Advances in Mathematics of Communications doi:10.3934/amc.2021058

NEW NONEXISTENCE RESULTS ON PERFECT PERMUTATION CODES UNDER THE HAMMING METRIC

Xiang Wang

National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), Beijing, 100029, China

Wenjuan Yin*

School of Mathematical Sciences, Tiangong University, Tianjin, 300387, China

(Communicated by Massimiliano Sala)

Abstract. Permutation codes under the Hamming metric are interesting topics due to their applications in power line communications and block ciphers. In this paper, we study perfect permutation codes in S_n, the set of all permutations on n elements, under the Hamming metric. We prove the nonexistence of perfect t-error-correcting codes in S_n under the Hamming metric, for more values of n and t. Specifically, we propose some sufficient conditions of the nonexistence of perfect permutation codes. Further, we prove that there does not exist a perfect t-error-correcting code in S_n under the Hamming metric for some n and $t = 1, 2, 3, 4$, or $2t + 1 \leq n \leq \max\{4t^2e^{-2+1/t} - 2, 2t + 1\}$ for $t \geq 2$, or $\min\{\frac{e}{2}\sqrt{n+2}, \lfloor\frac{n-1}{2}\rfloor\} \leq t \leq \lfloor\frac{n-1}{2}\rfloor$ for $n \geq 7$, where e is the Napier's constant.

1. Introduction

Permutation codes were first studied in [2, 3, 9, 13]. Recently, they have attracted considerable attention due to their applications as varied as power line communications[24, 6, 21, 5], block ciphers[7], and the rank modulation scheme for flash memories[1, 17, 16]. A permutation code is a subset of S_n, the set of all permutations over $\{1, 2, \ldots, n\}$. Permutation codes under various metrics have been studied, such as the ℓ_∞-metric [18, 26, 29], the Ulam metric [12], the Kendall τ-metric [1, 17, 25, 30], and the Hamming metric [24, 10, 6, 21, 5, 28]. Moreover, a survey on metrics related to permutations is given in [8]. The *Hamming distance* between permutations π and σ in S_n is the number of positions in which their vector components differ. In this paper, we only consider the Hamming metric.

Permutation codes under the Hamming distance have been widely studied due to their applications in data transmission over power line [24, 6, 21, 5]. There are three main forms of noise (the permanent narrow-band noise, the impulse noise of short duration, and white Gaussian noise) which affect the transmission in the power line application. Permutation codes under the Hamming distance with minimum distance d can correct $\lfloor\frac{d-1}{2}\rfloor$ errors. Ding et al. [10] and some authors in [14, 15, 23, 22, 11, 20, 28] studied permutation codes and presented some bounds on the size of permutation codes under the Hamming metric. Previous work to study the perfect permutation codes under various distance metrics (Hamming, Kendall, Ulam) can

2020 *Mathematics Subject Classification:* Primary: 94A15; Secondary: 68P30.

Key words and phrases: Perfect codes, Hamming metric, permutation codes.

* Corresponding author: Wenjuan Yin.

be found in [3, 19, 4, 27]. Blake [3] first studied perfect permutation codes under the Hamming metric and proposed some necessary conditions of the existence of these perfect permutation codes. Meanwhile, Buzaglo and Etzion [4] discovered the existence of a perfect permutation code under the cyclic Kendall τ-metric, and proved the nonexistence of perfect single-error-correcting permutation codes in S_n under the Kendall τ-distance, where $n > 4$ is a prime or $4 \leq n \leq 10$. Further, Wang et al. [27] proved that there does not exist a perfect t-error-correcting code in S_n under the Kendall τ-metric for some n and $t = 2, 3, 4, 5$, or $\frac{5}{8}\binom{n}{2} < 2t + 1 \leq \binom{n}{2}$. Recently, Kong and Hagiwara [19] proved the nonexistence of non-trivial perfect permutation codes under the Ulam metric. In this paper, we study the nonexistence of perfect t-error-correcting codes in S_n under the Hamming metric. We propose some sufficient conditions of the nonexistence of perfect permutation codes under the Hamming metric. Moreover, we prove that there does not exist a perfect one-error-correcting code in S_n. We also prove that there does not exist a perfect two-error-correcting code in S_n under the Hamming metric, where $n^2 - n + 2$ has a prime factor $p > n$, or $5 \leq n < 11$, or $12 \leq n \leq 17$. We prove that there does not exist a perfect three-error-correcting code in S_n under the Hamming metric, where $n + 1 > 7$ is a prime, or $2n^2 - 5n + 6$ has a prime factor $p > n$, or $7 \leq n \leq 47$. We prove that there does not exist a perfect four-error-correcting code in S_n, where $9n^4 - 46n^3 + 87n^2 - 50n + 24$ has a prime factor $p > n$, or $9 \leq n \leq 50$. We further prove the nonexistence results of perfect t-error-correcting codes in S_n, where $2t + 1 \leq n \leq \max\{4t^2 e^{-2+1/t} - 2, 2t + 1\}$ for $t \geq 2$, or $\min\{\frac{e}{2}\sqrt{n+2}, \lfloor\frac{n-1}{2}\rfloor\} \leq t \leq \lfloor\frac{n-1}{2}\rfloor$ for $n \geq 7$, and e is the Napier's constant.

The rest of this paper is organized as follows. In Section 2, we give the definitions and notations of permutation codes under the Hamming metric and summarize some important facts regarding the bounds. In Section 3, we propose some sufficient conditions of the nonexistence of perfect permutation codes under the Hamming metric. In Section 4, we prove the nonexistence of perfect t-error-correcting codes in S_n for some n and t under the Hamming metric. Section 5 concludes this paper.

2. Preliminaries

In this section we give some definitions of permutation codes under the Hamming metric and summarize some important facts regarding the bounds.

