An Improvement on the Gilbert–Varshamov Bound for Permutation Codes

Fei Gao, Yiting Yang, and Gennian Ge

***Abstract*—Permutation codes have been shown to be useful in power line communications, block ciphers, and multilevel flash memory models. Construction of such codes is extremely difficult. In fact, the only general lower bound known is the Gilbert–Varshamov type bound. In this paper, we establish a connection between permutation codes and independent sets in certain graphs. Using the connection, we improve the Gilbert–Varshamov bound asymptotically by a factor $\log(n)$, when the code length n goes to infinity.**

***Index Terms*—Gilbert–Varshamov bound, permutation codes.**

I. Introduction

THE investigation of permutation codes (sometimes called permutation arrays) began more than 30 years ago with the articles [5], [9]. However, little attention was given to this topic until the past decade. Permutation codes have recently enjoyed a resurgence due to their applications in data transmission over power lines [8], [18], [21], as well as in the design of block ciphers [4] and in multilevel flash memories [11], [12]. In the power line application, we consider a common electric power line. While the primary function of the power line is to deliver the electric power, the frequency of the current can be modulated to produce a family of n "close" frequencies. At the receiver, as the power itself is received, these small variations in frequency can be decoded as symbols (see [2] and [18]). In order for this information transmission not to interfere with the power transmission, it is important that the frequencies remain as constant as possible. One way to achieve this is to use block coding with length n, and to insist that each codeword uses each of the n frequencies exactly once. In this transmission model, there are three main forms of noise:

1) permanent narrow-band noise, which affects some frequencies over a long period (e.g., noise from electrical equipment);
2) impulse noise of short duration, which affects many frequencies; and
3) white Gaussian noise (background noise).

In many traditional data transmission media (e.g., telephone lines and satellite communications), white Gaussian noise is the dominant type of errors affecting the system. But in our model, the other two types of errors are more important. In [8] and [21], permutation codes are used to correct errors for this type of transmission. The problem then reduces to finding the maximum number of codewords in a permutation code of a given length n subject to given distance requirements.

Let S_n be the symmetric group of permutations on n elements. A *permutation code* C is just a subset of S_n. The *length* of C is n and each permutation in C is called a *codeword*. The error-correction capability of C is related to its minimum Hamming distance. For two distinct permutations $\sigma, \pi \in S_n$, we define the *Hamming distance* $d_H(\sigma, \pi)$ between them to be the number of positions where they differ, i.e.,

$$d_H(\sigma, \pi) = |\{i \in [n] : \sigma(i) \neq \pi(i)\}|$$

where $[n] = \{1, 2, \ldots, n\}$. Alternatively, σ and π are at distance δ if $\sigma\pi^{-1}$ has exactly $n - \delta$ fixed points, in other words,

$$\left|\{i \in [n] : \sigma\pi^{-1}(i) = i\}\right| = n - \delta.$$

Therefore, we have $d_H(\sigma, \pi) = d_H(id, \sigma\pi^{-1})$, where id is the identity in S_n. We can always assume that $id \in C$ without loss of generality. We say that a permutation code C has *minimum Hamming distance* d if the distance between any two distinct permutations in C is at least d. A permutation code of length n with minimum Hamming distance d will be called an (n, d) permutation code (or a $PA(n, d)$), and the maximum number of codewords in such a code is denoted by $M(n, d)$. To deal with different error models, other types of distances have also been studied. For instance, permutation codes under Chebyshev distance constraint have been investigated in [14] and [15]. In this paper, we consider only the Hamming distance.

We will use a well-known connection between codes and independent sets in certain graphs. The main idea is to identify the code as an independent set in the corresponding graph and then study the maximum size of an independent set (called the independence number) using graph-theoretic tools and properties. Although this approach is universal, the difficulty is that for certain codes, the corresponding graph may not have the desired properties and/or some of the relevant parameters of this graph may be hard to compute.

