PAPER Special Section on Signal Design and Its Applications in Communications

A New Construction of Permutation Arrays*

Jung Youl PARK[†a)], ***Member and*** **Hong-Yeop SONG**[††b)], ***Nonmember***

SUMMARY Let $PA(n, d)$ be a permutation array (PA) of order n and the minimum distance d. We propose a new construction of the permutation array $PA\left(p^m, p^{m-1}k\right)$ for a given prime number p, a positive integer $k < p$ and a positive integer m. The resulted array has $\left(|PA(p, k)| \cdot p^{(m-1)(p-k)}\right)^m$ rows. Compared to the other constructions, the new construction gives a permutation array of far bigger size with a large minimum distance, for example, when $k \geq 2p/3$. Moreover the proposed construction provides an algorithm to find the i-th row of $PA\left(p^m, p^{m-1}k\right)$ for a given index i very simply.

key words: *permutation array, error correcting code*

1. Introduction

Permutation codes were introduced first in [1] for communications over discrete channels such as powerlines [19]. Let n be a positive integer and S_n be the symmetric group of order n. An element $\eta \in S_n$ is usually represented as an n-tuple of integers from its images:

$$\eta = (\eta(1), \eta(2), \ldots, \eta(n)) .$$

With this representation, we define a Hamming distance function d_H on S_n as follows:

$$d_H(\eta_1, \eta_2) = \left|\{i \mid 1 \leq i \leq n, \eta_1(i) \neq \eta_2(i)\}\right|, \quad (1)$$

for $\eta_1, \eta_2 \in S_n$. Since (S_n, d_H) is a metric space, we can construct a permutation code with a minimum distance d on S_n by considering each permutation as a codeword. If we write them as rows, we obtain an array with n columns whose rows are permutations with a minimum distance d. This array is called a permutation array (PA) and denoted by $PA(n, d)$. The number of rows of $PA(n, d)$ is often denoted by $|PA(n, d)|$. See [5, §VI.44] for some known results for $|PA(n, d)|$.

Manuscript received January 17, 2012.
Manuscript revised June 1, 2012.
†The author is with the Attached Institute of ETRI, Daejeon, Korea.
††The author is with the School of Electrical and Electronic Engineering, Yonsei University, Seoul, Korea.
*This paper is a full version of 2011 IWSDA proceeding paper titled “An extended construction of permutation arrays with a polynomial-time sampling algorithm.” This paper is the result of research performed in Yonsei University while the author J.Y. Park was working as a Post-Doc Research Associate in TMS BK21 Institute of Yonsei University.
a) E-mail: xenore@ensec.re.kr
b) E-mail: hysong@yonsei.ac.kr
DOI: 10.1587/transfun.E95.A.1855

In the research of permutation arrays, the most important issue is to construct a permutation array with a large number of rows for given n and d, see e.g., [1], [2], [4], [6]–[12] and [18]. Another issue, which is considered less in literature, is to find the row of the array corresponding to a given index. This issue has been treated explicitly in only [6], and in no others, as far as authors are aware.

In this paper we first propose a new construction of permutation arrays $PA\left(p^2, pk\right)$ from $PA(p, k)$ for a prime number p and a positive integer $k < p$. Then we extend the construction to $PA\left(p^m, p^{m-1}k\right)$ for a integer $m \geq 2$. We also show that all the proposed construction provide algorithms to pick up the designated row from the arrays for a given index in a natural way.

2. Previous Results

There are mainly two categories of constructions of $PA(n, d)$; one is to decide its rows one by one in a brute-force manner, and the other is a class of systematic constructions.

The most traditional approach in the first category is to place as many balls of radius $d/2$ into S_n as possible. Similarly one can do a clique search in a graph $G(n, d)$ whose vertices are elements in S_n and edges are connected between two permutations with Hamming distance $\geq d$. A greedy algorithm and a search via automorphisms can be also applied as shown in [6] or [18]. These constructions are based basically on an exhaustive search; hence it is hard to find the row for any given index unless we store the whole array.

For the second category, there are two kinds of notable constructions [4], [6], [12] that provide algorithms to find the designated rows implicitly. Let $\{0, 1\}^n$ be a set of binary vectors of length n. A map f from $\{0, 1\}^n$ to S_n is called an n-distance-preserving map (n-DPM) if

$$d_H(f(\mathbf{a}), f(\mathbf{b})) \geq d(\mathbf{a}, \mathbf{b}) \quad (2)$$

is satisfied for any $\mathbf{a}, \mathbf{b} \in \{0, 1\}^n$. A proper construction of n-DPMs are given in [4], and they proposed to construct $PA(n, d)$ by applying a DPM onto an (n, d)-binary code. As a result, they constructed $PA(n, d)$ whose cardinality is the same as that of the (n, d)-binary code. Similar construction based on ternary codes are given in [12]. These constructions are simple, but the arrays have relatively small number of rows because of the Singleton bound and the Plotkin bound. Especially the Plotkin bound [15] and its analogy

[13] show that the cardinality of an (n, d)-binary code for $d \geq n/2$ is at most $2n + 2$, and that of an (n, d)-ternary code for $d \geq 2n/3$ is at most $3n$.

Another kind of construction is based on some kind of *divide-and-conquer* strategy [6]. When we construct $PA(n, d)$, first we compute $PA(n_i, d_i)$ for $i = 1, \ldots, k$, such that $\sum_{i=1}^{k} n_i = n$ and the sum of any l of d_i's is larger than or equal to d for some positive integer l. Then we can use transversals of distance l and type $|PA(n_1, d_1)|, |PA(n_2, d_2)|, \ldots, |PA(n_k, d_k)|$ to choose k rows, one row from each $PA(n_i, d_i)$. Combining them, we produce rows of a permutation array $PA(n, d)$. Though this algorithm gives a PA with a large number of rows, too much precomputation is required on finding enough number of such transversals.