Let $[n] \triangleq \{1, 2, \ldots, n-1, n\}$ and e be the Napier's constant. Let S_n be the set of all permutations over $[n]$. For any permutation $\pi \in S_n$, we denote the permutation by $\pi \triangleq [\pi(1), \pi(2), \ldots, \pi(n)]$. For two permutations $\sigma, \pi \in S_n$, the product $\pi \circ \sigma$ is defined as the composition of σ on π, that is, $\pi \circ \sigma(i) = \sigma(\pi(i))$ for all $i \in [n]$. Hence, S_n forms a noncommutative *group* of size $n!$ under this operation. Let $\epsilon_n \triangleq [1, 2, \ldots, n]$ be the identity element of S_n. For each $\pi \in S_n$, let π^{-1} be the *inverse* element of π.

For two permutations $\sigma, \pi \in S_n$, the Hamming distance between them is the number of positions in which their vector components differ, that is,

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

For $1 \leq d \leq n$, we say that $C \subset S_n$ is an (n, d)-*permutation code under the Hamming metric*, if $d(\sigma, \pi) \geq d$ for any two distinct permutations $\pi, \sigma \in C$. We denote the largest size of an (n, d)-permutation code under the Hamming metric as $A(n, d)$. For a permutation $\sigma \in S_n$, a Hamming ball or sphere of radius t centered at σ, denoted as $B^n(\sigma, t)$ and $S^n(\sigma, t)$, is defined by $B^n(\sigma, t) \triangleq \{\pi \in S_n | d(\sigma, \pi) \leq t\}$

and $S^n(\sigma,t) \triangleq \{\pi \in S_n | d(\sigma,\pi) = t\}$, respectively. Clearly, the size of a Hamming ball or a sphere of radius t under the Hamming metric does not depend on the center of the ball or the sphere. For convenience, we denote the size of $B^n(\pi,t)$ and $S^n(\pi,t)$ as $B^n(t)$ and $S^n(t)$, respectively. Then, we obtain that

$$S^n(t) = |\{\pi \in S_n | d(\pi,\epsilon_n) = t\}|.$$

We now summarize some important results of the lower and upper bounds on $A(n,d)$.

A derangement of order t is a permutation $\pi \in S_t$ with no fixed points, that is, $\pi(i) \neq i$ for $1 \leq i \leq t$. Let D_t be the number of derangements of order t. Then from [28] we have

$$S^n(t) = \binom{n}{t} D_t. \tag{1}$$

Clearly, due to the relationship between $B^n(t)$ and $S^n(t)$, it follows that

$$B^n(t) = 1 + \sum_{i=1}^{t} S^n(i) = 1 + \sum_{i=1}^{t} \binom{n}{i} D_i. \tag{2}$$

The Gilbert-Varshamov bound and the sphere-packing bound for permutation codes under the Hamming metric are given as follows:

Proposition 1. [28, Proposition 3]

$$\frac{n!}{B^n(d-1)} \leq A(n,d) \leq \frac{n!}{B^n(\lfloor \frac{d-1}{2} \rfloor)}. \tag{3}$$

Frankl and Deza [13] proposed another upper bound in the following proposition.

Proposition 2. [13, Theorem 4]

$$A(n,d) \leq \frac{n!}{(d-1)!}. \tag{4}$$

When $d = 2t+1$, an $(n, 2t+1)$-permutation code C of size M under the Hamming metric is a t-error-correcting code. Furthermore, if $M \cdot B^n(t) = n!$, we call the code C a *perfect* $(n, 2t+1)$-permutation code under the Hamming metric. That is, the balls with radius t centered at the codewords of C form a partition of S_n. A perfect $(n, 2t+1)$-permutation code under the Hamming metric is also called a perfect t-error-correcting code under the Hamming metric.

Based on the above definitions and notations, by using some upper bounds and the properties of $B^n(t)$ and $S^n(t)$, we will prove the nonexistence of perfect t-error-correcting codes in S_n under the Hamming metric for some n and $t = 1, 2, 3, 4$, or $2t+1 \leq n \leq \max\{4t^2 e^{-2+1/t} - 2, 2t+1\}$ for $t \geq 2$, or $\min\{\frac{e}{2}\sqrt{n+2}, \lfloor \frac{n-1}{2} \rfloor\} \leq t \leq \lfloor \frac{n-1}{2} \rfloor$ for $n \geq 7$.

3. Some sufficient conditions of the nonexistence of perfect permutation codes

In this section, we will give some sufficient conditions of the nonexistence of a perfect t-error-correcting code in S_n under the Hamming metric. By using some

properties of $B^n(t)$, we compute polynomial representations of $B^n(t)$ for some t. Due to the definition of D_t [13], we have the following expression

$$D_t = t! \sum_{j=0}^{t} \frac{(-1)^j}{j!}. \tag{5}$$

To avoid confusion, we illustrate that n, t, s are all integers in the sequel. By (5), it follows that $D_1 = 0, D_2 = 1, D_3 = 2$, and $D_4 = 9$. Hence, by (2), we give the polynomial representations of $B^n(t)$ for $t = 1, 2, 3, 4$ as follows.

Lemma 3.1. *It holds that*

$$B^n(1) = 1,$$
$$B^n(2) = \frac{n^2 - n + 2}{2},$$
$$B^n(3) = \frac{(n+1)(2n^2 - 5n + 6)}{6},$$
$$B^n(4) = \frac{9n^4 - 46n^3 + 87n^2 - 50n + 24}{24}.$$

Proof. By (2) and (5), it can be readily verified that $B^n(1) = 1 + \binom{n}{1} D_1 = 1$. We also compute that $B^n(2) = B^n(1) + \binom{n}{2} D_2 = 1 + \binom{n}{2} = \frac{n^2-n+2}{2}$. Similarly, we have that $B^n(3) = \frac{(n+1)(2n^2-5n+6)}{6}$ and $B^n(4) = \frac{9n^4-46n^3+87n^2-50n+24}{24}$. □

In the following, we present a sufficient condition of the nonexistence of a perfect t-error-correcting code under the Hamming metric by using the sphere packing upper bound and the property of $B^n(t)$, where $1 \leq t \leq \lfloor \frac{n-1}{2} \rfloor$.

