Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Information Processing Letters 100 (2006) 83–89

Information Processing Letters

www.elsevier.com/locate/ipl

New simple constructions of distance-increasing mappings from binary vectors to permutations

Jyh-Shyan Lin [a], Jen-Chun Chang [b], Rong-Jaye Chen [a,*]

[a] Department of Computer Science and Information Engineering, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu, 300 Taiwan
[b] Department of Computer Science and Information Engineering, National Taipei University, San-Sia, Taipei County, 237 Taiwan

Received 27 May 2005; received in revised form 9 August 2005; accepted 14 September 2005

Available online 11 July 2006

Communicated by W.-L. Hsu

Abstract

Distance-increasing mappings (DIMs) are mappings from the set of binary vectors of a fixed length to the set of permutations of the same length that increase Hamming distances except when that is obviously not possible. In this paper, we propose new non-recursive constructions of DIMs which are based on simple compositions of permutations. In comparison with Chang's constructions, our new constructions do not need any table-lookup operations, and usually have better distance expansion distributions when the length is odd.

Keywords: Combinatorial problems; Distance-preserving mappings; Distance-increasing mappings; Permutation arrays; Hamming distance

1. Introduction

A mapping from the set of all binary vectors of length n to the set of all permutations of $Z_n = \{1, 2, \ldots, n\}$ is called a distance-preserving mapping (DPM) if every two binary vectors are mapped to permutations with the same or even larger Hamming distance than that of the binary vectors. A distance-increasing mapping (DIM) is a special DPM such that the distances of mapped permutations are strictly increased except when that is obviously not possible [10]. DPMs and DIMs are themselves interesting combinatorial objects and can be used to construct permutation arrays (PAs) which are applied to various applications, such as trellis code modulations and power line communications [1–7]. Recently, several constructions of DPMs and DIMs were proposed [8–10], in which these mappings were not only applied to construct new PAs but also used to improve the lower bound on the size of PAs.

The DIMs proposed by Chang were constructed based on a small table which was obtained by a customized computer search program [10]. In this paper, we propose new constructions of DIMs that do not need any table-lookup operations. These constructions are based on simple compositions of permutations; the new DIMs constructed usually have better distance expansion distributions than Chang's when the length is odd.

* Corresponding author.
E-mail addresses: linch@csie.nctu.edu.tw (J.-S. Lin), jcchang@mail.ntpu.edu.tw (J.-C. Chang), rjchen@csie.nctu.edu.tw (R.-J. Chen).

0020-0190/$ – see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.ipl.2005.09.019

2. Definitions and notations

Let Z_2^n denote the set of all binary vectors of length n. The Hamming distance between two vectors $\boldsymbol{a} = (a_1, a_2, \dots, a_n)$ and $\boldsymbol{b} = (b_1, b_2, \dots, b_n)$ is denoted by $d(\boldsymbol{a}, \boldsymbol{b})$ and is defined as

$$d(\boldsymbol{a}, \boldsymbol{b}) = \bigl|\{j \in Z_n\colon a_j \neq b_j\}\bigr|.$$

Let S_n denote the set of all $n!$ permutations of $Z_n = \{1, 2, \dots, n\}$. A permutation $\pi : Z_n \to Z_n$ can be represented by

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi_1 & \pi_2 & \cdots & \pi_n \end{pmatrix},$$

i.e., $\pi(i) = \pi_i$. This representation is called the *standard form*. For simplicity, we represent π in the *vector form*, $\pi = (\pi_1, \pi_2, \dots, \pi_n)$.

Definition 1. A mapping $f : Z_2^n \to S_n$ is called a distance-increasing mapping of length n (n-DIM) if for any two distinct binary vectors $x, y \in Z_2^n$,

$$d\bigl(f(x), f(y)\bigr) \geqslant \min\bigl\{d(x, y) + 1, n\bigr\}.$$

Definition 2. Let ρ and μ be two permutations on Z_n, the composition operation $\rho \circ \mu$ is defined as

$$\rho \circ \mu(x) = \rho\bigl(\mu(x)\bigr).$$

For example,

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} \quad \text{and}$$

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}.$$

Then

$$\rho \circ \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}.$$

For simplicity, we write $\rho \circ \mu = \rho\mu$. Note that permutation composition is not commutative. We denote $\iota = (1, 2, \dots, n)$ and for a permutation ρ on Z_n, define $\rho^0 = \iota$.