3. A New Construction of $PA\left(p^2, pk\right)$

3.1 Notation

Let p be a prime number, $\mathbb{F}_p$ be a finite field of p elements and $S_{\mathbb{F}_p \times \mathbb{F}_p}$ be a set of permutations on $\mathbb{F}_p \times \mathbb{F}_p$. $S_{\mathbb{F}_p \times \mathbb{F}_p}$ can be easily identified with S_{p^2} via a natural map from $\mathbb{F}_p \times \mathbb{F}_p$ to $\left\{1, 2, \ldots, p^2\right\}$, given by $(a, b) \mapsto p \cdot a + b + 1$.

Let $\mathcal{P}_{p,k}$ be the set of permutations obtained from the rows of $PA(p, k)$ by considering the rows as defined over $\mathbb{F}_p$, instead of $\{1, 2, \ldots, p\}$. And let $\mathcal{Q}_{p,k}$ be the set of polynomial functions induced by all the polynomials of degrees at most $p - k$ defined over $\mathbb{F}_p$ whose constant terms are zero, but including the zero polynomial itself. Observe that $(t_1 - t_2)(x) = 0$ has at most $p - k$ solutions over $\mathbb{F}_p$ for any two polynomials $t_1, t_2 \in \mathcal{Q}_{p,k}$.

3.2 The Construction Proposed

We define a map

$$\phi : \mathcal{P}_{p,k} \times \mathcal{P}_{p,k} \times \mathcal{Q}_{p,k} \times \mathcal{Q}_{p,k} \hookrightarrow S_{\mathbb{F}_p \times \mathbb{F}_p} \tag{3}$$

by

$$\begin{aligned}\phi(s_1, s_2, t_1, t_2)(x, y) \\ = \Big(s_1(x+t_1(y)), s_2\Big(y+t_2\Big(s_1(x+t_1(y))\Big)\Big)\Big),\end{aligned} \tag{4}$$

where $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$. For convenience, we denote $\phi(s_1, s_2, t_1, t_2)$ by ϕ_{s_1,s_2,t_1,t_2}. It is easy to check that ϕ_{s_1,s_2,t_1,t_2} is a permutation on $\mathbb{F}_p \times \mathbb{F}_p$. The images of ϕ are the rows of $PA\left(p^2, pk\right)$.

Theorem 1: The map ϕ generates a $PA\left(p^2, pk\right)$ whose number of rows is $\left(\left|\mathcal{P}_{p,k}\right| \cdot \left|\mathcal{Q}_{p,k}\right|\right)^2$.

When $k = 2$, we have the powerful corollary.

Corollary 1: The map ϕ generates a $PA\left(p^2, 2p\right)$ with $\left(p! \cdot p^{p-2}\right)^2$ rows.

Proof Since a distance between two distinct permutations is at least 2, $\mathcal{P}_{p,2} = S_p$. □

We need the following lemma to prove Theorem 1.

Lemma 1: Let $(s, t) \neq (u, v)$ be two distinct elements in $\mathcal{P}_{p,k} \times \mathcal{Q}_{p,k}$. Then

$$s(x + t(y)) = u(x + v(y)) \tag{5}$$

has at most $p(p - k)$ solutions $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$.

Proof Suppose that $s = u$. (5) is equivalent to

$$t(y) = v(y). \tag{6}$$

Since $t \neq v$ and $t, v \in \mathcal{Q}_{p,k}$, (6) has at most $p - k$ solutions; thus (5) has at most $p(p - k)$ solutions.

When $s \neq u$, let $\delta = x + t(y)$. If $t = v$, (5) is equivalent to

$$s(\delta) = u(\delta), \tag{7}$$

which has at most $p - k$ solutions since $d_H(s, u) \geq k$. Let us write them by $\delta_1, \delta_2, \ldots, \delta_l$ where $l \leq p - k$. For each δ_i,

$$\delta_i = x + t(y) \Leftrightarrow x = \delta_i - t(y) \tag{8}$$

has at most p solutions for (x, y); hence (7) have at most $p(p - k)$ solutions. Finally suppose that $s \neq u$ and $t \neq v$. When we write $(v - t)(y) = \epsilon$, (5) is equivalent to

$$s(\delta) = u(\delta + \epsilon). \tag{9}$$

For each $\delta = \delta_0 \in \mathbb{F}_p$, there is exactly one value for ϵ satisfying the above equation since s and u are permutations. Let us denote it by ϵ_{δ_0}. Clearly

$$\epsilon_{\delta_0} = (v - t)(y) \tag{10}$$

has at most $p-k$ solutions for y because $v-t \in \mathcal{Q}_{p,k}$ and $t \neq v$. Since x is determined uniquely from δ and y, we conclude that (5) has at most $p(p - k)$ solutions again. □