Manuscript received May 29, 2012; revised October 06, 2012; accepted November 21, 2012. Date of publication January 04, 2013; date of current version April 17, 2013. F. Gao was supported by the Scholarship Award for Excellent Doctoral Student granted by the Ministry of Education of China. Y. Yang was supported in part by the National Natural Science Foundation of China under Grant 11101360 and in part by the China Postdoctoral Science Foundation funded project under Grant 20110491798. G. Ge was supported in part by the National Outstanding Youth Science Foundation of China under Grant 10825103, in part by the National Natural Science Foundation of China under Grant 61171198, and in part by the Specialized Research Fund for the Doctoral Program of Higher Education.

F. Gao is with the Department of Mathematics, Zhejiang University, Hangzhou 310027, China (e-mail: feigao.chn@gmail.com).

Y. Yang is with the Department of Mathematics, Tongji University, Shanghai 200092, China (e-mail: ytyang@tongji.edu.cn).

G. Ge is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China (e-mail: gnge@zju.edu.cn).

Communicated by G. Cohen, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2013.2237945

For example, Jiang and Vardy [13] and later Vu and Wu [22] used the previous connection to improve the Gilbert–Varshamov bound on binary and q-ary (nonlinear) codes, respectively. Jiang and Vardy [13] estimated the total number of edges t in the neighborhood of any vertex, and found that this number of edges is relatively small. They used this "locally sparse" property of the graph to obtain their results.

In this paper, we will use a different property. Specifically, we consider the maximum degree m in the neighborhood of any vertex in the corresponding graph, in order to obtain an improvement of the Gilbert–Varshamov-type lower bound for permutation codes. We choose this approach mainly due to its feasibility. While we can compute relatively good estimates of the maximum degree m, it seems infeasible to estimate the total number of edges t.

It should be noted that other properties of a graph could be also employed to derive bounds on its independence number. For a general discussion of bounds on the independence number from a graph-theoretic perspective, see Alon and Spencer [1].

The rest of this paper is organized as follows. In Section II, we review the known upper and lower bounds for permutation codes. In Section III, we introduce the relevant terminology and an important theorem from graph theory. Our improvements of the lower bound on $M(n,d)$ are presented in Section IV.

II. Some Known Bounds

A crucial problem in the theory of permutation codes is to determine the value of $M(n,d)$. Unfortunately, this problem turns out to be extremely difficult. In fact, not much progress has been made for $4 \le d \le n-1$, except for the small lengths. Therefore, most efforts are focused on seeking good upper or lower bounds for $M(n,d)$ (see [3], [6], [7], [10], and the references therein). The following are some well-known elementary consequences by basic combinatorial techniques.

Lemma 1:

1) $M(n,2) = n!$;
2) $M(n,3) = n!/2$;
3) $M(n,n) = n$;
4) $M(n,d) \le nM(n-1,d)$;
5) $M(n,d) \le n!/(d-1)!$.

Before proceeding, we need to introduce a useful notation which will greatly simplify our discussions throughout this paper. Let $D(n,k)$ $(k = 0,1,\ldots,n)$ denote the set of all permutations in S_n which are exactly at distance k from the identity, i.e.,

$$D(n,k) = \{\sigma \in S_n : d_H(\sigma, id) = k\}.$$

The cardinality of $D(n,k)$ is

$$|D(n,k)| = \binom{n}{k} D_k$$

where D_k is the number of derangements of order k.

Example 1: Since every nonidentity permutation moves at least two elements, we have $D(n,1) = \emptyset$. The sets $D(n,2)$ and $D(n,3)$ consist of cycles of length 2 (transpositions) and length 3, respectively. Elements in $D(n,4)$ are of two types: cycles of length 4 and the composition of two disjoint two cycles.

The Gilbert–Varshamov and sphere-packing bounds for permutation codes are well known, and generally outperform other bounds for small values of d.

Theorem 2:

$$\frac{n!}{\sum_{k=0}^{d-1} |D(n,k)|} \le M(n,d) \le \frac{n!}{\sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} |D(n,k)|}.$$

Using linear programming and representation theory of the characters of S_n, Dukes and Sawchuck [7] improve the upper bound on the special case $d = 4$ as follows.