Theorem 3.2. *For $1 \leq t \leq \lfloor \frac{n-1}{2} \rfloor$, if $B^n(t)$ has a prime factor $p > n$, then there does not exist a perfect t-error-correcting code in S_n under the Hamming metric.*

Proof. By the sphere-packing upper bound in Proposition 1, if there exists a perfect t-error-correcting code C of size M in S_n under the Hamming τ-metric then $B^n(t) \cdot M = n!$. If $B^n(t)$ has a prime factor $p > n$ then $B^n(t) \nmid n!$. Therefore, if $B^n(t)$ has a prime factor $p > n$, then there does not exist a perfect t-error-correcting code in S_n under the Hamming metric. So, we prove the above result. □

By comparing two upper bounds on $A(n, d)$ in Propositions 1 and 2, we can give another sufficient condition of the nonexistence of a perfect t-error-correcting code under the Hamming metric. We present an upper estimation of $B^n(t)$ by using the following lemma.

Lemma 3.3. *For $1 \leq t$, we have that*

$$D_t \leq t!(1 - \frac{1}{t+1}).$$

Proof. By (5), it follows that

$$D_{t+1} = (t+1)D_t + (-1)^{t+1}. \tag{6}$$

Moreover, we compute

$$\begin{aligned}(t+1)!(1 - \frac{1}{t+2}) - (t+1)\big(t!(1 - \frac{1}{t+1})\big) &= (t+1)!(\frac{1}{t+1} - \frac{1}{t+2}) \\ &= \frac{t!}{t+2} \geq 1,\end{aligned} \tag{7}$$

where $t \geq 3$. Since $D_1 = 0$ and $D_2 = 1$, it can be easily verified that $D_t \leq t!(1-\frac{1}{t+1})$ for $1 \leq t \leq 3$. When $t \geq 3$, we will prove that

$$D_t \leq t!(1 - \frac{1}{t+1}). \tag{8}$$

by induction. When $t = 3$, we easily have that $D_3 = 2 \leq 3!(1 - \frac{1}{3+1})$.

Now assume that D_s satisfies the condition in (8) for some integers $s \geq 3$, that is, $D_s \leq s!(1 - \frac{1}{s+1})$.

When $t = s + 1$, it follows that

$$\begin{aligned} D_{s+1} &\overset{(a)}{=} (s+1)D_s + (-1)^{s+1} \leq (s+1)D_s + 1 \\ &\overset{(b)}{\leq} (s+1)!(1 - \frac{1}{s+1}) + 1 \\ &\overset{(c)}{\leq} (s+1)!(1 - \frac{1}{s+2}), \end{aligned} \tag{9}$$

where $\overset{(a)}{=}, \overset{(b)}{\leq}, \overset{(c)}{\leq}$ follows from (6), the induction hypothesis on D_s, and (7), respectively. Hence, by induction, we have that

$$D_t \leq t!(1 - \frac{1}{t+1}),$$

for $t \geq 3$. Since $t = 1, 2$, this result also holds. Thus, the lemma follows. □

Next, by using Lemma 3.3, we will present the upper bound on $B^n(t)$, that is, $B^n(t) \leq \frac{n!}{(n-t)!}$ as follows.

Lemma 3.4. *For $1 \leq t \leq \lfloor \frac{n-1}{2} \rfloor$, we have that*

$$B^n(t) \leq \frac{n!}{(n-t)!}. \tag{10}$$

Proof. We prove this result by induction. When $t = 1$, by Lemma 3.1, it follows that $B^n(1) = 1$. Hence, $B^n(1) < \frac{n!}{(n-1)!} = n$. Now assume that $B^n(s)$ satisfies the condition in (10) for some integers $s \geq 1$, that is, $B^n(s) \leq \frac{n!}{(n-s)!}$.

When $t = s + 1$, we have that

$$\begin{aligned} B^n(s+1) &\overset{(d)}{=} B^n(s) + \binom{n}{s+1} D_{s+1} \\ &\overset{(e)}{\leq} \frac{n!}{(n-s)!} + \binom{n}{s+1} D_{s+1} \\ &\overset{(f)}{\leq} \frac{n!}{(n-s)!} + \binom{n}{s+1} (s+1)!(1 - \frac{1}{s+2}), \end{aligned} \tag{11}$$

where $\overset{(d)}{=}, \overset{(e)}{\leq}, \overset{(f)}{\leq}$ follows from (2), the induction hypothesis on $B^n(s)$, and Lemma 3.3, respectively. If $t = s + 1$ then $n \geq 2s + 3$. Hence, we have that

$$1 - \frac{1}{s+2} \leq 1 - \frac{1}{n-s}. \tag{12}$$

By (11) and (12), we have that

$$B^n(s+1) \leq \frac{n!}{(n-s)!} + \binom{n}{s+1}(s+1)!(1 - \frac{1}{n-s}) = \frac{n!}{(n-s-1)!}.$$

Hence, by induction, it follows that

$$B^n(t) \leq \frac{n!}{(n-t)!},$$

for $1 \leq t \leq \lfloor \frac{n-1}{2} \rfloor$. So, the lemma follows. □

In the following TABLE 1, we compare the values of $B^n(t)$ and $\frac{n!}{(n-t)!}$ for $t = 2, 3,$ or 4, and $2t+1 \leq n \leq 10$.

TABLE 1. The values of $(B^n(t), \frac{n!}{(n-t)!})$ for $2 \leq t \leq 4$ and $n \leq 10$.

$(B^n(t), \frac{n!}{(n-t)!})$	$n=5$	$n=6$	$n=7$	$n=8$	$n=9$	$n=10$
$t=2$	$(11,20)$	$(16,30)$	$(22,42)$	$(29,56)$	$(37,72)$	$(46,90)$
$t=3$	–	–	$(92,210)$	$(141,336)$	$(205,504)$	$(286,720)$
$t=4$	–	–	–	–	$(1339,3024)$	$(2176,5040)$

Assume that C is a perfect t-error-correcting code of size M in S_n under the Hamming metric. By Proposition 1, then $M = \frac{n!}{B^n(t)}$. By Proposition 2, we present another sufficient condition of the nonexistence of a perfect t-error-correcting code in S_n under the Hamming metric in the following theorem.