Proof [Proof of Theorem 1] It suffices to show that

$$d_H(\phi_{s_1,s_2,t_1,t_2}, \phi_{u_1,u_2,v_1,v_2}) \geq pk, \tag{11}$$

or equivalently,

$$\phi_{s_1,s_2,t_1,t_2}(x, y) = \phi_{u_1,u_2,v_1,v_2}(x, y) \tag{12}$$

has at most $p(p-k)$ solutions $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ for two distinct elements $(s_1, s_2, t_1, t_2), (u_1, u_2, v_1, v_2) \in \mathcal{P}_{p,k} \times \mathcal{P}_{p,k} \times \mathcal{Q}_{p,k} \times \mathcal{Q}_{p,k}$. From (12), we have the following system:

$$\begin{cases} s_1(x + t_1(y)) = u_1(x + v_1(y)), & \text{(13a)} \\ s_2(y + t_2(z)) = u_2(y + v_2(z)), & \text{(13b)} \end{cases}$$

where $z = s_1(x + t_1(y)) = u_1(x + v_1(y))$. Note that if $(s_1, s_2, t_1, t_2) \neq (u_1, u_2, v_1, v_2)$, then $(s_1, t_1) \neq (u_1, v_1)$ or $(s_2, t_2) \neq (u_2, v_2)$. When $(s_1, t_1) \neq (u_1, v_1)$, Lemma 1 shows that (13a) has at most $p(p - k)$ solutions. Similarly, (13b) has at most $p(p - k)$ solutions if $(s_2, t_2) \neq (u_2, v_2)$. Thus (12) has at most $p(p-k)$ solutions, as desired. □

4. Extension to $PA\left(p^m, p^{m-1}k\right)$

The construction of $PA\left(p^2, pk\right)$ can be extended to construct $PA\left(p^m, p^{m-1}k\right)$ for $m \geq 2$ easily [16]. Let $\mathcal{P}_{p,k}$ and $\mathcal{Q}_{p,k}$ be defined as in the previous section.

4.1 First Extension

We extend ϕ coordinate-wise to define the map

$$\varphi : \mathcal{P}_{p,k}^m \times \mathcal{Q}_{p,k}^m \hookrightarrow S_{(\mathbb{F}_p)^m} \tag{14}$$

by

$$\begin{aligned}\varphi(s_1, \ldots, s_m, t_1, \ldots, t_m)(x_1, \ldots, x_m) &= \big(s_1(x_1 + t_1(x_2)), \\ &\quad s_2(x_2 + t_2(x_3)), \\ &\quad \ldots, \\ &\quad s_m(x_m + t_m(s_1(x_1 + t_1(x_2))))\big).\end{aligned} \tag{15}$$

Clearly φ induces permutations on $\left(\mathbb{F}_p\right)^m$.

Theorem 2: We can construct a $PA\left(p^m, p^{m-1}k\right)$ whose number of rows is $\left(\left|\mathcal{P}_{p,k}\right| \cdot \left|\mathcal{Q}_{p,k}\right|\right)^m$ from the map φ.

Proof Analogy of the proof of Theorem 1. □

4.2 Second Extension

For the second extension, first we define a coordinate function

$$f : \mathcal{P}_{p,k} \times \mathcal{Q}_{p,k}^{m-1} \times \left(\mathbb{F}_p\right)^m \to \mathbb{F}_p \tag{16}$$

by

$$f(g, h_1, \ldots, h_{m-1}; y_1, \ldots, y_m) = g\left(y_1 + \sum_{j=1}^{m-1} h_j\left(y_{j+1}\right)\right). \tag{17}$$

Here additions are done over $\mathbb{F}_p$. Let $(x_1, x_2, \ldots, x_m)$ be an element of $\mathbb{F}_p^m$. For $s_1, s_2, \ldots, s_m \in \mathcal{P}_{p,k}$ and $t_{1,1}, t_{1,2}, \ldots, t_{m,m-1} \in \mathcal{Q}_{p,k}$, we define $x_{m+1}, \ldots, x_{2m}$ by

$$x_{m+i} = f(s_i, t_{i,1}, \ldots, t_{i,m-1}; x_i, \ldots, x_{m+i-1}), \tag{18}$$

for $i = 1, 2, \ldots, m$. Now the map

$$\psi : \mathcal{P}_{p,k}^m \times \mathcal{Q}_{p,k}^{m(m-1)} \hookrightarrow S_{(\mathbb{F}_p)^m} \tag{19}$$

is defined by

$$\begin{aligned}\psi(s_1, \ldots, s_m, t_{1,1}, t_{1,2}, \ldots, t_{m,m-1})(x_1, \ldots, x_m) &= \big(f(s_1, t_{1,1}, \ldots, t_{1,m-1}; x_1, \ldots, x_m), \\ &\quad f(s_2, t_{2,1}, \ldots, t_{2,m-1}; x_2, \ldots, x_{m+1}), \\ &\quad \ldots, \\ &\quad f(s_m, t_{m,1}, \ldots, t_{m,m-1}; x_m, \ldots, x_{2m-1})\big) \\ &= (x_{m+1}, x_{m+2}, \ldots, x_{2m}),\end{aligned} \tag{20}$$

where $(x_1, \ldots, x_m) \in \left(\mathbb{F}_p\right)^m$. When we need to specify the functions s_i's and t_i's, we will use the notation $x_{m+j}^{(s,t)}$ for x_{m+j}. We need to verify that ψ generates the permutations on $\left(\mathbb{F}_p\right)^m$.

Lemma 2: The image of ψ is $S_{(\mathbb{F}_p)^m}$.

