國立交通大學

資訊工程學系

博士論文

向量至排列之保距映射之建構與分析

Construction and Analysis of Distance-Preserving Mappings from Vectors to Permutations

研究生：林志賢

指導教授：陳榮傑 博士

中華民國九十六年十二月

向量至排列之保距映射之建構與分析

Construction and Analysis of Distance-Preserving Mappings from Vectors to Permutations

研究生：林志賢

Student：Jyh-Shyan Lin

指導教授：陳榮傑 博士

Advisor：Dr. Rong-Jaye Chen

國立交通大學資訊學院
資訊工程學系
博士論文

A Thesis
Submitted to Department of Computer Science
College of Computer Science
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy
in

Computer Science

December 2007

Hsinchu, Taiwan, Republic of China

中華民國九十六年十二月

向量至排列之保距映射之建構與分析

研究生：林志賢　　指導教授：陳榮傑 博士

國立交通大學資訊學院資訊工程學系博士班

摘要

一個從長度為 n 的所有 q 元向量所成之集合，到 $\{1, 2, \ldots, N\}$ 所有可能排列所成之集合$(N \geq n)$的映射，若任二個向量所對應之排列彼此之間的漢明距離(Hamming distance) 大於或等於原本向量之間的漢明距離，稱之為『保距映射』(distance-preserving mapping)。有一種特殊的『保距映射』，會讓排列之間的漢明距離絕對大於原本向量之間的漢明距離，除非在不可能的情況之下。這種映射稱之為『增距映射』(distance-increasing mapping)。在本論文中，我們提出數個建構方法，以建構從二元向量(binary vectors)至排列的『增距映射』。跟早期發表的方法比起來，這些方法具有某些優點。另外，我們也會提出幾個建構方法，以建構從三元向量(ternary vectors)至排列的『保距映射』與『增距映射』。這是在文獻中，第一次有人提出源自三元向量的『保距映射』與『增距映射』之建構方法。這些建構方法的一項貢獻是它們可以用來提升一個下限量 —『排列陣列』(permutation arrays)，又稱為『排列碼』(permutation codes) 的大小的最大下限。在設計一個以電源線為媒介的通訊系統時，『排列碼』是一種很有用的碼。

Construction and Analysis of Distance-Preserving Mappings from Vectors to Permutations

Student : Jyh-Shyan Lin Advisor : Dr. Rong-Jaye Chen

Department of Computer Science
College of Computer Science
National Chiao Tung University

Abstract

A mapping from the set of all q-ary vectors of length n to the set of all permutations of $\{1, 2, \ldots , N\}$ where $N \geq n$ is called a distance-preserving mapping (DPM) if every two vectors are mapped to permutations with the same or even larger Hamming distance than that of the 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. In this dissertation, we propose several constructions of DIMs from binary vectors. These constructions possess some advantages over previous proposed constructions. In addition, we also propose constructions of DPMs and DIMs from ternary vectors. This is the first time that constructions of DPMs and DIMs from ternary vectors are proposed in the literature. A contribution of these constructions is their application to the improvement of the lower bounds on the maximal size of permutation arrays (or permutation codes), which are useful in the design of a power line communication system.

誌　　謝

這篇論文得以順利完成，首先要感謝指導老師陳榮傑教授，五年多來耐心的指導與教誨。也要感謝師母李惠慈女士，多次細心地批改論文並加以訂正。同時感謝實驗室的學長張仁俊教授以及遠在挪威的Torleiv Kløve教授，在論文發表上諸多的協助與建議。再者，感謝論文審查委員曾文貴教授與楊武教授，從論文計畫書到論文口試，給予我適時的建議與指引。另外，感謝李新林教授、呂育道教授、與石維寬教授擔任我的論文口試委員，並給予我許多寶貴的意見。

在我報考博士班之初，楊慶隆教授曾給予我適時的鼓勵與建議。在此獻上我由衷的謝意。實驗室中的學長鈞祥與緯凱，以及學弟凱群、漢璋、家瑋、輔國、佩娟、與用翔，感謝你們這些年來陪伴我一起學習、討論、與成長。

我要將這份榮耀，獻給我的父親林金雄先生、母親林連世女士、以及兄長林志英先生，並感謝他們在我求學的過程中，不斷地給予我關懷與鼓勵。

最後，要感謝我的太太慧玲，多年來默默的犧牲奉獻，讓我無後顧之憂，得以專心地完成學業。並在我遭遇挫折、情緒低落之時，適時地給予我支持與鼓勵。她的支持與鼓勵，是我完成博士學位最重要的動力來源。

Contents

List of Tables

Chapter 1

Introduction

1.1 Research Motivations

A distance-preserving mapping (DPM) is a function from the set of all q-ary vectors of length n to the set of all permutations of $\{1, 2, \ldots , N\}$ where $N \geq n$ such that every two vectors are mapped to permutations with the same or even larger Hamming distance than that of the vectors. The Hamming distance between two vectors, or two permutations, is the number of positions where they differ. The inspiration of researches on DPM is mainly from its application to the construction of permutation arrays (or permutation codes), a set of permutations of the same length in which the Hamming distance of every two distinct permutations is at least D where $D \geq 2$. In 2000, Ferreira and Vinck used permutation codes to design a modulation/demodulation scheme which is able to make robust transmission over power lines [9]. The permutation codes they used were constructed via DPMs from binary vectors. They found a DPM from binary vectors of length 4 by computer search. From this mapping they constructed DPMs from binary vectors of length n = 5, 6, 7, and 8, using an *ad hoc* “prefix method.” In this paper it was not clear that if and how their method could be generalized to all $n > 8$. This raised a question: how to design a systematic method to construct DPMs from vectors to permutations for a given length (if it is possible). Ever from this paper was published, many constructions of DPMs were proposed. Recently, the research interests in DPM have turned to a special type of DPM, called distance-increasing mapping (DIM). A mapping is called a DIM if every two distinct vectors are mapped to permutations such that the Hamming distance between them is strictly increased except when that is obviously not possible. In later chapters, we will describe the constructions of DPMs/DIMs proposed so far in the literature, including those that we proposed.

1.2 Outline of the Dissertation

The remaining part of this dissertation is organized as follows. In Chapter 2 an introduction to permutations, permutation arrays, and power line communications is given. The formal definitions and previous research results of DPMs and DIMs are also given in this chapter. In Chapter 3 we propose new simple constructions of distance-increasing mappings from binary vectors. These constructions possess some advantages over previously proposed constructions. In Chapter 4, we propose several constructions of DPMs and DIMs from ternary vectors. This is the first time that constructions of DPMs and DIMs from ternary vectors are proposed in the literature. Finally, conclusions and future works are given in Chapter 5.

Chapter 2

Preliminaries

2.1 Permutations

A permutation of a set A is a one to one and onto function on A. For example, let A = {#, %, &}, the function ϕ given schematically as follows is a permutation of A.

$$\begin{array}{ccc} & \phi & \\ \# & \to & \% \\ \% & \to & \& \\ \& & \to & \# \end{array}$$

By renaming the elements of a set, any set with N elements can be mapped to the set $F_N = \{1, 2, \dots, N\}$. Thus, a permutation of any set of length N can be redefined as a permutation of F_N. A more standard notation of a permutation $\pi : F_N \to F_N$ is represented by

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

where $\pi_1, \pi_2, \dots, \pi_N \in F_N$. This representation is called the *standard form*. Since π is a function, we may denote $\pi(i) = \pi_i$. For simplicity, π can also be represented by an n-tuple $\pi = (\pi_1, \pi_2, \dots, \pi_N)$, which is called the *vector form*.

Example 2.1 The above set A can be mapped to F_3 = {1, 2, 3}. With the new symbols, the above permutation ϕ can be rewritten as

$$\phi' = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ or equivalently,}$$

$$\phi' = (2, 3, 1).$$

Let S_N denote the set of all N! permutations of F_N. The function composition $\circ$ is a binary operation on S_N. We call this operation *permutation multiplication*, which is defined as follows.

Definition 2.1 Let ρ and μ be two permutations of F_N, the composition operation $\rho \circ \mu$ is defined as

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

Example 2.2 Suppose that

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

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, sometimes we denote $\rho \circ \mu$ by $\rho\mu$. It is clear that $\rho\mu$ is also a permutation of F_N. Note that permutation multiplication is associative but not commutative. It can be proven that S_N is a group under permutation multiplication [20]. The identity of S_N, (1, 2, … , N), is denoted by ι. For a permutation ρ of F_N, we define $\rho^0 = \iota$.

For a permutation ρ, the inverse function, ρ^{-1}, is the permutation such that $\rho\rho^{-1} = \rho^{-1}\rho = \iota$. ρ^{-1} can be obtained by setting $\rho^{-1}(i) = j$ for i = 1, 2, …, N where j is the integer such that $\rho(j) = i$.

Example 2.3 Suppose that

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}. \text{ Then } \rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix}.$$

Definition 2.2 A set of permutations is called a *commutative set* if any two permutations ρ and μ in the set commute, that is, $\rho\mu = \mu\rho$.

2.2 Permutation Arrays and Power Line Communications

A *permutation array* (or *permutation code*) of length N and distance D, or an (N, D)-PA for short, is a subset of S_N such that the Hamming distance between any two distinct permutations (in vector form) in the array is at least D. The Hamming distance $d_H(\mathbf{a}, \mathbf{b})$ between two N-tuple $\mathbf{a} = (a_1, a_2, \dots , a_N)$ and $\mathbf{b} = (b_1, b_2, \dots , b_N)$ of elements of any kind is the number of positions where they differ. That is,

$$d_H(\mathbf{a}, \mathbf{b}) = |\{ j \in F_N : a_j \neq b_j \}|.$$

Example 2.4 The following set C is a (4, 4)-PA.

$$\begin{aligned} C = \{ & (1, 2, 3, 4), \\ & (4, 1, 2, 3), \\ & (3, 4, 1, 2), \\ & (2, 3, 4, 1) \}. \end{aligned}$$

Permutation arrays were somewhat studied in 1970s. Some representative papers from that period are [12], [24], and [28]. Recently, an application of permutation arrays on data communication over power lines introduced by Vinck [2] has created renewed interest in permutation arrays [1], [3], [5], [6], [8], [9], [10], [32], [33], [36]. In addition, permutation arrays have also been applied in the design of block ciphers [7].

Power line communications (PLC) are of recent interest because they are one of the possible solutions to the “last dirty mile” problem in communication systems. Although the primary function of power lines is to deliver electric power, the signal can be used as carrier to deliver messages. The frequency of the signal can be modulated, corresponding to a message transmitted, to produce a family of N “close” frequencies that are orthogonal. When the modulated signal reaches the receiver, these small variations in frequency can be decoded as symbols and then the message could be retrieved [26]. This modulation process must not interfere with the power transmission. For this reason, while minor variations in frequency (and commensurate minor variations in power) are acceptable, it is imperative that the power signal remains as constant as possible. One way to achieve this is to use a constant composition code in which each codeword represents a message, and each symbol in a codeword represents a frequency. More specifically, let C be a code of length L , $L \geq N$, over alphabet $A = \{a_1, a_2, \ldots , a_N\}$, $r_1, r_2, \ldots , r_N$ be integers such that

$$\sum_{i=1}^{N} r_i = L .$$

If each codeword in C has exactly r_i occurrences of the symbol a_i, then C is a constant composition code. Using C to encode each message and modulate the signal (each symbol a_i corresponds to a frequency f_i), the power delivered in the transmission for any message is a constant. Furthermore, if L is close to N, then the power envelope remains very close to constant.

In addition to keeping the power envelope constant, an effective design of a PLC system must address the source of errors unique to power lines. There are three main types of noise which may cause errors in PLC as reported in [25] and [27].

- *Permanent narrow-band noise* caused by electrical equipments such as television sets and refrigerators. This type of noise is permanent and affects some frequencies over a long period of time;
- *Impulse noise* caused by all kinds of switching operations. Such a noise

affects the entire frequency band for a very short period of time (typically less than 100 μs); and

- *White Gaussian noise* (background noise).

In many traditional data transmission media (e.g., telephone lines and satellite communications), white Gaussian noise is the most dominating type of noise affecting the communications, but in PLC the other two types of noise are more important. Narrow-band noise can be addressed by using many frequencies but not using any frequency too often. On the other hand, using many time slots is a good way to deal with impulse noise. In the tradeoff between these objectives and the requirement for constant power envelope, we choose $r_1 = r_2 = \ldots = r_N = 1$ and $L = N$, resulting in each type of noise not affecting a single symbol in a codeword more than one time, and in keeping the length as short as possible. Now considering the structure of a codeword, we found that each codeword is a permutation. In order to detect or correct errors caused by these noises, the codewords must be chosen elaborately such that the Hamming distance between any two distinct codewords in C is at least D and D is as large as possible. Such a code C is then an (N, D)-PA. This is the reason why permutation arrays are so important in power line communications.

Example 2.5 Twelve messages are encoded as in Table 2.1. The codewords form a (4, 3)-PA. As an example, message 2 is encoded as (1, 3, 4, 2) and is transmitted in time as a sequence of frequencies f_1, f_3, f_4, and f_2. While the message is transmitting, if a narrow-band noise is present at the sub-channel of frequency f_4, causing a sequence of frequencies (f_1, f_4), (f_3, f_4), f_4, and (f_2, f_4) arrived in time at the receive end. With these frequencies received, the receive end could obtain a demodulated output ((1, 4), (3, 4), 4, (2, 4)). By maximum likelihood decoding, i.e., comparing this output with all codewords and choosing the one with the maximum number of agreements in all positions, the demodulator outputs the codeword (1, 3, 4, 2) and then the receiver obtains the correct message.

Impulse noises can be viewed as “erasures” which may cause the demodulator to output the presence of all frequencies. Typically, the duration of impulse noise is

Table 2.1 Listing of 12 messages and the corresponding codewords.

Massage	Codeword
1	(1, 2, 3, 4)
2	(1, 3, 4, 2)
3	(2, 1, 4, 3)
4	(2, 4, 3, 1)
5	(3, 1, 2, 4)
6	(3, 4, 1, 2)
7	(4, 2, 1, 3)
8	(4, 3, 2, 1)
9	(1, 4, 2, 3)
10	(2, 3, 1, 4)
11	(3, 2, 4, 1)
12	(4, 1, 3, 2)

less than 100 μs, and the inter-arrival times are independent and are 0.1 to 1 second apart. In a PLC using a signaling rate of 10 kHz, we have symbol duration of 100 μs. Hence, an impulse noise may affect at most two adjacent symbols in such a communication system. Suppose an impulse noise occurs between the two first symbols while message 2 is transmitting, we may have a demodulated output ((1, 2, 3, 4), (1, 2, 3, 4), 4, 2). Comparing this output with all codewords, we find that (1, 3, 4, 2) agrees with the output in all of the four positions and all the other codewords agree with the output in two or three positions. Hence, the correct message is obtained.

White Gaussian noise causes errors by introducing unwanted (called insertion) transmitted frequencies or causing absence (called deletion) of symbols in the demodulated output. Suppose f_1 is inserted and f_3 is deleted in the transmission of message 2 due to the white Gaussian noise, we may have a demodulated output (1, 1, (1, 4), (1, 2)). Comparing this output with all codewords, we find that (1, 3, 4, 2) is the closest and, as a result, message 2 is obtained.

In conclusion, a PLC with an (N, D)-PA is able to correct at most $D - 1$ errors caused by narrow-band, impulse, or white Gaussian noises. While a large D is good for error correction, increasing the minimum distance may reduce the size of a permutation array, resulting in inefficiency of the transmission. Let $P(N, D)$ denote the maximal size of an (N, D)-PA. The exact value of $P(N, D)$ is an open problem except for some specific cases. In most cases we know just a lower bound and an upper bound. Trying to find a tight bound on $P(N, D)$ is a typical research topic in the literature. The following are some well-known elementary properties of $P(N, D)$.

Proposition 2.1 [36]

i) $P(N, 2) = N!$,

ii) $P(N, 3) = N!/2$,

iii) $P(N, N) = N$,

iv) $P(N, D) \geq P(N - 1, D)$,

v) $P(N, D) \geq P(N, D + 1)$,

vi) $P(N, D) \geq N$,

vii) $P(N, D) \leq N \times P(N - 1, D)$,

viii) $P(N, D) \leq N!/(D - 1)!$.

Proposition 2.2 [6] If q is a prime-power, then $P(q, q - 1) = q(q - 1)$.

Proposition 2.3 [28] If q is a prime-power, then $P(q + 1, q - 1) = (q + 1)q(q - 1)$.

Construction of permutation arrays is another typical research topic due to the importance of permutation arrays in PLC. Given a length N and a minimum distance D, we want to construct a permutation array of size as large as possible. The simplest way to construct permutation arrays is by computer search as in [24]. However, this method is only practical for small N due to the search space. Another approach of constructions is to construct permutation arrays by combining existing PAs and other codes, e.g. binary codes as in [5], [8], [33], and [36]. Nevertheless, these methods are restricted to some specific values of N and D. The other constructions take an indirect approach, which begins with constructing a mapping from vectors to permutations, called distance-preserving mapping, and then transforms a code with a minimum distance into a permutation array by using such a mapping. We will describe distance-preserving mappings in the following sections, including the definitions and the research results in the literature. After that, we will propose distance-preserving mappings from binary vectors and from ternary vectors in the next two chapters, respectively.

2.3 Distance-Preserving Mappings (DPMs) and Distance-Increasing Mappings (DIMs)

Being an important way to construct permutation arrays, distance-preserving mappings come into notice in recent years. A mapping from the set of all q-ary vectors of length n to the set S_N is called a distance-preserving mapping (DPM) if every two vectors are mapped to permutations with the same or even larger Hamming distance than that of the vectors.

Let $Z_q = \{0, 1, \ldots, q-1\}$ and Z_q^n denote the set of all q-ary vectors of length n. That is,

$$Z_q^n = \{(z_1, z_2, \ldots, z_n) : z_1, z_2, \ldots, z_n \in Z_q\}.$$

Definition 2.3 A mapping $f: Z_q^n \to S_N$ is called a distance-preserving mapping if any two vectors x, y in Z_q^n satisfy

$$d_H(f(x), f(y)) \geq d_H(x, y).$$

A mapping that increases more distances than that of input vectors may be more interesting for applications. 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.

Definition 2.4 A mapping $f: Z_q^n \rightarrow S_N$ is called a distance-increasing mapping if any two distinct vectors x, y in Z_q^n satisfy

$$d_H(f(x), f(y)) \geq \min\{ d_H(x, y) + 1, N \}.$$

Let $\mathcal{F}(q, n, N)$ denote the set of all mappings from Z_q^n to S_N, $\mathcal{P}(q, n, N)$ denote the set of all DPMs from Z_q^n to S_N, and $\mathcal{I}(q, n, N)$ denote the set of all DIMs from Z_q^n to S_N. A mapping in $\mathcal{P}(q, n, N)$ is called a q-ary n_N-DPM. A mapping in $\mathcal{I}(q, n, N)$ is called a q-ary n_N-DIM. If $n = N$, then an n_N-DPM/n_N-DIM can be denote by n-DPM/n-DIM for simplicity. Besides, a DPM/DIM from binary vectors ($q = 2$) to permutations is called a binary DPM/DIM, and a DPM/DIM from ternary vectors ($q = 3$) to permutations is called a ternary DPM/DIM.

Example 2.6 The following table lists the elements $x \in Z_2^4$ and the corresponding values of $f(x) \in S_4$. It can be checked that $f \in \mathcal{I}(2, 4, 4)$, i.e., f is a binary 4-DIM.

Table 2.2　Mapping table of $f \in \mathcal{I}(2, 4, 4)$.

x	$f(x)$	x	$f(x)$
(0,0,0,0)	(1,2,3,4)	(1,0,0,0)	(2,1,3,4)
(0,0,0,1)	(4,2,3,1)	(1,0,0,1)	(4,1,3,2)
(0,0,1,0)	(1,3,2,4)	(1,0,1,0)	(2,3,1,4)
(0,0,1,1)	(4,3,2,1)	(1,0,1,1)	(4,3,1,2)
(0,1,0,0)	(1,2,4,3)	(1,1,0,0)	(2,1,4,3)
(0,1,0,1)	(3,2,4,1)	(1,1,0,1)	(3,1,4,2)
(0,1,1,0)	(1,4,2,3)	(1,1,1,0)	(2,4,1,3)
(0,1,1,1)	(3,4,2,1)	(1,1,1,1)	(3,4,1,2)

For a mapping $f \in \mathcal{F}(q, n, N)$, let $D_f = [\,D_{i,j}\,]$ be an n by N matrix where $D_{i,j}$ is the number of unordered pairs $\{x, y\}$ in Z_q^n such that $d_H(x, y) = i$ and $d_H(f(x), f(y)) = j$. We call D_f the *distance expansion distribution* or *distance expansion matrix* of f. Distance expansion matrix shows the distance increasing property of a mapping and is an important criterion to compare different DPMs/DIMs of the same length (the same vector length and the same permutation length).

