Permutation Arrays Under the Chebyshev Distance

Torleiv Kløve, *Fellow, IEEE*, Te-Tsung Lin, Shi-Chun Tsai, *Member, IEEE*, and Wen-Guey Tzeng, *Member, IEEE*

***Abstract*—An (n, d) permutation array (PA) is a subset of S_n with the property that the distance (under some metric) between any two permutations in the array is at least d. They became popular recently for communication over power lines. Motivated by an application to flash memories, in this paper, the metric used is the Chebyshev metric. A number of different constructions are given, as well as bounds on the size of such PA.**

***Index Terms*—Bounds, Chebyshev distance, code constructions, flash memory, permutation arrays.**

I. Introduction

Let S_n denote the set of all permutations of length n. A permutation array of length n is a subset of S_n. Recently, Jiang *et al.* [5], [6] showed an interesting new application of permutation arrays for flash memories, where they used different distance metrics to investigate efficient rewriting schemes. Under the multilevel flash memory model, we find the metric induced by the l_∞ norm very appropriate for studying the recharging and error correcting issues. This metric is known as the Chebyshev metric. We consider a noisy channel where pulse amplitude modulation (PAM) is used with different amplitude levels for each permutation symbol. The noise in the channel is an independent Gaussian distribution with zero mean for each position. The received sequence is the original permutation distorted by Gaussian noise, and its ranking can be seen as a permutation, which can be different from the original one.

To study the correlations between ranks, several metrics on permutations were introduced, such as the Hamming distance, the minimum number of transpositions taking one permutation to another, etc. [3], [7]. For instance, Stoll and Kurz [14] investigated a detection scheme of permutation arrays using Spearman's rank correlation. Chadwick and Kurz [2] studied the permutation arrays based on Kendall's tau.

Under the model of additive white Gaussian noise (AWGN) [4], there is a probability for any amplitude level to deviate from the original one, which may yield a large Hamming distance but with a rather small Chebyshev distance. Meanwhile, the original rank may still be in good shape even after some perturbation. Observe that two permutations with a large Hamming distance can actually have a small Chebyshev distance and vice versa. They appear to complement each other in some sense. This inspired us to use the Chebyshev distance. Technically, with l_∞ norm, we find it is much easier to encode, decode and estimate the sphere size of permutation arrays than with the other l_p norms.

In this paper, we give a number of constructions of PAs. For some we give efficient decoding algorithms. We also consider encoding from vectors into permutations.

Manuscript received July 06, 2009; revised February 18, 2010. Current version published May 19, 2010. This work was supported in part by the National Science Council of Taiwan under contracts NSC-95-2221-E-009-094-MY3, NSC-96-2221-E-009-026, NSC-96-2628-E-009-011-MY3, NSC-97-2221-E-009-064-MY3, and NSC-98-2218-E-009-020, and in part by the Norwegian Research Council. The material in this paper was presented in part at the 2008 IEEE International Symposium on Information Theory.

T. Kløve is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (e-mail: torleiv.klove@ii.uib.no).

T.-T. Lin, S.-C. Tsai, and W.-G. Tzeng are with the Department of Computer Science, National Chiao Tung University, Hsinchu 30050, Taiwan, R.O.C. (e-mail: atman.cs94g@nctu.edu.tw; sctsai@csie.nctu.edu.tw; wgtzeng@cs.nctu.edu.tw).

Communicated by E. Viterbo, Associate Editor for Coding Techniques.

Digital Object Identifier 10.1109/TIT.2010.2046212

II. Notations

We use $[n]$ to denote the set $\{1, \ldots, n\}$. S_n denotes the set of all permutations of $[n]$. For any set X, X^n denotes the set of all n-tuples with elements from X.

Let id_n denote the identity permutation in S_n. The Chebyshev distance between two permutations $\pi, \sigma \in S_n$ is

$$d_{\max}(\pi, \sigma) = \max\{|\pi_j - \sigma_j| \mid 1 \le j \le n\}.$$

An (n, d) permutation array (PA) is a subset of S_n with the property that the Chebyshev distance between any two distinct permutations in the array is at least d. We sometimes refer to the elements of a PA as code words.

The maximal size of an (n, d) PA is denoted by $P(n, d)$. Let $V(n, d)$ denote the number of permutations in S_n within Chebyshev distance d of the identity permutation. Since $d_{\max}(\mathrm{id}_n, \sigma) = d_{\max}(\pi, \pi\sigma)$, the number of permutations in S_n within Chebyshev distance d of any permutation $\pi \in S_n$ will also be $V(n, d)$. Bounds on $P(n, d)$ and $V(n, d)$ will be considered in Section IV.

III. Constructions

In this section, we give a number of constructions of PAs, one explicit and some recursive.