Theorem 3: If $k^2 \le n \le k^2 + k - 2$ for some integer $k \ge 2$, then

$$\frac{n!}{M(n,4)} \ge 1 + \frac{(n+1)n(n-1)}{n(n-1) - (n-k^2)((k+1)^2 - n)((k+2)(k-1) - n)}.$$

For the small values of n and d, researchers have developed many computer searching strategies to directly look for permutation codes with some prescribed automorphisms. These methods usually provide the best known lower bounds on $M(n,d)$. The exact value of $M(n,d)$ could be determined whenever an exhaustive searching algorithm with only trivial automorphism finished running. Interested readers may refer to the tables in [19] and the references therein.

III. Graph Theory

A. Cayley Graph

Suppose that H is a group and S is a subset of H called the *generating set*. The *Cayley graph* $\Gamma = \Gamma(H,S)$ is a colored directed graph constructed as follows.

1) Each element g of H is assigned a vertex: the vertex set $V(\Gamma)$ of Γ is identified with H.
2) Each generator s of S is assigned a color c_s.
3) For any $g \in H$ and $s \in S$, the vertices corresponding to the elements g and gs are joined by a directed edge of color c_s. Thus, the edge set $E(\Gamma)$ consists of pairs of the form (g, gs), with $s \in S$ providing the color.

In geometric group theory, the set S is usually assumed to be finite, symmetric (i.e., $S = S^{-1}$) and not containing the identity element of the group. In this case, the uncolored Cayley graph is an ordinary graph: its edges are not oriented and it does not contain loops (single-element cycles).

B. Independence Number

An independent set of a graph G is a subset of vertices such that no two vertices in the subset represent an edge of G. The *independence number* $\alpha(G)$ of the graph G is the cardinality of the largest independent set. Formally,

$$\alpha(G) = \max\{|U| : U \subseteq V(G), U \text{ is an independent set}\}$$

where $V(G)$ is the vertex set of G and $|U|$ denotes the cardinality of the set U.

The independence number is an important parameter in graph theory and has been studied for a long time. It is also related to some other parameters such as chromatic number, clique

number, and so on. Here, we quote a result on the independence number from [16] and [17].

For $m \geq 1$ and $x \geq 0$, we define the function $f_m(x)$ by

$$f_m(x) = \int_0^1 \frac{(1-t)^{1/m}}{m + (x-m)t} dt.$$

This function has the following property. We use $\log(\cdot)$ to denote the natural logarithmic function hereafter.

Proposition 4: For $0 \leq x \leq m$, $f_m(x) \leq 1/(1+x)$; and for $m \geq 1$, $f_m(x) \geq \frac{\log(x/m)-1}{x}$.

Theorem 5 [16], [17]: Let $m \geq 1$ be an integer, and let G be a graph of order N with average degree Δ. If any subgraph induced by a neighborhood has maximum degree less than m, then

$$\alpha(G) \geq N \cdot f_m(\Delta) \geq N \cdot \frac{\log(\Delta/m) - 1}{\Delta}.$$

IV. New Lower Bound

In this section, we will improve the Gilbert–Varshamov lower bound of $M(n,d)$ by reformulating the problem to a problem of finding an independent set in the Cayley graph on group $H = S_n$ with some proper generating set S.

Let $S(n,k) = \cup_{i=1}^{k} D(n,i)$. Then, the Cayley graph we are interested in is

$$\Gamma(n,d) := \Gamma(S_n, S(n,d-1)).$$

By the definition of $S(n,k)$, we see that any two distinct permutations σ and π have distance $d_H(\sigma,\pi) \leq k$ if and only if $\sigma\pi^{-1} \in S(n,k)$. Therefore, there is an edge between σ and π in $\Gamma(n,d)$ if and only if their distance is less than d. Hence, we can identify an (n,d) permutation code with an independent set in $\Gamma(n,d)$ as follows.

Lemma 6: The codewords of an (n,d) permutation code are vertices of an independent set in $\Gamma(n,d)$. Conversely, any independent set in $\Gamma(n,d)$ is an (n,d) permutation code.

