

Received 28 August 2025, accepted 8 September 2025,
date of publication 10 September 2025, date of current version 17 September 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3608654

RESEARCH ARTICLE

A New Lower Bound for Permutation Codes Using Reed–Solomon Codes

RANA T. SHWAYYEA¹, J. BAGHERIAN², REZA SOBHANI¹, AND ALIREZA ABDOLLAHI²

¹Department of Applied Mathematics and Computer Science, Faculty of Mathematics and Statistics, University of Isfahan, Isfahan 81746-73441, Iran

²Department of Pure Mathematics, Faculty of Mathematics and Statistics, University of Isfahan, Isfahan 81746-73441, Iran

Corresponding author: J. Bagherian (bagherian@sci.ui.ac.ir)

ABSTRACT We present a constructive lower bound for permutation codes under Kendall's τ -metric that improves upon the classical Gilbert–Varshamov estimate for many parameters. For any length $p > 5$, we construct codes with minimum Kendall's τ -distance 6 and size at least $p!/p^3$. This result is achieved by proving that Reed–Solomon codes of length p and dimension $p - 3$ have a minimum Lee distance of 6, and then applying a metric embedding from the Lee metric to the Kendall's τ -metric.

INDEX TERMS Permutation code, Reed–Solomon code, Kendall's τ -metric, Lee distance.

I. INTRODUCTION

Permutation codes have become increasingly important in modern coding theory due to their wide-ranging applications in non-volatile storage systems, such as flash memory, power-line communication, and rank modulation schemes [2], [6]. In these systems, data is represented by the relative order of charge levels rather than their absolute values, making permutations a natural and effective data representation.

To measure dissimilarity between permutations, various metrics have been studied, including the Hamming, Ulam, and Kendall's τ -metrics. Among them, the Kendall's τ -metric has gained particular attention due to its close alignment with adjacent transposition errors, which frequently occur in rank modulation-based storage systems. This metric counts the minimum number of adjacent swaps required to transform one permutation into another, thus capturing the most common types of distortions in practice [6].

A. PRIOR WORK AND LITERATURE SUMMARY

Over the past decade, extensive research has focused on establishing bounds on the size of permutation codes with prescribed minimum Kendall's τ -distance. Buzaglo and Etzion [3], as well as Wang et al. [12], derived upper and lower bounds using combinatorial and probabilistic

techniques. More recently, Abdollahi et al. [1] and Parvaresh et al. [9] proposed improved upper bounds and new constructions of permutation codes with refined distance properties. In parallel, efforts such as those of Wang et al. [13] resolved key questions about the nonexistence of perfect codes under the Kendall's τ -metric. In smaller cases, Vijayakumaran [14] computed exact maximal sizes for permutation codes in S_5 and S_6 , providing concrete benchmarks to validate theoretical bounds and guide code constructions. From an application perspective, Barg and Mazumdar [2] investigated error correction for rank modulation schemes using permutation codes, and Lu and Wang [7] studied the reconstruction of permutations corrupted by single Kendall errors, addressing practical decoding challenges. Zhang [16] recently introduced a novel metric on symmetric groups, broadening the scope of permutation codes and offering new design opportunities beyond the Kendall's τ -metric. A particularly promising approach for constructing large permutation codes is to relate them to well-studied classes of linear codes over finite fields [6], [10]. In particular, this connection has been explored in [6], where the authors develop an embedding of linear codes into the space of permutations using a bijection $\psi : S_n \rightarrow \mathbb{Z}_n!$, where $\mathbb{Z}_n! = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_n$, and they have shown that if C_L is a linear code of length $n - 1$ and minimum Lee distance d over $\mathbb{Z}_q$, $q \geq n$, then there exists a permutation code $C_K = \{\sigma \in S_n \mid \psi(\sigma) \in C_L\}$ of length n and minimum Kendall's τ -distance d such that $|C_K| = |C_L \cap \mathbb{Z}_n!|$.

The associate editor coordinating the review of this manuscript and approving it for publication was Sukhdev Roy.

TABLE 1. Summary of key results on permutation codes.

Ref.	Authors	Year	Bound Type	Method	Key Result
[6]	Jiang et al.	2010	Upper and lower bounds	Metric-embedding techniques	Code constructions and decoding algorithms for correcting limited-magnitude charge errors in rank modulation
[2]	Barg and Mazumdar	2010	Upper and lower bounds	Combinatorial and algebraic methods	Fundamental bounds and constructions for permutation codes under Kendall's τ -metric in the context of rank modulation
[3]	Buzaglo and Etzion	2015	Upper and lower bounds	Combinatorial arguments	New upper and lower bounds including sphere-packing and Singleton-type bounds under Kendall's τ -metric
[14]	Vijayakumaran	2016	Lower bound and exact value	Integer linear programming, exhaustive search	Exact maximal sizes of permutation codes under Kendall's τ -metric for S_5 and S_6
[12]	Wang et al.	2017	Lower bound	Combinatorial arguments	Improved sphere-packing upper bounds under the Hamming and Kendall's τ -metrics
[10]	Sobhani et al.	2019	Lower bound	Algebraic arguments	Construction of permutation codes under the Hamming metric by using Reed–Solomon codes over $\mathbb{Z}_q$
[13]	Wang et al.	2021	Non-existence perfect code	Combinatorial and algebraic arguments	Nonexistence of perfect permutation codes under Kendall's τ -metric for most parameters
[7]	Lu and Wang	2022	Improved bound	Graph-theoretic modeling, greedy selection	Improved bounds for recovering permutations from a single Kendall's τ -error
[16]	Zhang	2023	Upper and lower bounds	Combinatorial constructions, greedy algorithms	Construction of block permutation codes with guaranteed minimum block Kendall's τ -distance
[11]	Abdollahi et al.	2023	Upper bound	Algebraic and combinatorial techniques	New upper bounds on permutation code size using anticode and algebraic techniques
[9]	Parvaresh et al.	2025	Upper and lower bounds	Linear programming, algebraic constructions	Improved asymptotic and numerical bounds on permutation code size under the Kendall's τ -metric via new combinatorial constructions and refined anticode-based upper bounds

Table 1 presents a comparative summary of relevant literature, highlighting construction methods and key results.

B. DRAWBACKS AND RESEARCH GAP

Despite substantial progress, several important limitations remain:

- Many lower bounds, including those of Gilbert–Varshamov type or [12], are non-constructive or depend on special assumptions such as $p - 2$ being a prime power.
- Embedding techniques depend on the availability of linear codes with high minimum Lee distance, which are difficult to guarantee across all parameter regimes.
- Existing constructions are often applicable only to small values of n , lack scalability, or are tied to specific algebraic structures.

C. OUR CONTRIBUTION

To address the above limitations, this paper proposes a new algebraic and constructive approach to build permutation codes under the Kendall's τ -metric using Reed–Solomon codes. Our main contributions include:

- We show that for every prime $p > 5$, the dual of the Reed–Solomon code $RS[p, 3]$ has minimum Lee distance 6.
- Using a known embedding from the Lee metric to Kendall's τ -space, we derive the following explicit lower bound (Theorem 8):

$$P(p, 6) \geq \frac{p!}{p^3}.$$

- This bound is constructive for all prime lengths $p > 5$, and often stronger than the Gilbert–Varshamov bound.

D. ADVANTAGES OF OUR METHOD

Our approach offers several benefits over prior constructions:

- **Field independence:** Unlike methods requiring $p - 2$ to be a prime power, our construction applies for all primes $p > 5$.
- **Explicit and scalable:** The construction yields a closed-form lower bound without relying on probabilistic arguments or numerical search.
- **Algebraically grounded:** The use of dual Reed–Solomon codes leverages well-known code structures with provable properties.

