Cryptography and Communications
https://doi.org/10.1007/s12095-025-00809-3

RESEARCH

Upper bounds on the size of permutation codes with a Hamming distance of five

Alireza Abdollahi[1] · Javad Bagherian[1] · Fatemeh Jafari[1] · Maryam Khatami[1] · Farzad Parvaresh[2] · Reza Sobhani[3]

Received: 19 June 2024 / Accepted: 19 May 2025

Abstract
In this paper, we study the largest size $A(n, d)$ of permutation codes of length n, i.e., subsets of the set S_n of all permutations on n letters with the minimum distance at least d under the Hamming metric. In Abdollahi et al. (Cryptogr. Commun. **15**, 891–903 2023) we have developed a method using the representation theory of symmetric groups to find upper bounds on the size of permutation codes in S_n with the minimum distance of d under the Kendall τ-metric. The latter method is used for the permutation codes under the metric induced by Cayley graphs of S_n. Since the metric induced by any Cayley graph of S_n is not equivalent to the Hamming metric, we can not use the method for the Hamming metric. In this paper we find a trick by which we can again use the method to find upper bounds for $A(n, 2t + 1)$. We present three practical results that prove the non-existence of perfect 2-error-correcting codes in S_n under the Hamming metric for numerous values of n. Specifically, we prove that 91 and 907 are the only values for $n \leq 1000$ for which S_n may contain a perfect 2-error-correcting code under the Hamming metric. Additionally, we prove that for any integer n such that $n^2 - n + 2$ is divisible by a prime exceeding $n - \lfloor \frac{n}{7} \rfloor$,

$$A(n, 5) \leq \frac{2 \times n!}{n^2 - n + 2} - \frac{20n - 56}{(n^2 - n + 2)\sqrt{698n^2 - 1428n + 1274}} \sqrt{\frac{n!}{(n - \lfloor \frac{n}{7} \rfloor)!}}.$$

The result improves the known upper bounds of $A(n, 5)$ for all integers $n \geq 35$ such that $n^2 - n + 2$ is divisible by a prime exceeding $n - \lfloor \frac{n}{7} \rfloor$.

Keywords Perfect codes · Hamming metric · Permutation codes

Mathematics Subject Classification (2010) 94B25 · 94B65 · 68P30

1 Introduction

Permutation Codes (PCs) are defined as subsets of the symmetric group S_n which consists of all permutations of $[n] := \{1, \ldots, n\}$. The study of PCs originated over 50 years ago with articles such as [10, 11, 16, 19]. In recent years, there has been a resurgence of interest in PCs due to their potential applications in various fields, including power line communications [13, 14, 34], block ciphers [15], multilevel flash memories [3, 23, 24] and DNA storage [4].

Extended author information available on the last page of the article

Published online: 24 May 2025

When a PC is used in a power line communication, its error correction capability depends on its minimum Hamming distance. For any two permutations $\sigma, \tau \in S_n$, the Hamming distance $d_H(\sigma, \tau)$ between σ and τ is defined by $|M(\sigma\tau^{-1})|$, where $M(\alpha) := \{i \in [n] \,|\, \alpha(i) \neq i\}$ for all $\alpha \in S_n$. For $1 \leq d \leq n$, a subset $C \subseteq S_n$ is called a (n, d)-PC under the Hamming metric, if $\min\{d_H(\sigma, \rho) \,|\, \sigma \neq \rho, \sigma, \rho \in S_n\} \geq d$. The largest size of a (n, d)-PC under the Hamming metric is denoted by $A(n, d)$. It is known that $A(n, 1) = A(n, 2) = n!$, $A(n, 3) = \frac{n!}{2}$ and $A(n, n) = n$ (see [18, Lemma 1.1]). These results arise from the permutations of the symmetric group S_n, the alternating group A_n and a single orbit of a cyclic group of order n, respectively. Also, in [19], when q is a prime power, using this fact that the affine general linear group $AGL(1, q)$ is sharply 2-transitive and the projective general linear group $PGL(2, q)$ is sharply 3-transitive, it is proved that $A(q, q-1) = q(q-1)$ and $A(q+1, q-1) = (q+1)q(q-1)$. However, determining $A(n, d)$ is challenging for $4 \leq d \leq n-1$, except in some specific cases. So far, several researchers have presented lower bounds (see, e.g., [5–9, 13, 14, 19, 20, 26, 36]) and upper bounds (see, e.g., [12, 16, 18, 19, 25, 32]) on $A(n, d)$. The goal of this paper is to provide new upper bounds on $A(n, 5)$. As part of this goal, we study perfect 2-error-correcting codes in S_n under the Hamming metric, which we define below.

For a positive integer t, a Hamming ball centered at $\sigma \in S_n$ of radius t in S_n under the Hamming metric, denoted as $\mathcal{B}_n^H(\sigma, t)$, is defined by $\mathcal{B}_n^H(\sigma, t) := \{\alpha \in S_n \,|\, d_H(\sigma, \alpha) \leq t\}$. Notably, the size of a Hamming ball of radius t under the Hamming metric is independent of the ball's center. For convenience, we denote by $\mathcal{B}_n^H(t)$ the size of $\mathcal{B}_n^H(\sigma, t)$.

In the context of the Hamming metric, an $(n, 2t+1)$-PC C of size M serves as a t-error-correcting code. According to the sphere packing bound (see [36, Proposition 3]), we have the inequality $M \cdot \mathcal{B}_n^H(t) \leq n!$. An $(n, 2t+1)$-PC C that achieves this bound, i.e., $M \cdot \mathcal{B}_n^H(t) = n!$, is referred to as a perfect t-error-correcting code or a perfect PC of radius t under the Hamming metric. That is, the balls with a radius of t around the codewords of C partition S_n, meaning that $S_n = \bigcup_{c \in C} \mathcal{B}_n^H(c, t)$, and $\mathcal{B}_n^H(c, t) \cap \mathcal{B}_n^H(c', t) = \varnothing$ for any two distinct $c, c' \in C$.

The study of perfect PCs under the Hamming metric began with Blake's foundational work [10], where he introduced necessary conditions for their existence. More recently, Wang and Yin [35] expanded on this research, demonstrating the non-existence of perfect t-error-correcting codes in S_n under the Hamming metric for various n and t. They concluded, based on $A(n, 3) = \frac{n!}{2}$ and $\mathcal{B}_n^H(\sigma, 1) = \{\sigma\}$, that for $n \geq 3$, S_n does not contain a 1-error-correcting code under the Hamming metric (see [35, Theorem 4.2]). Furthermore, in their work [35], they determined $\mathcal{B}_n^H(2)$ to be $\frac{n^2-n+2}{2}$. By noting that $M = \frac{n!}{\mathcal{B}_n^H(2)}$ must be an integer, they derived the following result:

Theorem 1.1 [35, Theorem 4.3] *There does not exist a perfect 2-error-correcting code in S_n, where $n^2 - n + 2$ has a prime factor $p > n$, or $5 \leq n < 11$, or $12 \leq n \leq 17$.*

We have developed a method in [2] using the representation theory of symmetric groups to obtain upper bounds on the size of PCs of minimum distance d under the Kendall τ-metric. Since this method is suited for PCs under the metrics induced by Cayley graphs of S_n, it cannot be directly applied to the Hamming metric. In this paper, we introduce a new method that makes this approach usable for obtaining upper bounds on $A(n, d)$ (see Lemma 3.3). Regarding the non-existence of perfect 2-error-correcting code in S_n under the Hamming metric, we present three results below. We improve Theorem 1.1 as follows.

Theorem 1.2 *Let n and r be integers such that $r \leq \frac{n}{5}$. If $\frac{n^2-n+2}{2}$ is divisible by a prime exceeding $n-r$, then there does not exist a perfect 2-error-correcting code in S_n under the Hamming metric.*

The following result is obtained by using the main result of [29] and improves Theorems 1.1 and 1.2.

Theorem 1.3 *If $\frac{n^2-n+2}{2}$ is divisible by a prime exceeding $\sqrt{n}+2$, then there does not exist a perfect 2-error-correcting code in S_n under the Hamming metric.*

By a number partition λ of n with length m we mean an m-tuple $(\lambda_1, \ldots, \lambda_m)$ of positive integers such that $\lambda_1 \geq \cdots \geq \lambda_m$ and $n = \sum_{i=1}^{m} \lambda_i$. Also, by using the representation theory of symmetric groups, we prove the following practical result.

Theorem 1.4 *Suppose that n is an integer such that it admits a partition $\Lambda = (\lambda_1, \ldots, \lambda_m)$ with the following property:*

(1) $\frac{1}{2}\sum_{j=1}^{m}[(\lambda_j - j)(\lambda_j - j + 1) - j(j-1)] > -1$,
(2) $2\frac{\lambda_1! \cdots \lambda_m!}{n^2-n+2}$ *is not integer.*

Then S_n contains no perfect 2-error-correcting code under the Hamming metric.

Note that according to [35, Theorem 4.3], the existence or non-existence of a perfect 2-error-correcting code in S_n under the Hamming metric remains unproven for a significant number of cases, including 217 cases for $n \leq 1000$ (17 cases for $n \leq 100$). However, by utilizing Theorems 1.3 and 1.4, we can establish the non-existence of perfect 2-error-correcting codes in S_n under the Hamming metric for very large values of n. So as a result we can give the following corollary.

