Des. Codes Cryptogr. (2017) 85:533–545
DOI 10.1007/s10623-016-0321-5

New bounds of permutation codes under Hamming metric and Kendall's τ-metric

Xin Wang[1,2] · **Yiwei Zhang**[1] · **Yiting Yang**[3] · **Gennian Ge**[1,4]

Received: 30 June 2016 / Revised: 27 November 2016 / Accepted: 16 December 2016 /
Published online: 30 December 2016

Abstract Permutation codes are widely studied objects due to their numerous applications in various areas, such as power line communications, block ciphers, and the rank modulation scheme for flash memories. Several kinds of metrics are considered for permutation codes according to their specific applications. This paper concerns some improvements on the bounds of permutation codes under Hamming metric and Kendall's τ-metric respectively, using mainly a graph coloring approach. Specifically, under Hamming metric, we improve the Gilbert–Varshamov bound asymptotically by a factor n, when the minimum Hamming distance d is fixed and the code length n goes to infinity. Under Kendall's τ-metric, we narrow the gap between the known lower bounds and upper bounds. Besides, we also obtain some sporadic results under Kendall's τ-metric for small parameters.

Keywords Permutation codes · Hamming metric · Kendall's τ-metric · Gilbert–Varshamov bound · Independent set

Mathematics Subject Classification 94B25 · 94B65

1 Introduction

Let S_n be the symmetric group on n elements. A permutation code is a subset of S_n satisfying certain constraints. Permutation codes have been studied under various metrics according to

Communicated by C. Ding.

✉ Gennian Ge
gnge@zju.edu.cn

[1] School of Mathematical Sciences, Capital Normal University, Beijing 100048, China

[2] School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, Zhejiang, China

[3] Department of Mathematics, Tongji University, Shanghai 200092, China

[4] Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing 100048, China

specific applications. In this paper we focus on two kinds of metrics, the Hamming metric and the Kendall's τ-metric. We now briefly introduce the motivations for these two metrics.

During the last decade, permutation codes under Hamming metric have attracted considerable attention, due to their applications in data transmission over power lines [10,18,21]. Permutation codes under Hamming metric are used to correct errors caused by the permanent narrow-band noise and the impulse noise of short duration in power line transmissions. Besides, permutation codes under Hamming metric have been applied in the design of block ciphers [7]. The research on permutation codes under Kendall's τ-metric has a relatively shorter history, which originates from the development of flash memories. *Rank modulation* is introduced in [14] as a proper framework for dealing with errors caused by over-programming and charge leakage in flash memories. Instead of encoding information with the absolute values of charge levels, data is represented by the relative rankings of the charge levels on a group of cells. That is, if we have n cells and $c_1, c_2, \ldots, c_n \in \mathbb{R}$ represent the charge levels, then this group of cells is said to encode the permutation $\sigma \in S_n$ such that $c_{\sigma(1)} > c_{\sigma(2)} > \cdots > c_{\sigma(n)}$. To detect and/or correct errors in the relative rankings, several metrics on permutations are used such as Kendall's τ-metric [1,3,15,17], Ulam metric [9] and l_∞-metric [16,20].

The rest of this paper is organized as follows. In Sect. 2 we give the definitions and notations of permutation codes under Hamming metric and Kendall's τ-metric and summarize some important known facts regarding the bounds on them, and then we introduce the corresponding graph models as a preparatory step for the upcoming analysis. A lower bound of permutation codes under Hamming metric is given in Sect. 3 which improves the Gilbert–Varshamov bound by a factor of n. A lower bound of permutation codes under Kendall's τ-metric is given in Sect. 4. In Sect. 5 some other sporadic results concerning permutation codes under Kendall's τ-metric are listed. We conclude in Sect. 6.

2 Preliminaries

In this section we first give some definitions and notations for permutation codes under Hamming metric and Kendall's τ-metric and summarize some important known facts regarding the bounds.

Let $[n]$ denote $\{1, 2, \ldots, n\}$. Let $\pi = [\pi_1, \pi_2, \ldots, \pi_n]$ be a permutation over $[n]$ such that for each $i \in [n]$ we have $\pi(i) = \pi_i$. This form is known as the *vector notation* for a permutation. For an integer $x \in [n]$, $\pi^{-1}(x)$ indicates the position of x appearing in π. For two permutations σ and π, their composition, denoted by $\sigma\pi$, is the permutation with $\sigma\pi(i) = \sigma(\pi(i))$ for all $i \in [n]$. All the permutations under this operation form the noncommutative group S_n known as the symmetric group on $[n]$ of size $|S_n| = n!$. Denote by $\varepsilon \triangleq [1, 2, \ldots, n]$ the identity element of the group. For an unordered pair of distinct numbers $x, y \in [n]$, this pair forms an *inversion* in a permutation π if $x < y$ and simultaneously $\pi^{-1}(x) > \pi^{-1}(y)$. Let $I(\pi)$ denote the total number of inversions in a permutation π. π is called an even/odd permutation accordingly due to the parity of $I(\pi)$.

2.1 Hamming metric

For two permutations σ and π, the *Hamming distance* between them is the number of positions in which their vector notations differ, i.e.