A key application of our results lies in flash memory systems using rank modulation, where data is encoded by the relative ordering of charge levels in memory cells. Errors in such systems typically manifest as adjacent swaps, naturally modeled by the Kendall's τ -metric. Constructing large permutation codes with high Kendall's τ -distance is therefore essential for robust and reliable storage [2], [6].

E. PAPER ORGANIZATION

The paper is organized as follows. Section II reviews background on linear codes, Lee distance, and permutation codes. Section III analyzes the Lee distance of dual Reed–Solomon codes. Section IV presents our main construction and new lower bound. Section V provides comparisons with classical results. Section VI concludes the paper and outlines future directions.

II. PRELIMINARIES

In this section we recall the basic notions of linear codes endowed with the Hamming and Lee distances, and the theory of permutation codes.

A. LINEAR CODES

Let q be a prime power and n be a positive integer. We denote $\mathbb{F}_q$ as a finite field with q elements. For every two elements $u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_q^n$, the Hamming distance of u and v is defined by

$$d_H(u, v) = |\{i \in \{1, \dots, n\} \mid u_i \neq v_i\}|.$$

Moreover, for every $v = (v_1, \dots, v_n) \in \mathbb{F}_q^n$ the number

$$w_H(v) = |\{i \in \{1, \dots, n\} \mid v_i \neq 0\}|,$$

is defined as Hamming weight of v . Clearly, $w_H(v) = d_H(0, v)$. A k -dimensional subspace C of $\mathbb{F}_q^n$ is referred to as an $[n, k]$ linear code over $\mathbb{F}_q$. The integer

$$d_H(C) = \min\{d_H(u, v) \mid u \neq v \in C\},$$

is called the minimum distance of C . By a $[n, k, d]$ linear code, we mean a linear code C with length n , dimension k and minimum distance d .

Let C be a $[n, k]$ linear code over $\mathbb{F}_q$. The dual code of C , denoted $C^\perp$, is the set of all vectors in the vector space $\mathbb{F}_q^n$ which are orthogonal to all codewords of C . This means that

$$C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot c = 0, \quad \forall c \in C\},$$

where $x \cdot c = x_1 c_1 + \dots + x_n c_n$ for $x = (x_1, \dots, x_n)$ and $c = (c_1, \dots, c_n)$. One can see that $C^\perp$ is a $[n, n - k]$ linear code over $\mathbb{F}_q$.

For any vector $c = (c_1, c_2, \dots, c_n) \in \mathbb{F}_q^n$, the Lee weight of c is defined as

$$w_L(c) = w_L(c_1) + w_L(c_2) + \dots + w_L(c_n),$$

where $w_L(c_i) = \min\{c_i, q - c_i\}$.

Let $u = (u_1, \dots, u_n)$ and $v = (v_1, \dots, v_n)$ be vectors in $\mathbb{F}_q^n$. The Lee distance between u and v , denoted $d_L(u, v)$, is defined as the following:

$$d_L(u, v) = w_L(u - v).$$

For every $[n, k]$ linear code C , the minimum Lee distance C , denoted $d_L(C)$, is defined as

$$\min\{d_L(c) \mid c \in C\}.$$

Remark 1: For any vector $c \in \mathbb{F}_q^n$, one can see that

$$w_H(c) \leq w_L(c).$$

In particular, for every $[n, k]$ linear code C , $w_H(C) \leq w_L(C)$. The Reed–Solomon codes as one of the most significant and widely utilized classes of error-correcting codes, are defined by polynomial evaluations on a given subset in a finite field ([5], [8]). In this paper, we will focus on the standard Reed–Solomon code, which is defined as follows.

Definition 1 ([5]): Let $\mathbb{F}_q = \{0, \alpha_1, \dots, \alpha_{q-1}\}$ and $1 \leq k \leq q$. Then $RS[q, k] = \{(f(0), f(\alpha_1), \dots, f(\alpha_{q-1})) \in \mathbb{F}_q^q \mid f(x) \in \mathbb{F}_q[x] \text{ and } \deg(f) \leq k - 1\}$, is called the standard Reed–Solomon code of length q and dimension k .

It is known that the dual of Reed–Solomon code $RS[q, k]$ is the Reed–Solomon code $RS[q, q - k]$. The next easy lemma is useful.

Lemma 1: Let $C = RS[q, k]$, where $k > 0$. If $c = (c_1, c_2, \dots, c_q) \in C^\perp$, then $c_1 + c_2 + \dots + c_q \stackrel{q}{\equiv} 0$.

Consider the polynomial $f(x) = 1$. Then $(f(x_1), f(x_2), \dots, f(x_q)) = (1, 1, \dots, 1) \in C = RS[q, k]$. Since $c = (c_1, c_2, \dots, c_q) \in C^\perp$ we have $(c_1, c_2, \dots, c_q) \cdot (1, 1, \dots, 1) \stackrel{q}{\equiv} 0$. Therefore we have:

$$c_1 + c_2 + \dots + c_q \stackrel{q}{\equiv} 0. \quad (1)$$

■

B. PERMUTATION CODES

Let $n \in \mathbb{N}$ be a positive integer and denote by S_n the symmetric group on set $[n] = \{1, \dots, n\}$. Throughout this paper, for a permutation $\sigma \in S_n$, we use the vector notation of σ as $[\sigma(1), \sigma(2), \dots, \sigma(i), \dots, \sigma(n)]$. The identity element of S_n is denoted by $e := [1, 2, \dots, n]$. For distinct elements

$i, j \in [n]$, the transposition (i, j) is the permutation obtained from exchanging i and j in e . For $1 \leq i \leq n - 1$, the transposition $(i, i + 1)$ which converts permutation $[\sigma(1), \dots, \sigma(i), \sigma(i + 1), \dots, \sigma(n)] \in S_n$, into permutation $[\sigma(1), \dots, \sigma(i + 1), \sigma(i), \dots, \sigma(n)]$ is called an adjacent transposition.

For two permutations σ and $\pi \in S_n$, the Kendall's τ -distance, denoted by $d_K(\sigma, \pi)$, is defined as the minimum number of adjacent transpositions required to transform σ into π . Formally,

$$d_K(\sigma, \pi) = \min\{k \mid \exists \tau_1, \dots, \tau_k \in A_n, \pi = \sigma \circ \tau_1 \circ \dots \circ \tau_k\},$$

where $A_n = \{(i, i + 1) \mid 1 \leq i < n\}$ is the set of adjacent transpositions in S_n . For example, the Kendall's τ -distance between $\sigma = [1, 2, 3, 4]$ and $\pi = [2, 4, 1, 3]$ is 3, since the transformation

$$[1, 2, 3, 4] \xrightarrow{(1,2)} [2, 1, 3, 4] \xrightarrow{(3,4)} [2, 1, 4, 3] \xrightarrow{(2,3)} [2, 4, 1, 3]$$

uses three adjacent transpositions $(1, 2)$, $(3, 4)$, and $(2, 3)$. It can be verified that no shorter sequence of adjacent transpositions exists, so $d_K(\sigma, \pi) = 3$. As shown in [6], an equivalent expression for $d_K(\sigma, \pi)$ is given by:

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

In the example above, we have $\sigma^{-1} = [1, 2, 3, 4]$ and $\pi^{-1} = [3, 1, 4, 2]$. Therefore, the set $\{(i, j) \mid \sigma^{-1}(i) < \sigma^{-1}(j) \wedge \pi^{-1}(i) > \pi^{-1}(j)\}$ is equal to $\{(1, 2), (3, 4), (1, 4)\}$, yielding $d_K(\sigma, \pi) = 3$.