Corollary 1.5 *The numbers 91 and 907 are the only cases for $n \leq 1000$ for which it is possible that S_n contains a perfect 2-error-correcting code under the Hamming metric.*

We observe that, based on the results presented in [12, 16, 25, 32] (see also [31, Table 2]), the upper bound of $A(n, 5)$ is significantly improved when $n \leq 14$ compared to the sphere packing bound. Thus, the non-existence of a 2-error-correcting code in S_n is evident for these cases. However, for $n \geq 15$, the best known upper bound for $A(n, 5)$ is the sphere packing bound (see also [19, Theorem 4]). Note that Theorem 1.1 does not reduce the upper bound for $A(n, 5)$, as its proof relies on when $M = \frac{n!}{\mathcal{B}_n^H(2)}$ is not an integer. However, in cases where n holds true in Theorems 1.3 and 1.4 and $\frac{2n!}{n^2-n+2}$ is an integer, the upper bound for $A(n, 5)$ decreases by one. So as a result we can give the following corollary.

Corollary 1.6 *If $\frac{n^2-n+2}{2}$ is divisible by a prime exceeding $\sqrt{n}+2$ and $\frac{2n!}{n^2-n+2}$ is an integer, then $A(n, 5) \leq \frac{2n!}{n^2-n+2} - 1$.*

By Corrollary 1.6, the upper bound of $A(n, 5)$ is improved by one for the special cases of n such as $n \in \{18, 27, 37, 38, 46\}$. Here we prove an additional upper bound on $A(n, 5)$ as follows.

Theorem 1.7 *Let n be an integer such that $n^2 - n + 2$ is divisible by a prime exceeding $n - \lfloor \frac{n}{7} \rfloor$. Then*

$$A(n,5) \leq \frac{2 \times n!}{n^2-n+2} - \frac{20n-56}{(n^2-n+2)\sqrt{698n^2-1428n+1274}}\sqrt{\frac{n!}{(n-\lfloor \frac{n}{7} \rfloor)!}}.$$

Note that, as we show in Corollary 4.6, the set of integers n for which Theorem 1.7 provides an improved upper bound for $A(n, d)$ is infinite. The following result shows that Theorem 1.7 improves the upper bound of $A(n, 5)$ for all $n \geq 35$ such that such that $n^2 - n + 2$ is divisible by a prime greater than $n - \lfloor \frac{n}{7} \rfloor$.

Corollary 1.8 *Let $n \geq 35$ be an integer such that $n^2 - n + 2$ is divisible by a prime exceeding $n - \lfloor \frac{n}{7} \rfloor$. Then*

$$A(n, 5) < \frac{2 \times n!}{n^2 - n + 2} - 3.334 \times (n - \lfloor \frac{n}{7} \rfloor + 1)^{\frac{\lfloor \frac{n}{7} \rfloor - 5}{2}}.$$

It is worth noting that the upper bound for $A(n, 5)$ obtained in Theorem 1.7 is significantly better than the upper bound provided in Corollary 1.8. For example, Theorem 1.7 reduces the upper bounds of $A(56, 5)$ and $A(63, 5)$ by 1830 and 17435, respectively. However, Corollary 1.8 reduces the upper bounds of $A(56, 5)$ and $A(63, 5)$ by 812 and 10085, respectively.

2 Preliminaries

In this paper, we will adhere to the definitions and notations provided in [2]. For the reader's convenience, this section includes a summary of these notations and definitions. Additionally, we prove Theorem 2.12 (below), which is essential for proving Theorem 1.4.

Definition 2.1 Let G be a finite group, and let B and C be two non-empty subsets of G. The product of B and C, denoted by BC, is defined as $\{bc \mid b \in B, c \in C\}$, where by bc we refer to the group operation. Additionally, for any $g \in G$, the product of B and the singleton set $\{g\}$ is denoted by Bg. Moreover, for any integer $r \geq 1$, the product of B with itself r times, denoted by B^r, is defined as $B^r := \{b_1 b_2 \dots b_r \mid b_1, b_2, \dots, b_r \in B\}$. A subset B of G is called *inverse closed* if $B = B^{-1} := \{b^{-1} \mid b \in B\}$. The identity element of G is denoted by ξ.

A *simple graph* Γ consists of a non-empty set of vertices $V(\Gamma)$ and a possibly empty set of edges $E(\Gamma)$, forming a subset of all 2-element subsets of $V(\Gamma)$. Two vertices σ_1 and σ_2 are called adjacent, denoted by $\sigma_1 \sim \sigma_2$, if $\{\sigma_1, \sigma_2\} \in E(\Gamma)$.

Consider a finite group G and a non-empty inverse closed subset S of G such that $\xi \notin S$. Then the *Cayley graph* $\Gamma := \mathrm{Cay}(G, S)$ is a simple graph with $V(\Gamma) = G$ and $E(\Gamma) = \left\{\{g, h\} \,\middle|\, g, h \in G, gh^{-1} \in S\right\}$. Subsequently, a metric d_Γ is stablished on G by Γ, representing the shortest path length between two vertices in $\mathrm{Cay}(G, S)$.

Definition 2.2 Consider G a finite group and S a non-empty inverse-closed subset of G such that $\xi \notin S$. For a positive integer r and an element $g \in G$, we use the notation $\mathcal{B}_r^S(g)$ to denote the *ball* of radius r in G under the metric d_Γ induced by the Cayley graph $\Gamma := \mathrm{Cay}(G, S)$, defined as $\mathcal{B}_r^S(g) := \{h \in G \mid d_\Gamma(g, h) \leq r\}$.

Remark 2.3 [2, Remark 2.6] Notice that $\mathcal{B}_r^S(g) = (S \cup \{\xi\})^r g$, for all $g \in G$, and therefore, $|\mathcal{B}_r^S(g)| = |\mathcal{B}_r^S(\xi)| = |(S \cup \{\xi\})^r|$.

Definition 2.4 Consider a finite group G and a non-empty inverse closed subset S of G such that $\xi \notin S$. Let d_Γ be the metric induced by $\mathrm{Cay}(G, S)$. A subset $C \subseteq S_n$ is termed an (n, d)-PC under the metric d_Γ, if $\min\{d_\Gamma(\sigma, \rho) \mid \sigma \neq \rho, \sigma, \rho \in S_n\} \geq d$. Additionally, an *r-perfect code* or a *perfect code of radius r* of G under the metric d_Γ is a subset C of G such that $G = \cup_{c \in C} \mathcal{B}_r^S(c)$ and $\mathcal{B}_r^S(c) \cap \mathcal{B}_r^S(c') = \varnothing$ for any two distinct $c, c' \in C$.

Definition 2.5 [2, Definition 2.10] Let G be a group and Θ be a non-empty set.

- We say G acts on Θ (from the right) if there exists a function $\Theta \times G \to \Theta$ denoted by $(\theta, g) \mapsto \theta^g$ for all $(\theta, g) \in \Theta \times G$ if $(\theta^g)^h = \theta^{gh}$ and $\theta^\xi = \theta$ for all $\theta \in \Theta$ and all $g, h \in G$.
- For any $\theta \in \Theta$ the set $\mathrm{Stab}_G(\theta) := \{g \in G \mid \theta^g = \theta\}$ is called the stabilizer of θ in G, which is a subgroup of G.
- If the action is transitive (i.e., for any two elements $\theta_1, \theta_2 \in \Theta$, there exists $g \in G$ such that $\theta_1^g = \theta_2$), all stabilizers are conjugate under the elements of G, more precisely $g^{-1}\,\mathrm{Stab}_G(\theta_1)g = \mathrm{Stab}_G(\theta_2)$ whenever $\theta_1^g = \theta_2$.
- Suppose that G acts on Θ and $|\Theta| = k$ is finite. Fix an arbitrary ordering on the elements of Θ so that $\theta_i < \theta_j$ whenever $i < j$ for distinct elements $\theta_i, \theta_j \in \Theta$. Denote by ρ_Θ^G the map from G to $\mathrm{GL}_k(\mathbb{Z})$ (the group of all $k \times k$ invertible matrices with integer entries) defined by $g \mapsto P_g$, where P_g is the $|\Theta| \times |\Theta|$ matrix whose (i, j) entry is 1 if $\theta_i^g = \theta_j$ and 0 otherwise.

Definition 2.6 Let G be a finite group and k be a positive integer. A group homomorphism ρ from G to the general linear group $\mathrm{GL}_k(\mathbb{C})$, which consists of $k \times k$ invertible matrices over $\mathbb{C}$, is called a (complex) representation of G with dimension k.

Definition 2.7 The (complex) representation ρ of a finite group G with dimension k is called irreducible if it is impossible to find a matrix $P \in \mathrm{GL}_k(\mathbb{C})$ and positive integeres $k_1, \ldots, k_m$, $m \geq 2$, such that $\sum_{i=1}^m k_i = k$ and for all $g \in G$, $P^{-1}\rho(g)P$ has the form

$$\begin{pmatrix} A_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & A_m \end{pmatrix}, \tag{2.1}$$

where for each $1 \leq i \leq m$, $A_i \in GL_{k_i}(\mathbb{C})$.

