[16] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*. Berlin, Germany: Springer-Verlag, 1991, vol. 561, Lecture Notes in Computer Science.
[17] D. H. Lee, J. Kim, J. Hong, J. W. Han, and D. Moon, "Algebraic attacks on summation generators," in *FSE 2004*. Berlin, Germany: Springer-Verlag, 2004, vol. 3017, Lecture Notes in Computer Science, pp. 34–48.
[18] N. Li and W. F. Qi, "Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2271–2273, May 2006.
[19] F. MacWilliams and N. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.
[20] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," in *Advances in Cryptology – EUROCRYPT 2004*. Berlin, Germany: Springer-Verlag, 2004, vol. 3027, Lecture Notes in Computer Science, pp. 474–491.
[21] L. Qu, G. Feng, and C. Li, On the Boolean Functions with Maximum Possible Algebraic Immunity: Construction and a Lower Bound of the Count [Online]. Available: http://eprint.iacr.org/2005/449.pdf.

Distance-Preserving and Distance-Increasing Mappings From Ternary Vectors to Permutations

Jyh-Shyan Lin, Jen-Chun Chang, Rong-Jaye Chen, and Torleiv Kløve, *Fellow, IEEE*

***Abstract*—Permutation arrays have found applications in powerline communication. One construction method for permutation arrays is to map good codes to permutations using a distance-preserving mappings (DPM). DPMs are mappings from the set of all q-ary vectors of a fixed length to the set of permutations of some fixed length (the same or longer) such that every two distinct vectors are mapped to permutations with the same or larger Hamming distance than that of the vectors. A DPM is called distance increasing (DIM) if the distances are strictly increased (except when the two vectors are equal). In this correspondence, we propose constructions of DPMs and DIMs from ternary vectors. The constructed DPMs and DIMs improve many lower bounds on the maximal size of permutation arrays.**

***Index Terms*—Distance-increasing mappings, distance-preserving mappings, permutation arrays, powerline communication.**

I. Introduction

Permutation arrays as combinatorial objects have been studied for many years. However, a few years ago, Ferreira and Vinck [6] found applications in powerline communication: permutations arrays can be used as error correcting codes. For a given length N, a permutation array (of length N) is a set of permutations of the set $F_N = \{1, 2, \ldots, N\}$. The minimum distance D of the permutation array is, as usual, the smallest Hamming distance between the permutations. For the application, there is the usual trade off between minimum distance and size of the code (permutation array).

Because of the application in powerline communication, there has been a renewed interest in permutation arrays, and a substantial number of papers with new and better constructions have appeared during the last 6–7 years, see the list of references. One way to construct permutation arrays, introduced by Ferreira and Vinck [6] is to use the image of codes under a distance preserving mapping (DPM) from binary vectors to permutations. A mapping from the set of all binary vectors of length n to the set of all permutations of $\{1, 2, \ldots, N\}$ is called a distance-preserving mapping (DPM) if every two distinct vectors are mapped to permutations with the same or even larger Hamming mutual distance than that of the vectors. A distance-increasing mapping (DIM) is a special DPM such that the distances are strictly increased (except when the two vectors are equal). Since the mapping is distance preserving, the minimum distance of the image (which is a permutation array) is lower bounded by the minimum distance of the code. A DIM will increase the minimum distance. A number of papers have studied various constructions of DPMs and DIMs, with variations: [2]–[15], [17]. The permutation arrays constructed by this method are the best known for many values of the parameters N and D.

Since the largest ternary codes of length n and minimum distance d are (in most cases) larger (often substantially larger) than the binary codes with the same parameters, it is clear that a DPM from ternary vectors in many cases will give larger permutation arrays than the known constructions. Existence of such DPM has therefore been an interesting and important open question. The main result of this correspondence is the construction of a DPM from ternary vectors of length $n \geq 13$ to permutations of the same length. We also construct DIM from ternary vectors of length $n \geq 3$ to permutations of length $n + 2$. We give a few numerical examples to illustrate that this indeed gives much better permutation arrays. We note that another construction of a DPM from ternary vectors [15] has been submitted after our initial submission of this correspondence. The construction method is quite different and certainly of independent interest.

The correspondence is organized as follows. In the next section, we introduce some notations and state our main results. In Section III, we introduce a general recursive construction of DPMs and DIMs. In Sections IV and V, we introduce mappings that can be used to start the recursion in the three cases we consider.

II. Notations and Main Results

Let S_N denote the set of all $N!$ permutations of F_N. A permutation $\pi : F_N \to F_N$ is represented by an N-tuple $\pi = (\pi_1, \pi_2, \ldots, \pi_N)$ where $\pi_i = \pi(i)$. Let Z_3^n denote the set of all ternary vectors of length n. The Hamming distance between two permutations $\pi, \rho \in S_N$ is

$$d_H(\pi, \rho) = |\{j \in F_N : \pi_j \neq \rho_j\}|.$$

Let $\mathcal{F}_{n,N}$ be the set of injective functions from Z_3^n to S_N. Note that $\mathcal{F}_{n,N}$ is empty if $N! < 3^n$.

For $N \geq n$, let $\mathcal{P}_{n,N}$ be the set of functions in $\mathcal{F}_{n,N}$ such that

$$d_H(f(\mathbf{x}), f(\mathbf{y})) \geq d_H(\mathbf{x}, \mathbf{y})$$

for all $\mathbf{x}, \mathbf{y} \in Z_3^n$. These mappings are called distance-preserving mappings (DPM).

Manuscript received January 8, 2007; revised November 20, 2007. The work of J.-S. Lin and R.-J. Chen was supported in part by Taiwan National Council under Contracts NSC 96-2221-E-009-089 and NSC 96-2219-E-009-013 and in part by TWISC@NCTU. The work of J.-C. Chang was supported by Taiwan National Council under Contracts NSC 96-2221-E-305-006 and NSC 96-2628-E-305-002-MY3. The work of T. Kløve was supported by The Norwegian Research Council under Contract 160236/V30.

J.-S. Lin is with the Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan (e-mail: linch@csie.nctu.edu.tw).

J.-C. Chang is with the Department of Computer Science and Information Engineering, National Taipei University, Taipei, Taiwan (e-mail: jcchang@mail.ntpu.edu.tw).

R.-J. Chen is with the Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan (e-mail: rjchen@csie.nctu.edu.tw).

T. Kløve is with the Department of Informatics, University of Bergen, Bergen, Norway (e-mail: Torleiv.Klove@ii.uuib.no).

Communicated by V. Vaishampayan, Associate Editor At Large.

Digital Object Identifier 10.1109/TIT.2007.915706

For $N > n$, let $\mathcal{I}_{n,N}$ be the set of functions in $\mathcal{F}_{n,N}$ such that

$$d_H(f(\mathbf{x}), f(\mathbf{y})) > d_H(\mathbf{x}, \mathbf{y}) \tag{1}$$

for all distinct $\mathbf{x}, \mathbf{y} \in Z_3^n$. These mappings are called distance-increasing mappings (DIM).