Definition 3. A set of permutations is called a *commutative set* if any two permutations ρ and μ in the set commute, that is, $\rho\mu = \mu\rho$.

Let $\langle \rho_1, \rho_2, \dots, \rho_n \rangle$ be an ordered set of permutations in S_n. For $J \subseteq Z_n$, we define

$$\prod_{j \in J} \rho_j = \rho_{j_1} \circ \rho_{j_2} \circ \cdots \circ \rho_{j_k},$$

where $J = \{j_1, j_2, \dots, j_k\}$, k is a positive integer and $j_1 < j_2 < \cdots < j_k$.

Let $B_f = \langle \rho_1, \rho_2, \dots, \rho_n \rangle$ be an ordered set of permutations in S_n. We define a mapping from Z_2^n to S_n as

$$f(x_1, x_2, \dots, x_n) = \rho_1^{x_1} \circ \rho_2^{x_2} \circ \cdots \circ \rho_n^{x_n} = \prod_{j \in J_x} \rho_j, \tag{1}$$

where $J_x = \{j \mid x_j = 1, 1 \leqslant j \leqslant n\}$. B_f is called the *basic construction set* of f.

3. The new DIMs

In this section, we first prove two lemmas that are important for the construction of the new DIMs. The constructions of n-DIM for even or odd n are then described separately.

Lemma 1. *Let f be a mapping constructed by* (1) *using the basic construction set $B_f = \langle \rho_1, \rho_2, \dots, \rho_n \rangle$. Then f is an n-*DIM *if for any two distinct subset J_1 and J_2 of Z_n,*

$$d\Bigl(\prod_{j \in J_1} \rho_j, \prod_{j \in J_2} \rho_j\Bigr) > |J_1 \oplus J_2| \quad \text{when } |J_1 \oplus J_2| < n, \text{ and} \tag{2}$$

$$d\Bigl(\prod_{j \in J_1} \rho_j, \prod_{j \in J_2} \rho_j\Bigr) = |J_1 \oplus J_2| \quad \text{when } |J_1 \oplus J_2| = n, \tag{3}$$

where $J_1 \oplus J_2$ is the symmetric difference of J_1 and J_2, i.e., $J_1 \oplus J_2 = (J_1 \cup J_2) - (J_1 \cap J_2)$.

Proof. For any two distinct vectors $\boldsymbol{a}, \boldsymbol{b} \in Z_2^n$. Let $\boldsymbol{a} = (a_1, a_2, \dots, a_n)$, $\boldsymbol{b} = (b_1, b_2, \dots, b_n)$, $J_1 = \{j \mid a_i = 1, 1 \leqslant j \leqslant n\}$, and $J_2 = \{j \mid b_i = 1, 1 \leqslant j \leqslant n\}$. Then $d(\boldsymbol{a}, \boldsymbol{b}) = |J_1 \oplus J_2|$ and

$$f(a) = \prod_{j \in J_1} \rho_j, \qquad f(b) = \prod_{j \in J_2} \rho_j.$$

It is clear that f is an n-DIM if (2) and (3) are true. □

Lemma 1 states the criteria that the basic construction set of a DIM should meet. However, we must consider $\binom{2^n}{2}$ combinations of any two distinct subsets of B_f. Under some conditions, Lemma 2 considers only 2^n subsets of B_f.

