Designs, Codes and Cryptography (2023) 91:2255–2271
https://doi.org/10.1007/s10623-023-01197-6

A new metric on symmetric groups and applications to block permutation codes

Zihan Zhang[1,2]

Received: 22 October 2021 / Revised: 12 August 2022 / Accepted: 6 February 2023 /
Published online: 3 March 2023

Abstract

Permutation codes have received a great attention due to various applications. For different applications, one needs permutation codes under different metrics. The generalized Cayley metric was introduced by Chee and Vu (in: 2014 IEEE international symposium on information theory, Honolulu, June 29–July 4, 2014, pp 2959–2963, 2014) and this metric includes several other metrics as special cases. However, the generalized Cayley metric is not easily computable in general. Therefore the block permutation metric was introduced by Yang et al. (IEEE Trans Inf Theory 65(8):4746–4763, 2019) as the generalized Cayley metric and the block permutation metric have the same magnitude. In this paper, by introducing a novel metric closely related to the block permutation metric, we build a bridge between some advanced algebraic methods and codes in the block permutation metric. More specifically, based on some techniques from algebraic function fields originated in Xing (IEEE Trans Inf Theory 48(11):2995–2997, 2002), we give an algebraic-geometric construction of codes in the novel metric with reasonably good parameters. By observing a trivial relation between the novel metric and block permutation metric, we then produce non-systematic codes in block permutation metric that improve all known results given in Xu et al. (Des Codes Cryptogr 87(11):2625–2637, 2019) and Yang et al. (2019). More importantly, based on our non-systematic codes, we provide an explicit and systematic construction of codes in the block permutation metric which improves the systematic result shown in Yang et al. (2019). In the end, we demonstrate that our codes in the novel metric itself have reasonably good parameters by showing that our construction beats the corresponding Gilbert–Varshamov bound.

Keywords Block permutation codes · Cyclic block permutation codes · Rational function fields · Gilbert–Varshamov bound

Communicated by M. Lavrauw.

✉ Zihan Zhang
zzhsdj@foxmail.com

[1] Present Address: Department of Computer Science and Engineering, The Ohio State University, Columbus, OH 43210, USA

[2] School of Mathematics, Sichuan University, Chengdu 610065, China

Mathematics Subject Classification 94B25 · 94B65 · 94B27

1 Introduction

In the years of 1977–1978, permutation codes were first introduced as a purely combinatorial problem (see [6, 9]). Recently, due to several applications, the topic of permutation codes has attracted much attention from both coding scientists and mathematicians (see [4, 5, 7, 10, 16, 18]). Permutation codes under different metrics such as Kendall's τ-metric, Ulam metric and Cayley metric have been extensively studied in clouding storage systems, genome re-sequencing and the rank modulation scheme of flash memories (see [1, 2, 8, 11, 12]).

Chee and Vu [3] first introduced the generalized Cayley metric which includes the aforementioned metrics as special cases. Furthermore, they gave an explicit construction of such codes based on the interleaving technique. However, due to the fact that the generalized Cayley metric is difficult to compute, there is large room for improving the codes given in the construction of [3].

Recently, Yang et al. [22] introduced the block permutation metric, which could be easily computed and is of the same magnitude order as the generalized Cayley metric. Via the metric embedding method, they reduced the problem of constructing codes with generalized Cayley metric to the problem of constructing codes with block permutation metric. In the meantime, they first gave a non-explicit and non-systematic construction of codes in block permutation metric. Based on their non-explicit construction, they then gave an explicit and systematic[1] construction of codes in block permutation metric. Moreover, they proved that both of their proposed codes above in generalized Cayley metric are more rate efficient than the one constructed in [3].

Very recently, Xu et al. gave a better non-explicit and non-systematic construction of codes with block permutation metric through an idea for constructing constant weight binary codes under Hamming metric, as a part of their results (see [21]).

1.1 Our contributions

From the mathematical point of view, the block permutation metric is not natural as the last pair $(n, 1)$ is not included in the characteristic set making the characteristic set less symmetric. As a result, this restricts the use of some potential mathematical tools to study block permutation codes. On the other hand, if we include $(n, 1)$ in the characteristic set, then the definition would not yield a valid distance as two distinct permutations could have distance 0. To solve this problem, we can consider a certain quotient group of the symmetric group $\mathcal{S}_n$ (or equivalently a subset of $\mathcal{S}_n$ consisting of those elements that belong to distinct cosets). We refer the reader to Sect. 2 for more details.

In this paper, by including $(n, 1)$ in the characteristic set, we introduce a new metric which we call the cyclic block permutation metric. This new metric is defined on a quotient group $\mathcal{S}_n/\langle\omega\rangle$, where ω is the cycle $(123\cdots n)$. Under this new metric, we introduce a class of codes which we call cyclic block permutation codes. Based on some techniques from algebraic function fields that originated in [19], we give an algebraic-geometric construction

[1] For a permutation $\sigma \in \mathcal{S}_n$, denote $\sigma_{(k)}$ by the permutation in $\mathcal{S}_k$ obtained from σ after deleting all the elements of $\{k+1, k+2, \ldots, n\}$ in σ. Recall that a permutation code $\mathcal{C} \subset \mathcal{S}_n$ is called (n, k) systematic if for every $\alpha \in \mathcal{S}_k$ there exists exactly one codeword σ of $\mathcal{C}$ such that $\sigma_{(k)} = \alpha$. Otherwise, we call the permutation codes non-systematic (See [2, Section II]).

Table 1 Several known constructions of the block permutation codes

Source	Systematic?	Explicit?	Length	Distance	Code size
See [22]	×	×	n	$\geq d$	$\Omega_d\left(n!/n^{4d-6}\right)$
See [21]	×	×	n	$\geq d$	$\Omega_d\left(n!/n^{2d-2}\right)$
Theorem 1(i)	×	×	n	$\geq d$	$\Omega_d\left(n!/n^{d}\right)$
See [22]	✓	✓	n	$\geq d$	$(n-28d+28)!$
Theorem 1(ii)	✓	✓	n	$\geq d$	$(n-3d+1)!$

of cyclic block permutation codes with reasonably good parameters. By observing a trivial relation between the cyclic block permutation metric and the block permutation metric, we produce non-systematic codes in the block permutation metric that improve all known results given in [21, 22]. More importantly, based on our non-systematic construction, we gave an explicit and systematic construction of codes in the block permutation metric with parameters better than those given in [22]. One major novelty of this paper is that we build a new carefully designed metric on symmetric groups (closely related to block permutation metric) so that an algebraic-geometric method can be modified to construct better block permutation codes. We present our main contributions of both non-systematic and systematic constructions by a summarized theorem below. A table summarizing all related works is presented in Table 1.

Theorem 1 (Main results, informal version) (i) *A non-explicit construction of block permutation codes* $\mathcal{C} \subset \mathcal{S}_n$ *with minimum distance at least* d *and size at least* $\Omega_d\left(\frac{n!}{n^d}\right)$ *is given in Theorem 5 based on our algebraic-geometric-based construction* (*see Sect.* 3.2). (ii) *We provide an explicit construction of systematic block permutation codes of length* n*, distance* d *and size* $(n-3d+1)!$*, whenever* $n \geq 37, d \geq 4$ *and* $n \geq 9d+1$ (*see Corollary* 2).