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

For $1 \le d \le n$, we say that $\mathcal{C} \subset S_n$ is an (n, d)-*permutation code under Hamming metric*, if $d_H(\sigma, \pi) \ge d$ for every two distinct permutations $\sigma, \pi \in \mathcal{C}$. Denote the largest size of an (n, d)-permutation code under Hamming metric as $A_H(n, d)$ and a code attaining this size is said to be optimal. The exact value of $A_H(n, d)$ and the constructions of optimal codes are the main research objectives. There are some fundamental results by basic combinatorial techniques.

Proposition 1 [5, Proposition 1.1]

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

However, deciding $A_H(n, d)$ turns out to be difficult for $4 \le d \le n-1$, except for some specifical cases.

Proposition 2 1. [6] *If there are m mutually orthogonal Latin squares of order n, then* $A_H(n, n-1) \ge mn$. *In particular, if q is a prime power, then* $A_H(q, q-1) = q(q-1)$.
2. [11] *If q is a prime power, then* $A_H(q+1, q-1) = (q+1)q(q-1)$.

We now summarize some important general results concerning the lower and upper bounds of $A_H(n, d)$.

Let $D(n, k)$ $(k = 0, 1, \ldots, n)$ denote the set of all permutations in S_n which are exactly at distance k under Hamming metric from the identity permutation ε:

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

A *derangement* of order k is a permutation $\pi \in S_k$ with no fixed points, i.e., $\pi_i \ne i$ for $1 \le i \le k$. Let D_k be the number of derangements of order k. Then the cardinality of $D(n, k)$ is

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

For any permutation $\pi \in S_n$, the *Hamming ball* of radius r centered at π, denoted as $B_H(\pi, r)$, is defined by $B_H(\pi, r) \triangleq \{\sigma \in S_n : d_H(\sigma, \pi) \le r\}$. Clearly under Hamming metric the size of a ball of radius r does not depend on the center of the ball and we denote its size as $B_H(r)$:

$$B_H(r) = \sum_{k=0}^{r} |D(n, k)|.$$

The Gilbert–Varshamov bound and sphere-packing bound for permutation codes under Hamming metric are well-known.

Proposition 3

$$\frac{n!}{B_H(d-1)} \le A_H(n, d) \le \frac{n!}{B_H\left(\lfloor \frac{d-1}{2} \rfloor\right)}.$$

Improved lower bound for the case when d is fixed and $n \to \infty$ is derived by Gao, Yang and Ge in [12].

Proposition 4 [12, Theorem 10] *Let d be fixed and $n \to \infty$. Then*

$$A_H(n,d) \geq \Omega\big(\log n \frac{n!}{B_H(d-1)}\big).$$

Later, Tait, Vardy and Verstraëte [19] consider the case when the ratio d/n is fixed and improve the Gilbert–Varshamov bound by a factor of n.

Proposition 5 [19, Theorem 2] *Let d/n be a fixed ratio with $0 < d/n < 0.5$. Then as $n \to \infty$, we have*

$$A_H(n,d) \geq \Omega\big(n \frac{n!}{B_H(d-1)}\big).$$

2.2 Kendall's τ-metric

Given a permutation $\pi = [\pi_1, \pi_2, \ldots, \pi_n] \in S_n$, an *adjacent transposition* is an exchange of two adjacent elements π_i, π_{i+1}, for some $1 \leq i \leq n-1$, resulting in the permutation $[\pi_1, \ldots, \pi_{i-1}, \pi_{i+1}, \pi_i, \pi_{i+2}, \ldots, \pi_n]$. The *Kendall's τ-distance* between two permutations σ and π, denoted by $d_K(\sigma, \pi)$, is the minimum number of adjacent transpositions required to transform one permutation into the other. For example, the Kendall's τ-distance between $\pi_1 = [1, 2, 3, 4, 5]$ and $\pi_2 = [2, 3, 1, 5, 4]$ is three, since we may do the adjacent transpositions $[1, 2, 3, 4, 5] \to [2, 1, 3, 4, 5] \to [2, 3, 1, 4, 5] \to [2, 3, 1, 5, 4]$ and one may easily check that only two adjacent transpositions are not enough. A well-known equivalent expression for $d_K(\sigma, \pi)$ [15] is as follows:

$$d_K(\sigma, \pi) = |\{(i, j) : \sigma^{-1}(i) < \sigma^{-1}(j) \wedge \pi^{-1}(i) > \pi^{-1}(j)\}|.$$

For $1 \leq d \leq \binom{n}{2}$, we say that $\mathcal{C} \subset S_n$ is an (n, d)-*permutation code under Kendall's τ-metric*, if $d_K(\sigma, \pi) \geq d$ for every two distinct permutations $\sigma, \pi \in \mathcal{C}$. Denote the largest size of an (n, d)-permutation code under Kendall's τ-metric as $A_K(n, d)$ and a code attaining this size is said to be optimal. The exact value of $A_K(n, d)$ and the constructions of optimal codes are the main research objectives. There are some fundamental results as follows.