An (N, D) permutation array (PA) is a subset of S_N such that the Hamming distance between any two distinct permutations in the array is at least D. An $(n, d; q)$ code is a subset of vectors (codewords) of length n over an alphabet of size q and with distance at least d between distinct codewords. One construction method of PAs is to construct an (N, D)-PA from an $(n, d; q)$ code using DPMs or DIMs. More precisely, if C is an $(n, d; q)$ code and there exists a DPM f from Z_q^n to S_N, then $f(C)$ is an (N, d)-PA. If f is a DIM, then $f(C)$ is an $(N, d+1)$-PA. This has been a main motivation for studying DPMs. Let $P(N, D)$ denote the largest possible size of an (N, D)-PA. The exact value of $P(N, D)$ is still an open problem in most cases, but we can lower bound this value by the maximal size of a suitable code provided a DPM (or DIM) is known. Let $A_q(n, d)$ denote the largest possible size of an (n, d) code over a code alphabet of size q. In [5], Chang *et al.* used this approach to show that for $N \geq 4$ and $2 \leq D \leq N$, we have $P(N, D) \geq A_2(N, D-1)$. In [4], Chang further improved the bound to $P(N, D) \geq A_2(N, D-\delta)$ for any δ such that $3 \leq \delta + 1 \leq D \leq N$ and any $N \geq N_\delta$, where N_δ is a positive integer determined by δ, e.g., $N_2 = 16$.

Our main result is the following theorem.

Theorem 1:

a) For $N \geq 5$ and $2 \leq D \leq N$, we have
$$P(N, D) \geq A_3(N-2, D-1).$$
b) For $N \geq 10$ and $2 \leq D \leq N$, we have
$$P(N, D) \geq A_3(N-1, D).$$
c) For $N \geq 13$ and $2 \leq D \leq N$, we have
$$P(N, D) \geq A_3(N, D).$$

Bounds on $A_2(n, d)$ and $A_3(n, d)$ have been studied by many researchers, see e.g., [16, Ch. 5], and [1]. In general, the lower bounds on $P(N, D)$ obtained from use of ternary codes are better than those obtained from binary codes. For example, using Chang's bound [4], we get $P(16, 5) \geq A_2(16, 3) \geq 2720$, whereas Theorem 1 gives $P(16, 5) \geq A_3(16, 5) \geq 19683$. Similarly, Chang's bound gives $P(16, 9) \geq A_2(16, 7) \geq 36$ whereas the new bound gives $P(16, 9) \geq A_3(16, 9) \geq 243$.

The proof of the theorem is done by explicit construction of DPMs and DIMs. More precisely, we give constructions that show the following lemma which in turn implies the theorem.

Lemma 1:

a) $\mathcal{I}_{n,n+2}$ is nonempty for $n \geq 3$.
b) $\mathcal{P}_{n,n+1}$ is nonempty for $n \geq 9$.
c) $\mathcal{P}_{n,n}$ is nonempty for $n \geq 13$.

A relatively simple recursive method is given (in the next section) to construct a mapping of length $n+1$ from a mapping of length n. Explicit mappings that start the recursion in the three cases are given in last part of the correspondence.

III. The General Recursive Construction

For any array $\mathbf{u} = (u_1, u_2, \ldots, u_n)$, we use the notation $\mathbf{u}_i$ to denote the element u_i in position i.

We start with a recursive definition of functions from Z_3^n to S_N. For $f \in \mathcal{F}_{n,N}$, define $g = H(f) \in \mathcal{F}_{n+1,N+1}$ as follows. Let

$$\mathbf{x} = (x_1, x_2, \ldots, x_n) \in Z_3^n \text{ and } f(\mathbf{x}) = (\varphi_1, \varphi_2, \ldots, \varphi_N).$$

Suppose that the element $N-4$ occurs in position r, that is $\varphi_r = N-4$. Then

$$g(\mathbf{x}|0)_i = \begin{cases} N+1, & \text{for } i = N+1 \\ \varphi_i, & \text{for } i \neq N+1 \end{cases}$$

$$g(\mathbf{x}|1)_i = \begin{cases} N-4, & \text{for } i = N+1 \\ N+1, & \text{for } i = r \\ \varphi_i, & \text{for } i \notin \{r, N+1\}. \end{cases}$$

If n is even and $x_n = 2$, then

$$g(\mathbf{x}|2)_i = \begin{cases} N+1, & \text{for } i = N-1 \\ \varphi_{N-1}, & \text{for } i = N+1 \\ \varphi_i, & \text{for } i \notin \{N-1, N+1\}. \end{cases}$$

otherwise (n is odd or $x_n < 2$), then

$$g(\mathbf{x}|2)_i = \begin{cases} N+1, & \text{for } i = N \\ \varphi_N, & \text{for } i = N+1 \\ \varphi_i, & \text{for } i \notin \{N, N+1\}. \end{cases}$$

We note that $g(\mathbf{x}|a)_i \neq f(\mathbf{x})_i$ for at most one value of $i \leq N$.

For $f \in \mathcal{F}_{m,M}$, we define a sequence of functions $f_n \in \mathcal{F}_{n,n+M-m}$, for all $n \geq m$, recursively by

$$f_m = f \text{ and } f_{n+1} = H(f_n) \text{ for } n \geq m.$$

Lemma 2: If $f_m \in \mathcal{P}_{m,M}$ where $M \geq m$, m is odd, and

$$f_m(\mathbf{x})_M \notin \{M-4, M-3\} \text{ for all } \mathbf{x} \in Z_3^m$$

then $f_n \in \mathcal{P}_{n,n+M-m}$ for all $n \geq m$.

Lemma 3: If $f_m \in \mathcal{I}_{m,M}$, where $M > m$ and m is odd, and

$$f_m(\mathbf{x})_M \notin \{M-4, M-3\} \text{ for all } \mathbf{x} \in Z_3^m$$

then $f_n \in \mathcal{I}_{n,n+M-m}$ for all $n \geq m$.

Proof: We prove Lemma 3; the proof of Lemma 2 is similar (and a little simpler). The proof is by induction. First we prove that $g = f_{m+1} \in \mathcal{I}_{m+1,M+1}$. Let $\mathbf{x}, \mathbf{y} \in Z_3^m$ and

$$f(\mathbf{x}) = (\varphi_1, \varphi_2, \ldots, \varphi_M),\ \varphi_r = M-4$$
$$f(\mathbf{y}) = (\gamma_1, \gamma_2, \ldots, \gamma_M),\ \gamma_s = M-4.$$

We want to show that

$$d_H(g(\mathbf{x}|a), g(\mathbf{y}|b)) > d_H((\mathbf{x}|a), (\mathbf{y}|b))$$

if $(\mathbf{x}|a) \neq (\mathbf{y}|b)$.