A. Explicit Construction

Let n and d be given. Define

$$C = \{(\pi_1, \ldots, \pi_n) \in S_n | \pi_i \equiv i \pmod d \text{ for all } i \in [n]\}.$$

Theorem 1: If $n = ad + b$, where $0 \le b < d$, then C is an (n, d) PA and

$$|C| = ((a+1)!)^b (a!)^{d-b}.$$

Proof: Let $1 \le m \le d$ and $u = \lfloor (n-m)/d \rfloor$. For $\pi \in C$, we see that $(\pi_m, \pi_{m+d}, \pi_{m+2d}, \ldots, \pi_{m+ud})$ is a permutation of the set $\{m, m+d, m+2d, \ldots, m+ud\}$. This set contains $(a+1)$ elements if $1 \le m \le b$ and so there are $(a+1)!$ possible choices for $(\pi_m, \pi_{m+d}, \pi_{m+2d}, \ldots, \pi_{m+ud})$ and all can used. Similarly, there are $a!$ choices if $m > b$. Hence, the total number of permutations in C is $((a+1)!)^b (a!)^{d-b}$. ∎

In particular, we get the following bound.

Theorem 2: If $n = ad + b$, where $0 \le b < d$, then

$$P(n,d) \ge ((a+1)!)^b (a!)^{d-b}.$$

Example 1: For $d = 2$, we get

$$P(2a, 2) \ge (a!)^2.$$

We note that if $2d > n$, then $a = 1$ and $b = n - d$ and so $|C| = 2^{n-d}$. If $2d = n$, then $a = 2$, $b = 0$, and we have $|C| = 2^d = 2^{n-d}$ as well. However, if $2d < n$, then $|C| > 2^{n-d}$. Especially, when d is small relative to n, $|C|$ is much larger than 2^{n-d}. For example, for $n = 30$, $d = 2$, $|C|/2^{n-d} \approx 6.37 \times 10^{15}$.

This construction has a very simple error correcting algorithm. For $d \ge 2t + 1$, we can correct error up to size t in any coordinate. For coordinate i, the codeword has value $\pi_i \equiv i \pmod{d}$. Suppose that this coordinate is changed into $\sigma = \pi_i + u$, where $|u| \le t$. Then π_i is the integer congruent to i which is closest to σ. Therefore, decoding of position i is done by first computing

$$a \equiv i - \sigma \pmod{d}$$

where $-(d-1)/2 \le a \le (d-1)/2$. Then $a = -u$, and so we decode into $\sigma + a = \pi_i$.

B. First Recursive Construction

Let C be an (n,d) PA of size M, and let $r \ge 2$ be an integer. We define an (rn, rd) PA, C_r, of size M^r as follows: for each multiset of r code words from C

$$\left(\pi_1^{(j)}, \ldots, \pi_n^{(j)}\right), \quad j = 0, 1, \ldots, r-1$$

let

$$\rho_j = \left(r\pi_1^{(j)} - j, \ldots, r\pi_n^{(j)} - j\right), \quad j = 0, 1, \ldots, r-1$$

and include $(\rho_0|\rho_1|\cdots|\rho_{r-1})$ as a codeword in C_r. It is clear that under this construction the distance between any two distinct ρ_j, $\rho_{j'}$ is at least rd. It is also easy to check that $(\rho_0|\rho_1|\cdots|\rho_{r-1}) \in S_{rn}$. Hence, $|C_r| = M^r$. In particular, we get the following bound.

Theorem 3: If $n > d$ and $r \ge 2$, then

$$P(rn, rd) \ge P(n,d)^r.$$

Proof: Let C be an (n,d) PA of size $P(n,d)$. Then the construction above gives an (rn, rd) PA of C_r. Hence, $P(rn, rd) \ge |C_r| = |C|^r = P(n,d)^r$. ∎

C. Second Recursive Construction

For a permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n) \in S_n$ and an integer m, $1 \le m \le n+1$ define

$$\varphi_m(\pi) = (m, \pi_1', \pi_2', \ldots, \pi_n') \in S_{n+1}$$

by

$$\pi_i' = \pi_i \text{ if } \pi_i \le m$$
$$\pi_i' = \pi_i + 1 \text{ if } \pi_i > m.$$

Let C be an (n,d) PA, and let

$$1 \le s_1 < s_2 < \cdots < s_t \le n+1$$

be integers. Define

$$C[s_1, s_2, \ldots, s_t] = \{\varphi_{s_j}(\pi) \mid 1 \le j \le t, \ \pi \in C\}.$$

Theorem 4: If C is an (n,d) PA of size M and

$$s_j + d \le s_{j+1} \text{ for } 1 \le j \le t-1$$

then $C[s_1, s_2, \ldots, s_t]$ is an $(n+1, d)$ PA of size tM.

Theorem 5: If C is an (n,d) PA of size M and $n \le 2d$, then $C[d]$ is an $(n+1, d+1)$ PA of size M.