Theorem 3.5. *For $1 \leq t \leq \lfloor \frac{n-1}{2} \rfloor$, if $(2t)! > \frac{n!}{(n-t)!}$, then there does not exist a perfect t-error-correcting code in S_n under the Hamming metric.*

Proof. Since C is a perfect t-error-correcting code of size M in S_n under the Hamming metric, we have that $M = \frac{n!}{B^n(t)}$. By Proposition 2, it follows that

$$M = \frac{n!}{B^n(t)} \leq \frac{n!}{(2t)!}.$$

If $(2t)! > \frac{n!}{(n-t)!}$, by Lemma 3.4, then we have that $(2t)! > B^n(t)$. Therefore, if $(2t)! > \frac{n!}{(n-t)!}$ then there does not exist a perfect t-error-correcting code in S_n under the Hamming metric. □

4. The nonexistence of perfect t-error-correcting codes in S_n

In the section, we will study the nonexistence of a perfect t-error-correcting code in S_n for some n and t by using Theorems 3.2 and 3.5. We need some results of the exact values of $A(n,d)$ as follows.

Lemma 4.1. [5, Proposition 1.1] *It holds that*

$$A(n,2) = n!,$$

$$A(n,3) = n!/2,$$

$$A(n,n) = n.$$

4.1. THE NONEXISTENCE OF PERFECT ONE-ERROR-CORRECTING CODE. When $t = 1$, by the exact value of $A(n, 3)$ in Lemma 4.1, we will discuss the nonexistence of a perfect one-error-correcting code in S_n in the following theorem.

Theorem 4.2. *For $n \geq 3$, there does not exist a perfect one-error-correcting code in S_n under the Hamming metric.*

Proof. Assume that C is a perfect one-error-correcting code of size M in S_n under the Hamming metric. By Lemma 3.1 and Proposition 1, it follows that $M = \frac{n!}{B^n(1)} = n!$. By Lemma 4.1, we have that $M \leq n!/2$. So, for $n \geq 3$, there does not exist a perfect one-error-correcting code C in S_n under the Hamming metric. □

Example 1. When $n = 3$, let $C = \{[1, 2, 3], [2, 3, 1], [3, 1, 2]\}$ be a permutation code with minimum distance 3 and maximum size $A(3, 3) = 3$. Obviously, $[1, 3, 2] \notin C$ and $d([1, 3, 2], \pi) \geq 2$ for every $\pi \in C$. Hence, C is not a perfect one-error-correcting code of size $A(3, 3)$ in S_3 under the Hamming metric.

4.2. THE NONEXISTENCE OF PERFECT t-ERROR-CORRECTING CODE FOR $t = 2, 3,$ OR 4. When $t = 2, 3,$ or 4, by Lemma 3.1 and Theorem 3.2, we will study the nonexistence of a perfect t-error-correcting code in S_n as follows.

When $t = 2$, by Lemma 3.1, we have that $B^n(2) = \frac{n^2-n+2}{2}$. By computing the value of $n^2 - n + 2$ for $5 \leq n \leq 17$, it follows that $n^2 - n + 2$ has a prime factor $p > n$ except for $n = 6, 11, 16$. If $n = 6$ then $B^6(2) = 16 < (2 \times 2)! = 24$. If $n = 16$ then $B^{16}(2) = 121 = 11^2$. Thus, $121 \nmid 16!$. So, by Theorem 3.2, we prove the nonexistence of a perfect two-error-correcting code in S_n, where $n^2 - n + 2$ has a prime factor $p > n$, or $5 \leq n < 11$, or $12 \leq n \leq 17$.

When $t = 3$, by Lemma 3.1, we have that $B^n(3) = \frac{(n+1)(2n^2-5n+6)}{6}$. First, if $n+1 > 8$ is a prime then $B^n(3)$ have a prime factor $n+1 > n$. Second, we compute $2n^2 - 5n + 6$ for $7 \leq n \leq 47$ and obtain that $(n + 1)(n^2 + 2n - 6)$ has a prime factor $p > n$ except for $n = 38$. If $n = 38$ then $B^{38}(3) = 17576 = 2^3 \times 13^3$. Thus, $17576 \nmid 38!$. So, by Theorem 3.2, we prove the nonexistence of a perfect three-error-correcting code in S_n, where $n+1 > 6$ is a prime, or $2n^2-5n+6$ has a prime factor $p > n$, or $7 \leq n \leq 47$.

When $t = 4$, by Lemma 3.1, we have that $B^n(4) = \frac{9n^4-46n^3+87n^2-50n+24}{24}$. By computing the value of $9n^4 - 46n^3 + 87n^2 - 50n + 24$ for $9 \leq n \leq 50$, it follows that $9n^4 - 46n^3 + 87n^2 - 50n + 24$ has a prime factor $p > n$. So, by Theorem 3.2, we prove the nonexistence of a perfect four-error-correcting code in S_n, where $9n^4 - 46n^3 + 87n^2 - 50n + 24$ has a prime factor $p > n$, or $9 \leq n \leq 50$.

By the above discussion, the following theorem is easily obtained.

Theorem 4.3. *When $t = 2$, there does not exist a perfect two-error-correcting code in S_n, where $n^2 - n + 2$ has a prime factor $p > n$, or $5 \leq n < 11$, or $12 \leq n \leq 17$. When $t = 3$, there does not exist a perfect three-error-correcting code in S_n, where $n + 1 > 6$ is a prime, or $2n^2 - 5n + 6$ has a prime factor $p > n$, or $7 \leq n \leq 47$. When $t = 4$, there does not exist a perfect four-error-correcting code in S_n, where $9n^4 - 46n^3 + 87n^2 - 50n + 24$ has a prime factor $p > n$, or $9 \leq n \leq 50$.*

4.3. THE NONEXISTENCE OF PERFECT t-ERROR-CORRECTING CODE FOR SOME FIXED $t \geq 2$. Given a fixed value of t, by Theorem 3.5, we compute the range of n such that there are no perfect t-error-correcting codes in S_n under the Hamming metric as follows. For convenience, let $f(n) = \frac{n!}{(n-t)!}$, where $n \geq 2t + 1$ and $t \geq 2$ is a fixed integer.