Proposition 6 1. *$A_K(n, 2) = n!/2$ and the optimal codes are either the set of all even permutations or the set of all odd permutations;*
4. [3, Theorem 10] *For $\frac{2}{3}\binom{n}{2} < d \leq \binom{n}{2}$, $A_K(n, d) = 2$.*

However, deciding $A_K(n, d)$ turns out to be difficult for $3 \leq d \leq \frac{2}{3}\binom{n}{2}$. We now summarize some important results concerning the lower and upper bounds of $A_K(n, d)$.

Similarly as above we first introduce the Gilbert–Varshamov type lower bound and the sphere-packing upper bound. For any permutation $\pi \in S_n$, the *Kendall's τ-ball* of radius r centered at π, denoted as $B_K(\pi, r)$, is defined by $B_K(\pi, r) \triangleq \{\sigma \in S_n : d_K(\sigma, \pi) \leq r\}$. Clearly under Kendall's τ-metric the size of a ball of radius r does not depend on the center of the ball and we denote its size as $B_K(r)$. The Gilbert–Varshamov bound and sphere-packing bound for permutation codes under Kendall's τ-metric are as follows:

Proposition 7 [15, Theorems 17 and 18]

$$\frac{n!}{B_K(d-1)} \leq A_k(n, d) \leq \frac{n!}{B_K(\lfloor \frac{d-1}{2} \rfloor)}.$$

For two permutations σ and π with $d_K(\sigma, \pi) = 1$, the *double ball of radius* r centered at σ and π is defined by $DB(\sigma, \pi, r) \triangleq B(\sigma, r) \cup B(\pi, r)$. Denote by $DB_{n,r}$ the double ball of radius r in S_n centered at the identity permutation ε and the permutation $[2, 1, 3, 4, \ldots, n]$. Improved upper bound for the cases when d is even is derived in [3], using a code-anticode approach. An *anticode* is a subset of codewords with a given maximum distance.

Proposition 8 [3, Corollaries 3 & 5] *If a code $\mathcal{C} \subset S_n$ has minimum Kendall's τ-distance d, and an anticode $\mathcal{A} \subset S_n$ has maximum Kendall's τ-distance $d - 1$, then $|\mathcal{C}| \cdot |\mathcal{A}| \leq n!$. Particularly, since $DB_{n,r}$ is an anticode of diameter $2r + 1$, so we have*

$$A_K(n, 2(r+1)) \leq \frac{n!}{|DB_{n,r}|}.$$

Regarding the improvements on the lower bound, first we note that we could just concentrate on $A_K(n, d)$ with odd d, since we have the following simple but useful fact [15]:

Lemma 9 [15, Theorem 26] *For all n and $t \geq 1$ we have $A_K(n, 2t) \geq \frac{1}{2} A_K(n, 2t - 1)$.*

An important improvement of the lower bound is derived in [1], which is a generalization of a construction of an $(n, 3)$-permutation code under Kendall's τ-metric using codes in the Lee metric appeared in [15]. The generalization leads to a construction of an $(n, 2t + 1)$-permutation code under Kendall's τ-metric, which is of optimal size up to a constant factor, for a fixed t.

Proposition 10 [1, Theorem 4.5] *Let $m = ((n-2)^{t+1} - 3)/(n-3)$, where $n - 2$ is a prime power. Then we have*

$$A_K(n, 2t+1) \geq \begin{cases} n!/(t(t+1)m), & t \ \textit{odd}; \\ n!/(t(t+2)m), & t \ \textit{even}. \end{cases}$$

2.3 Graph models

Finally in this section we introduce a natural connection between codes and independent sets of their corresponding graphs. A graph G consists of a set of vertices $V(G)$ and a set of edges $E(G)$. Two vertices u and v are called adjacent if $\{u, v\} \in E(G)$. An independent set in a graph is a set of vertices where every pair of vertices are nonadjacent. The size of the largest independent set in a graph G is called the independence number, denoted as $\alpha(G)$.

Let G_H and G_K be graphs with the same vertex set S_n. Two vertices are connected in G_H (respectively, G_K) if and only if their Hamming distance (respectively, Kendall's τ-distance) is at most $d - 1$. Then, an (n, d)-permutation code under Hamming metric (respectively, Kendall's τ-metric) is equivalent to an independent set in G_H (respectively, G_K). Via this natural connection, graph-theoretic tools for analyzing independence numbers can be used for analyzing bounds of codes.

In this paper, we mainly use a coloring approach to analyze the lower bound of the independence numbers of G_H and G_K. A *coloring* of a graph assigns a color to each vertex. It is called a *proper coloring* if it never assigns the same color to both endpoints of an edge. The chromatic number of a graph G, denoted by $\chi(G)$, is the smallest integer k such that a proper coloring of G using k colors exists. Given a proper coloring, by definition every set of vertices with a same color constitutes an independent set. So we have

Lemma 11 $\alpha(G) \geq |V(G)|/\chi(G)$.

Thus, lower bounds of $\alpha(G)$ could be derived via analyzing upper bounds of $\chi(G)$.