Proof Suppose that $\psi(s_1, \ldots, s_m, t_{1,1}, t_{1,2}, \ldots, t_{m,m-1})$ is not a permutation on $\left(\mathbb{F}_p\right)^m$ for some $s_1, \ldots, s_m \in \mathcal{P}_{p,k}$ and $t_{1,1}, t_{1,2}, \ldots, t_{m,m-1} \in \mathcal{Q}_{p,k}$. Then we can choose two distinct $(x_1, \ldots, x_m), (y_1, \ldots, y_m) \in \left(\mathbb{F}_p\right)^m$ such that

$$\begin{aligned}&\psi(s_1, \ldots, s_m, t_{1,1}, t_{1,2}, \ldots, t_{m,m-1})(x_1, \ldots, x_m) \\ &\quad = \psi(s_1, \ldots, s_m, t_{1,1}, t_{1,2}, \ldots, t_{m,m-1})(y_1, \ldots, y_m),\end{aligned} \tag{21}$$

or equivalently,

$$x_{m+i} = y_{m+i} \qquad \forall i = 1, \ldots, m. \tag{22}$$

From (17) and (18), the equality $x_{2m} = y_{2m}$ implies that

$$x_m + \sum_{j=1}^{m-1} t_{m,j}\left(x_{m+j}\right) = y_m + \sum_{j=1}^{m-1} t_{m,j}\left(y_{m+j}\right), \tag{23}$$

and we get $x_m = y_m$. Similarly we can show that $x_i = y_i$ for $i = m-1, m-2, \ldots, 1$, which contradicts the choice that $(x_1, \ldots, x_m) \neq (y_1, \ldots, y_m)$. □

As it is intended, ψ generates rows of $PA\left(p^m, p^{m-1}k\right)$.

Theorem 3: The map ψ generates a $PA\left(p^m, p^{m-1}k\right)$ whose number of rows is $\left(\left|\mathcal{P}_{p,k}\right| \cdot \left|\mathcal{Q}_{p,k}\right|^{m-1}\right)^m$.

We will prove Theorem 3 using following two lemmas.

Lemma 3: Let $h_1, \ldots, h_{m-1}$ be polynomial functions in $\mathcal{Q}_{p,k}$ and $c \in \mathbb{F}_p$ be a constant. If h_j is not a zero function for some $1 \leq j \leq m-1$, then

$$h_1(y_2) + h_2(y_3) + \cdots + h_{m-1}(y_m) + c = 0 \tag{24}$$

has at most $p^{m-2}(p-k)$ solutions for $(y_2, \ldots, y_m) \in \left(\mathbb{F}_p\right)^{m-1}$.

Proof Without loss of generality, we may assume that h_1 is not a zero function. Then for each $y_3, \ldots, y_m \in \mathbb{F}_p$, (24) has at most $p-k$ solutions for $y_2 \in \mathbb{F}_p$ since $\deg(h_1) \leq p-k$. Thus (24) has at most $p^{m-2}(p-k)$ solutions for $(y_2, \ldots, y_m) \in \left(\mathbb{F}_p\right)^{m-1}$. □

Lemma 4: Let $(s, t_1, \ldots, t_{m-1})$ and $(u, v_1, \ldots, v_{m-1})$ be two distinct elements of $\mathcal{P}_{p,k} \times Q_{p,k}^{m-1}$, then

$$f(s, t_1, \ldots, t_{m-1}; y_1, \ldots, y_m) = f(u, v_1, \ldots, v_{m-1}; y_1, \ldots, y_m) \tag{25}$$

has at most $p^{m-1}(p-k)$ solutions for $(y_1, y_2, \ldots, y_m) \in \left(\mathbb{F}_p\right)^m$.

Proof First suppose that $s = u$, then (25) is equivalent to

$$(t_1 - v_1)(y_2) + \cdots + (t_{m-1} - v_{m-1})(y_m) = 0. \tag{26}$$

Thus from Lemma 3 with $h_i = t_i - v_i$ and $c = 0$, (26) has at most $p^{m-2}(p-k)$ solutions for $(y_2, \ldots, y_m)$, and so (25) has at most $p^{m-1}(p-k)$ solutions for $(y_1, \ldots, y_m)$ in this case. Now suppose that $s \neq u$. Let us define δ and ϵ by

$$\delta = y_1 + t_1(y_2) + \cdots + t_{m-1}(y_m), \tag{27}$$
$$\epsilon = (v_1 - t_1)(y_2) + \cdots + (v_{m-1} - t_{m-1})(y_m). \tag{28}$$

If $t_i = v_i$ for all $i = 1, \ldots, m-1$, then $\epsilon = 0$ and (25) is equivalent to

$$s(\delta) = u(\delta), \tag{29}$$

which has at most $p - k$ solutions for $\delta \in \mathbb{F}_p$. Let us write them by $\delta_1, \ldots, \delta_l$ for some $l \leq p - k$. For each δ_i, (27) has at most p^{m-1} solutions for $y_1, \ldots, y_m \in \mathbb{F}_p$ since $y_1 = \delta_i - \sum_{j=1}^{m-1} t_j\left(y_{j+1}\right)$ is determined uniquely by each $(y_2, \ldots, y_m) \in \left(\mathbb{F}_p\right)^{m-1}$. Thus, (25) has $p^{m-1}(p-k)$ solutions in total.

Finally, assume that $t_j \neq v_j$ for some j, then $\epsilon \neq 0$ and (25) is equivalent to

$$s(\delta) = u(\delta + \epsilon). \tag{30}$$

For each $\delta = \delta_0 \in \mathbb{F}_p$, there exists exactly one ϵ satisfying (30), since s and u are permutations. Let us denote it by ϵ_{δ_0}. From Lemma 3 with $h_i = v_i - t_i$ and $c = -\epsilon_{\delta_0}$, the equation (28) has at most $p^{m-2}(p-k)$ solutions for $y_2, \ldots, y_m$. Thus we have at most $p^{m-1}(p-k)$ numbers of m-tuples of $(\delta_0, y_2, \ldots, y_m)$ satisfying (28) and (30) simultaneously. From each m-tuple, y_1 is determined uniquely by (27); hence we conclude that (25) has at most $p^{m-1}(p-k)$ solutions $y_1, \ldots, y_m \in \mathbb{F}_p$. □

Now we are ready to prove Theorem 3.