First, consider $\mathbf{x} = \mathbf{y}$ and $a \neq b$. Since $\varphi_M \neq M-4$, it follows immediately from the definition of g that

$$d_H(g(\mathbf{x}|a), g(\mathbf{x}|b)) \geq 2 > 1 = d_H((\mathbf{x}|a), (\mathbf{x}|b)).$$

For $\mathbf{x} \neq \mathbf{y}$, we want to show that

$$d_H(g(\mathbf{x}|a), g(\mathbf{y}|b)) - d_H(f(\mathbf{x}), f(\mathbf{y})) \geq d_H(a, b) \tag{2}$$

for all $a, b \in Z_3$ since this implies

$$\begin{aligned} d_H(g(\mathbf{x}|a), g(\mathbf{y}|b)) &\geq d_H(f(\mathbf{x}), f(\mathbf{y})) + d_H(a, b) \\ &> d_H(\mathbf{x}, \mathbf{y}) + d_H(a, b) \\ &= d_H((\mathbf{x}|a), (\mathbf{y}|b)). \end{aligned}$$

The condition (2) is equivalent to the following:

$$\sum_{i=1}^{M+1} (\Delta_{g,i} - \Delta_{f,i}) \geq d_H(a, b) \tag{3}$$

where

$$\Delta_{g,i} = d_H(g(\mathbf{x}|a)_i, g(\mathbf{y}|b)_i) \text{ and } \Delta_{f,i} = d_H(f(\mathbf{x})_i, f(\mathbf{y})_i)$$

and where, for technical reasons, we define $\Delta_{f,M+1} = 0$. The point is that at most three of the terms $\Delta_{g,i} - \Delta_{f,i}$ are nonzero. We look at one combination of a and b in detail as an illustration, namely $a = 1$

and $b = 2$. Then $g(\mathbf{x}|a)_i = f(\mathbf{x})_i$ and $g(\mathbf{y}|b)_i = f(\mathbf{y})_i$ and so $\Delta_{g,i} = \Delta_{f,i}$ for all $i \leq M+1$, *except* in the following three cases:

i	$f(\mathbf{x})_i$	$f(\mathbf{y})_i$	$g(\mathbf{x}\|a)_i$	$g(\mathbf{y}\|b)_i$
r	$M-4$	γ_r	$M+1$	γ_r
M	φ_M	γ_M	φ_M	$M+1$
$M+1$	$-$	$-$	$M-4$	γ_M

i	$\Delta_{f,i}$	$\Delta_{g,i}$	$\Delta_{g,i} - \Delta_{f,i}$
r	0 or 1	1	0 or 1
M	0 or 1	1	0 or 1
$M+1$	0	1	1.

Note that we have used the fact that $\gamma_M \neq M-4$. We see that $\sum(\Delta_{g,i} - \Delta_{f,i}) \geq 1 = d_H(a,b)$.

The other combinations of a and b are similar. This proves that $f_{m+1} = g \in \mathcal{I}_{m+1,M+1}$.

Now, let $h = H(g) = f_{m+2}$. A similar analysis will show that $h \in \mathcal{I}_{m+2,M+2}$. We first give a table of the last three symbols in $h(\mathbf{x}|a_1a_2)$ as these three symbols are the most important in the proof. Let $\varphi_s = M-3$. By assumption, $s < M$

a_1a_2	$h(\mathbf{x}\|a_1a_2)_M$	$h(\mathbf{x}\|a_1a_2)_{M+1}$	$h(\mathbf{x}\|a_1a_2)_{M+2}$
00	φ_M	$M+1$	$M+2$
10	φ_M	$M-4$	$M+2$
20	$M+1$	φ_M	$M+2$
01	φ_M	$M+1$	$M-3$
11	φ_M	$M-4$	$M-3$
21	$M+1$	φ_M	$M-3$
02	φ_M	$M+2$	$M+1$
12	φ_M	$M+2$	$M-4$
22	$M+2$	φ_M	$M+1$.

In addition

$$h(\mathbf{x}|1a_2)_r = M+1 \text{ and } h(\mathbf{x}|a_11)_s = M+2.$$

Note that we have used the fact that $\varphi_M \neq M-3$ here, since if we had $\varphi_M = M-3$, then we would for example have had $h(\mathbf{x}|01)_M = h(\mathbf{x}|01)_{M+2}$. From the table, we first see that

$$d_H(h(\mathbf{x}|a_1a_2), h(\mathbf{x}|b_1b_2)) > d_H(a_1a_2, b_1b_2)$$

if $a_1a_2 \neq b_1b_2$. For example $h(\mathbf{x}|10)$ and $h(\mathbf{x}|21)$ differ in positions $r, s, M, M+1$ and $M+2$. As another example, $h(\mathbf{x}|02)$ and $h(\mathbf{x}|22)$ differ in positions M and $M+1$.

Next, consider $d_H(h(\mathbf{x}|a_1a_2), h(\mathbf{y}|b_1b_2))$ for $\mathbf{x} \neq \mathbf{y}$. We see that

$$d_H(h(\mathbf{x}|a_1a_2)_i, h(\mathbf{y}|b_1b_2)_i) \geq d_H(f(\mathbf{x})_i, f(\mathbf{y})_i)$$

for $i < M$: from the table above, we can see that

$$\begin{aligned} &d_H(h(\mathbf{x}|a_1a_2)_M h(\mathbf{x}|a_1a_2)_{M+1} h(\mathbf{x}|a_1a_2)_{M+2}, \\ &\quad h(\mathbf{y}|b_1b_2)_M h(\mathbf{y}|b_1b_2)_{M+1} h(\mathbf{y}|b_1b_2)_{M+2}) \\ &\geq d_H(\varphi_M, \gamma_M) + d_H(a_1a_2, b_1b_2). \end{aligned}$$

As an example, let $a_1a_2 = 10$ and $b_1b_2 = 02$. Then

$$h(\mathbf{x}|10)_M, h(\mathbf{x}|10)_{M+1}, h(\mathbf{x}|10)_{M+2} = \varphi_M, M-4, M+2$$

and

$$h(\mathbf{y}|02)_M, h(\mathbf{y}|02)_{M+1}, h(\mathbf{y}|02)_{M+2} = \gamma_M, M+2, M+1.$$

The distance between the two is 2 (if $\varphi_M = \gamma_M$) or 3 (otherwise). The other combinations of a_1a_2 and b_1b_2 are similar. From this we can conclude that $h \in \mathcal{I}_{m+2,M+2}$ in a similar way we showed that $g \in \mathcal{I}_{m+1,M+1}$ above.