Back to the cyclic block permutation codes, to demonstrate that our construction indeed has reasonably good parameters, we compare our codes with the Gilbert–Varshamov bound for cyclic block permutation codes. The comparison shows that our codes beat the Gilbert–Varshamov bound by a multiplicative factor n for constant distance d. It should be mentioned that to compare with the Gilbert–Varshamov bound, one needs to estimate the size of a ball under the cyclic block permutation metric. We managed to obtain a lower bound on the size of a ball and we believe that this is close to the exact size up to a constant factor.

1.2 Outline of this paper

In Sect. 2, we introduce a new metric called the cyclic block permutation metric and study some properties that are needed in this paper. In Sect. 3, we provide some background on function fields and give a construction of cyclic block permutation codes from function fields. In Sect. 4, via a simple relation between the cyclic block permutation metric and the block permutation metric, we first produce non-systematic block permutation codes which have the best-known parameters. Then we gave our explicit systematic block permutation codes, which also have the best-known parameters. In Sect. 5, we show that our algebraic-geometric construction beats the Gilbert–Varshamov bound. In the last section, we give several possible future directions for improving both our methods and results.

2 A new metric

This section gives a brief introduction to our novel metric. To be noted, this could be seen as one of the crucial contributions in this paper since it connects codes in the block permutation metric with the advanced algebraic-geometric methods shown in Sect. 3. As far as we are concerned, those tricks can't be applied directly to the construction of codes in the block permutation metric.

By abuse of notation, we denote by $\mathbb{Z}_n$ the set $\{1, 2, \ldots, n\}$. We define the addition $\oplus$ in $\mathbb{Z}_n$ as follows: for any $i, j \in \mathbb{Z}_n$, define

$$i \oplus j = \begin{cases} i + j \pmod n & \text{if} n \nmid (i \pm j) \\ n & \text{if} n \mid (i \pm j) \end{cases}$$

We define subtraction $\ominus$ in $\mathbb{Z}_n$ similarly. Our new addition/subtraction will be mainly applied in the following of this section as well as in our construction (3.1). In case there is no confusion, we still use ± to denote addition and subtraction in $\mathbb{Z}_n$. Denote by $\mathcal{S}_n$ the set of bijections from $\mathbb{Z}_n$ to $\mathbb{Z}_n$, i.e., $\mathcal{S}_n$ is the symmetric group of order $n!$. For an element $\sigma \in \mathcal{S}_n$, recall that the characteristic set of σ is defined as follows (see [22])

$$A(\sigma) := \{(\sigma(i), \sigma(i+1)) : i \in \mathbb{Z}_n \setminus \{n\}\}.$$

The pair $(\sigma(n), \sigma(n+1)) = (\sigma(n), \sigma(1))$ is missing in the set $A(\sigma)$. We complete the characteristic set $A(\sigma)$ by including $(\sigma(n), \sigma(1))$. Thus we define the *cyclic characteristic set* of σ by

$$A_c(\sigma) = \{(\sigma(i), \sigma(i+1)) : i \in \mathbb{Z}_n\}.$$

It is clear that

$$A_c(\sigma) = \{(i, \pi(i)) : i \in \mathbb{Z}_n\}$$

for some $\pi \in \mathcal{S}_n$.

Lemma 1 *If*

$$A_c(\sigma) = \{(i, \pi(i)) : i \in \mathbb{Z}_n\}$$

for some $\pi \in \mathcal{S}_n$, then $\pi(i) = \sigma(\sigma^{-1}(i) + 1)$ for all $i \in \mathbb{Z}_n$, i.e.,

$$A_c(\sigma) = \{(i, \sigma(\sigma^{-1}(i) + 1)) : i \in \mathbb{Z}_n\}.$$

Proof Let $\sigma(j) = i$ for some $j \in \mathbb{Z}_n$. Then we must have $\pi(i) = \sigma(j+1)$. As $j = \sigma^{-1}(i)$, we have

$$\pi(i) = \sigma(j+1) = \sigma(\sigma^{-1}(i) + 1).$$

The proof is completed. □

Throughout this paper, we denote by ϵ and ω the identity of $\mathcal{S}_n$ and the cycle $(12 \cdots n)$, respectively. Then the block permutation distance between two permutations $\sigma, \tau \in \mathcal{S}_n$ given by

$$d_B(\sigma, \tau) := |A(\sigma) \setminus A(\tau)| = n - |A(\sigma) \cap A(\tau)|$$

is indeed a distance on S_n (see [22]). Hence, it induces a metric on $\mathcal{S}_n$ given by

$$\|\sigma\|_B := |A(\sigma) \setminus A(\epsilon)| = n - |A(\sigma) \cap A(\epsilon)|.$$

However, a similar definition induced by the cyclic characteristic set does not produce a distance on $\mathcal{S}_n$, i.e.,

$$d_C(\sigma, \tau) := |A_c(\sigma) \setminus A_c(\tau)| = n - |A_c(\sigma) \cap A_c(\tau)|$$

is not a distance on $\mathcal{S}_n$. This is because $d_C(\omega, \epsilon) = 0$, but $\omega \neq \epsilon$. To make d_C into a distance, we consider left cosets of $\langle\omega\rangle$ in $\mathcal{S}_n$.

Lemma 2 *Let $\sigma, \tau \in \mathcal{S}_n$ be two permutations. Then $A_c(\sigma) = A_c(\tau)$ if and only if σ, τ belong to the same left coset of $\langle\omega\rangle$.*

Proof Assume that σ, τ belong to the same left coset of $\langle\omega\rangle$. Then $\tau = \sigma\omega^k$ for some $k \geq 0$. Hence

$$\begin{aligned}\tau(\tau^{-1}(i) + 1) &= \sigma\omega^k((\sigma\omega^k)^{-1}(i) + 1) = \sigma\omega^k(\omega^{-k}\sigma^{-1}(i) + 1)\\ &= \sigma\omega^k(\sigma^{-1}(i) + 1 - k) = \sigma(\sigma^{-1}(i) + 1).\end{aligned}$$

This implies that $A_c(\sigma) = A_c(\tau)$ by Lemma 1. Now we assume that $A_c(\sigma) = A_c(\tau)$. By Lemma 1, we have $\tau(\tau^{-1}(i)+1) = \sigma(\sigma^{-1}(i)+1)$ for all $i \in \mathbb{Z}_n$. Let $\sigma(j) = 1$ and $\tau(\ell) = 1$ for some $j, \ell \in \mathbb{Z}_n$. Then we have

$$\begin{aligned}\tau(\ell + 1) &= \tau(\tau^{-1}(\tau(\ell)) + 1) = \tau(\tau^{-1}(1) + 1)\\ &= \sigma(\sigma^{-1}(1) + 1) = \sigma(\sigma^{-1}(\sigma(j)) + 1) = \sigma(j + 1).\end{aligned}$$

Put $u = \tau(\ell + 1) = \sigma(j + 1)$. Then we have

$$\begin{aligned}\tau(\ell + 2) &= \tau(\tau^{-1}(\tau(\ell + 1)) + 1) = \tau(\tau^{-1}(u) + 1)\\ &= \sigma(\sigma^{-1}(u) + 1) = \sigma(\sigma^{-1}(\sigma(j + 1)) + 1) = \sigma(j + 2).\end{aligned}$$