Proof: If $j > j'$, then

$$d_{\max}(\varphi_{s_j}(\pi), \varphi_{s_{j'}}(\sigma)) \ge s_j - s_{j'} \ge d.$$

Next, consider $j' = j$. If $\pi, \sigma \in C$, $\pi \ne \sigma$, then w.l.o.g, there exist an i such that $\pi_i \ge \sigma_i + d$. Hence

$$d_{\max}(\varphi_{s_j}(\pi), \varphi_{s_j}(\sigma)) \ge \begin{cases} \pi_i - \sigma_i + 1 > d, & \text{if } \pi_i > s_j \ge \sigma_i \\ \pi_i - \sigma_i \ge d, & \text{otherwise.} \end{cases}$$

This proves Theorem 4. To complete the proof of Theorem 5, we note that

$$\pi_i \ge \sigma_i + d \ge d + 1 > d$$
and
$$\sigma_i \le \pi_i - d \le n - d \le d.$$

Hence, $\pi_i > d \ge \sigma_i$, and so

$$d_{\max}(\varphi_{s_j}(\pi), \varphi_{s_j}(\sigma)) \ge d + 1.$$

∎

The constructions imply bounds on $P(n,d)$.

Theorem 6: If $n > d \ge 1$, then

$$P(n+1, d) \ge \left(\left\lfloor \frac{n}{d} \right\rfloor + 1\right) P(n,d).$$

Proof: Let $t = \lfloor n/d \rfloor + 1$. Then $(t-1)d + 1 \le n + 1$. If C is an (n,d) PA of size $P(n,d)$, then Theorem 4 implies that

$C[1, d+1, 2d+1, \ldots, (t-1)d+1]$ is an $(n+1, d)$ PA of size $tP(n,d)$. Hence, $P(n+1,d) \geq tP(n,d)$. ∎

Example 2: In Example 1, we showed that the explicit construction implied that $P(2a, 2) \geq (a!)^2$. Combining Theorem 6 and search, we can improve this bound. We have found that $P(7,2) \geq 582$, see the table at the end of Section IV. From repeated use of Theorem 6, we get

$$P(2a,2) \geq (a(a-1)\cdots 5)^2 \cdot 4P(7,2) \geq \frac{97}{24}(a!)^2.$$

Theorem 5 implies the following bound.

Theorem 7: If $d < n \leq 2d$, then

$$P(n+1, d+1) \geq P(n,d).$$

Proof: Let C be an (n,d) PA of size $P(n,d)$. By Theorem 5, $C[d]$ is an $(n+1, d+1)$ PA of size $P(n,d)$. Hence

$$P(n+1, d+1) \geq |C[d]| = P(n,d).$$

∎

Theorem 7 shows in particular that for a fixed r

$$P(d+1+r, d+1) \geq P(d+r, d) \quad \text{for} \quad d \geq r. \tag{1}$$

We will show that $P(d+r, d)$ is bounded. We show the following theorem.

Theorem 8: For fixed r, there exist constants c_r and d_r such that $P(d+r,d) = c_r$ for $d \geq d_r$. Moreover

$$c_r \leq 2^{2r}(2r)! \tag{2}$$

and

$$d_r \leq 1 + (2r-1)c_r - r. \tag{3}$$

Remark: The main point of Theorem 8 is the existence of c_r and d_r. The actual bounds given are probably quite weak in general. For example, Theorem 8 gives the bounds $c_1 \leq 8$ and $d_1 \leq 8$. In Theorem 9 below, we will show that $c_1 = 3$ and $d_1 = 2$. Theorem 8 gives $c_2 \leq 384$ and $d_2 \leq 1151$, whereas numerical computation indicate that $c_2 = 9$ and $d_2 = 5$.

We split the proof of Theorem 8 into three lemma.

Lemma 1: If $d \geq r$, then $P(d+r, d) \leq 2^{2r}(2r)!$.

Proof: Suppose that there exists an $(d+r, d)$ PA C of size $M > 2^{2r}(2r)!$. We call the integers

$$1, 2, \ldots, r \text{ and } d+1, d+2, \ldots, d+r$$

potent, the first r *smaller potent*, the last r *larger potent*. Two potent integers are called *equipotent* if both are smaller potent or both are larger potent. If the distance between two permutations $(\pi_1, \pi_2, \ldots, \pi_n)$, $(\rho_1, \rho_2, \ldots, \rho_n)$ is at least d, then there exists some position i such that, w.l.o.g, $\pi_i - \rho_i \geq d$, Then π_i is a larger potent element and ρ_i is smaller potent. Each permutation in S_{d+r} contains $2r$ potent elements and we call the set of positions of these the *potency support* $\chi(\pi)$ of the permutation, that is, the potency support of π is

$$\chi(\pi) = \{i \mid 1 \leq \pi_i \leq r\} \cup \{i \mid d+1 \leq \pi_i \leq d+r\}.$$

The potency support of C is the union of the potency support of the permutations in C, that is

$$\chi(C) = \{i \mid 1 \leq \pi_i \leq r \ \text{ for some } \ \pi \in C\} \cup \{i \mid d+1 \leq \pi_i \leq d+r \ \text{ for some } \ \pi \in C\}.$$