Definition 2.8 The character χ_ρ of the representation ρ is a function from G to the complex numbers, defined as $\chi_\rho(\sigma) = \mathrm{Tr}[\rho(\sigma)]$, where Tr denotes the trace operation. The trace of a square matrix A is the sum of its diagonal elements. The character χ_ρ is called irreducible if ρ is irreducible.

Definition 2.9 For any subset X of a finite group G, the notation $\hat{X}$ refers to the element $\sum_{x \in X} x$ in the complex group algebra $\mathbb{C}[G]$ (see [2, P. 3-4]). Also $\widehat{X^{\rho_\Theta^G}}$ refers to the element $\sum_{x \in X} x^{\rho_\Theta^G}$ which is an element of $\mathrm{GL}_k(\mathbb{Z})$, where ρ_Θ^G is the representation of G obtained from the action of G on a non-empty set Θ of size k [2, Definition 2.10 and Remarks 2.11 and 2.12]).

Remark 2.10 Let H be a subgroup of a finite group G and X be the set of right cosets of H in G, i.e., $X := \{Hg \mid g \in G\}$. Then G acts transitively on X via $(Hg, g_0) \longrightarrow Hgg_0$. It is known that X partitions G, i.e., $G = \cup_{x \in X} x$ and $x \cap x' = \varnothing$ for all distinct elements x and x' of X, and $|X| = |G|/|H|$.

Definition 2.11 According to [2, Definition 3.1 and Remark 3.2], the Young subgroup corresponding to a partition $(\lambda_1, \ldots, \lambda_m)$ of a positive integer n refers to the subgroup H of S_n defined as $H := S_{\Delta_1} \times \cdots \times S_{\Delta_m} = \{\sigma_1 \cdots \sigma_m \mid \sigma_i \in S_{\Delta_i}, 1 \leq i \leq m\}$, where $(\Delta_1, \ldots, \Delta_m) = (\{1, \ldots, \lambda_1\}, \{\lambda_1 + 1, \ldots, \lambda_1 + \lambda_2\}, \ldots, \{n - \lambda_m + 1, \ldots, n\})$, and S_{Δ_i} denotes the symmetric group on the set Δ_i for all $i = 1, \ldots, m$. Furthermore, if λ and μ are

two partitions of n, we say that λ dominates μ, denoted as $\lambda \trianglerighteq \mu$, if $\sum_{i=1}^{j} \lambda_i \geq \sum_{i=1}^{j} \mu_i$ holds for all j.

Theorem 2.12 *Let G be a finite group, S be an inverse closed set not containing the identity and $C \subset G$ be an r-perfect code under the metric induced by $Cay(G, S)$. Suppose that G acts transitively on a finite set X. If $\sum_{b\in(S\cup\{\xi\})^r} b^{\rho_X^G}$ is invertible, then $|\{h \in C \mid x^h = y\}| = \frac{|Stab_G(z)|}{|(S\cup\{\xi\})^r|}$ for any three elements $x, y, z \in X$.*

Proof Denote ρ_X^G by ρ, $|(S \cup \{\xi\})^r|$ by τ and the constant $|Stab_G(x)|$ (for all $x \in X$) by κ.

In view of [2, Remark 2.9], since C is a r-perfect code, $\hat{T}\hat{C} = \hat{G}$, where $T := (S \cup \{\xi\})^r$. Apply ρ on latter (see [2, Equation 2.3]). In view of the last part of Definitions 2.5 and 2.9, the (i, j) entry of $\sum_{g\in G} g^\rho$ is $|\{g \in G \mid x_i^g = x_j\}|$ for any two elements x_i and x_j of X. If the latter cardinality is not zero, it is $|Stab_G(x_i)f|$ for any $f \in \{g \in G \mid x_i^g = x_j\}$. Note that $|Stab_G(x_i)f| = |Stab_G(x_i)|$. Now $\sum_{g\in G} g^\rho = \kappa\mathbf{J}$, where $\mathbf{J}$ is the $|X| \times |X|$ matrix all of whose entries are 1.

Denote the matrix $\sum_{b\in(S\cup\{\xi\})^r} b^\rho$ by $\mathbf{B}$. It follows that

$$\mathbf{B}\mathbf{C}_\ell = \kappa\mathbf{j}, \tag{2.2}$$

where $\mathbf{C}_\ell$ is the ℓth column of $\sum_{c\in C} c^\rho$ and $\mathbf{j}$ is any column of $\mathbf{J}$. Since the sum of each row of the matrix $\mathbf{B}$ is τ, we have $\mathbf{B}\mathbf{j} = \tau\mathbf{j}$. Thus $\mathbf{B}\left(\frac{\kappa}{\tau}\mathbf{j}\right) = \kappa\mathbf{j}$. Since $\mathbf{B}$ is invertible, it follows that $\mathbf{C}_\ell = \frac{\kappa}{\tau}\mathbf{j}$. Thus (i, j) entry of $\mathbf{C}$ is

$$|\{c \in C \mid x_i^c = x_j\}| = \frac{\kappa}{\tau}$$

for all i, j. This completes the proof. □

3 Non-existence of perfect 2-error-correcting codes

In this section, we will prove Theorems 1.2, 1.4 and 1.3. First, in Lemma 3.3 (below), we show that the non-existence of 1-perfect codes in S_n under the metric induced by $Cay(S_n, \mathfrak{S}_t^{n\#})$ (see Definition 3.1, below) is equivalent to the non-existence of perfect t-error-correcting codes in S_n under the Hamming metric. After that, using the method we developed in [2], we prove Theorems 1.2 and 1.4. Finally, by utilizing the main result of [29], we prove Theorem 1.3.

Throughout this paper, for a permutation $\pi \in S_n$, we employ the vector notation of π as $[\pi(1), \pi(2), \ldots, \pi(i), \pi(i + 1), \ldots, \pi(n)]$. The composition of two permutations π and σ in S_n, denoted by $\sigma\pi$, is defined as $\sigma\pi(i) = \pi(\sigma(i))$ for all $i \in [n]$. For distinct elements $i, j \in [n]$, (i, j), which is called transposition, is the permutation obtained from exchanging i and j in ξ.

Definition 3.1 Let t be an integer. We denote by $\mathfrak{S}_t^n$ and $\mathfrak{S}_t^{n\#}$ the sets $\{\sigma \in S_n \mid |M(\sigma)| \leq t\}$ and $\mathfrak{S}_t^n \setminus \{\xi\}$, respectively. Note that since $M(\sigma) = M(\sigma^{-1})$ for all $\sigma \in S_n$, $\mathfrak{S}_t^n$ is an inverse closed subset of S_n.

Remark 3.2 According to Definition 3.1, it is clear that for each $\tau \in S_n$ and $1 \leq t \leq n$, $\mathcal{B}_n^H(\tau, t) = \mathfrak{S}_t^n\tau$ and also $\mathfrak{S}_2^n$ is the set consisting of the identity and all transpositions in S_n.

The following lemma helps us to use the method we developed in [2] to find the upper bound of $A(n,5)$ and to prove the non-existence of perfect 2-error-correcting codes in S_n under the Hamming metric for some values of n.

Lemma 3.3 *Let $2 \leq t \leq \frac{n}{2}$ be an integer and d_Γ be the metric induced by the graph $\Gamma = Cay(S_n, \mathfrak{S}_t^{n\#})$. If $C \subseteq S_n$ is an $(n, 2t+1)$-PC under the Hamming metric, then C is an $(n,3)$-PC under the metric d_Γ. In particular, if C is a perfect t-error-correcting code in S_n under the Hamming metric, then C is an 1-perfect code in S_n under the metric d_Γ.*

Proof Let $S := \mathfrak{S}_t^{n\#}$. In View of Remark 2.3, $B_1^S(\tau) = \mathfrak{S}_t^n \tau$ for all $\tau \in S_n$. Also by Remark 3.2, $\mathcal{B}_n^H(\tau, t) = \mathfrak{S}_t^n \tau$ and so $B_1^S(\tau) = \mathcal{B}_n^H(\tau, t)$ for all $\tau \in S_n$. Let C be an $(n, 2t+1)$-PC under the Hamming metric. Suppose that c and c' are two distinct elements of C such that there exists $\sigma \in \mathcal{B}_n^H(c,t) \cap \mathcal{B}_n^H(c',t)$. Then it follows from the triangle inequality, $d_H(c,c') \leq d_H(c,\sigma) + d_H(c',\sigma) \leq 2t$ that is a contradiction. So $\mathcal{B}_n^H(c,t) \cap \mathcal{B}_n^H(c',t) = \varnothing$ for all distinct elements $c, c' \in C$. Hence, $\mathcal{B}_1^S(c) \cap \mathcal{B}_1^S(c') = \varnothing$ for all distinct elements $c, c' \in C$. Now suppose on the contrary that there exist distinct elements c and c' in C such that $d_\Gamma(c,c') < 3$. If $d_\Gamma(c,c') = 1$, then $\{c, c'\} \subseteq \mathcal{B}_1^S(c) \cap \mathcal{B}_1^S(c')$ that is a contradiction. If $d_\Gamma(c,c') = 2$, then there exists $\sigma_0 \in S_n$ such that $c \sim \sigma_0 \sim c'$ is the shortest path in the graph Γ between c and c'. So $\sigma_0 \in \mathcal{B}_1^S(c) \cap \mathcal{B}_1^S(c')$ that is a contradiction. Therefore, C is an $(n,3)$-PC under the metric d_Γ. This completes the proof of first part. The proof of the second part follow from the definitions of perfect t-error-correcting codes in S_n under the Hamming metric and 1-perfect codes in S_n under the metric d_Γ and the fact that $B_1^S(\tau) = \mathcal{B}_n^H(\tau, t)$ for all $\tau \in S_n$. This completes the proof. □

Lemma 3.4 *Let H be the Young subgroup of S_n corresponding to the partition $\lambda := (n-r, \underbrace{1, \ldots, 1}_{r})$ and X be the set of right cosets of H in S_n. Then $\widehat{(\mathfrak{S}_2^n)^{\rho_X^{S_n}}}$ is a symmetric matrix $A = (a_{ij})_{\ell \times \ell}$, where $\ell = \frac{n!}{(n-r)!}$, with the following properties:*

(1) $a_{ii} = \frac{(n-r)(n-r-1)+2}{2}$ *for all* $i \in [\ell]$.
(2) $a_{ij} \in \{0,1\}$ *for all distinct elements* $i, j \in [\ell]$.
(3) $\sum_{j=1}^{\ell} a_{ij} = \frac{n^2-n+2}{2}$ *for all* $i \in [\ell]$.