Continuing in this fashion, one can prove that $\tau(\ell+i) = \sigma(j+i)$ for all $i \in \mathbb{Z}_n$. This implies that $\tau = \sigma\omega^{\ell-j}$, i.e., they belong to the same coset. □

By abuse of notation, we denote by $\mathcal{S}_n/\langle\omega\rangle$ the set of left cosets of $\langle\omega\rangle$. For $\sigma \in \mathcal{S}_n$, we denote by $\overline{\sigma} \in \mathcal{S}_n/\langle\omega\rangle$ the coset represented by σ. Due to Lemma 2, we can define a map d_C from $(\mathcal{S}_n/\langle\omega\rangle) \times (\mathcal{S}_n/\langle\omega\rangle)$ to $[0, n]$ by

$$d_C(\overline{\sigma}, \overline{\tau}) := |A_c(\sigma) \setminus A_c(\tau)| = n - |A_c(\sigma) \cap A_c(\tau)|. \tag{2.1}$$

Theorem 2 *The map d_C given in (2.1) is a distance on $\mathcal{S}_n/\langle\omega\rangle$.*

Proof By the definition of d_C and Lemma 2, one immediately deduces that $d_C(\overline{\sigma}, \overline{\tau}) \geq 0$ and $d_C(\overline{\sigma}, \overline{\tau}) = 0$ if and only if $\overline{\sigma} = \overline{\tau}$, for any $\overline{\sigma}, \overline{\tau} \in \mathcal{S}_n/\langle\omega\rangle$. From (2.1), one has $d_C(\overline{\sigma}, \overline{\tau}) = n - |A_c(\sigma) \cap A_c(\tau)| = d_C(\overline{\tau}, \overline{\sigma})$.

It remains to prove the triangle inequality. To do so, let A, B, C be three sets with $|A| = |B| = |C| = n$. Then,

$$\begin{aligned}n = |B| &\geq |(A \cap B) \cup (C \cap B)| = |A \cap B| + |C \cap B| - |A \cap B \cap C|\\ &\geq |A \cap B| + |C \cap B| - |A \cap C|\end{aligned}$$

This gives

$$n - |A \cap C| \leq n - |A \cap B| + n - |C \cap B|. \tag{2.2}$$

Now put $A = A_c(\sigma)$, $B = A_c(\tau)$, $C = A_c(\theta)$ for any three permutations $\sigma, \tau, \theta \in \mathcal{S}_n$. It follows from (2.2) that

$$d_C(\overline{\sigma}, \overline{\theta}) \leq d_C(\overline{\sigma}, \overline{\tau}) + d_C(\overline{\tau}, \overline{\theta}).$$

In conclusion, the $d_C : (\mathcal{S}_n/\langle\omega\rangle) \times (\mathcal{S}_n/\langle\omega\rangle) \to [0, n]$ is a distance on $\mathcal{S}_n/\langle\omega\rangle$. □

The distance defined in (2.1) is called the *cyclic block permutation distance*. Now one can define the *cyclic block permutation metric* on $\mathcal{S}_n/\langle\omega\rangle$:

$$||\overline{\sigma}||_C := |A_c(\sigma) \setminus A_c(\epsilon)| = n - |A_c(\sigma) \cap A_c(\epsilon)|.$$

Furthermore, we introduce a new class of codes called the *cyclic block permutation codes* under the cyclic block permutation metric. A cyclic block permutation code is a subset of $\mathcal{S}_n/\langle\omega\rangle$ equipped with the cyclic block permutation distance. The minimum distance of a cyclic block permutation code is defined to be the smallest distance between any pair of two distinct cosets in the code.

3 Construction via rational function fields

In this section, we first introduce some background on function fields that is needed for the construction of cyclic block permutation codes. Then we present the details of our construction of cyclic block permutation codes.

3.1 Background on function fields

This section provides some necessary background on algebraic function fields. The reader may refer to [17] for details. Let p be a rational prime and let x be a transcendental element over the finite field $\mathbb{F}_p$. Let us consider the rational function field $F := \mathbb{F}_p(x)$. For every irreducible polynomial $P(x) \in \mathbb{F}_p[x]$, we define a discrete valuation ν_P which is a map from $\mathbb{F}_p[x]$ to $\mathbb{Z} \cup \{\infty\}$ given by $\nu_P(0) = \infty$ and $\nu_P(f) = a$, where f is a nonzero polynomial and a is the unique nonnegative integer satisfying $P^a | f$ and $P^{a+1} \nmid f$. This map can be extended to $\mathbb{F}_p(x)$ by defining $\nu_P(f/g) = \nu_P(f) - \nu_P(g)$ for any two polynomials $f, g \in \mathbb{F}_p[x]$ with $g \neq 0$. Apart from the above finite discrete valuation ν_P, we have an infinite valuation ν_∞ (or ν_{P_∞}) defined by $\nu_\infty(f/g) = \deg(g) - \deg(f)$ for any two polynomials $f, g \in \mathbb{F}_p[x]$ with $g \neq 0$. Note that we define $\deg(0) = \infty$. The set of places of F is denoted by $\mathbb{P}_F$.

For each discrete valuation ν_P (P is either a polynomial or $P_\infty = \infty$), by abuse of notation we still denote by P the set $\{y \in F : \nu_P(y) > 0\}$. Then the set P is called a place of F. If $P = x - \alpha$, then we denote P by P_α. The degree of the place P is defined to be the degree of the corresponding polynomial $P(x)$. If P is the infinite place ∞, then the degree of ∞ is defined to be 1. A place of degree 1 is called rational.

Let F'/F be a finite separable extension. Then for every place of P' of F', there is only one place P of F such that $P \subseteq P'$. The ramification of P' or P'/P, denoted by $e(P'|P)$, is defined to be the number e satisfying $\nu_{P'}(f) = e \cdot \nu_P(f)$ for all $f \in F$. There is a close relation between the ramification index $e(P'|P)$ and the different exponent $d(P'|P)$ (see [17, Definition 3.4.3] for the definition of different exponent). Precisely speaking, it is given by the following result (see [17, Theorem 3.5.1]).

Lemma 3 *Let F'/F be a finite separable extension of algebraic function fields having the same constant field K and $P' \mid P$, then*

i $d(P'|P) \geq e(P'|P) - 1$ *and equality holds if* $\gcd(e(P'|P), p) = 1$;
ii $d(P'|P) \geq e(P'|P)$ *if* $p|e(P'|P)$,

The following results play a very important role in our construction.