Lemma 2. *Let $B_f = \langle \rho_1, \rho_2, \ldots, \rho_n \rangle$ be the basic construction set of f and assume that $\{\rho_1, \ldots, \rho_{\lfloor n/2 \rfloor}\}$ and $\{\rho_{\lfloor n/2 \rfloor+1}, \ldots, \rho_n\}$ are commutative sets. Besides, all permutations in B_f are self-inverse, i.e., $\rho_i^2 = \iota$ for all $\rho_i \in B_f$. Then f is an n-DIM if for any subset $J \subseteq Z_n$,*

$$d\left(\prod_{j\in J} \rho_j, \iota\right) > |J| \quad \text{when } |J| < n, \text{ and} \tag{4}$$

$$d\left(\prod_{j\in J} \rho_j, \iota\right) = |J| \quad \text{when } |J| = n. \tag{5}$$

Proof. For any two subsets $J_1, J_2 \subseteq Z_n$, let $J = J_1 \oplus J_2 \subseteq Z_n$. Using the properties of commutativity and self-inversion, we have

$$d\left(\prod_{j\in J_1} \rho_j, \prod_{j\in J_2} \rho_j\right) = d\left(\prod_{j\in J_1 \oplus J_2} \rho_j, \iota\right).$$

For example, let $n = 4$, $J_1 = \{\rho_2, \rho_3, \rho_4\}$, and $J_2 = \{\rho_1, \rho_3\}$. Then

$$\begin{aligned} d\left(\prod_{j\in J_1} \rho_j, \prod_{j\in J_2} \rho_j\right) &= d(\rho_2\rho_3\rho_4, \rho_1\rho_3) \\ &= d(\rho_1\rho_2\rho_3\rho_4\rho_3, \rho_1\rho_1\rho_3\rho_3) \\ &= d(\rho_1\rho_2\rho_3\rho_3\rho_4, \iota) = d(\rho_1\rho_2\rho_4, \iota) \\ &= d\left(\prod_{j\in J_1\oplus J_2} \rho_j, \iota\right). \end{aligned}$$

Thus, according to Lemma 1, f is an n-DIM if the statement is true. □

According to Lemma 2, we can construct an n-DIM for even n as follows.

Construction 1. Let $n = 2m, m \geqslant 2$, construct a mapping f_n using the following basic construction set

$$\begin{aligned} B_{f_n} = \big\langle\, &\rho_1 = (2, 1, 3, 4, \ldots, n), \\ &\rho_2 = (1, 2, 4, 3, 5, 6, \ldots, n), \\ &\vdots \\ &\rho_m = (1, 2, \ldots, n-2, n, n-1), \\ &\rho_{m+1} = (1, 3, 2, 4, \ldots, n), \\ &\rho_{m+2} = (1, 2, 3, 5, 4, 6, \ldots, n), \\ &\vdots \\ &\rho_n = (n, 2, \ldots, n-1, 1)\big\rangle. \end{aligned}$$

Theorem 1. *The mapping f_n constructed by Construction 1 is an n-DIM for even n.*

Proof. It is clear that both $\langle \rho_1, \rho_2, \ldots, \rho_m \rangle$ and $\langle \rho_{m+1}, \rho_{m+2}, \ldots, \rho_n \rangle$ are commutative and all permutations in B_{f_n} are self-inverse. Thus, it suffices to prove that (4) and (5) are true for any subset $J \subseteq Z_n$.

First we notice that $d(\rho_i, \iota) = 2$ for all $\rho_i \in B_{f_n}$. Furthermore, for any two distinct permutations $\rho_i, \rho_j \in B_{f_n}$, $d(\rho_i\rho_j, \iota) = 4$ if ρ_i and ρ_j commute, and $d(\rho_i\rho_j, \iota) = 3$ if ρ_i and ρ_j do not commute. Thus, we can define a function $I : B_{f_n} \times B_{f_n} \to Z$ as

$$I(\rho_i, \rho_j) = \begin{cases} 0 & \text{if } \rho_i \text{ and } \rho_j \text{ commute,} \\ 1 & \text{otherwise,} \end{cases}$$

and write $d(\rho_i\rho_j, \iota) = 4 - I(\rho_i, \rho_j)$. This formula can be extended to

$$d\left(\prod_{j\in J} \rho_j, \iota\right) = 2|J| - \sum_{i,j\in J, i\neq j} I(\rho_i, \rho_j). \tag{6}$$

