Designs, Codes and Cryptography (2019) 87:2625–2637
https://doi.org/10.1007/s10623-019-00641-w

New theoretical bounds and constructions of permutation codes under block permutation metric

Zixiang Xu[1] · Yiwei Zhang[2] · Gennian Ge[1]

Received: 12 November 2018 / Revised: 6 May 2019 / Accepted: 9 May 2019 / Published online: 17 May 2019

Abstract

Permutation codes under different metrics have been extensively studied due to their potentials in various applications. Generalized Cayley metric is introduced to correct generalized transposition errors, including previously studied metrics such as Kendall's τ-metric, Ulam metric and Cayley metric as special cases. Since the generalized Cayley distance between two permutations is not easily computable, Yang et al. introduced a related metric of the same order, named the block permutation metric. Given positive integers n and d, let $\mathcal{C}_B(n, d)$ denote the maximum size of a permutation code in S_n with minimum block permutation distance d. In this paper, we focus on the theoretical bounds of $\mathcal{C}_B(n, d)$ and the constructions of permutation codes under block permutation metric. Using a graph theoretic approach, we improve the Gilbert–Varshamov type bound by a factor of $\Omega(\log n)$, when d is fixed and n goes into infinity. We also propose a new encoding scheme based on binary constant weight codes. Moreover, an upper bound beating the sphere-packing type bound is given when d is relatively close to n.

Keywords Permutation codes · Block permutation metric · Gilbert–Varshamov bound · Sphere-packing bound · Independence number

Mathematics Subject Classification 94B25 · 94B65

Communicated by J. H. Koolen.

Y. Zhang: Supported in part by a Technion fellowship. G. Ge: Research supported by the National Natural Science Foundation of China under Grant Nos. 11431003 and 61571310, Beijing Scholars Program, Beijing Hundreds of Leading Talents Training Project of Science and Technology, and Beijing Municipal Natural Science Foundation.

✉ Gennian Ge
gnge@zju.edu.cn

Zixiang Xu
zxxu8023@qq.com

Yiwei Zhang
ywzhang@cs.technion.ac.il

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

[2] Department of Computer Science, Technion – Israel Institute of Technology, 32000 Haifa, Israel

1 Introduction

Let S_n be the symmetric group on n elements. A permutation code is a subset of S_n with some certain constraints. Permutation codes under several different metrics are widely used due to their various applications. Especially in recent years, permutation codes under Kendall's τ-metric, Ulam metric and Cayley metric have been extensively studied in clouding storage systems, genome resequencing and the rank modulation scheme of flash memories [3,4,6,8,10,12,16,18]. Under these metrics, codes are designed to correct transposition errors or translocation errors. In [5], Chee and Vu introduced the generalized Cayley metric which includes the metrics aforementioned as special cases. However, the generalized Cayley distance between two permutations is in general not easily computable and thus the construction of codes is difficult. In [17], Yang et al. introduced the block permutation metric which could be simply computed and is of the same order as the generalized Cayley metric. By the metric embedding method, the problem of constructing codes in the generalized Cayley metric is transformed into constructing codes in the block permutation metric. Several theoretical bounds (Gilbert–Varshamov type and sphere-packing type) and constructions of codes under block permutation metric are shown in [17].

In this paper we further consider permutation codes in S_n under the block permutation metric. We first establish a connection between permutation codes and independent sets in a corresponding graph and then study the bounds of the independence number of the graph. By this graph theoretic approach, we improve the Gilbert–Varshamov type bound asymptotically by a factor of $\Omega(\log n)$, when the minimum distance d is fixed while n goes into infinity. We also propose a new encoding scheme based on certain constructions of binary constant weight codes. Compared with the known constructions, we improve the size of codes by a factor of $\Theta(n^{2d-4})$. As for the upper bound, each permutation can be represented as a corresponding characteristic set and then we apply some methods from extremal set theory to obtain an upper bound of a new type, which beats the sphere-packing type bound when d is relatively close to n.

The rest of this paper is organized as follows. In Sect. 2, we review some basic backgrounds about block permutation metric. In Sect. 3, we introduce some relevant terminologies and results from extremal graph theory and then establish the correspondence between permutation codes and independent sets in some certain graph. The asymptotic improvement of the Gilbert–Varshamov type bound is presented in Sect. 4. Section 5 contains a new encoding scheme based on binary constant weight codes. The upper bound based on extremal set theory is presented in Sect. 6. We conclude in Sect. 7.

2 Block permutation metric

In this section, we give some definitions and notations for permutation codes under block permutation metric.

Let $[n]$ denote $\{1, 2, 3, \dots, n\}$. $\pi = (\pi(1), \pi(2), \dots, \pi(n))$ is a permutation over $[n]$, known as the vector notation of a permutation. The symbol $\circ$ denotes the composition of permutations. Specifically, for two permutations σ and τ, their composition, denoted by $\sigma \circ \tau$, is the permutation with $\sigma \circ \tau(i) = \sigma(\tau(i))$ 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 $|S_n| = n!$. The subsequence of σ from indices i to j is written as $\sigma[i : j] \triangleq (\sigma(i), \sigma(i + 1), \dots, \sigma(j))$.

Definition 2.1 A permutation $\pi \in S_n$ is called *minimal* if and only if no consecutive elements in π are also consecutive in the identity permutation $e = (1, 2, \ldots, n)$, i.e., for all $1 \leqslant i \leqslant n-1$, $\pi(i+1) \neq \pi(i) + 1$. Denote the set of all the minimal permutations in S_n as $\mathcal{D}_n$.