Lemma 4 (Separable Extension) *Let* $f_1(x), \ldots, f_r(x) \in \mathbb{F}_p[x]$ *be pairwise coprime irreducible polynomials. Let* $e_i \in \mathbb{Z}$ *be integers for* $1 \leq i \leq r$. *Let* z *be the rational function* $\prod_{i=1}^r f_i(x)^{e_i}$. *We assume that* $e_i \not\equiv 0 \pmod{p}$ *for at least one* i. *Denote by* I^+ *and* I^- *the set* $\{1 \leq i \leq r \mid e_i > 0\}$ *and the set* $\{1 \leq i \leq r \mid e_i < 0\}$, *respectively. Then*

(i) *The extension* $\mathbb{F}_p(x)/\mathbb{F}_p(z)$ *is a finite separable extension.*
(ii) $\mathbb{F}_p(x)/\mathbb{F}_p(z)$ *is a separable extension of degree* $\max\left\{\sum_{i\in I^+} e_i, -\sum_{j\in I^-} e_j\right\}$.
(iii) *In the extension* $\mathbb{F}_p(x)/\mathbb{F}_p(z)$, *the zero of* z *splits into those places corresponding to the irreducible polynomials* $f_i(x)$ *with ramification index* e_i *for* $i \in I^+$, *while the pole of* z *splits into those places corresponding to the irreducible polynomials* $f_j(x)$ *with ramification index* e_j *for* $i \in I^-$.
(iv) *The ramification index of the pole of* x *is*

$$\left|\sum_{i=1}^r e_i\right| = \max\left\{\sum_{i\in I^+} e_i, -\sum_{j\in I^-} e_j\right\} - \min\left\{\sum_{i\in I^+} e_i, -\sum_{j\in I^-} e_j\right\}.$$

Proof (i) follows from [17, Proposition 3.10.2(a)]. (ii)–(iv) follows from the fact that the principal divisor of z is

$$(z) = \left(\prod_{i=1}^r f_i^{e_i}\right) = \sum_{i=1}^r P_i^{e_i} - \left(\sum_{i=1}^r e_j\right) P_\infty,$$

where P_i is the place of $\mathbb{F}_p(x)$ corresponding to $f_i(x)$ and P_∞ is the pole of x. □

The genus $g(F)$ of a function field F is an important invariant. We refer to [17, Section 1.5] for the definition of genus. The rational function field always has genus 0. On the other hand, every non-rational function field has genus greater than 0. The following result is called the Hurwitz Genus Formula (see [17, Theorem 3.4.13]).

Theorem 3 (Hurwitz Genus Formula) *Let* F'/F *be a finite separable extension of algebraic function fields having the same constant field with genus* $g(F')$ *and* $g(F)$, *respectively, then*

$$2g(F') - 2 = [F' : F](2g(F) - 2) + \sum_{P\in\mathbb{P}_F} \sum_{P'|P} d(P'|P) \deg P',$$

where $\mathbb{P}_F$ *stands for the set of places of* F.

For our construction, we need to consider a residue ring and its multiplicative group. Let $f \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree m. Consider the residue group

$$G := (\mathbb{F}_p[x]/(f^2))^\times = \left\{\widetilde{h} \in \mathbb{F}_p[x]/(f^2) \middle| \gcd(h, f) = 1\right\}.$$

Denote by G^p the p-th power of G, i.e., $G^p := \{a^p \mid a \in G\}$. Then the group structure of the quotient group G/G^p can be found in [15, Lemma 4.2.5].

Lemma 5 *The quotient group is an elementary abelian group of rank* m, *i.e.,*

$$G/G^p \simeq \mathbb{F}_p^m.$$

3.2 Construction

In this section, we provide an algebraic-geometric-based construction of cyclic block permutation codes with reasonable parameters. The main idea of our construction was first used by Xing in [19, 20] for the construction of classical block codes. Later the same idea was employed by Jin [13] for the construction of permutation codes with Hamming distance. In this section, we make use of the same idea to construct our cyclic block permutation codes. In order to apply Xing's idea, one of our crucial modifications is the key map (3.1) below. Our Theorem 4 below is influenced by the Theorem 2 in [13]. However, we consider it by considering $\alpha_{\sigma(i)}$ instead of α_i as showed in (3.1). Note that this step makes our construction essentially different from what Jin constructed.

For an integer $n \geq 4$, we choose the smallest prime number p such that $p \geq n$. Therefore, we can have n different elements $\alpha_1, \cdots, \alpha_n \in \mathbb{F}_p$. Next, we choose an arbitrary irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ such that $\deg f = d - 2$ with $d \geq 4$. Define the map:

$$\Delta_d : \mathcal{S}_n/\langle\omega\rangle \to G/G^p; \quad \overline{\sigma} \mapsto \left[\widetilde{\prod_{i \in \mathbb{Z}_n} \left(x - \alpha_{\sigma(i)}\right)^{\sigma(i+1)}}\right], \tag{3.1}$$

where the group $G := (\mathbb{F}_p[x]/f^2)^{\times}$ and $[\cdot]$ stands for an element of G/G^p. It is easy to see that the map Δ_d is well defined.

In the rest of this section, we will show that every non-empty fiber of the map Δ_d is a cyclic block permutation code with minimum distance at least d.

Theorem 4 *For any fixed $[\widetilde{y}] \in G/G^p$, any non-empty set $\Delta_d^{-1}([\widetilde{y}]) \subset \mathcal{S}_n/\langle\omega\rangle$ is a cyclic block permutation code with minimum distance at least d.*

Proof Let $\overline{\sigma}, \overline{\tau}$ be two different elements in $\Delta_d^{-1}([\widetilde{y}])$. By definition, one has $\Delta_d(\overline{\sigma}) = \Delta_d(\overline{\tau}) = [\widetilde{y}]$, i.e., $\left[\widetilde{\left(\frac{\prod_{i=1}^n (x-\alpha_{\sigma(i)})^{\sigma(i+1)}}{\prod_{i=1}^n (x-\alpha_{\tau(i)})^{\tau(i+1)}}\right)}\right] = [\widetilde{1}]$. Therefore, there are two polynomials $h, g \in \mathbb{F}_p[x]$ with $\gcd(hg, f) = 1$ such that

$$\widetilde{\left(\frac{\prod_{i=1}^n \left(x - \alpha_{\sigma(i)}\right)^{\sigma(i+1)}}{\prod_{i=1}^n \left(x - \alpha_{\tau(i)}\right)^{\tau(i+1)}}\right)} = \left(\widetilde{\frac{g(x)}{h(x)}}\right)^p.$$

This is equivalent to

$$\frac{h(x)^p \prod_{i=1}^n y \left(x - \alpha_{\sigma(i)}\right)^{\sigma(i+1)}}{g(x)^p \prod_{i=1}^n \left(x - \alpha_{\tau(i)}\right)^{\tau(i+1)}} \equiv 1 \mod f(x)^2. \tag{3.2}$$

We denote by z the function

$$z := \frac{h(x)^p \prod_{i=1}^n \left(x - \alpha_{\sigma(i)}\right)^{\sigma(i+1)}}{g(x)^p \prod_{i=1}^n \left(x - \alpha_{\tau(i)}\right)^{\tau(i+1)}}.$$

Assume that $A_c(\sigma) = \{(i, \pi(i)) \mid i \in \mathbb{Z}_n\}$ for some $\pi \in \mathcal{S}_n$ and $A_c(\tau) = \{(i, \psi(i)) \mid i \in \mathbb{Z}_n\}$ for some $\psi \in \mathcal{S}_n$. Put $S = \{i \in \mathbb{Z}_n \mid \pi(i) > \psi(i)\}$ and $T = \{i \in \mathbb{Z}_n \mid \psi(i) > \pi(i)\}$. Then $d_C(\overline{\sigma}, \overline{\tau}) = |S| + |T|$ and z can be rewritten as

$$z = \frac{\prod_{k=1}^r h_k(x)^{pa_k}}{\prod_{\ell=1}^r g_\ell(x)^{pb_\ell}} \times \frac{\prod_{i \in S} (x - \alpha_i)^{u_i}}{\prod_{j \in T} (x - \alpha_j)^{v_j}}, \tag{3.3}$$

where $h_k(x)$, $g_\ell(x)$ are irreducible polynomials and a_k, b_l, u_i, v_j are positive integers satisfying $1 \le u_i, v_i \le n-1 \le p-1$. By Lemma 4, $\mathbb{F}_p(x)/\mathbb{F}_p(z)$ is separable. Let us summarize a few facts listed below.