Let $\pi \in C$. For each $\rho \in C$, $\rho \neq \pi$, we have $d(\pi, \rho) \geq d$. Hence, there exists some $i \in \chi(\pi)$ such that ρ_i is potent. Therefore, the set

$$\{(\rho, i) \mid \rho \in C \ \text{ and } \ i \in \chi(\pi)\}$$

contains at least $2r + (M-1) > M$ elements. Hence, there is an $i \in \chi(\pi)$ such that

$$|\{\rho \in C \mid \rho_i \text{ is potent}\}| > M/(2r) > 2^{2r}(2r-1)!.$$

Since

$$\{\rho \in C \mid \rho_i \text{ is potent}\} = \{\rho \in C \mid \rho_i \text{ is smaller potent}\} \cup \{\rho \in C \mid \rho_i \text{ is larger potent}\}$$

there exists a subset $C_1 \subset C$ such that

$$|C_1| > 2^{2r-1}(2r-1)!$$

and the elements in position $i_1 = i$ are equipotent.

We can now repeat the procedure. Let $\pi \in C_1$. There must exist an $i_2 \in \chi(\pi) \setminus \{i_1\}$ such that

$$|\{\rho \in C_1 \mid \rho_{i_2} \text{ is potent}\}| \geq |C_1|/(2r-1) > 2^{2r-1}(2r-2)!.$$

Hence, we get subset $C_2 \subset C_1$ such that

$$|C_2| > 2^{2r-2}(2r-2)!$$

and the elements in position i_2 are equipotent (and the elements in position i_1 are equipotent).

Repeated use of the same argument will produce for each j, $1 \leq j \leq 2r$ a set C_j such that

$$|C_j| > 2^{2r-j}(2r-j)!$$

and for j positions $i_1, i_2, \ldots i_j$, the elements in those positions are all equipotent. In particular, $|C_{2r}| > 1$, all permutations in C_{2r} have the same potency support $\{i_1, i_2, \ldots, i_{2r}\}$, and for each of these positions, all the elements in that position are equipotent. This is a contradiction since the distance between two such permutations must be less than d. Hence, the assumption that a PA of size larger than $2^{2r}(2r)!$ exists leads to a contradiction. ∎

Lemma 1 combined with (1) proves the existence of c_r and d_r and gives the bound (2).

Lemma 2: If C is a $(d+r, d)$ PA of size M where

$$d > r \text{ and } d + r > |\chi(C)|$$

then there exists a $(d-1+r, d-1)$ PA of size M. In particular, if $M = P(d+r, d)$, then

$$P(d-1+r, d-1) = P(d+r, d).$$

Proof: Replace all elements in range $r+1, r+2, \ldots, d$ in the permutations of C by a star $*$ which will denote "unspecified". The permutations in C is transformed into *vectors* containing the potent elements and $d-r$ stars. Note that if we replace the unspecified elements in each vector by the integers $r+1, r+2, \ldots, d$ in some order, we get a permutation, and the distance between two such permutations will be at least d since we have not changed the potent elements.

Since the length $d+r$ of C is larger than $|\chi(C)|$, there exists a position where all the vectors contains a star. Remove this position from each vector and reduce all the larger potent elements by one. This given a set of M vectors of length $d-1+r$ and such that the distance between any two is at least $d-1$. Replacing the $d-1-r$ stars in each vector by $r+1, r+1, \ldots, d-1$ in some order, we get a $(d-1+r, d-1)$ PA of size M.

If $M = P(d+r, d)$, then we get

$$P(d-1+r, d-1) \geq P(d+r, d).$$

Since $P(d-1+r, d-1) \leq P(d+r, d)$ by (1), the lemma follows. ■

Lemma 3: If C is a $(d+r, d)$ PA of size M and $d \geq r$, then

$$|\chi(C)| \leq M(2r-1) + 1.$$

Proof: Each permutation has potency support of size $2r$. The potency support of any two permutations in C must overlap since their distance is at least d. Hence, each permutation after the first will contribute at most $2r-1$ new elements to the total potency support. Therefore

$$|\chi(C)| \leq 2r + (M-1)(2r-1).$$

■

Remark: By a more involved analysis, we can improve this bound somewhat. For example, we see that two new permutations can contribute at most $4r-3$ to the total support.

We can now complete the proof of Theorem 8. Let C be a $(d+r, r)$ code of size c_r. By Lemma 3, $|\chi(C)| \leq c_r(2r-1)+1$. If $d > 1 + c_r(2r-1) - r$, then $d + r > |\chi(C)|$. Hence, by Lemma 2, $P(d-1+r, d-1) = P(d+r, d)$. Therefore, $d_r \leq 1 + c_r(2r-1) - r$, that is, (3) is satisfied. This completes the proof of Theorem 8.

Theorem 9: We have $P(d+1, d) = 3$ for $d \geq 2$.