Example 2.7 The following table shows the distance expansion matrix of the mapping f in Example 2.6. The element $d_{12} = 32$ means that all of the $\frac{1}{2} \cdot 2^4 \cdot \binom{4}{1} = 32$ unordered pairs $\{x, y\}$ in Z_2^4 with distance $d_H(x, y) = 1$ were mapped to $f(x)$ and $f(y)$ with distance $d_H(f(x), f(y)) = 2$. The 0's on the lower triangular part and the diagonal of the matrix justify that f is distance increasing. Since we focus on DPMs and DIMs only, in the rest of the dissertation we will omit the 0's in the lower triangular part of a distance expansion matrix.

Table 2.3 Distance expansion matrix of the mapping in Table 2.2.

	1	2	3	4
1	0	32	0	0
2	0	0	32	16
3	0	0	0	32
4	0	0	0	8

While distance expansion matrix is an important criterion to compare DPMs, the comparison can be tedious since we have to compare $n \times N$ matrices. For a mapping $f \in \mathcal{P}(q, n, N)$, define

$$\Delta(f) = \sum_{x,y\in Z_q^n}\left\{ d_H(f(x),f(y)) - d_H(x,y) \right\}$$

$$= 2\sum_{i=1}^{n}\sum_{j=i+1}^{N}(j-i)D_{i,j} = \Delta_1(f) - \Delta_0$$

where

$$\Delta_0 = \sum_{x,y\in Z_q^n} d_H(x,y) = q^n\sum_{i=1}^{n} i\binom{n}{i}(q-1)^i = n(q-1)q^{2n-1},$$

and

$$\Delta_1(f) = \sum_{x,y\in Z_q^n} d_H(f(x),f(y)) = 2\sum_{i=1}^{n}\sum_{j=i}^{N} j\cdot D_{i,j}\ .$$

$\Delta_1(f)$ is called the *total distance* of f and $\Delta(f)$ is called the *total distance increase* of *f*. For example, the total distance and the total distance increase of the DIM in Table 2.2 are 768 and 256, respectively. Total distance and total distance increase are also important criteria for the comparisons of different DPMs/DIMs of the same length. Swart, de Beer, and Ferreira gave the following upper bound on $\Delta_1(f)$ [29], [30].

Proposition 2.4 Let $\alpha = \lfloor q^n / N \rfloor$ and $\beta = q^n \bmod N$. Then

$$\Delta_1(f) \le N\,(q^{2n} - (2\beta\alpha + \beta + \alpha^2 N)).$$

Furthermore, if $N = q^r$, where $r \le n$, then

$$\Delta_1(f) \le q^{2n}\,(q^r - 1).$$

The maximum possible value of $\Delta_1(f)$ is denoted by $\Delta_{\max}$.

DPMs and DIMs can be used to construct permutation arrays. Given an (n, d) code C over Z_q (C is a subset of Z_q^n, each member of C is called a codeword, and the Hamming distance between any two distinct codewords in C is at least d), if a

DPM f from Z_q^n to S_N can be found, then $f(C)$ is an (N, d)-PA. From this mapping we immediately get the bound that for $2 \le d \le n$,

$$P(N, d) \ge A_q(n, d)$$

where $A_q(n, d)$ denotes the maximal size of such an (n, d) code. Furthermore, if a DIM g from Z_q^n to S_N can be found, then $g(C)$ is an $(N, d + 1)$-PA. From this mapping we immediately get the bound that for $2 \le d \le n$,

$$P(N, d) \ge A_q(n, d - 1)$$

It means that the plentiful research results on coding theory can be applied to permutation arrays, including construction methods and lower bounds on the size of an (n, d) code.

2.4 Previous Works

DPMs were first discussed in the paper [11] where Ferreira *et al.* utilized DPMs to transform a linear convolutional code into a runlength constrained or balanced trellis code with the same or larger free distance. In 2000, Ferreira and Vinck constructed binary n-DPMs for $5 \le n \le 8$ and used them to construct permutation trellis codes [9]. They found a mapping in $P(2, 4, 4)$ by computer search and from this mapping they recursively constructed binary n-DPMs, using an *ad hoc* “prefix method,” for $n = 5, 6, 7$, and 8. However, it was not clear in their paper if and how this method could be generalized to $n > 8$. This paper brought distance-preserving mappings to the attention of researchers and many papers on this topic have been available ever since.

Three years later, Chang *et al.* proposed a recursive systematic method to construct binary n-DPMs for all $n \ge 4$ [17]. The construction extends a binary DPM of length $n - 1$ to a binary DPM of length n with the assistance of a position function of length $n - 1$. In addition to the recursive construction, in that paper they also provided a non-recursive construction of DPMs from binary vectors of even length. Form these constructions they derived the following result which improved the lower bound on $P(N, D)$ known before.

Proposition 2.5 [17] For $N \geq 4$ and $2 \leq D \leq N$,

$$P(N, D) \geq A_2(N, D - 1). \tag{2.1}$$

Later in 2004, Lee proposed a non-recursive construction of DPMs from binary vectors of odd length [23]. In that paper he introduced the concept of distance expansion distribution and applied it as a criterion to compare the distance increasing property of different DPMs of the same length.

In 2005, Chang introduced the concept of distance-increasing mapping and proposed recursive and non-recursive constructions of binary n-DIMs for any length $n \geq 4$ [14]. The non-recursive construction is based on three mappings $r_4 \in \boldsymbol{I}(2, 4, 4)$, $r_5 \in \boldsymbol{I}(2, 5, 5)$, and $r_6 \in \boldsymbol{I}(2, 6, 6)$ where r_5 is found by computer search and r_4 as well as r_6 are obtained by the construction described in [17, Construction 3]. Hence, a small lookup table containing r_5 is needed for further construction of r_n for $n \geq 7$.

Later in the same year, Lee proposed a non-recursive construction of n-DPMs from binary vectors for all $n \geq 4$ [21]. He viewed a permutation as lying on circles and constructed DIMs of even length as well as DPMs of odd length.

With the similar way (viewing a permutation as lying on circles), Lee improved his method and finally proposed a new construction of DIMs for both even and odd length in 2006 [22].

Also in 2006, Chang proposed another non-recursive construction of binary n-DIMs that does not need any table lookup operations [15]. The construction was based on a number of swap operations. In fact, all constructions of DPMs/DIMs described above except computer search were swap based. The author claimed that the new construction needed fewer swap operations than other previously proposed constructions.

In the same year, Chang also proposed two new recursive constructions of binary n-DIMs which strictly increased the Hamming distance by at least δ ($\delta \geq 2$) except when it was obviously not possible [13]. That is, let f be such a mapping, for any two distinct binary vectors $x, y \in Z_2^n$,

$$d_H(f(x), f(y)) \geq \min\{ d_H(x, y) + \delta, n \}.$$

We called such a mapping a binary (n_n, δ)-DIM, or a binary (n, δ)-DIM for short. The first construction combined two DIMs, a binary (m, $\delta - 1$)-DIM and a binary (n, $\delta - 1$)-DIM, into a binary ($m \times n$, δ)-DIM. In that paper a binary (16, 2)-DIM was constructed from two binary (4, 1)-DIMs as an example. The second construction combined a binary (m, δ)-DIM and a binary (n, δ)-DIM into a binary ($m + n$, δ)-DIM. Apart from the constructions, the author also proved that for any $\delta \geq 2$ there existed a smallest positive integer n_δ such that a binary (n, δ)-DIM could be constructed for any $n \geq n_\delta$. An explicit upper bound on n_δ was given in that paper. As a consequence, for all $N \geq n_\delta$ and $\delta + 1 \leq D \leq N$, we had

$$P(N, D) \geq A_2(N, D - \delta). \tag{2.2}$$

Swart *et al.* proposed a class of multilevel constructions for binary n-DPMs for $n \geq 4$ from September 2005 to August 2006 [29], [30], [31]. The constructed DPMs were superior in total distance. They showed that if the sequences of swaps corresponding to the input vectors were suitably chosen, then the resulting DPM might possess higher total distance than other constructions. In particular, if $n = 2^r$, then the maximum possible value of the total distance of a DPM was reached for these constructions. That is,

$$\Delta_1(f) = 2^{2n}(2^r - 1).$$

Note that the construction method can also be used to construct DIMs.

In August 2006, Huang *et al.* proposed a recursive construction of binary (n_(n+2), 3)-DIMs for $n \geq 6$ with some predefined lookup tables [37]. With this construction, they obtained the following bound which was better than (2.1) but worse than (2.2).

Proposition 2.6 [37] For $N \geq 8$ and $4 \leq D \leq N$,

$$P(N, D) \geq A_2(N-2, D-3) > A_2(N, D-1).$$

In July 2007, Chang proposed another recursive construction of a binary $(m+n, \delta)$-DIM from a binary (m, δ)-DIM and a binary (n, δ)-DIM [16]. In this paper he also proposed a new way to construct PAs from the proposed DIMs and, with this construction, he improved the lower bound on the size of PAs as follows.

Proposition 2.7 [16] For $N > 2\delta > 0$, $M > 0$, and $\delta + 1 \leq D \leq MN$, if there exists an (N, δ)-DIM, then

$$P(MN, D) \geq A_2(MN, D-\delta)P(M, \lceil D/(N-2\delta) \rceil).$$

Chapter 3

DIMs from Binary Vectors

In most papers, DPMs and DIMs are implicitly described by algorithms [14], [15], [17], [21], [22], [23], [37]. Although the algorithmic presentations are more convenient for a computer programmer to implement, they are theoretically informal and most readers will not be comfortable with them. In this chapter we explicitly define mappings from vectors to permutations based on simple composition of permutations (permutation multiplication). With this definition, we first propose non-recursive constructions of binary n-DIMs for even and odd length, respectively. In these constructions, binary vectors and the mapped permutations are of the same length, i.e. $n = N$. Thus, in this chapter we use the notation n only. These constructions are still easy to implement. Comparisons of our DIMs with other previously proposed DPMs and DIMs are given as well.

Definition 3.1 Let $B = \langle \rho_1, \rho_2, \ldots , \rho_n \rangle$ be an ordered set of permutations in S_n. We define a mapping from Z_2^n to S_n as

$$f(x_1, x_2, \ldots, x_n) = \rho_1^{x_1} \circ \rho_2^{x_2} \circ \cdots \circ \rho_n^{x_n} = \prod_{j \in J_x} \rho_j \, . \tag{3.1}$$

where $J_x = \{ j \mid x_j = 1, j = 1, \ldots, n \}$. Note that by the notation $\prod$ the multiplication is performed in the order of the integers in J_x. B is called the *basic construction set* of f.

Example 3.1 Suppose f is constructed by (3.1) with the basic construction set

$$B = \langle\, \rho_1 = (2, 1, 3, 4), \rho_2 = (1, 2, 4, 3),$$
$$\rho_3 = (1, 3, 2, 4), \rho_4 = (4, 2, 3, 1)\,\rangle.$$

Then,

$$f(0, 0, 0, 0) = \rho_1{}^0 \circ \rho_2{}^0 \circ \rho_3{}^0 \circ \rho_4{}^0 = \iota \circ \iota \circ \iota \circ \iota = \iota = (1, 2, 3, 4), \text{ and}$$
$$f(1, 0, 1, 1) = \rho_1\rho_3\rho_4 = \prod_{j\in\{1,3,4\}} \rho_j = (2, 1, 3, 4)\ (1, 3, 2, 4)\ (4, 2, 3, 1)$$
$$= (4, 3, 1, 2).$$

3.1 DIMs of Even Length

Based on a basic construction set, (3.1) gives us a mapping from Z_2^n to S_n. However, the mapping is not necessarily distance preserving or distance increasing. Remember that our goal is to construct distance-increasing mappings from Z_2^n to S_n. The following lemmas indicate how to choose the members of a basic construction set such that the constructed mapping is distance increasing.

Lemma 3.1 Let f be a mapping constructed by (3.1) with the basic construction set $B_f = \langle \rho_1, \rho_2, \dots, \rho_n \rangle$. Then $f \in \mathcal{I}(2, n, n)$ if for any two distinct subset J_1 and J_2 of F_n,

$$d_H\left(\prod\nolimits_{j\in J_1} \rho_j, \prod\nolimits_{j\in J_2} \rho_j\right) > |\, J_1 \oplus J_2 \,| \text{ when } |\, J_1 \oplus J_2 \,| < n, \text{ and} \tag{3.2}$$

$$d_H\left(\prod\nolimits_{j\in J_1} \rho_j, \prod\nolimits_{j\in J_2} \rho_j\right) = |\, J_1 \oplus J_2 \,| \text{ when } |\, J_1 \oplus J_2 \,| = n, \tag{3.3}$$

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

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

$| J_1 \oplus J_2 |$ and

$$f(\mathbf{a}) = \prod\nolimits_{j \in J_1} \rho_j \,,\; f(\mathbf{b}) = \prod\nolimits_{j \in J_2} \rho_j \,.$$

It is clear that $f \in I(2, n, n)$ if (3.2) and (3.3) are true. □

Lemma 3.1 states the criteria that the basic construction set of a binary $(n, 0)$ DIM should meet. However, we must consider $\binom{2^n}{2}$ combinations of any two distinct subsets of B_f. Under some conditions, the following lemma considers only 2^n subsets of B_f.

Lemma 3.2 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 $f \in I(2, n, n)$ if every subset $J \subseteq F_n$ satisfies

$$d_H(\prod\nolimits_{j \in J} \rho_j, \iota) > | J | \text{ when } | J | < n, \text{ and} \tag{3.4}$$

$$d_H(\prod\nolimits_{j \in J} \rho_j, \iota) = | J | \text{ when } | J | = n. \tag{3.5}$$

where $| J |$ denotes the number of elements of J.

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

$$d_H(\prod\nolimits_{j \in J_1} \rho_j, \prod\nolimits_{j \in J_2} \rho_j) = d_H(\prod\nolimits_{j \in J_1 \oplus J_2} \rho_j,\; \iota)\,.$$

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

$$\begin{aligned} d_H(\prod\nolimits_{j \in J_1} \rho_j, \prod\nolimits_{j \in J_2} \rho_j) &= d_H(\rho_2\rho_3\rho_4, \rho_1\rho_3) \\ &= d_H(\rho_1\rho_2\rho_3\rho_4\rho_3, \rho_1\rho_1\rho_3\rho_3) \\ &= d_H(\rho_1\rho_2\rho_3\rho_3\rho_4, \iota) = d_H(\rho_1\rho_2\rho_4, \iota) \\ &= d_H(\prod\nolimits_{j \in J_1 \oplus J_2} \rho_j,\; \iota)\,. \end{aligned}$$

As a consequence, according to Lemma 3.1, $f \in I\,(2, n, n)$ if the statement is true. □

According to Lemma 3.2, we can construct a binary n-DIM for even n as follows.

Construction 3.1 Let $n = 2m$ and $m \geq 2$. Construct a mapping f_n with the following basic construction set

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

Theorem 3.1 The mapping f_n constructed by Construction 3.1 is a DIM for even n.

Proof. It is clear that both $\langle\rho_1, \rho_2, \dots, \rho_m\rangle$ and $\langle\rho_{m+1}, \rho_{m+2}, \dots, \rho_n\rangle$ are commutative and all permutations in B_{f_n} are self-inverse. Thus, it suffices to prove that (3.4) and (3.5) are true for any subset $J \subseteq F_n$.

Notice that $d_H\,(\rho_i, \iota) = 2$ for all $\rho_i \in B_{f_n}$. Furthermore, for any two distinct permutations $\rho_i, \rho_j \in B_{f_n}$, $d_H\,(\rho_i\rho_j, \iota) = 4$ if ρ_i and ρ_j commute, and $d_H\,(\rho_i\rho_j, \iota) = 3$ if ρ_i and ρ_j do not commute. Thus, we can define a function $I : B_{f_n} \times B_{f_n} \rightarrow Z$ 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 $d_H\,(\rho_i\rho_j, \iota) = 4 - I\,(\rho_i, \rho_j)$. This formula can be extended to

$$
d_H\Big(\prod\nolimits_{j \in J} \rho_j,\ \iota\Big) = 2\,|\,J\,| - \sum\nolimits_{i, j \in J, i \neq j} I(\rho_i, \rho_j) \tag{3.6}
$$

Now let

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

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

Formula (3.6) can be rewritten as

$$d_H\left(\prod\nolimits_{j\in J} \rho_j,\ \iota\right) = 2|\,B_1\,| + 2|\,B_2\,| - \sum\nolimits_{\rho_i \in B_1} \sum\nolimits_{\rho_j \in B_2} I(\rho_i, \rho_j) \qquad (3.7)$$

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

$$\sum\nolimits_{\rho_i \in B_1} \sum\nolimits_{\rho_j \in B_2} I(\rho_i, \rho_j) \le 2 \times \min\,\{|\,B_1\,|, |\,B_2\,|\}.$$

Thus

$$d_H\left(\prod\nolimits_{j\in J} \rho_j,\ \iota\right) \ge 2 \times \max\,\{|\,B_1\,|, |\,B_2\,|\} > |\,B_1\,| + |\,B_2\,| = |\,J\,|.$$

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,

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

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,

$$d_H\left(\prod\nolimits_{j\in J} \rho_j,\ \iota\right) = 2|\,B_1\,| = |\,J\,|.$$

For any subset $J \subseteq F_n$, Case 1 and Case 2 show that (3.4) is true and Case 3 shows that (3.5) is true. Thus, $f_n \in I\,(2, n, n)$. □

Example 3.2 (n = 6) $f_6 : Z_2^6 \rightarrow S_6$ is constructed with the following basic construction set

$$\begin{aligned} B_{f_6} = \langle\, \rho_1 &= (2, 1, 3, 4, 5, 6), \\ \rho_2 &= (1, 2, 4, 3, 5, 6), \\ \rho_3 &= (1, 2, 3, 4, 6, 5), \\ \rho_4 &= (1, 3, 2, 4, 5, 6), \\ \rho_5 &= (1, 2, 3, 5, 4, 6), \\ \rho_6 &= (6, 2, 3, 4, 5, 1)\,\rangle. \end{aligned}$$

The mapping table of f_6 is listed in Appendix A and the distance expansion matrix of f_6 is listed in Table 3.7. From Table 3.7 it is easy to see that f_6 is a DIM.

We have to mention that the DIM $f_n \in I(2, n, n)$ for even n proposed here is identical to z_n proposed in [22], and is similar to the mapping $h_{2m} \in I(2, 2m, 2m)$ for $m = 2$, or $m > 2$ and m is odd, as proposed in [17]. Although h_{2m} is described by an algorithm there, it can be described as the mapping corresponding to the basic construction set $B_{h_{2m}} = \langle\, \mu_1, \mu_2, \dots, \mu_{2m} \rangle$ where

$$\mu_i = (1, 2, \dots, 2i-2, 2i, 2i-1, 2i+2, \dots, 2m), \text{ and}$$

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

for $i = 1, 2, \dots, m$. Note that $\rho_i = \mu_i$ for $1 \le i \le m$, but $\rho_i \ne \mu_i$ for $m+1 \le i \le 2m$.

3.2 DIMs of Odd Length

We cannot construct a binary 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 when n is odd. In the following, we develop a different construction method for odd n.

Lemma 3.3 Let $n = 2m + 1$, $m \ge 2$, f_n be a mapping constructed by (3.1) with the following basic construction set

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

and suppose

$$\rho_{m+1} = (\pi_1, \pi_2, \ldots, \pi_n).$$

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 $1 \le k \le \frac{n-1}{2}$, 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 $\bigcup_{i=1}^{k} u_i \ne \bigcup_{i=1}^{k} v_i$, then for any subset $J \subseteq F_n \backslash \{m+1\}$,

$$d_H(\prod_{j\in J\cup\{m+1\}} \rho_j, \rho_{m+1}) > |\,J\,|. \tag{3.8}$$

Proof. Let $J_1 = \{\, j \mid j \in J$ and $1 \le j \le m\}$, $J_2 = \{\, j \mid j \in J$ and $m+2 \le j \le n\}$, $B_1 = \langle\, \rho_j \mid j \in J_1\,\rangle$, 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 $|\,B_2\,| = k$, $0 \le k \le \frac{n-1}{2}$. Consider the permutation $\mu = \rho_{m+1}\prod_{j\in J_2} \rho_j$. We know that $d_H(\mu, \rho_{m+1}) = 2k$. Let $P = \{\pi_i \mid \mu(i) \ne \pi_i\}$. For a permutation $\rho_c \in B_1$, $1 \le c \le m$, we have

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

The following shows that (3.8) is true in all possible cases.

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

$$\begin{aligned} d_H(\prod\nolimits_{j\in J\cup\{m+1\}}\rho_j,\rho_{m+1}) &\geq 2\times\max\{|B_1|,|B_2|\} \\ &> |B_1|+|B_2| = |J|. \end{aligned}$$

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

$$d_H(\prod\nolimits_{j\in J\cup\{m+1\}}\rho_j,\rho_{m+1}) > 2\times|B_1| = |J|.$$ □

Lemma 3.4 Let $n = 2m + 1$, $m \geq 2$, f be a mapping constructed by (3.1) with the basic construction set B_f in Lemma 3.3. Then $f \in I(2, n, n)$ if the following statements are true.