Further, we note that

$$h(\mathbf{x}|a_1a_2)_{M+2} \notin \{(M+2)-4, (M+2)-3\}.$$

Therefore, we can repeat the argument and, by induction, obtain $f_n \in \mathcal{I}_{n,n+M-m}$ for all $n \geq m$.

A function $F \in \mathcal{I}_{3,5}$ such that $F(\mathbf{x})_5 \notin \{1,2\}$ was found by computer search. Here is a listing of the elements $\mathbf{x} \in Z_3^3$ and the corresponding values of $F(\mathbf{x}) \in S_5$

$$\begin{array}{lll} (0,0,0)(1,2,3,4,5), & (0,0,1)(1,2,5,4,3), & (0,0,2)(1,2,3,5,4) \\ (0,1,0)(4,2,3,1,5), & (0,1,1)(4,2,5,1,3), & (0,1,2)(5,2,3,1,4) \\ (0,2,0)(1,4,3,2,5), & (0,2,1)(1,4,5,2,3), & (0,2,2)(1,5,3,2,4) \\ (1,0,0)(2,3,1,4,5), & (1,0,1)(2,5,1,4,3), & (1,0,2)(2,3,1,5,4) \\ (1,1,0)(2,3,4,1,5), & (1,1,1)(2,5,4,1,3), & (1,1,2)(2,3,5,1,4) \\ (1,2,0)(4,3,1,2,5), & (1,2,1)(4,5,1,2,3), & (1,2,2)(5,3,1,2,4) \\ (2,0,0)(3,1,2,4,5), & (2,0,1)(5,1,2,4,3), & (2,0,2)(3,1,2,5,4) \\ (2,1,0)(3,4,2,1,5), & (2,1,1)(5,4,2,1,3), & (2,1,2)(3,5,2,1,4) \\ (2,2,0)(3,1,4,2,5), & (2,2,1)(5,1,4,2,3), & (2,2,2)(3,1,5,2,4). \end{array}$$

This, combined with Lemma 3, proves Lemma 1 a).

Remark: The recursive construction can be generalized. In the construction above we defined r by $\varphi_r = N-4$. The recursion would work equally well if we defined r by $\varphi_r = N-t$ for some fixed $t \geq 3$ and changed the conditions in the lemmas to

$$f_m(\mathbf{x})_M \notin \{M-t, M-t+1\}. \tag{4}$$

It is also possible to vary the t from one step to the next as long as, for all $\mathbf{x} \in Z_3^n$

$$\begin{cases} N-t \neq f_n(\mathbf{x})_N, & \text{if } n \text{ is odd} \\ N-t \notin \{f_n(\mathbf{x})_{N-1}, f_n(\mathbf{x})_N\}, & \text{if } n \text{ is even.} \end{cases} \tag{5}$$

One reason we chose a fixed t is that if the condition (4) is satisfied at the start of the recursion, then (5) is satisfied for all $n \geq m$.

IV. Construction of a Mapping in $\mathcal{P}_{n,n+1}$ for $n \geq 9$

To prove Lemma 1 b), using Lemma 2, we need some $f \in \mathcal{P}_{9,10}$ such that

$$f(\mathbf{x})_{10} \notin \{6,7\} \text{ for all } \mathbf{x} \in Z_3^9. \tag{6}$$

An extensive computer search has been unsuccessful in coming up with such a mapping. However, an indirect approach has been successful. The approach is to construct f from two simpler mappings found by computer search. We describe this construction.

For a vector $\rho = (\rho_1, \rho_2, \ldots, \rho_n)$ and a set

$$X \subset \{1, 2, \ldots, n\}$$

let $\rho_{\setminus X}$ denote the vector obtained from ρ by removing the elements with subscript in X. For example

$$(\rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6)_{\setminus\{1,5\}} = (\rho_2, \rho_3, \rho_4, \rho_6).$$

By computer search we have found mappings $G \in \mathcal{F}_{5,7}$ and $H \in \mathcal{F}_{4,6}$ that satisfy the following conditions:

a) for every $\mathbf{x} \in Z_3^5$, $6 \in \{G(\mathbf{x})_1, G(\mathbf{x})_2, G(\mathbf{x})_3\}$;

b) for every $\mathbf{x} \in Z_3^5$, $7 \in \{G(\mathbf{x})_4, G(\mathbf{x})_5, G(\mathbf{x})_6\}$;

c) for every distinct $\mathbf{x}, \mathbf{y} \in Z_3^5$;
$d_H(G(\mathbf{x})_{\setminus\{7\}}, G(\mathbf{y})_{\setminus\{7\}}) \geq d_H(\mathbf{x}, \mathbf{y})$;

d) for every $\mathbf{u} \in Z_3^4$, $1 \in \{H(\mathbf{u})_1, H(\mathbf{u})_2, H(\mathbf{u})_3\}$;

e) for every distinct $\mathbf{u}, \mathbf{v} \in Z_3^4$;
$d_H(H(\mathbf{u})_{\setminus\{5,6\}}, H(\mathbf{v})_{\setminus\{5,6\}}) \geq d_H(\mathbf{u}, \mathbf{v})$.

Explicit listing of the mappings G and H have been omitted for space reasons (page limitation on correspondences), but it has been included in an early version of the manuscript stored in arXiv, [14]. We will now show how these mappings can be combined to produce a mapping $f \in \mathcal{P}_{9,10}$ satisfying (6).

Let $\mathbf{x} \in Z_3^9$. Then $\mathbf{x} = (\mathbf{x}_L, \mathbf{x}_R)$, where $\mathbf{x}_L \in Z_3^5$ and $\mathbf{x}_R \in Z_3^4$. Let

$$(\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \varphi_7) = G(\mathbf{x}_L)$$
$$(\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6) = H(\mathbf{x}_R) + (4, 4, 4, 4, 4, 4).$$

We note that Condition d) implies that $\gamma_5 \geq 6$ and $\gamma_6 \geq 6$. Similarly, Conditions a) and b) imply that $\varphi_7 \leq 5$.