To apply Theorem 5 to get a lower bound for $M(n,d)$, we need a detailed calculation of the parameters of the Cayley graph $\Gamma(n,d)$. The number of vertices of $\Gamma(n,d)$ is $|S_n| = n!$. By the definition, $\Gamma(n,d)$ is a regular graph of degree $\Delta(n,d)$ which equals the size of the generating set, i.e.,

$$\Delta(n,d) = |S(n,d-1)| = \sum_{k=1}^{d-1} \binom{n}{k} D_k.$$

We use $G(n,d)$ to denote the subgraph induced by the neighborhood of identity in $\Gamma(n,d)$. Then, $G(n,d)$ has vertex set

$$V(G(n,d)) = S(n,d-1) = \bigcup_{k=1}^{d-1} D(n,k).$$

There is an edge between two distinct vertices σ and π in $V(G(n,d))$ if and only if they are with distance less than d, i.e., $\sigma\pi^{-1} \in S(n,d-1)$. We denote the maximum degree in $G(n,d)$ by $m(n,d)$.

Lemma 7: For any positive integer $n \geq 7$, we have $m(n,2) = 0$, $m(n,3) = 0$, $m(n,4) = 4n-8$, and $m(n,5) = 7n^2 - 31n + 34$.

Proof: Since $D(n,1) = \emptyset$, we have $m(n,2) = 0$.

The equality $m(n,3) = 0$ comes from the fact

$$d_H((ij),(kl)) = \begin{cases} 0, & \text{if } |\{i,j\} \cap \{k,l\}| = 2 \\ 3, & \text{if } |\{i,j\} \cap \{k,l\}| = 1 \\ 4, & \text{if } |\{i,j\} \cap \{k,l\}| = 0 \end{cases}$$

where $1 \leq i < j \leq n$ and $1 \leq k < l \leq n$.

By the definition, the vertices of $G(n,4)$ are $V(G(n,4)) = S(n,3) = D(n,2) \cup D(n,3)$, i.e., the 2-cycles and the 3-cycles. Without loss of generality, we only need to consider two special cases $(12) \in D(n,2)$ and $(123) \in D(n,3)$.

For the case of (12), we partition all the other vertices in $G(n,4)$ into four subsets.

$$\begin{aligned} N_{2,1} &= \{(1x),(2x) : 3 \leq x \leq n\}, \\ N_{2,2} &= \{(12x),(21x) : 3 \leq x \leq n\}, \\ N_{2,3} &= \{(xy),(1xy),(2xy) : 3 \leq x,y \leq n, x \neq y\}, \text{ and} \\ N_{2,4} &= \{(xyz),(xzy) : 3 \leq x < y < z \leq n\}. \end{aligned}$$

Then, $d_H(\sigma,(12))$ for each vertex σ is

$$d_H(\sigma,(12)) = \begin{cases} 3, & \text{if } \sigma \in N_{2,1} \\ 2, & \text{if } \sigma \in N_{2,2} \\ 4, & \text{if } \sigma \in N_{2,3} \\ 5, & \text{if } \sigma \in N_{2,4}. \end{cases}$$

Hence, the neighbors of (12) in $G(n,4)$ are $N_2 := N_{2,1} \cup N_{2,2}$.

For the case of (123), we partition all the other vertices into five subsets.

$$\begin{aligned} N_{3,1} &= \{(12),(13),(23)\}, \\ N_{3,2} &= \{(132),(12x),(23x),(31x) : 4 \leq x \leq n\}, \\ N_{3,3} &= \{(ix),(13x),(21x),(32x) : 1 \leq i \leq 3 < x \leq n\}, \\ N_{3,4} &= \{(xy),(ixy),(iyx) : 1 \leq i \leq 3 < x < y \leq n\}, \text{ and} \\ N_{3,5} &= \{(xyz),(xzy) : 4 \leq x < y < z \leq n\}. \end{aligned}$$

Then, $d_H(\sigma,(123))$ for each vertex σ is

$$d_H(\sigma,(123)) = \begin{cases} 2, & \text{if } \sigma \in N_{3,1} \\ 3, & \text{if } \sigma \in N_{3,2} \\ 4, & \text{if } \sigma \in N_{3,3} \\ 5, & \text{if } \sigma \in N_{3,4} \\ 5, & \text{if } \sigma \in N_{3,5}. \end{cases}$$

Hence, the neighbors of (123) are $N_3 := N_{3,1} \cup N_{3,2}$.