Definition 2.2 The block permutation distance $d_B(\pi_1, \pi_2)$ between two permutations $\pi_1, \pi_2 \in S_n$ is equal to d if

$$\pi_1 = (\psi_1, \psi_2, \ldots, \psi_{d+1}), \pi_2 = \left(\psi_{\sigma(1)}, \psi_{\sigma(2)}, \ldots, \psi_{\sigma(d+1)}\right),$$

where $\sigma \in \mathcal{D}_{d+1}$, $\psi_k = \pi_1 \left[i_{k-1} + 1 : i_k\right]$ for $0 = i_0 < i_1 < \cdots < i_d < i_{d+1} = n$ and $1 \leqslant k \leqslant d+1$.

The definition suggests that in order to turn π_1 into π_2, one way is to first divide π_1 into $d+1$ segments $\pi_1 = (\psi_1, \psi_2, \ldots, \psi_{d+1})$ and then perform a block level permutation of these segments according to a permutation $\sigma \in \mathcal{D}_{d+1}$. The constraint of σ being minimal indicates that $d_B(\pi_1, \pi_2) = d$ if and only if $d+1$ is the minimum number of segments that π_1 needs to be divided into for such an operation. This definition is somehow not intuitive enough and thus Yang et al. [17] found another way to characterize the block permutation distance explicitly by the *characteristic set* of a permutation.

Definition 2.3 The characteristic set $A(\pi)$ for any $\pi \in S_n$ is defined as set of all the consecutive pairs in π, i.e.,

$$A(\pi) \triangleq \{(\pi(i), \pi(i+1)) \mid 1 \leqslant i < n\}.$$

Note that the characteristic set of a permutation is equivalent to representing a permutation by a directed Hamiltonian path on n vertices. That is, the Hamiltonian path corresponding to π is the set of edges in $\{(x, y)|x, y \in [n], (x, y) \in A(\pi)\}$. The following idea will be frequently used throughout the paper. Given a subset of $A(\pi)$, the directed edges corresponding to the subset constitute a disjoint union of several directed paths (an isolated vertex v will be also regarded as a path starting and ending with v). Then π should be obtained by concatenating these directed paths into a directed Hamiltonian path.

Let $\mathcal{P}_n$ be the set $\{(i, j)| i \neq j, i \in [n], j \in [n]\}$. $|\mathcal{P}_n| = n(n-1)$. For each permutation $\pi \in S_n$, the corresponding characteristic set $A(\pi)$ is then a subset of $\mathcal{P}_n$ of cardinality $|A(\pi)| = n - 1$. The block permutation metric can be characterized by the characteristic set and then some basic properties of the metric can be derived. These are summarized in the following two lemmas proposed in [17].

Lemma 2.4 *For all* $\pi_1, \pi_2 \in S_n$,

$$d_B(\pi_1, \pi_2) = |A(\pi_1) \setminus A(\pi_2)|.$$

Lemma 2.5 *For all* $\pi_1, \pi_2, \pi_3 \in S_n$, *the block permutation distance* d_B *satisfies the following properties:*

1. (*Symmetry*) $d_B(\pi_1, \pi_2) = d_B(\pi_2, \pi_1)$.
2. (*Left-invariance*) $d_B(\pi_3 \circ \pi_1, \pi_3 \circ \pi_2) = d_B(\pi_1, \pi_2)$.
3. (*Triangle Inequality*) $d_B(\pi_1, \pi_3) \leqslant d_B(\pi_1, \pi_2) + d_B(\pi_2, \pi_3)$.

The following example shows how to compute the block permutation distance between two permutations following the terminologies above.

Example 2.6 Let $\pi_1 = (4, 8, 3, 2, 6, 7, 5, 1, 9)$, $\pi_2 = (6, 7, 8, 3, 2, 5, 1, 9, 4)$. Their characteristic sets are

$$A(\pi_1) = \{(4, 8), (8, 3), (3, 2), (2, 6), (6, 7), (7, 5), (5, 1), (1, 9)\},$$
$$A(\pi_2) = \{(6, 7), (7, 8), (8, 3), (3, 2), (2, 5), (5, 1), (1, 9), (9, 4)\},$$

and thus we have

$$d_B(\pi_1, \pi_2) = |A(\pi_1) \setminus A(\pi_2)| = |\{(4, 8), (2, 6), (7, 5)\}| = 3.$$

On the other hand, to compute $d_B(\pi_1, \pi_2)$ by Definition 2.2, we should find ψ_i, $1 \leqslant i \leqslant 4$ and $\sigma \in \mathcal{D}_4$ as follows:

$$\psi_1 = (4), \psi_2 = (8, 3, 2), \psi_3 = (6, 7), \psi_4 = (5, 1, 9), \sigma = (3, 2, 4, 1).$$

Then we have

$$\begin{aligned}\pi_1 &= (\psi_1, \psi_2, \psi_3, \psi_4),\\ \pi_2 &= (\psi_{\sigma(1)}, \psi_{\sigma(2)}, \psi_{\sigma(3)}, \psi_{\sigma(4)}),\end{aligned}$$

and thus $d_B(\pi_1, \pi_2) = 3$.

Note that it is usually not easy to find such ψ_i and σ to compute the block permutation distance between two permutations, while finding the difference between two characteristic sets is relatively easier. Next we introduce the permutation code under block permutation metric.

Definition 2.7 Given positive integers n and d, $\mathcal{C} \subseteq S_n$ is called an (n, d)-permutation code under block permutation metric, if $d_B(\sigma, \pi) \geqslant d$ for any two distinct permutations $\sigma, \pi \in \mathcal{C}$. Let $\mathcal{C}_B(n, d)$ denote the maximum size of an (n, d)-permutation code $\mathcal{C}$.

The best known upper bound and lower bound of $\mathcal{C}_B(n, d)$ are proposed in [17], which are the so-called sphere-packing type bound and Gilbert–Varshamov type bound. Both bounds are derived from the estimation on the size of a block permutation ball.