Proof: We use the same notation as in the proof of Lemma 2. Let C be an $(d+1, d)$ PA. The only potent elements are 1 and n. W.lo.g. we may assume the first permutation in C is $(1, n, *, *, \ldots)$ where $*$ denotes some unspecified integer in the range $2, 3, \ldots, d$. W.l.o.g, a second permutation has one of three forms

$$(n, 1, *, *, \ldots), (n, *, 1, *, \ldots), (*, 1, n, *, \ldots).$$

We see that if the second permutation is of the first form, there cannot be more permutations. If the second permutation is of the form $(n, *, 1, *, \ldots)$, then there is only one possible form for a third permutation, namely $(1, *, n, *, \ldots)$. Hence, we see that $P(d+1, d) \leq 3$ and that $P(d+1, d) = 3$ for $d \geq 2$. ■

To determine $P(d+r, d)$ along the same lines for $r \geq 2$ seems to be difficult because of the many cases that have to be considered. Even to determine $P(d+2, d)$ will involve a large number of cases. For example, for the second permutation there are 138 essentially different possibilities for the four positions in the potency support of the first permutation. For each of these there are many possible third permutations, etc.

D. Encoding/Decoding of Some PA Constructed by the Second Recursive Construction

Suppose we start with the PA

$$C_d = \{(1, 2, 3, \ldots, d)\}.$$

For $\nu = d, d+1, \ldots, n-1$ let

$$C_{\nu+1} = C_\nu[1, \nu+1].$$

Then C_n is an (n, d) PA of size 2^{n-d}. For some applications, we may want to map a set of binary vectors to a permutation array. One algorithm for mapping a binary vector $(x_1, x_2, \ldots, x_{n-d})$ into C_n would be to use the recursive construction of C_n by mapping $(x_1, x_2, \ldots, x_i)$ into a permutation π in C_{d+i}. Recursively, we can then map $(x_1, x_2, \ldots, x_i, 0)$ to $\varphi_1(\pi)$ and $(x_1, x_2, \ldots, x_i, 1)$ to $\varphi_{d+i+1}(\pi)$.

However, there is an alternative algorithm which requires less work. Retracing the steps of the construction, we see that given some initial part of length less than $n-d$ of a permutation in C_n, there are exactly two possibilities for the next element, one "larger" and one "smaller". More precisely, induction shows that if the initial part of length $i-1$ contains exactly t "smaller" elements, then element number i is either $t+1$ (the "smaller") or $n-i+t+1$ (the "larger"). This is the basis for a simple mapping from Z_2^{n-d} to C_n. We give this algorithm in Fig. 1.

Input: $(x_1, \ldots, x_{n-d}) \in Z_2^{n-d}$
Output: $(\pi_1, \ldots, \pi_n) \in C_n$
  for $i \leftarrow n-d+1$ **to** n **do** $x_i \leftarrow 0$;
  $t \leftarrow 0$; //* t is the number of zeros seen so far.*//
  for $i \leftarrow 1$ **to** n **do**
    if $x_i = 0$
      then $\{\pi_i \leftarrow t+1;\ t \leftarrow t+1;\}$
      else $\{\pi_i \leftarrow n-i+t+1;\}$

Fig. 1. Algorithm mapping Z_2^{n-d} to C_n.

We see that the difference between the larger and the smaller element in position $i \leq n-d$ is $n-i$. Hence, we can recover from any error of size less than $(n-i)/2$ by choosing the closest

```
Input: (π_1, ..., π_n) ∈ [n]^n
Output: (x_1, ..., x_{n-d})
  t ← 0; //* t is number of zeros determined. *//
  for i ← 1 to n − d do
      if π_i < (n − i)/2 + t + 1
        then {x_i ← 0; t ← t + 1;}
        else {x_i ← 1;}
```

Fig. 2. Decoding algorithm recovering the binary preimage from a corrupted permutation in C_n.

of the two possible values, and the corresponding binary value. We give the decoding algorithm in Fig. 2.

Without going into all details, we see that we can get a similar mapping from q-ary vectors. Now we start with the PA

$$C_{(q-1)d} = \{(1, 2, 3, \ldots, (q-1)d)\}.$$

For $(q-1)d \le \nu \le n-1$ let $s_j = (j-1)\lfloor \nu/(q-1) \rfloor + 1$ for $1 \le j \le q-1$ and $s_q = \nu + 1$. Let

$$C_{\nu+1} = C_\nu[s_1, s_2, \ldots, s_q].$$

Then C_n is an (n, d) PA of size $q^{n-(q-1)d}$. Encoding and decoding correcting errors of size at most $(d-1)/2$, based on the recursion, is again relatively simple.

IV. Further Bounds on $P(n,d)$

A. General Bounds

Since $d_{\max}(\pi, \sigma) \le n-1$ for any two distinct permutations in S_n, we have $P(n,n) = 1$. Therefore, we only consider $d < n$.