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

ii) For each $i \in F_n\backslash\{m+1\}$, $d_H(\prod_{j\in Z_n\backslash\{i,m+1\}}\rho_j,\rho_{m+1}) = n.$

iii) Let $U = \{\{\pi_2, \pi_3\}, \{\pi_4, \pi_5\}, \dots, \{\pi_{n-1}, \pi_n\}\}$, $V = \{\{1, 2\}, \{3, 4\}, \dots, \{n-2, n-1\}\}$. For $1\leq k \leq \frac{n-1}{2}$, let $u_1, \dots, u_k$ be any k distinct elements of U, and $v_1, \dots, v_k$ 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 (3.3) in Lemma 3.1 is true. Second, for any two distinct subsets $J_1, J_2 \subseteq F_n$, there are three possible cases:

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

No matter in which case, we show that (3.2) in Lemma 3.1 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 3.1 above. Thus

$$d_H(\prod\nolimits_{j\in J_1}\rho_j,\prod\nolimits_{j\in J_2}\rho_j) = d_H(\prod\nolimits_{j\in J_1\oplus J_2}\rho_j,\iota) > |J_1\oplus J_2|.$$

Case 2: Without loss of generality, assume $m + 1 \in J_1$ and $m + 1 \notin J_2$. We prove (3.2) 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 (3.2) is true for $| J_1 \oplus J_2 | = k + 1$ but is not true for $| J_1 \oplus J_2 | = k$. That is,

$$d_H(\prod_{j \in J_1 \oplus J_2} \rho_j,\ \iota) \leq k$$

for some $| J_1 \oplus J_2 | = k$. However, the only possibility for this assumption is

$$d_H(\prod_{j \in J_1 \oplus J_2} \rho_j,\ \iota)\ = k.$$

Because according to the hypothesis,

$$d_H(\prod_{j \in J_1 \oplus J_2 \cup \{i\}} \rho_j,\ \iota) > k + 1$$

for all $i \in F_n - (J_1 \oplus J_2)$, and ρ_i is a transposition 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 $i \in F_n - (J_1 \oplus J_2)$ changes exactly two of these positions to make

$$d_H(\prod_{j \in J_1 \oplus J_2 \cup \{i\}} \rho_j,\ \iota) = k + 2.$$

There are totally $n - k$ permutations each corresponding to an element of $F_n - (J_1 \oplus J_2)$. By the same logic as in Lemma 3.3, it is not possible for those $n - k$ permutations, which consist of two commutative sets and one of them is of size $\geq \left\lceil \frac{n-k}{2} \right\rceil$, that change only $n - k$ positions, which is a contradiction! Thus, we have

$$d_H(\prod_{j \in J_1 \oplus J_2} \rho_j,\ \iota) > k \text{ for } | J_1 \oplus J_2 | = k.$$

Case 3: $m + 1 \in J_1$ and $m + 1 \in J_2$. According to Lemma 3.3, we have

$$d_H\left(\prod_{j\in J_1}\rho_j, \prod_{j\in J_2}\rho_j\right) = d_H\left(\prod_{j\in J_1\oplus J_2\cup\{m+1\}}\rho_j, \rho_{m+1}\right)$$

$$> |\, J_1 \oplus J_2 \,|.$$ □

So if we can find a ρ_{m+1} satisfying i), ii), and iii) in Lemma 3.4, then we have a binary n-DIM for odd n. The following examples exhibit how to find a suitable permutation for ρ_{m+1} for $n = 5$ and $n = 7$ respectively.

Example 3.3 (n = 5) Suppose $f_5 : Z_2^5 \rightarrow S_5$ is constructed by (3.1) with 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 DIM, the following requirements should be satisfied:

i) $d_H(\rho_1\rho_2\rho_4\rho_5, \rho_3) = 5$.

ii) $d_H(\rho_2\rho_4\rho_5, \rho_3) = 5$, $d_H(\rho_1\rho_4\rho_5, \rho_3) = 5$, $d_H(\rho_1\rho_2\rho_4, \rho_3) = 5$, and $d_H(\rho_1\rho_2\rho_5, \rho_3) = 5$.

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

$$\begin{aligned} \rho_1\rho_2\rho_4\rho_5 &= (2, 4, 1, 5, 3), \\ \rho_2\rho_4\rho_5 &= (1, 4, 2, 5, 3), \\ \rho_1\rho_4\rho_5 &= (2, 3, 1, 5, 4), \\ \rho_1\rho_2\rho_5 &= (2, 1, 4, 5, 3), \\ \rho_1\rho_2\rho_4 &= (2, 4, 1, 3, 5), \end{aligned}$$

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) above 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). The mapping table of f_5 is listed in Appendix A and the distance expansion matrix of f_5 is listed in Table 3.6.

Example 3.4 (n = 7): Assume $f_7 : Z_2^7 \rightarrow S_7$ is constructed by (3.1) with the basic construction set described in Lemma 3.3. Based on the requirements depicted in Lemma 3.4, we exclude some values for ρ_4 in the same way as Example 3.1. The excluded values are summarized in Table 3.1.

Table 3.1 The excluded values for ρ_4 in the construction of $f_7 \in I\,(2, 7, 7)$.

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

In Table 3.1 the marks "×" denote the values that should be excluded. Besides, the selection of the values should satisfy the condition iii) in Lemma 3.4. There are many solutions for ρ_4 (totally 68). In order to make the distance expansion matrix as good as possible, we can choose a solution such that $d_H(\rho_4, \iota)$ is the largest among all possible solutions, for example, (5, 6, 3, 7, 1, 2, 4). The mapping table of f_7 is listed in Appendix A and the distance expansion matrix of f_7 is listed in Table 3.12.

Now we give a general construction of binary n-DIMs for odd n as follows.

Construction 3.2 Let $n = 2m + 1$ and $m \geq 2$. Construct a mapping f_n with the basic construction set described in Lemma 3.3 where

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

Theorem 3.2 The mapping f_n constructed by Construction 3.2 is a DIM for odd n.

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

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

for $i = 1, 2, \ldots, (n-3)/2$. The excluded values and the values selected for ρ_{m+1} are summarized in Table 3.2 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 3.4. □

Table 3.2 The excluded values for ρ_{m+1} in the construction of $f_n \in I(2, n, n)$ for odd n.

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

3.3 Comparisons

In this section, we compare our DIMs f_n with other mappings, including DPMs h_n proposed by Chang *et al.* [17], DPMs l_n of odd length proposed by Lee [23], DIMs r_n proposed by Chang [14], DIMs Q_n proposed by Chang [15], DIMs z_n proposed by Lee [22], and DPMs M_n proposed by Lee [31]. Tables 3.3 ~ 3.27 list the distance expansion matrices of these mappings for comparisons for $5 \le n \le 11$. Table 3.28 lists the distance expansion matrix of f_n for n = 13. The total distances $\Delta_1(f)$ of these mappings are listed in Table 3.29. The asterisk behind a number indicates that this number is the largest among all items. In the comparisons of distance expansion distributions, we only compare f_n with h_n, l_n, and r_n for $5 \le n \le 9$, and also compare f_n with Q_n for $8 \le n \le 10$ because only those mappings are given in the above-mentioned papers. We do not compare f_n with M_n for their distance expansion matrices since there is no such matrix in the corresponding paper. For even n, the distance expansion distribution of z_n and f_n are exactly the same since z_n and f_n are identical when n is even.

For n = 5, Tables 3.3 and 3.4 show that both h_5 and l_5 are DPMs but not DIMs, whereas Tables 3.5 and 3.6 show that r_5, z_5, and f_5 are all DIMs (the distance expansion distribution of z_5 and f_5 are exactly the same). The distance expansion distribution of r_5 is better than that of z_5 and f_5, and the total distances of these mappings justify this argument. This is reasonable since r_5 is obtained by computer search.

Table 3.3 Distance expansion matrix of h_5.

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

Table 3.4 Distance expansion matrix of l_5.

0	64	6	2	8
	4	68	64	24
		14	76	70
			22	58
				16

Table 3.5 Distance expansion matrix of r_5.

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

Table 3.6 Distance expansion matrix of z_5 and f_5.

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

For $n = 6$, l_6 is not compared since the paper [23] focuses on DPMs of odd length only. Although f_6 is not identical to h_6 and r_6 ($h_6 = r_6$), the distance expansion matrices of these mapping is just the same (see Table 3.7).

Table 3.7 Distance expansion matrix of h_6, r_6, z_6, and f_6.

0	192	0	0	0	0
	0	192	288	0	0
		0	192	384	64
			0	192	288
				0	192
					32

For $n = 7$, we see again that both h_7 and l_7 are DPMs but not DIMs, whereas r_7, z_7, and f_7 are all DIMs (see Tables 3.8 ~ 3.12). One notable thing is that the distance expansion distribution of f_7 is better than that of r_7 and z_7, and the total distance of f_7 is the best (equal to that of M_7).

Table 3.8 Distance expansion matrix of h_7.

0	448	0	0	0	0	0
	0	512	832	0	0	0
		0	576	1344	320	0
			0	640	1344	256
				0	704	640
					64	384
						64

Table 3.9 Distance expansion matrix of l_7.

0	384	0	0	6	22	36
	0	516	444	28	128	228
		0	582	658	396	604
			4	524	776	936
				34	436	874
					56	392
						64

Table 3.10 Distance expansion matrix of r_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

Table 3.11 Distance expansion matrix of z_7.

0	384	64	0	0	0	0
	0	352	832	160	0	0
		0	320	1280	576	64
			0	352	1280	608
				0	384	960
					0	448
						64

Table 3.12 Distance expansion matrix of f_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

For $n = 8$, the distance expansion distribution of f_8 is worse than that of r_8 and Q_8 but is better than that of h_8 (see Tables 3.13 ~ 3.16).

Table 3.13 Distance expansion matrix of h_8.

0	1024	0	0	0	0	0	0
	0	1280	2304	0	0	0	0
		0	1600	4160	1408	0	0
			0	1920	4992	1920	128
				0	2240	3840	1088
					128	1792	1664
						192	832
							128

Table 3.14 Distance expansion matrix of r_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

Table 3.15 Distance expansion matrix of Q_8.

0	768	256	0	0	0	0	0
	0	512	2432	512	128	0	0
		0	256	3840	2304	768	0
			0	256	4224	3584	896
				0	512	3840	2816
					0	768	2816
						0	1024
							128

Table 3.16 Distance expansion matrix of z_8 and f_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

For n = 9, we find that large numbers of quantity aggregate on the rightmost column of the distance expansion matrix of f_9 (see Table 3.22). Hence, the distance expansion distribution of f_9 is obviously the best among the six mappings. In addition, $\Delta_1(f_9)$ is the largest among all mappings, including M_9. We also notice that r_9 and z_9 are almost the same except the fourth row (see Table 3.19 and 3.21). The aggregation of quantity in the rightmost column of the distance expansion matrix is a characteristic of f_n for $n \geq 9$ and n is odd (see Tables 3.22, 3.27, and 3.28 for examples). Thus, the distance expansion distribution of f_n is better than that of h_n, l_n, r_n, Q_n, and z_n for $n \geq 9$ and n is odd. Therefore, we conclude that f_n has better distance expansion distribution than these five previously proposed DPMs or DIMs for $n \geq 7$ and n is odd. The total distance of f_n is also better then that of these mappings, but worse than that of M_n for $n \geq 11$ and n is odd. However, f_n is a DIM while M_n is not a DIM.

Table 3.17 Distance expansion matrix of h_9.

0	2304	0	0	0	0	0	0	0
	0	3072	6144	0	0	0	0	0
		0	4160	12096	5248	0	0	0
			0	5376	16384	9472	1024	0
				0	6592	16128	8768	768
					256	6272	11520	3456
						448	4672	4096
							512	1792
								256

Table 3.18 Distance expansion matrix of l_9.

0	2048	0	0	0	0	6	68	182
	0	3076	4092	0	0	40	514	1494
		0	4176	8016	2144	126	1646	5396
			0	4848	9512	3560	3170	11166
				0	4492	7650	5462	14652
					4	3200	5496	12804
						82	1980	7154
							136	2168
								256

Table 3.19 Distance expansion matrix of r_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

Table 3.20 Distance expansion matrix of Q_9.

0	1536	768	0	0	0	0	0	0
	0	896	5568	2368	384	0	0	0
		0	640	7296	10240	3008	320	0
			0	512	8640	15424	7104	576
				0	704	9344	16704	5504
					0	1024	9792	10688
						0	1600	7616
							0	2304
								256

Table 3.21 Distance expansion matrix of z_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	1280	12800	13824	4352	0
				0	1536	12544	14848	3328
					0	1792	11008	8704
						0	2048	7168
							0	2304
								256

Table 3.22 Distance expansion matrix of f_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

Table 3.23 Distance expansion matrix of r_{10}.

0	4096	1024	0	0	0	0	0	0	0
	0	3200	14720	5120	0	0	0	0	0
		0	2304	22784	29184	7168	0	0	0
			0	2560	24320	56192	21376	3072	0
				0	2560	27392	65792	29440	3840
					0	2560	30464	55168	19328
						0	3328	27904	30208
							0	4224	18816
								0	5120
									512

Table 3.24 Distance expansion matrix of Q_{10}.

0	4096	1024	0	0	0		0	0	0
	0	3200	14720	5120	0		0	0	0
		0	2304	22784	29184	7168	0	0	0
			0	2560	24320	56192	21376	3072	0
				0	2560	27392	65792	29440	3840
					0	2560	30464	55168	19328
						0	3328	27904	30208
							0	4224	18816
								0	5120
									512

Table 3.25 Distance expansion matrix of z_{10} and f_{10}.

0	5120	0	0	0	0	0	0	0	0
	0	5120	17920	0	0	0	0	0	0
		0	5120	30720	25600	0	0	0	0
			0	5120	38400	51200	12800	0	0
				0	5120	40960	61400	20480	1024
					0	5120	38400	51200	12800
						0	5120	30720	25600
							0	5120	17920
								0	5120
									512

Table 3.26 Distance expansion matrix of z_{11}.

0	10240	1024	0	0	0	0	0	0	0	0
	0	9728	39936	6656	0	0	0	0	0	0
		0	9216	67584	78848	13312	0	0	0	0
			0	8704	86016	158208	76800	8192	0	0
				0	8192	97280	206848	137216	22528	1024
					0	8704	97280	214528	133120	19456
						0	9216	90112	168960	69632
							0	9728	73728	85504
								0	10240	46080
									0	11264
										1024

Table 3.27 Distance expansion matrix of f_{11}.

0	10240	0	0	0	0	0	0	0	0	1024
	0	9216	36864	0	0	0	0	0	0	10240
		0	8192	57344	57344	0	0	0	0	46080
			0	7168	64512	107520	35840	0	0	122880
				0	6144	61440	122880	61440	6144	215040
					0	5120	51200	102400	51200	263168
						0	4096	36864	61440	235520
							0	3072	21504	144384
								0	2048	54272
									0	11264
										1024

Table 3.28 Distance expansion matrix of f_{13}.

0	49152	0	0	0	0	0	0	0	0	0	0	4096
	0	45056	225280	0	0	0	0	0	0	0	0	49152
		0	40960	368640	491520	0	0	0	0	0	0	270336
			0	36864	442368	1032192	516096	0	0	0	0	901120
				0	32768	458752	1376256	1146880	229376	0	0	2027520
					0	28672	430080	1433600	1433600	430080	28672	3244032
						0	24576	368640	1228800	1228800	368640	3809280
							0	20480	286720	860160	716800	3387392
								0	16384	196608	458752	2256896
									0	12288	110592	1048576
										0	8192	311296
											0	53248
												4096

Table 3.29 List of total distance of various DPMs.

n	$\Delta_{\max}$	h_n	l_n	r_n	Q_n	z_n	M_n	f_n
5	4090	3712	3872	4020*	–	–	3712	3968
6	20472	18432	–	18432	–	18432	19456*	18432
7	98294	83968	91016	88064	–	88064	94208*	94208*
8	458752	378880	–	413312	409600	393216	458752*	393216
9	2097144	1689600	1911000	1802240	1863680	1802240	1982464	1998848*
10	9437160	7281792	–	8110080	8110080	7863680	9043968*	7863680
11	41943022	31923328	37741432	36330496	–	35127296	40108032*	39321600
12	184549344	138878080	–	154927104	–	150994944	180355072*	150994944
13	805306346	600251520	717371576	677117952	–	–	780140544*	746586112

Chapter 4

DPMs from Ternary Vectors

All DPMs and DIMs proposed so far are from binary vectors ([6], [13], [14], [15], [17], [18], [21], [22], [23], [29], [30], [31], [37]) except [19] and [34]. In this chapter, we propose a general construction method that constructs DPMs or DIMs from ternary vectors. That is, the proposed method constructs DPMs or DIMs from Z_3^n to S_N. By using this method, we construct DIMs for $N = n + 2$ for all $n \geq 3$, DPMs for $N = n + 1$ for all $n \geq 9$, as well as DPMs for $N = n$ for all $n \geq 13$.

4.1 The General Recursive Construction

Here we present a recursive construction E that constructs mappings from Z_3^n to S_N. Given a mapping $f_m \in \mathcal{F}(3, m, M)$, $E(f_m) = f_{m+1}$ is a mapping in $\mathcal{F}(3, m+1, M+1)$. That is, the construction "extends" the mapping $f_m : Z_3^m \to S_M$ to the mapping $f_{m+1} : Z_3^{m+1} \to S_{M+1}$. Repeated use of the construction E gives a sequence of mappings $f_{m+2} = E(f_{m+1}) = E(E(f_m)) \in \mathcal{F}(3, m+2, M+2)$, $f_{m+3} = E(f_{m+2}) = E(E(E(f_m)) \in \mathcal{F}(3, m+3, M+3)$, … , and so on. We will show that

i) $f_n \in P(3, n, N)$ for all $n > m$ if $f_m \in P(3, m, M)$.

ii) $f_n \in I(3, n, N)$ for all $n > m$ if $f_m \in I(3, m, M)$ and $M > m$.

iii) $f_n \in P(3, n, N)$ for all $n > m$ if $f_m \in I(3, m, M)$ and $M = m$.

where $N - n = M - m$.

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. For example, let $\mathbf{a} = (5, 3, 2, 4, 6, 1)$, then $\mathbf{a}_5 = 6$.

Construction *E*: For $f \in F(3, n, N)$, define $g = E(f) \in F(3, n+1, N+1)$ as follows. Let $x = (x_1, x_2, \ldots, x_n) \in Z_3^n$ and $f(x) = (\rho_1, \rho_2, \ldots, \rho_N)$. Suppose that the element $N - 4$ occurs in position r, that is $\rho_r = N - 4$. Then

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

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

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

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

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

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

To help the reader understand the construction, we give an alternative algorithmic description in Table 4.1.

Table 4.1 An algorithmic description of Construction E.

```
Algorithm of Construction E
Input: $x = (x_1, x_2, \ldots, x_{n+1}) \in Z_3^{n+1}$
Output: $(\mu_1, \mu_2, \ldots, \mu_{N+1}) = g(x)$
Begin
    $(\rho_1, \rho_2, \ldots, \rho_N) \leftarrow f(x_1, x_2, \ldots, x_n)$;
    $(\mu_1, \mu_2, \ldots, \mu_N, \mu_{N+1}) \leftarrow (\rho_1, \rho_2, \ldots, \rho_N, N + 1)$
    Case $x_{n+1} = 1$:
        $r \leftarrow \mu^{-1}(N - 4)$;
        swap $(\mu_r, \mu_{N+1})$;
    Case $x_{n+1} = 2$:
        If ($n$ is odd) and ($x_n = 2$) then swap $(\mu_{N-1}, \mu_{N+1})$;
        Else swap $(\mu_N, \mu_{N+1})$;
End
```

Example 4.1 Let $f(0,0,0) = (1,2,3,4,5)$. By Construction 4.1, we have

$$g(0,0,0,0) = (1,2,3,4,5,6),$$
$$g(0,0,0,1) = (6,2,3,4,5,1),$$
$$g(0,0,0,2) = (1,2,3,4,6,5).$$

Furthermore, let $h = E(g)$, we have

$$h(0,0,0,0,0) = (1,2,3,4,5,6,7),$$
$$h(0,0,0,0,1) = (1,7,3,4,5,6,2),$$
$$h(0,0,0,0,2) = (1,2,3,4,5,7,6),$$
$$h(0,0,0,1,0) = (6,2,3,4,5,1,7),$$
$$h(0,0,0,1,1) = (6,7,3,4,5,1,2),$$
$$h(0,0,0,1,2) = (6,2,3,4,5,7,1),$$
$$h(0,0,0,2,0) = (1,2,3,4,6,5,7),$$
$$h(0,0,0,2,1) = (1,7,3,4,6,5,2),$$
$$h(0,0,0,2,2) = (1,2,3,4,7,5,6).$$

For $f \in \mathcal{F}(3, m, M)$, we define a sequence of mappings $f_n \in \mathcal{F}(3, n, n + M - m)$, for all $n \geq m$, recursively by

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

Now we show that based on an initial mapping $f \in \mathcal{P}(3, m, M)$, $f_n \in \mathcal{P}(3, n, n + M - m)$ for all $n > m$. Furthermore, if f is a DIM, i.e. $f \in \mathcal{I}(3, m, M)$, then $f_n \in \mathcal{I}(3, n, n + M - m)$ or $f_n \in \mathcal{P}(3, n, n + M - m)$ for all $n > m$.