Define $\rho = (\rho_1, \rho_2, \ldots, \rho_{10})$ as follows:

$$\begin{aligned}
&\rho_i = \gamma_5, && \text{if } 1 \leq i \leq 3 && \text{and} && \varphi_i = 6\\
&\rho_i = \gamma_6, && \text{if } 4 \leq i \leq 6 && \text{and} && \varphi_i = 7\\
&\rho_i = \varphi_i, && \text{if } 1 \leq i \leq 6 && \text{and} && \varphi_i \leq 5\\
&\rho_i = \varphi_7, && \text{if } 7 \leq i \leq 9 && \text{and} && \gamma_{i-6} = 5\\
&\rho_i = \gamma_{i-6}, && \text{if } 7 \leq i \leq 10 && \text{and} && \gamma_{i-6} \geq 6.
\end{aligned}$$

In ρ, swap 1 and 6 and also swap 2 and 7, and let the resulting array be denoted by π. More formally

$$\begin{aligned}
&\pi_i = 1, && \text{if } \rho_i = 6\\
&\pi_i = 2, && \text{if } \rho_i = 7\\
&\pi_i = 6, && \text{if } \rho_i = 1\\
&\pi_i = 7, && \text{if } \rho_i = 2\\
&\pi_i = \rho_i, && \text{otherwise.}
\end{aligned}$$

Then define

$$f(\mathbf{x}) = \pi.$$

We will show that f has the stated properties. We first show that $\pi \in S_{10}$. We have $\varphi \in S_7$ and γ is a permutation of $(5, 6, 7, 8, 9, 10)$. In particular, $5, 6$, and 7 appear both in φ and γ. The effect of the first line in the definition of ρ is to move another element (γ_5) into the position where φ has a 6. Similarly, the second line overwrites the 7 in ρ, and the fourth line overwrites the 5 in γ. The definition of ρ is then the concatenation of the six first (overwritten) elements of φ and the five first (overwritten) elements of γ. Therefore, ρ contains no duplicate elements, that is, $\rho \in S_{10}$.

The element 1 in ρ must be either in one of the first six positions, coming from φ, or in one of the positions 7–9 (if $\varphi_7 = 1$). Similarly, the element 2 must be in one of the first nine positions of ρ. Therefore, both 6 and 7 must be among the first nine elements of π, that is $\pi_{10} \notin \{6, 7\}$.

Finally, we must show that f is distance-preserving. Let $\mathbf{x} \neq \mathbf{x}'$, and let the arrays corresponding to $\mathbf{x}'$ be denoted by φ', γ', ρ' and π'. By assumption

$$\begin{aligned}
d_H(\mathbf{x}, \mathbf{x}') &= d_H(\mathbf{x}_L, \mathbf{x}'_L) + d_H(\mathbf{x}_R, \mathbf{x}'_R)\\
&\leq d_H(\varphi_{\setminus\{7\}}, \varphi'_{\setminus\{7\}}) + d_H(\gamma_{\setminus\{5,6\}}, \gamma'_{\setminus\{5,6\}}). \qquad (7)
\end{aligned}$$

For $1 \leq i \leq 6$ we have

$$d_H(\varphi_i, \varphi'_i) \leq d_H(\rho_i, \rho'_i). \qquad (8)$$

If $\varphi_i = \varphi'_i$ this is obvious. Otherwise, we may assume without loss of generality that $\varphi'_i < \varphi_i$ and we must show that $\rho_i \neq \rho'_i$. If $\varphi_i \leq 5$, then

$$\rho'_i = \varphi'_i < \varphi_i = \rho_i.$$

If $\varphi_i = 6$, then

$$\rho'_i = \varphi'_i \leq 5 \text{ and } \rho_i = \gamma_5 \geq 6.$$

If $\varphi_i = 7$, then $4 \leq i \leq 6$ and so $\varphi'_i \neq 6$. Hence

$$\rho'_i = \varphi'_i \leq 5 \text{ and } \rho_i = \gamma_6 \geq 6.$$

This completes that proof of (8). A similar arguments show that for $7 \leq i \leq 10$ we have

$$d_H(\gamma_{i-6}, \gamma'_{i-6}) \leq d_H(\rho_i, \rho'_i) \qquad (9)$$

and that for $1 \leq i \leq 10$ we have

$$d_H(\rho_i, \rho'_i) \leq d_H(\pi_i, \pi'_i). \qquad (10)$$

Combining (7)–(10), we get

$$\begin{aligned}
d_H(\mathbf{x}, \mathbf{x}') &\leq d_H(\varphi_{\setminus\{7\}}, \varphi'_{\setminus\{7\}}) + d_H(\gamma_{\setminus\{5,6\}}, \gamma'_{\setminus\{5,6\}})\\
&\leq d_H(\rho, \rho') \leq d_H(\pi, \pi').
\end{aligned}$$

Hence, f is distance-preserving.

V. Construction of a Mapping in $\mathcal{P}_{n,n}$ for $n \geq 13$

The construction of a mapping $f \in \mathcal{P}_{13,13}$ which proves Lemma 1 c) is similar to the construction in the previous section. However, the construction is more involved and contains several steps. We will describe the constructions and properties of the intermediate mappings. The details of proofs are similar to the proof in the previous section and we omit these details.

We start with three mappings $R, S \in \mathcal{F}_{3,5}$ and $T \in \mathcal{F}_{4,6}$. These were found by computer search and are listed explicitly below. These mappings are used as building blocks similarly to what was done in the previous section. They have the following properties:

- for every $\mathbf{x} \in Z_3^3$, $1 \in \{R(\mathbf{x})_1, R(\mathbf{x})_2, R(\mathbf{x})_3\}$;
- for every $\mathbf{x} \in Z_3^3$, $R(\mathbf{x})_5 \neq 5$;
- for every distinct $\mathbf{x}, \mathbf{y} \in Z_3^3$;
  $d_H(R(\mathbf{x})_{\setminus\{4,5\}}, R(\mathbf{y})_{\setminus\{4,5\}}) \geq d_H(\mathbf{x}, \mathbf{y})$;
- for every $\mathbf{x} \in Z_3^3$, $2 \in \{S(\mathbf{x})_1, S(\mathbf{x})_2, S(\mathbf{x})_3\}$;
- for every $\mathbf{x} \in Z_3^3$, $S(\mathbf{x})_5 \neq 1$;
- for every distinct $\mathbf{x}, \mathbf{y} \in Z_3^3$
  $d_H(S(\mathbf{x})_{\setminus\{4,5\}}, S(\mathbf{y})_{\setminus\{4,5\}}) \geq d_H(\mathbf{x}, \mathbf{y})$;
- for every $\mathbf{x} \in Z_3^4$, $2 \in \{T(\mathbf{x})_1, T(\mathbf{x})_2, T(\mathbf{x})_3\}$;
- for every $\mathbf{x} \in Z_3^4$, $T(\mathbf{x})_6 \neq 1$;
- for every distinct $\mathbf{x}, \mathbf{y} \in Z_3^4$;
  $d_H(T(\mathbf{x})_{\setminus\{5,6\}}, T(\mathbf{y})_{\setminus\{5,6\}}) \geq d_H(\mathbf{x}, \mathbf{y})$.