The Kendall's τ -distance is widely used in ranking and sorting problems where the relative order of elements is more important than their absolute values [4]. It measures the number of pairwise disagreements between two ranked lists, making it highly relevant in areas such as recommendation systems and preference aggregation [15]. In computational biology, Kendall's τ -distance has also been applied to compare gene orderings or evolutionary rearrangements in genomic sequences [11]. These applications justify the study of permutation codes under the Kendall's τ -metric, as they enhance robustness in data transmission or storage where rank-based errors are common.

A subset C of S_n is called permutation code of length n and minimum Kendall's τ -distance d , if $d_K(\sigma, \pi) \geq d$ for all distinct elements $\sigma, \pi \in C$. The largest size of a permutation code of length n and minimum Kendall's τ -distance d is denoted by $P(n, d)$. As the required minimum Kendall's τ -distance d increases, each codeword must be farther from every other codeword. This enlarges the surrounding forbidden region around each codeword, typically modeled as a Kendall's τ -ball of radius $\lfloor (d - 1)/2 \rfloor$. A Kendall's τ -ball of radius r centered at a permutation $\pi \in S_n$ consists of all permutations reachable from π via at most r adjacent transpositions, and thus represents the set of permutations that are too close to be valid codewords. Since the total space of permutations S_n has fixed size $n!$, fewer such non-overlapping balls can be packed as d increases.

Therefore, the maximum number of codewords $P(n, d)$ naturally decreases. This geometric intuition parallels the behavior observed in classical codes over Hamming spaces.

It is known that $P(n, 1) = n!$ and $P(n, 2) = \frac{n!}{2}$. Moreover, it follows from [3] that $P(n, d) = 2$ for every $\frac{2}{3}\binom{n}{2} \leq d \leq \binom{n}{2}$. Furthermore, for $d \in \{1, 2\}$ and $\frac{2}{3}\binom{n}{2} \leq d \leq \binom{n}{2}$, the exact value of $P(n, d)$ has been given in [3].

For a positive integer r and a permutation $\sigma \in S_n$, the set

$$B_r(\sigma) = \{\pi \in S_n \mid d_K(\sigma, \pi) \leq r\}$$

is called the ball of radius r which centered at σ in S_n under the Kendall's τ -distance. Since the size of a ball of radius r is independent of its center, we denote it by $B_K(r)$. However, computing or even estimating the size of $B_K(r)$ is non-trivial. The number of permutations at a fixed Kendall's τ -distance involves complex combinatorics of inversion vectors and the distribution of adjacent transpositions. Closed-form expressions are only known in small cases, and approximations grow less accurate as n increases. This computational difficulty limits the practical sharpness of the Gilbert–Varshamov bound for large n . Furthermore, for fixed r , the quantity $B_K(r)$ grows super-polynomially in n , because the number of permutations with bounded inversion count increases rapidly with dimension.

The Gilbert–Varshamov bound provides a general lower bound but becomes loose when the code distance is fixed and the permutation length grows, due to the super-polynomial growth of Kendall's τ -balls [3]. But the sphere-packing (Hamming-type upper) bound offers an upper limit on code size but often overestimates the true covering size of the permutation space, especially for small minimum distances [6]. The Gilbert–Varshamov bound and sphere-packing bound for permutation codes under Kendall's τ -metric are as follows. Unlike classical bounds derived over linear vector spaces, these results deal with covering and packing arguments in a discrete, non-linear space.

Theorem 1 ([6]): For every positive integers $n, d \geq 1$,

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

The Gilbert–Varshamov bound provides a constructive lower bound based on greedy packing: one iteratively adds permutations to the code as long as newly added codewords remain at least distance d apart [3]. However, this approach becomes loose when the Kendall's τ -distance d is fixed and the code length n grows, because the size of a ball in the Kendall's τ -metric (i.e., $B_K(d-1)$) grows super-polynomially with n [12]. As a result, the Gilbert–Varshamov bound quickly underestimates the true code size for fixed d and large n . On the other hand, the sphere-packing (or Hamming-type) upper bound assumes that balls of radius $\lfloor (d-1)/2 \rfloor$ pack the space efficiently without overlap [3]. But this assumption overestimates the number of disjoint balls that can fit, especially when d is small compared to n , leading to loose upper bounds in that regime [14]. Thus, while both bounds

are asymptotically useful, they are tight only under specific parameter conditions.

In [6], some lower bounds under Kendall's τ -metric have been presented as below.

Theorem 2 ([6]): (i) For all $n \geq 1$ and $d \geq 2$ even, $P(n, d) \geq \frac{1}{2}P(n, d-1)$.

(ii) For all $d, n \geq 2$, $P(n+1, d) \geq \lceil \frac{n+1}{d} \rceil P(n, d)$.

The inequalities in Theorem 2 offer a recursive mechanism to build lower bounds for larger parameters based on smaller ones. Specifically, part (i) shows that if a bound is known for $P(n, d-1)$, then a bound for $P(n, d)$ can be derived by halving it. Part (ii) allows extension in the length parameter n while preserving minimum distance d , using a multiplicative factor. By combining these two rules, one can construct bounds inductively from known small cases, which is particularly useful when explicit constructions are only available for small n .

In [12] a lower bound when $n-2$ is a prime power has been given as follows.

Theorem 3 ([12, Theorem 18]): Let $m = ((n-2)^{t+1} - 1)/(n-3)$, where $n-2$ is a prime power. Then $P(n, 2t+1) \geq \frac{n!}{(2t+1)^m}$.

The condition that $n-2$ is a prime power arises from constructions based on projective spaces over finite fields. Specifically, the authors employ incidence structures from finite projective geometries (e.g., $\text{PG}(k, q)$) to design sets of permutations with guaranteed pairwise distances. These constructions are explicit and algebraic, and give rise to families of codes with relatively large size and fixed minimum Kendall's τ -distance. However, they are only applicable when $n-2$ satisfies the prime power condition, limiting their generality.

Remark 2: It follows from Theorem 2 and Theorem 3 that if $n-2$ is a prime power, then $P(n, 2t) \geq \frac{n!}{2(2t+1)^m}$, where $m = ((n-2)^{t+1} - 1)/(n-3)$.

This bound scales factorially in n , with a denominator polynomial in n and exponential in t , due to the term $(n-2)^{t+1}$. As a result, it yields strong asymptotic performance for fixed t as $n \rightarrow \infty$, provided that $n-2$ remains a prime power.

However, the applicability of this result is structurally limited. Since the construction relies on projective geometries over finite fields, it is only valid for values of n satisfying the prime power condition. In contrast, recursive bounds like those in Theorem 2 are more broadly applicable but typically yield weaker asymptotic rates. This trade off highlights the need for new algebraic constructions such as the one proposed in this paper that work uniformly across all primes or general values of n .

C. NOTATION AND CONSTANTS

For clarity and reproducibility, we summarize the principal constants and notation used throughout this work:

- $\mathbb{F}_q$: a finite field with q elements.
- $C \subseteq \mathbb{F}_q^n$: a linear block code over a finite field $\mathbb{F}_q$.

- $d_H(x, y)$: the Hamming distance between vectors $x, y \in \mathbb{F}_q^n$.
- $d_L(x, y)$: the Lee distance between vectors $x, y \in \mathbb{F}_q^n$.
- $d_L(C)$: minimum Lee distance of a code C in $\mathbb{F}_q^n$.
- $d_H(C)$: minimum Hamming distance of a code C in $\mathbb{F}_q^n$.
- $RS[q, k]$: the Reed–Solomon code of length q and dimension k over $\mathbb{F}_q$.
- $C^\perp$: the dual of code C .
- S_n : the symmetric group of all permutations on n elements.
- $\sigma, \pi \in S_n$: permutations of length n .
- $d_K(\sigma, \pi)$: Kendall's τ -distance between permutations σ and π , defined as the minimum number of adjacent transpositions needed to convert σ into π .
- $B_K(r)$: the size of a Kendall's τ -ball of radius r , i.e., the number of permutations $\pi \in S_n$ such that $d_K(\sigma, \pi) \leq r$ for a fixed center $\sigma \in S_n$.
- $P(n, d)$: the maximum number of permutations in S_n that form a code with minimum Kendall's τ -distance at least d .