It follows that $\frac{f(n+1)}{f(n)} = \frac{n+1}{n-t+1} > 1$ and $f(n)$ is an increasing function. When $n = 2t+1$, we have that

$$f(2t+1) = \frac{(2t+1)!}{(t+1)!}.$$

Thus,

$$\frac{f(2t+1)}{(2t)!} = \frac{(2t+1)}{(t+1)!} < \frac{2t+1}{2(t+1)} < 1,$$

where $t \geq 2$. When $n = 4t^2+t-1$, we have that

$$\frac{f(4t^2+t-1)}{(2t)!} = \frac{(4t^2+t-1)\cdots 4t^2}{(2t)!} > \frac{(2t)^{2t}}{(2t)!} > 1.$$

Hence, there exists some integer $(2t+1) < n_0 < 4t^2+t-1$ such that $f(n_0) < (2t)!$ and $f(n_0+1) \geq (2t)!$. For convenience, let $n_0(t)$ be the integer such that $f\big(n_0(t)\big) < (2t)!$ and $f\big(n_0(t)+1\big) \geq (2t)!$, where $t \geq 2$.

By Theorem 3.5, we easily obtain the following lemma.

Lemma 4.4. *Given an integer $t \geq 2$, if $2t+1 \leq n \leq n_0(t)$ then there does not exist a perfect t-error-correcting code in S_n.*

Proof. By the definition of $n_0(t)$, we have that $\frac{f(n)}{(2t)!} < 1$ for $2t+1 \leq n \leq n_0(t)$. Hence, by Theorem 3.5, it follows that there does not exist a perfect t-error-correcting code in S_n for $2t+1 \leq n \leq n_0(t)$. □

Example 2. When $t = 2$, we have that $\frac{f(5)}{4!} = \frac{5}{6}$ and $\frac{f(6)}{4!} = \frac{5}{4}$. Hence, $n_0(2) = 5$. When $t = 3$, we have that $\frac{f(9)}{6!} = \frac{7}{10}$ and $\frac{f(10)}{6!} = 1$. Thus, $n_0(3) = 9$. When $t = 4$, we have that $\frac{f(15)}{8!} = \frac{13}{16}$ and $\frac{f(16)}{8!} = \frac{13}{12}$. It follows that $n_0(4) = 15$. When $t = 5$, we have $\frac{f(22)}{10!} = \frac{209}{240}$ and $\frac{f(23)}{10!} = \frac{4807}{4320}$. Therefore, $n_0(5) = 22$.

Now, we present the lower and upper bounds on $n_0(t)$ as follows.

Lemma 4.5. *Given an integer $t \geq 2$ and $n_0(t)$ is defined as above, we have that*

$$n_0(t) < (4t^2+4t+1)e^{-2+\gamma(t)}e^{\left(\ln(2t+1)\right)/t}, \tag{13}$$

and

$$n_0(t) \geq \max\{4t^2e^{-2+1/t} - 2, 2t+1\}, \tag{14}$$

where $\gamma(t) = \frac{t}{2(T-t)}$ and $T = \max\{4t^2e^{-2+1/t} - 2, 2t+1\}$.

Proof. First, we present the lower bound on $n_0(t)$. By the definition of $n_0(t)$ and $f(n)$, it follows that

$$f\big(n_0(t)+1\big) = \frac{\big(n_0(t)+1\big)!}{\big(n_0(t)+1-t\big)!} \geq (2t)!.$$

Then, we have that

$$\sum_{i=n_0(t)-t+2}^{n_0(t)+1} \ln i \geq \sum_{i=1}^{2t} \ln i.$$

Since $\ln i < \int_i^{i+1} \ln x dx < \ln(i+1)$ for $1 \leq i$, we have that

$$\sum_{i=1}^{2t} \ln i = \sum_{i=2}^{2t} \ln i > \sum_{i=2}^{2t} \int_{i-1}^{i} \ln x dx = \int_1^{2t} \ln x dx = 2t\ln(2t) - (2t-1), \tag{15}$$

and

$$\sum_{i=n_0(t)-t+2}^{n_0(t)+1} \ln i < \sum_{i=n_0(t)-t+2}^{n_0(t)+1} \int_i^{i+1} \ln x dx = \int_{n_0(t)-t+2}^{n_0(t)+2} \ln x dx$$

$$= \big(n_0(t)+2\big) \ln \big(n_0(t)+2\big) - \big(n_0(t)+2-t\big) \ln \big(n_0(t)+2-t\big) - t. \tag{16}$$

By (15) and (16), it follows that

$$\big(n_0(t)+2\big) \ln \big(n_0(t)+2\big) - \big(n_0(t)+2-t\big) \ln \big(n_0(t)+2-t\big) - t > 2t \ln(2t) - (2t-1).$$

Hence,

$$t \ln \big(n_0(t)+2\big) + \big(n_0(t)+2-t\big) \ln \frac{n_0(t)+2}{n_0(t)+2-t} > 2t \ln(2t) - (t-1). \tag{17}$$

Since $\ln(1+x) < x$ for $0 < x < 1$, we have that

$$\big(n_0(t)+2-t\big) \ln \frac{n_0(t)+2}{n_0(t)+2-t} > \big(n_0(t)+2-t\big) \frac{t}{n_0(t)+2-t} = t, \tag{18}$$

where $0 < \frac{t}{n_0(t)+2-t} < 1$. By (17) and (18), it follows that

$$t \ln \big(n_0(t)+2\big) > 2t \ln(2t) - (2t-1).$$

Hence, we have that

$$n_0(t) > e^{\left(2t \ln(2t) - (2t-1)\right)/t} - 2.$$

It is easily verified that

$$e^{\left(2t \ln(2t) - (2t-1)\right)/t} - 2 = e^{2 \ln(2t)} e^{-2+1/t} - 2 = 4t^2 e^{-2+1/t} - 2.$$

Moreover, since $n_0(t) \geq 2t+1$, it follows that $n_0(t) \geq \max\{4t^2 e^{-2+1/t} - 2, 2t+1\}$.