Lemma 4.1 If $f_m \in \mathcal{P}(3, m, M)$, m is odd, and $f_m(x)_M \neq M - 4$ for all $x \in Z_3^m$. Then $f_{m+1} \in \mathcal{P}(3, m + 1, M + 1)$.

The proof of Lemma 4.1 is similar to that of the following lemma (and a little simpler). Thus, we omit the proof.

Lemma 4.2 If $f_m \in \mathcal{I}(3, m, M)$, m is odd, and $f_m(x)_M \neq M - 4$ for all $x \in Z_3^m$. Then

i) $f_{m+1} \in \mathcal{I}(3, m + 1, M + 1)$ if $M > m$, or

ii) $f_{m+1} \in \mathcal{P}(3, m + 1, M + 1)$ if $M = m$.

Proof. For every two distinct vectors $x = (x' \,|\, x_{m+1})$, $y = (y' \,|\, y_{m+1})$ in Z_3^{m+1} where x', y' $\in Z_3^m$, consider the following cases.

Table 4.2 Possible cases for two distinct vectors in Z_3^{m+1}.

	$y_{m+1} = 0$	$y_{m+1} = 1$	$y_{m+1} = 2$
$x_{m+1} = 0$	Case 1	Case 2	Case 3
$x_{m+1} = 1$	Case 4	Case 5	Case 6
$x_{m+1} = 2$	Case 7	Case 8	Case 9

i) $M > m$:

Case 1, 5, 9:
$$\begin{aligned} d_H(f_{m+1}(x), f_{m+1}(y)) &= d_H(f_m(x'), f_m(y')) \\ &> d_H(x', y') \\ &= d_H(x, y). \end{aligned}$$

Case 2: $f_{m+1}(x)_{M+1} = M + 1 \neq f_{m+1}(y)_{M+1} = M - 4$; $f^k_{m+1}(y)_r = M + 1$ and $f_{m+1}(x)_r \neq M + 1$ where $r = f_m(y')^{-1}(M-4)$. Thus,

$$\begin{aligned} d_H(f_{m+1}(x), f_{m+1}(y)) &\geq d_H(f_m(x'), f^k_m(y')) + 1 \\ &> d_H(x', y') + 1 \\ &= d_H(x, y). \end{aligned}$$

Case 3, 4, 7: similar to Case 2.

Case 6: Table 4.3 illustrates the values of $f_m(x')_i$, $f_m(y')_i$, $f_{m+1}(x)_i$, and $f_{m+1}(y)_i$ for $i = r$, M, and $M + 1$ respectively. In the table we see that $f_{m+1}(x)_{M+1} = M - 4$ and $f_{m+1}(y)_{M+1} = f_m(y')_M \neq M - 4$ (by the fact that $f_m(x')_M \neq M - 4$); $f_{m+1}(x)_r = M + 1$ and $f_{m+1}(y)_r = f_m(y')_r \neq M + 1$ where $r = f_m(x')^{-1}(M-4)$ and $r < M$; $f_{m+1}(y)_M = M + 1$ and $f_{m+1}(x)_M = f_m(x')_M \neq M + 1$. Thus,

$$\begin{aligned} d_H(f_{m+1}(x), f_{m+1}(y)) &\geq d_H(f_m(x'), f^k_m(y')) + 1 \\ &> d_H(x', y') + 1 \\ &= d_H(x, y). \end{aligned}$$

Table 4.3 List of some values of f_m and f_{m+1} in the case of $x_{m+1} = 1$ and $y_{m+1} = 2$.

i	$f_m(x')_i$	$f_m(y')_i$	$f_{m+1}(x)_i$	$f_{m+1}(y)_i$
r	$M-4$	$f_m(y')_r$	$M+1$	$f_m(y')_r$
M	$f_m(x')_M$	$f_m(y')_M$	$f_m(x')_M$	$M+1$
$M+1$	–	–	$M-4$	$f_m(y')_M$

Case 8: similar to Case 6.

In all cases, $d_H(f_{m+1}(x), f_{m+1}(y)) > d_H(x, y)$. Thus,

$$f_{m+1} \in I(3, m+1, M+1).$$

ii) $M = m$:

The proof is similar to i) except in Case 1, 5, and 9, when $d_H(x', y') = m$,

$$\begin{aligned} d_H(f_{m+1}(x), f_{m+1}(y)) &= d_H(f_m(x'), f_m(y')) \\ &= d_H(x', y') = d_H(x, y) \\ &< m + 1, \end{aligned}$$

which means that f_{m+1} is possible to increase the distance but it just preserves the distance. Thus,

$$f_{m+1} \in P(3, m+1, M+1). \qquad \square$$

Theorem 4.1 If $f_m \in P(3, m, M)$, m is odd, and $f_m(x)_M \notin \{M-3, M-4\}$ for all $x \in Z_3^m$, then $f_n \in P(3, n, n+M-m)$ for all $n > m$.

We omit the proof of Theorem 4.1 since it is similar to that of the following theorem (and a little simpler).

Theorem 4.2 If $f_m \in I(3, m, M)$, m is odd, and $f_m(x)_M \notin \{M-3, M-4\}$ for all $x \in Z_3^m$. Then

i) $f_n \in I(3, n, N)$ for all $n > m$ if $M > m$, or

ii) $f_n \in P(3, n, N)$ for all $n > m$ if $M = m$.

where $N = n + M - m$.

Proof. i) $M > m$: The proof is done by induction. We have proved that $f_n \in I(3, n, N)$ for $n = m + 1$ in Lemma 4.2. For $n \geq m + 2$, suppose that $f_{n-1} \in I(3, n-1, N-1)$. For any two distinct vectors $x = (x' \mid x_n)$, $y = (y' \mid y_n)$ in Z_3^n where $x', y' \in Z_3^{n-1}$, consider the cases listed in Table 4.2.

Case 1, 5, 9: $d_H(f_n(x), f_n(y)) > d_H(x, y)$ (similar to Lemma 4.2).

Case 2, 3, 4, 7: $d_H(f_n(x), f_n(y)) > d_H(x, y)$ (similar to Lemma 4.2).

Case 6: Since $x_n = 1$, we have $f_n(x)_N = (N-1) - 4 = N - 5$. Furthermore, $y_n = 2$

(a) If n is even, then

$$f_n(y)_N = f_{n-1}(y')_{N-1} = \begin{cases} N-1 & \text{if } y_{n-1} = 0, \\ N-6 & \text{if } y_{n-1} = 1, \\ N-2 \text{ or } N-7 & \text{if } y_{n-1} = 2. \end{cases}$$

Thus, $f_n(x)_N \neq f_n(y)_N$. Besides, $f_n(y)_{N-1} = N$ and $f_n(x)_{N-1} \neq N$ (by the fact that $f_m(x_1, \ldots, x_m)_M \notin \{M-3, M-4\}$).

(b) If n is odd, then

$$f_n(y)_N = \begin{cases} f_{n-1}(y')_{N-1} = N-1 & \text{if } y_{n-1} = 0, \\ f_{n-1}(y')_{N-1} = N-6 & \text{if } y_{n-1} = 1, \\ f_{n-1}(y')_{N-2} = N-1 & \text{if } y_{n-1} = 2. \end{cases}$$

Thus, $f_n(x)_N \neq f_n(y)_N$. Furthermore, if $y_{n-1} = 2$, then

$f_n(y)_{N-2} = N$ and $f_n(x)_{N-2} \neq N$ (also by the fact that

$f_m(x_1, \ldots, x_m)_M \notin \{M-3, M-4\}$).

Otherwise ($y_{n-1} \neq 2$),

$$f_n(y)_{N-1} = N \text{ and } f_n(x)_{N-1} \neq N.$$

Besides, $f_n(x)_r = N$ and $f_n(y)_r \neq N$ where $r = f_{n-1}(x')^{-1}(N-5)$ and $r < N - 1$ if n is even, or $r < N - 2$ if n is odd. Therefore,

$$\begin{aligned} d_H(f_n(x), f_n(y)) &\geq d_H(f_{n-1}(x'), f_{n-1}(y')) + 1 \\ &> d_H(x', y') + 1 \\ &= d_H(x, y). \end{aligned}$$

Table 4.4 gives a summarization of possible values of $f_n(x)_N$ for all $n > m$.

Case 8: similar to Case 6.

In all cases, $d_H(f_n(x), f_n(y)) > d_H(x, y)$. Thus, $f_n \in I(3, n, N)$.

ii) $M = m$: Since $f_{m+1} \in P(3, m + 1, M + 1)$ (proved in Lemma 4.1), similar to the above proof, we have $f_n \in P(3, n, N)$ for all $n > m$. □

Table 4.4 Possible values of $f_n(x)_N$ for all $n > m$.

x_n	x_{n-1}	$f_n(x)_N$	
		$n = m + 1$	$n \geq m + 2$
0		$N + 1$	N
1		$N - 4$	$N - 5$
2	0	$f_m(x)_M$	$N - 1$
	1		$N - 6$
	2		$N - 1$ $N - 2$ $N - 7$

The recursive construction E can be generalized. In the construction E we defined r by $\rho_r = N - 4$. The recursion would work equally well if we defined r by

$\rho_r = N - t$ for some fixed $t \geq 3$ and changed the conditions in the lemmas and theorems to

$$f_m(x)_M \notin \{ M - (t-1), M - t \}. \tag{4.1}$$

Because if we list the last three symbols in $f_{m+2} = E(E(f_m))$ as follows,

Table 4.5 Listing the last three symbols in $f_{m+2} = E(E(f_m))$.

x_{m+1}	x_{m+2}	$f_{m+2}(x)_M$	$f_{m+2}(x)_{M+1}$	$f_{m+2}(x)_{M+2}$
0	0	ρ_M	$M+1$	$M+2$
1	0	ρ_M	$M-t$	$M+2$
2	0	$M+1$	ρ_M	$M+2$
1	1	ρ_M	$M+1$	$M-(t-1)$
1	1	ρ_M	$M-t$	$M-(t-1)$
2	1	$M+1$	ρ_M	$M-(t-1)$
0	2	ρ_M	$M+2$	$M+1$
1	2	ρ_M	$M+2$	$M-t$
2	2	$M+2$	ρ_M	$M+1$

then, in order to make f_{m+2} suitable for subsequent recursions, we have

$$M + 2 - (t-1) \notin \{M+1, M+2, M-t, M-(t-1)\}, \text{ and}$$
$$M + 2 - t \notin \{ M+1, M+2, M-t, M-(t-1) \}.$$

Note that $m + 2$ is odd since m is odd. Hence, $t \notin \{0, 1, 2\}$.

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

$$\begin{aligned} &N - t \neq f_n(x)_N && \text{if } n \text{ is odd,} \\ &N - t \notin \{f_n(x)_{N-1}, f_n(x)_N\} && \text{if } n \text{ is even.} \end{aligned} \tag{4.2}$$

One reason we chose a fixed t is that if the condition (4.1) is satisfied at the start of the recursion, then (4.2) is satisfied for all $n \geq m$.

4.2 DIMs from Z_3^n to S_{n+2}

Now we construct DIMs from Z_3^n to S_{n+2} by using Construction *E*. According to Theorem 4.2, all we have to do is to find a suitable initial mapping $f \in I(3, n, n+2)$ for some odd n such that

$$f(x)_{n+2} \notin \{(n+2)-3, (n+2)-4\} \text{ for all } x \in Z_3^n .$$

We construct DIMs in $I(3, n, n+2)$ because, in contrast to $I(3, n, n+1)$ and $I(3, n, n)$, it is easier to find such an initial mapping. In fact, $I(3, n, n+2)$ is not empty for $n = 1$ and $n = 2$. For example, Table 4.6 exhibits a DIM $g \in I(3, 1, 3)$ and Table 4.7 shows a DIM $h \in I(3, 2, 4)$, respectively.

Table 4.6 The mapping table and the distance expansion matrix of $g \in I(3, 1, 3)$.

x	$g(x)$	x	$g(x)$	x	$g(x)$
(0)	(1,2,3)	(1)	(2,3,1)	(2)	(3,1,2)

0	0	3

Table 4.7 The mapping tables and the distance expansion matrix of $h \in I(3, 2, 4)$.

x	$h(x)$	x	$h(x)$	x	$h(x)$
(0,1)	(1,2,3,4)	(0,1)	(4,2,3,1)	(0,2)	(1,4,3,2)
(1,0)	(2,3,1,4)	(1,1)	(2,3,4,1)	(1,2)	(4,3,1,2)
(2,0)	(3,1,2,4)	(2,1)	(3,4,2,1)	(2,2)	(3,1,4,2)

0	6	12	0
		3	15

However, neither g nor h can be a suitable initial mapping for Construction E. Here we define a DIM $f_3 \in \boldsymbol{I}(3, 3, 5)$ which is suitable for Construction E to construct a sequence of DIMs in $\boldsymbol{I}(3, n, n + 2)$ for all $n > 3$. That is, $f_3(x)_5 \notin \{1, 2\}$ for all $x \in Z_3^n$. f_3 is obtained by the algorithm listed in Table 4.10.

The mapping f_3 is listed in Table 4.8. From the mapping table we see that $f_3(x)_5 \notin \{1, 2\}$ for all $x \in Z_3^3$. In addition, the distance expansion matrix listed in Table 4.9 shows that f_3 is distance increasing. Hence, f_3 is suitable for Construction E to construct a sequence of DIMs in $\boldsymbol{I}(3, n, n + 2)$ for all $n > 3$. Based on this result and the examples given in Table 4.6 and Table 4.7, we have the following result.

Theorem 4.3 $\boldsymbol{I}(3, n, n + 2)$ is not empty for $n \geq 1$.

Table 4.8 Mapping table of $f_3 \in \boldsymbol{I}(3, 3, 5)$.

x	$f_3(x)$	x	$f_3(x)$	x	$f_3(x)$
(0,0,0)	(1,2,3,4,5)	(0,0,1)	(1,2,5,4,3)	(0,0,2)	(1,2,3,5,4)
(1,0,0)	(2,3,1,4,5)	(1,0,1)	(2,5,1,4,3)	(1,0,2)	(2,3,1,5,4)
(2,0,0)	(3,1,2,4,5)	(2,0,1)	(5,1,2,4,3)	(2,0,2)	(3,1,2,5,4)
(0,1,0)	(4,2,3,1,5)	(0,1,1)	(4,2,5,1,3)	(0,1,2)	(5,2,3,1,4)
(1,1,0)	(2,3,4,1,5)	(1,1,1)	(2,5,4,1,3)	(1,1,2)	(2,3,5,1,4)
(2,1,0)	(3,4,2,1,5)	(2,1,1)	(5,4,2,1,3)	(2,1,2)	(3,5,2,1,4)
(0,2,0)	(1,4,3,2,5)	(0,2,1)	(1,4,5,2,3)	(0,2,2)	(1,5,3,2,4)
(1,2,0)	(4,3,1,2,5)	(1,2,1)	(4,5,1,2,3)	(1,2,2)	(5,3,1,2,4)
(2,2,0)	(3,1,4,2,5)	(2,2,1)	(5,1,4,2,3)	(2,2,2)	(3,1,5,2,4)

Table 4.9 Distance expansion matrix of f_3 .

0	36	45	0	0
	0	27	111	24
		0	18	90

Table 4.10 Construction algorithm for f_3 .

```
**Construction algorithm for** $f_3$
**Input:** $(x_1, x_2, x_3) \in Z_3^3$
**Output:** $(\varphi_1, \varphi_2, \ldots, \varphi_5) = f_3(x_1, x_2, x_3)$
**Begin**
    **case** $x_1 = 0$:
        $(\varphi_1, \varphi_2, \ldots, \varphi_5) \leftarrow (1, 2, 3, 4, 5)$;
    **case** $x_1 = 1$:
        $(\varphi_1, \varphi_2, \ldots, \varphi_5) \leftarrow (2, 3, 1, 4, 5)$;
    **case** $x_1 = 2$:
        $(\varphi_1, \varphi_2, \ldots, \varphi_5) \leftarrow (3, 1, 2, 4, 5)$;
    **case** $x_2 = 1$:
        $i \leftarrow \pi^{-1}(1)$;
        swap $(\varphi_i, \varphi_4)$;
    **case** $x_2 = 2$:
        $i \leftarrow \pi^{-1}(2)$;
        swap $(\varphi_i, \varphi_4)$;
    **case** $x_3 = 1$:
        $i \leftarrow \pi^{-1}(3)$;
        swap $(\varphi_i, \varphi_5)$;
    **case** $x_3 = 2$:
        $i \leftarrow \pi^{-1}(4)$;
        swap $(\varphi_i, \varphi_5)$;
**End**
```

Example 4.2 We construct $f_4 \in I(3, 4, 6)$ and $f_5 \in I(3, 5, 7)$ from f_3 . The distance expansion matrices of f_4 and f_5 are listed in Table 4.11 and Table 4.12, respectively.

Table 4.11 Distance expansion matrix of $f_4 \in I(3, 4, 6)$.

0	162	162	0	0	0
	0	135	549	270	18
		0	144	720	432
			0	108	540

Table 4.12 Distance expansion matrix of $f_5 \in I(3, 5, 7)$.

0	648	540	27	0	0	0
	0	567	2457	1584	234	18
		0	630	3828	4224	1038
			0	720	4500	4500
				0	648	3240

4.3 DPMs from Z_3^n to S_{n+1}

To construct DPMs from Z_3^n to S_{n+1}, using Construction E, we need a mapping $f \in P(3, n, n + 1)$ as an initial mapping such that

$$f(x)_{n+1} \notin \{(n+1)-3, (n+1)-4\} \text{ for all } x \in Z_3^n .$$

Finding an initial mapping in $P(3, n, n + 1)$ is a tough work. For a DPM $f : Z_3^n \to S_{n+1}$ to be existing, $n \geq 4$ is a necessary condition since

$$4! = 24 < 3^3 = 27 \text{ and } 5! = 120 > 3^4 = 81.$$

In the beginning, we tried to find such a mapping by computer search. Unfortunately, an extensive computer search has been unsuccessful. In our experiment, computer search is almost infeasible due to the large search space. As a result, we tried some other approaches. Finally, an indirect approach has been successful. This approach is to construct f from two simpler mappings found by computer search.

For a vector $\mathbf{u} = (u_1, u_2, \dots, u_n)$, and a set $\boldsymbol{X} \subset \{1, 2, \dots, n\}$, let $\mathbf{u}_{\backslash \boldsymbol{X}}$ denote the vector obtained from $\mathbf{u}$ by removing the elements with subscript in $\boldsymbol{X}$. For example,

$$(u_1, u_2, u_3, u_4, u_5, u_6)_{\backslash \{1,5\}} = (u_2, u_3, u_4, u_6).$$

By computer search we have found mappings $G \in F(3, 5, 7)$ and $H \in F(3, 4, 6)$ that satisfy the following conditions:

i) For every $x \in Z_3^5$, $6 \in \{G(x)_1, G(x)_2, G(x)_3\}$,

ii) For every $x \in Z_3^5$, $7 \in \{G(x)_4, G(x)_5, G(x)_6\}$,

iii) For every distinct $x, y \in Z_3^5$, $d_H(G(x)_{\backslash\{7\}}, G(y)_{\backslash\{7\}}) \ge d_H(x, y)$,

iv) For every $u \in Z_3^4$, $1 \in \{H(x)_1, H(x)_2, H(x)_3\}$,

v) For every distinct $u, v \in Z_3^4$, $d_H(H(u)_{\backslash\{5,6\}}, H(v)_{\backslash\{5,6\}}) \ge d_H(u, v)$.

The mappings G and H are listed explicitly in Appendix B. We will now show how these mappings can be combined to produce a mapping $f \in P(3, 9, 10)$ satisfying

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

Construction 4.2 Construction of $f \in P(3, 9, 10)$.

Let $x \in Z_3^9$ and $x = (x_L, x_R)$ where $x_L \in Z_3^5$ and $x_R \in Z_3^4$. In addition, let

$$\varphi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \varphi_7) = G(x_L),$$
$$\gamma = (\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6) = H(x_R) + (4, 4, 4, 4, 4, 4).$$

Note that Condition iv) implies that $\gamma_5 \geq 6$ and $\gamma_6 \geq 6$. Similarly, Condition i) and ii) imply that $\varphi_7 \leq 5$.

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

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

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

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

Then define

$$f(x) = \pi.$$

In order to help the reader understand the combination, we give an alternative algorithmic description in Table 4.13.