Definition 2.8 For given integers n, t and a given center point $\pi \in S_n$, the t-block permutation ball centered at π is defined as the set of all permutations $\sigma \in S_n$, $d_B(\pi, \sigma) \leqslant t$. We denote the t-block permutation ball centered at π as $b_B(n, t, \pi)$.

Note that by the left-invariance property of d_B, the size of $b_B(n, t, \pi)$ is independent of the center π and thus we can denote the size of the ball as $|b_B(n, t)|$.

Lemma 2.9 [17] *For given integers n and t, $t \leqslant n - \sqrt{n} - 1$, denote the size of a t-block permutation ball as $|b_B(n, t)|$, then we have*

$$\prod_{i=1}^{t}(n - i) \leqslant |b_B(n, t)| \leqslant \prod_{i=0}^{t}(n - i).$$

Lemma 2.10 [17] *For given integers n and t, let $d = 2t + 1$, then we can bound $\mathcal{C}_B(n, d)$ as*

$$\frac{n!}{|b_B(n, 2t)|} \leqslant \mathcal{C}_B(n, d) \leqslant \frac{n!}{|b_B(n, t)|}.$$

In [17] several constructions of (n, d)-permutation codes with $d = 2t+1$ were presented, including a code of size $\frac{n!}{q^{2d-3}}$, where $n(n-1) \leqslant q \leqslant 2n(n-1)$ is a prime number. Moreover [17] contains some explicit systematic constructions and decoding algorithms.

3 Graph models

We use the standard terminologies and notations in graph theory. A graph G consists of a set of vertices $V(G)$ and a set of edges $E(G)$. Each edge is a pair of vertices. Two vertices u and v are called adjacent if there is an edge $\{u, v\} \in E(G)$. We say that H is a subgraph of G if $V(H) \subset V(G)$ and $E(H) \subset E(G)$. Furthermore if H contains all edges of G joining two vertices in $V(H)$, then H is said to be the subgraph of G induced by $V(H)$. The neighborhood of a vertex v is the set of all vertices adjacent to v, denoted by $\Gamma(v)$. The neighborhood graph of v is the subgraph induced by $\Gamma(v)$. The size of $|\Gamma(v)|$ is called the degree of the vertex v. Let $\Delta(G)$ denote the maximum vertex degree. An independent set in a graph is a set of vertices where every pair is nonadjacent. The size of the largest independent set in G is called the independence number, denoted as $\alpha(G)$.

In this section we introduce a natural relationship between codes and independent sets of a corresponding graph. Take the set of all the candidate codewords as the vertex set of a graph (say for example, the vertex set could be $\{0, 1\}^n$ when we consider binary codes of length n, or it could be S_n when we consider permutation codes). Two candidate codewords with distance less than d are connected via an edge. Then we can take any independent set of this graph as a code since every two distinct codewords have distance no less than d. Thus we have a correspondence between an independent set and a code with minimum distance d. The problem of estimating the maximal size of a code turns into analyzing the independence number of the corresponding graph. This well-known approach has already been shown to be powerful in studying several kinds of codes. Take the permutation code under Hamming metric as an example. Gao et al. [7] improved the Gilbert–Varshamov bound by a factor of $\Omega(\log n)$, when the minimum distance d is fixed and n goes into infinity. Tail et al. [14] improved the Gilbert–Varshamov bound by a factor of $\Omega(n)$, when $\frac{d}{n}$ is fixed and n goes into infinity. Recently, Wang et al. [16] used a coloring approach to analyze the independence number and improved the Gilbert–Varshamov bound by a factor of $\Omega(n)$ when the minimum distance d is fixed and n goes into infinity.

Here we introduce some results about the independence number of locally sparse graphs. A graph is called triangle-free if and only if the neighborhood of every vertex is an independent set. Ajtai et al. [1] showed the relationship between triangle-free property and independence number in the following lemma.

Lemma 3.1 *Let G be a graph with maximum degree Δ. If G is triangle-free, then we have*

$$\alpha(G) \geqslant \frac{|V(G)|}{8\Delta} \log_2 \Delta.$$

In [2] the lemma above was extended from triangle-free graphs into graphs with relatively few triangles.

Lemma 3.2 *Let G be a graph with maximum degree Δ. If G has at most T triangles, then we have*

$$\alpha(G) \geqslant \frac{|V(G)|}{10\Delta}\left(\log_2 \Delta - \frac{1}{2}\log_2\left(\frac{T}{|V(G)|}\right)\right).$$

Note that a graph has relatively few triangles when the neighborhoods of its vertices are relatively sparse. Jiang and Vardy [11] generalized the results above for locally sparse graphs as follows.

Lemma 3.3 *Let G be a graph with maximum degree Δ. Suppose for any vertex $v \in V(G)$, the subgraph induced by the neighborhood of v has at most P edges, then we have*

$$\alpha(G) \geqslant \frac{|V(G)|}{10\Delta}\left(\log_2 \Delta - \frac{1}{2}\log_2\left(\frac{P}{3}\right)\right).$$

4 An asymptotic improvement of the lower bound

Before presenting the main results of this section, it should be noted that $\mathcal{C}_B(n, d)$ can be determined under some special cases.

Theorem 4.1 $\mathcal{C}_B(n, 1) = n!$. $\mathcal{C}_B(n, 2) = (n-1)!$. $\mathcal{C}_B(n, n-1) \leqslant n$ *and equality holds if* n *is not* 3 *or* 5.

Proof 1. Trivially take all the permutations in S_n and we have $\mathcal{C}_B(n, 1) = n!$.