Now let

$$B_1 = \langle \rho_j \mid j \in J \text{ and } 1 \leqslant j \leqslant m \rangle \subseteq B_{f_n},$$
$$B_2 = \langle \rho_j \mid j \in J \text{ and } m+1 \leqslant j \leqslant n \rangle \subseteq B_{f_n},$$

(6) can be rewritten as

$$d\left(\prod_{j\in J} \rho_j, \iota\right) = 2|B_1| + 2|B_2| - \sum_{\rho_i\in B_1} \sum_{\rho_j\in B_2} I(\rho_i, \rho_j). \tag{7}$$

For a permutation $\rho_i \in B_1$, there are at most two permutations in B_2 not commuting with ρ_i. Similarly, each permutation in B_2 does not commute with at most two permutations in B_1. Consider the following possible cases.

Case 1: $|B_1| \neq |B_2|$. We have

$$\sum_{\rho_i\in B_1} \sum_{\rho_j\in B_2} I(\rho_i, \rho_j) \leqslant 2 \times \min\big\{|B_1|, |B_2|\big\}.$$

Thus

$$\begin{aligned} d\left(\prod_{j\in J} \rho_j, \iota\right) &\geqslant 2 \times \max\big\{|B_1|, |B_2|\big\} \\ &> |B_1| + |B_2| = |J|. \end{aligned}$$

Case 2: $|B_1| = |B_2|$ and $|J| < n$. At least one permutation in B_2 does not commute with at most one permutation in B_1, or else $|J| = n$. Thus,

$$d\left(\prod_{j\in J} \rho_j, \iota\right) > 2|B_1| = |J|.$$

Case 3: $|B_1|=|B_2|$ and $|J|=n$. Each permutation in B_1 (B_2) does not commute with exactly two permutations in B_2 (B_1). Thus,

$$d\left(\prod_{j\in J}\rho_j,\iota\right)=2|B_1|=|J|.$$

For any subset $J\subseteq Z_n$, Cases 1 and 2 show that (4) is true and Case 3 shows that (5) is true. Thus, f_n is an n-DIM. □

The n-DIM for even n proposed here is similar to the mapping h_{2m}, a $2m$-DIM ($n=2m$) for $m=2$ or $m>2$ and odd, as proposed in [8]. Although h_{2m} is described by an algorithm there, it can be described as the mapping corresponding to the basic construction set $B_{h_{2m}}=\langle\mu_1,\mu_2,\ldots,\mu_{2m}\rangle$ where

$$\mu_i=(1,2,\ldots,2i-2,2i,2i-1,2i+2,\ldots,2m)$$

and

$$\mu_{m+i}=(1,2,\ldots,i-1,m+i,i+1,\ldots,m+i-1,\\ i,m+i+1,\ldots,2m)$$

for $i=1,2,\ldots,m$. Note that $\rho_i=\mu_i$ for $1\leqslant i\leqslant m$, but $\rho_i\neq\mu_i$ for $m+1\leqslant i\leqslant 2m$.

We cannot construct an n-DIM for odd n in the same way as Construction 1 because it is infeasible to find two commutative sets which form a basic construction set. In the following, we develop a construction method for odd n.

Lemma 3. *Let $n=2m+1, m\geqslant 2$, f_n be a mapping constructed by using the following basic construction set*

$$\begin{aligned}B_{f_n}=\big\langle\,&\rho_1=(2,1,3,4,\ldots,n),\\ &\rho_2=(1,2,4,3,5,6,\ldots,n),\\ &\vdots\\ &\rho_m=(1,2,\ldots,n-3,n-1,n-2,n),\\ &\rho_{m+1}=(\pi_1,\pi_2,\ldots,\pi_n),\\ &\rho_{m+2}=(1,3,2,4,\ldots,n),\\ &\rho_{m+3}=(1,2,3,5,4,6,\ldots,n),\\ &\vdots\\ &\rho_n=(1,2,\ldots,n-2,n,n-1)\big\rangle.\end{aligned}$$