Proof In view of [2, Remark 3.2], without loss of generality we may assume that λ is the partition $\{[n-r], \{n-r+1\}, \{n-r+2\}, \ldots, \{n\}\}$ of n and therefore $H \cong S_{n-r}$. Let $\mathcal{F} := \{(f_1, f_2, \ldots, f_r) \in [n]^r \mid \forall\, i \neq j,\ f_i \neq f_j\}$. Corresponding to each ordered r-tuple $F = (f_1, \ldots, f_r) \in \mathcal{F}$, let $S_n^F := \{\sigma \in S_n \mid \sigma(n-r+1) = f_1, \sigma(n-r+2) = f_2, \ldots, \sigma(n) = f_r\}$. It is easy to see that $S_n^F = H\sigma$ for each $\sigma \in S_n^F$. So S_n^F is a right coset of H in S_n. Further, if F and $\bar{F}$ are two distinct elements of $\mathcal{F}$, then it is clear that $S_n^F \cap S_n^{\bar{F}} = \varnothing$. Hence, it follows from $|\mathcal{F}| = \ell$ and Remark 2.10 that $X = \{S_n^F \mid F \in \mathcal{F}\}$ is the set of all right cosets of H in S_n. Suppose that $F_1, F_2, \ldots, F_\ell$ are all ordered r-tuples in $\mathcal{F}$. Fix the ordering of X such that $S_n^{F_i} < S_n^{F_j}$ if $i < j$, for all $i, j \in [\ell]$. In view of Definition 2.5, the (i,j) entry of $\widehat{(\mathfrak{S}_2^n)^{\rho_X^{S_n}}}$ is equal to $|\mathcal{O}_{ij}|$, where $\mathcal{O}_{ij} := \{t \in \mathfrak{S}_2^n \mid S_n^{F_i} t = S_n^{F_j}\}$. Since $\mathcal{O}_{ij} = \mathcal{O}_{ji}$ for all $i, j \in [\ell]$, A is a symmetric matrix. Let $(i,j) \in \mathfrak{S}_2^n$ and let $F = (f_1, \ldots, f_r)$ and $\bar{F} = (\bar{f}_1, \ldots, \bar{f}_r)$ be two distinct elements of $\mathcal{F}$. The sufficient condition for $S_n^F(i,j) = S_n^F$ is $\{i,j\} \cap \{f_1, \ldots, f_r\} = \varnothing$. So it follows from $S_n^F \xi = S_n^F$ that $a_{ss} = \frac{(n-r)(n-r-1)}{2} + 1$ for all $s \in [\ell]$. Suppose on the contrary that there exists $(i', j') \in \mathfrak{S}_2^n \setminus \{(i,j)\}$ such that $S_n^F(i,j) = S_n^{\bar{F}} = S_n^F(i', j')$. Since $F \neq \bar{F}$ we have $P_1 := \{f_1, \ldots, f_r\} \cap \{i,j\} \neq \varnothing$ and

$P_2 := \{f_1, \ldots, f_r\} \cap \{i', j'\} \neq \varnothing$. Suppose that $f_m \in P_1$ for some $m \in [r]$. Then since $\{i, j\} \neq \{i', j'\}$, $\big(\sigma(i, j)\big)(n - r + m) \neq \big(\sigma(i', j')\big)(n - r + m)$, for all $\sigma \in S_n^F$. Hence, $S_n^F(i, j) \neq S_n^F(i', j')$ that is a contradiction. Therefore, $a_{ij} \in \{0, 1\}$ for all distinct elements $i, j \in [\ell]$. Note that for each $x \in [\ell]$, since $\cup_{y=1}^{\ell} \mathcal{O}_{xy} = \mathfrak{S}_2^n$ and $\mathcal{O}_{xy} \cap \mathcal{O}_{xy'} = \varnothing$ for all $y \neq y' \in [\ell]$, we have $\sum_{j=1}^{\ell} a_{ij} = \frac{n^2-n}{2} + 1$ for all $i \in [\ell]$. This completes the proof. □

Proof of Theorem 1.2 Let H be the Young subgroup of S_n corresponding to the partition $\lambda := (n - r, \underbrace{1, \ldots, 1}_{r})$ and X be the set of right cosets of H in S_n. Suppose on the contrary that C is an 1-perfect code in S_n under the metric d_Γ, where d_Γ is the metric induced by the graph $\Gamma = Cay(S_n, \mathfrak{S}_2^{n\#})$. So, in view of [2, Remark 2.9 and Equation 2.3], we have

$$\Big(\sum_{s \in \mathfrak{S}_2^n} s^{\rho_X^{S_n}}\Big)\Big(\sum_{c \in C} c^{\rho_X^{S_n}}\Big) = \sum_{g \in S_n} g^{\rho_X^{S_n}}. \tag{3.1}$$

Suppose that $X = \{Ha_1, \ldots, Ha_\ell\}$, where $\ell = \frac{n!}{(n-r)!}$. Without loss of generality, we may assume that $a_1 = \xi$. We fix the ordering $Ha_i < Ha_j$ whenever $i < j$. By [2, Lemma 2.13], the (i, j) entry of $\sum_{g \in S_n} g^{\rho_X^{S_n}}$ is equal to $|S_n \cap {a_i}^{-1} Ha_j|$ and since ${a_i}^{-1} Ha_j \subseteq S_n$, the (i, j) entry of $\sum_{g \in S_n} g^{\rho_X^{S_n}}$ is equal to $|{a_i}^{-1} Ha_j| = |H|$. So if $\boldsymbol{\beta}$ is a column of $\sum_{g \in S_n} g^{\rho_X^{S_n}}$, then $\boldsymbol{\beta} = |H|\mathbf{1} = (n - r)!\mathbf{1}$. Let $\boldsymbol{\rho}$ be the first column of $\sum_{c \in C} c^{\rho_X^{S_n}}$. Then [2, Lemma 2.13] implies that for all $1 \leq i \leq \ell$, i-th row of $\boldsymbol{\rho}$, denoted by ρ_i, is equal to $|C \cap Ha_i|$. Since $C = C \cap S_n = \cup_{i=1}^{\ell}(C \cap Ha_i)$ and $(C \cap Ha_i) \cap (C \cap Ha_j) = \varnothing$ for all $i \neq j$, $\sum_{i=1}^{\ell} \rho_i = |C|$. Therefore $\boldsymbol{\rho}$ is an integer solution for the following system of equations

$$\mathbf{A}(x_1, \ldots, x_\ell)^t = |H|\mathbf{1} = (n - r)!\mathbf{1}, \tag{3.2}$$

where $\mathbf{A} := \widehat{(\mathfrak{S}_2^n)^{\rho_X^{S_n}}}$ and $\mathbf{1}$ is the column vector of order $\ell \times 1$. It follows from Lemma 3.4 that $\mathbf{A}$ is a matrix of dimension $\ell \times \ell$, with properties specified in parts (1), (2) and (3). Clearly, $\boldsymbol{\alpha} = \frac{2(n-r)!}{n^2-n+2}\mathbf{1}$ is a solution for the the system of (3.2). It follows from Lemma 3.4 that, for all $1 \leq i \leq \ell$, $a_{ii} = \frac{(n-r)(n-r-1)+2}{2}$ and $\sum_{j=1, i \neq j}^{\ell} a_{ij} = \frac{n^2-n+2}{2} - \frac{(n-r)(n-r-1)+2}{2}$. So $r \leq \frac{n}{5}$ implies that $a_{ii} > \sum_{j=1, i \neq j}^{\ell} a_{ij}$ for all $1 \leq i \leq \ell$. Therefore, in view of Levy-Desplanques Theorem [21, p. 125], $\mathbf{A}$ is a non-singular matrix. Hence $\boldsymbol{\alpha}$ is the only solution for the the system of (3.2). On the other hands, since $\frac{n^2-n+2}{2}$ is divisible by a prime exceeding $n - r$, $\boldsymbol{\alpha}$ is not integer vector and so the system of (3.2) has not solution that is contradiction. Then S_n contains no 1-perfect code under the metric d_Γ and so the result follows from Lemma 3.3. This completes the proof. □

Definition 3.5 Let χ be a character of S_n and let τ be a transposition in S_n. We define $\lambda_\chi := \frac{n(n-1)}{2\chi(\xi)}\chi(\tau)$.