2. It is easy to check that for any two permutations π and σ, $d_B(\pi, \sigma) = 1$ if and only if σ is a cyclic shift of π. That is, if $\pi = (\pi(1), \ldots, \pi(n))$ and $d_B(\pi, \sigma) = 1$, then σ is of the form $\sigma = (\pi(t), \ldots, \pi(n), \pi(1), \ldots, \pi(t-1))$ for some $2 \leqslant t \leqslant n$. Under the operation of cyclic shifting, S_n is divided into $(n-1)!$ equivalent classes where each class is known as a circular permutation. By picking an arbitrary permutation from each equivalent class we obtain an $(n, 2)$-permutation code of cardinality $(n-1)!$.
3. For any two distinct permutations π and σ in an $(n, n-1)$-permutation code, their characteristic sets are disjoint according to Lemma 2.4. Since each characteristic set is a subset of $\mathcal{P}_n$ of cardinality $n-1$, $|\mathcal{P}_n| = n(n-1)$, then the number of codewords is at most n.

   (a) Suppose n is even, $n = 2p$. Define $a_{2i-1} = 2i-1$ for $1 \leqslant i \leqslant p$ and $a_{2i} = 2p-2i$ for $1 \leqslant i \leqslant p-1$, i.e., $(a_1, a_2, \ldots, a_{n-1}) = (1, 2p-2, 3, 2p-4, \ldots, p, \ldots, 4, 2p-3, 2, 2p-1)$. For every $1 \leqslant i \leqslant n$, let the i-th codeword be $(i, i+a_1, i+a_1+a_2, \ldots, i+\sum_{j=1}^{k} a_j, \ldots, i+\sum_{j=1}^{n-1} a_j)$, where each entry is taken modulo n (and note that we use 'n' instead of '0' for some entry). It is routine to check that $\sum_{j=1}^{2i} a_j \equiv -i \pmod{n}$, $1 \leqslant i \leqslant p-1$ and $\sum_{j=1}^{2i-1} a_j \equiv i \pmod{n}$, $1 \leqslant i \leqslant p$. Therefore $\sum_{j=1}^{k} a_j$ are distinct modulo n for $1 \leqslant k \leqslant n$. So these n codewords defined above are indeed codewords in S_n. For every pair (c, d) with $d - c \equiv a_k \pmod{n}$, it appears exactly once, in the i-th codeword with $c \equiv i + \sum_{j=1}^{k-1} a_j$ and $d \equiv i + \sum_{j=1}^{k} a_j$.

   (b) Suppose n is odd. To construct an $(n, n-1)$-permutation code of size n, consider the complete directed graph on $n+1$ vertices $[n] \cup \{\infty\}$. For each π, its characteristic set $A(\pi)$ also represents the directed Hamiltonian path on n vertices. Further add the edges $(\infty, \pi(1))$ and $(\pi(n), \infty)$ into $A(\pi)$. Then each permutation corresponds to a directed Hamiltonian cycle on $[n] \cup \{\infty\}$. Thus an $(n, n-1)$-permutation code of size n is equivalent to a Hamiltonian decomposition in the complete directed graph on $[n] \cup \{\infty\}$. Hamiltonian decomposition is a well studied topic, for example in [15]. It has been shown that for odd integers $n \geqslant 7$, the edges of the complete directed graph on $n+1$ vertices can be partitioned into n directed Hamiltonian cycles.

Therefore, $\mathcal{C}_B(n, n-1) \leqslant n$ and equality holds if n is even or $n \geqslant 7$ is odd. Moreover, it can be easily checked that $\mathcal{C}_B(3, 2) = 2$ and $\mathcal{C}_B(5, 4) = 4$.

□

Remark 4.2 When $n+1$ is prime, there is another construction of an $(n, n-1)$-permutation code of size n different from the one in the proof above. Consider the code $\{(i, 2i, \dots, (n-1)i, ni) : 1 \leqslant i \leqslant n\}$, with each entry modulo $(n+1)$. It is straightforward to check that every pair of (a, b) appears exactly once (in the ith codeword, $i \equiv (b-a) \pmod{n+1}$).

After solving these special cases, the rest of this section is devoted to improving the asymptotic lower bound of $\mathcal{C}_B(n, d)$ with $d \geqslant 3$ being a fixed constant, while n approaches infinity. The idea is to analyze the independence number of the corresponding block permutation graph, defined as follows.

Definition 4.3 For given positive integers n and $d \geqslant 3$, the (n, d)-block permutation graph $\mathcal{G}_{n,d}$ is the graph with vertex set S_n and edge set $\{(\pi, \sigma) : \pi \neq \sigma, d_B(\pi, \sigma) < d\}$.

The codewords of an (n, d)-permutation code under block permutation metric are vertices of an independent set in $\mathcal{G}_{n,d}$. Conversely, any independent set in $\mathcal{G}_{n,d}$ is an (n, d)-permutation code. To get a lower bound of $\mathcal{C}_B(n, d)$ via the graph theoretic approach using Lemma 3.3, we need to calculate some parameters of the graph $\mathcal{G}_{n,d}$.

Let $\mathcal{H}_{n,d}$ be the subgraph induced by the neighborhood of the identity permutation $(1, 2, 3, \dots, n)$, and let $R(n, k)$ be the set of all permutations in S_n which are exactly at distance k from the identity, i.e.,

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

Then the induced subgraph $\mathcal{H}_{n,d}$ has the vertex set $V(\mathcal{H}_{n,d}) = \bigcup_{k=1}^{d-1} R(n, k)$. The size of $R(n, k)$ is a well-studied topic in [13].

Lemma 4.4 [13] *For all integers* $1 \leqslant k \leqslant n-1$,

$$|R(n, k)| = k!\binom{n-1}{k} \sum_{i=0}^{k} (-1)^{k-i} \frac{(i+1)}{(k-i)!}.$$

Since $\binom{n}{a} = \Theta(n^a)$ when a is a fixed positive integer and n goes to infinity, then asymptotically $|R(n, k)| = \Theta(n^k)$, $1 \leqslant k \leqslant d-1$ and thus $|b_B(n, d-1)| = \sum_{k=0}^{d-1} |R(n, k)| = \Theta(n^{d-1})$, when d is fixed and n goes to infinity.