III. DUAL OF REED-SOLOMON CODES

In this section, we give some results about the minimum Hamming and Lee distance for the Reed–Solomon codes over the finite field $\mathbb{F}_p$, where p is a prime number. It is worth noting that classical coding theory references such as [5], [8] provide foundational discussions on Lee distance and related metrics. However, specific results on the Lee distance of Reed–Solomon codes especially exact values or tight bounds are limited. MacWilliams and Sloane [8] provided foundational results on the Lee metric and its applications in coding theory. They defined the Lee weight and Lee distance over $\mathbb{Z}_q$ and established general upper bounds for the minimum Lee distance of linear codes, namely $d_L \leq d_H \cdot \lfloor q/2 \rfloor$, where d_H is the minimum Hamming distance. While their work includes exact Lee distances for several small linear and cyclic codes over $\mathbb{Z}_q$, they do not specifically analyze Reed–Solomon codes under the Lee metric. As main result in this section we prove that a Reed–Solomon code of length p and dimension $p - 3$ over $\mathbb{Z}_p$ has minimum Lee distance 6 (see Theorem 6).

Lemma 2: Let p be a prime number greater than 3. If $C = RS[p, 2]$, then $d_H(C^\perp) = 3$.

Let $\mathbb{F}_p = \{0, 1, \dots, p-1\}$. Then the dual code is $C^\perp = \{(f(0), f(1), \dots, f(p-1)) \mid f(x) \in \mathbb{F}_p[x], \deg f \leq p-3\}$. By the basic fact that a nonzero polynomial over $\mathbb{F}_p$ of degree at most d has at most d distinct zeros in $\mathbb{F}_p$, any nonzero f with $\deg f \leq p-3$ vanishes at no more than $p-3$ points. Hence every nonzero codeword $c = (f(0), \dots, f(p-1)) \in C^\perp$ has at least $p - (p-3) = 3$ nonzero coordinates, so $w_H(c) \geq 3$ and therefore $d_H(C^\perp) \geq 3$.

Moreover, this lower bound is tight. Indeed, fix any distinct $i, j, k \in \mathbb{F}_p$ and take

$$f(x) = \prod_{t \in \mathbb{F}_p \setminus \{i, j, k\}} (x - t),$$

which is a nonzero polynomial of degree exactly $p-3$ that vanishes at precisely $p-3$ points of $\mathbb{F}_p$ and is nonzero at $x = i, j, k$. The corresponding codeword $c = (f(0), \dots, f(p-1))$ has Hamming weight 3. Thus $d_H(C^\perp) \leq 3$.

Combining the two inequalities gives $d_H(C^\perp) = 3$. ■

Lemma 3: Let p be a prime number greater than 3. If $C = RS[p, 2]$ then $d_L(C^\perp) = 4$.

From Lemma 2, we know that $d_H(C^\perp) = 3$. By Remark 1, we have $d_L(C^\perp) \geq d_H(C^\perp) = 3$.

Step 1: No Codeword of Lee Weight 3: Suppose, for the sake of contradiction, that there exists a nonzero codeword $c \in C^\perp$ such that $w_L(c) = 3$. Since the minimum Lee weight is the sum of the coordinate-wise Lee weights, this would require that c has exactly three nonzero components, each with Lee weight 1. In $\mathbb{F}_p$, this means the nonzero entries of c must belong to the set $\{1, p-1\}$, since those are the only elements with Lee weight 1. Let $c = (f(0), f(1), \dots, f(p-1)) \in C^\perp$ be such a codeword, corresponding to a polynomial $f(x) \in \mathbb{F}_p[x]$ of degree at most $p-3$, such that $f(i), f(j), f(k) \in \{1, p-1\}$ and $f(t) = 0$ for all $t \notin \{i, j, k\}$. Then c has support at three positions only, and the sum of its entries is

$$f(i) + f(j) + f(k) \in \{p-3, p-1, 1, 3\} \setminus \{0\},$$

since the sum of any three elements from $\{1, p-1\}$ cannot be zero in $\mathbb{F}_p$ (for $p > 3$). But Lemma 2.3 states that for any codeword $c \in C^\perp$, the sum of its coordinates must be zero modulo p . This yields a contradiction. Therefore, no codeword of Lee weight 3 can exist in $C^\perp$, and we conclude that $d_L(C^\perp) \geq 4$.

Step 2: Existence of a Codeword of Lee Weight 4: Consider the polynomial

$$f(x) = 2(x-3)(x-4) \cdots (x-(p-1)) \in \mathbb{F}_p[x].$$

This polynomial has degree $p-3$ and clearly, $f(t) = 0$ for every $t \in \{3, 4, \dots, p-1\}$. Let $c = (f(0), f(1), f(2), 0, 0, \dots, 0)$. Since by Wilson's Theorem

$$\prod_{t \in \mathbb{F}_p \setminus \{x\}} (x-t) = (p-1)! \stackrel{p}{\equiv} -1 \quad (2)$$

we have

$$2 \prod_{t \in \mathbb{F}_p \setminus \{0\}} (i-t) \stackrel{p}{\equiv} -2.$$

So

$$(-1)(-2)f(0) \stackrel{p}{\equiv} -2,$$

and then

$$f(0) \stackrel{p}{\equiv} -1$$

Similarly, the equations

$$2 \prod_{t \in \mathbb{F}_p \setminus \{1\}} (i-t) \stackrel{p}{\equiv} -2$$

and

$$2 \prod_{t \in \mathbb{F}_p \setminus \{2\}} (i - t) \stackrel{p}{\equiv} -2$$

yield that $-f(1) \stackrel{p}{\equiv} -2$ and $2f(2) \stackrel{p}{\equiv} -2$, respectively. So $f(1) = 2$ and $f(2) \stackrel{p}{\equiv} -1$. Then

$$c = (f(0), f(1), f(2), 0, 0, \dots, 0) \\ = (p-1, 2, p-1, 0, \dots, 0).$$

This implies that

$$w_L(c) = 1 + 2 + 1 = 4.$$

Remark 3: If $C = RS[3, 2]$, then

$$C^\perp = RS[3, 1] = \{(0, 0, 0), (1, 1, 1), (2, 2, 2)\},$$

and so $d_H(C^\perp) = d_L(C^\perp) = 3$. Moreover, if $C = RS[3, 3]$, then $C^\perp = \emptyset$.

Theorem 4: Suppose that $C = RS[5, 3]$. Then $d_H(C^\perp) = 4$ and $d_L(C^\perp) = 5$.

Since $C^\perp = \{(f(0), f(1), f(2), f(3), f(4)) \mid f(x) \in \mathbb{F}_5[x], \deg(f) \leq 1\}$, we have

$$C^\perp = \{(0, 0, 0, 0, 0), (1, 1, 1, 1, 1), (2, 2, 2, 2, 2), \\ (3, 3, 3, 3, 3), (4, 4, 4, 4, 4), (0, 1, 2, 3, 4), (0, 2, 4, 3, 1), \\ (0, 3, 1, 4, 2), (0, 4, 3, 2, 1), (1, 2, 3, 4, 0), (1, 3, 0, 2, 4), \\ (1, 4, 2, 0, 3), (1, 0, 4, 3, 2), (2, 3, 4, 0, 1), (2, 4, 1, 3, 0), \\ (2, 0, 3, 1, 4), (2, 1, 0, 4, 3), (3, 4, 0, 1, 2), (3, 0, 2, 4, 1), \\ (3, 1, 4, 2, 0), (3, 2, 1, 0, 4), (4, 0, 1, 2, 3), (4, 1, 3, 0, 2), \\ (4, 2, 0, 3, 1), (4, 3, 2, 1, 0)\}.$$

Then one can see that $d_H(C^\perp) = 4$ and $d_L(C^\perp) = 5$. ■

Theorem 5: Let p be a prime number greater than 5. If $C = RS[p, 3]$ over a finite field $\mathbb{F}_p$, then $d_H(C^\perp) = 4$.