Another fact concerning the independence number of a graph is as follows. An *automorphism* of a graph G is a bijective function $f : V(G) \to V(G)$, such that for any pair of vertices $u, v \in V(G)$, $(f(u), f(v)) \in E(G)$ if and only if $(u, v) \in E(G)$. A graph G is called *vertex transitive* if for any two vertices u and v, there exists some automorphism $f : V(G) \to V(G)$ such that $f(u) = v$. Then it is well known that (see, for example [13])

Lemma 12 *If the graph G is vertex-transitive and G' is any induced subgraph of G. Then we have*

$$\frac{\alpha(G)}{|V(G)|} \leq \frac{\alpha(G')}{|V(G')|}.$$

3 A lower bound of permutation codes under Hamming metric

In this section we consider the lower bound of $A_H(n, d)$ by giving a proper coloring for the graph G_H.

Theorem 13 *Let n, d be integers, $4 \leq d \leq n - 1$. Let p be the smallest prime number greater than or equal to n. Then, we have*

$$A_H(n, d) \geq \frac{n!}{p^{d-2}}.$$

Proof Let $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ denote the residue class modulo p. View the vector notation of a permutation as an $n \times 1$ vector. Consider the coloring map

$$f : S_n \to \mathbb{Z}_p^{d-1},$$

whose value at $\sigma \in S_n$ is determined by

$$f(\sigma) = A\sigma \pmod{p},$$

where A is a $(d-1) \times n$ Vandermonde matrix as follows ($x_1, x_2 \ldots, x_n$ are distinct numbers in $\{0, 1, \ldots, p-1\}$):

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{d-2} & x_2^{d-2} & \cdots & x_n^{d-2} \end{pmatrix}.$$

We claim that this coloring is proper. For any two distinct permutations σ and π with a same color $v \in \mathbb{Z}_p^{d-1}$, we have $A\sigma \equiv A\pi \equiv v \pmod{p}$. So $A(\sigma - \pi) \equiv 0 \pmod{p}$. Suppose the distance between σ and π is less than d, then there are at most $d-1$ nonzero coordinates in $\sigma - \pi$. Then we can deduce that there exist $d-1$ columns in A which are linearly dependent in $\mathbb{Z}_p$, which is a contradiction to the fact that every $d-1$ columns in A are linearly independent in $\mathbb{Z}_p$. Thus every two vertices with the same color are nonadjacent in G_H. So our coloring is proper.

Now we count the number T of colors we used. The colors are in $\mathbb{Z}_p^{d-1}$ and note that the first coordinate is a constant $1 + 2 + \cdots + n \pmod{p}$. Thus $T \leq p^{d-2}$. Now each color corresponds to an independent set in G_H, or equivalently, an (n, d)-permutation code under Hamming metric. By Lemma 11 we have

$$|A_H(n,d)| \geq \frac{n!}{p^{d-2}}.$$

□

Consider the asymptotic behavior of our lower bound. The following notations simplify the upcoming statements and comparisons. In the remaining part of this section, $A_H(n, d)$ denotes the bound we get in Theorem 13, $A_H^{GV}(n, d)$ denotes the classical Gilbert–Varshamov bound and $\widetilde{A}_H(n, d)$ denotes the lower bound derived in [12].

Corollary 14 *When d is a fixed constant and n goes into infinity, $A_H(n, d)$ improves the classical Gilbert–Varshamov bound by a factor of n, that is,*

$$\frac{A_H(n,d)}{A_H^{GV}(n,d)} = \Omega(n).$$

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

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

It is well known [4] that there exists a prime p, satisfying $n \leq p \leq 2n$,

$$A_H(n,d) \geq \frac{n!}{p^{d-2}} \geq \frac{n!}{(2n)^{d-2}}.$$

Then

$$\frac{A_H(n,d)}{A_H^{GV}(n,d)} \geq \frac{B_H(d-1)}{(2n)^{d-2}} = \Omega(n).$$

□

Furthermore, our lower bound also performs quite well when n is small. For $d = 5$ and $8 \leq n \leq 20$, we list the results of $\widetilde{A}_H(n, d)$ and $A_H(n, d)$ in Table 1. Relatively better values are in bold form.

To sum up, the analysis above gives:

Theorem 15 *When d is a fixed constant and n goes into infinity,*

$$A_H(n,d) \geq \Omega\Big(n \frac{n!}{B_H(d-1)}\Big).$$

A final remark is a comparison of our result with Proposition 5, the result obtained by Tait, Vardy and Verstraëte [19]. They are restricted to the case when d/n is a fixed ratio with $0 < d/n < 0.5$. Whereas our result considers the case when d is fixed and n goes into infinity, that is, the ratio d/n goes into zero. So in some sense our result works as a complement of theirs.

4 A lower bound of permutation codes under Kendall's τ-metric

In the rest of this paper we turn our attention into Kendall's τ-metric. As has been noted in Proposition 10, the lower bound of $A_K(n, d)$ derived by [1] meets the sphere-packing upper

Table 1 A comparison of $A_H(n,d)$ and $\widetilde{A}_H(n,d)$ with $d = 5$ and $8 \le n \le 20$

n	$A_H(n,d)$	$\widetilde{A}_H(n,d)$
8	30	**90**
9	272	**509**
10	2726	**3386**
11	**29,990**	25,885
12	218,025	**223,378**
13	**2,834,328**	2,147,724
14	17,744,410	**22,767,826**
15	**266,166,164**	263,832,788
16	**4,258,658,637**	3,317,928,906
17	**72,397,196,844**	45,006,297,715
18	**933,426,695,688**	655,021,291,542
19	**17,735,107,218,083**	10,181,693,092,799
20	**199,959,070,286,565**	168,351,610,362,186

bound asymptotically for any fixed d. There's only a constant gap between the lower and upper bounds. In this section we attempt to narrow this gap.