To apply Lemma 3.3, we already have $V(\mathcal{G}_{n,d}) = n!$ and $\mathcal{G}_{n,d}$ is a regular graph of degree $\Delta = b_B(n, d-1) - 1 = \Theta(n^{d-1})$. The remaining parameter to compute is $P(n, d)$, the number of edges in the induced subgraph $\mathcal{H}_{n,d}$.

Lemma 4.5 *For a fixed positive integer* $d \geqslant 3$, $P(n, d) = O(n^{2d-3})$ *when* n *goes to infinity.*

Proof The number of vertices in $R(n, k)$ is asymptotically $\Theta(n^k)$. Thus the number of edges connecting some $\pi \in R(n, k_1)$ and some $\sigma \in R(n, k_2)$ is $\Theta(n^{k_1+k_2}) = O(n^{2d-3})$ as long as $k_1 + k_2 \leqslant 2d-3$. Therefore, to prove the lemma we only need to focus on bounding the number of edges connecting some $\pi \in R(n, d-1)$ and some $\sigma \in R(n, d-1)$.

Consider the characteristic sets of such π and σ. $|A(id)\setminus A(\pi)| = |A(id)\setminus A(\sigma)| = d-1$. Let $x(\pi, \sigma)$ be the number of consecutive pairs in $A(id)$ contained in neither $A(\pi)$ nor $A(\sigma)$, i.e.,

$$x(\pi, \sigma) = |\big(A(id) \setminus A(\pi)\big) \cap \big(A(id) \setminus A(\sigma)\big)|.$$

For a fixed $\pi \in R(n, d-1)$, the number of permutations $\sigma \in R(n, d-1)$ with $x(\pi, \sigma) = x$ is at most $\Theta\big(\binom{d-1}{x}\binom{n-d}{d-1-x}\big) = \Theta(n^{d-1-x})$. This is because $A(id) \setminus A(\sigma)$ contains exactly x pairs out of the $d-1$ pairs in $A(id) \setminus A(\pi)$ and $d-1-x$ pairs out of the $n-d$ pairs in $A(id) \cap A(\pi)$ and every proper choice of $A(id) \setminus A(\sigma)$ only induces a constant number of permutations σ. Recall that $|R(n, d-1)| = \Theta(n^{d-1})$ and then the number of edges connecting $\pi, \sigma \in R(n, d-1)$ with $1 \leqslant x(\pi, \sigma) \leqslant d-1$ is at most $\Theta(n^{2d-3})$. Therefore, to prove the lemma we only need to focus on bounding the number of edges connecting some $\pi \in R(n, d-1)$ and some $\sigma \in R(n, d-1)$, with $x(\pi, \sigma) = 0$. Now we claim that in fact there are no such edges.

Since $x(\pi, \sigma) = 0$, then $\big(A(id) \setminus A(\sigma)\big) \subset \big(A(\pi) \setminus A(\sigma)\big)$ and thus $d_B(\pi, \sigma) \geqslant d-1$. If π and σ are connected, then it must hold that $d_B(\pi, \sigma) = d-1$ and

$$A(id) \setminus A(\sigma) \;=\; A(\pi) \setminus A(\sigma)$$

and simultaneously

$$A(id) \setminus A(\pi) \;=\; A(\sigma) \setminus A(\pi).$$

Up until now, based on these two formulas, we can observe that π, σ, and the identity permutation induce three different Hamiltonian paths and no arc is involved in exactly one path (for example, if an arc only appears in $A(\pi)$, then the constraint $A(id) \setminus A(\sigma) = A(\pi) \setminus A(\sigma)$ is violated). The remaining task is then to show that such three different Hamiltonian paths cannot exist.

Now consider the $n-d$ pairs in $A(\pi) \cap A(\sigma)$. In the graph with vertex $[n]$, label all the directed edges (x, y) where $(x, y) \in A(\pi) \cap A(\sigma)$ and call this graph $\mathcal{G}$. The union of $A(\pi) \cap A(\sigma)$ and $A(id) \setminus A(\sigma)$ is $A(\pi)$, the directed Hamiltonian path corresponding to π. Therefore $\mathcal{G}$ is a union of d non-intersecting directed paths (there may exist isolated vertices and each isolated vertex is also considered as a directed path), where the jth path is denoted as $P_j = (x_j \to \cdots \to y_j)$, indicating that it starts with x_j and ends with y_j, $1 \leqslant j \leqslant d$. The directed Hamiltonian path corresponding to π is then a concatenation of these paths and without loss of generality it can be written as $P_1 \to P_2 \to \cdots \to P_d$. Since the edges connecting the P_j's arise from $A(id) \setminus A(\sigma)$, then it implies that $x_{j+1} = y_j + 1$ for $1 \leqslant j \leqslant d-1$.

Now since the directed Hamiltonian path corresponding to σ is also formed by using the $d-1$ edges in $A(id) \setminus A(\pi)$ to connect the P_j's, then there are only two cases. The first case is when $x_1 \neq y_d + 1$, then there is only a unique way to connect the P_j's via edges corresponding to consecutive pairs, i.e., $\sigma = \pi$. The other case is when $x_1 = y_d + 1$ and the directed Hamiltonian path corresponding to σ will be of the form $P_t \to P_{t+1} \to \cdots \to P_d \to P_1 \to \cdots \to P_{t-1}$. However, since $d \geqslant 3$, then σ and π will share $d-2$ edges $\{(y_j, x_{j+1}) | j \neq t-1, 1 \leqslant j \leqslant d-1\}$, which contradicts to $x(\pi, \sigma) = 0$.