Listing of the elements $\mathbf{x} \in Z_3^3$ and the corresponding values of $R(\mathbf{x}) \in S_5$

$(0,0,0)(1,2,3,5,4)$, $(0,0,1)(1,4,3,5,2)$, $(0,0,2)(1,5,3,4,2)$
$(0,1,0)(1,2,4,5,3)$, $(0,1,1)(1,4,2,5,3)$, $(0,1,2)(1,5,4,3,2)$
$(0,2,0)(1,2,5,4,3)$, $(0,2,1)(1,4,5,3,2)$, $(0,2,2)(1,3,5,4,2)$
$(1,0,0)(4,1,3,5,2)$, $(1,0,1)(5,1,3,4,2)$, $(1,0,2)(2,1,3,5,4)$
$(1,1,0)(3,1,4,5,2)$, $(1,1,1)(5,1,4,3,2)$, $(1,1,2)(2,1,4,5,3)$
$(1,2,0)(4,1,5,3,2)$, $(1,2,1)(5,1,2,4,3)$, $(1,2,2)(2,1,5,4,3)$
$(2,0,0)(4,2,1,5,3)$, $(2,0,1)(5,4,1,3,2)$, $(2,0,2)(2,5,1,4,3)$
$(2,1,0)(3,2,1,5,4)$, $(2,1,1)(3,4,1,5,2)$, $(2,1,2)(3,5,1,4,2)$
$(2,2,0)(4,3,1,5,2)$, $(2,2,1)(5,3,1,4,2)$, $(2,2,2)(2,3,1,5,4)$.

Listing of the elements $\mathbf{x} \in Z_3^3$ and the corresponding values of $S(\mathbf{x}) \in S_5$

$(0,0,0)(2,1,3,4,5)$, $(0,0,1)(2,4,3,1,5)$, $(0,0,2)(2,5,3,1,4)$
$(0,1,0)(2,1,4,5,3)$, $(0,1,1)(2,4,1,5,3)$, $(0,1,2)(2,5,4,1,3)$
$(0,2,0)(2,1,5,4,3)$, $(0,2,1)(2,4,5,1,3)$, $(0,2,2)(2,3,5,1,4)$
$(1,0,0)(4,2,3,1,5)$, $(1,0,1)(5,2,3,1,4)$, $(1,0,2)(1,2,3,5,4)$
$(1,1,0)(3,2,4,1,5)$, $(1,1,1)(5,2,4,1,3)$, $(1,1,2)(1,2,4,5,3)$
$(1,2,0)(4,2,5,1,3)$, $(1,2,1)(5,2,1,4,3)$, $(1,2,2)(1,2,5,4,3)$
$(2,0,0)(4,1,2,5,3)$, $(2,0,1)(5,4,2,1,3)$, $(2,0,2)(1,5,2,4,3)$
$(2,1,0)(3,1,2,5,4)$, $(2,1,1)(3,4,2,1,5)$, $(2,1,2)(3,5,2,1,4)$
$(2,2,0)(4,3,2,1,5)$, $(2,2,1)(5,3,2,1,4)$, $(2,2,2)(1,3,2,5,4)$.

Listing of the elements $\mathbf{x} \in Z_3^4$ and the corresponding values of $T(\mathbf{x}) \in S_6$

$(0,0,0,0)(2,4,3,1,5,6)$, $(0,0,0,1)(2,4,3,6,1,5)$
$(0,0,0,2)(2,4,3,5,1,6)$, $(0,0,1,0)(2,1,4,6,5,3)$
$(0,0,1,1)(2,1,4,3,6,5)$, $(0,0,1,2)(2,1,4,5,6,3)$
$(0,0,2,0)(2,3,1,6,5,4)$, $(0,0,2,1)(2,3,1,5,6,4)$
$(0,0,2,2)(2,3,1,4,6,5)$, $(0,1,0,0)(2,5,3,1,6,4)$
$(0,1,0,1)(2,4,5,3,1,6)$, $(0,1,0,2)(2,5,3,4,1,6)$
$(0,1,1,0)(2,5,4,1,6,3)$, $(0,1,1,1)(2,5,4,3,1,6)$
$(0,1,1,2)(2,1,5,4,6,3)$, $(0,1,2,0)(2,3,5,1,6,4)$
$(0,1,2,1)(2,5,1,3,6,4)$, $(0,1,2,2)(2,5,1,4,6,3)$
$(0,2,0,0)(2,6,3,1,5,4)$, $(0,2,0,1)(2,4,6,3,1,5)$
$(0,2,0,2)(2,6,3,4,1,5)$, $(0,2,1,0)(2,6,4,1,5,3)$
$(0,2,1,1)(2,6,4,3,1,5)$, $(0,2,1,2)(2,1,6,4,5,3)$
$(0,2,2,0)(2,3,6,1,5,4)$, $(0,2,2,1)(2,6,1,3,5,4)$
$(0,2,2,2)(2,6,1,4,5,3)$, $(1,0,0,0)(1,2,3,5,6,4)$
$(1,0,0,1)(1,2,3,6,5,4)$, $(1,0,0,2)(1,2,3,4,6,5)$
$(1,0,1,0)(3,2,4,1,6,5)$, $(1,0,1,1)(3,2,4,6,1,5)$
$(1,0,1,2)(3,2,4,5,1,6)$, $(1,0,2,0)(4,2,1,5,6,3)$
$(1,0,2,1)(4,2,1,3,6,5)$, $(1,0,2,2)(4,2,1,6,5,3)$
$(1,1,0,0)(6,2,3,1,5,4)$, $(1,1,0,1)(1,2,5,3,6,4)$
$(1,1,0,2)(6,2,3,4,1,5)$, $(1,1,1,0)(3,2,5,1,6,4)$
$(1,1,1,1)(6,2,5,3,1,4)$, $(1,1,1,2)(6,2,5,4,1,3)$
$(1,1,2,0)(4,2,5,1,6,3)$, $(1,1,2,1)(6,2,1,3,5,4)$
$(1,1,2,2)(6,2,1,4,5,3)$, $(1,2,0,0)(5,2,3,1,6,4)$
$(1,2,0,1)(1,2,6,3,5,4)$, $(1,2,0,2)(5,2,3,4,1,6)$
$(1,2,1,0)(5,2,4,1,6,3)$, $(1,2,1,1)(5,2,6,3,1,4)$
$(1,2,1,2)(5,2,6,4,1,3)$, $(1,2,2,0)(4,2,6,1,5,3)$
$(1,2,2,1)(5,2,1,3,6,4)$, $(1,2,2,2)(5,2,1,4,6,3)$
$(2,0,0,0)(1,4,2,5,6,3)$, $(2,0,0,1)(1,4,2,3,6,5)$
$(2,0,0,2)(1,4,2,6,5,3)$, $(2,0,1,0)(3,1,2,5,6,4)$
$(2,0,1,1)(3,1,2,6,5,4)$, $(2,0,1,2)(3,1,2,4,6,5)$
$(2,0,2,0)(4,3,2,1,6,5)$, $(2,0,2,1)(4,3,2,6,1,5)$
$(2,0,2,2)(4,3,2,5,1,6)$, $(2,1,0,0)(6,4,2,1,5,3)$
$(2,1,0,1)(6,4,2,3,1,5)$, $(2,1,0,2)(1,5,2,4,6,3)$
$(2,1,1,0)(3,5,2,1,6,4)$, $(2,1,1,1)(6,1,2,3,5,4)$
$(2,1,1,2)(6,5,2,4,1,3)$, $(2,1,2,0)(6,3,2,1,5,4)$
$(2,1,2,1)(4,5,2,3,1,6)$, $(2,1,2,2)(6,3,2,4,1,5)$
$(2,2,0,0)(5,4,2,1,6,3)$, $(2,2,0,1)(5,4,2,3,1,6)$
$(2,2,0,2)(1,6,2,4,5,3)$, $(2,2,1,0)(3,6,2,1,5,4)$
$(2,2,1,1)(5,1,2,3,6,4)$, $(2,2,1,2)(5,6,2,4,1,3)$
$(2,2,2,0)(5,3,2,1,6,4)$, $(2,2,2,1)(4,6,2,3,1,5)$
$(2,2,2,2)(5,3,2,4,1,6)$