Let $U=\{\{\pi_2,\pi_3\},\{\pi_4,\pi_5\},\ldots,\{\pi_{n-1},\pi_n\}\}$, $V=\{\{1,2\},ak\{3,4\},\ldots,\{n-2,n-1\}\}$. For 1$\leqslant k\leqslant(n-1)/2$, let $u_1,\ldots,u_k$ be any k distinct elements of U, and $v_1,\ldots,v_k$ be any k distinct elements of V. If $\bigcup_{i=1}^k u_i\neq\bigcup_{i=1}^k v_i$, then for any subset $J\subseteq Z_n\backslash\{m+1\}$,

$$d\left(\prod_{j\in J\cup\{m+1\}}\rho_j,\rho_{m+1}\right)>|J|.\tag{8}$$

Proof. Let $J_1=\{j\mid j\in J$ and $1\leqslant j\leqslant m\}$, $J_2=\{j\mid j\in J$ and $m+2\leqslant j\leqslant n\}$, $B_1=\langle\rho_j\mid j\in J_1\rangle$, and $B_2=\langle\rho_j\mid j\in J_2\rangle$, $B_1,B_2\subseteq B_{f_n}$. B_1 is commutative, and so is B_2. Let $|B_2|=k, 0\leqslant k\leqslant(n-1)/2$. Consider the permutation$\mu=\rho_{m+1}\prod_{j\in J_2}\rho_j$, we know that $d(\mu,\rho_{m+1})=2k$. Let $P=\{\pi_i\mid\mu(i)\neq\pi_i\}$. For a permutation $\rho_c\in B_1, 1\leqslant c\leqslant m$, we have

$$d(\rho_c\mu,\rho_{m+1})\\ =\begin{cases}2k, & \text{if } 2c-1\in P \text{ and } 2c\in P\\ & \quad\text{(the distance never decreased)},\\ 2k+1, & \text{if either } 2c-1\in P \text{ or } 2c\in P\\ & \quad\text{but not both},\\ 2k+2, & \text{if } 2c-1\notin P \text{ and } 2c\notin P.\end{cases}$$

The following shows that (8) is true in all possible cases.

Case 1: $|B_1|\neq|B_2|$.

$$d\left(\prod_{j\in J\cup\{m+1\}}\rho_j,\rho_{m+1}\right)\geqslant 2\times\max\big\{|B_1|,|B_2|\big\}\\ >|B_1|+|B_2|=|J|.$$

Case 2: $|B_1|=|B_2|$. Since the union of any k distinct element of U is not equal to the union of any k distinct element of V. We have

$$d\left(\prod_{j\in J\cup\{m+1\}}\rho_j,\rho_{m+1}\right)>2\times\mid B_1|=|J|.\qquad\square$$

Lemma 4. *Let $n=2m+1, m\geqslant 2$, f be a mapping constructed by using the basic construction set B_f in Lemma 3. Then f is an n-DIM if the following statements are true.*

(i) $d(\prod_{j\in Z_n\backslash\{m+1\}}\rho_j,\rho_{m+1})=n$.

(ii) *For each $i\in Z_n\backslash\{m+1\}$,*

$$d\left(\prod_{j\in Z_n\backslash\{i,m+1\}}\rho_j,\rho_{m+1}\right)=n.$$

(iii) *Let $U=\{\{\pi_2,\pi_3\},\{\pi_4,\pi_5\},\ldots,\{\pi_{n-1},\pi_n\}\}$, $V=\{\{1,2\},\{3,4\},\ldots,\{n-2,n-1\}\}$. For 1$\leqslant k\leqslant(n-1)/2$, let $u_1,\ldots,u_k$ be any k distinct elements of U, and $v_1,\ldots,v_k$ be any k distinct elements of V, $\bigcup_{i=1}^k u_i\neq\bigcup_{i=1}^k v_i$.*

Proof. First, (i) implies that (3) in Lemma 1 is true. Second, for any two distinct subsets $J_1, J_2 \subseteq Z_n$, there are three possible cases:

(1) Neither J_1 nor J_2 contains $m+1$.
(2) Either J_1 or J_2 but not both contains $m+1$.
(3) Both J_1 and J_2 contain $m+1$.

No matter in which case, we show that (2) in Lemma 1 is always true.