Proof of Theorem 3 Let $(s_1, \ldots, s_m, t_{1,1}, \ldots, t_{m,m-1})$ and $(u_1, \ldots, u_m, v_{1,1}, \ldots, v_{m,m-1})$ be two distinct elements of $\mathcal{P}_{p,k}^m \times Q_{p,k}^{m(m-1)}$. It is sufficient to show that

$$\psi(s_1, \ldots, s_m, t_{1,1}, \ldots, t_{m,m-1})(x_1, \ldots, x_m) = \psi(u_1, \ldots, u_m, v_{1,1}, \ldots, v_{m,m-1})(x_1, \ldots, x_m), \tag{31}$$

or equivalently,

$$\left(x_{m+1}^{(s,t)}, \ldots, x_{2m}^{(s,t)}\right) = \left(x_{m+1}^{(u,v)}, \ldots, x_{2m}^{(u,v)}\right) \tag{32}$$

has at most $p^{m-1}(p-k)$ solutions for $(x_1, \ldots, x_m) \in \left(\mathbb{F}_p\right)^m$. Since $x_{m+1}^{(s,t)}, \ldots, x_{2m}^{(s,t)}$ and $x_{m+1}^{(u,v)}, \ldots, x_{2m}^{(u,v)}$ are same pairwise,we may denote them by $x_{m+1}, \ldots x_{2m}$. Clearly there exists some i_0 such that

$$(s_{i_0}, t_{i_0,1}, \ldots, t_{i_0,m-1}) \neq (u_{i_0}, v_{i_0,1}, \ldots, v_{i_0,m-1}), \tag{33}$$

so we examine the i_0-th coordinate of (31):

$$f(s_{i_0}, t_{i_0,1}, \ldots, t_{i_0,m-1}; x_{i_0}, \ldots, x_{i_0+m-1}) = f(u_{i_0}, v_{i_0,1}, \ldots, v_{i_0,m-1}; x_{i_0}, \ldots, x_{i_0+m-1}). \tag{34}$$

From Lemma 4 and (33), there exist at most $p^{m-1}(p-k)$ solutions for $(x_{i_0}, \ldots, x_{i_0+m-1}) \in \left(\mathbb{F}_p\right)^m$ satisfying (34).

Note that (18) implies the explicit formula

$$x_i = s_i^{-1}(x_{i+m}) - \sum_{j=1}^{m-1} t_{i,j}\left(x_{i+j}\right), \tag{35}$$

so we can compute x_i uniquely from $x_{i+1}, \ldots, x_{i+m}$ for $i = 1, \ldots, m$. Consequently we can determine $x_1, \ldots, x_m$ associated to $x_{i_0}, \ldots, x_{i_0+m-1}$ uniquely. This implies that there exist at most $p^{m-1}(p-k)$ number of $(x_1, \ldots, x_m)$ satisfying (34) regardless of i_0. Therefore, (31) has at most $p^{m-1}(p-k)$ solutions. □

5. Examples

5.1 $PA(4,2)$: $p = 2$, $k = 1$ and $m = 2$

Recall that an element of $\mathcal{P}_{p,k}$ is represented by a p-tuple and an element of $Q_{2,1}$ is represented by a polynomial of degree at most $p - k$. By the definition of $\mathcal{P}_{p,k}$ and $Q_{p,k}$, we have

$$\mathcal{P}_{2,1} = \{(0,1), (1,0)\}, \tag{36}$$
$$Q_{2,1} = \{0, x\}. \tag{37}$$

Table 1 The proposed construction of $PA(4,2)$.

s_1	s_2	t_1	t_2	Rows of $PA(4,2)$
(0, 1)	(0, 1)	0	0	(1, 2, 3, 4)
(0, 1)	(0, 1)	0	x	(1, 2, 4, 3)
(0, 1)	(0, 1)	x	0	(1, 4, 3, 2)
(0, 1)	(0, 1)	x	x	(1, 3, 4, 2)
(0, 1)	(1, 0)	0	0	(2, 1, 4, 3)
(0, 1)	(1, 0)	0	x	(2, 1, 3, 4)
(0, 1)	(1, 0)	x	0	(2, 3, 4, 1)
(0, 1)	(1, 0)	x	x	(2, 4, 3, 1)
(1, 0)	(0, 1)	0	0	(3, 4, 1, 2)
(1, 0)	(0, 1)	0	x	(4, 3, 1, 2)
(1, 0)	(0, 1)	x	0	(3, 2, 1, 4)
(1, 0)	(0, 1)	x	x	(4, 2, 1, 3)
(1, 0)	(1, 0)	0	0	(4, 3, 2, 1)
(1, 0)	(1, 0)	0	x	(3, 4, 2, 1)
(1, 0)	(1, 0)	x	0	(4, 1, 2, 3)
(1, 0)	(1, 0)	x	x	(3, 1, 2, 4)

Table 2 A part of the proposed construction of $PA(8,4)$.