For a permutation $\pi \in S_n$, an *inversion vector* $x_\pi = (x_\pi(2), x_\pi(3), \ldots, x_\pi(n)) \in \mathbb{Z}_n! \triangleq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \cdots \times \mathbb{Z}_n$ is defined as:

$$x_\pi(i) = |\{j : j < i, \pi^{-1}(j) > \pi^{-1}(i)\}|, 2 \le i \le n.$$

That is, $x_\pi(i) \in \mathbb{Z}_i$ counts the number of inversions formed by 'i' and 'j', $1 \le j \le i-1$. For example, let $\pi = [4, 5, 2, 1, 3]$. Then $x_\pi = (1, 0, 3, 3)$. The sum of all entries equals the total number of inversions $I(\pi)$.

An adjacent transposition results in an error of weight one in the inversion vector x_π. Specifically, suppose we have two consecutive numbers a and b in the original permutation, with $a < b$. Then an adjacent transposition which switches a and b will result in an error $\mathbf{e}_\mathbf{b}^+$, which is a vector with $+1$ on the entry $x_\pi(b)$ and 0 elsewhere. Continuing the example, switch '4' and '5' in π, we have $\pi' = [5, 4, 2, 1, 3]$ and $x_{\pi'} = (1, 0, 3, 4)$. Then $x_{\pi'} - x_\pi = (0, 0, 0, 1) = \mathbf{e}_\mathbf{5}^+$.

In contrast, if we have two consecutive numbers b and a in the original permutation, with $b > a$, then an adjacent transposition which switches b and a will result in an error $\mathbf{e}_\mathbf{b}^-$, which is a vector with -1 on the entry $x_\pi(b)$ and 0 elsewhere. Continuing the example, switch '5' and '2' in π, we have $\pi' = [4, 2, 5, 1, 3]$ and $x_{\pi'} = (1, 0, 3, 2)$. Then $x_{\pi'} - x_\pi = (0, 0, 0, -1) = \mathbf{e}_\mathbf{5}^-$.

Between two permutations, t adjacent transpositions together lead to an error vector $\mathbf{e}$, which is the summation of each error vector corresponding to each adjacent transposition. Let $\omega(\mathbf{e})$ be the summation of all the entries in $\mathbf{e}$, performed over the integers. Note that since there may be some offsets of the form $\mathbf{e}_\mathbf{b}^+$ and $\mathbf{e}_\mathbf{b}^-$, $\omega(\mathbf{e})$ will be an integer with absolute value no more than t.

The key tool is the following famous theorem of Bose and Chowla [2]:

Lemma 16 [2] *Let q be a power of a prime and $m = \frac{q^{t+1}-1}{q-1}$. There exist $q+1$ integers $d_1 = 0, d_2, \ldots, d_{q+1}$ in $\mathbb{Z}_m$ such that the sums*

$$d_{i_1} + d_{i_2} + \cdots + d_{i_t} \qquad (1 \le i_1 \le i_2 \le \cdots \le i_t \le q + 1)$$

are all distinct modulo m.

Set $q + 1 = n - 1$. We now deal with $A_K(n, 2t + 1)$. Color each permutation in S_n using colors $(c_1, c_2) \in \mathbb{Z}_{2t+1} \times \mathbb{Z}_m$.

Theorem 17 *Under the parameters given above, for any permutation* $\pi \in S_n$*, let* $c_1(\pi) \equiv I(\pi) \pmod{2t+1}$ *and let* $c_2(\pi) \equiv \sum_{i=1}^{n-1} d_i x_\pi(i+1) \pmod{m}$*. Then for any two permutations* π *and* σ *with* $d_K(\pi, \sigma) < 2t + 1$*, we have* $(c_1(\pi), c_2(\pi)) \neq (c_1(\sigma), c_2(\sigma))$*.*

Proof Let $\mathbf{e} = x_\pi - x_\sigma$ be the error vector between the inversion vectors of the two permutations. Since $d_K(\pi, \sigma) < 2t + 1$, $|\omega(\mathbf{e})| \le 2t$. If $|\omega(\mathbf{e})| \neq 0$, then clearly $c_1(\pi) \neq c_1(\sigma)$. Otherwise, $\omega(\mathbf{e}) = 0$, then the value of $c_2(\pi) - c_2(\sigma)$ modulo m is the difference of two parts of summations. Each summation is the sum of some s integers among $\{d_1, \ldots, d_{q+1}\}$, with $s \le t$. By the Bose-Chowla theorem, this difference is nonzero so $c_2(\pi) \neq c_2(\sigma)$. □

So the coloring is a proper coloring in the graph G_K. A remark is that the proof of Barg and Mazumdar [1] could be stated similarly in the framework above. Their coloring scheme aims at simultaneously dealing with all the possible error vectors. However, this simultaneousness also restricts the number of colors to be of order $t^2 m$ (see Proposition 10), which is larger than $(2t + 1)m$ in our approach. The trick in our framework, which deals with errors respectively according to whether $|\omega(\mathbf{e})|$ is zero or not, turns out to be useful. In summary, our coloring framework gives:

Theorem 18 *Let* $m = ((n-2)^{t+1} - 1)/(n-3)$*, where* $n - 2$ *is a prime power. Then* $A_K(n, 2t + 1) \ge \frac{n!}{(2t+1)m}$.