Case 1: $m+1 \notin J_1$ and $m+1 \notin J_2$. This case is basically the same situation as in Theorem 1 above. Thus

$$d\Bigl(\prod_{j\in J_1}\rho_j, \prod_{j\in J_2}\rho_j\Bigr) = d\Bigl(\prod_{j\in J_1\oplus J_2}\rho_j, \iota\Bigr) > |J_1 \oplus J_2|.$$

Case 2: Without loss of generality, assume $m+1 \in J_1$ and $m+1 \notin J_2$. We prove (2) by induction on the size of $J_1 \oplus J_2$. The base step is stated in (ii) for $|J_1 \oplus J_2| = n-1$. Now assume (2) is true for $|J_1 \oplus J_2| = k+1$ but is not true for $|J_1 \oplus J_2| = k$. That is,

$$d\Bigl(\prod_{j\in J_1\oplus J_2}\rho_j, \iota\Bigr) \leqslant k \quad \text{for some } |J_1 \oplus J_2| = k.$$

However, the only possibility for this assumption is $d(\prod_{j\in J_1\oplus J_2}\rho_j, \iota) = k$ because according to the hypothesis, $d(\prod_{j\in J_1\oplus J_2\cup\{i\}}\rho_j, \iota) > k+1$ for all $i \in Z_n - (J_1 \oplus J_2)$, and ρ_i is a swap operation that changes exactly two positions (note that $m+1 \in J_1 \oplus J_2$). Thus, $\prod_{j\in J_1\oplus J_2}\rho_j$ agrees with ι in $n-k$ positions, and each permutation ρ_i such that $i \in Z_n - (J_1 \oplus J_2)$ changes exactly two of these positions to make $d(\prod_{j\in J_1\oplus J_2\cup\{i\}}\rho_j, \iota) = k+2$. There are totally $n-k$ permutations each corresponding to an element of $Z_n - (J_1 \oplus J_2)$. By the same logic as in Lemma 3, it is not possible for those $n-k$ permutations, which consist of two commutative sets and one of them is of size $\geqslant \lceil (n-k)/2 \rceil$, that change only $n-k$ positions, a contradiction! Thus, we have $d(\prod_{j\in J_1\oplus J_2}\rho_j, \iota) > k$ for $|J_1 \oplus J_2| = k$.

Case 3: $m+1 \in J_1$ and $m+1 \in J_2$. According to Lemma 3, we have

$$d\Bigl(\prod_{j\in J_1}\rho_j, \prod_{j\in J_2}\rho_j\Bigr) = d\Bigl(\prod_{j\in J_1\oplus J_2\cup\{m+1\}}\rho_j, \rho_{m+1}\Bigr) > |J_1 \oplus J_2|. \qquad \square$$

So if we can find ρ_{m+1} satisfying (i)–(iii), then we have an n-DIM for odd n.

Table 1

	π_1	π_2	π_3	π_4	π_5	π_6	π_7
1	×	×	×				
2	×		×				
3		×		×	×		
4		×	×		×		
5				×		×	×
6				×	×		×
7	×					×	×

Example 1. ($n = 5$) Assume $f_5 : Z_2^5 \to S_5$ is constructed using the following basic construction set

$$\begin{aligned} B_{f_5} = \langle\, & \rho_1 = (2,1,3,4,5),\\ & \rho_2 = (1,2,4,3,5),\\ & \rho_3 = (\pi_1,\pi_2,\pi_3,\pi_4,\pi_5),\\ & \rho_4 = (1,3,2,4,5),\\ & \rho_5 = (1,2,3,5,4)\rangle. \end{aligned}$$

To make f_5 a 5-DIM, the following requirements should be satisfied:

(i) $d(\rho_1\rho_2\rho_4\rho_5, \rho_3) = 5$.
(ii) $d(\rho_2\rho_4\rho_5, \rho_3) = 5$, $d(\rho_1\rho_4\rho_5, \rho_3) = 5$, $d(\rho_1\rho_2\rho_4, \rho_3) = 5$, and $d(\rho_1\rho_2\rho_5, \rho_3) = 5$.
(iii) $\{\pi_2, \pi_3\}, \{\pi_4, \pi_5\} \notin \{\{1,2\}, \{3,4\}\}$ and $\{\pi_2, \pi_3, \pi_4, \pi_5\} \neq \{1,2,3,4\}$.