Example 4.3 Let $G(0,1,0,1,2) = (6,5,2,1,7,4,3)$ and $H(0,1,0,2) = (1,5,3,2,4,6)$. Then

$$\varphi = (6, 5, 2, 1, 7, 4, 3),$$

$\gamma = (5, 9, 7, 6, 8, 10)$,

$\rho = (8, 5, 2, 1, 10, 4, 3, 9, 7, 6)$, and

$f(0, 1, 0, 1, 2, 0, 1, 0, 2) = (8, 5, 7, 6, 10, 4, 3, 9, 2, 1)$.

Table 4.13 An algorithmic description of the construction of $f \in P(3, 9, 10)$.

```
Combining algorithm for the initial mapping $f \in P(3, 9, 10)$
Input: $x = (x_1, x_2, \dots, x_9) \in Z_3^9$
Output: $(\pi_1, \pi_2, \dots, \pi_{10}) = f(x_1, x_2, \dots, x_9)$
Begin
    $\varphi : (\varphi_1, \varphi_2, \dots, \varphi_7) \leftarrow G(x_1, x_2, x_3, x_4, x_5)$;
    $(\phi_1, \phi_2, \dots, \phi_6) \leftarrow H(x_6, x_7, x_8, x_9)$;
    $\gamma : (\gamma_1, \gamma_2, \dots, \gamma_6) \leftarrow (\phi_1 + 4, \phi_2 + 4, \phi_3 + 4, \phi_4 + 4, \phi_5 + 4, \phi_6 + 4)$;
    $i \leftarrow \gamma^{-1}(5)$;
    $j \leftarrow \varphi^{-1}(6)$;
    $k \leftarrow \varphi^{-1}(7)$;
    $\gamma_i \leftarrow \varphi_7$;
    $\varphi_j \leftarrow \gamma_5$;
    $\varphi_k \leftarrow \gamma_6$;
    $\rho : (\rho_1, \rho_2, \dots, \rho_{10}) \leftarrow (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \gamma_1, \gamma_2, \gamma_3, \gamma_4)$;
    $i \leftarrow \rho^{-1}(1)$;
    $j \leftarrow \rho^{-1}(2)$;
    $k \leftarrow \rho^{-1}(6)$;
    $l \leftarrow \rho^{-1}(7)$;
    swap $(\rho_i, \rho_k)$;
    swap $(\rho_j, \rho_l)$;
    $\pi : (\pi_1, \pi_2, \dots, \pi_{10}) \leftarrow (\rho_1, \rho_2, \dots, \rho_{10})$;
End
```

Now we show that f has the started property.

Lemma 4.3 $f \in P(3, 9, 10)$ and $f(x)_{10} \notin \{6, 7\}$ for every $x \in Z_3^9$.

Proof. 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 remove another element (γ_5) into the position where φ has a 6. Similarly, the second line overwrites the 7 in φ, 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 four first (overwritten) elements of γ. Therefore, ρ contains no duplicate elements, that is, $\rho \in S_{10}$. And so $\pi \in S_{10}$.

The element 1 in ρ must be in any one of the first six positions, coming from φ, or in one of the positions 7, 8, or 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 positions of π, that is $\pi_{10} \notin \{6, 7\}$.

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

$$\begin{aligned} d_H(x, x') &= d_H(x_L, x'_L) + d_H(x_R, x'_R) \\ &\leq d_H(\varphi_{\setminus\{7\}}, \varphi'_{\setminus\{7\}}) + d_H(\gamma_{\setminus\{5,6\}}, \gamma'_{\setminus\{5,6\}}). \end{aligned} \tag{4.3}$$

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

$$d_H(\varphi_i, \varphi'_i) \leq d_H(\rho_i, \rho'_i). \tag{4.4}$$

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 the proof of (4.4). A similar argument shows that for $7 \leq i \leq 10$ we have

$$d_H(\gamma_{i-6}, \gamma'_{i-6}) \leq d_H(\rho_i, \rho'_i), \tag{4.5}$$

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

$$d_H(\rho_i, \rho'_i) \leq d_H(\pi_i, \pi'_i). \tag{4.6}$$

Combining (4.3) – (4.6), we get

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

Hence, f is distance preserving. □

Table 4.14 lists the distance expansion matrix of f. With f as an initial mapping, we can prove the following theorem with Theorem 4.1.

Theorem 4.4: $P(3, 9, 10)$ is not empty for $n \geq 9$.

Table 4.14 Distance expansion matrix of $f \in P(3, 9, 10)$.

0	51354	41391	45441	33210	5751	0	0	0	0
	34344	112865	269143	323206	291836	192492	124626	57474	11190
		53806	366311	958353	1434482	1568770	1297158	739170	195438
			140255	910577	2837002	4931228	5640290	4032984	1348128
				310621	2275959	7345554	12583794	12049018	5115982
					698738	4980708	14847858	20652244	11728356
						1258982	8380434	19598010	16112206
							1675300	8824024	12175492
								1191024	3847824

4.4 DPMs from Z_3^n to S_n

For a DPM $f : Z_3^n \to S_n$ to be existing, $n \geq 7$ is a necessary condition since

$$6! = 720 < 3^6 = 729 \text{ and } 7! = 5040 > 3^7 = 2187.$$

Like the construction of $\mathcal{P}(3, n, n + 1)$, we cannot find an initial mapping by simply searching a DPM from Z_3^n to S_n. Hence, similar to the previous section, we construct an initial mapping by an indirect approach. However, the construction is more involved and contains several steps. We will describe the constructions of the intermediate mappings and the desired initial mapping $f \in \mathcal{P}(3, 13, 13)$. The properties of the intermediate mappings and the started property of the mapping f will also be shown.

We start with three mappings R, $S \in \mathcal{F}(3, 3, 5)$ and $T \in \mathcal{F}(3, 4, 6)$. These mappings were found by computer search and are used as building blocks for the constructions of the intermediate mappings. They have the following properties:

i) For every $x \in Z_3^3$, $1 \in \{R(x)_1, R(x)_2, R(x)_3\}$,

ii) For every $x \in Z_3^3$, $R(x)_5 \neq 5$,

iii) For every distinct $x, y \in Z_3^3$, $d_H(R(x)_{\setminus\{4,5\}}, R(y)_{\setminus\{4,5\}}) \geq d_H(x, y)$,

iv) For every $x \in Z_3^3$, $2 \in \{S(x)_1, S(x)_2, S(x)_3\}$,

v) For every $x \in Z_3^3$, $S(x)_5 \neq 1$,

vi) For every distinct $x, y \in Z_3^3$, $d_H(S(x)_{\setminus\{4,5\}}, S(y)_{\setminus\{4,5\}}) \geq d_H(x, y)$,

vii) For every $x \in Z_3^4$, $2 \in \{T(x)_1, T(x)_2, T(x)_3\}$,

viii) For every $x \in Z_3^4$, $T(x)_6 \neq 1$,

ix) For every distinct $x, y \in Z_3^4$, $d_H(T(x)_{\setminus\{5,6\}}, T(y)_{\setminus\{5,6\}}) \geq d_H(x, y)$.

The mappings R, S, and T are listed explicitly in Appendix B. Based on these mappings, we construct two mapping $U \in \mathcal{F}(3, 6, 8)$ and $V \in \mathcal{F}(3, 7, 9)$ where U is obtained by combining R with S, and V is obtained by combining R with T, respectively.

Construction 4.3 Construction of $U \in \mathcal{F}(3, 6, 8)$.

Let $x \in Z_3^6$ and let

$$\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = R(x_1, x_2, x_3),$$
$$\beta = (\beta_1, \beta_2, \beta_3, \beta_4, \beta_5) = S(x_4, x_5, x_6) + (3, 3, 3, 3, 3).$$

Define $\eta = (\eta_1, \eta_2, \dots, \eta_8)$ as follows.

$$\begin{array}{llll}
\eta_i = \beta_5 & \text{if } 1 \le i \le 4 & \text{and} & \alpha_i = 5 \\
\eta_i = \alpha_i & \text{if } 1 \le i \le 4 & \text{and} & \alpha_i \ne 5, \\
\eta_i = \alpha_5 & \text{if } 5 \le i \le 8 & \text{and} & \beta_{i-4} = 4, \\
\eta_i = \beta_{i-4} & \text{if } 5 \le i \le 8 & \text{and} & \beta_{i-4} \ne 4.
\end{array}$$

In η, swap 1 and 7 and also swap 5 and 8, and let the resulting array be denoted by σ. Then define $U(x) = \sigma$.

Construction 4.4 Construction of $V \in \mathcal{F}(3, 7, 9)$.

Let $x \in Z_3^7$ and let

$$\lambda = (\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = R(x_1, x_2, x_3),$$
$$\theta = (\theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6) = T(x_4, x_5, x_6, x_7) + (3, 3, 3, 3, 3, 3).$$

Define $\mu = (\mu_1, \mu_2, \dots, \mu_9)$ as follows:

$$\begin{array}{llll}
\mu_i = \theta_6 & \text{if } 1 \le i \le 4 & \text{and} & \lambda_i = 5 \\
\mu_i = \lambda_i & \text{if } 1 \le i \le 4 & \text{and} & \lambda_i \ne 5, \\
\mu_i = \lambda_5 & \text{if } 5 \le i \le 9 & \text{and} & \theta_{i-4} = 4, \\
\mu_i = \theta_{i-4} & \text{if } 5 \le i \le 9 & \text{and} & \theta_{i-4} \ne 4.
\end{array}$$

In μ, swap 2 and 5, and let the resulting array be denoted by τ. Then define $V(x) = \tau$.

In order to help the reader understand the constructions, we give alternative algorithmic descriptions for Constructions 4.3 and 4.4 in Tables 4.15 and 4.16, respectively.

Table 4.15 An algorithmic description of the construction of $U \in F(3, 6, 8)$.

```
Combining algorithm for U ∈ F(3, 6, 8)
Input: $x = (x_1, x_2, \dots, x_6) \in Z_3^6$
Output: $(\sigma_1, \sigma_2, \dots, \sigma_8) = U(x_1, x_2, \dots, x_6)$
Begin
    $\alpha : (\alpha_1, \alpha_2, \dots, \alpha_5) \leftarrow R(x_1, x_2, x_3)$;
    $(\phi_1, \phi_2, \dots, \phi_5) \leftarrow S(x_4, x_5, x_6)$;
    $\beta : (\beta_1, \beta_2, \dots, \beta_5) \leftarrow (\phi_1 + 3, \phi_2 + 3, \phi_3 + 3, \phi_4 + 3, \phi_5 + 3)$;
    $i \leftarrow \beta^{-1}(4)$;
    $j \leftarrow \alpha^{-1}(5)$;
    $\beta_i \leftarrow \alpha_5$;
    $\alpha_j \leftarrow \beta_5$;
    $\eta : (\eta_1, \eta_2, \dots, \eta_8) \leftarrow (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta_1, \beta_2, \beta_3, \beta_4)$;
    $i \leftarrow \eta^{-1}(1)$;
    $j \leftarrow \eta^{-1}(5)$;
    $k \leftarrow \eta^{-1}(7)$;
    $l \leftarrow \eta^{-1}(8)$;
    swap $(\eta_i, \eta_k)$;
    swap $(\eta_j, \eta_l)$;
    $\sigma : (\sigma_1, \sigma_2, \dots, \sigma_8) \leftarrow (\eta_1, \eta_2, \dots, \eta_8)$;
End
```

Table 4.16 An algorithmic description of the construction of $V \in F(3, 7, 9)$.

```
Combining algorithm for $V \in F(3, 7, 9)$
Input: $x = (x_1, x_2, \dots, x_7) \in Z_3^7$
Output: $(\tau_1, \tau_1, \dots, \tau_9) = V(x_1, x_2, \dots, x_7)$
Begin
1.    $\lambda : (\lambda_1, \lambda_2, \dots, \lambda_5) \leftarrow R(x_1, x_2, x_3)$;
2.    $(\phi_1, \phi_2, \dots, \phi_6) \leftarrow T(x_4, x_5, x_6, x_7)$;
3.    $\theta : (\theta_1, \theta_2, \dots, \theta_6) \leftarrow (\phi_1 + 3, \phi_2 + 3, \phi_3 + 3, \phi_4 + 3, \phi_5 + 3, \phi_6 + 3)$;
4.    $i \leftarrow \theta^{-1}(4)$;
5.    $j \leftarrow \lambda^{-1}(5)$;
6.    $\theta_i \leftarrow \lambda_5$;
7.    $\lambda_j \leftarrow \theta_6$;
8.    $\mu : (\mu_1, \mu_2, \dots, \mu_9) \leftarrow (\lambda_1, \lambda_2, \lambda_3, \lambda_4, \theta_1, \theta_2, \theta_3, \theta_4, \theta_5)$;
9.    $i \leftarrow \mu^{-1}(2)$;
10.   $j \leftarrow \mu^{-1}(5)$;
11.   swap $(\mu_i, \mu_j)$;
12.   $\tau : (\tau_1, \tau_2, \dots, \tau_9) \leftarrow (\mu_1, \mu_2, \dots, \mu_9)$
End
```

Example 4.4 Let $R(0, 1, 0) = (1, 2, 4, 5, 3)$ and $S(1, 0, 2) = (1, 2, 3, 5, 4)$. Then

$$\alpha = (1, 2, 4, 5, 3),$$

$$\beta = (4, 5, 6, 8, 7),$$

$$\eta = (1, 2, 4, 7, 3, 5, 6, 8), \text{ and}$$

$$U(0, 1, 0, 1, 0, 2) = (7, 2, 4, 1, 3, 8, 6, 5).$$

Example 4.5 Let $R(0, 1, 0) = (1, 2, 4, 5, 3)$ and $T(1, 0, 2, 2) = (4, 2, 1, 6, 5, 3)$. Then

$$\lambda = (1, 2, 4, 5, 3),$$
$$\theta = (4, 2, 1, 6, 5, 3),$$
$$\mu = (1, 2, 4, 6, 7, 5, 3, 9, 8), \text{ and}$$
$$V(0, 1, 0, 1, 0, 2, 2) = (1, 5, 4, 6, 7, 2, 3, 9, 8).$$

The intermediate mappings U and V have the following properties which are important to the construction of the initial mapping $f \in P(3, 13, 13)$.

Lemma 4.4

i) For every $x \in Z_3^6$, $7 \in \{U(x)_1, U(x)_2, U(x)_3\}$,

ii) For every $x \in Z_3^6$, $8 \in \{U(x)_5, U(x)_6, U(x)_7\}$,

iii) For every distinct $x, y \in Z_3^6$, $d_H(U(x)_{\backslash\{4,8\}}, U(y)_{\backslash\{4,8\}}) \geq d_H(x, y)$,

Proof. We first show that $\sigma \in S_8$. We have $\alpha \in S_5$ and β is a permutation of (4, 5, 6, 7, 8). In particular, 4 and 5 appear both in α and β. The effect of the first line in the definition of η is to remove another element (β_5) into the position where α has a 5. Similarly, the third line overwrites the 4 in β. Note that $\alpha_5 \neq 5$ and $\beta_5 \neq 4$. The definition of η is then the concatenation of the four first (overwritten) elements of α and the four first (overwritten) elements of β. Therefore, η contains no duplicate elements, that is, $\eta \in S_8$. And so $\sigma \in S_8$.

The element 1 in η must be in any one of the first three positions, coming from α, since according to Construction 4.3

$$\eta_i = \alpha_i \text{ if } 1 \leq i \leq 4 \text{ and } \alpha_i \neq 5,$$

and the fact that $1 \in \{\alpha_1, \alpha_2, \alpha_3\}$.

Similarly, the element 5 in η must be in either one of the positions 5, 6, or 7, coming from β, since

$$\eta_i = \beta_{i-4} \text{ if } 5 \leq i \leq 8 \text{ and } \beta_{i-4} \neq 4,$$

and the fact that $5 \in \{\beta_1, \beta_2, \beta_3\}$.

Since σ is obtained by swapping 1 and 7 as well as swapping 5 and 8 in η, we have $7 \in \{\sigma_1, \sigma_2, \sigma_3\}$ and $8 \in \{\sigma_5, \sigma_6, \sigma_7\}$. Thus, Conditions i) and ii) are proved.

Finally, let $x = (x_L, x_R)$ and $y = (y_L, y_R)$ where $x_L, x_R, y_L, y_R \in Z_3^3$. Let the arrays corresponding to y be denoted by α', β', η', and σ'. By assumption,

$$\begin{aligned} d_H(x, y) &= d_H(x_L, y_L) + d_H(x_R, y_R) \\ &\leq d_H(\alpha_{\setminus\{4,5\}}, \alpha'_{\setminus\{4,5\}}) + d_H(\beta_{\setminus\{4,5\}}, \beta'_{\setminus\{4,5\}}). \end{aligned} \tag{4.7}$$

For $1 \leq i \leq 3$ we have

$$d_H(\alpha_i, \alpha'_i) \leq d_H(\eta_i, \eta'_i). \tag{4.8}$$

If $\alpha_i = \alpha'_i$ this is obvious. Otherwise, we may assume without loss of generality that $\alpha'_i < \alpha_i$ and we must show that $\eta_i \neq \eta'_i$. If $\alpha_i < 5$, then

$$\eta'_i = \alpha'_i < \alpha_i = \eta_i.$$

If $\alpha_i = 5$, then

$$\eta'_i = \alpha'_i < 5 \text{ and } \eta_i = \beta_5 \geq 5.$$

This completes the proof of (4.8). A similar argument shows that for $5 \leq i \leq 7$ we have

$$d_H(\beta_{i-4}, \beta'_{i-4}) \leq d_H(\eta_i, \eta'_i). \tag{4.9}$$

and that for $1 \leq i \leq 8$ we have

$$d_H(\eta_i, \eta'_i) \leq d_H(\sigma_i, \sigma'_i). \tag{4.10}$$

Combining (4.7) – (4.10), we get

$$\begin{aligned} d_H(x, y) &\le d_H(\alpha_{\setminus\{4,5\}}, \alpha'_{\setminus\{4,5\}}) + d_H(\beta_{\setminus\{4,5\}}, \beta'_{\setminus\{4,5\}}) \\ &\le d_H(\eta_{\setminus\{4,8\}}, \eta'_{\setminus\{4,8\}}) \le d_H(\sigma_{\setminus\{4,8\}}, \sigma'_{\setminus\{4,8\}}). \end{aligned}$$

Hence, Condition iii) is proved. □

Lemma 4.5

i) For every $x \in Z_3^7$, $1 \in \{V(x)_1, V(x)_2, V(x)_3\}$,

ii) For every $x \in Z_3^7$, $2 \in \{V(x)_5, V(x)_6, V(x)_7\}$,

iii) For every distinct $x, y \in Z_3^7$, $d_H(V(x)_{\setminus\{4,9\}}, V(y)_{\setminus\{4,9\}}) \ge d_H(x, y)$,

Proof. We first show that $\tau \in S_9$. We have $\lambda \in S_5$ and θ is a permutation of (4, 5, 6, 7, 8, 9). In particular, 4 and 5 appear both in λ and θ. The effect of the first line in the definition of μ is to remove another elements (θ_6) into the position where λ has a 5. Similarly, the third line overwrites the 4 in θ. Note that $\lambda_5 \neq 5$ and $\theta_6 \neq 4$. The definition of μ is then the concatenation of the four first (overwritten) elements of λ and the five first (overwritten) elements of θ. Therefore, μ contains no duplicate elements, that is, $\mu \in S_9$. And so $\tau \in S_9$.

The element 1 in μ must be in any one of the first three positions, coming from λ, since according to Construction 4.4

$$\mu_i = \lambda_i \text{ if } 1 \le i \le 4 \text{ and } \lambda_i \neq 5,$$

and the fact that $1 \in \{\lambda_1, \lambda_2, \lambda_3\}$.

Similarly, the element 5 in μ must be in either one of the positions 5, 6, or 7, coming from θ, since

$$\mu_i = \theta_{i-4} \text{ if } 5 \le i \le 9 \text{ and } \theta_{i-4} \neq 4,$$

and the fact that $5 \in \{\theta_1, \theta_2, \theta_3\}$.

Since τ is obtained by swapping 2 and 5 in μ, we have $1 \in \{\tau_1, \tau_2, \tau_3\}$ and

$2 \in \{\tau_5, \tau_6, \tau_7\}$. Thus, Condition i) and ii) are proved.