Since $C^\perp = RS[p, p-3] = \{(f(0), f(1), \dots, f(p-1)) \mid f(x) \in \mathbb{F}_p[x], \deg(f) \leq p-4\}$, for any $c \in C^\perp$, we have $c = (f(0), f(1), \dots, f(p-1)) \in C^\perp$ for some $f(x) \in \mathbb{F}_p[x]$ of degree at most $p-4$. Since $f(x)$ can vanish at no more than $p-4$ elements of $\mathbb{F}_p$, c has at least 4 non-zero entries. Then $w_H(c) \geq 4$. Therefore, for any codeword $c \in C^\perp$, we have $w_H(c) \geq 4$ and so $d_H(C^\perp) = 4$. ■

Theorem 6: Let p be a prime number greater than 5. If $C = RS[p, 3]$ over the finite field $\mathbb{F}_p$, then $d_L(C^\perp) = 6$.

By Theorem 5 and Remark 1, we know that $d_L(C^\perp) \geq 4$. We now show that $d_L(C^\perp) \geq 6$ by ruling out the existence of codewords of Lee weight 4 or 5.

Step 1: No codeword of Lee Weight 4: Assume, for contradiction, that there exists a codeword $c \in C^\perp$ with $w_L(c) = 4$. Then $c = (f(0), f(1), \dots, f(p-1))$, where $f(x) \in \mathbb{F}_p[x]$ is a polynomial of degree at most $p-4$, and the nonzero values of f occur at exactly four positions $a < b < c < d \in \mathbb{F}_p$. Since the total Lee weight is 4, each nonzero value must have Lee weight 1, which implies that

$$f(a), f(b), f(c), f(d) \in \{1, p-1\}.$$

Moreover, by Lemma 2.3, we must have

$$f(a) + f(b) + f(c) + f(d) \stackrel{p}{\equiv} 0.$$

We now consider all combinations of four values from $\{1, p-1\}$ whose sum is zero:

- (i) All values equal (e.g., $f(a) = f(b) = f(c) = f(d) = 1$) yields a total of $\{4, p-4\}$, which is nonzero modulo p .
- (ii) Three of one sign and one of the opposite (e.g., $1 + 1 + 1 + (p-1) = 2$) also yields a nonzero sum.
- (iii) Only the combination with two 1s and two $(p-1)$ s results in a total sum of 0, which is compatible with Lemma 2.3.

Thus, the only cases that do not contradict Lemma 2.3 are:

- (1) $f(a) = f(b) = 1, f(c) = f(d) = p-1$,
- (2) $f(a) = f(b) = p-1, f(c) = f(d) = 1$.

Moreover, since by Wilson's Theorem,

$$\prod_{t \in \mathbb{F}_p \setminus \{x\}} (x - t) = (p-1)! \stackrel{p}{\equiv} -1$$

we have

$$\prod_{t \in \mathbb{F}_p \setminus \{a\}} (a - t) \stackrel{p}{\equiv} -1$$

and so $f(a)(a-b)(a-c)(a-d) \stackrel{p}{\equiv} -\gamma$. Similarly, $f(b)(b-a)(b-c)(b-d) \stackrel{p}{\equiv} f(c)(c-a)(c-b)(c-d) \stackrel{p}{\equiv} f(d)(d-a)(d-b)(d-c) \stackrel{p}{\equiv} -\gamma$. This shows that

$$f(a)(a-b)(a-c)(a-d) \stackrel{p}{\equiv} f(b)(b-a)(b-c)(b-d) \\ f(a)(a-b)(a-c)(a-d) \stackrel{p}{\equiv} f(c)(c-a)(c-b)(c-d) \\ f(a)(a-b)(a-c)(a-d) \stackrel{p}{\equiv} f(d)(d-a)(d-b)(d-c).$$

Then

$$f(a)(a-c)(a-d) \stackrel{p}{\equiv} f(b)(c-b)(b-d) \\ f(a)(a-b)(a-d) \stackrel{p}{\equiv} f(c)(b-c)(c-d) \\ f(a)(a-b)(a-c) \stackrel{p}{\equiv} f(d)(b-d)(d-c).$$

First assume that $f(a) = f(b) = 1$ and $f(c) = f(d) = p-1$. Then

$$(a-c)(a-d) \stackrel{p}{\equiv} (c-b)(b-d) \quad (3)$$

$$(a-b)(a-d) \stackrel{p}{\equiv} (c-b)(c-d) \quad (4)$$

$$(a-b)(a-c) \stackrel{p}{\equiv} (d-b)(d-c) \quad (5)$$

From equations (4) we have $a^2 - a(b+d) + bd \stackrel{p}{\equiv} c^2 - c(b+d) + bd$. So

$$(a-c)(a+c) \stackrel{p}{\equiv} (a-c)(b+d).$$

Therefore,

$$a + c \stackrel{p}{\equiv} b + d. \quad (6)$$

Similarly, from equation (5), we have $a^2 - a(b + c) + bc \equiv d^2 - d(b + c) + bc$ and then

$$a + d \equiv b + c. \quad (7)$$

It follows from equations (6) and (7) that $2a + c + d \equiv 2b + d + c$, and hence $a = b$, a contradiction. Similarly, if $f(a) = f(b) = p - 1$ and $f(c) = f(d) = 1$ we have a contradiction. Therefore, there is no codeword $c \in C^\perp$ with $w_L(c) = 4$. So $w_L(c) \geq 5$ for all $c \in C^\perp$.

Step 2: No Codeword of Lee Weight 5 Now suppose there exists $c \in C^\perp$ with $w_L(c) = 5$. Then c must have either 4 or 5 non-zero elements. Let $c = (0, \dots, f(i), \dots, f(j), \dots, f(k), \dots, f(l), \dots, 0)$ for some $i, j, k, l \in \mathbb{F}_p$ and some $f(x) \in \mathbb{F}_p[x]$ of degree at most $p - 4$. Suppose c has 4 non-zero elements. Then three of these non-zero elements $\{f(i), f(j), f(k), f(l)\}$ belong to the set $\{1, p - 1\}$ and another one belongs to the set $\{2, p - 2\}$. But in this case one can see that

$$f(i) + f(j) + f(k) + f(l) \not\equiv 0,$$

and it follows from Lemma 1 that $c \notin C^\perp$. Similarly, if c has 5 non-zero elements, then all the elements must belong to the set $\{1, p - 1\}$ and similarly, one can see that $c \notin C^\perp$. Therefore, there exists no codeword $c \in C^\perp$ with $w_L(c) = 5$. Hence, $w_L(c) \geq 6$ for all $c \in C^\perp$.