Theorem 3.6 *Let n be a positive integer. Assume that n admits a partition Λ such that $\frac{n^2-n+2}{2}$ does not divide the size of the Young subgroup of Λ and $\lambda_\chi > -1$ for the irreducible character χ corresponding to the partition Λ. Then $Cay(S_n, \mathfrak{S}_2^{n\#})$ has no 1-perfect code.*

Proof Let H be the Young subgroup of S_n corresponding to the partition Λ and X be the set of right cosets of H in S_n. In view of Definition 2.5 and Remark 2.10, since the action of S_n on X is transitive, $|Stab_{S_n}(Hx)| = |H|$, for all right coset $Hx \in X$. Since $\mathfrak{S}_2^{n\#}$ is the set of

all transpositions in S_n, $|\mathfrak{S}_2^n| = \frac{n^2-n+2}{2}$. So if we prove that $\widehat{(\mathfrak{S}_2^n)^{\rho_X^{S_n}}}$ is invertible, then since $|\mathfrak{S}_2^n| \nmid |Stab_{S_n}(Hx)|$ for some right coset $Hx \in X$, Theorem 2.12 completes the proof.

It is known that each irreducible representation appearing in the decomposition of $\rho_X^{S_n}$ into irreducible representations are equivalent to the irreducible representation $\rho_{\Lambda'}$ of S_n corresponding to some partition Λ' of n such that $\Lambda' \trianglelefteq \Lambda$ (see [22, Corollary 2.2.22]). It follows from [17, Lemma 10] that $\lambda_{\chi_{\Lambda'}} \geq \lambda_\chi > -1$, where $\chi_{\Lambda'}$ is the character corresponding to $\rho_{\Lambda'}$. Since all transpositions are conjugate in S_n (i.e., for any two transpositions $\sigma, \pi \in S_n$, there exists $\rho \in S_n$ such that $\sigma = \rho^{-1}\pi\rho$) it follows from [17, Lemma 5] that $\widehat{(\mathfrak{S}_2^n)^{\rho_{\Lambda'}}} = (1 + \lambda_{\chi_{\Lambda'}})I$, where I denotes the identity matrix. Therefore $\widehat{(\mathfrak{S}_2^n)^{\rho_X^{S_n}}}$ is invertible and this completes the proof. □

Proof of Theorem 1.4 It follows from [17, Lemma 7] that for any transposition $\tau \in S_n$ and any irreducible character χ of S_n corresponding to the partition $\Lambda = (\lambda_1, \ldots, \lambda_m)$, we have

$$\frac{\chi(\tau)}{\chi(\xi)} = \frac{1}{n(n-1)} \sum_{j=1}^{m} [(\lambda_j - j)(\lambda_j - j + 1) - j(j-1)].$$

Therefore, if Λ is a partition with property (1) in the hypothesis and χ is the irreducible character of S_n corresponding to the partition Λ, then $\lambda_\chi > -1$. Let H be the Young subgroup of S_n corresponding to the partition Λ. Since $|H| = \lambda_1! \cdots \lambda_m!$, it follows from Theorem 3.6 that there is no 1-perfect code in $Cay(S_n, \mathfrak{S}_2^{n\#})$. So the result follows from Lemma 3.3 and this completes the proof. □

Definition 3.7 [29] Let G be a group and T be a non-empty subset of G. We say that T divides G if and only if G contains a subset S such that every element of G has a unique representation as ts with $t \in T$ and $s \in S$, where by ts we refer to the group operation, in which case we write $G = T \cdot S$.

Lemma 3.8 *If C is a perfect t-error-correcting code in S_n under the Hamming metric, then $S_n = \mathfrak{S}_t^n \cdot C$.*

Proof Since C is a perfect t-error-correcting code in S_n under the Hamming metric, for every element $\sigma \in S_n$, there exists a unique element $c \in C$ such that $\sigma \in \mathcal{B}_n^H(c, t)$. Now Remark 3.2 implies that there exists a unique element $s \in \mathfrak{S}_t^n$ such that $\sigma = sc$ and this completes the proof. □

Remark 3.9 The result of Lemma 3.8 can be generalized to any group G equipped with a right-invariant metric d, i.e., $d(xh, yh) = d(x, y)$ for all $x, y, h \in G$. By the right-invariance of d, the metric ball centered at $c \in G$ with radius t can be expressed as $B(c, t) := \{g \in G \mid d(c, g) \leq t\} = B(\xi, t)c$. Using a similar argument as in the proof of Lemma 3.8, it follows that if C is a t-perfect code in G under the metric d, then $G = B(\xi, t) \cdot C$. Where a t-perfect code in G under d is a subset $C \subseteq G$ such that $G = \bigcup_{c \in C} B(c, t)$ and $B(c_1, t) \cap B(c_2, t) = \varnothing$ for all $c_1 \neq c_2$.

Theorem 3.10 [29] *Let T be the set consisting of the identity and all transpositions in S_n. If $\frac{n^2-n+2}{2}$ is divisible by a prime exceeding $\sqrt{n} + 2$, then T does not divide S_n.*

We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3 Since $\mathfrak{S}_2^n$ is the set consisting of the identity and all transpositions in S_n, the result follows from Theorem 3.10 and Lemma 3.8. This completes the proof. □

Lemma 3.11 *If $n \in \{6, 137, 733\}$, then S_n contains no perfect 2-error-correcting code under the Hamming metric.*

Proof If $n = 6$, 137 and 733, respectively, then consider the partition Λ as $[3, 3]$, $[21, 21, \underbrace{10, \ldots, 10}_{9}, 5]$ and $[57, 57, \underbrace{28, \ldots, 28}_{22}, 3]$. Then Λ satisfies Theorem 1.4 and this completes the proof. □

We now prove Corollary 1.5.

Proof of Corollary 1.5 In light of Theorem 1.3, we find that $n = 6$, 91, 137, 733, and 907 are the only values for $n \leq 1000$ where it is possible for S_n to contain a perfect 2-error-correcting code under the Hamming metric. Furthermore, according to Lemma 3.11, if $n \in 6, 137, 733$, then S_n does not contain a perfect 2-error-correcting code under the Hamming metric. This completes the proof. □

4 New upper bound of $A(n, 5)$

In this section, we prove Theorem 1.7. For the latter, we use a method similar to the one we used in [27] to find an upper bound for the size of the largest PC with a minimum Kendall τ-distance of 3. Here, we provide some notations used in the proof of Theorem 1.7. The transposition of a matrix or vector is denoted by $\cdot^t$. The inner product of two vectors $\mathbf{x} = (x_1, \ldots, x_n)^t$ and $\mathbf{y} = (y_1, \ldots, y_n)^t$ in $\mathbb{R}^n$ is defined as $\langle \mathbf{x}, \mathbf{y} \rangle := \mathbf{x}^t\mathbf{y} = \sum_{i=1}^{n} x_i y_i$, the notation $\| \mathbf{x} \| := \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$ denotes the 2-norm of vector $\mathbf{x}$ and the notation $\| \mathbf{x} \|_1 := \sum_{i=1}^{n} |x_i|$ denotes the 1-norm of vector $\mathbf{x}$, where $|a|$ denotes the absolute value of real number a.

Definition 4.1 [30] A polyhedral cone is a subset $\mathcal{C} \subset \mathbb{R}^n$ of the form $\mathcal{C} := \{\mathbf{x} \in \mathbb{R}^n \mid A\mathbf{x} \leq \mathbf{0}\}$, for a matrix $A \in \mathbb{R}^{m \times n}$ and column vector $\mathbf{0}$ of order $m \times 1$ whose entries are equal to 0.

Remark 4.2 [27, Remark V.3] Let $\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n \mid A\mathbf{x} \leq \mathbf{0}\}$ be a polyhedral cone for a non-singular matrix $A \in \mathbb{R}^{n \times n}$. In view of [30, p. 104-105], the vector $\mathbf{d} \in \mathbb{R}^n$ is called an extreme ray of C, if there exists $1 \leq i \leq n$ such that $A_i\mathbf{d} = \mathbf{0}$ and $a_i\mathbf{d} \leq 0$, where a_i denotes the i-th row of the matrix A and A_i is the submatrix of A obtained by removing a_i. We say that two extreme rays $\mathbf{d}$ and $\mathbf{d}'$ of $\mathcal{C}$ are equivalent, and denote it by $\mathbf{d} \sim \mathbf{d}'$, if one is a positive multiple of the other. In view of [30, p. 101-105], the number of equivalence classes of extreme rays in $\mathcal{C}$ is finite. Also according to [30, p. 105], if $\{\mathbf{w}_1, \ldots, \mathbf{w}_s\}$ is a complete set of representatives of all equivalence classes of extreme rays in $\mathcal{C}$, then $\mathcal{C} = \{\sum_{i=1}^{s} \lambda_i \mathbf{w}_i \mid \lambda_i \geq 0\}$.