Finally, let $x = (x_L, x_R)$ and $y = (y_L, y_R)$ where $x_L, y_L \in Z_3^3$ and $x_R, y_R \in Z_3^4$. Let the arrays corresponding to y be denoted by λ', θ', μ', and τ'. By assumption,

$$\begin{aligned} d_H(x, y) &= d_H(x_L, y_L) + d_H(x_R, y_R) \\ &\le d_H(\lambda_{\backslash\{4,5\}}, \lambda'_{\backslash\{4,5\}}) + d_H(\theta_{\backslash\{5,6\}}, \theta'_{\backslash\{5,6\}}). \end{aligned} \tag{4.11}$$

For $1 \le i \le 3$ we have

$$d_H(\lambda_i, \lambda'_i) \le d_H(\mu_i, \mu'_i). \tag{4.12}$$

If $\lambda_i = \lambda'_i$ this is obvious. Otherwise, we may assume without loss of generality that $\lambda'_i < \lambda_i$ and we must show that $\mu_i \ne \mu'_i$. If $\lambda_i < 5$, then

$$\mu'_i = \lambda'_i < \lambda_i = \mu_i .$$

If $\lambda_i = 5$, then

$$\mu'_i = \lambda'_i < 5 \text{ and } \mu_i = \theta_6 \ge 5.$$

This completes the proof of (4.12). A similar argument shows that for $5 \le i \le 8$ we have

$$d_H(\theta_{i-4}, \theta'_{i-4}) \le d_H(\mu_i, \mu'_i). \tag{4.13}$$

and that for $1 \le i \le 9$ we have

$$d_H(\mu_i, \mu'_i) \le d_H(\tau_i, \tau'_i). \tag{4.14}$$

Combining (4.11) – (4.14), we get

$$\begin{aligned} d_H(x, y) &\le d_H(\lambda_{\backslash\{4,5\}}, \lambda'_{\backslash\{4,5\}}) + d_H(\theta_{\backslash\{5,6\}}, \theta'_{\backslash\{5,6\}}) \\ &\le d_H(\mu_{\backslash\{4,9\}}, \mu'_{\backslash\{4,9\}}) \le d_H(\tau_{\backslash\{4,9\}}, \tau'_{\backslash\{4,9\}}). \end{aligned}$$

Hence, Condition iii) is proved. □

Now it is time for us to see the construction of the initial mapping

$f \in P(3, 13, 13)$. The construction is described in Construction 4.5. An alternative algorithmic description is given in Table 4.17 in order to help the reader understand the construction.

Construction 4.5 Construction of $f \in P(3, 13, 13)$.

Let $x \in Z_3^{13}$ and $x = (x_L, x_R)$ where $x_L \in Z_3^6$ and $x_R \in Z_3^7$. In addition, let

$$\varphi = (\varphi_1, \varphi_2, \ldots, \varphi_8) = U(x_L),$$

$$\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_9) = V(x_R) + (4, 4, \ldots, 4).$$

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

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

In ρ, swap 1 and 9 and also swap 2 and 10, and let the resulting array be denoted by π. Then define

$$f(x) = \pi.$$

Example 4.6 Let

$$\begin{array}{ll}
U(0, 1, 0, 1, 0, 2) & = (7, 2, 4, 1, 3, 8, 6, 5), \text{ and} \\
V(0, 1, 0, 1, 0, 2, 2) & = (1, 5, 4, 6, 7, 2, 3, 9, 8).
\end{array}$$

Then

$\varphi = (7, 2, 4, 1, 3, 8, 6, 5)$,

$\gamma = (5, 9, 8, 10, 11, 6, 7, 13, 12)$,

$\rho = (10, 2, 4, 3, 12, 6, 1, 9, 8, 11, 5, 7, 13)$, and
$f(0, 1, 0, 1, 0, 2, 0, 1, 0, 1, 0, 2, 2) = (2, 10, 4, 3, 12, 6, 9, 1, 8, 11, 5, 7, 13)$.

Table 4.17 An algorithmic description of the construction of $f \in P(3, 13, 13)$.

```
Combining algorithm for $f \in P(3, 13, 13)$
Input: $x = (x_1, x_2, \dots, x_{13}) \in Z_3^{13}$
Output: $(\pi_1, \pi_2, \dots, \pi_{13}) = f(x_1, x_2, \dots, x_{13})$
Begin
    $\varphi : (\varphi_1, \varphi_2, \dots, \varphi_8) \leftarrow U(x_1, x_2, \dots, x_6)$;
    $(\phi_1, \phi_2, \dots, \phi_9) \leftarrow V(x_7, x_8, \dots, x_{13})$;
    $\gamma : (\gamma_1, \gamma_2, \dots, \gamma_9) \leftarrow (\phi_1 + 4, \phi_2 + 4, \dots, \phi_9 + 4)$;
    $i \leftarrow \gamma^{-1}(5)$;
    $j \leftarrow \gamma^{-1}(6)$;
    $k \leftarrow \varphi^{-1}(7)$;
    $l \leftarrow \varphi^{-1}(8)$;
    $\gamma_i \leftarrow \varphi_4$;
    $\gamma_j \leftarrow \varphi_8$;
    $\varphi_k \leftarrow \rho_4$;
    $\varphi_l \leftarrow \rho_9$;
    $\rho : (\rho_1, \rho_2, \dots, \rho_{13}) \leftarrow (\varphi_1, \varphi_2, \varphi_3, \varphi_5, \varphi_6, \varphi_7, \gamma_1, \gamma_2, \gamma_3, \gamma_5, \gamma_6, \gamma_7, \gamma_8)$;
    $i \leftarrow \rho^{-1}(1)$;
    $j \leftarrow \rho^{-1}(2)$;
    $k \leftarrow \rho^{-1}(9)$;
    $l \leftarrow \rho^{-1}(10)$;
    swap $(\rho_i, \rho_k)$;
    swap $(\rho_j, \rho_l)$;
    $\pi : (\pi_1, \pi_1, \dots, \pi_{13}) \leftarrow (\rho_1, \rho_2, \dots, \rho_{13})$;
End
```

Now we show that f has the started property.

Lemma 4.6 $f \in P(3, 13, 13)$ and $f(x)_{13} \notin \{9, 10\}$ for every $x \in Z_3^{13}$.

Proof. We first show that $\pi \in S_{13}$. We have $\varphi \in S_8$ and γ is a permutation of $(5, 6, \ldots, 13)$. In particular, 5, 6, 7, and 8 appear in both φ and γ. The effect of the first line in the definition of ρ is to remove another elements (γ_4) into the position where φ has a 7. Similarly, the third line overwrites the 8 in φ, the fifth line overwrites the 5 in γ, and the seventh line overwrites the 6 in γ. The definition of ρ is then the concatenation of the elements φ_1, φ_2, φ_3, φ_5, φ_6, and φ_7 (overwritten) of φ as well as the elements γ_1, γ_2, γ_3, γ_5, γ_6, γ_7, and γ_8 (overwritten) of γ. Therefore, ρ contains no duplicate elements, that is, $\rho \in S_{13}$. And so $\pi \in S_{13}$.

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, 8, … , or 12 (if $\varphi_4 = 1$ or $\varphi_8 = 1$). Similarly, the element 2 must be in one of the first twelve positions of ρ. Therefore, both 9 and 10 must be among the first twelve positions of π, that is, $\pi_{13} \notin \{9, 10\}$.

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

$$\begin{aligned} d_H(x, x') &= d_H(x_L, x'_L) + d_H(x_R, x'_R) \\ &\leq d_H(\varphi_{\setminus\{4,8\}}, \varphi'_{\setminus\{4,8\}}) + d_H(\gamma_{\setminus\{4,9\}}, \gamma'_{\setminus\{4,9\}}). \end{aligned} \tag{4.15}$$

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

$$d_H(\varphi_i, \varphi'_i) \leq d_H(\rho_i, \rho'_i) \qquad \text{if } 1 \leq i \leq 3, \text{ and} \tag{4.16}$$

$$d_H(\varphi_{i+1}, \varphi'_{i+1}) \leq d_H(\rho_i, \rho'_i) \qquad \text{if } 4 \leq i \leq 6. \tag{4.17}$$

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 $\varphi_i \leq 6$, then

$$\rho'_i = \varphi'_i < \varphi_i = \rho_i \qquad \text{if } 1 \leq i \leq 3, \text{ or}$$

$$\rho'_i = \varphi'_{i+1} < \varphi_{i+1} = \rho_i \qquad \text{if } 4 \leq i \leq 6.$$

If $\varphi_i = 7$, then

$$\begin{array}{ll} \rho_i = \gamma_4 \geq 7 & \text{, and} \\ \rho'_i = \varphi'_i \leq 6 & \text{if } 1 \leq i \leq 3\text{, or} \\ \rho'_i = \varphi'_{i+1} < 6 & \text{if } 4 \leq i \leq 6. \end{array}$$

If $\varphi_i = 8$, then $4 \leq i \leq 6$ and so $\varphi'_i \neq 7$. Hence

$$\begin{array}{ll} \rho_i = \gamma_9 \geq 7 & \text{, and} \\ \rho'_i = \varphi'_i \leq 6 & \text{if } 1 \leq i \leq 3\text{, or} \\ \rho'_i = \varphi'_{i+1} < 6 & \text{if } 4 \leq i \leq 6. \end{array}$$

This completes that proof of (4.16) and (4.17). A similar arguments show that for $7 \leq i \leq 13$ we have

$$d_H(\gamma_{i-6}, \gamma'_{i-6}) \leq d_H(\rho_i, \rho'_i) \quad \text{if } 7 \leq i \leq 9\text{, and} \tag{4.18}$$

$$d_H(\gamma_{i-5}, \gamma'_{i-5}) \leq d_H(\rho_i, \rho'_i) \quad \text{if } 10 \leq i \leq 13. \tag{4.19}$$

and that for $1 \leq i \leq 13$ we have

$$d_H(\rho_i, \rho'_i) \leq d_H(\pi_i, \pi'_i). \tag{4.20}$$

Combining (4.15) – (4.20), we get

$$\begin{aligned} d_H(x, x') &\leq d_H(\varphi_{\backslash\{4,8\}}, \varphi'_{\backslash\{4,8\}}) + d_H(\gamma_{\backslash\{4,9\}}, \gamma'_{\backslash\{4,9\}}) \\ &\leq d_H(\rho, \rho') \leq d_H(\pi, \pi'). \end{aligned}$$

Hence, f is distance preserving. □

Table 4.21 lists the distance expansion matrix of f. In order to fit the table into a page, we split the distance expansion matrix into two parts from left to right. With f as an initial mapping, we can prove the following theorem with Theorem 4.1.

Theorem 4.5: $P(3, n, n)$ is not empty for $n \geq 13$.

4.5 Application to Permutation Arrays

Chang *et al*. in [17] showed that for $n \geq 4$ and $2 \leq D \leq n$, $P(N, D) \geq A_2(n, D - 1)$. Chang in [13] further improved the bound to $P(N, D) \geq A_2(N, D - \delta)$ for $n \geq n_\delta$ and $\delta + 1 \leq D \leq n$ where $\delta \geq 2$ and n_δ is a positive integer determined by δ, e.g., $n_\delta \geq 16$ for $\delta = 2$. Here we give other lower bounds.

Theorem 4.6 Let n_k be the least integer such that for $n \geq n_k$, $\mathcal{I}(3, n, N)$ is not empty, then for $n \geq n_k$ and $2 \leq D \leq n$, $P(N, D) \geq A_3(n, D - 1)$.

Proof. Let A be a code alphabet of size 3 and C be a $(n, D - 1)$ code over A. Let $f \in \mathcal{I}(3, n, N)$. It is obvious that $f(C)$ is an (N, D)-PA. Therefore,

$$P(N, D) \geq A_3(n, D - 1). \qquad □$$

Theorem 4.7 Let n_k be the least integer such that for $n \geq n_k$, $\mathcal{P}(3, n, N)$ is not empty. Then for $n \geq n_k$ and $2 \leq D \leq n$, $P(N, D) \geq A_3(n, D)$.

Proof. Similar to Theorem 4.6. □

We have shown that $\mathcal{I}(3, n, n + 2)$ is not empty for $n \geq 1$, $\mathcal{P}(3, n, n + 1)$ is not empty for $n \geq 9$, and $\mathcal{P}(3, n, n)$ is not empty for $n \geq 13$. With these results, we can prove the following corollaries.

Corollary 4.1 For $N \geq 3$ and $2 \leq D \leq N$, $P(N, D) \geq A_3(N - 2, D - 1)$.

Corollary 4.2 For $N \geq 10$ and $2 \leq D \leq N$, $P(N, D) \geq A_3(N - 1, D)$.

Corollary 4.3 For $N \geq 13$ and $2 \leq D \leq N$, $P(N, D) \geq A_3(N, D)$.

Bounds on $A_2(n, d)$ and $A_3(n, d)$ have been studied by many researchers, for example, [4] and [35, Ch. 5]. Tables 4.19 and 4.20 list the best known lower bounds on $A_2(n, d)$ and $A_3(n, d)$ for $8 \le n \le 16$, respectively. In general, the lower bound on $P(N, D)$ obtained from use of ternary codes are better than those obtained from binary codes. For example, using Chang's bound [13], we get $P(16, 5) \ge A_2(16, 3) \ge 2720$ whereas Corollary 4.4 gives $P(16, 5) \ge A_3(16, 5) \ge 19683$. Similarly, we get $P(16, 9) \ge A_2(16, 7) \ge 36$, and $P(16, 9) \ge A_3(16, 9) \ge 243$. A more complete comparison of the lower bound on $P(16, D)$ for $5 \le D \le 12$ is listed in Table 4.18. The asterisk behind a number indicates that this number is the largest among all items.

Remark. After we submitted our paper, Te-Tsung *et al.* also proposed a construction of DPMs from ternary vectors [34]. Their construction method is different from ours. They first constructed ternary DPMs $A_{8n} \in P(3, 8n, 8n)$ for $n \ge 2$ by an algorithm, and then constructed ternary DPMs of length $8n + 1$, $8n + 2$, ... , and $8n + 7$ from the mapping A_{8n}. As a result, their DPMs start from $n = 16$, which is worse than ours.

Table 4.18 Comparison of the lower bound on $P(16, D)$.

D	Chang *et al.*	Huang *et al.*	Chang	Lin *et al.* [19]		
	[17]	[37]	[13]	Corollary 4.1	Corollary 4.2	Corollary 4.3
5	2048	8192	2720	24057*	6561	19683
6	256	1024	2048	6561*	2187	6561*
7	256	512	256	2187*	729	729
8	36	128	256	243	243	297*
9	32	64	36	81	81	243*
10	6	16	32	31	27	54*
11	4	8	6	12	10	18*
12	2	4	4	6	6	9*

Table 4.19 Best known lower bounds on $A_2(n, d)$ for $8 \le n \le 16$.

8	20								
9	40	20							
10	72	40	12						
11	144	72	24	12					
12	256	144	32	24	4				
13	512	256	64	32	8	4			
14	1024	512	128	64	16	8	4		
15	2048	1024	256	128	32	16	4	4	
16	2720	2048	256	256	36	32	6	4	2
n *d*	3	4	5	6	7	8	9	10	11

Table 4.20 Best known lower bounds on $A_3(n, d)$ for $8 \le n \le 16$.

8	243								
9	729	243							
10	2187	729	---						
11	6561	1458	---	---					
12	---	4374	729	---	54				
13	---	8019	2187	729	105	42			
14	118098	24057	6561	2187	243	81	31		
15	354294	72171	6561	2187	729	243	81	27	
16	1062882	216513	19683	6561	729	297	243	54	18
n *d*	3	4	5	6	7	8	9	10	11

Table 4.21 Distance expansion matrix of $f \in P(3, 13, 13)$.

0	7499223	7735419	3857868	3267378	0	0
	5412825	13677741	54993657	77247942	56888015	30417032
		10747809	77580494	211825026	421803519	501911682
			36626024	242982187	846887509	1769590178
				105263378	773056332	2824925916
					285879216	2265593524
						753257142

(a) The left part

0	0	0	0	0	0
8677294	1279370	120512	0	0	0
364081528	174922222	52509696	8102560	420976	0
2483941294	2139969740	1151920836	373881088	67888104	5840600
6385449644	9260453002	8042859708	4127290924	1166653528	144346784
8520370780	19387502504	26647039408	20610803256	8407198472	1423077416
6071844564	22632413854	48294677760	56644950656	33095930128	7601855048
1859300480	14543002936	50842947800	91894856296	78620491736	24881794480
	4110998704	29891105728	89126735840	116260882432	52435159216
		7789174080	48592527648	105417407040	71660796768
			11696151456	54106672320	61538942880
				12183187968	30264067584
					6530347008

(b) The right part

Chapter 5

Conclusions

5.1 Summary

In this dissertation we have proposed several constructions of DPMs and DIMs, either from binary vectors or ternary vectors. In Chapter 3, non-recursive constructions of binary DIMs of odd and even length were proposed. These constructions are based on simple compositions of permutations of an ordered set, called basic construction set. We have proved that in some conditions the mapping "generated" by a basic construction set is distance increasing. As the numerical results in Section 3.3 showed, our new DIMs have sound distance expansion distributions for odd length.

In Chapter 4, we proposed a general recursive construction method that constructs DPMs or DIMs from ternary vectors and then, based on this method, we proposed three constructions of ternary DPMs or DIMs. The first one constructs ternary *n*_(*n*+2)-DIMs for $n \geq 3$, the second one constructs ternary *n*_(*n*+1)-DPMs for $n \geq 9$, and the third one constructs ternary *n*-DPMs for $n \geq 13$. This is the first time that constructions of DPMs or DIMs from ternary vectors are proposed in the literature. As we have showed, the proposed constructions improve the lower bounds on $P(N, D)$.

5.2 Future Works

Distance-preserving mappings are well studied in the past few years, especially binary distance-preserving mappings. However, there are still a lot of topics worth exploring.

- An initial mapping for the construction of ternary n_(n+1)-DIMs.

  If a DIM from Z_3^m to S_{m+1} can be found, then ternary n_(n+1)-DIMs for all $n \geq m$ can be constructed by using Construction E in Section 4.1.

- Constructions of ternary n-DIMs.

  Construction E can only construct ternary n-DPMs even though the initial mapping is distance increasing. Thus, a new construction method must be found.

- A non-recursive systematic construction method of (n, δ)-DIMs from binary or ternary vectors.

  A mapping that increases more distance than that of input vectors may be more interesting for applications. Although Chang has proposed constructions of binary (n, δ)-DIMs for $\delta \geq 2$ [13], the constructions are recursive and are unable to construct binary (n, δ)-DIMs for all $n > n_\delta$ where n_δ is the smallest positive integer n_δ such that a binary (n, δ)-DIM could be constructed for any $n \geq n_\delta$.The concept can also be applied to ternary DIMs. No ternary (n, δ)-DIM has been found for $\delta \geq 1$.

- A tighter bound on the smallest positive integer n_δ such that a binary (n, δ)-DIM exists for all $n > n_\delta$.

  For any $\delta \geq 2$, Chang provided a bound on the smallest positive integer n_δ by which a binary (n, δ)-DIM can be constructed for all $n > n_\delta$ [13]. It seems that the bound can be further improved.

- A general construction method of DPMs or DIMs from Z_q^n to S_N.

  DPMs and DIMs from Z_q^n to S_N are useful in converting a q-ary code, e.g. Reed-Solomon code, to a permutation array. The constructions of DPMs or DIMs proposed so far are from binary or ternary vectors and can not be generalized to q-ary vectors for all $q \geq 2$. It is a great contribution if one can propose a general construction of DPMs or DIMs from q-ary vectors for all $q \geq 2$. If the construction is recursive, an initial mapping should also be provided.

- Construct DPMs or DIMs from a subset of vectors.

  In present DPMs and DIMs, all vectors are considered. The distance between each pair of vectors in the vector space should be preserved or even increased. However, this is somewhat overkill. In constructing permutation arrays from distance-preserving mappings, only a subset of vectors, which form a (n, d) code, is mapped to permutations, whereas the other vectors are irrelevant. Therefore, only the subset of vectors should be either distance preserving or distance increasing.

Bibliography

[1] A. J. H. Vinck and J. Häring, “Coding and modulation for power-line communications,” in *Proc. Int. Symp. Power Line Communication*, Limerick, Ireland, Apr. 5–7, 2000.

[2] A. J. H. Vinck, “Coded modulation for powerline communications,” *A.E.Ü. Int. J. Electron. Commun.*, vol. 54, no. 1, pp. 45–49, 2000.

[3] A. J. H. Vinck, J. Häring, and T. Wadayama, “Coded M-FSK for power-line communications,” in *Proc. IEEE Int. Symp. Information Theory*, Sorrento, Italy, June 2000, p. 137.

[4] A.E. Brouwer, Heikki O. Hämäläinen, Patric R.J. Östergård, N.J.A. Sloane, “Bounds on Mixed Binary/Ternary Codes,” *IEEE Trans. Inform. Theory*, vol. 44, no. 1, pp. 140–161, Jan. 1998.

[5] C. Ding, F.-W. Fu, T. Kløve, and V. K. Wei, “Constructions of permutation arrays,” *IEEE Trans. Inform. Theory*, vol. 48, pp. 977–980, Apr. 2002.

[6] C. J. Colbourn, T. Kløve, and Alan C. H. Ling, “Permutation Arrays for Powerline Communication and Mutually Orthogonal Latin Squares,” *IEEE Trans. Inform. Theory*, vol. 50, no.6, pp. 1289–1291, June 2004.

[7] D. R. de la Torre, C. J. Colbourn, and A. C. H. Ling, “An application of permutation arrays to block ciphers.” *Proceedings of the Thirty-first Southeastern International Conference on Combinatorics, Graph Theory and Computing* (Boca Raton, FL, 2000), vol. 145, pp. 5–7, 2000.