(a) S, T are two disjoint non-empty subsets of $\mathbb{Z}_n$;
(b) $d_C(\overline{\sigma}, \overline{\tau}) = |S| + |T|$;
(c) $\sum_{i\in S} u_i - \sum_{j\in T} v_j = 0$;
(d) The extension degree is

$$[\mathbb{F}_p(x) : \mathbb{F}_p(z)] = \max\left\{ \sum_{k=1}^{r} pa_k \deg h_k + \sum_{i\in S} u_i, \sum_{\ell=1}^{t} pb_\ell \deg g_\ell + \sum_{j\in T} v_j \right\}.$$

Without loss of generality, we may assume that $\sum_{k=1}^{r} pa_k \deg h_k + \sum_{i\in S} u_i \ge \sum_{\ell=1}^{t} pb_\ell \deg g_\ell + \sum_{j\in T} v_j$. In order to apply the Hurwitz Genus Formula, we have to analyze ramification indices of places. By Lemma 4, we have the following facts:

(e) The ramification index of the pole of x is

$$\left| \sum_{k=1}^{r} pa_k \deg h_k - \sum_{\ell=1}^{t} pb_\ell \deg g_\ell \right| = \sum_{k=1}^{r} pa_k \deg h_k - \sum_{\ell=1}^{t} pb_\ell \deg g_\ell.$$

(f) The ramification index of the place corresponding to $h_k(x)$ is pa_k and the ramification index of the place corresponding to $g_\ell(x)$ is pb_ℓ.
(g) The ramification index of $x - \alpha_i$ for $i \in S$ is u_i and the ramification index $x - \alpha_i$ for $i \in T$ is v_i.
(h) As $f(x)^2$ divides $z - 1$, the ramification index of the place corresponding to $f(x)$ is at least 2.

Now we apply the Hurwitz Genus Formula for the extension as well as Lemma 3.

$$\begin{aligned}
-2 = 2g(\mathbb{F}_p(x)) - 2 &= (2g(\mathbb{F}_p(z)) - 2)[\mathbb{F}_p(x) : \mathbb{F}_p(z)] + \sum_{P\in\mathbb{P}_{\mathbb{F}_p(z)}} \sum_{P'|P} d(P'|P) \deg P' \\
&\ge -2\left(\sum_{k=1}^{r} pa_k \deg h_k + \sum_{i\in S} u_i\right) + \left(\sum_{k=1}^{r} pa_k \deg h_k - \sum_{\ell=1}^{t} pb_\ell \deg g_\ell\right) \\
&\quad + \sum_{k=1}^{r} pa_k \deg h_k + \sum_{\ell=1}^{t} pb_\ell \deg g_\ell + \sum_{i\in S}(u_i - 1) + \sum_{j\in T}(v_j - 1) + \deg(f) \\
&= -|S| - |T| + d - 2 = -d_C(\overline{\sigma}, \overline{\tau}) + d - 2.
\end{aligned}$$

This gives $d_C(\overline{\sigma}, \overline{\tau}) \ge d$ and the proof is completed. □

Let $M_C(n, d)$ denote the maximum size of a cyclic block permutation code in $\mathcal{S}_n/\langle\omega\rangle$ of minimum distance at least d.

Corollary 1 *For any $n, d \ge 4$, we have*

$$M_C(n, d) \ge \frac{(n-1)!}{p^{d-2}}.$$

Proof By the Pigeonhole Principle and Theorem 4, there exists an element $[\widetilde{y_0}] \in G/G^p$ such that the size $\Delta_d^{-1}([\widetilde{y_0}])$ is at least

$$\frac{|\mathcal{S}_n/\langle\omega\rangle|}{|G/G^p|} = \frac{(n-1)!}{p^{d-2}}.$$

By Theorem 4, $\Delta_d^{-1}([\widetilde{y_0}])$ is a cyclic block permutation code in $\mathcal{S}_n/\langle\omega\rangle$ of minimum distance at least d. □

4 Applications to block permutation codes

In this section, we first show that our cyclic block permutation codes constructed in Subsect. 3.2 can be easily converted into a class of non-systematic block permutation codes. Furthermore, block permutation codes obtained from our construction improve the best-known non-systematic construction.

Secondly, we provide an explicit systematic construction of block permutation codes based on our improved non-systematic construction. The main idea of our construction came from [22]. Moreover, our explicit systematic construction largely improves the best-known parameters.

4.1 Non-systematic construction

In this paper, if we can partition $\mathcal{S}_n$ into disjoint sets, each is a block permutation code with distance at least d, we call this a non-systematic construction and codes obtained in this way are called non-systematic block permutation codes.

In this section, via our construction given in Subsect. 3.2, we provide a construction of non-systematic block permutation codes by partitioning $\mathcal{S}_n$ into disjoint block permutation codes, each with minimum distance at least d.

Theorem 5 *For any $n, d \geq 4$ and a prime $p \in [n, 2n)$, there exists a map*

$$\nabla_{(p,d)} : \mathcal{S}_n \to \mathbb{F}_p^{d-1} \times \mathbb{Z}_n,$$

where we can partition $\mathcal{S}_n$ into at most $n \times p^{d-1}$ disjoint block permutation codes by

$$\{\nabla_{(p,d)}^{-1}((\boldsymbol{\alpha}, s)) \mid (\boldsymbol{\alpha}, s) \in \mathbb{F}_p^{d-1} \times \mathbb{Z}_n, \nabla_{(p,d)}^{-1}((\boldsymbol{\alpha}, s)) \neq \emptyset\}, \tag{4.1}$$

each with minimum distance at least d.

Proof In Subsect. 3.2, we replace d by $d+1$. Recall our key map Δ_{d+1} defined in (3.1). Now we define

$$\widetilde{\Delta_{d+1}} : \mathcal{S}_n/\langle\omega\rangle \to \mathbb{F}_p^{d-1}; \quad \widetilde{\Delta_{d+1}} := \phi \circ \Delta_{d+1},$$

where $\phi : G/G^p \to \mathbb{F}_p^{d-1}$ is a natural group isomorphism given by Lemma 5. Then, one immediately obtains a partition of $\mathcal{S}_n/\langle\omega\rangle$ given by

$$\{\widetilde{\Delta_{d+1}}^{-1}(\boldsymbol{\alpha}) \mid \boldsymbol{\alpha} \in \mathbb{F}_p^{d-1}, \widetilde{\Delta_{d+1}}^{-1}(\boldsymbol{\alpha}) \neq \emptyset\}.$$

Theorem 4 shows that every non-empty subset $\widetilde{\Delta_{d+1}}^{-1}(\boldsymbol{\alpha}) \subset \mathcal{S}_n/\langle\omega\rangle$ is a cyclic block permutation code with minimum distance at least $d+1$.