s_1	$t_{1,1}$	$t_{1,2}$	s_2	$t_{2,1}$	$t_{2,2}$	s_3	$t_{3,1}$	$t_{3,2}$	Rows of $PA(8,4)$
(0, 1)	0	0	(0, 1)	0	0	(0, 1)	0	0	(1, 2, 3, 4, 5, 6, 7, 8)
(0, 1)	0	0	(0, 1)	0	0	(0, 1)	0	x	(1, 2, 4, 3, 5, 6, 8, 7)
(0, 1)	0	0	(0, 1)	0	0	(0, 1)	x	0	(1, 2, 3, 4, 6, 5, 8, 7)
(0, 1)	0	0	(0, 1)	0	0	(0, 1)	x	x	(1, 2, 4, 3, 6, 5, 7, 8)
(0, 1)	0	0	(0, 1)	0	0	(1, 0)	0	0	(2, 1, 4, 3, 6, 5, 8, 7)
(0, 1)	0	0	(0, 1)	0	0	(1, 0)	0	x	(2, 1, 3, 4, 6, 5, 7, 8)
(0, 1)	0	0	(0, 1)	0	0	(1, 0)	x	0	(2, 1, 4, 3, 5, 6, 7, 8)
(0, 1)	0	0	(0, 1)	0	0	(1, 0)	x	x	(2, 1, 3, 4, 5, 6, 8, 7)
					⋮				
(1, 0)	x	x	(1, 0)	x	x	(0, 1)	0	0	(5, 2, 1, 6, 3, 8, 7, 4)
(1, 0)	x	x	(1, 0)	x	x	(0, 1)	0	x	(6, 2, 1, 5, 3, 7, 8, 4)
(1, 0)	x	x	(1, 0)	x	x	(0, 1)	x	0	(5, 2, 1, 6, 4, 7, 8, 3)
(1, 0)	x	x	(1, 0)	x	x	(0, 1)	x	x	(6, 2, 1, 5, 4, 8, 7, 3)
(1, 0)	x	x	(1, 0)	x	x	(1, 0)	0	0	(6, 1, 2, 5, 4, 7, 8, 3)
(1, 0)	x	x	(1, 0)	x	x	(1, 0)	0	x	(6, 1, 2, 5, 3, 8, 7, 4)
(1, 0)	x	x	(1, 0)	x	x	(1, 0)	x	0	(5, 1, 2, 6, 4, 8, 7, 3)
(1, 0)	x	x	(1, 0)	x	x	(1, 0)	x	x	(5, 1, 2, 6, 3, 7, 8, 4)

We can compute permutations on $\mathbb{F}_2 \times \mathbb{F}_2$ using ϕ. If we apply a natural mapping $(x, y) \mapsto (2x+y+1)$ from $\mathbb{F}_2 \times \mathbb{F}_2$ to $\{1, 2, 3, 4\}$ on our permutations, we obtain results in Table 1.

5.2 $PA(8,4)$: $p = 2, k = 1$ and $m = 3$

Since $\mathcal{P}_{2,1} = \{(0,1),(1,0)\}$ and $Q_{2,1} = \{0, x\}$, the constructed $PA(8,4)$ has $\left(2 \cdot 2^{3-1}\right)^3 = 512$ rows. We display only the first and the last 8 rows in Table 2 due to the lack of the space. Note that the proposed construction is not always the best; there exists a construction of $PA(8,4)$ with 2688 rows [6, Table 5].

6. Discussion

6.1 Performance Analysis

To analyze the performance, we compare the number of rows of permutation arrays generated by the proposed construction and other constructions in Sect. 2. Though there described two kinds of notable constructions, we consider only one kind of them based on distance-preserving maps [4], [12]; this is because the information required for the construction in [6] such as a table of transversals is not given properly. We concentrate our efforts on the comparison for the case $m = 2$.

The minimum distance is chosen to be $k = 2$ and $k = p-5, p-4, p-3, p-2, p-1$; for those k's, we can compute the attainable upper bounds of $\left|PA\left(p^2, pk\right)\right|$ for the proposed construction with a help of the complete classification for $\mathcal{P}_{p,k}$ in [5, §VI.45.9].

Upper bounds for the construction based on DPMs are obtained from [4], [12] and the cardinality of binary and ternary codes. The upper bounds for the cardinality of an (n, d)-binary code are obtained from the Singleton bound and [3], [14], [15]. For the ternary codes, the upper bounds come from the table in [3] for $p^2 \leq 16$, from the Singleton bound for $p^2 > 16$ and $k < 2p/3$, and from the Plotkin bound for ternary codes [13] for $p^2 > 16$ and $k \geq 2p/3$, respectively. Note that $PA(4,4)$ cannot be constructed by [4] and [12]. It should be stressed that these upper bounds for DPMs are not always achievable, while for the proposed constructions they are always reachable. Results are displayed in Table 3.

As we can see, if k is large, then $\left|PA\left(p^2, pk\right)\right|$ of the new construction overwhelms that of the construction based on DPMs. In particular the size of an (n, d)-ternary code for $d \geq 2n/3$ is at most $3n$ [13]. Thus we may conclude that the new construction gives $PA(p^2, pk)$ of larger size than those in [12] when $k \geq 2p/3$.

6.2 Searching for the Designated Row of the PA

Another advantage of our construction is that we have an easy algorithm to choose the i-th row of the permutation array for a given positive integer i. Note that without such an algorithm a permutation array is not practical. We will describe the algorithm briefly for only $m = 2$ as an example since the algorithms for $m \geq 3$ are analogous.