Step 3: Existence of a codeword of Lee weight 6. Consider the polynomial $f(x) = 12x(x - 3)(x - 4) \dots (x - (p - 3)) \in \mathbb{F}_p[x]$. Clearly, $f(x)$ is a polynomial of degree $p - 4$. Let $c = (0, f(1), f(2), 0, 0, \dots, 0, f(p - 2), f(p - 1))$. Since

$$12 \prod_{t \in \mathbb{F}_p \setminus \{i\}} (i - t) \equiv -12$$

we have

$$12 \prod_{t \in \mathbb{F}_p \setminus \{1\}} (1 - t) \equiv -12$$

and so

$$(-1)(3)(2)f(1) \equiv -12$$

and then $f(1) = 2$. Similarly, since

$$\begin{aligned} 12 \prod_{t \in \mathbb{F}_p \setminus \{2\}} (2 - t) &\equiv -12, \\ 12 \prod_{t \in \mathbb{F}_p \setminus \{p-2\}} (p - 2 - t) &\equiv -12, \\ 12 \prod_{t \in \mathbb{F}_p \setminus \{p-1\}} (p - 1 - t) &\equiv -12, \end{aligned}$$

we have $12f(2) \equiv -12$, $-12f(p - 2) \equiv -12$ and $6f(p - 1) \equiv -12$, respectively. So we get $f(2) = p - 1$, $f(p - 2) = 1$ and $f(p - 1) = p - 2$. Therefore, $c = (0, f(1), f(2), 0, \dots, 0, f(p - 2), f(p - 1)) = (0, 2, p - 1, 0, \dots, 0, 1, p - 2)$. The Lee weight of c is

$$w_L(c) = 2 + 1 + 1 + 2 = 6$$

This implies that the minimum Lee weight $C^\perp$ is 6 and so $d_L(C^\perp) = 6$. ■

Let p be a prime and k a positive integer. For $k = 2, 3$, the value of $d_L(RS[p, p - k])$ is completely determined by the preceding results. In addition, direct computation yields the following values: $d_L(RS[7, 3]) = 7$, $d_L(RS[11, 7]) = 8$, $d_L(RS[11, 6]) = 10$, $d_L(RS[11, 5]) = 11$. In each of these cases, the equality

$$d_L(RS[p, p - k]) = \min\{p, 2k\}$$

holds. Motivated by this observation, we propose the following conjecture.

Conjecture 1: Let p be a prime and k be a positive integer. If $C = RS[p, k]$ over a finite field $\mathbb{F}_p$, then $d_L(C^\perp) = \min\{p, 2k\}$.

Remark 4: The conjecture is based on empirical evidence. In all computed cases of the Reed–Solomon codes $RS[p, p - k]$ over $\mathbb{Z}_p$, we observe that the minimum Lee distance is equal to $\min\{p, 2k\}$. This includes all primes $p \leq 17$ and selected larger examples. These results suggest that the behavior of dual Reed–Solomon codes under the Lee metric consistently follows this pattern. We conjecture that $2k$ represents a typical lower bound arising from the polynomial structure of the dual code, while p acts as a soft cap due to vector length. To the best of our knowledge, no such counterexamples are known for larger primes. We acknowledge, however, that a complete theoretical justification is still missing. We view this conjecture as a promising direction for future research and encourage further investigation, both computational and theoretical.

IV. APPLICATION TO PERMUTATION CODES

In this section, we present a new lower bound for permutation codes under Kendall's τ -metric. As a first step, we introduce a metric embedding, originally presented in [6].

For $n \in \mathbb{N}$, let

$$\mathbb{Z}_n! = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \dots \times \mathbb{Z}_n.$$

For every $u = (u_2, \dots, u_n)$, $v = (v_2, \dots, v_n) \in \mathbb{Z}_n!$, their l_1 -distance is define as

$$d_1(u, v) = \sum_{i=2}^n |u_i - v_i|.$$

We regard $\mathbb{Z}_n!$ as a graph whose vertices correspond to the elements of $\mathbb{Z}_n!$, with an edge between two vertices if their l_1 -distance is equal to 1.

Remark 5: For every $q \geq n$, the graph $\mathbb{Z}_n!$ can be viewed as a subgraph of $\mathbb{Z}_q^{n-1}$, where $\mathbb{Z}_q^{n-1}$ denotes the graph whose vertices are the elements of $\mathbb{Z}_q^{n-1}$, and where two vertices are adjacent if and only if their Lee distance is 1.

Define the mapping $\psi : S_n \rightarrow \mathbb{Z}_n!$ such that map every $\sigma \in S_n$ to the vector $u = (u_2, \dots, u_n) \in \mathbb{Z}_n!$, where u_j equals the number of inversions in σ of the form (j, i) , $1 \leq i \leq j - 1$. As shown in [6], ψ is a bijection and for every $\sigma, \pi \in S_n$,

$$d_1(\sigma, \pi) \leq d_K(\sigma, \pi).$$

TABLE 2. Embedding $\psi : S_7 \rightarrow \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_7$ for selected permutations.

Permutation σ	Vector $\psi(\sigma)$
[1, 2, 3, 4, 5, 6, 7]	(0, 0, 0, 0, 0, 0)
[1, 3, 4, 6, 7, 2, 5]	(0, 0, 0, 0, 5, 3)
[7, 6, 4, 5, 3, 1, 2]	(1, 2, 1, 3, 5, 4)
[5, 7, 6, 3, 2, 4, 1]	(0, 1, 3, 4, 2, 6)
[3, 5, 7, 2, 6, 1, 4]	(0, 0, 3, 1, 5, 2)

Example 1: The following table presents selected permutations from S_7 along with their corresponding inversion vectors under the embedding $\psi : S_7 \rightarrow \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_7$. The map ψ assigns to each permutation $\sigma \in S_7$ a vector $\psi(\sigma)$ that records the number of inversions at each position, thereby capturing the relative order of elements in σ .

Remark 6: Using the following algorithm, one can generate further examples for arbitrary n .

Note that each coordinate u_j in the image vector $\psi(\sigma) = (u_2, u_3, \dots, u_n)$ counts the number of inversions involving the position j , that is, the number of indices $i < j$ such that $\sigma(i) > \sigma(j)$.

Algorithm Embedding $\psi : S_n \rightarrow \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_n$

Input: A permutation $\sigma = [\sigma(1), \sigma(2), \dots, \sigma(n)] \in S_n$,

Output: Vector $\psi(\sigma) = (u_2, u_3, \dots, u_n)$.

- 1) Initialize an empty vector $u = []$
- 2) For $j = 2$ to n , do:
 - a) Set $u_j \leftarrow 0$
 - b) For $i = 1$ to $j - 1$, do:
 - i) If $\sigma(i) > \sigma(j)$, then set $u_j \leftarrow u_j + 1$
 - c) Append u_j to vector u
- 3) Return $v = (u_2, u_3, \dots, u_n)$

Theorem 7 ([6, Theorem 10]): Let C_L be a linear code of length $n - 1$ and minimum Lee distance d over $\mathbb{Z}_q$, $q \geq n$. Then there exists a permutation code C_K of length n and minimum Kendall's τ -distance d such that $|C_K| = |C_L \cap \mathbb{Z}_n!|$.

From Theorem 7 we can give a lower bound for $P(n, d)$.

Corollary 1: Let C_L be a linear code of length $n - 1$ and dimension k with minimum Lee distance d over $\mathbb{Z}_q$, $q \geq n$. Then there exist a code C_K of length n and minimum Kendall's τ -distance d such that $|C_K| \geq \frac{n!}{q^{n-k-1}}$.

Consider the vector space $V = \mathbb{Z}_q^{n-1}$. The linear code $C_L \subset V$ has q^{n-k-1} cosets in V . These cosets induce a partition of $\mathbb{Z}_n!$, since $\mathbb{Z}_n! \subset V$. Let T be the coset for which the intersection $T \cap \mathbb{Z}_n!$ has maximum cardinality, and denote $M = |T \cap \mathbb{Z}_n!|$. Then, since $|\mathbb{Z}_n!| = |S_n| = n!$, it follows that

$$M \geq \frac{n!}{q^{n-k-1}}.$$

Now, consider the embedding $\psi : S_n \rightarrow \mathbb{Z}_n!$, and define

$$C_K = \{\sigma \in S_n \mid \psi(\sigma) \in T\}.$$

Then C_K is a permutation code of length n and minimum Kendall's τ -distance at least d (see Theorem 7), with size satisfying

$$|C_K| \geq \frac{n!}{q^{n-k-1}}.$$

Theorem 8: For every prime p greater than 5, there exists a permutation code C_K of length p and minimum Kendall's τ -distance 6 such that $|C_K| \geq \frac{p!}{p^3}$. In particular, $P(p, 6) \geq \frac{p!}{p^3}$.

