ 2\ 4\ 3\ 1\ 1\ 3\ 0 \\
\rho_6 & 3\ 4\ 2\ 0\ 2\ 4\ 3\ 1\ 1\ 0 \\
\rho_7 & 1\ 3\ 4\ 2\ 0\ 2\ 4\ 3\ 1\ 0 \\
\rho_8 & 1\ 1\ 3\ 4\ 2\ 0\ 2\ 4\ 3\ 0
\end{array}$$

5 Binary equidistant frequency permutation arrays

It has been shown that equidistant $CCC(n, d, (\frac{n}{2})^2)$s of size greater than 1 can exist only for even distances d. Moreover, it is known ([15]) that the maximum size of an equidistant $CCC(n, d, (\frac{n}{2})^2)$ is at most n. Binary FPAs are binary constant weight codes, and have been much-studied. Below, for reference, we list a few construction methods which are specific to binary EFPAs: since these are easily derived from known results, we omit details of proofs (see references such as [12] for further details).

Definition 2 A Hadamard matrix of order n is an $n \times n$ matrix with entries $+1, -1$ satisfying $HH^t = nI$, i.e. its rows are pairwise orthogonal. For a Hadamard matrix of order n to exist, n must be 1, 2 or $4k$ for some positive integer k.

Construction 1 *For any n for which there exists a Hadamard matrix of order n, an equidistant $CCC(n, \frac{n}{2}, (\frac{n}{2})^2)$ can be constructed of size $n-1$.* ***Method:*** *Take a normalized Hadamard matrix $H(n)$ (i.e. all entries in its first row and first column are equal to 1) and remove the first row, then convert each occurrence of -1 to 0.*

Definition 3 A Legendre sequence is a binary sequence $v = [v_0, v_1, \ldots, v_{p-1}]$ of length p (prime), where $\frac{p-1}{2}$ is odd, such that $v_i = 0$ if i is a quadratic non-residue modulo p, and $v_i = 1$ if i is a quadratic residue modulo p; the digit v_0 can be either 0 or 1.

Construction 2 *For a prime p with $\frac{p-1}{2}$ odd (i.e. $p \equiv 3 \bmod 4$), an equidistant $CCC(p+1, \frac{p+1}{2}, (\frac{p+1}{2})^2)$ can be constructed of size p.* ***Method:*** *Form a $p \times p$ array by taking as rows a Legendre sequence v, and its $(p-1)$ rightward cyclic shifts. It can be shown that the Hamming distance between each row is $\frac{p+1}{2}$. To make the EFPA, append a column to the array consisting entirely of 0's if $v_0 = 1$, or 1's if $v_0 = 0$.*

A maximal length feedback shift register sequence (m-sequence for short) is a type of pseudorandom sequence possessing many useful properties (for more details see [8]). There exists a binary m-sequence of length $2^n - 1$ for any integer $n > 1$.

Construction 3 *For a Mersenne prime p (a prime of the form $2^n - 1$), an equidistant $CCC(p+1, \frac{p+1}{2}, (\frac{p+1}{2})^2)$ can be constructed of size p.* ***Method:*** *Let v be a binary m-sequence of length p. Then the array obtained from v together with all its $(p-1)$ cyclic rightward shifts is equidistant as a code. Each row has $\frac{p+1}{2}$ 1's, $\frac{p-1}{2}$ 0's and distance $\frac{p+1}{2}$. To make the EFPA, append a column of 0's to this array.*

Acknowledgments The author is supported by a Royal Society Dorothy Hodgkin Research Fellowship. Thanks to the Constraint Programming Group in the School of Computer Science at the University of St Andrews for their assistance in searching for examples. The author thanks the associate editor and referees who provided very helpful comments and suggestions.

References

1. Abrham J., Kotzig A.: Skolem sequences and additive permutations. Discrete Math. **37**, 143–146 (1981).
2. Baranyai Z.: On the factorization of the complete uniform hypergraph. In: Infinite and Finite Sets, Proc. Conf. Keszthely, 1973, Colloquium of the Mathematical Society Janos Bolyai, vol. 10, pp. 91–108, North-Holland, Amsterdam (1975).
3. Chu W., Colbourn C.J., Dukes P.: Constructions for permutation codes in powerline communications. Des. Codes Cryptogr. **32**, 51–64 (2004).
4. Chu W., Colbourn C.J., Dukes P.: On constant composition codes. Discrete Appl. Math. **154**, 912–929 (2006).
5. Colbourn C.J., Dinitz J.H. (eds.): The CRC Handbook of Combinatorial Designs. CRC Press, Boca Raton, FL (1996).
6. Ding C., Yin J.: Combinatorial constructions of constant composition codes. IEEE Trans. Inform. Theory **51**, 3671–3674 (2005).
7. Ding C., Yin J.: A construction of optimal constant composition codes. Des. Codes Cryptogr. **40**, 157–165 (2006).
8. Golomb S.: Shift Register Sequences. Holden-Day, San Francisco (1967).
9. Heinrich K., Van Rees G.H.J., Wallis W.D.: A general construction for equidistant permutation arrays. In: Graph Theory and Related Topics Proc. Conf., University of Waterloo, Waterloo, Ontario, 1977, pp. 247–252. Academic Press, New York-London (1979).
10. Huczynska S., Mullen G.L.: Frequency permutation arrays. J. Combin. Des. **14**, 463–478 (2006).
11. Luo Y., Fu F-W., Han Vinck A.J., Chen W.: On constant-composition codes over $\mathbb{Z}_q$. IEEE Trans. Inform. Theory **49**, 3010–3016 (2003).
12. Nguyen Q.A., Gyorfi L., Massey J.L.: Constructions of binary constant-weight cyclic codes and cyclically permutable codes. IEEE Trans. Inform. Theory **38**, 940–949 (1992).
13. Semakov N.V., Zinoviev V.A.: Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs. Probl. Inform. Trans. **4**, 1–7 (1968).
14. Vanstone, S.A.: The asymptotic behaviour of equidistant permutation arrays. Can. J. Math. **21**, 45–48 (1979).
15. Zeng F.: Construction of constant weight code and some upper bounds. In: ISIT 2005 Proceedings, Information Theory (2005).