Theorem 4.3 *Let n and $r \leq \frac{n}{7}$ be integers such that $\frac{n^2-n+2}{2} \nmid (n-r)!$. Then*

$$A(n, 5) \leq \frac{2 \times n!}{n^2 - n + 2} - \frac{20n - 56}{(n^2 - n + 2)\sqrt{698n^2 - 1428n + 1274}} \sqrt{\frac{n!}{(n-r)!}}.$$

Proof Let C be an $(n, 5)$-PC in S_n under the Hamming metric. It follows from Lemma 3.3 that C is an $(n, 3)$-PC in S_n under the metric d_Γ, where d_Γ is the metric induced by the graph $\Gamma = Cay(S_n, \mathfrak{S}_2^{n\#})$. Let H be the Young subgroup of S_n corresponding to the partition $\lambda := (n-r, \underbrace{1, \ldots, 1}_{r})$ and Y be the set of right cosets of H in S_n. It follows from Lemma 3.4 that $\widehat{(\mathfrak{S}_2^n)^{\rho_Y^{S_n}}}$ is a matrix $A = (a_{ij})_{\ell \times \ell}$, with $\ell = \frac{n!}{(n-r)!}$, which satisfies the properties listed

in parts (1), (2), and (3) of Lemma 3.4. [2, Theorem 2.14] implies that the optimal value of the objective function of the following integer programming problem gives an upper bound on $|C|$

$$\begin{aligned} \text{Maximize} \quad & \sum_{i=1}^{\ell} x_i, \\ \text{subject to} \quad & A(x_1, \ldots, x_\ell)^t \leq |H|\mathbf{1} = (n-r)!\mathbf{1}, \\ & x_i \in \mathbb{Z},\ x_i \geq 0,\ i \in \{1, \ldots, \ell\}, \end{aligned}$$

where $\mathbf{1}$ is a column vector of order $\ell \times 1$ whose entries are equal to 1. Let $\boldsymbol{\alpha}$ be a feasible solution for the above linear inequality system that achieves the optimum of the objective function and $\boldsymbol{\beta} := \frac{2(n-r)!}{n^2-n+2}\mathbf{1}$. It follows from the part (3) of Lemma 3.4 that the sum of every row in A is equal to $\frac{n^2-n+2}{2}$ and so $A\boldsymbol{\beta} = (n-r)!\mathbf{1}$. Since $\frac{n^2-n+2}{2} \nmid (n-r)!$, we have $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$. It is clear that $\sum_{i=1}^{\ell} \alpha_i \leq \frac{2(n!)}{n^2-n+2}$, where α_i denotes the i-th entry of $\boldsymbol{\alpha}$, and suppose that $\sum_{i=1}^{\ell} \alpha_i = \frac{2(n!)}{n^2-n+2} - k$ for a non-negative number k. Consider two vectors $\overrightarrow{\boldsymbol{\beta\alpha}} := \boldsymbol{\alpha} - \boldsymbol{\beta}$ and $-\mathbf{1}$. We let

$$\begin{aligned} \mu &:= \frac{\left\langle -\mathbf{1}, \overrightarrow{\boldsymbol{\beta\alpha}} \right\rangle}{\| -\mathbf{1} \| \| \overrightarrow{\boldsymbol{\beta\alpha}} \|} = \frac{\langle -\mathbf{1}, \boldsymbol{\alpha} - \boldsymbol{\beta} \rangle}{\| -\mathbf{1} \| \| \boldsymbol{\alpha} - \boldsymbol{\beta} \|} \\ &= \frac{\langle -\mathbf{1}, \boldsymbol{\alpha} \rangle + \langle -\mathbf{1}, -\boldsymbol{\beta} \rangle}{\| -\mathbf{1} \| \| \boldsymbol{\alpha} - \boldsymbol{\beta} \|} \\ &= \frac{\ell \frac{2(n-r)!}{n^2-n+2} - \sum_{i=1}^{\ell} \alpha_i}{\sqrt{\ell}\sqrt{\sum_{i=1}^{\ell} (\alpha_i - \beta_i)^2}} \\ &= \frac{k}{\sqrt{\ell}\sqrt{\sum_{i=1}^{\ell} (\alpha_i - \beta_i)^2}}, \end{aligned}$$

where β_i denotes the i-th entry of $\boldsymbol{\beta}$. Since for each $i \in [\ell]$, α_i is an integer number, we have $|\alpha_i - \beta_i| \geq \frac{2}{n^2-n+2}$. Hence,

$$k \geq \mu\sqrt{\ell}\sqrt{\frac{4\ell}{(n^2-n+2)^2}} = \mu\frac{2\ell}{n^2-n+2}. \tag{4.1}$$

Let $\mathcal{C} := \{\mathbf{x} \in \mathbb{R}^\ell \mid A\mathbf{x} \leq (n-r)!\mathbf{1}\} = \{\mathbf{x} \in \mathbb{R}^\ell \mid A(\mathbf{x} - \boldsymbol{\beta}) \leq \mathbf{0}\}$. In view of Definition 4.1, $\mathcal{C}$ is a polyhedral cone. It follows from Lemma 3.4 that, for all $1 \leq i \leq \ell$, $a_{ii} = \frac{(n-r)(n-r-1)+2}{2}$ and $\sum_{j=1, i\neq j}^{\ell} a_{ij} = \frac{n^2-n+2}{2} - \frac{(n-r)(n-r-1)+2}{2}$. So $r \leq \frac{n}{7}$ implies that $a_{ii} > \sum_{j=1, i\neq j}^{\ell} a_{ij}$ for all $1 \leq i \leq \ell$. Therefore, Levy-Desplanques Theorem [21, p. 125] implies that A is a non-singular matrix. Also, since $\lambda_0\mathbf{u} + (1-\lambda_0)\mathbf{v} \in \mathcal{C}$ for all $\mathbf{u}, \mathbf{v} \in \mathcal{C}$ and $\lambda_0 \in [0, 1]$, $\mathcal{C}$ is a convex set. It is clear that $\boldsymbol{\beta}, \boldsymbol{\alpha} \in \mathcal{C}$ and so the vector $\overrightarrow{\boldsymbol{\beta\alpha}}$ belongs to $\mathcal{C}$. Suppose that $\{\mathbf{w}_1, \ldots, \mathbf{w}_s\}$ is a complete set of representatives of all equivalence classes of extreme rays in $\mathcal{C}$ such that $\| \mathbf{w}_i \| = 1$ for all $1 \leq i \leq s$. Since $\overrightarrow{\boldsymbol{\beta\alpha}} \in \mathcal{C}$, it follows from Remark 4.2 that there exist non-negative real numbers $\lambda_1, \ldots, \lambda_s$ such that $\overrightarrow{\boldsymbol{\beta\alpha}} = \sum_{i=1}^{s} \lambda_i \mathbf{w}_i$. Then

$$\mu = \frac{\left\langle -\mathbf{1}, \overrightarrow{\boldsymbol{\beta\alpha}} \right\rangle}{\| \mathbf{1} \| \| \overrightarrow{\boldsymbol{\beta\alpha}} \|} = \frac{\left\langle -\mathbf{1}, \sum_{i=1}^{s} \lambda_i \mathbf{w}_i \right\rangle}{\| -\mathbf{1} \| \| \sum_{i=1}^{s} \lambda_i \mathbf{w}_i \|}.$$

Since $\| \sum_{i=1}^{s} \lambda_i \mathbf{w}_i \| \leq \sum_{i=1}^{s} \lambda_i \| \mathbf{w}_i \|$,

$$\mu \geq \frac{\sum_{i=1}^{s} \lambda_i \langle -\mathbf{1}, \mathbf{w}_i \rangle}{\| -\mathbf{1} \| (\sum_{i=1}^{s} \lambda_i \| \mathbf{w}_i \|)},$$

and since $\| \mathbf{w}_i \| = 1$ for all $1 \leq i \leq s$,

$$\begin{aligned} \mu &\geq \sum_{i=1}^{s} \frac{\lambda_i \langle -\mathbf{1}, \mathbf{w}_i \rangle}{(\sum_{j=1}^{s} \lambda_j) \| -\mathbf{1} \|} \\ &= \sum_{i=1}^{s} \frac{\lambda_i}{\sum_{j=1}^{s} \lambda_j} \frac{\langle -\mathbf{1}, \mathbf{w}_i \rangle}{\| -\mathbf{1} \|} \geq \sum_{i=1}^{s} \frac{\lambda_i}{\sum_{j=1}^{s} \lambda_j} \mu_0 = \mu_0, \end{aligned} \tag{4.2}$$

where $\mu_0 := \min \left\{ \frac{\langle -\mathbf{1}, \mathbf{w}_i \rangle}{\| -\mathbf{1} \|} \mid 1 \leq i \leq s \right\}$.