Since the spheres of radius d in S_n all have size $V(n,d)$, we can get a Gilbert type lower bound on $P(n,d)$.

Theorem 10: For $n > d \ge 2$ we have

$$P(n,d) \ge \frac{n!}{V(n,d-1)}.$$

Proof: It is clear that the following greedy algorithm produces a permutation array with cardinality at least $n!/V(n,d-1)$.

1) Start with any permutation in S_n.
2) Choose a permutation whose distance is at least d to all previous chosen permutations.
3) Repeat step 2 as long as such a permutation exists.

Let C be the permutation array produced by the above greedy algorithm. Once the algorithm stops, S_n will be covered by the $|C|$ spheres of radius $d-1$ centered at the code words in C. Thus, $n! \le |P| \cdot V(n, d-1)$ which implies our claim. ■

Similarly, we get a Hamming type upper bound in the usual way.

Theorem 11: If $n > d \ge 1$, then

$$P(n,d) \le \frac{n!}{V(n, \lfloor (d-1)/2 \rfloor)}.$$

Proof: Let C be an (n,d) PA of size $P(n,d)$. The spheres of radius $\lfloor (d-1)/2 \rfloor$ around the permutations in C are pairwise disjoint. The union of these spheres is a subset of S_n. Hence

$$P(n,d)V(n, \lfloor (d-1)/2 \rfloor) = |C|V(n, \lfloor (d-1)/2 \rfloor) \le n!$$

and the bound follows. ■

If $n \le 2d$ and d is even, we can combine the bound in Theorem 11 with Theorem 7 to get the following bound which is stronger than the ordinary Hamming bound, at least in the cases we have tested.

Theorem 12: If d is even and $2d \ge n > d \ge 2$, then

$$P(n,d) \le \frac{(n+1)!}{V(n+1, d/2)}.$$

Proof:

$$P(n,d) \le P(n+1, d+1) \le \frac{(n+1)!}{V(n, d/2)}.$$

■

Example 3: For $n = 11$ and $d = 6$, Theorem 11 gives

$$P(11,6) \le \left\lfloor \frac{11!}{V(11,2)} \right\rfloor = \left\lfloor \frac{11!}{11854} \right\rfloor = 3367$$

whereas Theorem 12 gives

$$P(11,6) \le \left\lfloor \frac{12!}{V(12,3)} \right\rfloor = \left\lfloor \frac{12!}{563172} \right\rfloor = 850.$$

Remark: Remark. We can of course use Theorem 7 repeatedly r times and then Theorem 11 to get

$$P(n,d) \le \frac{(n+r)!}{V(n+r, \lfloor (d+r-1)/2 \rfloor)}$$

for all $r \ge 0$. However, it appears we get the best bounds for $r = 1$ when d is even and $r = 0$ when d is odd.

In general, no simple expression of $V(n,d)$ is known. A survey of known results as well as a number of new results on $V(n,d)$ were given by Kløve [8]. See also Kløve [9] and [10]. Here, we briefly give some main results.

As observed by Lehmer [11], $V(n,d)$ can be expressed as a permanent. The permanent of an $n \times n$ matrix A is defined by

$$\mathrm{per}A = \sum_{\pi \in S_n} a_{1,\pi_1} \cdots a_{n,\pi_n}.$$

In particular, if A is a $(0,1)$-matrix, then

$$\mathrm{per}A = |\{\pi \in S_n : a_{i,\pi_i} = 1 \text{ for all } i\}|.$$

Let $A^{(n,d)}$ be the $n \times n$ matrix with $a_{i,j}^{(n,d)} = 1$ if $|i-j| \le d$ and $a_{i,j}^{(n,d)} = 0$ otherwise.

Lemma 4: $V(n,d) = \mathrm{per}A^{(n,d)}$.

TABLE I
μ_d AND ITS UPPER BOUND

d	μ_d	$[(2d+1)!]^{1/(2d+1)}$	$\mu_d/(2d+1)$
1	1.61803	1.81712	0.53934
2	2.33355	2.60517	0.46671
3	3.06177	3.38002	0.43739
4	3.79352	4.14717	0.42150
5	4.52677	4.90924	0.41152
6	5.26082	5.66769	0.40468
7	5.99534	6.42342	0.39969
8	6.73016	7.17704	0.39589

Proof:

$$\begin{aligned} V(n,d) &= |\{\pi \in S_n : d_{\max}(\mathrm{id},\pi) \le d\}| \\ &= |\{\pi \in S_n : |\pi_i - i| \le d \text{ for all } i\}| \\ &= |\{\pi \in S_n : a^{(n,d)}_{i,\pi_i} = 1 \text{ for all } i\}| \\ &= \mathrm{per} A^{(n,d)}. \end{aligned}$$

■

For fixed d, $V(n,d)$ satisfies a linear recurrence in n. A proof is given in [13] (Proposition 4.7.8 on page 246). For $1 \le d \le 3$, these recurrences were determined explicitly by Lehmer [11], and for $4 \le d \le 6$ by Kløve [8]. In particular, this implies that

$$\lim_{n\to\infty} V(n,d)^{1/n} = \mu_d$$

where μ_d is the largest root of the minimal polynomial corresponding to the linear recurrence of $V(n,d)$. Lehmer [11] determined μ_d approximately for $d = 1,2,3$ and Kløve [8] for $d \le 8$.