Second, we give the upper bound on $n_0(t)$. By the definition of $n_0(t)$, it follows that

$$f\big(n_0(t)\big) = \frac{n_0(t)!}{\big(n_0(t)-t\big)!} < (2t)!.$$

Then,

$$\sum_{i=n_0(t)-t+1}^{n_0(t)} \ln i < \sum_{i=1}^{2t} \ln i.$$

Since $\ln i < \int_i^{i+1} \ln x dx < \ln(i+1)$ for $1 \leq i$, we have that

$$\sum_{i=1}^{2t} \ln i < \sum_{i=1}^{2t} \int_i^{i+1} \ln x dx = \int_1^{2t+1} \ln x dx = (2t+1) \ln(2t+1) - 2t, \tag{19}$$

and

$$\sum_{i=n_0(t)-t+1}^{n_0(t)} \ln i > \sum_{i=n_0(t)-t}^{n_0(t)-1} \int_i^{i+1} \ln x dx = \int_{n_0(t)-t}^{n_0(t)} \ln x dx$$

$$= n_0(t) \ln n_0(t) - \big(n_0(t)-t\big) \ln \big(n_0(t)-t\big) - t. \tag{20}$$

By (19) and (20), it follows that

$$n_0(t) \ln n_0(t) - \big(n_0(t)-t\big) \ln \big(n_0(t)-t\big) - t < (2t+1) \ln(2t+1) - 2t.$$

Further, we have that

$$t\ln n_0(t) + \big(n_0(t)-t\big)\ln\frac{n_0(t)}{n_0(t)-t} < (2t+1)\ln(2t+1) - t. \tag{21}$$

For convenience, let $\alpha(t) = \frac{t}{2\big(n_0(t)-t\big)}$. Since $\ln(1+x) > x - x^2/2$ for $0 < x < 1$, we have that

$$\begin{aligned}\big(n_0(t)-t\big)\ln\frac{n_0(t)}{n_0(t)-t} &> \big(n_0(t)-t\big)\Big(\frac{t}{n_0(t)-t} - \frac{t^2}{2\big(n_0(t)-t\big)^2}\Big)\\ &= t\Big(1-\frac{t}{2\big(n_0(t)-t\big)}\Big) = t\big(1-\alpha(t)\big),\end{aligned} \tag{22}$$

where $0 < \frac{t}{n_0(t)-t} < 1$. By (21) and (22), it follows that

$$t\ln n_0(t) < (2t+1)\ln(2t+1) - \big(2-\alpha(t)\big)t.$$

Then,

$$n_0(t) < e^{\big((2t+1)\ln(2t+1)-(2-\alpha(t))t\big)/t}.$$

By (14) and the definition of $\gamma(t)$, since $\gamma(t) = \frac{t}{2(T-t)}$ and $n_0(t) > T$, it follows that $\gamma(t) > \alpha(t) > 0$. Hence, we have that

$$n_0(t) < e^{\big((2t+1)\ln(2t+1)-(2-\gamma(t))t\big)/t}.$$

Moreover, $e^{\big((2t+1)\ln(2t+1)-(2-\gamma(t))t\big)/t} = (4t^2+4t+1)e^{-2+\gamma(t)}e^{\big(\ln(2t+1)\big)/t}$. So, we prove the above result. □

Next, we compare the upper and lower bounds on $n_0(t)$ with the exact value of $n_0(t)$ as follows. For convenience, we denote $e^{\big((2t+1)\ln(2t+1)-(2-\gamma(t))t\big)/t}$ and $e^{\big(2t\ln(2t)-(2t-1)\big)/t} - 2$ as $Un_0(t)$ and $Ln_0(t)$, respectively.

Example 3. When $t = 2$, it follows that $Un_0(2) \approx 10.5$ and $Ln_0(2) = 5$. When $t = 3$, we have that $Un_0(3) \approx 18.5$ and $Ln_0(3) = 7$. When $t = 4$, it follows that $Un_0(4) \approx 28.4$ and $Ln_0(4) \approx 9.1$. When $t = 5$, we obtain that $Un_0(5) \approx 30.4$ and $Ln_0(5) \approx 14.5$. Moreover, we give the values of $n_0(t)$, $Un_0(t)$, and $Ln_0(t)$ for $2 \le t \le 10$, or $t = 100, 200$ in TABLE 2.

TABLE 2. The values of $n_0(t)$, $Un_0(t)$, and $Ln_0(t)$ for $2 \le t \le 10$, or $t = 100, 200$.

t	2	3	4	5	6	7	8	9	10	100	200
$n_0(t)$	5	9	15	22	30	39	49	61	73	5659	22181
$Un_0(t)$	10.5	18.5	28.4	30.4	42.9	52.5	62.8	75.2	88.2	5819.4	22528.4
$Ln_0(t)$	5	7	9.1	14.5	21.0	28.6	36.9	46.9	57.9	5465.8	21760.2

When t tends to be infinity, we will prove that $\lim\limits_{t\to\infty}\frac{Un_0(t)}{Ln_0(t)} = 1$ as follows.

Lemma 4.6. *When t tends to be infinity, we have that*

$$\lim_{t\to\infty}\frac{Un_0(t)}{Ln_0(t)} = 1.$$

Proof. First, we compare the sizes of $4t^2e^{-2+1/t}-2$ and $2t+1$ where t tends to be infinity. It is easily obtained that

$$4t^2e^{-2+1/t}-2>2t+1, \tag{23}$$

when t tends to be infinity. Thus, we only prove that $\lim_{t\to\infty}\frac{Un_0(t)}{4t^2e^{-2+1/t}-2}=1$.