Suppose that $\mu_0 = \frac{\langle -\mathbf{1}, \mathbf{w}_r \rangle}{\| -\mathbf{1} \|}$ for some $1 \leq r \leq s$. Hence it follows from Remark 4.2 that there exists $i \in [n]$ such that $A_i \mathbf{w}_r = \mathbf{0}$ and $a_i \mathbf{w}_r \leq 0$, where a_i is the i-th row of the matrix A and A_i is the matrix obtained by removing a_i of the matrix A. According to the properties of the matrix A, without loss of generality, we may assume that $i = \ell$. Suppose that $\boldsymbol{\rho}$ is the ℓ-th column of A_ℓ and J is the $(\ell - 1) \times (\ell - 1)$ matrix obtained by removing the column $\boldsymbol{\rho}$ of the matrix A_ℓ. Levy-Desplanques Theorem implies J is a non-singular matrix. Hence, $A_\ell(x_1, \ldots, x_\ell)^t = J(x_1, \ldots, x_{\ell-1})^t + \boldsymbol{\rho} x_\ell = \mathbf{0}$ implies $(x_1, \ldots, x_{\ell-1})^t = -J^{-1} \boldsymbol{\rho} x_\ell$.
In the sequal, we show that $a_\ell (J^{-1} \boldsymbol{\rho}, -1)^t \leq 0$ and therefore by placing $x_\ell = -1$ we have $(-J^{-1} \boldsymbol{\rho} x_\ell, x_\ell)^t \sim \mathbf{w}_r$. It follows from [33, Theorem 1] and Lemma 3.4 that if $\Delta := \min\{|J_{ii}| - \sum_{j=1, j \neq i}^{\ell-1} |J_{ij}| \mid 1 \leq i \leq \ell - 1\}$, then $\| J^{-1} \|_\infty := \max\{\sum_{j=1}^{\ell-1} |(J^{-1})_{ij}| \mid 1 \leq i \leq \ell - 1\} \leq \frac{1}{\Delta}$. Lemma 3.4 and $r \leq \frac{n}{7}$ imply that

$$\Delta = \frac{(n-r)(n-r-1)}{2} + 1 - \left(\frac{n^2 - n}{2} + 1 - \frac{(n-r)(n-r-1)}{2} - 1\right) > \frac{23n^2 - 35n}{98}.$$

So $\| J^{-1} \|_\infty \leq \frac{98}{23n^2 - 35n}$. For each matrix $\mathbf{M} = (m_{ij})_{n \times n}$, we let $|\mathbf{M}| := (|m_{ij}|)_{n \times n}$. So we have

$$\| J^{-1} \boldsymbol{\rho} \|_1 = \mathrm{tr}(|J^{-1} \boldsymbol{\rho}| \mathbf{1}^t) \leq \mathrm{tr}(|J^{-1}| \boldsymbol{\rho} \mathbf{1}^t).$$

Since the inverse of a symmetric matrix is a symmetric matrix, J^{-1} is a symmetric matrix. Suppose that ρ_i denotes the i-th entry of $\boldsymbol{\rho}$. It follows from Lemma 3.4 that $\rho_i \in \{0, 1\}$ for all $1 \leq i \leq \ell - 1$ and if $\tau := \{i \in [\ell - 1] \mid \rho_i = 1\}$, then it follows from $r \leq \frac{n}{7}$ that

$$|\tau| = \frac{n^2 - n}{2} + 1 - \frac{(n-r)(n-r-1)}{2} - 1 \leq \frac{13n^2 - 7n}{98}.$$

Then we have

$$\begin{aligned}\mathrm{tr}(|J^{-1}|\boldsymbol{\rho}\mathbf{1}^t) &= \sum_{i=1}^{\ell-1}\sum_{j\in\tau}|(J^{-1})_{ij}| \\ &= \sum_{j\in\tau}\sum_{i=1}^{\ell-1}|(J^{-1})_{ij}| \\ &= \sum_{j\in\tau}\sum_{i=1}^{\ell-1}|(J^{-1})_{ji}| \\ &\leq \sum_{j\in\tau}\parallel J^{-1}\parallel_\infty \leq |\tau|\parallel J^{-1}\parallel_\infty,\end{aligned}$$

and therefore,

$$\parallel J^{-1}\boldsymbol{\rho}\parallel_1 \leq \frac{13n^2-7n}{98}\times\frac{98}{23n^2-35n} = \frac{13n-7}{23n-35}. \tag{4.3}$$

So, parts (1) and (2) of Lemma 3.4 and $r \leq \frac{n}{7}$ imply that

$$a_\ell(J^{-1}\boldsymbol{\rho}, -1)^t \leq \parallel J^{-1}\boldsymbol{\rho}\parallel_1 - \frac{(n-r)(n-r-1)}{2} - 1 \leq 0$$

and so $(J^{-1}\boldsymbol{\rho}, -1)^t \sim \mathbf{w}_r$. Hence,

$$\begin{aligned}\mu_0 &= \frac{\langle -\mathbf{1}, (J^{-1}\boldsymbol{\rho}, -1)^t\rangle}{\parallel\mathbf{1}\parallel\parallel(J^{-1}\boldsymbol{\rho}, -1)^t\parallel} = \frac{1-\langle\mathbf{1}, J^{-1}\boldsymbol{\rho}\rangle}{\sqrt{\ell}\sqrt{1+\parallel J^{-1}\boldsymbol{\rho}\parallel^2}} \\ &\geq \frac{1-\parallel J^{-1}\boldsymbol{\rho}\parallel_1}{\sqrt{\ell}\sqrt{1+\parallel J^{-1}\boldsymbol{\rho}\parallel_1^2}}.\end{aligned} \tag{4.4}$$

Hence, relations (4.3) and (4.4) imply

$$\mu_0 \geq \frac{10n-28}{\sqrt{\ell}\sqrt{(23n-35)^2+(13n-7)^2}}, \tag{4.5}$$

and therefore the result follows from relations (4.1), (4.2) and (4.5). This completes the proof. □

Remark 4.4 Since the best possible bound in Theorem 4.3 is achieved for $r = \lfloor\frac{n}{7}\rfloor$, and since the condition that n^2-n+2 is divisible by a prime exceeding $n-\lfloor\frac{n}{7}\rfloor$ is a sufficient condition for the $\frac{n^2-n+2}{2} \nmid (n-\lfloor\frac{n}{7}\rfloor)!$, we reformulated Theorem 4.3 as Theorem 1.7.

In the following, we demonstrate that Theorem 1.7 provides a better upper bound for $A(n,d)$ for infinitely many natural numbers n. This case corresponds to the question posed in [1]. For the reader's convenience, we restate the result as Theorem 4.5 and Corollary 4.6.

Next, we review the definitions necessary for proving Theorem 4.5. A polynomial of degree k over $\mathbb{Z}$ is defined as $f(x) = a_kx^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0$, where $a_i \in \mathbb{Z}$ for all $0 \leq i \leq k$ and $a_k \neq 0$. A polynomial $f(x)$ is called a constant polynomial if $a_i = 0$ for all $1 \leq i \leq k$. Additionally, a non-constant polynomial over $\mathbb{Z}$ is called irreducible if it cannot be factored into two polynomials of lower degree with integer coefficients. For a polynomial $f(x)$ over $\mathbb{Z}$, we define Φ_f as the smallest subset of prime numbers such that for every integer $n \in \mathbb{Z}$, all prime factors of $f(n)$ belong to Φ_f.

Theorem 4.5 *Let $f(x)$ be an irreducible polynomial over $\mathbb{Z}$ of degree greater than* 1. *Then there are infinitely many positive integers n for which $f(n)$ has a prime divisor greater than n.*

Proof We first show that Φ_f is an infinite set (see [28]). Assume that $f(x) = a_m x^m + \cdots + a_1 x + a_0$, where $m \geq 2$ and $a_i \in \mathbb{Z}$ for all $0 \leq i \leq m$. Since $f(x)$ is an irreducible polynomial, $f(0) = a_0 \neq 0$. Define $g(x) := \frac{f(a_0 x)}{a_0}$. It is clear that $g(x)$ is a non-constant polynomial over $\mathbb{Z}$ such that $g(0) = 1$.

As a contradiction, assume that Φ_g is a finite set and $p_1, \ldots, p_k$ are all elements of Φ_g. Let $q := \prod_{i=1}^{k} p_i$. It is obvious that for all non-zero elements $t \in \mathbb{Z}$, $g(qt) \equiv g(0) \equiv 1 \pmod{q}$. Suppose that there exists $1 \leq i \leq k$ such that $p_i \mid g(qt)$. Hence, there are non-zero integers s and r such that $p_i s = g(qt)$ and $g(qt) = qr + 1$. So, $p_i(s - \frac{q}{p_i} r) = 1$, which implies $p_i = 1$, a contradiction. Thus, we must have $p_i \nmid g(qt)$ for all $1 \leq i \leq k$. Therefore, $g(qt) = 1$ for all non-zero elements $t \in \mathbb{Z}$. Hence, since $g(x)$ takes a constant value for infinitely many integers, $g(x)$ must be a constant polynomial that is a contradiction. Thus, Φ_g that is a subset of Φ_f is an infinite set and therefore Φ_f is an infinite set.