Therefore, we have

$$\begin{aligned} m(n,4) &= \max\{|N_2|, |N_3|\} \\ &= \max\{4(n-2), 3(n-3)+4\} \\ &= 4n-8. \end{aligned}$$

With a similar analysis to that of $m(n,4)$, we can obtain that (12) has the largest neighborhood and $m(n,5) = 7n^2 - 31n + 34$. Here, we need to consider the neighbors of every type of vertices in $G(n,5)$, namely $(12) \in D(n,2)$, $(123) \in D(n,3)$, and $(12)(34), (1234) \in D(n,4)$. ■

Applying the previous analysis to Theorem 5, we have the following lower bound on $M(n,d)$.

TABLE I
LOWER BOUNDS FOR $M(n,d)$ WITH $d=4,5$ AND $8 \le n \le 20$

n	$d=4$	$d=5$
8	605	90
9	4046	509
10	31047	3386
11	268673	25885
12	2588633	223378
13	27484422	2147724
14	318853331	22767826
15	4013217263	263832788
16	54470270765	3317928906
17	793090335806	45006297715
18	12331219009156	655021291542
19	203926244407855	10181693092799
20	3574258846215948	168351610362186

Theorem 8: Let $m'(n,d) = m(n,d)+1$, and

$$M_{IS}(n,d) := n! \cdot \int_0^1 \frac{(1-t)^{1/m'(n,d)}}{m'(n,d)+[\Delta(n,d)-m'(n,d)]\,t} \cdot dt.$$

Then, $M(n,d) \ge M_{IS}(n,d)$.

For $d=4,5$ and $8 \le n \le 20$, we list the evaluations of integrals $M_{IS}(n,d)$ in Table I. These values are computed by the open source mathematics software Sage [20]. In the special case $(n,d)=(13,5)$, our evaluated value 2 147 724 greatly improves the result in [2] and [19] which is $M(13,5) \ge 878\,778$.

In the rest of this paper, we consider the asymptotic behavior of our lower bounds $M_{IS}(n,d)$ when d is fixed and n goes to infinity.

Lemma 9: $m(n,d) = O(n^{d-3})$.

Proof: Let $\sigma \in D(n,k)$ $(1 \le k \le d-1)$ be a fixed neighbor of identity. We shall estimate the degree of σ in $G(n,d)$, i.e., the number of π's in $G(n,d)$ which is also a neighbor of σ.

First, we partition $[n]$ into (at most) five disjoint subsets due to their images under id, σ, and π, respectively. Let

$$\begin{aligned}
X &= \{i \in [n] : \sigma(i) \ne i, \pi(i) = i\},\\
Y &= \{i \in [n] : \sigma(i) \ne i, \pi(i) = \sigma(i)\},\\
Z &= \{i \in [n] : \sigma(i) \ne i, \pi(i) \ne i, \sigma(i) \ne \pi(i)\},\\
U &= \{i \in [n] : \sigma(i) = i, \pi(i) \ne i\}, \text{ and}\\
V &= \{i \in [n] : \sigma(i) = \pi(i) = i\}.
\end{aligned}$$

Let x, y, z, u, and v be the cardinalities of X, Y, Z, U, and V respectively. Then, the distance constraints give us the following inequalities:

$$x+y+z = k \le d-1 \quad (1)$$
$$y+z+u \le d-1 \quad (2)$$
$$x+z+u \le d-1 \text{ and} \quad (3)$$
$$x+y+z+u+v = n.$$

In particular, $(2)+(3)-(1)$ gives

$$u \le \frac{2d-2-(k+z)}{2} \le d-1-\lfloor \frac{k+z}{2} \rfloor.$$

The number of π's in the neighborhood of σ is determined by the images of Y, Z, and U under π. Since $y+z$ is bounded by k, the dominating term in the estimation would be the number of choices of U. Before we do a case-by-case analysis on k, we give the following claim:

Claim: If $z=0$, then $x \ne 1$ and $y \ne 1$.

Proof of Claim: Assume that $Z=\emptyset$ and $X=\{i\}$, then $i \in \sigma(Y) = \pi(Y)$; this contradicts to the fact that $\pi(i)=i$ followed by the definition of X. A similar discussion shows that $z=0$ and $y=1$ cannot hold simultaneously.