Let $C = RS[p, 3]$ be a Reed–Solomon code of length p over the finite field $\mathbb{F}_p$. By Theorem 6, the dual code $C^\perp$ is a linear code of length p , dimension $p - 3$, over $\mathbb{Z}_p$, with minimum Lee distance 6. Let C_L be the shortened code obtained from $C^\perp$ by deleting the first coordinate from all codewords of $C^\perp$ that have a 0 in the first position. Then C_L is a linear code of length $p - 1$, dimension $p - 4$, and minimum Lee distance 6 over $\mathbb{Z}_p$.

Now consider the embedding $\psi : S_p \rightarrow \mathbb{Z}_p! \subseteq \mathbb{Z}_p^{p-1}$, and define

$$C_K = \{\sigma \in S_p \mid \psi(\sigma) \in C_L\}.$$

Then, by Theorem 1, C_K is a permutation code of length p , minimum Kendall's τ -distance 6, and satisfies the size bound

$$|C_K| \geq \frac{p!}{p^3}.$$

Remark 7: The embedding $\psi : S_n \rightarrow \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_n$ plays a central role in relating the Kendall's τ -metric on permutations to the ℓ_1 -distance on the product space $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_n$. In particular, for any two permutations $\sigma, \pi \in S_n$, we have $d_1(\psi(\sigma), \psi(\pi)) \leq d_K(\sigma, \pi)$. This inequality allows us to construct permutation codes under the Kendall's τ -metric by using linear codes over $\mathbb{Z}_q$ (with $q \geq n$) that have guaranteed Lee distance. Through this embedding, algebraic properties of such linear codes especially those derived from Reed–Solomon codes can be translated into distance guarantees for permutation codes, as shown in Theorem 8.

Example 2: Let $C = RS[7, 3]$ be a Reed–Solomon code over the finite field $\mathbb{Z}_7$. Then the dual code $C^\perp$ is a $[7, 4]$ linear code over $\mathbb{Z}_7$ with minimum Lee distance 6. By shortening $C^\perp$ at a coordinate where the symbol is zero, we obtain a code C_L of length 6, dimension 4, and minimum Lee distance 6 over $\mathbb{Z}_7$. Consider the embedding $\psi : S_7 \rightarrow \mathbb{Z}_7! \subseteq \mathbb{Z}_7^6$, and define the set

$$C_K = \{\sigma \in S_7 \mid \psi(\sigma) \in C_L\}.$$

Then C_K is a permutation code of length 7 with minimum Kendall's τ -distance at least 6. Moreover, it satisfies the bound

$$|C_K| \geq \frac{7!}{7^3} = \frac{5040}{343} \geq 15.$$

Remark 8: The lower bound in Theorem 8 is fundamentally algebraic in nature. It relies on the existence of Reed–Solomon codes over the finite field $\mathbb{F}_p$, where p is a prime. The derivation of the minimum Lee distance of the dual code $C^\perp$ and the embedding $\psi : S_n \rightarrow \mathbb{Z}_n!$ jointly rely on the algebraic structure of $\mathbb{F}_p$ and the fact that the dual of an $[n, k]$ Reed–Solomon code is again a Reed–Solomon code. These techniques are not purely combinatorial and would not directly apply in non-prime or composite modulus settings. This highlights the special role that prime (and, more

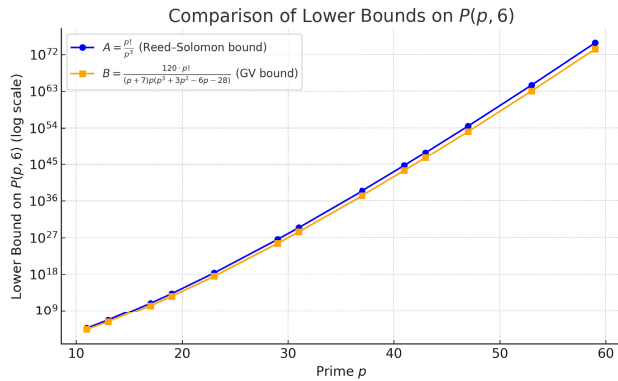


FIGURE 1. Comparison of lower bounds on $P(p, 6)$ for increasing prime values p . The constructive bound $A = \frac{p!}{p^3}$ from Reed–Solomon codes outgrows the Gilbert–Varshamov-type bound $B = \frac{120 \cdot p!}{(p+7)p(p^3+3p^2-6p-28)}$ as p increases. Both curves are plotted on a logarithmic scale.

generally, prime power) field structures play in enabling our construction.

V. COMPARISON WITH OTHER CLASSICAL BOUNDS

Let p be a prime such that $p - 2$ is a prime power. Then, by Remark 2, we have the lower bound

$$P(p, 6) \geq \frac{p!}{10(p^2 - 3p + 3)}.$$

In this case, the bound may outperform the lower bound given in Theorem 8. On the other hand, if $p - 2$ is not a prime power, the Gilbert–Varshamov lower bound (see Theorem 1) gives

$$P(p, 6) \geq \frac{p!}{B_K(5)}.$$

From [13], the Kendall’s τ -ball of radius 5 satisfies

$$B_K(5) = \frac{(p+7)p(p^3+3p^2-6p-28)}{120},$$

and hence,

$$P(p, 6) \geq \frac{120 \cdot p!}{(p+7)p(p^3+3p^2-6p-28)}.$$

Therefore, when $p - 2$ is not a prime power, the lower bound in Theorem 8 often provides a better estimate than the Gilbert–Varshamov bound.

Remark 9: Let us denote:

TABLE 3. Comparison of Lower Bounds for $P(p, 6)$.

p	$\frac{p!}{p^3}$	$\frac{120 \cdot p!}{(p+7)p(p^3+3p^2-6p-28)}$	$\frac{p!}{10(p^2-3p+3)}$
11	29983.3	15117.9	43865.7
13	2,834,057.4	1,104,500.4	4,685,714.3
17	7.24×10^{10}	1.85×10^{10}	N/A
27	5.53×10^{23}	6.53×10^{22}	1.83×10^{25}
37	2.72×10^{38}	1.87×10^{37}	N/A
47	2.49×10^{54}	1.11×10^{53}	N/A

- $A = \frac{p!}{p^3}$, which is the explicit lower bound on $P(p, 6)$ obtained from our construction using Reed–Solomon codes (see Theorem 8);
- $B = \frac{120 \cdot p!}{(p+7)p(p^3+3p^2-6p-28)}$, which is the Gilbert–Varshamov-type lower bound derived from the known upper bound on the size of a Kendall’s τ -ball of radius 5 (as given in [13]).

Both A and B are explicit theoretical lower bounds on the maximum size $P(p, 6)$ of a permutation code in S_p with minimum Kendall’s τ -distance 6. The bound A is constructive and algebraic, arising from a specific embedding via dual Reed–Solomon codes, while B is based on a volumetric covering argument under the Kendall’s τ -metric.