A. Construction of $U \in \mathcal{F}_{6,8}$

Let $\mathbf{x} \in Z_3^6$ and let

$$(\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5) = R(x_1, x_2, x_3)$$
$$(\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5) = S(x_4, x_5, x_6) + (3,3,3,3,3).$$

Define $\rho = (\rho_1, \rho_2, \ldots, \rho_8)$ as follows:

$$\begin{aligned}
&\rho_i = \gamma_5, && \text{if } 1 \le i \le 4 \quad \text{and} \quad \varphi_i = 5\\
&\rho_i = \varphi_i, && \text{if } 1 \le i \le 4 \quad \text{and} \quad \varphi_i \ne 5\\
&\rho_i = \varphi_5, && \text{if } 5 \le i \le 8 \quad \text{and} \quad \gamma_{i-4} = 4\\
&\rho_i = \gamma_{i-4}, && \text{if } 5 \le i \le 8 \quad \text{and} \quad \gamma_{i-4} \ne 4.
\end{aligned}$$

In ρ, swap 1 and 7 and also swap 5 and 8, and let the resulting array be $U(\mathbf{x})$. It has the following properties:

- for every $\mathbf{x} \in Z_3^6$, $7 \in \{U(\mathbf{x})_1, U(\mathbf{x})_2, U(\mathbf{x})_3\}$
- for every $\mathbf{x} \in Z_3^6$, $8 \in \{U(\mathbf{x})_5, U(\mathbf{x})_6, U(\mathbf{x})_7\}$
- for every distinct $\mathbf{x}, \mathbf{y} \in Z_3^6$ $d_H(U(\mathbf{x})_{\setminus\{4,8\}}, U(\mathbf{y})_{\setminus\{4,8\}}) \ge d_H(\mathbf{x}, \mathbf{y})$.

B. Construction of $V \in \mathcal{F}_{7,9}$

Let $\mathbf{x} \in Z_3^7$ and let

$$(\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5) = R(x_1, x_2, x_3)$$
$$(\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6) = T(x_4, x_5, x_6, x_7) + (3,3,\ldots,3).$$

Define $\rho = (\rho_1, \rho_2, \ldots, \rho_9)$ as follows:

$$\begin{aligned}
&\rho_i = \gamma_6, && \text{if } 1 \le i \le 4 \quad \text{and} \quad \varphi_i = 5\\
&\rho_i = \varphi_i, && \text{if } 1 \le i \le 4 \quad \text{and} \quad \varphi_i \ne 5\\
&\rho_i = \varphi_5, && \text{if } 5 \le i \le 9 \quad \text{and} \quad \gamma_{i-4} = 4\\
&\rho_i = \gamma_{i-4}, && \text{if } 5 \le i \le 9 \quad \text{and} \quad \gamma_{i-4} \ne 4.
\end{aligned}$$

In ρ, swap 2 and 5, and let the resulting array be $V(\mathbf{x})$. It has the following properties:

- for every $\mathbf{x} \in Z_3^7$, $1 \in \{V(\mathbf{x})_1, V(\mathbf{x})_2, V(\mathbf{x})_3\}$
- for every $\mathbf{x} \in Z_3^7$, $2 \in \{V(\mathbf{x})_5, V(\mathbf{x})_6, V(\mathbf{x})_7\}$
- for every distinct $\mathbf{x}, \mathbf{y} \in Z_3^7$ $d_H(V(\mathbf{x})_{\setminus\{4,9\}}, V(\mathbf{y})_{\setminus\{4,9\}}) \ge d_H(\mathbf{x}, \mathbf{y})$.

C. Construction of $f \in \mathcal{P}_{13,13}$

Let $\mathbf{x} \in Z_3^{13}$ and let

$$(\varphi_1, \varphi_2, \ldots, \varphi_8) = U(x_1, x_2, \ldots, x_6)$$
$$(\gamma_1, \gamma_2, \ldots, \gamma_9) = V(x_7, x_8, \ldots, x_{13}) + (4,4,\ldots,4).$$

Define $\rho = (\rho_1, \rho_2, \ldots, \rho_{13})$ as follows:

$$\begin{aligned}
&\rho_i = \gamma_4, && \text{if } 1 \le i \le 3 && \text{and} \quad \varphi_i = 7\\
&\rho_i = \varphi_i, && \text{if } 1 \le i \le 3 && \text{and} \quad \varphi_i \ne 7\\
&\rho_i = \gamma_9, && \text{if } 4 \le i \le 6 && \text{and} \quad \varphi_{i+1} = 8\\
&\rho_i = \varphi_{i+1}, && \text{if } 4 \le i \le 6 && \text{and} \quad \varphi_{i+1} \ne 8\\
&\rho_i = \varphi_4, && \text{if } 7 \le i \le 9 && \text{and} \quad \gamma_{i-6} = 5\\
&\rho_i = \gamma_{i-6}, && \text{if } 7 \le i \le 9 && \text{and} \quad \gamma_{i-6} \ne 5\\
&\rho_i = \varphi_8, && \text{if } 10 \le i \le 13 && \text{and} \quad \gamma_{i-5} = 6\\
&\rho_i = \gamma_{i-5}, && \text{if } 10 \le i \le 13 && \text{and} \quad \gamma_{i-5} \ne 6.
\end{aligned}$$

In ρ, swap 1 and 9 and also swap 2 and 10, and let the resulting array be $f(\mathbf{x})$. Then

$$f \in \mathcal{P}_{13,13} \text{ and } f(\mathbf{x})_{13} \notin \{9, 10\}.$$

VI. Conclusion

We have given a recursive construction method for DPMs and DIMs from ternary vectors. In three cases we have found DPMs that can be used to start off the recursion, in one of the cases the DPMs are DIMs. Hence, in one case we get an infinite class of DIMs and in the other

two cases we get infinite classes of DPM. The most important result is the construction of DPM from ternary vectors of lengths at least 13 to permutations of the same length. Using the DPMs (or the DIMs) and known ternary codes, we get new larger permutation arrays in many cases; a couple of examples are gives as illustrations.