[8] F.-W. Fu and T. Kløve, “Two constructions of permutation arrays,” *IEEE Trans. Inform. Theory*, vol. 50, pp. 881–883, May 2004.

[9] H. C. Ferreira and A. J. H. Vinck, “Inference cancellation with permutation trellis arrays,” *Proc. IEEE Vehicular Technology Conf.*, pp. 2401–2407, 2000.

[10] H. C. Ferreira, A. J. H. Vinck, T. G. Swart, and A. L. Nel, “Permutation trellis codes,” *Proc. IEEE Trans. on Communications*, vol. 53, no. 11, pp. 1782-1789, Nov. 2005.

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

[12] I. Blake, G. Cohen, and M. Deza, “Coding with permutations,” *Inform. Contr.*, vol. 43, no. 1, pp. 1-19, 1979.

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

[14] J.-C. Chang, “Distance-Increasing Mappings from Binary Vectors to Permutations,” *IEEE Trans. Inform. Theory*, vol. 51, no. 1 pp. 359–363, Jan. 2005.

[15] J.-C. Chang, “New Algorithms of Distance-Increasing Mappings from Binary Vectors to Permutations by Swaps,” *Designs, Codes and Cryptography*, vol. 39, no. 3, pp. 335–345, June 2006.

[16] J.-C. Chang, “New constructions of distance-increasing mappings and permutation arrays,” *Journal of Inform. Science and Engineering*, vol. 23, no. 4, pp. 1227-1239, July 2007.

[17] J.-C. Chang, R.-J. Chen, T. Kløve, and S.-C. Tsai, “Distance-preserving mappings from binary vectors to permutations,” *IEEE Trans. Inform. Theory*, vol. 49, pp. 1054–1059, Apr. 2003.

[18] J.-S. Lin, J.-C. Chang, and R.-J. Chen, “New Simple Constructions of Distance- Increasing Mappings from Binary Vectors to Permutations,” *Information Processing Letters*. vol. 100, no. 2, pp. 83–89, Oct. 2006.

[19] J.-S. Lin, J.-C. Chang, R.-J. Chen, T. Kløve, "Distance-preserving mappings and distance-increasing mappings from ternary vectors to permutations," to appear in *IEEE Trans. on Inform. Theory*.

[20] John B. Fraleigh, *A first course in abstract algebra, 7th ed.*, Boston: Addison-Wesley, 2003.

[21] K. Lee, "Cyclic constructions of distance-preserving maps," *IEEE Trans. on Inform. Theory*, vol. 51, no. 12, pp. 4392-4396, Dec. 2005.

[22] K. Lee, "Distance-increasing maps of all length by simple mapping algorithms," *IEEE Trans. on Inform. Theory*, vol. 52, no. 7, pp. 3344-3348, July 2006.

[23] K. Lee, "New distance-preserving maps of odd length," *IEEE Trans. Inform. Theory*, vol. 50, no. 10, Oct. 2004.

[24] M. Deza and S. A. Vanstone, "Bounds on permutation arrays," *J. Statist. Planning and Inference*, vol. 2, pp. 197-209, 1978.

[25] Morgan H.L.Chan and Robert W. Donaldson, "Amplitude, Width, and Interarrival Distributions for Noise Impulses on Intrabuilding Power Line Communication Networks," *IEEE Trans. on Electromagnetic Compatibility*, vol. 31, pp. 320–323, Aug, 1989.

[26] N. Pavlidou, A. J. Han Vinck, J. Yazdani, and B. Honary, "Power line communications: state of the art and future trends," *IEEE Communications Magazine*, vol. 41, no. 4, pp. 34–40, Apr. 2003.

[27] O. Hooijen, "A Channel Model for the Residential Power Circuit Used as a Digital Communication Medium," *IEEE Trans. on Electromagn. Compat.*, vol 40, pp.331–336, 1998.

[28] P. Frankel and M. Deza, "On the maximum number of permutations with given maximal and minimal distance," *J. Comb. Theory, Ser A*, vol. 22, pp. 352-360, 1977.

[29] T. G Swart and H. C. Ferreira, "A multilevel construction for mappings from binary sequences to permutation sequences," *Proc. IEEE Int. Symp. Information Theory*, Seattle, USA, pp. 1895-1899, July 2006.

[30] T. G Swart, I. de Beer, and H. C. Ferreira, “On the distance optimality of permutation mappings,” *Proc. IEEE Int. Symp. Information Theory*, Adelaide, Australia, pp. 1068-1072, Sep. 2005.

[31] T. G. Swart and H. C. Ferreira, “A Generalized Upper Bound and a Multilevel Construction for Distance-Preserving Mappings,” *IEEE Trans. on Inform. Theory*, vol. 52, no. 8, pp. 3685-3695, Aug. 2006.

[32] T. Kløve, “Classification of permutation codes of length 6 and minimum distance 5,” in *Proc. Int. Symp. Information Theory and Its Applications*, 2000, pp. 465–468.

[33] T. Wadayama and A. J. H. Vinck, “A multilevel construction of permutation codes,” *IEICE Trans. Fundamentals Electron., Commun. Comp. Sci.*, vol. 84, pp. 2518–2522, 2001.

[34] T.-T. Lin, S.-C. Tsai, H.-L. Wu, “Distance-preserving mappings from ternary vectors to permutations,” submitted to *IEEE Trans. on Inform. Theory*, Manuscript 2007.

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

[36] W. Chu, C. J. Colbourn, and P. Dukes, “Constructions for Permutation Codes in Powerline Communications,” *Designs, Codes and Cryptography*, vol. 32, no. 1–3, pp.51–64, May 2004.

[37] 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 and Cryptography*, vol. 40, no. 2, pp. 139–155, Aug. 2006.

Appendix A

Mapping table of $f_5 \in I\,(2, 5, 5)$.

x	$f_5(x)$	x	$f_5(x)$
(0,0,0,0,0)	(1,2,3,4,5)	(1,0,0,0,0)	(2,1,3,4,5)
(0,0,0,0,1)	(1,2,3,5,4)	(1,0,0,0,1)	(2,1,3,5,4)
(0,0,0,1,0)	(1,3,2,4,5)	(1,0,0,1,0)	(2,3,1,4,5)
(0,0,0,1,1)	(1,3,2,5,4)	(1,0,0,1,1)	(2,3,1,5,4)
(0,0,1,0,0)	(3,2,5,4,1)	(1,0,1,0,0)	(3,1,5,4,2)
(0,0,1,0,1)	(3,2,5,1,4)	(1,0,1,0,1)	(3,1,5,2,4)
(0,0,1,1,0)	(3,5,2,4,1)	(1,0,1,1,0)	(3,5,1,4,2)
(0,0,1,1,1)	(3,5,2,1,4)	(1,0,1,1,1)	(3,5,1,2,4)
(0,1,0,0,0)	(1,2,4,3,5)	(1,1,0,0,0)	(2,1,4,3,5)
(0,1,0,0,1)	(1,2,4,5,3)	(1,1,0,0,1)	(2,1,4,5,3)
(0,1,0,1,0)	(1,4,2,3,5)	(1,1,0,1,0)	(2,4,1,3,5)
(0,1,0,1,1)	(1,4,2,5,3)	(1,1,0,1,1)	(2,4,1,5,3)
(0,1,1,0,0)	(4,2,5,3,1)	(1,1,1,0,0)	(4,1,5,3,2)
(0,1,1,0,1)	(4,2,5,1,3)	(1,1,1,0,1)	(4,1,5,2,3)
(0,1,1,1,0)	(4,5,2,3,1)	(1,1,1,1,0)	(4,5,1,3,2)
(0,1,1,1,1)	(4,5,2,1,3)	(1,1,1,1,1)	(4,5,1,2,3)

Mapping table of $f_6 \in I(2, 6, 6)$.

x	$f_6(x)$	x	$f_6(x)$
(0,0,0,0,0,0)	(1,2,3,4,5,6)	(1,0,0,0,0,0)	(2,1,3,4,5,6)
(0,0,0,0,0,1)	(6,2,3,4,5,1)	(1,0,0,0,0,1)	(6,1,3,4,5,2)
(0,0,0,0,1,0)	(1,2,3,5,4,6)	(1,0,0,0,1,0)	(2,1,3,5,4,6)
(0,0,0,0,1,1)	(6,2,3,5,4,1)	(1,0,0,0,1,1)	(6,1,3,5,4,2)
(0,0,0,1,0,0)	(1,3,2,4,5,6)	(1,0,0,1,0,0)	(2,3,1,4,5,6)
(0,0,0,1,0,1)	(6,3,2,4,5,1)	(1,0,0,1,0,1)	(6,3,1,4,5,2)
(0,0,0,1,1,0)	(1,3,2,5,4,6)	(1,0,0,1,1,0)	(2,3,1,5,4,6)
(0,0,0,1,1,1)	(6,3,2,5,4,1)	(1,0,0,1,1,1)	(6,3,1,5,4,2)
(0,0,1,0,0,0)	(1,2,3,4,6,5)	(1,0,1,0,0,0)	(2,1,3,4,6,5)
(0,0,1,0,0,1)	(5,2,3,4,6,1)	(1,0,1,0,0,1)	(5,1,3,4,6,2)
(0,0,1,0,1,0)	(1,2,3,6,4,5)	(1,0,1,0,1,0)	(2,1,3,6,4,5)
(0,0,1,0,1,1)	(5,2,3,6,4,1)	(1,0,1,0,1,1)	(5,1,3,6,4,2)
(0,0,1,1,0,0)	(1,3,2,4,6,5)	(1,0,1,1,0,0)	(2,3,1,4,6,5)
(0,0,1,1,0,1)	(5,3,2,4,6,1)	(1,0,1,1,0,1)	(5,3,1,4,6,2)
(0,0,1,1,1,0)	(1,3,2,6,4,5)	(1,0,1,1,1,0)	(2,3,1,6,4,5)
(0,0,1,1,1,1)	(5,3,2,6,4,1)	(1,0,1,1,1,1)	(5,3,1,6,4,2)
(0,1,0,0,0,0)	(1,2,4,3,5,6)	(1,1,0,0,0,0)	(2,1,4,3,5,6)
(0,1,0,0,0,1)	(6,2,4,3,5,1)	(1,1,0,0,0,1)	(6,1,4,3,5,2)
(0,1,0,0,1,0)	(1,2,4,5,3,6)	(1,1,0,0,1,0)	(2,1,4,5,3,6)
(0,1,0,0,1,1)	(6,2,4,5,3,1)	(1,1,0,0,1,1)	(6,1,4,5,3,2)
(0,1,0,1,0,0)	(1,4,2,3,5,6)	(1,1,0,1,0,0)	(2,4,1,3,5,6)
(0,1,0,1,0,1)	(6,4,2,3,5,1)	(1,1,0,1,0,1)	(6,4,1,3,5,2)
(0,1,0,1,1,0)	(1,4,2,5,3,6)	(1,1,0,1,1,0)	(2,4,1,5,3,6)
(0,1,0,1,1,1)	(6,4,2,5,3,1)	(1,1,0,1,1,1)	(6,4,1,5,3,2)
(0,1,1,0,0,0)	(1,2,4,3,6,5)	(1,1,1,0,0,0)	(2,1,4,3,6,5)
(0,1,1,0,0,1)	(5,2,4,3,6,1)	(1,1,1,0,0,1)	(5,1,4,3,6,2)
(0,1,1,0,1,0)	(1,2,4,6,3,5)	(1,1,1,0,1,0)	(2,1,4,6,3,5)
(0,1,1,0,1,1)	(5,2,4,6,3,1)	(1,1,1,0,1,1)	(5,1,4,6,3,2)
(0,1,1,1,0,0)	(1,4,2,3,6,5)	(1,1,1,1,0,0)	(2,4,1,3,6,5)
(0,1,1,1,0,1)	(5,4,2,3,6,1)	(1,1,1,1,0,1)	(5,4,1,3,6,2)
(0,1,1,1,1,0)	(1,4,2,6,3,5)	(1,1,1,1,1,0)	(2,4,1,6,3,5)
(0,1,1,1,1,1)	(5,4,2,6,3,1)	(1,1,1,1,1,1)	(5,4,1,6,3,2)

Mapping table of $f_7 \in I\,(2, 7, 7)$:

x	$f_7(x)$	x	$f_7(x)$
(0,0,0,0,0,0,0)	(1,2,3,4,5,6,7)	(1,0,0,0,0,0,0)	(2,1,3,4,5,6,7)
(0,0,0,0,0,0,1)	(1,2,3,4,5,7,6)	(1,0,0,0,0,0,1)	(2,1,3,4,5,7,6)
(0,0,0,0,0,1,0)	(1,2,3,5,4,6,7)	(1,0,0,0,0,1,0)	(2,1,3,5,4,6,7)
(0,0,0,0,0,1,1)	(1,2,3,5,4,7,6)	(1,0,0,0,0,1,1)	(2,1,3,5,4,7,6)
(0,0,0,0,1,0,0)	(1,3,2,4,5,6,7)	(1,0,0,0,1,0,0)	(2,3,1,4,5,6,7)
(0,0,0,0,1,0,1)	(1,3,2,4,5,7,6)	(1,0,0,0,1,0,1)	(2,3,1,4,5,7,6)
(0,0,0,0,1,1,0)	(1,3,2,5,4,6,7)	(1,0,0,0,1,1,0)	(2,3,1,5,4,6,7)
(0,0,0,0,1,1,1)	(1,3,2,5,4,7,6)	(1,0,0,0,1,1,1)	(2,3,1,5,4,7,6)
(0,0,0,1,0,0,0)	(5,6,3,7,1,2,4)	(1,0,0,1,0,0,0)	(5,6,3,7,2,1,4)
(0,0,0,1,0,0,1)	(5,6,3,7,1,4,2)	(1,0,0,1,0,0,1)	(5,6,3,7,2,4,1)
(0,0,0,1,0,1,0)	(5,6,3,1,7,2,4)	(1,0,0,1,0,1,0)	(5,6,3,2,7,1,4)
(0,0,0,1,0,1,1)	(5,6,3,1,7,4,2)	(1,0,0,1,0,1,1)	(5,6,3,2,7,4,1)
(0,0,0,1,1,0,0)	(5,3,6,7,1,2,4)	(1,0,0,1,1,0,0)	(5,3,6,7,2,1,4)
(0,0,0,1,1,0,1)	(5,3,6,7,1,4,2)	(1,0,0,1,1,0,1)	(5,3,6,7,2,4,1)
(0,0,0,1,1,1,0)	(5,3,6,1,7,2,4)	(1,0,0,1,1,1,0)	(5,3,6,2,7,1,4)
(0,0,0,1,1,1,1)	(5,3,6,1,7,4,2)	(1,0,0,1,1,1,1)	(5,3,6,2,7,4,1)
(0,0,1,0,0,0,0)	(1,2,3,4,6,5,7)	(1,0,1,0,0,0,0)	(2,1,3,4,6,5,7)
(0,0,1,0,0,0,1)	(1,2,3,4,6,7,5)	(1,0,1,0,0,0,1)	(2,1,3,4,6,7,5)
(0,0,1,0,0,1,0)	(1,2,3,6,4,5,7)	(1,0,1,0,0,1,0)	(2,1,3,6,4,5,7)
(0,0,1,0,0,1,1)	(1,2,3,6,4,7,5)	(1,0,1,0,0,1,1)	(2,1,3,6,4,7,5)
(0,0,1,0,1,0,0)	(1,3,2,4,6,5,7)	(1,0,1,0,1,0,0)	(2,3,1,4,6,5,7)
(0,0,1,0,1,0,1)	(1,3,2,4,6,7,5)	(1,0,1,0,1,0,1)	(2,3,1,4,6,7,5)
(0,0,1,0,1,1,0)	(1,3,2,6,4,5,7)	(1,0,1,0,1,1,0)	(2,3,1,6,4,5,7)
(0,0,1,0,1,1,1)	(1,3,2,6,4,7,5)	(1,0,1,0,1,1,1)	(2,3,1,6,4,7,5)
(0,0,1,1,0,0,0)	(6,5,3,7,1,2,4)	(1,0,1,1,0,0,0)	(6,5,3,7,2,1,4)
(0,0,1,1,0,0,1)	(6,5,3,7,1,4,2)	(1,0,1,1,0,0,1)	(6,5,3,7,2,4,1)
(0,0,1,1,0,1,0)	(6,5,3,1,7,2,4)	(1,0,1,1,0,1,0)	(6,5,3,2,7,1,4)
(0,0,1,1,0,1,1)	(6,5,3,1,7,4,2)	(1,0,1,1,0,1,1)	(6,5,3,2,7,4,1)
(0,0,1,1,1,0,0)	(6,3,5,7,1,2,4)	(1,0,1,1,1,0,0)	(6,3,5,7,2,1,4)
(0,0,1,1,1,0,1)	(6,3,5,7,1,4,2)	(1,0,1,1,1,0,1)	(6,3,5,7,2,4,1)
(0,0,1,1,1,1,0)	(6,3,5,1,7,2,4)	(1,0,1,1,1,1,0)	(6,3,5,2,7,1,4)
(0,0,1,1,1,1,1)	(6,3,5,1,7,4,2)	(1,0,1,1,1,1,1)	(6,3,5,2,7,4,1)

x	$f_7(x)$	*x*	$f_7(x)$
(0,1,0,0,0,0,0)	(1,2,4,3,5,6,7)	(1,1,0,0,0,0,0)	(2,1,4,3,5,6,7)
(0,1,0,0,0,0,1)	(1,2,4,3,5,7,6)	(1,1,0,0,0,0,1)	(2,1,4,3,5,7,6)
(0,1,0,0,0,1,0)	(1,2,4,5,3,6,7)	(1,1,0,0,0,1,0)	(2,1,4,5,3,6,7)
(0,1,0,0,0,1,1)	(1,2,4,5,3,7,6)	(1,1,0,0,0,1,1)	(2,1,4,5,3,7,6)
(0,1,0,0,1,0,0)	(1,4,2,3,5,6,7)	(1,1,0,0,1,0,0)	(2,4,1,3,5,6,7)
(0,1,0,0,1,0,1)	(1,4,2,3,5,7,6)	(1,1,0,0,1,0,1)	(2,4,1,3,5,7,6)
(0,1,0,0,1,1,0)	(1,4,2,5,3,6,7)	(1,1,0,0,1,1,0)	(2,4,1,5,3,6,7)
(0,1,0,0,1,1,1)	(1,4,2,5,3,7,6)	(1,1,0,0,1,1,1)	(2,4,1,5,3,7,6)
(0,1,0,1,0,0,0)	(5,6,4,7,1,2,3)	(1,1,0,1,0,0,0)	(5,6,4,7,2,1,3)
(0,1,0,1,0,0,1)	(5,6,4,7,1,3,2)	(1,1,0,1,0,0,1)	(5,6,4,7,2,3,1)
(0,1,0,1,0,1,0)	(5,6,4,1,7,2,3)	(1,1,0,1,0,1,0)	(5,6,4,2,7,1,3)
(0,1,0,1,0,1,1)	(5,6,4,1,7,3,2)	(1,1,0,1,0,1,1)	(5,6,4,2,7,3,1)
(0,1,0,1,1,0,0)	(5,4,6,7,1,2,3)	(1,1,0,1,1,0,0)	(5,4,6,7,2,1,3)
(0,1,0,1,1,0,1)	(5,4,6,7,1,3,2)	(1,1,0,1,1,0,1)	(5,4,6,7,2,3,1)
(0,1,0,1,1,1,0)	(5,4,6,1,7,2,3)	(1,1,0,1,1,1,0)	(5,4,6,2,7,1,3)
(0,1,0,1,1,1,1)	(5,4,6,1,7,3,2)	(1,1,0,1,1,1,1)	(5,4,6,2,7,3,1)
(0,1,1,0,0,0,0)	(1,2,4,3,6,5,7)	(1,1,1,0,0,0,0)	(2,1,4,3,6,5,7)
(0,1,1,0,0,0,1)	(1,2,4,3,6,7,5)	(1,1,1,0,0,0,1)	(2,1,4,3,6,7,5)
(0,1,1,0,0,1,0)	(1,2,4,6,3,5,7)	(1,1,1,0,0,1,0)	(2,1,4,6,3,5,7)
(0,1,1,0,0,1,1)	(1,2,4,6,3,7,5)	(1,1,1,0,0,1,1)	(2,1,4,6,3,7,5)
(0,1,1,0,1,0,0)	(1,4,2,3,6,5,7)	(1,1,1,0,1,0,0)	(2,4,1,3,6,5,7)
(0,1,1,0,1,0,1)	(1,4,2,3,6,7,5)	(1,1,1,0,1,0,1)	(2,4,1,3,6,7,5)
(0,1,1,0,1,1,0)	(1,4,2,6,3,5,7)	(1,1,1,0,1,1,0)	(2,4,1,6,3,5,7)
(0,1,1,0,1,1,1)	(1,4,2,6,3,7,5)	(1,1,1,0,1,1,1)	(2,4,1,6,3,7,5)
(0,1,1,1,0,0,0)	(6,5,4,7,1,2,3)	(1,1,1,1,0,0,0)	(6,5,4,7,2,1,3)
(0,1,1,1,0,0,1)	(6,5,4,7,1,3,2)	(1,1,1,1,0,0,1)	(6,5,4,7,2,3,1)
(0,1,1,1,0,1,0)	(6,5,4,1,7,2,3)	(1,1,1,1,0,1,0)	(6,5,4,2,7,1,3)
(0,1,1,1,0,1,1)	(6,5,4,1,7,3,2)	(1,1,1,1,0,1,1)	(6,5,4,2,7,3,1)
(0,1,1,1,1,0,0)	(6,4,5,7,1,2,3)	(1,1,1,1,1,0,0)	(6,4,5,7,2,1,3)
(0,1,1,1,1,0,1)	(6,4,5,7,1,3,2)	(1,1,1,1,1,0,1)	(6,4,5,7,2,3,1)
(0,1,1,1,1,1,0)	(6,4,5,1,7,2,3)	(1,1,1,1,1,1,0)	(6,4,5,2,7,1,3)
(0,1,1,1,1,1,1)	(6,4,5,1,7,3,2)	(1,1,1,1,1,1,1)	(6,4,5,2,7,3,1)