Therefore, the last kind of edges we focus on do not exist at all and the total number of edges in the graph $\mathcal{H}_{n,d}$ is $P(n, d) = O(n^{2d-3})$. □

Now we are ready to apply Lemma 3.3 to obtain the new lower bound of $\mathcal{C}_B(n, d)$.

Theorem 4.6 *When d is fixed, $d \geqslant 3$ and n goes into infinity, there exists an (n, d)-permutation code under block permutation metric with size*

$$\mathcal{C}_B(n,d) = \alpha(\mathcal{G}_{n,d}) \geqslant \frac{n!}{10\Delta}\left(\log_2 \Delta - \frac{1}{2}\log_2\left(\frac{P(n,d)}{3}\right)\right) = \Omega\left(\frac{n!\log n}{n^{d-1}}\right).$$

Particularly, it improves the Gilbert–Varshamov bound by a factor of $\Omega(\log(n))$.

Proof Using our graph notations, the Gilbert–Varshamov bound is

$$A_{GV}(n,d) := \frac{n!}{1+\Delta(n,d)} = \Theta\left(\frac{n!}{n^{d-1}}\right).$$

By Lemmas 3.3 and 4.5, we have

$$\frac{\alpha(\mathcal{G}_{n,d})}{A_{GV}(n,d)} \geqslant \frac{\frac{n!}{10\Delta(n,d)}\left(\log_2 \Delta(n,d) - \frac{1}{2}\log_2\left(\frac{P(n,d)}{3}\right)\right)}{\frac{n!}{1+\Delta(n,d)}}$$
$$\geqslant \frac{1}{10}\log_2\left(\frac{\Delta(n,d)}{\sqrt{\frac{P(n,d)}{3}}}\right) \geqslant \frac{1}{10}\log_2\left(\frac{c_b n^{d-1}}{c_s n^{d-\frac{3}{2}}}\right) = c\log(n),$$

where c_b, c_s and c are constants independent of n.

Hence we have

$$\frac{\alpha(\mathcal{G}_{n,d})}{A_{GV}(n,d)} = \Omega(\log(n)).$$

□

5 Construction

In this section, we propose a new construction of permutation codes under block permutation metric. The main idea arises from constructing constant weight binary codes under Hamming metric [9].

Recall that $\mathcal{P}_n = \{(x,y) : x \neq y, x, y \in [n]\}$ and $|\mathcal{P}_n| = n(n-1)$. Suppose $q \geqslant n(n-1)/2$ is a prime number. From *Bertrand's postulate*, there is always such a q, $n(n-1)/2 \leqslant q \leqslant n(n-1)$.

Let $\mathcal{V} : \mathcal{P} \to \mathbb{F}_q$ be a map from $\mathcal{P}$ to the finite field $\mathbb{F}_q$ such that for distinct pairs (x, y) and (x', y'), $\mathcal{V}(x,y) = \mathcal{V}(x',y')$ if and only if $x' = y$ and $y' = x$. The range of $\mathcal{V}$ has size $n(n-1)/2$ and can be satisfied since we set $q \geqslant n(n-1)/2$.

Then for any permutation $\pi \in S_n$, $\mathcal{V}$ maps its characteristic set $A(\pi) = \{(\pi(i), \pi(i+1)) \mid 1 \leqslant i < n\}$ into $\{\mathcal{V}((\pi(i), \pi(i+1)) \mid 1 \leqslant i < n\}$, which is a subset of $\mathbb{F}_q$ of cardinality $n-1$. Denote these $n-1$ elements as $\gamma_1, \gamma_2, \ldots, \gamma_{n-1}$.

We then define a map F from S_n to $\mathbb{F}_q^{d-1}$ as follows:

$$F(\pi) = (F_1(\pi), F_2(\pi), ..., F_{d-1}(\pi)),$$

where

$$F_1(\pi) = \sum_{1 \leqslant i \leqslant n-1} \gamma_i,$$

$$F_2(\pi) = \sum_{1 \leqslant i < j \leqslant n-1} \gamma_i \gamma_j,$$

$$F_3(\pi) = \sum_{1 \leqslant i < j < k \leqslant n-1} \gamma_i \gamma_j \gamma_k,$$

$$\ldots$$

Theorem 5.1 *For any two distinct permutations $\pi, \sigma \in S_n$, if $F(\pi) = F(\sigma)$, then $d_B(\pi, \sigma) \geqslant d$.*

Proof Suppose on the contrary that there exist two distinct permutations $\pi, \sigma \in S_n$ such that $F(\pi) = F(\sigma)$ and $d_B(\pi, \sigma) = \delta < d$. Recall that $d_B(\pi, \sigma) = |A(\pi) \setminus A(\sigma)| = |A(\sigma) \setminus A(\pi)|$. Therefore $\mathcal{V}$ maps the set $A(\pi) \setminus A(\sigma)$ into a subset $\{\alpha_1, \alpha_2, \ldots, \alpha_\delta\}$ and similarly $\mathcal{V}$ maps the set $A(\sigma) \setminus A(\pi)$ into a subset $\{\beta_1, \beta_2, \ldots, \beta_\delta\}$.

The condition $F(\pi) = F(\sigma)$ will infer the following equations.

$$\zeta_1 = \sum_{1 \leqslant i \leqslant \delta} \alpha_i = \sum_{1 \leqslant i \leqslant \delta} \beta_i,$$

$$\zeta_2 = \sum_{1 \leqslant i < j \leqslant \delta} \alpha_i \alpha_j = \sum_{1 \leqslant i < j \leqslant \delta} \beta_i \beta_j,$$

$$\ldots$$

$$\zeta_{d-1} = \sum_{i_1 < \ldots < i_{d-1}} \alpha_{i_1} \ldots \alpha_{i_{d-1}} = \sum_{i_1 < \ldots < i_{d-1}} \beta_{i_1} \ldots \beta_{i_{d-1}}.$$

Consider the polynomial $x^\delta - \zeta_1 x^{\delta-1} + \zeta_2 x^{\delta-2} - \cdots + (-1)^{\delta+1} \zeta_\delta = \prod_{1 \leqslant i \leqslant \delta}(x - \alpha_i) = \prod_{1 \leqslant i \leqslant \delta}(x - \beta_i)$. Then $\{\alpha_1, \alpha_2, \ldots, \alpha_\delta\}$ and $\{\beta_1, \beta_2, \ldots, \beta_\delta\}$ are both the zeros of this polynomial and thus these two sets are identical.