To compare their asymptotic behavior, we compute the ratio:

$$\frac{A}{B} = \frac{(p+7)p(p^3+3p^2-6p-28)}{120p^3}.$$

Dividing both numerator and denominator by p^3 , we obtain:

$$\frac{A}{B} = \frac{p+7}{120} \left(1 + \frac{3}{p} - \frac{6}{p^2} - \frac{28}{p^3} \right).$$

Taking the limit as $p \rightarrow \infty$, we find

$$\lim_{p \rightarrow \infty} \frac{A}{B} = \infty,$$

which implies that the bound A eventually dominates B for sufficiently large p , and therefore provides a strictly better asymptotic estimate for $P(p, 6)$ when p is large and $p - 2$ is not a prime power.

VI. CONCLUSION AND FUTURE WORK

In this paper, we proposed a new constructive lower bound for permutation codes under the Kendall’s τ -metric by leveraging the algebraic structure of dual Reed–Solomon codes. We demonstrated that, for every prime $p > 5$, the dual code of $RS[p, 3]$ has minimum Lee distance 6. Through an established embedding into the symmetric group, this leads to an explicit permutation code of length p and minimum Kendall’s τ -distance 6 with cardinality at least $p!/p^3$.

This result improves upon both the Gilbert–Varshamov bound and prior algebraic bounds in many regimes—particularly when $p - 2$ is not a prime power, where earlier constructions are not applicable.

FUTURE DIRECTIONS

Several open problems and directions emerge from this work:

- **Metric extensions:** It would be valuable to extend this embedding technique to other metrics on permutations, such as the Ulam or Cayley metrics, potentially using alternative algebraic codes.
- **Generalized bounds:** A natural generalization is to investigate whether, for all primes p and positive integers k , the following bound holds:

$$P(p, t) \geq \frac{p!}{p^{p-k-1}}, \quad \text{where } t = \min\{p, 2k\}.$$

This would unify lower bounds across a wider range of code parameters and distances.

REFERENCES

- [1] A. Abdollahi, J. Bagherian, F. Jafari, M. Khatami, F. Parvaresh, and R. Sobhani, “New upper bounds on the size of permutation codes under Kendall τ -metric,” *Cryptogr. Commun.*, vol. 15, no. 5, pp. 891–903, Sep. 2023.
 - [2] A. Barg and A. Mazumdar, “Codes in permutations and error correction for rank modulation,” *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3158–3165, Jul. 2010.
 - [3] S. Buzaglo and T. Etzion, “Bounds on the size of permutation codes with the Kendall τ -metric,” *IEEE Trans. Inf. Theory*, vol. 61, no. 6, pp. 3241–3250, Jun. 2015.
 - [4] D. A. Christie, “Sorting permutations by block-interchanges,” *Inf. Process. Lett.*, vol. 60, no. 4, pp. 165–169, 1996.
 - [5] W. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
 - [6] A. Jiang, M. Schwartz, and J. Bruck, “Correcting charge-constrained errors in the rank-modulation scheme,” *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2112–2120, May 2010.
 - [7] J. Lu and X. Wang, “New results on the reconstruction of permutations distorted by single Kendall τ -errors,” *IEEE Access*, vol. 10, pp. 98761–98768, 2022.
 - [8] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
 - [9] F. Parvaresh, R. Sobhani, A. Abdollahi, J. Bagherian, F. Jafari, and M. Khatami, “Improved bounds on the size of permutation codes under Kendall τ -metric,” *IEEE Trans. Inf. Theory*, vol. 71, no. 6, pp. 4156–4166, Jun. 2025.
 - [10] R. Sobhani, A. Abdollahi, J. Bagherian, and M. Khatami, “A note on good permutation codes from Reed–Solomon codes,” *Des., Codes Cryptogr.*, vol. 87, no. 10, pp. 2335–2340, Oct. 2019.
 - [11] T. Tuller, M. Kupiec, and E. Ruppín, “Reordering of expression determinants in yeast using Kendall’s tau,” *Genome Biol.*, vol. 11, p. R111, Jan. 2010.
 - [12] X. Wang, Y. Zhang, Y. Yang, and G. Ge, “New bounds of permutation codes under Hamming metric and Kendall’s τ -metric,” *Des., Codes Cryptogr.*, vol. 85, no. 3, pp. 533–545, Dec. 2017.
 - [13] X. Wang, Y. Wang, W. Yin, and F.-W. Fu, “Nonexistence of perfect permutation codes under the Kendall τ -metric,” *Des., Codes Cryptogr.*, vol. 89, no. 11, pp. 2511–2531, Nov. 2021.
 - [14] S. Vijayakumaran, “Largest permutation codes with the Kendall τ -metric in S_5 and S_6 ,” *IEEE Commun. Lett.*, vol. 20, no. 10, pp. 1912–1915, Oct. 2016.
 - [15] M. Yaghoobi, S. Haghighi, M. Rahgozar, and M. Asadpour, “User ranking in collaborative tagging systems using a weighted Kendall’s tau distance,” *J. Inf. Sci.*, vol. 38, pp. 313–325, Jan. 2012.
 - [16] Z. Zhang, “A new metric on symmetric groups and applications to block permutation codes,” *Des., Codes Cryptogr.*, vol. 91, no. 6, pp. 2255–2271, Jun. 2023.
- RANA T. SHWAYYEA** obtained the bachelor’s degree from Al-Qadisiyah University, Iraq, in 2002, the Higher Diploma degree in computer science from the Higher Institute of Computers and Informatics, Iraq, in 2005, and the master’s degree in applied mathematics in Egypt, in 2016. She is currently pursuing the Ph.D. degree with the University of Isfahan, Iran. Since 2005, she has been a Faculty Member with the Department of Mathematics, Al-Qadisiyah University, where she was recently appointed as an Assistant Professor. Her research interests are diverse and include numerical analysis, computer networks, numerical equations, and coding theory.
- J. BAGHERIAN** received the B.S. degree in applied mathematics from the University of Kharazmi, Tehran, Iran, in 2002, and the M.S. degree in applied mathematics and the Ph.D. degree in pure mathematics from the Institute for Advanced Studies in Basic Sciences (IASBS), Zanjan, Iran, in 2004 and 2008, respectively. From 2008 to 2016, he was an Assistant Professor with the Mathematics and Computer Science Department, University of Isfahan, Iran, where he has been an Associate Professor, since 2016. He published more than 30 articles. His research interests include scheme theory, graph theory, and permutation codes.
- 
- REZA SOBHANI** received the B.Sc. degree from Isfahan University of Technology, Iran, in 2003, the M.Sc. degree from Sharif University of Technology, Iran, in 2005, and the Ph.D. degree in applied mathematics from Isfahan University of Technology, in 2010. Since 2010, he has been with the Department of Mathematics, University of Isfahan, as a Faculty Member, and he has been an Associate Professor of mathematics with the University of Isfahan, since 2009. He is the author of more than 30 articles. His research interests include algebraic coding theory, combinatorics, and graph theory with applications in communication theory.
- ALIREZA ABDOLLAHI** received the B.Sc., M.Sc., and Ph.D. degrees in mathematics from the University of Isfahan, Iran, in 1996, 1997, and 2000, respectively, and the second Ph.D. degree in mathematics from the Université de Provence, CMI France, in 2001. Since 2001, he has been with the Department of Mathematics, University of Isfahan, as a Faculty Member, and he has been a Professor of mathematics with the University of Isfahan, since 2009. He is the author of more than 120 articles. His research interests include group theory and combinatorics. He was a recipient of the Alkharazmi Young Prize in 1999 and the Sheikh Bahaei Prize in 1999. He also received the “Institute for Studies in Theoretical Physics and Mathematics (IPM)” Young Mathematician Prize of 2005, and he was the Head of the Distinguished Center of Excellence in Basic Sciences selected by the Ministry of Science and Education of Iran in 2010. He is the Editor-in-Chief of *Journal of the Iranian Mathematical Society* and the Founder and the Editor-in-Chief of *International Journal of Group Theory and Transactions on Combinatorics*.

...