As for $A_K(n, 2t)$, by the theorem above and Lemma 9, we immediately have:

Theorem 19 *Let* $m = ((n-2)^t - 1)/(n-3)$*, where* $n-2$ *is a prime power. Then* $A_K(n, 2t) \ge \frac{n!}{2(2t-1)m}$.

We mention that there's still a slight chance of doing better. In our framework above, when dealing with errors with $|\omega(\mathbf{e})| \neq 0$, we calculate the inversion number of a permutation modulo $2t + 1$. Could we lower this number? We now state another Bose–Chowla theorem also appeared in [2]. Note that in the framework above, both of the two Bose–Chowla theorems could be applied, and actually they lead to similar results, with Lemma 16 performing slightly better. However, the following lemma will benefit our analysis later.

Lemma 20 [2] *Let* $q = p^n$ *be a prime power. Then we can find* q *nonzero integers (less than* q^t*)* $d_1 = 1, d_2, \ldots, d_q$ *such that the sums*

$$d_{i_1} + d_{i_2} + \cdots + d_{i_t} \qquad (1 \le i_1 \le i_2 \le \cdots \le i_t \le q)$$

are all distinct modulo $q^t - 1$.

The exact constructions of these integers are as follows. Let $\alpha_1 = 0, \alpha_2, \ldots, \alpha_q$ denote all the elements in $\mathbb{F}_{p^n}$. Let y be a primitive element of the extension field $\mathbb{F}_{p^{nt}}$. Let $y^{d_i} = y + \alpha_i$ for $i = 1, 2 \ldots, q$, where $d_i < p^{nt}$. Then $\{d_i\}_{1 \le i \le q}$ is the desired set of integers for carrying out our coloring scheme in Theorem 17. The choice of the primitive element y, or equivalently, the choice of the irreducible polynomial of degree t with coefficients from $\mathbb{F}_{p^n}$, uniquely determines $\{d_i\}_{1\le i\le q}$. We now expect more properties from the choice of the irreducible polynomial.

Take $A_K(n,5)$ as an example. Now we need an appropriate irreducible polynomial of degree 2 with coefficients from $\mathbb{F}_{p^n}$, denoted as $y^2 = ay+b, a, b \in \mathbb{F}_{p^n}$. We further demand that the set of integers $\{d_i\}_{1\le i\le q}$ satisfies: the sum of any three integers is nonzero modulo $p^{2n}-1$. That is, $(y+i)(y+j)(y+k) \neq 1$ for any $i, j, k \in \mathbb{F}_{p^n}$. It can be checked that this is equivalent to the following problem.

Problem: For any prime power p^n, find $a, b \in \mathbb{F}_{p^n}$ such that

- $y^2 = ay + b$ is an irreducible polynomial in $\mathbb{F}_{p^n}$, and
- the following system of equations,

$$\begin{cases} a^2+b+ai+aj+ak+ij+ik+jk=0 \\ ab+ib+jb+kb+ijk=1 \end{cases}$$

with i, j, k being indeterminate, has no solution in $\mathbb{F}^3_{p^n}$.

Via computer search, although the desired a and b do not exist for $\mathbb{F}_5$ and $\mathbb{F}_7$, yet they do exist for primes 11, 13, 17, 19, 23. We conjecture that it may be true that there are infinitely many prime powers for which the desired a and b exist.

Once a and b exist for a prime power p^n, then we could do a small adjustment for our coloring map. Now let $\widetilde{c}_1(\pi) \equiv I(\pi) \pmod 3$ instead of modulo 5. For any two permutations σ and τ with $d_K(\sigma,\pi) < 5$, the only possibility for $\widetilde{c}_1(\sigma) = \widetilde{c}_1(\pi)$ and $\omega(x_\pi - x_\sigma) \neq 0$ is that the error vector between their inversion vectors x_σ and x_π is a vector with exactly three entries being '1' and otherwise '0'. Then the difference of $c_2(\sigma)$ and $c_2(\pi)$ will be a summation of three integers out of $\{d_i\}_{1\le i\le q}$. But by the further demand of the properties of a and b we choose, this difference is ensured to be nonzero modulo $p^{2n}-1$. Thus it is guaranteed that $c_2(\sigma) \neq c_2(\pi)$. So in this manner, the constant gap between the lower bound and the sphere-packing upper bound could be a little bit smaller.

5 Sporadic results on $A_K(n, d)$

In this section we provide some other sporadic results concerning permutation codes under Kendall's τ-metric.