Now, suppose that $p \in \Phi_f$ and $p \mid f(n)$ for some $n \in \mathbb{Z}$. If $n \equiv j \pmod{p}$, then it is clear that there is a non-zero integer d such that $f(n) = dp + f(j)$. Therefore $p \mid f(j)$. Hence, for each $p \in \Phi_f$ we may choose $n < p$ such that $p \mid f(n)$. Finally, since for each $n \in \mathbb{Z}$, $f(n) \neq 0$, the result follows from the fact that there are only finitely many primes p such that $p \mid f(n)$. This completes the proof. □

Corollary 4.6 *There are infinity many natural numbers n such that $n^2 - n + 2$ has a prime divisor greater than n.*

Proof Since $f(x) = x^2 - x + 2$ is an irreducible polynomial over $\mathbb{Z}$, the result follows from Theorem 4.5. This completes the proof. □

Proof of Corollary 1.8 It follows from Theorem 1.7 that $A(n, 5) \leq \frac{2n!}{n^2-n+2} - k$, where

$$k = \frac{20n - 56}{(n^2 - n + 2)\sqrt{698n^2 - 1428n + 1274}} \sqrt{\frac{n!}{(n - \lfloor \frac{n}{7} \rfloor)!}}.$$

Since $n \geq 35$, $r := \lfloor \frac{n}{7} \rfloor \geq 5$. Hence,

$$\begin{aligned} k &= \sqrt{\frac{(20n - 56)^2 n(n-1)(n-2)(n-3)(n-4)}{(n^2 - n + 2)^2 (698n^2 - 1428n + 1274)}} \times \sqrt{\prod_{i=5}^{r-1} (n - i)} \\ &= \sqrt{\frac{400n^7 - 6240n^6 + 39536n^5 - 129760n^4 + 231360n^3 - 210560n^2 + 75264n}{698n^6 - 1408n^5 + 7604n^4 - 6050n^3 + 9730n^2 - 5660n + 5096}} a, \end{aligned}$$

where $a = \prod_{i=5}^{r-1} (n - i)^{\frac{1}{2}}$. Now, $n \geq 35$ implies that

$$\begin{aligned} k &\geq \sqrt{\frac{7760n^6 + 1383760n^4 + 7887040n^2 + 75264n}{698n^6 - 53326n^4 - 202020n^2 - 193004}} \times (n - r + 1)^{\frac{r-5}{2}} \\ &> \sqrt{\frac{7760}{698}} \times (n - r + 1)^{\frac{r-5}{2}} \simeq 3.334 \times (n - r + 1)^{\frac{r-5}{2}}, \end{aligned}$$

and this completes the proof. □

Remark 4.7 The numbers 37, 38, 46, 51, 60, 62, 66, 68, 79, 83, 91, 92, and 95 are the only integers between 35 and 100 that do not satisfy the condition that $n^2 - n + 2$ is divisible by a prime greater than $n - \lfloor \frac{n}{7} \rfloor$.

Acknowledgements This work is based upon research funded by Iran National Science Foundation (INSF) under project No. 4024979.

Author Contributions All authors read and approved the final manuscript.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Competing Interests The authors declare no competing interests.

References

1. Abdollahi, A.: (https://mathoverflow.net/users/19075/alireza-abdollahi). Possible prime divisors of $n^2 - n + 2$ which are greater than n, URL (version: 2025-01-22): https://mathoverflow.net/q/486408
2. Abdollahi, A., Bagherian, J., Jafari, F., Khatami, M., Parvaresh, F., Sobhani, R.: New upper bounds on the size of permutation codes under Kendall τ-metric. Cryptogr. Commun. **15**, 891–903 (2023)
3. Barg, A., Mazumdar, A.: Codes in permutations and error correction for rank modulation. IEEE Trans. Inf. Theory **56**, 3158–3165 (2010)
4. Beeri, N., Schwartz, M.: Improved rank-modulation codes for DNA storage with shotgun sequencing. IEEE Trans. Inform. Theory **68**, 3719–3730 (2022)
5. Bereg, S., Malouf, B., Morales, L., Stanley, T., Sudborough, I.H.: Using permutation rational functions to obtain permutation arrays with large hamming distance. Des. Codes Cryptogr. **90**(7), 1659–1677 (2022)
6. Bereg, S., Morales, L., Sudborough, I.H.: Extending permutation arrays: Improving MOLS bounds. Des. Codes Cryptogr. **83**, 661–683 (2017)
7. Bereg, S., Levy, A., Sudborough, I.H.: Constructing permutation arrays from groups. Des. Codes Cryptogr. **86**, 1095–1111 (2018)
8. Bereg, S., Miller, Z., Mojica, L.G., Morales, L., Sudborough, I.H.: New lower bounds for permutation arrays using contraction. Des. Codes Cryptogr. **87**, 2105–2128 (2019)
9. Bereg, S., Mojica, L.G., Morales, L., Sudborough, I.H.: Constructing permutation arrays using partition and extension. Des. Codes Cryptogr. **88**, 311–339 (2020)
10. Blake, I.F.: permutation codes for discrete channels. IEEE Trans. Inform. Theory **20**, 138–140 (1974)
11. Blake, I.F., Cohen, G., Deza, M.: Coding with permutations. Inf. Control **43**, 1–19 (1979)
12. Bogaerts, M.: New upper bounds for the size of permutation codes via linear programming. Electr. J. Comb. **17**, R135 (2010)
13. Chu, W., Colbourn, C.J., Dukes, P.: Constructions for permutation codes in powerline communications. Des. Codes Cryptogr. **32**, 51–64 (2004)
14. Colbourn, C.J., Klove, T., Ling, A.C.H.: Permutation arrays for powerline communication and mutually orthogonal Latin squares. IEEE Trans. Inform. Theory **50**, 1289–1291 (2004)
15. de la Torre, D.R., Colbourn, C.J., Ling, A.C.H.: An application of permutation arrays to block ciphers. Congr. Numer. **145**, 5–8 (2000)
16. Deza, M., Vanstone, S.A.: Bounds for permutation arrays. J. Statist. Plann. Inference **2**, 197–209 (1978)
17. Diaconis, P., Shahshahani, M.: Generating a random permutation with random transpositions. Z. Wahrscheinlichkeitstheorie verw Gebiete **57**, 159–179 (1981)
18. Dukes, P., Sawchuck, N.: Bounds on permutation codes of distance four. J. Algebr. Comb. **31**, 143–158 (2010)
19. Frankl, P., Deza, M.: On the maximum number of permutations with given maximal or minimal distance. J. Combin. Theory Series A **22**, 352–360 (1977)
20. Gao, F., Yang, Y., Ge, G.: An improvement on the Gilbert-Varshamov bound for permutation codes. IEEE Trans. Inform. Theory **59**, 3059–3063 (2013)
21. Horn, R.A., Johnson, C.R.: Matrix analysis. Cambridge Univ. Press, Cambridge (1991)

22. James, G., Kerber, A.: The representation theory of the symmetric group. Encyclopedia Math. Appl., 16, Addison-Wesley Publishing Co., Reading, Mass. (1981)
23. Jiang, A., Schwartz, M., Bruck, J.: Error-correcting codes for rank modulation. Proc. IEEE Int. Symp. Inf. Theory, 6-11 (2008)
24. Jiang, A., Schwartz, M., Bruck, J.: Correcting charge-constrained errors in the rank modulation scheme. IEEE Trans. Inf. Theory **56**, 2112–2120 (2010)
25. Montemanni, R., Barta, J., Smith, D.H.: Permutation codes: a branch and bound approach. In: Proceedings of the International Conference on Informatics and Advanced Computing 1-3 (2014)
26. Micheli, G., Neri, A.: New lower bounds for permutation codes using linear block codes. IEEE Trans. Inf. Theory **66**(7), 4019–4025 (2020)
27. Parvaresh, F., Sobhani, R., Abdollahi, A., Bagherian, J., Jafari, F., Khatami, M.: Improved bounds on the size of permutation codes under Kendall τ-metric. IEEE Trans. Inf. Theory (2025). https://ieeexplore.ieee.org/abstract/document/10965831 https://doi.org/10.1109/TIT.2025.3561119
28. qwenty (https://math.stackexchange.com/users/202599/qwenty), Infiniteness of the set of primes such f have root mode p, URL (version: 2024-03-28): https://math.stackexchange.com/q/1250302
29. Rothaus, O., Thompson, J.: A combinatorial problem in the symmetric group. Pacific J. Math. **18**, 175–178 (1966)
30. Schrijver, A.: Theory of linear and integer programming. John Wiley and Sons, (1998)
31. Smith, D.H., Montemanni, R.: A new table of permutation codes. Des. Codes Cryptogr. **63**, 241–253 (2012)
32. Tarnanen, H.: Upper bounds on permutation codes via linear programming. European J. Combin. **20**(1), 101–114 (1999)
33. Varah, J.M.: A lower bound for the smallest singular value of a matrix. Linear Algebra Appl. **11**(1), 3–5 (1975)
34. Vinck, A.J.H.: Coded modulation for power line communications. In: AE Int. J. Electron. and Commun, 45-49 (2011)
35. Wang, X., Yin, W.: New non-existence results on perfect permutation codes under the Hamming metric. Adv. Math. Commun. **17**(6), 1440–1452 (2021)
36. Wang, X., Zhang, Y.W., Yang, Y.T., Ge, G.N.: New bounds of permutation codes under Hamming metric and Kendall's τ-metric. Des. Codes Cryptogr. **85**, 533–545 (2017)

Authors and Affiliations

Alireza Abdollahi[1] · Javad Bagherian[1] · Fatemeh Jafari[1] · Maryam Khatami[1] · Farzad Parvaresh[2] · Reza Sobhani[3]

✉ Fatemeh Jafari
math_fateme@yahoo.com

Alireza Abdollahi
a.abdollahi@math.ui.ac.ir

Javad Bagherian
bagherian@sci.ui.ac.ir

Maryam Khatami
m.khatami@sci.ui.ac.ir

Farzad Parvaresh
f.parvaresh@eng.ui.ac.ir

Reza Sobhani
r.sobhani@sci.ui.ac.ir

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

2 Department of Electrical Engineering, Faculty of Engineering, University of Isfahan, Isfahan 81746-73441, Iran

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