Now we collect only one element from each coset in $\mathcal{S}_n/\langle\omega\rangle$ to form an embedding map from $\mathcal{S}_n/\langle\omega\rangle$ to $\mathcal{S}_n$. Repeating this process n times, one can easily find n embedding maps $\{i_s\}_{s=1}^n$ from $\mathcal{S}_n/\langle\omega\rangle$ to $\mathcal{S}_n$, which exactly partition off $\mathcal{S}_n$ into n parts by $\{i_s(\mathcal{S}_n/\langle\omega\rangle) \subset \mathcal{S}_n \mid 1 \leq s \leq n\}$.

The definition of $\{i_s\}_{s=1}^n$ implies that for any $\sigma \in \mathcal{S}_n$, there's a unique s_σ with $1 \le s_\sigma \le n$ such that $i_{s_\sigma}(\overline{\sigma}) = \sigma$. Therefore, we can define our desire map $\nabla_{(p,d)}$ by

$$\nabla_{(p,d)} : \mathcal{S}_n \to \mathbb{F}_p^{d-1} \times \mathbb{Z}_n; \quad \nabla_{(p,d)}(\sigma) \mapsto (\widetilde{\Delta_{d+1}}(\overline{\sigma}), s_\sigma).$$

It is easy to see that the above map is well defined.

Finally, to finish the proof, we only need to show that any non-empty subset $\nabla_{(p,d)}^{-1}((\boldsymbol{\alpha}, s)) \subset \mathcal{S}_n$ is a block permutation code with minimum distance at least d, where $(\boldsymbol{\alpha}, s) \in \mathbb{F}_p^{d-1} \times \mathbb{Z}_n$. Recalling the definition of d_B and d_C, we have the following relation between two distances:

$$d_B(\sigma, \tau) + 1 \ge d_C(\overline{\sigma}, \overline{\tau}) \ge d_B(\sigma, \tau) - 1, \tag{4.2}$$

for any $\sigma, \tau \in \mathcal{S}_n$. In the meantime, by definition, we can conclude $\nabla_{(p,d)}^{-1}((\boldsymbol{\alpha}, s)) = i_s\left(\widetilde{\Delta_{d+1}}^{-1}(\boldsymbol{\alpha})\right)$. Therefore, combining the inequality (4.2) and the fact that $\widetilde{\Delta_{d+1}}^{-1}(\boldsymbol{\alpha})$ has minimum distance at least $d + 1$, we deduce that any non-empty subset $\nabla_{(p,d)}^{-1}((\boldsymbol{\alpha}, s))$ is a block permutation code with minimum distance at least d, which completes the proof. □

Remark 1 By the Pigeonhole Principle and Theorem 5, there exists at least one element $(\boldsymbol{\alpha}_0, s_0) \in \mathbb{F}_p^{d-1} \times \mathbb{Z}_n$, such that the size of our block permutation code $\nabla_{(p,d)}^{-1}((\boldsymbol{\alpha}_\mathbf{0}, s_0)) \subset \mathcal{S}_n$ is at least

$$\frac{|\mathcal{S}_n|}{|\mathbb{F}_p^{d-1} \times \mathbb{Z}_n|} = \frac{(n-1)!}{p^{d-1}} = \Omega_d\left(\frac{n!}{n^d}\right),$$

where $\nabla_{(p,d)}^{-1}((\boldsymbol{\alpha}_0, s_0))$ has minimum distance at least d.

Remark 2 Recall in [22], Yang et al. first gave a non-explicit and non-systematic construction of a block permutation code of distance d and size $\frac{n!}{q^{2d-3}} = \Omega_d\left(\frac{n!}{n^{4d-6}}\right)$, where $n(n-1) \le q \le 2n(n-1)$ is a prime number. Xu et al. [21] improved this result by showing the existence of a block permutation code of distance d and size $\frac{n!}{q^{d-1}} = \Omega_d\left(\frac{n!}{n^{2d-2}}\right)$, where $n(n-1)/2 \le q \le n(n-1)$ is a prime. As shown in Remark 1, the size of our construction is $\Omega_d\left(\frac{n!}{n^d}\right)$, which improves the parameters of the above two non-systematic block permutation codes.

4.2 Systematic construction

Unfortunately, the use of the Pigeonhole Principle is inevitable in all known constructions of non-systematic block permutation codes including ours, which makes the codes non-explicit. However, Yang et al. [22] gave an explicit systematic construction based on their non-systematic codes. In fact, as demonstrated in [22], once we have a partition of block permutation codes, there is a way of constructing explicit systematic block permutation codes.

In this section, using the same idea, we propose an explicit systematic construction of block permutation codes with parameters better than the best-known ones. To demonstrate our construction, we need to give some necessary definitions and lemmas which can be found in [22]. By abuse of notation, in this section we denote a permutation $\sigma \in \mathcal{S}_n$ by the vector $(\sigma(1), \sigma(2), \ldots, \sigma(n))$ (note that this is not a cycle).

Definition 1 For any permutation $\sigma \in \mathcal{S}_n$ and an integer $1 \leq s \leq n$, we define the extended permutation $E(\sigma, s) \in \mathcal{S}_{(n+1)}$ by

$$E(\sigma, s) := (\sigma(1), \dots, \sigma(k), n+1, \sigma(k+1), \dots, \sigma(n)),$$

where $k = \sigma^{-1}(s)$. Furthermore, consider a sequence $S = (s_1, s_2, \dots, s_K)$, where $1 \leq s_m \leq n$ for all $1 \leq m \leq K$. Similarly, we define the extension $E(\sigma, S)$ to be the permutation in $\mathcal{S}_{(n+K)}$ derived from inserting the elements $n+1, \dots, n+K$ sequentially after the elements $s_1, \cdots, s_K$ in σ, i.e.,

$$E(\sigma, S) := E\left(E\left(\cdots E\left(E\left(\sigma, s_1\right), s_2\right) \cdots, s_{(K-1)}\right), s_K\right).$$

Remark 3 The elements $s_1, \cdots, s_K$ in the sequence S are not necessarily distinct. If different symbols are sequentially inserted after the same element, then they are all placed right after this element in descending order, as shown in the example below.

Example 1 Suppose $\sigma = (3, 2, 5, 4, 1, 8, 7, 6) \in \mathcal{S}_8$ and $S = (8, 2, 4, 4, 4)$, then

$$E(\sigma, S) = (3, 2, 10, 5, 4, 13, 12, 11, 1, 8, 9, 7, 6) \in \mathcal{S}_{13}.$$

Lemma 6 (See [22, Lemma 10]) *For any two permutations $\sigma, \tau \in \mathcal{S}_n$ and a sequence $S = (s_1, s_2, \cdots, s_K)$, where $1 \leq s_m \leq n$ for all $1 \leq m \leq K$, we have*

$$d_B(E(\sigma, S), E(\tau, S)) = d_B(\sigma, \tau).$$

Definition 2 For any two sequences S_1, S_2 of integers with length K, where $S_i := (s_{i,1}, \cdots, s_{i,K})$ for $i = 1, 2$, we define the *Hamming set* of S_1 with respect to S_2 by

$$H(S_1, S_2) := \{s_{1,m} \mid s_{1,m} \neq s_{2,m}, 1 \leq m \leq K\}.$$

Lemma 7 (See [22, Lemma 11]) *Let $\sigma, \tau \in \mathcal{S}_n$ and sequences $S_i = (s_{i,1}, s_{i,2}, \cdots, s_{i,K})$, where $1 \leq s_{i,m} \leq n$ for all $1 \leq m \leq K$ and $i = 1, 2$, then we have*

$$d_B(E(\sigma, S_1), E(\tau, S_2)) \geq |H(S_1, S_2)|.$$

Definition 3 A subset $A(n, K, d) \subset \mathbb{Z}_n^K$ is called a *d-auxiliary set* of length K and range n if for any two different elements $S_1, S_2 \in A(n, K, d)$, $|H(S_1, S_2)| \geq d$ holds.