5.1 A generalization of the code-anticode method

First we take a look at Lemma 12. The code-anticode method used in [3] corresponds to finding a subset G' of vertices, satisfying $\alpha(G') = 1$, with $|G'|$ as large as possible. A natural generalization is to jump out of the restriction $\alpha(G') = 1$. That is, as Lemma 12 suggests, we want to search for a subset G' with $\alpha(G')/|G'|$ as small as possible. An illustrative example is the following precise determination of the value $A_K(5,3)$. In [3] it has been verified that $20 \le A_K(5,3) \le 23$. We now show that 20 is the exact value.

Theorem 21

$$A_K(5,3) = 20.$$

Proof Select $G' = \{[1,2,3,4,5], [1,2,3,5,4], [1,2,4,3,5], [1,2,4,5,3], [1,2,5,3,4], [1,2,5,4,3], [2,1,3,4,5], [2,1,3,5,4], [2,1,4,3,5], [2,1,4,5,3], [2,1,5,3,4], [2,1,5,4,3]\}$. It can be easily verified that $\alpha(G') = 2$. So we have $\frac{A_K(5,3)}{5!} \le \frac{\alpha(G')}{|G'|} = \frac{2}{12}$, which leads to $A_K(5,3) \le 20$ and thus fixes this value. □

Although this is only a simple case, yet the idea lying behind it may have potentials for other parameters, or even perhaps for analyzing upper bounds for other various codes.

5.2 Sporadic results by computer search

Some other sporadic results concerning small parameters $n = 5$ and $n = 6$ could be obtained by computer search, via some algorithms designed for searching maximal independent sets. We obtain some values better than those listed in the table in [3], by the program developed by Ashay Dharwadker [8]. These values are listed as follows and examples of their corresponding codewords are listed in the appendix of the full version of the paper [22]. Although lacking strictly mathematical analysis, the power of the program suggests that these may be the exact values.

Theorem 22 [22, Appendix]

$$\begin{aligned}&A_K(5,4) \geq 12,\ A_K(5,6) \geq 5,\\&A_K(6,3) \geq 101,\ A_K(6,4) \geq 64,\ A_K(6,5) \geq 25,\\&A_K(6,6) \geq 20,\ A_K(6,7) \geq 11,\ A_K(6,8) \geq 7.\end{aligned}$$

5.3 Counting pairs of inversions: a Plotkin-type bound

In this subsection we prove a Plotkin-type bound by counting pairs of inversions. Recall that we have the following expression for Kendall's τ-metric:

$$d_K(\sigma,\pi) = |\{(i,j) : \sigma^{-1}(i) < \sigma^{-1}(j) \wedge \pi^{-1}(i) > \pi^{-1}(j)\}|.$$

Theorem 23 *If $A_K(n, 2t) \geq M$, then*

$$2\binom{M}{2}t \leq \binom{n}{2}\left\lceil\frac{M}{2}\right\rceil\left\lfloor\frac{M}{2}\right\rfloor,$$

and if $A_K(n, 2t+1) \geq M$, then

$$\binom{\lceil\frac{M}{2}\rceil}{2}(2t+2) + \binom{\lfloor\frac{M}{2}\rfloor}{2}(2t+2) + \left\lceil\frac{M}{2}\right\rceil\left\lfloor\frac{M}{2}\right\rfloor(2t+1) \leq \binom{n}{2}\left\lceil\frac{M}{2}\right\rceil\left\lfloor\frac{M}{2}\right\rfloor.$$

Proof Suppose now we have an (n, d)-permutation code $\mathcal{C}$ under Kendall's τ-metric of size M. We now calculate the summation of all the pair-wise distances $\sum = \Sigma_{c_1,c_2\in\mathcal{C}} d_K(c_1, c_2)$. Firstly, for any pair of numbers $1 \leq i < j \leq n$, we could partition $\mathcal{C}$ into two parts, according to whether i precedes j or vice versa. Then from the expression for Kendall's τ-metric, we know that the pair (i, j) contributes one to the distance between two permutations from different parts. Thus, the pair (i, j) contributes at most $\lceil\frac{M}{2}\rceil\lfloor\frac{M}{2}\rfloor$ to $\sum$. So we have,

$$\sum \leq \binom{n}{2}\left\lceil\frac{M}{2}\right\rceil\left\lfloor\frac{M}{2}\right\rfloor.$$

On the other hand, $\sum \geq \binom{M}{2}d$. And especially, if the distance d is odd, since the Kendall's τ-distance between two permutations of the same parity is even, then $\sum \geq \binom{\lceil\frac{M}{2}\rceil}{2}(d+1) + \binom{\lfloor\frac{M}{2}\rfloor}{2}(d+1) + \lceil\frac{M}{2}\rceil\lfloor\frac{M}{2}\rfloor d$.