For an $n \times n$ $(0,1)$-matrix it is known (see [16, Theorem 11.5]) that

$$\mathrm{per} A \le \prod_{i=1}^{n} (r_i!)^{1/r_i}$$

where r_i is the number of ones in row i.

For $A^{(n,d)}$, we clearly have $r_i \le 2d+1$ for all i. Hence

$$V(n,d) \le [(2d+1)!]^{n/(2d+1)} \text{ for all } n \quad (4)$$

and

$$\mu_d \le [(2d+1)!]^{1/(2d+1)}.$$

In Table I we give μ_d and this upper bound.

We note that for large d, $\mu_d/(2d+1) \approx 1/e \approx 0.36788$.

Combining Theorem 10 and (4), we get:

Corollary 1: For $n > d \ge 1$, we have

$$P(n,d) \ge \frac{n!}{[(2d-1)!]^{n/(2d-1)}}.$$

Combining (33) and (34) in Kløve [8], we get the following lower bound on $V(n,d)$:

$$V(n,d) \ge \frac{n!(2d+1)^n}{2^{2d} n^n}. \quad (5)$$

TABLE II
BOUNDS ON $P(n,d)$

	$d=2$	$d=3$	$d=4$
$n=d+1$	3	3	3
$n=d+2$	6 − 24	9	9 − 12
$n=d+3$	29 − 120	20 − 34	28 − 43
$n=d+4$	90 − 720	84 − 148	68 − 166
$n=d+5$	582 − 5040	401 − 733	283 − 4077

	$d=5$	$d=6$	$d=7$
$n=d+1$	3	3	3
$n=d+2$	9 − 12	9 − 18	9 − 18
$n=d+3$	28* − 43	28* − 60	28* − 60
$n=d+4$	95 − 166	95* − 216	95* − 216
$n=d+5$	236 − 714	236* − 850	236* − 850

For d odd, (5) gives

$$V(n, \lfloor (d-1)/2 \rfloor) = V(n,(d-1)/2) \ge \frac{n! d^n}{2^{d-1} n^n}.$$

Combining this with Theorem 11 we get the following explicit upper bound on $P(n,d)$.

Corollary 2: For d odd and $n > d \ge 1$, we have

$$P(n,d) \le \frac{2^{d-1} n^n}{d^n}.$$

Similarly, for d even, combining Theorem 11 and Theorem 12 with (5), we get the following.

Corollary 3: For d even and $n > d \ge 2$, we have

$$P(n,d) \le \min\left\{ \frac{2^{d-2} n^n}{(d-1)^n}, \frac{2^d (n+1)^{n+1}}{(d+1)^{n+1}} \right\}.$$

The bounds on $V(n,d)$, both the upper and the lower, are in most cases quite weak and so the bounds on $P(n,d)$ also become quite weak.

B. Table of Bounds on $p(n,d)$

We have used the following greedy algorithm to find an (n,d) PA C: Let the identity permutation in S_n be the first permutation in C. For any set of permutations chosen, choose as the next permutation in C the lexicographically next permutation in S_n with distance at least d to the chosen permutations in C if such a permutation exists. The size of the resulting PA is of course a lower bound on $P(n,d)$.

The lower bounds in Table II were in most cases found by this greedy algorithm. For $n = 8$, $d = 5$, the greedy algorithm gave a PA of size 26. However

$$P(8,5) \ge P(7,4) \ge 28$$

by Theorem 7. Similarly

$$P(10,7) \ge P(9,6) \ge P(8,5) \ge 28.$$

Some other of the lower bounds are also determined using Theorem 7. They are marked by $*$. The upper bound is the Hamming type bound in Theorem 11 or it's modified bound in Theorem 12. Since $P(n,1) = n!$ for all n, this is not included in the table.

V. Conclusion

We give a number of constructions of permutations arrays under the Chebyshev distance, some with efficient error correction algorithms. We also consider an explicit mapping of vectors to permutations with efficient encoding/decoding. Finally, we give some bounds on the size of PAs under the Chebyshev distance.

Tamo and Schwartz [15] independently considered this problem and gave, among other results, a construction equivalent to our first construction as well as some other constructions.

References

[1] P. Cappelletti, C. Golla, P. Olivo, and E. Zanoni, *Flash Memories*. Norwell, MA: Kluwer, 1999.

[2] H. Chadwick and L. Kurz, "Rank permutation group codes based on Kendall's correlation statistic," *IEEE Trans. Inf. Theory*, vol. IT-15, no. 3, pp. 306–315, Mar. 1969.