REFERENCES

[1] A. E. Brouwer, H. O. Hämäläinen, P. R. J. Östergård, and N. J. A. Sloane, "Bounds on mixed binary/ternary codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 140–161, Jan. 1998.

[2] J.-C. Chang, "Distance-increasing mappings from binary vectors to permutations," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 359–363, Jan. 2005.

[3] J.-C. Chang, "New algorithms of distance-increasing mappings from binary vectors to permutations by swaps," *Designs, Codes Cryptogr.*, vol. 39, pp. 335–345, Jan. 2006.

[4] J.-C. Chang, "Distance-increasing mappings from binary vectors to permutations that increase Hamming distances by at least two," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1683–1689, Apr. 2006.

[5] J.-C. Chang, R.-J. Chen, T. Kløve, and S.-C. Tsai, "Distance-preserving mappings from binary vectors to permutations," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 1054–1059, Apr. 2003.

[6] H. C. Ferreira and A. J. H. Vinck, "Inference cancellation with permutation trellis arrays," in *Proc. IEEE Veh. Technol. Conf.*, 2000, pp. 2401–2407.

[7] H. C. Ferreira, A. J. H. Vinck, T. G. Swart, and I. de Beer, "Permutation trellis codes," *IEEE Trans. Commun.*, vol. 53, no. 11, pp. 1782–1789, Nov. 2005.

[8] H. C. Ferreira, D. Wright, and A. L. Nel, "Hamming distance-preserving mappings and trellis codes with constrained binary symbols," *IEEE Trans. Inf. Theory*, vol. 35, no. 5, pp. 1098–1103, Sep. 1989.

[9] Y.-Y. Huang, S.-C. Tsai, and H.-L. Wu, "On the construction of permutation arrays via mappings from binary vectors to permutations," *Designs, Codes Cryptogr.*, vol. 40, pp. 139–155, 2006.

[10] K. Lee, "New distance-preserving maps of odd length," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2539–2543, Oct. 2004.

[11] K. Lee, "Cyclic constructions of distance-preserving maps," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4292–4396, Dec. 2005.

[12] K. Lee, "Distance-increasing maps of all length by simple mapping algorithms," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3344–3348, Jul. 2006.

[13] J.-S. Lin, J.-C. Chang, and R.-J. Chen, "New simple constructions of distance-increasing mappings from binary vectors to permutations," *Inf. Process. Lett.*, vol. 100, no. 2, pp. 83–89, Oct. 2006.

[14] J.-S. Lin, J.-C. Chang, R.-J. Chen, and T. Kløve, Distance-Preserving Mappings from Ternary Vectors to Permutations arXiv, 0704.1358v1 [cs.DM].

[15] T.-T. Lin, S.-C. Tsai, and H.-L. Wu, "Distance-preserving mappings from ternary vectors to permutations," *Manuscript*, 2007.

[16] V. S. Pless and W. C. Huffman, Eds., *Handbook of Coding Theory*. Amsterdam, The Netherlands: Elsevier, 1998.

[17] T. G. Swart and H. C. Ferreira, "A generalized upper bound and a multi-level construction for distance-preserving mappings," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3685–3695, Aug. 2006.

Complete Mutually Orthogonal Golay Complementary Sets From Reed–Muller Codes

Appuswamy Rathinakumar, *Student Member, IEEE*, and Ajit Kumar Chaturvedi, *Senior Member, IEEE*

***Abstract*—Recently Golay complementary sets were shown to exist in the subsets of second-order cosets of a q-ary generalization of the first-order Reed–Muller (RM) code. We show that mutually orthogonal Golay complementary sets can also be directly constructed from second-order cosets of a q-ary generalization of the first-order *RM* code. This identification can be used to construct zero correlation zone (ZCZ) sequences directly and it also enables the construction of ZCZ sequences with special subsets.**

***Index Terms*—Complementary sets, generalized Boolean function, mutually orthogonal Golay complementary sets, Reed–Muller (RM) codes, zero correlation zone (ZCZ) sequences.**

I. INTRODUCTION

Zero correlation zone (ZCZ) sequences are a generalization of orthogonal sequences. Their superior correlation properties can be utilized to improve the spectral efficiency of an approximately synchronized[1] CDMA system over a similar system that uses conventional orthogonal sequences [3]. Further, CDMA systems employing ZCZ sequences have been shown to be performing as well as OFDM systems in fast time-varying multipath channels at a considerably lower computational complexity [14]. Recently, ZCZ sequences have found applications in ternary direct sequence Ultra Wideband (TS-UWB) systems [13]. It has been shown that the TS-UWB (also known as multicode UWB) systems employing appropriate ZCZ sequences can support different data rate requirements at a constant bit error rate performance level [13]. They are also applicable in broadband satellite IP networks, where sequence sets with small autocorrelation and cross correlation within a detection aperture are needed [15], [16].

Mutually orthogonal Golay Complementary Sets (MOGCS) are an integral part in the construction of ZCZ sequences. Traditionally, ZCZ sequences have been constructed by iterative methods starting from a pair of MOGCS. In [3], several constructions of ZCZ sequences starting from any set of MOGCS were given. Many recursive constructions of MOGCS are known [9],[2] [3], [6], [7], [5], [3]. In [1] and [2], a long standing problem of directly constructing Golay Complementary Sets (GCS) [6] was solved by constructing GCS from Reed–Muller (RM) codes. Specifically, GCS were shown to be subsets in second-order cosets of a q-ary generalization $\mathrm{RM}_q(1, m)$ of the first-order RM code. Size of the set was shown to be directly related to a graph associated with the coset leader.

Manuscript received July 28, 2004; revised November 29, 2007.

A. Rathinakumar was with the Department of Electrical Engineering, Indian Institute of Technology, Kanpur, UP 208016, India. He is now with the Department of Electrical and Computer Engineering, University of California, San Diego, La Jolla, CA 92093 USA (e-mail: rathnam@ucsd.edu).

A. K. Chaturvedi is with the Department of Electrical Engineering, Indian Institute of Technology, Kanpur, UP 208016, India (e-mail: akc@iitk.ac.in).

Communicated by K. G. Paterson, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2007.915980

[1] A DS CDMA system is said to be approximately synchronized if the modulated sequences are synchronized up to a small fraction of the sequence length.

[2] The concept of zero correlation sequences first appears in [9] as semiperfect sequences.