Remark 4 In [22], their definition $\mathcal{A}(n, K, t)$ refers to the set $A(n, K, 2t+1)$ in our definition above.

Combining the above definitions and lemmas, we then demonstrate how a partition of block permutation codes transforms into systematic block permutation codes below.

Lemma 8 *For any $n, d \geq 4$ and a prime $p \in [n, 2n)$, we consider the map $\nabla_{(p,d)} : \mathcal{S}_n \to \mathbb{F}_p^{d-1} \times \mathbb{Z}_n$ shown in Theorem 5. Let $A(n, K, d)$ be a d-auxiliary set of length K and range n such that $|A(n, K, d)| \geq np^{d-1}$ and we define an arbitrary injection map $\psi : \mathbb{F}_p^{d-1} \times \mathbb{Z}_n \hookrightarrow A(n, K, d)$. Set $N = n + K$, then the set*

$$\mathcal{B}^{sys}(N, d) := \{E\left(\sigma, \psi \circ \nabla_{(p,d)}(\sigma)\right) \mid \sigma \in \mathcal{S}_n\} \subset \mathcal{S}_N$$

is a systematic block permutation code of distance d and size $(N - K)!$.

Proof By the choice of $E(\sigma, S)$, it is clear that $\mathcal{B}^{\text{sys}}(N, d)$ is systematic. For any two different permutations $\sigma, \tau \in \mathcal{S}_n$, set $\boldsymbol{\alpha}_1 := \nabla_{(p,d)}(\sigma)$ and $\boldsymbol{\alpha}_2 := \nabla_{(p,d)}(\tau)$. Consider the following two cases:

(1) $\boldsymbol{\alpha}_1 = \boldsymbol{\alpha}_2$, Then by Theorem 5 and Lemma 6,

$$d_B(E(\sigma, \psi(\boldsymbol{\alpha}_1)), E(\tau, \psi(\boldsymbol{\alpha}_2)) = d_B(\sigma, \tau) \geq d.$$

(2) $\boldsymbol{\alpha}_1 \neq \boldsymbol{\alpha}_2$, i.e., $\psi(\boldsymbol{\alpha}_1) \neq \psi(\boldsymbol{\alpha}_2)$, Then by Lemma 7 and Definition 3,

$$d_B(E(\sigma, \psi(\boldsymbol{\alpha}_1)), E(\tau, \psi(\boldsymbol{\alpha}_2)) \geq |H(\psi(\boldsymbol{\alpha}_1), \psi(\boldsymbol{\alpha}_2))| \geq d.$$

In conclusion, $\mathcal{B}^{\mathrm{sys}}(N, d)$ is indeed a systematic block permutation code of distance d and $|\mathcal{B}^{\mathrm{sys}}(N, d)| = n! = (N - K)!$. □

Finally, to explicitly construct systematic block permutation codes, by Lemma 8, we only need to give an explicit construction of d-auxiliary sets $A(n, K, d)$. Recall in [22], setting d as $2t+1$, they gave an explicit construction of d-auxiliary sets $A(n, 28d-28, d) = \mathcal{A}(n, 56t, t)$ with cardinality q^{2d-3}, when q is a prime number satisfying $n(n-1) \leq q \leq 2n(n-1)$.

We now provide an explicit construction of $A(n, K, d)$ using Reed–Solomon codes, whose parameters are better than those codes used in [22].

Theorem 6 *Set $n \geq 12, d \geq 4$ with $n \geq 6d$ and two primes $p \in [n, 2n)$, $q \in [\lfloor \frac{n}{2} \rfloor, n]$. We view elements in $\mathbb{F}_q^{3d-1}$ naturally as elements in $\mathbb{Z}_n^{3d-1}$ and $\mathsf{RS}_q[a, b, c] \subset \mathbb{F}_q^a$ as a q-ary Reed–Solomon code of length a, dimension b and minimum Hamming distance c. Then, the set*

$$A(n, 3d-1, d) := \mathsf{RS}_q[3d-1, 2d, d] \subset \mathbb{Z}_n^{3d-1}$$

is an explicit d-auxiliary set of length $3d-1$, range n and size at least np^{d-1}.

Proof By definition, we have $d_H(\boldsymbol{c}_1, \boldsymbol{c}_2) = |H(\boldsymbol{c}_1, \boldsymbol{c}_2)|$, where d_H is the Hamming distance of linear codes and $\boldsymbol{c}_i = (c_{i,1}, \cdots, c_{i,(3d-1)})$ $(i = 1, 2)$, where $1 \leq c_{i,m} \leq q$ for all $1 \leq m \leq 3d-1$. Since $q \geq \frac{n}{2} - 1 \geq 3d - 1$ and Reed–Solomon codes are MDS codes, we can guarantee the explicit existence of $\mathsf{RS}_q[3d-1, 2d, d]$. Combining the above two facts, we may conclude $A(n, 3d-1, d)$ as a d-auxiliary set of length $3d-1$ and range n. Finally, since $n \geq 12$ and $4q + 4 \geq p$, we have

$$|A(n, 3d-1, d)| = |\mathsf{RS}_q[3d-1, 2d, d]| = q^{2d} \geq (4q+4)^d \geq p^d \geq np^{d-1}.$$

□

Corollary 2 *There exists a class of explicit systematic block permutation codes of length N, distance d and size $(N - 3d + 1)!$, whenever $N \geq 37, d \geq 4$ and $N \geq 9d + 1$.*

Proof Put $K = 3d - 1$. Combining Lemma 8 and Theorem 6, one immediately obtains this result. □

Remark 5 Recall in [22], setting d as $2t + 1$, Yang et al. gave an explicit construction of $\mathcal{C}_B^{sys}(N - 56t, 56t, t)$ for some suitable N, d as one of their main results, which yields systematic block permutation codes of length N, distance d and size $(N - 28d + 28)!$. Apparently our result in Corollary 2 improves the one given in [22]. Moreover, via a metric embedding method, our result implies an explicit construction of codes in the generalized Cayley metric better than the results given in [3, 22].

5 The Gilbert–Varshamov bound

The Gilbert–Varshamov bound is one of the most important bounds in coding theory and in the geometry of numbers. It usually serves as the benchmark for a good code. Namely, a good code should achieve or almost achieve the Gilbert–Varshamov bound.