Since $\rho_1\rho_2\rho_4\rho_5 = (2,4,1,5,3)$, $\rho_2\rho_4\rho_5 = (1,4,2,5,3)$, $\rho_1\rho_4\rho_5 = (2,3,1,5,4)$, $\rho_1\rho_2\rho_5 = (2,1,4,5,3)$, and $\rho_1\rho_2\rho_4 = (2,4,1,3,5)$, we have $\pi_1 \notin \{1,2\}$, $\pi_2 \notin \{1,3,4\}$, $\pi_3 \notin \{1,2,4\}$, $\pi_4 \notin \{3,5\}$, and $\pi_5 \notin \{3,4,5\}$. Furthermore, from (iii) we have $\pi_1 \neq 5$. According to these restrictions and the rules stated in (iii), the only solution for ρ_3 is $(3,2,5,4,1)$.

Example 2. ($n = 7$) Assume $f_7 : Z_2^7 \to S_7$ is constructed using the basic construction set described in Lemma 3. Based on the requirements depicted in Lemma 4, we exclude some values for ρ_4 in the same way as Example 1. The excluded values are summarized in Table 1.

In the table the marks "×" denote the values that should be excluded. Besides, the selection of the values should satisfy the condition (iii) in Lemma 4. There are many solutions for ρ_4(totally 68). In order to make the distance expansion distribution as good as possible, we can choose a solution such that $d(\rho_4, \iota)$ is the largest among all possible solutions, for example, $(5,6,3,7,1,2,4)$.

Table 2

	π_1	π_2	π_3	π_4	π_5	π_6	π_7	$\cdots$	π_{n-1}	π_n
1	×	×	×		○					
2	×		×			○				
3		×		×	×		○			
4		×	×		×					
$\vdots$								$\ddots$		
$n-4$										○
$n-3$			○							
$n-2$		○							×	×
$n-1$	○									×
n	×			○					×	×

Now we give a general construction of n-DIM for odd n below.

Construction 2. Let $n = 2m + 1, m \geqslant 2$, construct a mapping f_n using the basic construction set described in Lemma 3, and

$$\rho_{m+1} = \begin{cases} (3, 2, 5, 4, 1), & \text{if } n = 5, \\ (5, 6, 3, 7, 1, 2, 4), & \text{if } n = 7, \\ (n-1, n-2, n-3, n, 1, 2, \ldots, n-4), & \\ & n \geqslant 9. \end{cases}$$

Theorem 2. *The mapping f_n constructed by Construction* 2 *is an n*-DIM *for odd n.*

Proof. It has been shown that f_5 and f_7 are DIMs from the above examples. For $n \geqslant 9$, like the constructions of f_5 and f_7, we exclude some values for ρ_{m+1} as follows:

$$\pi_1 \notin \{1, 2, n\},$$
$$\pi_{n-1} \notin \{n-2, n\},$$
$$\pi_n \notin \{n-2, n-1, n\},$$
$$\pi_{2i} \notin \{2i-1, 2i+1, 2i+2\}, \quad \text{and}$$
$$\pi_{2i+1} \notin \{2i-1, 2i, 2i+2\}$$

for $i = 1, 2, \ldots, (n-3)/2$. The excluded values and the values selected for ρ_{m+1} are summarized in Table 2 where the marks "×" denote the values excluded and the marks "○" denote the values selected. It can be checked that ρ_{m+1} satisfies (iii) in Lemma 4. □

4. Comparisons

In this section, we compare our DIMs f_n with Chang's DIMs r_n [10, Construction 2]. First, an advantage of our constructions is that it can do without table-lookup operations. Second, we compare the distance expansion distribution of f_n and r_n. Let $D_n = [d_{ij}]_{n \times n}$ be an n by n matrix in which d_{ij} is the number of unordered pairs $\{x, y\}$ in Z_2^n such that $d(x, y) = i$ and $d(f(x), f(y)) = j$. The comparison is made for $n = 5, 7, 8, 9$ because those D_n were presented in [10]. We find that the distance expansion distribution of f_n is better than r_n when n is odd, except for $n = 5$, where r_5 is obtained by a computer search program.