In the case $k=2$, the claim implies that either $x=0$ or $y=0$, and we have $u \le d-3$ from (2) or (3). Since $|Y \cup Z| \le k = 2$ and $|U| \le d-1-k = d-3$, the choice of π is bounded by the possible images of $Y \cup Z$ and U, i.e.,

$$\deg(\sigma) \le 2! \cdot \binom{n-2}{d-3}(d-3)! = O(n^{d-3}).$$

Let $k=3$. If $z=0$, the claim implies either $x=0$ and $y=3$, or $x=3$ and $y=0$. Both cases give $u \le d-4$. If $z \ge 1$, we obtain $u \le d-1-\lfloor \frac{k+z}{2} \rfloor \le d-3$. Hence, $\deg(\sigma) = O(n^{d-3})$.

When $k \ge 4$, we have $u \le d-1-\lfloor \frac{k+z}{2} \rfloor \le d-3-\lfloor \frac{k-3}{2} \rfloor \le d-3$. So, $\deg(\sigma) = O(n^{d-3})$.

Therefore

$$m(n,d) = \max_{2 \le k \le d-1} \{\deg(\sigma) : \sigma \in D(n,k)\} = O(n^{d-3}).$$

■

Using our notations, the Gilbert–Varshamov bound is

$$M(n,d) \ge M_{GV}(n,d) := \frac{n!}{1+\Delta(n,d)}.$$

Theorem 10: When d is fixed and n goes to infinity, we have

$$\frac{M_{IS}(n,d)}{M_{GV}(n,d)} = \Omega(\log(n)).$$

Proof:

$$\begin{aligned}
\frac{M_{IS}(n,d)}{M_{GV}(n,d)} &= \frac{n! \int_0^1 \frac{(1-t)^{1/m'(n,d)}}{m'(n,d)+[\Delta(n,d)-m'(n,d)]t} \cdot dt}{\frac{n!}{1+\Delta(n,d)}}\\
&\ge \frac{\frac{\log(\Delta(n,d)/m'(n,d))-1}{\Delta(n,d)}}{\frac{1}{\Delta(n,d)+1}}\\
&\ge \log\left(\frac{\Delta(n,d)}{m'(n,d)}\right) - 1.
\end{aligned}$$

Since $D_k = \lfloor \frac{k!}{e} + \frac{1}{2} \rfloor$, we have

$$\Delta(n,d) = \sum_{k=0}^{d-1} \binom{n}{k} D_k = \Theta(n^{d-1}).$$

Then

$$\begin{aligned}
\frac{M_{IS}(n,d)}{M_{GV}(n,d)} &\ge \log\left(\frac{\Delta(n,d)}{m'(n,d)}\right) - 1\\
&\ge \log(cn^2) - 1\\
&= 2\log(cn) - 1\\
&= \Omega(\log(n))
\end{aligned}$$

where c is some positive constant. ■

ACKNOWLEDGMENT

The authors express their gratitude to the two anonymous referees for their detailed and constructive comments which are very helpful to the improvement of the technical presentation of this paper and to Professor Gerard Cohen, the associate editor, for his insightful advice and excellent editorial job.

REFERENCES

[1] N. Alon and J. H. Spencer, *The Probabilistic Method*, ser. Wiley-Interscience Series in Discrete Mathematics and Optimization, 3rd ed. Hoboken, NJ, USA: Wiley, 2008.

[2] W. Chu, C. J. Colbourn, and P. Dukes, "Constructions for permutation codes in powerline communications," *Des. Codes Cryptogr.*, vol. 32, no. 1–3, pp. 51–64, 2004.

[3] 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, Jun. 2004.

[4] D. R. de la Torre, C. J. Colbourn, and A. C. H. Ling, "An application of permutation arrays to block ciphers," in *Proc. 31st Southeastern Int. Conf. Combinatorics, Graph Theory Comput.*, Boca Raton, FL, USA, 2000, vol. 145, pp. 5–7.

[5] M. Deza and S. A. Vanstone, "Bounds for permutation arrays," *J. Statist. Planning Inference*, vol. 2, no. 2, pp. 197–209, 1978.

[6] 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, Apr. 2002.