Suppose that we have an oracle O to find the j-th row of $PA(p, k)$ for a given positive integer $j \leq |PA(p, k)|$ that operates in a time polynomial to p. For a given positive integer i, we begin by dividing i into four nonnegative integers i_1, i_2, i_3 and i_4 satisfying the following conditions:

Table 3 Upper bounds of $\left|PA\left(p^2, pk\right)\right|$ for various p and k. They are always attainable for the proposed construction, but not for [4] and [12]. Exponents are rounded off to tenth.

p	method	k										
		2	3	4	5	6	7	8	9	10	11	12
2	Proposed	4	-	-	-	-	-	-	-	-	-	-
	DPM (binary code) [4]	-	-	-	-	-	-	-	-	-	-	-
	DPM (ternary code) [12]	-	-	-	-	-	-	-	-	-	-	-
3	Proposed	324	-	-	-	-	-	-	-	-	-	-
	DPM [4]	4	-	-	-	-	-	-	-	-	-	-
	DPM [12]	10	-	-	-	-	-	-	-	-	-	-
5	Proposed	$2^{27.7}$	$2^{21.1}$	$2^{13.3}$	-	-	-	-	-	-	-	-
	DPM [4]	2^{8}	6	2	-	-	-	-	-	-	-	-
	DPM [12]	$2^{19.0}$	$2^{9.5}$	6	-	-	-	-	-	-	-	-
7	Proposed	$2^{52.7}$	$2^{45.1}$	$2^{33.7}$	$2^{23.8}$	$2^{16.4}$	-	-	-	-	-	-
	DPM [4]	2^{22}	2^{9}	8	2	2	-	-	-	-	-	-
	DPM [12]	$2^{46.0}$	$2^{30.1}$	$2^{14.3}$	15	3	-	-	-	-	-	-
11	Proposed	$2^{112.8}$	$2^{103.9}$	$2^{88.1}$	$2^{73.3}$	$2^{61.1}$	$2^{53.6}$	$2^{46.7}$	$2^{28.4}$	$2^{20.5}$	-	-
	DPM [4]	2^{72}	2^{50}	2^{31}	2^{13}	12	4	2	2	2	-	-
	DPM [12]	$2^{134.7}$	$2^{110.9}$	$2^{82.4}$	$2^{55.5}$	$2^{31.7}$	$2^{12.7}$	12	3	3	-	-
13	Proposed	$2^{146.5}$	$2^{137.1}$	$2^{117.2}$	$2^{98.7}$	$2^{87.9}$	$2^{77.5}$	$2^{70.1}$	$2^{53.2}$	$2^{43.0}$	$2^{29.4}$	$2^{22.0}$
	DPM [4]	2^{109}	2^{84}	2^{60}	2^{34}	2^{14}	14	4	2	2	2	2
	DPM [12]	$2^{195.0}$	$2^{166.4}$	$2^{137.9}$	$2^{106.2}$	$2^{79.2}$	$2^{50.7}$	$2^{23.8}$	27	6	3	3

Algorithm 1 Choosing the designated row of $PA\left(p^2, pk\right)$

Input : O, an oracle that outputs the j-th row of $PA(p,k)$ for a given index j
i, the index for the designated row
Output : P, the i-th row

$i_1 \leftarrow \left\lfloor \frac{i-1}{|\mathcal{P}_{p,k}|\cdot|Q_{p,k}|^2} \right\rfloor$
$i_2 \leftarrow \left\lfloor \frac{i-1}{|Q_{p,k}|^2} \right\rfloor \mod |\mathcal{P}_{p,k}|$
$i_3 \leftarrow \left\lfloor \frac{i-1}{|Q_{p,k}|} \right\rfloor \mod |Q_{p,k}|$
$i_4 \leftarrow i \mod |Q_{p,k}|$
for $l = 1, 2$ **do**
  $s_l \leftarrow O(i_l)$
end for
for $l = 3, 4$ **do**
  Write i_l as the p-adic representation $i_l = i_l[1]\cdots i_l[p-k]_{(p)}$
  $t_{l-2}(X) \leftarrow \sum_{j=1}^{p-k} i_l[j]\cdot X^j$
end for
return $\phi(s_1, s_2, t_1, t_2)$ as P

- $0 \le i_1, i_2 < |\mathcal{P}_{p,k}|$ and $0 \le i_3, i_4 < |Q_{p,k}|$
- $\left(i_1 \cdot |\mathcal{P}_{p,k}| + i_2\right)|Q_{p,k}|^2 + \left(i_3 \cdot |Q_{p,k}| + i_4\right) + 1 = i$

It is easy to see that such i_1, i_2, i_3 and i_4 are computed uniquely. For i_1 and i_2, we determine two permutations s_1 and s_2 by $s_1 = O(i_1+1)$ and $s_2 = O(i_2+1)$. For i_3 and i_4, we write them as the p-adic representations $i_3 = i_3[1]\cdots i_3[p-k]$ and $i_4 = i_4[1]\cdots i_4[p-k]$, where $0 \le i[j] < p$ for $j = 1, \ldots, p-k$. Then we set $t_1 = \sum_{j=1}^{p-k} i_3[j]X^j$ and $t_2 = \sum_{j=1}^{p-k} i_4[j]X^j$. Now the designated i-th row of $PA\left(p^2, pk\right)$ is given by $\phi(s_1, s_2, t_1, t_2)$. The whole procedure is summarized in Algorithm 1.