Case n = 5.

0	49	8	10	13
	0	68	68	24
		0	93	67
			0	80
				16

r_5

0	64	16	0	0
	0	48	112	0
		0	64	96
			0	80
				16

f_5

Case n = 7.

0	384	64	0	0	0	0
	0	320	896	128	0	0
		0	256	1408	512	64
			0	320	1344	576
				0	384	960
					0	448
						64

r_7

0	384	0	0	0	64	0
	0	320	640	0	256	128
		0	256	768	640	576
			0	192	832	1216
				0	192	1152
					0	448
						64

f_7

Case n = 8.

0	680	120	112	104	8	0	0
	0	576	1704	744	336	216	8
		0	568	2856	2552	936	256
			0	528	3960	3456	1016
				0	744	3920	2504
					0	944	2640
						0	1024
							128

r_8

0	1024	0	0	0	0	0	0
	0	1024	2560	0	0	0	0
		0	1024	4096	2048	0	0
			0	1024	4608	3072	256
				0	1024	4096	2048
					0	1024	2560
						0	1024
							128

f_8

Case $n = 9$.

0	2048	256	0	0	0	0	0	0
	0	1792	6400	1024	0	0	0	0
		0	1536	10240	8704	1024	0	0
			0	1536	11776	15360	3328	256
				0	1536	12544	14848	3328
					0	1792	11008	8704
						0	2048	7168
							0	2304
								256

r_9

0	2048	0	0	0	0	0	0	256
	0	1792	5376	0	0	0	0	2048
		0	1536	7680	5120	0	0	7168
			0	1280	7680	7680	1280	14336
				0	1024	6144	6144	18944
					0	768	3840	16896
						0	512	8704
							0	2304
								256

f_9

5. Conclusion

In this paper, we have proposed new simple and non-recursive constructions of distance-increasing mappings (DIMs) and these constructions are applied for both even and odd lengths. The constructions take only compositions of permutations and no table-lookups are needed. As the numerical results in Section 4 show, for odd length, our new DIMs have sound distance expansion distributions.

References

[1] C. Ding, F.-W. Fu, T. Kløve, V.K. Wei, Constructions of permutation arrays, IEEE Trans. Inform. Theory 48 (2002) 977–980.

[2] H.C. Ferreira, A.J.H. Vinck, Inference cancellation with permutation trellis arrays, in: Proc. IEEE Vehicular Technology Conf., 2000, pp. 2401–2407.

[3] F.-W. Fu, T. Kløve, Two constructions of permutation arrays, IEEE Trans. Inform. Theory 50 (2004) 881–883.

[4] T. Kløve, Classification of permutation codes of length 6 and minimum distance 5, in: Proc. Internat. Symp. Information Theory and its Applications, 2000, pp. 465–468.

[5] A.J.H. Vinck, J. Häring, Coding and modulation for power-line communications, in: Proc. Internat. Symp. Power Line Communication, Limerick, Ireland, April 5–7, 2000.

[6] A.J.H. Vinck, J. Häring, T. Wadayama, Coded M-FSK for power-line communications, in: Proc. IEEE Internat. Symp. Information Theory, Sorrento, Italy, June 2000, p. 137.

[7] T. Wadayama, A.J.H. Vinck, A multilevel construction of permutation codes, IEICE Trans. Fundamentals Electron., Commun. Comp. Sci. 84 (2001) 2518–2522.

[8] J.-C. Chang, R.-J. Chen, T. Kløve, S.-C. Tsai, Distance-preserving mappings from binary vectors to permutations, IEEE Trans. Inform. Theory 49 (2003) 1054–1059.

[9] K. Lee, New distance-preserving maps of odd length, IEEE Trans. Inform. Theory 50 (10) (2004).

[10] J.-C. Chang, Distance-increasing mappings from binary vectors to permutations, IEEE Trans. Inform. Theory 51 (1) (2005) 359–363.