[7] P. Dukes and N. Sawchuck, "Bounds on permutation codes of distance four," *J. Algebr. Combinatorics*, vol. 31, no. 1, pp. 143–158, 2010.

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

[9] P. Frankl and M. Deza, "On the maximum number of permutations with given maximal or minimal distance," *J. Combinatorial Theory Series A*, vol. 22, no. 3, pp. 352–360, 1977.

[10] F.-W. Fu and T. Kløve, "Two constructions of permutation arrays," *IEEE Trans. Inf. Theory*, vol. 50, no. 5, pp. 881–883, May 2004.

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

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

[13] T. Jiang and A. Vardy, "Asymptotic improvement of the Gilbert-Varshamov bound on the size of binary codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1655–1664, Aug. 2004.

[14] T. Kløve, "Lower bounds on the size of spheres of permutations under the Chebychev distance," *Des. Codes Cryptogr.*, vol. 59, no. 1–3, pp. 183–191, 2011.

[15] T. Kløve, T.-T. Lin, S.-C. Tsai, and W.-G. Tzeng, "Permutation arrays under the Chebyshev distance," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2611–2617, Jun. 2010.

[16] Y. Li and C. C. Rousseau, "On book-complete graph Ramsey numbers," *J. Combinatorial Theory Series B*, vol. 68, no. 1, pp. 36–44, 1996.

[17] Y. Li, C. C. Rousseau, and W. Zang, "Asymptotic upper bounds for Ramsey functions," *Graphs Combinatorics*, vol. 17, no. 1, pp. 123–128, 2001.

[18] N. Pavlidou, A. J. H. Vinck, J. Yazdani, and B. Honary, "Power line communications: State of the art and future trends," *IEEE Commun. Mag.*, vol. 41, no. 4, pp. 34–40, Apr. 2003.

[19] D. H. Smith and R. Montemanni, "A new table of permutation codes," *Des. Codes Cryptogr.*, vol. 63, no. 2, pp. 241–253, 2012.

[20] W. Stein *et al.*, Sage Mathematics Software (Version 5.1) 2012 [Online]. Available: http://www.sagemath.org, The Sage Development Team

[21] A. J. H. Vinck, "Coded modulation for powerline communications," *A.E.Ü. Int. J. Electron. Commun.*, vol. 54, pp. 45–49, 2000.

[22] V. Vu and L. Wu, "Improving the Gilbert-Varshamov bound for q-ary codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3200–3208, Sep. 2005.

Fei Gao is currently a Ph.D. student at Zhejiang University, Hangzhou, Zhejiang, P. R. China. His research interests include combinatorial design theory, coding theory, cryptography, and their interactions.

Yiting Yang received his M.S. degree from Center for Combinatorics, Nankai University, Tianjin, P. R. China, in 2004. In 2010, he received his Ph.D. degree from Department of Mathematics, University of South Carolina, Columbia, U.S.A. After that, he was a postdoctor for two and a half years in Department of Mathematics, Zhejiang University, Hangzhou, P. R. China. Now he is an assistant professor in Department of Mathematics, Tongji University, Shanghai, P. R. China. His research interests include extremal combinatorics, probablistic method and their applications.

Gennian Ge received the M.S. and Ph.D. degrees in mathematics from Suzhou University, Suzhou, Jiangsu, P. R. China, in 1993 and 1996, respectively. After that, he became a member of Suzhou University. He was a postdoctoral fellow in the Department of Computer Science at Concordia University, Montreal, QC, Canada, from September 2001 to August 2002, and a visiting assistant professor in the Department of Computer Science at the University of Vermont, Burlington, Vermont, USA, from September 2002 to February 2004. He was a full professor in the Department of Mathematics at Zhejiang University, Hangzhou, Zhejiang, P. R. China, from March 2004 to February 2013. Currently, he is a full professor in the School of Mathematical Sciences at Capital Normal University, Beijing, P. R. China. His research interests include the constructions of combinatorial designs and their applications to codes and crypts.

Dr. Ge is on the Editorial Board of the *Journal of Combinatorial Designs, The Open Mathematics Journal,* and the *International Journal of Combinatorics*. He received the 2006 Hall Medal from the Institute of Combinatorics and its Applications.