Consider the complete directed graph with vertex set $[n]$ where each permutation corresponds to a directed Hamiltonian path indicated by its characteristic set. Now the path indicating π and the path indicating σ share $n - 1 - \delta$ directed edges in $A(\pi) \cap A(\sigma)$. Due to the property of the map $\mathcal{V}$, the set $\mathcal{E}$ of edges (without considering directions at this moment) corresponding to the pairs $\{\alpha_1, \alpha_2, \ldots, \alpha_\delta\} = \{\beta_1, \beta_2, \ldots, \beta_\delta\}$ are uniquely determined. With the given directions on the edges $A(\pi) \cap A(\sigma)$, there is a unique way to choose the directions for the edges in $\mathcal{E}$ to obtain a Hamiltonian path. Therefore π should be the same as σ, a contradiction. □

Therefore, we can construct (n, d)-permutation codes under block permutation metric as follows.

Theorem 5.2 *For every $\mathbf{f} \in \mathbb{F}_q^{d-1}$, $C_{\mathbf{f}}(n, d) = \{\pi | \pi \in S_n, F(\pi) = \mathbf{f}\}$ is an (n, d)-permutation code under block permutation metric.*

Consider all the vectors $\mathbf{f} \in \mathbb{F}_q^{d-1}$ and then $\{C_{\mathbf{f}}(n, d) : \mathbf{f} \in \mathbb{F}_q^{d-1}\}$ is a partition of S_n, where each component $C_{\mathbf{f}}(n, d)$ is a permutation code under block permutation metric. Suppose $C_{\mathbf{f}_{\max}}(n, d)$ is the one with maximal size, then by pigeonhole principle, we obtain that $|C_{\mathbf{f}_{\max}}(n, d)| \geqslant \frac{n!}{|\mathbb{F}_q^{d-1}|} = \frac{n!}{q^{d-1}} = \Theta(\frac{n!}{n^{2d-2}})$.

In [17], Yang et al. constructed a permutation code of size $\frac{n!}{q^{2d-3}}=\Theta(\frac{n!}{n^{4d-6}})$, where q is a prime number such that $n(n-1)\leqslant q\leqslant 2n(n-1)$. So our construction improves the size of permutation codes by a factor of $\Theta(n^{2d-4})$.

6 An upper bound

In this section, we obtain a new upper bound by means of analyzing the characteristic sets of the codewords. Recall that for each permutation $\pi\in S_n$, its characteristic set $A(\pi)=\{(\pi(i),\pi(i+1))|1\leqslant i<n\}$ is a subset of $\mathcal{P}_n$ of cardinality $|A(\pi)|=n-1$. Denote $I(\pi_1,\pi_2)=|A(\pi_1)\cap A(\pi_2)|$, then we have

Lemma 6.1 *For any $\pi_1,\pi_2\in S_n$, $d_B(\pi_1,\pi_2)\geqslant d$ if and only if $I(\pi_1,\pi_2)\leqslant n-d-1$.*

Given an (n,d)-permutation code $\mathcal{C}$, let $\mathcal{F}$ be the collection of all the characteristic sets $A(\pi)$ of the codewords, i.e., $\mathcal{F}=\{A(\pi)|\pi\in\mathcal{C}\}$. We translate the problem of analyzing the bound of codes into the following extremal set theory problem: find the maximal size of a family $\mathcal{F}$ of $(n-1)$-subsets of $\mathcal{P}_n$ satisfying that the intersection of each pair of subsets is at most $n-d-1$. Then we can obtain an upper bound of a new type as follows.

Theorem 6.2 *For given integers n and d,*

$$|\mathcal{F}|\leqslant\frac{\binom{n}{d}\binom{n}{d}(n-d)!}{\binom{n-1}{n-d}}.$$

Proof Let $T(n,d)$ be the family of all possible $(n-d)$-subsets of some $A(\pi)$, $\pi\in S_n$. Each $A(\pi)\in\mathcal{F}$ contains $\binom{n-1}{n-d}$ such subsets. By Lemma 6.1, any $(n-d)$-subset in $T(n,d)$ is contained in the characteristic set of at most one codeword. Therefore $|\mathcal{F}|\binom{n-1}{n-d}\leqslant|T(n,d)|$.

The remaining problem is to estimate $|T(n,d)|$. For each set $A\in T(n,d)$, consider the $n\times n$ matrix $M=(m_{i,j})$ where

$$m_{i,j}=\begin{cases}1, & \text{if pair } (i,j)\in A,\\ 0, & \text{otherwise.}\end{cases}$$

Since A is an $(n-d)$-subset of some $A(\pi)$, $\pi\in S_n$, then the matrix should contain exactly $n-d$ entries of '1' and the weight of each column and row is at most 1. Then the number of distinct A is upper bounded by the number of ways to select $n-d$ rows and $n-d$ columns and construct a permutation matrix from the chosen sub-matrix. Hence $T(n,d)\leqslant\binom{n}{n-d}\binom{n}{n-d}(n-d)!$. Therefore we have $|\mathcal{F}|\leqslant\frac{\binom{n}{d}\binom{n}{d}(n-d)!}{\binom{n-1}{n-d}}$. □

By Lemmas 2.9 and 2.10, if $t\leqslant n-\sqrt{n}-1$, denote the sphere-packing bound as $A_{SP}(n,2t+1)$, which falls in the range

$$\frac{n!}{\prod\limits_{i=0}^{t}(n-i)}\leqslant A_{SP}(n,2t+1)\leqslant\frac{n!}{\prod\limits_{i=1}^{t}(n-i)}.$$

Denote our new type upper bound $\frac{\binom{n}{d}\binom{n}{d}(n-d)!}{\binom{n-1}{n-d}}$ as $A_{new}(n,d)$.