6.3 Application

An interesting application of the proposed construction and Algorithm 1 is to obtain an one-to-one correspondence between a key space $\mathcal{K}$ and a set of keyed permutations $\mathcal{P}$ with some minimum distance. Refer [17] for a concrete example of the correspondence when $\mathcal{K} = (\mathbb{F}_2)^{49}$ and $\mathcal{P}$ is a set of rows of $PA(49, 14)$ constructed by the proposed method; up to the authors' knowledge, there is no other construction of $PA(49, 14)$ providing such a correspondence.

References

[1] I.F. Blake, "Permutation codes for discrete channels," IEEE Trans. Inf. Theory, vol.20, no.1, pp.138–140, 1974.
[2] M. Bogaerts, "Isometries and construction of permutation arrays," IEEE Trans. Inf. Theory, vol.56, no.7, pp.3177–3179, 2010.
[3] A.E. Brouwer, H.O. Hamalainen, P.R.J. Ostergard, and N.J.A. Sloane, "Bounds on mixed binary/ternary codes," IEEE Trans. Inf. Theory, vol.44, no.1, pp.140–161, Jan. 1998.
[4] J.-C. Chang, R.-J. Chen, T. Kløve, and S.-C. Tsai, "Distance-preserving mappings from binary vectors to permutations," IEEE Trans. Inf. Theory, vol.49, no.4, pp.1054–1059, 2003.
[5] C.J. Colbourn and J.H. Dinitz, ed., Handbook of Combinatorial Designs, second ed., Chapman & Hall/CRC, 2007.
[6] W. Chu, C.J. Colbourn, and P. Dukes, "Construction for permutation codes in powerline communications," Des. Codes Cryptogr., vol.32, no.1–3, pp.51–64, 2004.

[7] C.J. Colbourn, T. Kløve, and A.C.H. Ling, “Permutation arrays for powerline communication and mutually orthogonal latin squares,” IEEE Trans. Inf. Theory, vol.50, no.6, pp.1289–1291, 2004.
[8] M. Deja, “Matrices dont deux lignes quelconque coïncident dans un nombre donne de positions communes,” J. Combin. Theory Ser. A, vol.20, no.3, pp.306–318, 1976.
[9] C. Ding, F.-W. Fu, T. Kløve, and V.K.-W. Wei, “Constructions of permutation arrays,” IEEE Trans. Inf. Theory, vol.48, no.4, pp.977–980, 2002.
[10] P. Frankl and M. Deza, “On the maximum number of permutations with given maximal or minimum distance,” J. Combin. Theory Ser. A, vol.22, no.3, pp.352–360, 1977.
[11] F.-W. Fu and T. Kløve, “Two constructions of permutation arrays,” IEEE Trans. Inf. Theory, vol.50, no.5, pp.881–883, 2004.
[12] J.-S. Lin, J.-C. Chang, R.-J. Chen, and T. Kløve, “Distance-preserving and distance-increasing mappings from ternary vectors to permutations,” IEEE Trans. Inf. Theory, vol.54, no.3, pp.1334–1339, 2008.
[13] C. Mackenzie and J. Seberry, “Maximal ternary codes and Plotkin's bound,” Ars Combin., vol.17A, pp.251–270, 1984.
[14] V.S. Pless and W.C. Huffman, ed., Handbook of Coding Theory, first ed., Elsevier Science B.V., 1998.
[15] M. Plotkin, “Binary codes with specified minimum distance,” IRE Trans. Inf. Theory, vol.6, no.4, pp.445–450, 1960.
[16] J.Y. Park and H.-Y. Song, “An extended construction of permutation arrays with a polynomial-time sampling algorithm,” Proc. IWSDA'11 — The Fifth International Workshop on Signal Design and its Applications in Communications, Sept. 2011.
[17] J.Y. Park, K.-H. Park, and H.-Y. Song, “A condition on permutations for some cancelable biometric schemes,” preprint, 2012.
[18] J. Quistorff, “A survey on packing and covering problems in the hamming permutation space,” Elec. J. Comb., vol.13, no.1, 2006.
[19] A.J.H. Vinck, “Coded modulation for powerline communications,” AEÜ Int. J. Eletron. Commun., vol.54, no.1, pp.45–49, 2000.

Jung Youl Park received his B.S. and M.S. degrees in Mathematics and Ph.D. degree in Mathematical Science from KAIST (Korea Advanced Institute of Science and Technology), Korea in 2000, 2002 and 2010 respectively. He researched a cryptographic problems related to coding theory as a Post-Doc Research Associate at the School of Electrical and Electronic Engineering of Yonsei University, Seoul Korea, from 2010 to 2012. Currently he is working as a member of engineering staffs at the Attached Institute of ETRI, Daejeon, Korea. His area of interest covers elliptic curves, cryptographic protocols, algorithms and related topics of cryptography including their implementation.

Hong-Yeop Song received his B.S. degree in Electronic Engineering from Yonsei University in 1984, MSEE and Ph.D. degrees from the University of Southern California, Los Angeles, CA, in 1986 and 1991, respectively, specializing in the area of communication theory and coding. He spent 2 years as a senior engineer at Qualcomm Inc., San Diego, CA, from 1994 to 1995, contributed to a team developing North American CDMA Standards for PCS and cellular air-interface systems. Finally, in the fall of 1995, he joined the Dept. of Electrical and Electronic Engineering at Yonsei University, Seoul, Korea, and is currently working as a professor. He visited Dr. G. Gong at University of Waterloo, Canada, in the year 2002. He is interested in Communication and Coding Theory, including error-correcting codes, PN sequences, and crypto algorithms. He is a senior member of IEEE, member of MAA (Mathematical Association of America), and domestic societies: IEEK, KICS, KIISC and KMS(Korean Mathematical Society).