Second, we compute the value of $\gamma(t)$ when t tends to be infinity. By the definition of $\gamma(t)$ and (23), we have that

$$\lim_{t\to\infty}\gamma(t)=\lim_{t\to\infty}\frac{t}{2(4t^2e^{-2+1/t}-2-t)}=0 \tag{24}$$

Finally, by (23) and (24), it follows that

$$\lim_{t\to\infty}\frac{Un_0(t)}{Ln_0(t)}=\lim_{t\to\infty}\frac{(4t^2+4t+1)e^{-2}e^{\left(\ln(2t+1)\right)/t}}{4t^2e^{-2+1/t}-2}=1$$

Hence, the lemma follows. □

By Lemmas 4.4 and 4.5, the following theorem is easily obtained.

Theorem 4.7. *Given an integer $t\geq 2$, if $2t+1\leq n\leq\max\{4t^2e^{-2+1/t}-2,2t+1\}$ then there does not exist a perfect t-error-correcting code in S_n.*

Example 4. When $t=10$, we have that $Ln_0(10)\approx 57.9$. Then, by Theorem 4.7, we have that there does not exist a perfect 10-error-correcting code in S_n for $21\leq n\leq 57$.

4.4. THE NONEXISTENCE OF PERFECT t-ERROR-CORRECTING CODE FOR SOME FIXED $n\geq 7$. In this subsection, given a fixed value of n, by Theorem 3.5, we compute the range of t such that there are no perfect t-error-correcting codes in S_n under the Hamming metric as follows. When $t=\lfloor\frac{n-1}{2}\rfloor$, it is easily verified that $\frac{n!}{(n-t)!}<(2t)!$ for $n\geq 7$. Moreover, when $t=1$, we obtain that $\frac{n!}{(n-t)!}>(2t)!$ for $n\geq 7$. Similarly, we also find the integer $t_0(n)$ such that $\frac{n!}{\left(n-t_0(n)\right)!}<\left(2t_0(n)\right)!$ and $\frac{n!}{\left(n-t_0(n)+1\right)!}\geq\left(2t_0(n)-2\right)!$.

Next, we will give the estimation of $t_0(n)$. When $t\geq 5$, we have that

$$4t^2e^{-2}-2>2t+1.$$

Hence, when $t\geq 5$ and $2t+1\leq n\leq 4t^2e^{-2}-2<4t^2e^{-2+\frac{1}{t}}-2$, by using Theorem 4.7, we have that there does not exist a perfect t-error-correcting code in S_n. So, when $n\geq 11$ and $\frac{e}{2}\sqrt{n+2}\leq t\leq\lfloor\frac{n-1}{2}\rfloor$, there does not exist a perfect t-error-correcting code in S_n. Thus, it follows that $t_0(n)\leq\frac{e}{2}\sqrt{n+2}$ for $n\geq 11$. When $7\leq n\leq 10$, we have that $\frac{e}{2}\sqrt{n+2}>\lfloor\frac{n-1}{2}\rfloor$. Thus, it follows that

$$t_0(n)\leq\min\{\frac{e}{2}\sqrt{n+2},\lfloor\frac{n-1}{2}\rfloor\}, \tag{25}$$

for $n\geq 7$.

By the above discussion, we easily obtain the following theorem.

Theorem 4.8. *Given an integer $n\geq 7$, if $\min\{\frac{e}{2}\sqrt{n+2},\lfloor\frac{n-1}{2}\rfloor\}\leq t\leq\lfloor\frac{n-1}{2}\rfloor$ then there does not exist a perfect t-error-correcting code in S_n.*

Example 5. When $n = 7$, $\min\{\frac{e}{2}\sqrt{n+2}, \lfloor\frac{n-1}{2}\rfloor\} = 3$. Hence, there does not exist a perfect 3-error-correcting code in S_7. When $n = 100$, $\min\{\frac{e}{2}\sqrt{n+2}, \lfloor\frac{n-1}{2}\rfloor\} \approx 13.8$. Thus, there does not exist a perfect t-error-correcting code in S_{100} for $13.8 \leq t \leq 49$. When $n = 1000$, $\min\{\frac{e}{2}\sqrt{n+2}, \lfloor\frac{n-1}{2}\rfloor\} \approx 43.01$. Therefore, there does not exist a perfect t-error-correcting code in S_{1000} for $43.01 \leq t \leq 499$.

5. Conclusion

Permutation codes under the Hamming metric have been studied due to their applications in power line communications and block ciphers. In this paper, we considered the nonexistence of perfect codes under the Hamming metric. We gave two sufficient conditions of the nonexistence of perfect permutation codes under the Hamming metric. Moreover, we used these sufficient conditions to prove that there does not exist a perfect t-error-correcting code in S_n under the Hamming metric for some n and $t = 1, 2, 3, 4$, or $2t + 1 \leq n \leq \max\{4t^2e^{-2+1/t} - 2, 2t + 1\}$ for $t \geq 2$, or $\min\{\frac{e}{2}\sqrt{n+2}, \lfloor\frac{n-1}{2}\rfloor\} \leq t \leq \lfloor\frac{n-1}{2}\rfloor$ for $n \geq 7$. Specifically, we proved that there does not exist a perfect one-error-correcting code in S_n. We also proved that there does not exist a perfect two-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 further proved that there does not exist a perfect three-error-correcting code in S_n,where $n + 1 > 6$ is a prime, or $2n^2 - 5n + 6$ has a prime factor $p > n$, or $7 \leq n \leq 47$. We proved that there does not exist a perfect four-error-correcting code in S_n, where $9n^4-46n^3+87n^2-50n+24$ has a prime factor $p > n$, or $9 \leq n \leq 50$. Moreover, given an integer $t \geq 2$, we proved that there does not exist a perfect t-error-correcting code in S_n, where $2t + 1 \leq n \leq \max\{4t^2e^{-2+1/t} - 2, 2t + 1\}$. Given an integer $n \geq 7$, we also proved that there does not exist a perfect t-error-correcting code in S_n, where $\min\{\frac{e}{2}\sqrt{n+2}, \lfloor\frac{n-1}{2}\rfloor\} \leq t \leq \lfloor\frac{n-1}{2}\rfloor$.