Corollary 6.3 *Given n and $d=2t+1$, if $t\leqslant n-\sqrt{n}-1$, $n\cdot\prod\limits_{i=0}^{t}(n-i)\leqslant d\cdot d!$ and $d\leqslant n-1$, then $A_{new}(n,d)\leqslant A_{SP}(n,d)$.*

Table 1 A comparison of new bound and sphere-packing bound with some small parameters

n	d	Sphere-packing bound	Theorem 6.2	n	d	Sphere-packing bound	Theorem 6.2
13	9	$\geqslant$ 40320	**24787**	18	11	$\geqslant$ 479001600	**262461363**
15	11	$\geqslant$ 362880	**44672**	18	13	$\geqslant$ 39916800	**1423607**
16	11	$\geqslant$ 3628800	**762415**	19	11	$\geqslant$ 6227020800	**5263805324**
17	11	$\geqslant$ 39916800	**13771113**	19	13	$\geqslant$ 479001600	**28551213**
17	13	$\geqslant$ 3628800	**74696**	20	13	$\geqslant$ 6227020800	**601078154**

Better results are highlighted in bold

In Table 1 we list several cases for small parameters as supporting evidences to show that the new bound in Theorem 6.2 works better than sphere-packing bound when d is relatively close to n. Note that the values of sphere-packing bound in this table say that the size of codes is upper bounded by some value x, where x is not less than the values shown in the table. (For example, the size of a (13,9)-code is upper bounded by x, where $x \geqslant 40320$. It doesn't necessarily suggest that the size of a (13,9)-code is upper bounded by 40320. Our new result indicates that the size of a (13,9)-code is upper bounded by 24787, which is indeed an improvement over the sphere-packing bound.)

7 Conclusion

In this paper, we establish the correspondence between permutation codes and the independent sets of block permutation graphs. Using this approach, we improve the Gilbert–Varshamov bound asymptotically by a factor of $\Omega(\log n)$ when the minimum distance d is fixed and n goes into infinity. As for the upper bound, we clarify the relationship between block permutation distance of permutations and the intersection of their characteristic sets. Using some counting methods, we derive an upper bound of a new type, which beats the sphere-packing bound when d is relatively close to n. Moreover, we present the existence of a permutation code which improves the size of the known result by a factor of $\Theta(n^{2d-4})$. Explicit encoding schemes achieving this size are considered for future research.

Acknowledgements The authors express their gratitude to the anonymous reviewer for the detailed and constructive comments which are very helpful to the improvement of the presentation of this paper.

References

1. Ajtai M., Komlós J., Szemerédi E.: A note on Ramsey numbers. J. Comb. Theory Ser. A **29**(3), 354–360 (1980).
2. Bollobás B.: Random Graphs. Academic Press, London (1985).
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. Buzaglo S., Yaakobi E., Etzion T., Bruck J.: Systematic error-correcting codes for permutations and multi-permutations. IEEE Trans. Inf. Theory **62**(6), 3113–3124 (2016).
5. Chee Y.M., Van Khu V.: Breakpoint analysis and permutation codes in generalized Kendall tau and Cayley metrics. In: 2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, June 29–July 4, 2014, pp. 2959–2963 (2014).
6. 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).

7. 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).
8. Göloglu F., Lember J., Riet A., Skachek V.: New bounds for permutation codes in Ulam metric. In: IEEE International Symposium on Information Theory, ISIT 2015, Hong Kong, China, June 14–19, 2015, pp. 1726–1730 (2015).
9. Graham R.L., Sloane N.J.A.: Lower bounds for constant weight codes. IEEE Trans. Inf. Theory **26**(1), 37–43 (1980).
10. Hassanzadeh F.F., Milenkovic O.: Multipermutation codes in the Ulam metric for nonvolatile memories. IEEE J. Sel. Areas Commun. **32**(5), 919–932 (2014).
11. Jiang T., Vardy A.: Asymptotic improvement of the Gilbert–Varshamov bound on the size of binary codes. IEEE Trans. Inf. Theory **50**(8), 1655–1664 (2004).
12. Kendall M., Gibbons J.D.: Rank Correlation Methods. A Charles Griffin Title, 5th edn. Edward Arnold, London (1990).
13. Myers A.: Counting permutations by their rigid patterns. J. Comb. Theory Ser. A **99**(2), 345–357 (2002).
14. Tait M., Vardy A., Verstraëte J.: Asymptotic improvement of the Gilbert–Varshamov bound on the size of permutation codes (2013). CoRR arXiv:1311.4925
15. Tillson T.W.: A Hamiltonian decomposition of K^*_{2m}, $2m \geqslant 8$. J. Comb. Theory Ser. B **29**(1), 68–74 (1980).
16. Wang X., Zhang Y., Yang Y., Ge G.: New bounds of permutation codes under Hamming metric and Kendall's τ-metric. Des. Codes Cryptogr. **85**(3), 533–545 (2017).
17. Yang S., Schoeny C., Dolecek L.: Theoretical bounds and constructions of codes in the generalized Cayley metric. IEEE Trans. Inform. Theory (to appear). CoRR arXiv:1803.04314
18. Zhang Y., Ge G.: Snake-in-the-box codes for rank modulation under Kendall's τ-metric. IEEE Trans. Inf. Theory **62**(1), 151–158 (2016).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.