[3] P. Diaconis, *Group Representations in Probability and Statistics*. Hayward, CA: Inst. Math. Statist., 1988.

[4] S. Haykin, *Communication Systems*, 4th ed. Hoboken, NJ: Wiley, 2001.

[5] A. Jiang, R. Mateescu, M. Schwartz, and J. Bruck, "Rank modulation for flash memories," in *Proc. IEEE Int. Symp. Information Theory*, 2008, pp. 1731–1735.

[6] A. Jiang, M. Schwartz, and J. Bruck, "Error-correcting codes for rank modulation," in *Proc. IEEE Int. Symp. Information Theory*, 2008, pp. 1736–1740.

[7] M. Kendall and J. D. Gibbons, *Rank Correlation Methods*. London, U.K.: Edward Arnold, 1990.

[8] T. Kløve, Spheres of Permutations Under the Infinity Norm—Permutations With Limited Displacement, Reports in Informatics, Dept. Informatics, Univ. Bergen, 2008, Report no. 376.

[9] T. Kløve, "Generating functions for the number of permutations with limited displacement," *Electron. J. Combin., R104*, vol. 16, no. 1, Aug. 2009.

[10] T. Kløve, "Lower bounds on the size of spheres of permutations under the Chebychev distance," *Designs, Codes and Cryptography*, to be published.

[11] D. H. Lehmer, "Permutations with strongly restricted displacements," in *Combinatorial Theory and its Applications II*, P. Erdös, A. Rényi, and V. T. Sós, Eds. Amsterdam, The Netherlands: North Holland, 1970.

[12] K. W. Shum, "Permutation coding and MFSK modulation for frequency selective channel," *IEEE Personal, Indoor and Mobile Radio Commun.*, vol. 13, pp. 2063–2066, Sep. 2002.

[13] R. P. Stanley, *Enumerative Combinatorics*. Cambridge, U.K.: Cambridge Univ. Press, 1997, vol. I.

[14] E. Stoll and L. Kurz, "Suboptimum rank detection procedures using rank vector codes," *IEEE Trans. Commun.*, vol. COM-16, no. 6, pp. 402–410, Jun. 1968.

[15] I. Tamo and M. Schwartz, Correcting Limited-Magnitude Errors in the Rank-Modulation Scheme, 2009, arXiv:0907.3387.

[16] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2001.

Torleiv Kløve (M'89–SM'91–F'03) was born in Voss, Norway, 1943. He received the Cand. Mag., Cand. Real., and Dr. Philos. degrees from the University of Bergen, Norway, in 1966, 1967, and 1971, respectively.

He has been with the University of Bergen since 1971, first as Senior Lecturer in Mathematics, and, since 1982, Professor of Informatics. During the academic years 1975–1976, 1981–1982, and 1990–1991, he spent sabbaticals at the University of Hawaii at Manoa. During the academic year 2001–2002, he was a Visiting Professor at The Chinese University of Hong Kong, and during the fall semester 2002, he was Visiting Professor at Hong Kong University of Science and Technology. During the academic year 2008–2009, he spent a sabbatical at the University of California, Santa Cruz. His research interests include coding theory, number theory, and combinatorics. He is coauthor of the book *Error Detecting Codes* (Kluwer, 1995) and the author of the book *Codes for Error Detection* (World Scientific, 2007).

Prof. Kløve was Chairman of the 1996 IEEE Information Theory Workshop, Longyearbyen, Norway, Associate Editor for Coding Theory for IEEE Transactions on Information Theory (1996–1999), and member of the Board of Governors of the IEEE Information Theory Society (2001–2003).

Te-Tsung Lin received the B.S. and M.S. degrees in computer science from National Chiao Tung University, Taiwan, R.O.C., in 2005 and 2007, respectively. His research interests include combinatorics, coding theory, and algorithms.

Shi-Chun Tsai (M'06) received the B.S. and M.S. degrees in computer science and information engineering from National Taiwan University, Taiwan, R.O.C., in 1984 and 1988, respectively, and the Ph.D. degree in computer science from the University of Chicago, Chicago, IL, in 1996.

During 1993–1996, he served as Lecturer in the Computer Science Department, University of Chicago. During 1996–2001, he was an Associate Professor in the Information Management Department and Computer Science and Information Engineering Department, National Chi Nan University, Taiwan. He has been with the Department of Computer Science, National Chiao Tung University, Taiwan, since 2001, and was promoted to full Professor in 2007. His research interests include computational complexity, algorithms, coding theory, and combinatorics.

Wen-Guey Tzeng (M'07) received the B.S. degree in computer science and information engineering from National Taiwan University, Taiwan, R.O.C., in 1985, and the M.S. and Ph.D. degrees in computer science from the State University of New York at Stony Brook in 1987 and 1991, respectively.

He joined the Department of Computer and Information Science (now, Department of Computer Science), National Chiao Tung University, Taiwan, in 1991, where he now serves as Chairman of the department. His current research interests include cryptology, information security, and network security.