Acknowledgments

The authors are very grateful to the reviewers and the Editor for their comments and suggestions that improved the presentation and quality of this paper. This paper was supported by the National Natural Science Foundation of China (Grant No. 12001134) and the National Natural Science Foundation of China - Join Fund of Basic Research of General Technology (Grant U1836111).

References

[1] A. Barg and A. Mazumdar, Codes in permutations and error correction for rank modulation, *IEEE Trans. Inf. Theory*, **56** (2010), 3158–3165.

[2] I. F. Blake, Permutation codes for discrete channels (Corresp.), *IEEE Trans. Inform. Theory*, **20** (1974), 138–140.

[3] I. F. Blake, Coding with permutations, *Information and Control*, **43** (1979), 1–19.

[4] S. Buzaglo and T. Etzion, Bounds on the size of permutation codes with the Kendall τ-metric, *IEEE Trans. Inf. Theory*, **61** (2015), 3241–3250.

[5] W. Chu, C. J. Colbourn and P. Dukes, Constructions for permutation codes in powerline communications, *Des. Codes Cryptogr.*, **32** (2004), 51–64.

[6] C. J. Colbourn, T. Kløve and A. C. H. Ling, Permutation arrays for powerline communication and mutually orthogonal Latin squares, *IEEE Trans. Inform. Theory*, **50** (2004), 1289–1291.

[7] D. R. de la Torre, C. J. Colbourn and A. C. H. Ling, An application of permutation arrays to block ciphers, *Congr. Numer.*, **145** (2000), 5–7.

[8] M. Deza and H. Huang, Metrics on permutations, a survey, *J. Combinat. Inf. Syst. Sci.*, **23** (1998), 173–185.

[9] M. Deza and S. A. Vanstone, Bounds for permutation arrays, *J. Statist. Plann. Inference*, **2** (1978), 197–209.
[10] C. Ding, F-W. Fu, T. Kløve and V. K.-W. Wei, Constructions of permutation arrays, *IEEE Trans. Inf. Theory*, **48** (2002), 977–980.
[11] P. Dukes and N. Sawchuck, Bounds on permutation codes of distance four, *J. Algebraic Combin.*, **31** (2010), 143–158.
[12] F. Farnoud, V. Skachek and O. Milenkovic, Error-Correction in flash memories via codes in the Ulam metric, *IEEE Trans. Inf. Theory*, **59** (2013), 3003–3020.
[13] P. Frankl and M. Deza, On the maximum number of permutations with given maximal or minimal distance, *J. Combinatorial Theory, Series A*, **22** (1977), 352–360.
[14] F.-W. Fu and T. Kløve, Two constructions of permutations arrays, *IEEE Trans. Inform. Theory*, **50** (2004), 881–883.
[15] F. Gao, Y. Yang and G. N. Ge, An improvement on the Gilbert-Varshamov bound for permutation codes, *IEEE Trans. Inform. Theory*, **59** (2013), 3059–3063.
[16] A. Jiang, M. Schwartz and J. Bruck, Error-correcting codes for rank modulation, *Proc. IEEE Int. Symp. Information Theory*, (2008), 6–11.
[17] A. Jiang, M. Schwartz and J. Bruck, Correcting charge-constrained errors in the rank-modulation scheme, *IEEE Trans. Inf. Theory*, **56** (2010), 2112–2120.
[18] T. Kløve, T. T. Lin, S. C. Tsai and W. G. Tzeng, Permutation arrays under the Chebyshev distance, *IEEE Trans. Inf. Theory*, **56** (2010), 2611–2617.
[19] J. Kong and M. Hagiwara, Nonexistence of perfect permutation codes in the Ulam metric, *Proc. IEEE Int. Symp. Inf. Theory and its Applications*, (2016), 691–695.
[20] R. Montemanni and D. H. Smith, A new table of permutation codes, *Des. Codes Cryptogr.*, **63** (2012), 241–253.
[21] N. Pavlidou, A. J. H. Vinck, J. Yazdani and B. Honary, Power line communications: State of the art and future trends, *IEEE Communications Magazine*, **41** (2003), 34–40.
[22] M. Tait, A. Vardy and J. Verstraete, Asymptotic improvement of the Gilbert-Varshamov bound on the size of permutation codes, preprint, `arXiv:1311.4925`, 2013.
[23] H. Tarnanen, Upper bounds on permutation codes via linear programming, *European J. Combin.*, **20** (1999), 101–114.
[24] A. J. H. Vinck, Coded modulation for power line communications, *In AE Int. J. Electron. and Commun*, (2011), 45–49.
[25] X. Wang and F.-W. Fu, On the snake-in-the-box codes for rank modulation under Kendall's τ-metric, *Des. Codes Cryptogr.*, **83** (2017), 455–465.
[26] X. Wang and F.-W. Fu, Snake-in-the-box codes under the ℓ_∞-metric for rank modulation, *Des. Codes Cryptogr.*, **88** (2020), 487–503.
[27] X. Wang, Y. J. Wang, W. J. Yin and F-W. Fu, Nonexistence of perfect permutation codes under the Kendall τ-metric, *Des. Codes Cryptogr.*, **89** (2021), 2511–2531.
[28] X. Wang, Y. W. Zhang, Y. T. Yang and G. N. Ge, New bounds of permutation codes under Hamming metric and Kendall's τ-metric, *Des. Codes Cryptogr.*, **85** (2017), 533–545.
[29] Y. Yehezkeally and M. Schwartz, Snake-in-the-box codes for rank modulation, *IEEE Trans. Inf. Theory*, **58** (2012), 5471–5483.
[30] Y. W. Zhang and G. N. Ge, Snake-in-the-box codes for rank modulation under Kendall's τ-metric, *IEEE Trans. Inf. Theory*, **62** (2016), 151–158.

Received March 2021; 1st revision July 2021; 2nd revision September 2021; early access December 2021.

E-mail address: `xqwang@mail.nankai.edu.cn`
E-mail address: `ywjaimama@163.com`