The theorem follows from a comparison of the upper bound and lower bound of $\sum$. □

Now we analyze when will the theorem above be useful. Using the first constraint as an example, when $d \leq \frac{1}{2}\binom{n}{2}$, the constraint naturally holds for any M and thus does not provide any useful bound on M. However, when $\frac{1}{2}\binom{n}{2} < d \leq \frac{2}{3}\binom{n}{2}$, this bound may turn out to be better than the sphere packing upper bound or Proposition 8. It is generally unrealistic to compare the Plotkin-type bound to the sphere-packing upper bound or Proposition 8 since the precise size of a Kendall's τ-ball or a double-ball is difficult to analyze. Below we list several cases for small parameters, as supporting evidences to show that Theorem 23 may work slightly better.

n	d	Sphere-packing bound	Theorem 23
6	9	7	4
7	13	8	4
7	11	14	12
8	17	11	4

n	d	Proposition 8	Theorem 23
7	12	11	8
8	18	9	4
8	16	14	8

6 Conclusions

Permutation codes under different metrics are interesting topics due to their various applications. The bounds of permutation codes can be analyzed via studying the independence numbers of the corresponding graphs. We use a coloring approach to analyze the independence numbers, which leads to some improvements on the lower bounds of permutation codes under Hamming metric and Kendall's τ-metric, respectively. Although this coloring approach is well-known, the tricky part is the coloring strategy case-by-case. Besides, we also derive some other sporadic results concerning the upper bound of permutation codes under Kendall's τ-metric.

Acknowledgements The authors express their gratitude to the anonymous reviewers for their detailed and constructive comments which are very helpful to the improvement of this paper. Research supported by the National Natural Science Foundation of China under Grant Nos. 11431003 and 61571310.

References

1. Barg A., Mazumdar A.: Codes in permutations and error correction for rank modulation. IEEE Trans. Inf. Theory **56**(7), 3158–3165 (2010).
2. Bose R.C., Chowla S.: Theorems in the additive theory of numbers. Comment. Math. Helv. **37**, 141–147 (1962/1963).
3. Buzaglo S., Etzion T.: Bounds on the size of permutation codes with the Kendall τ-metric. IEEE Trans. Inf. Theory **61**(6), 3241–3250 (2015).
4. Čebyšev P.L.: Mémoire sur les nombres premiers. Académie Impériale des Sciences, Saint Petersburg (1850).

5. Chu W., Colbourn C.J., Dukes P.: Constructions for permutation codes in powerline communications. Des. Codes Cryptogr. **32**(1–3), 51–64 (2004).
6. Colbourn C.J., Kløve T., Ling A.C.H.: Permutation arrays for powerline communication and mutually orthogonal Latin squares. IEEE Trans. Inf. Theory **50**(6), 1289–1291 (2004).
7. de la Torre D.R., Colbourn C.J., Ling A.C.H.: An application of permutation arrays to block ciphers. Congr. Numer. **145**, 5–7 (2000).
8. Dharwadker A.: The Independent Set Algorithm. Yoda, New Delhi (2006).
9. Farnoud F., Skachek V., Milenkovic O.: Error-correction in flash memories via codes in the Ulam metric. IEEE Trans. Inf. Theory **59**(5), 3003–3020 (2013).
10. Ferreira H.C., Vinck A.J.H.: Interference cancellation with permutation trellis codes. In: 2000 VTC- Fall VTS 52nd Vehicular Technology Conference, vol. 5, pp. 2401–2407 (2000).
11. Frankl P., Deza M.: On the maximum number of permutations with given maximal or minimal distance. J. Comb. Theory Ser. A **22**(3), 352–360 (1977).
12. Gao F., Yang Y., Ge G.: An improvement on the Gilbert-Varshamov bound for permutation codes. IEEE Trans. Inf. Theory **59**(5), 3059–3063 (2013).
13. Godsil C., Royle G.: Algebraic Graph Theory. Graduate Texts in Mathematics, vol. 207. Springer, New York (2001).
14. Jiang A., Mateescu R., Schwartz M., Bruck J.: Rank modulation for flash memories. IEEE Trans. Inf. Theory **55**(6), 2659–2673 (2009).
15. Jiang A., Schwartz M., Bruck J.: Correcting charge-constrained errors in the rank-modulation scheme. IEEE Trans. Inf. Theory **56**(5), 2112–2120 (2010).
16. Kløve T., Lin T.-T., Tsai S.-C., Tzeng W.-G.: Permutation arrays under the Chebyshev distance. IEEE Trans. Inf. Theory **56**(6), 2611–2617 (2010).
17. Mazumdar A., Barg A., Zémor G.: Constructions of rank modulation codes. IEEE Trans. Inf. Theory **59**(2), 1018–1029 (2013).
18. Pavlidou N., Vinck A.J.H., Yazdani J., Honary B.: Power line communications: state of the art and future trends. IEEE Commun. Mag. **41**(4), 34–40 (2003).
19. Tait M., Vardy A., Verstraete J.: Asymptotic improvement of the Gilbert-Varshamov bound on the size of permutation codes. arXiv preprint arXiv:1311.4925 (2013).
20. Tamo I., Schwartz M.: Correcting limited-magnitude errors in the rank-modulation scheme. IEEE Trans. Inf. Theory **56**(6), 2551–2560 (2010).
21. Vinck A.J.H.: Coded modulation for power line communications. AE Int. J. Electron. Commun. **54**, 45–49 (2011).
22. Wang X., Zhang Y., Yang Y., Ge G.: New bounds of permutation codes under hamming metric and kendall's τ-metric. arXiv preprint arXiv:1611.07188 (2016).