Appendix B

Mapping table of $G \in F\,(3, 5, 7)$.

x	$G(x)$	x	$G(x)$	x	$G(x)$
(0,0,0,0,0)	(6,1,2,7,3,4,5)	(1,0,0,0,0)	(2,6,1,7,3,5,4)	(2,0,0,0,0)	(2,1,6,7,3,5,4)
(0,0,0,0,1)	(6,3,2,7,1,5,4)	(1,0,0,0,1)	(1,6,3,7,2,5,4)	(2,0,0,0,1)	(1,5,6,7,3,4,2)
(0,0,0,0,2)	(6,3,2,7,4,5,1)	(1,0,0,0,2)	(3,6,2,7,1,4,5)	(2,0,0,0,2)	(2,3,6,7,4,5,1)
(0,0,0,1,0)	(6,2,1,7,5,3,4)	(1,0,0,1,0)	(4,6,1,7,5,3,2)	(2,0,0,1,0)	(2,4,6,7,3,5,1)
(0,0,0,1,1)	(6,1,2,7,5,3,4)	(1,0,0,1,1)	(4,6,2,7,5,3,1)	(2,0,0,1,1)	(4,2,6,7,5,3,1)
(0,0,0,1,2)	(6,3,2,7,5,4,1)	(1,0,0,1,2)	(1,6,2,7,5,3,4)	(2,0,0,1,2)	(3,1,6,7,2,4,5)
(0,0,0,2,0)	(6,1,2,7,3,5,4)	(1,0,0,2,0)	(4,6,1,7,5,2,3)	(2,0,0,2,0)	(4,1,6,7,5,2,3)
(0,0,0,2,1)	(6,3,1,7,2,5,4)	(1,0,0,2,1)	(4,6,1,7,3,2,5)	(2,0,0,2,1)	(4,1,6,7,3,2,5)
(0,0,0,2,2)	(6,3,1,7,4,5,2)	(1,0,0,2,2)	(3,6,4,7,1,2,5)	(2,0,0,2,2)	(3,1,6,7,5,4,2)
(0,0,1,0,0)	(6,2,5,7,1,4,3)	(1,0,1,0,0)	(2,6,5,7,4,1,3)	(2,0,1,0,0)	(3,2,6,7,4,1,5)
(0,0,1,0,1)	(6,2,5,7,3,4,1)	(1,0,1,0,1)	(2,6,3,7,1,4,5)	(2,0,1,0,1)	(4,2,6,7,3,1,5)
(0,0,1,0,2)	(6,3,5,7,4,1,2)	(1,0,1,0,2)	(1,6,3,7,5,4,2)	(2,0,1,0,2)	(3,2,6,7,1,4,5)
(0,0,1,1,0)	(6,2,5,7,1,3,4)	(1,0,1,1,0)	(2,6,5,7,1,3,4)	(2,0,1,1,0)	(2,5,6,7,1,3,4)
(0,0,1,1,1)	(6,5,1,7,2,3,4)	(1,0,1,1,1)	(4,6,5,7,2,3,1)	(2,0,1,1,1)	(4,5,6,7,2,3,1)
(0,0,1,1,2)	(6,2,5,7,4,3,1)	(1,0,1,1,2)	(1,6,2,7,4,3,5)	(2,0,1,1,2)	(2,3,6,7,5,4,1)
(0,0,1,2,0)	(6,4,5,7,1,3,2)	(1,0,1,2,0)	(4,6,5,7,1,2,3)	(2,0,1,2,0)	(4,5,6,7,1,2,3)
(0,0,1,2,1)	(6,2,4,7,1,5,3)	(1,0,1,2,1)	(4,6,5,7,3,2,1)	(2,0,1,2,1)	(4,5,6,7,3,2,1)
(0,0,1,2,2)	(6,1,5,7,4,2,3)	(1,0,1,2,2)	(1,6,5,7,4,3,2)	(2,0,1,2,2)	(3,1,6,7,4,2,5)
(0,0,2,0,0)	(6,4,2,7,3,1,5)	(1,0,2,0,0)	(2,6,4,7,3,1,5)	(2,0,2,0,0)	(2,5,6,7,4,1,3)
(0,0,2,0,1)	(6,3,4,7,2,1,5)	(1,0,2,0,1)	(5,6,3,7,2,1,4)	(2,0,2,0,1)	(5,3,6,7,2,1,4)

x	$G(x)$	x	$G(x)$	x	$G(x)$
(0,0,2,0,2)	(6,3,2,7,4,1,5)	(1,0,2,0,2)	(5,6,3,7,4,1,2)	(2,0,2,0,2)	(5,3,6,7,4,1,2)
(0,0,2,1,0)	(6,4,1,7,5,3,2)	(1,0,2,1,0)	(2,6,4,7,5,1,3)	(2,0,2,1,0)	(3,4,6,7,2,1,5)
(0,0,2,1,1)	(6,5,4,7,2,3,1)	(1,0,2,1,1)	(2,6,4,7,5,3,1)	(2,0,2,1,1)	(3,4,6,7,2,5,1)
(0,0,2,1,2)	(6,5,2,7,4,3,1)	(1,0,2,1,2)	(5,6,3,7,4,2,1)	(2,0,2,1,2)	(5,3,6,7,4,2,1)
(0,0,2,2,0)	(6,4,1,7,5,2,3)	(1,0,2,2,0)	(3,6,1,7,5,2,4)	(2,0,2,2,0)	(3,4,6,7,5,1,2)
(0,0,2,2,1)	(6,5,4,7,3,2,1)	(1,0,2,2,1)	(1,6,5,7,3,2,4)	(2,0,2,2,1)	(3,4,6,7,5,2,1)
(0,0,2,2,2)	(6,5,3,7,4,2,1)	(1,0,2,2,2)	(5,6,1,7,4,2,3)	(2,0,2,2,2)	(5,1,6,7,4,2,3)
(0,1,0,0,0)	(6,1,3,2,7,5,4)	(1,1,0,0,0)	(3,6,5,4,7,1,2)	(2,1,0,0,0)	(3,5,6,4,7,1,2)
(0,1,0,0,1)	(6,3,2,4,7,5,1)	(1,1,0,0,1)	(3,6,2,5,7,4,1)	(2,1,0,0,1)	(4,1,6,5,7,3,2)
(0,1,0,0,2)	(6,3,2,5,7,4,1)	(1,1,0,0,2)	(3,6,5,2,7,4,1)	(2,1,0,0,2)	(3,5,6,2,7,4,1)
(0,1,0,1,0)	(6,4,2,5,7,3,1)	(1,1,0,1,0)	(4,6,1,2,7,3,5)	(2,1,0,1,0)	(4,1,6,2,7,5,3)
(0,1,0,1,1)	(6,2,1,5,7,3,4)	(1,1,0,1,1)	(3,6,2,4,7,5,1)	(2,1,0,1,1)	(4,2,6,1,7,5,3)
(0,1,0,1,2)	(6,5,2,1,7,4,3)	(1,1,0,1,2)	(4,6,3,1,7,5,2)	(2,1,0,1,2)	(4,3,6,1,7,5,2)
(0,1,0,2,0)	(6,2,1,3,7,5,4)	(1,1,0,2,0)	(4,6,1,2,7,5,3)	(2,1,0,2,0)	(4,1,6,3,7,5,2)
(0,1,0,2,1)	(6,3,1,4,7,5,2)	(1,1,0,2,1)	(4,6,1,3,7,5,2)	(2,1,0,2,1)	(4,2,6,3,7,5,1)
(0,1,0,2,2)	(6,5,2,3,7,4,1)	(1,1,0,2,2)	(4,6,2,3,7,5,1)	(2,1,0,2,2)	(5,1,6,3,7,4,2)
(0,1,1,0,0)	(6,3,5,2,7,1,4)	(1,1,1,0,0)	(4,6,5,2,7,1,3)	(2,1,1,0,0)	(4,5,6,2,7,1,3)
(0,1,1,0,1)	(6,2,3,5,7,4,1)	(1,1,1,0,1)	(5,6,2,4,7,1,3)	(2,1,1,0,1)	(5,2,6,4,7,1,3)
(0,1,1,0,2)	(6,3,5,2,7,4,1)	(1,1,1,0,2)	(4,6,3,5,7,1,2)	(2,1,1,0,2)	(4,3,6,5,7,1,2)
(0,1,1,1,0)	(6,2,5,4,7,3,1)	(1,1,1,1,0)	(5,6,2,1,7,3,4)	(2,1,1,1,0)	(5,2,6,1,7,3,4)
(0,1,1,1,1)	(6,2,5,1,7,3,4)	(1,1,1,1,1)	(4,6,5,1,7,3,2)	(2,1,1,1,1)	(4,5,6,1,7,3,2)
(0,1,1,1,2)	(6,3,5,1,7,4,2)	(1,1,1,1,2)	(3,6,4,1,7,5,2)	(2,1,1,1,2)	(5,2,6,1,7,4,3)
(0,1,1,2,0)	(6,2,5,3,7,1,4)	(1,1,1,2,0)	(4,6,5,3,7,1,2)	(2,1,1,2,0)	(4,5,6,3,7,1,2)
(0,1,1,2,1)	(6,5,1,3,7,2,4)	(1,1,1,2,1)	(4,6,5,3,7,2,1)	(2,1,1,2,1)	(4,5,6,3,7,2,1)
(0,1,1,2,2)	(6,4,5,3,7,2,1)	(1,1,1,2,2)	(5,6,1,3,7,4,2)	(2,1,1,2,2)	(5,2,6,3,7,4,1)
(0,1,2,0,0)	(6,5,4,2,7,1,3)	(1,1,2,0,0)	(5,6,3,2,7,1,4)	(2,1,2,0,0)	(5,3,6,2,7,1,4)
(0,1,2,0,1)	(6,4,3,2,7,1,5)	(1,1,2,0,1)	(5,6,3,4,7,1,2)	(2,1,2,0,1)	(5,3,6,4,7,1,2)
(0,1,2,0,2)	(6,5,3,2,7,4,1)	(1,1,2,0,2)	(5,6,3,2,7,4,1)	(2,1,2,0,2)	(5,3,6,2,7,4,1)
(0,1,2,1,0)	(6,4,2,1,7,3,5)	(1,1,2,1,0)	(5,6,4,1,7,3,2)	(2,1,2,1,0)	(5,4,6,1,7,3,2)
(0,1,2,1,1)	(6,5,4,1,7,3,2)	(1,1,2,1,1)	(5,6,3,4,7,2,1)	(2,1,2,1,1)	(5,3,6,4,7,2,1)
(0,1,2,1,2)	(6,3,4,5,7,2,1)	(1,1,2,1,2)	(5,6,4,1,7,2,3)	(2,1,2,1,2)	(5,4,6,1,7,2,3)
(0,1,2,2,0)	(6,5,4,3,7,1,2)	(1,1,2,2,0)	(5,6,4,2,7,3,1)	(2,1,2,2,0)	(5,4,6,2,7,3,1)
(0,1,2,2,1)	(6,5,4,3,7,2,1)	(1,1,2,2,1)	(5,6,4,3,7,1,2)	(2,1,2,2,1)	(5,4,6,3,7,1,2)
(0,1,2,2,2)	(6,4,3,1,7,2,5)	(1,1,2,2,2)	(5,6,4,3,7,2,1)	(2,1,2,2,2)	(5,4,6,3,7,2,1)

x	$G(x)$	x	$G(x)$	x	$G(x)$
(0,2,0,0,0)	(6,4,1,5,3,7,2)	(1,2,0,0,0)	(3,6,5,4,1,7,2)	(2,2,0,0,0)	(3,5,6,4,1,7,2)
(0,2,0,0,1)	(6,3,2,4,1,7,5)	(1,2,0,0,1)	(4,6,1,5,3,7,2)	(2,2,0,0,1)	(4,1,6,5,3,7,2)
(0,2,0,0,2)	(6,3,2,5,4,7,1)	(1,2,0,0,2)	(3,6,5,2,4,7,1)	(2,2,0,0,2)	(3,5,6,2,4,7,1)
(0,2,0,1,0)	(6,1,4,2,5,7,3)	(1,2,0,1,0)	(4,6,1,2,5,7,3)	(2,2,0,1,0)	(4,1,6,2,5,7,3)
(0,2,0,1,1)	(6,2,4,1,5,7,3)	(1,2,0,1,1)	(4,6,2,1,5,7,3)	(2,2,0,1,1)	(4,2,6,1,5,7,3)
(0,2,0,1,2)	(6,3,2,1,5,7,4)	(1,2,0,1,2)	(4,6,3,1,5,7,2)	(2,2,0,1,2)	(4,3,6,1,5,7,2)
(0,2,0,2,0)	(6,4,2,3,5,7,1)	(1,2,0,2,0)	(4,6,1,3,5,7,2)	(2,2,0,2,0)	(4,1,6,3,5,7,2)
(0,2,0,2,1)	(6,1,2,3,5,7,4)	(1,2,0,2,1)	(4,6,2,3,5,7,1)	(2,2,0,2,1)	(4,2,6,3,5,7,1)
(0,2,0,2,2)	(6,3,1,5,4,7,2)	(1,2,0,2,2)	(5,6,1,3,4,7,2)	(2,2,0,2,2)	(5,1,6,3,4,7,2)
(0,2,1,0,0)	(6,3,5,2,1,7,4)	(1,2,1,0,0)	(4,6,5,2,1,7,3)	(2,2,1,0,0)	(4,5,6,2,1,7,3)
(0,2,1,0,1)	(6,5,1,4,2,7,3)	(1,2,1,0,1)	(5,6,2,4,1,7,3)	(2,2,1,0,1)	(5,2,6,4,1,7,3)
(0,2,1,0,2)	(6,3,5,2,4,7,1)	(1,2,1,0,2)	(4,6,3,5,1,7,2)	(2,2,1,0,2)	(4,3,6,5,1,7,2)
(0,2,1,1,0)	(6,1,5,4,2,7,3)	(1,2,1,1,0)	(5,6,2,1,3,7,4)	(2,2,1,1,0)	(5,2,6,1,3,7,4)
(0,2,1,1,1)	(6,2,5,1,3,7,4)	(1,2,1,1,1)	(4,6,5,1,3,7,2)	(2,2,1,1,1)	(4,5,6,1,3,7,2)
(0,2,1,1,2)	(6,4,5,1,2,7,3)	(1,2,1,1,2)	(5,6,2,1,4,7,3)	(2,2,1,1,2)	(5,2,6,1,4,7,3)
(0,2,1,2,0)	(6,2,5,3,1,7,4)	(1,2,1,2,0)	(4,6,5,3,1,7,2)	(2,2,1,2,0)	(4,5,6,3,1,7,2)
(0,2,1,2,1)	(6,5,1,3,2,7,4)	(1,2,1,2,1)	(4,6,5,3,2,7,1)	(2,2,1,2,1)	(4,5,6,3,2,7,1)
(0,2,1,2,2)	(6,3,5,1,4,7,2)	(1,2,1,2,2)	(5,6,2,3,4,7,1)	(2,2,1,2,2)	(5,2,6,3,4,7,1)
(0,2,2,0,0)	(6,5,3,4,1,7,2)	(1,2,2,0,0)	(5,6,3,2,1,7,4)	(2,2,2,0,0)	(5,3,6,2,1,7,4)
(0,2,2,0,1)	(6,5,1,4,3,7,2)	(1,2,2,0,1)	(5,6,3,4,1,7,2)	(2,2,2,0,1)	(5,3,6,4,1,7,2)
(0,2,2,0,2)	(6,5,3,2,4,7,1)	(1,2,2,0,2)	(5,6,3,2,4,7,1)	(2,2,2,0,2)	(5,3,6,2,4,7,1)
(0,2,2,1,0)	(6,4,2,1,3,7,5)	(1,2,2,1,0)	(5,6,4,1,3,7,2)	(2,2,2,1,0)	(5,4,6,1,3,7,2)
(0,2,2,1,1)	(6,5,4,1,3,7,2)	(1,2,2,1,1)	(5,6,3,4,2,7,1)	(2,2,2,1,1)	(5,3,6,4,2,7,1)
(0,2,2,1,2)	(6,5,3,1,4,7,2)	(1,2,2,1,2)	(5,6,4,1,2,7,3)	(2,2,2,1,2)	(5,4,6,1,2,7,3)
(0,2,2,2,0)	(6,5,4,3,1,7,2)	(1,2,2,2,0)	(5,6,4,2,3,7,1)	(2,2,2,2,0)	(5,4,6,2,3,7,1)
(0,2,2,2,1)	(6,5,4,3,2,7,1)	(1,2,2,2,1)	(5,6,4,3,1,7,2)	(2,2,2,2,1)	(5,4,6,3,1,7,2)
(0,2,2,2,2)	(6,5,2,3,4,7,1)	(1,2,2,2,2)	(5,6,4,3,2,7,1)	(2,2,2,2,2)	(5,4,6,3,2,7,1)

Mapping table of $H \in F$ (3, 4, 6).

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

Mapping table of $R \in F\,(3, 3, 5)$.

x	$R(x)$	x	$R(x)$	x	$R(x)$
(0,0,0)	(1,2,3,5,4)	(1,0,0)	(4,1,3,5,2)	(2,0,0)	(4,2,1,5,3)
(0,0,1)	(1,4,3,5,2)	(1,0,1)	(5,1,3,4,2)	(2,0,1)	(5,4,1,3,2)
(0,0,2)	(1,5,3,4,2)	(1,0,2)	(2,1,3,5,4)	(2,0,2)	(2,5,1,4,3)
(0,1,0)	(1,2,4,5,3)	(1,1,0)	(3,1,4,5,2)	(2,1,0)	(3,2,1,5,4)
(0,1,1)	(1,4,2,5,3)	(1,1,1)	(5,1,4,3,2)	(2,1,1)	(3,4,1,5,2)
(0,1,2)	(1,5,4,3,2)	(1,1,2)	(2,1,4,5,3)	(2,1,2)	(3,5,1,4,2)
(0,2,0)	(1,2,5,4,3)	(1,2,0)	(4,1,5,3,2)	(2,2,0)	(4,3,1,5,2)
(0,2,1)	(1,4,5,3,2)	(1,2,1)	(5,1,2,4,3)	(2,2,1)	(5,3,1,4,2)
(0,2,2)	(1,3,5,4,2)	(1,2,2)	(2,1,5,4,3)	(2,2,2)	(2,3,1,5,4)

Mapping table of $S \in F\,(3, 3, 5)$.

x	$S(x)$	x	$S(x)$	x	$S(x)$
(0,0,0)	(2,1,3,4,5)	(1,0,0)	(4,2,3,1,5)	(2,0,0)	(4,1,2,5,3)
(0,0,1)	(2,4,3,1,5)	(1,0,1)	(5,2,3,1,4)	(2,0,1)	(5,4,2,1,3)
(0,0,2)	(2,5,3,1,4)	(1,0,2)	(1,2,3,5,4)	(2,0,2)	(1,5,2,4,3)
(0,1,0)	(2,1,4,5,3)	(1,1,0)	(3,2,4,1,5)	(2,1,0)	(3,1,2,5,4)
(0,1,1)	(2,4,1,5,3)	(1,1,1)	(5,2,4,1,3)	(2,1,1)	(3,4,2,1,5)
(0,1,2)	(2,5,4,1,3)	(1,1,2)	(1,2,4,5,3)	(2,1,2)	(3,5,2,1,4)
(0,2,0)	(2,1,5,4,3)	(1,2,0)	(4,2,5,1,3)	(2,2,0)	(4,3,2,1,5)
(0,2,1)	(2,4,5,1,3)	(1,2,1)	(5,2,1,4,3)	(2,2,1)	(5,3,2,1,4)
(0,2,2)	(2,3,5,1,4)	(1,2,2)	(1,2,5,4,3)	(2,2,2)	(1,3,2,5,4)

Mapping table of $T \in F$ (3, 4, 6).

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