Generally speaking, as long as there is a distance, one can deduce the Gilbert–Varshamov bound with respect to this distance. To have a precise statement on the Gilbert–Varshamov bound for a distance, let us assume that S is a finite set. Assume that we have a distance d on S. Define the ball of center u and radius r by

$$B_S(u,r) := \{v \in S : \ d(u,v) \le r\}.$$

Assume that the size $V(r)$ of $B_S(u,r)$ is independent of the center u and only dependent on the radius r, then the Gilbert–Varshamov bound says that there is a subset $C \subseteq S$ of size at least M such that $d(a,b) \ge d$ for all $a \ne b \in C$, where

$$M = \left\lceil \frac{|S|}{V(d-1)} \right\rceil. \tag{5.1}$$

Now we return to our cyclic block permutation distance d_C on $\mathcal{S}_n/\langle\omega\rangle$. We define the sphere

$$\mathrm{SP}_c(\overline{\sigma}, r) := \{\overline{\tau} \in \mathcal{S}_n/\langle\omega\rangle : \ d_C(\overline{\sigma}, \overline{\tau}) = r\}.$$

Lemma 9 *For $\sigma \in \mathcal{S}_n$, the map $\Psi \colon \mathrm{SP}_c(\overline{\sigma}, r) \to \mathrm{SP}_c(\overline{\epsilon}, r)$ given by $\overline{\tau} \mapsto \overline{\sigma}^{-1}\overline{\tau}$ is a bijection.*

Proof $\overline{\tau} \in \mathrm{SP}_c(\overline{\sigma}, r)$ if and only if $n - |A_c(\sigma) \cap A_c(\tau)| = r$, i.e., $|A_c(\sigma) \cap A_c(\tau)| = n - r$. By Lemma 1, we have

$$\begin{aligned}
|A_c(\sigma) \cap A_c(\tau)| &= |\{i \in \mathbb{Z}_n : \ \sigma(\sigma^{-1}(i)+1) = \tau(\tau^{-1}(i)+1)\}| \\
&= |\{i \in \mathbb{Z}_n : \ \sigma^{-1}(i)+1 = \sigma^{-1}\tau(\tau^{-1}(\sigma(\sigma^{-1}(i))+1))\}| \\
&= |\{i \in \mathbb{Z}_n : \ \sigma^{-1}(i)+1 = \sigma^{-1}\tau((\sigma^{-1}\tau)^{-1}(\sigma^{-1}(i))+1)\}| \\
&= |\{j \in \mathbb{Z}_n : \ j+1 = \sigma^{-1}\tau((\sigma^{-1}\tau)^{-1}(j)+1)\}| \quad (\text{replace } \sigma^{-1}(i) \text{ by } j) \\
&= |A_c(\sigma^{-1}\tau) \cap A_c(\epsilon)| = n - r.
\end{aligned}$$

This implies that $\sigma^{-1}\tau$ belongs to $\mathrm{SP}_c(\overline{\epsilon}, r)$. Hence, the map Ψ is well defined. It is clear that Ψ is injective. For any $\delta \in \mathrm{SP}_c(\overline{\epsilon}, r)$, we have $|A_c(\epsilon) \cap A_c(\delta)| = n - r$. In the same manner, we can show that $|A_c(\sigma) \cap A_c(\sigma\delta)| = n - r$, i.e., $\sigma\delta \in \mathrm{SP}_c(\overline{\sigma}, r)$. This implies that Ψ is surjective. □

By Lemma 9, we know that the size of a sphere is independent of the center. Thus, the size of the ball $B_c(\overline{\sigma}, r) = \bigcup_{i=0}^{r} \mathrm{SP}_c(\overline{\sigma}, i)$ is also independent of the center $\overline{\sigma}$. By the above Gilbert–Varshamov bound, one immediately obtains the following result.

Corollary 3 *One has*

$$M_C(n,d) \ge M_{GV}(n,d) := \frac{(n-1)!}{|B_c(\overline{\sigma}, d-1)|}. \tag{5.2}$$

The inequality (5.2) is called the Gilbert–Varshamov lower bound for cyclic block permutation codes. In the rest of this section, we show that our algebraic-geometric-based construction given in Sect. 3 breaks the Gilbert–Varshamov bound for constant distance d. One way to achieve this goal is to determine the exact size of the ball $B_c(\overline{\sigma}, d-1)$. We note that the exact size of a ball under block permutation distance was well-studied in [14]. Nevertheless, calculating the exact volume of $B_c(\overline{\sigma}, d-1)$ is interesting for further study. For our purpose, it is sufficient to give a good lower bound on the size of the ball $B_c(\overline{\sigma}, d-1)$.

Lemma 10 *For $d \geq 3$, one has*

$$|\mathrm{SP}_c(\overline{\epsilon}, d)| \geq \binom{n}{d}.$$

Proof To prove this lemma, it is sufficient to show that (i) for any d positive numbers $1 \leq j_1 < j_2 < \cdots < j_d \leq n$ with $J := \{j_1, j_2, \ldots, j_d\} \subset \{1, 2, 3, \ldots, n\}$, one can find at least one permutation σ such that $A_c(\epsilon) \backslash A_c(\sigma) = D_J := \{(j_s, j_s+1) : \ 1 \leq s \leq d\}$; (ii) these permutations belong to the pairwise distinct left cosets of $\langle \omega \rangle$.

Let us call an element in $\{1, 2, \ldots, n\}$ a point. Given D_J, we characterize points into the following four types

- Type I: Point i is called Type I if $(i-1, i), (i, i+1) \notin A_c(\epsilon) \setminus D_J$;
- Type II: Point i is called Type II if $(i-1, i), (i, i+1) \in A_c(\epsilon) \setminus D_J$;
- Type III: Point i is called Type III if $(i-1, i) \in A_c(\epsilon) \backslash D_J$ and $(i, i+1) \notin A_c(\epsilon) \backslash D_J$;
- Type IV: Point i is called Type IV if $(i, i+1) \in A_c(\epsilon) \backslash D_J$ and $(i-1, i) \notin A_c(\epsilon) \backslash D_J$.

It is not hard to see that points j_s $(1 \leq s \leq n)$ is either Type I or Type III.

For a point j_s of Type III, we observe that one always has a unique point i_s of Type IV such that

$$H_{(i_s, j_s)} := \{(i_s, i_s+1), (i_s+1, i_s+2), \cdots, (j_s-1, j_s)\} \subset A_c(\epsilon) \setminus D_J.$$

Define an ordered set

$$F_{j_s} = \begin{cases} \{j_s\}, & j_s \text{ is Type I ;} \\ \{i_s, i_s+1, \cdots, j_s-1, j_s\}, & j_s \text{ is type III.} \end{cases}$$

It is clear that the sets $\{F_{j_s}\}_{s=1}^{d}$ form a partition of $\{1, 2, \ldots, n\}$. We further define a set of pairs

$$G_{j_s, j_t} := \begin{cases} \{(j_s, j_t)\}, & j_s, j_t \text{ are both Type I;} \\ \{(j_s, i_t)\} \cup H_{(i_t, j_t)}, & j_s \text{ is Type I , } j_t \text{ is Type III;} \\ H_{(i_s, j_s)} \cup \{(j_s, j_t)\}, & j_s \text{ is Type III, } j_t \text{ is Type I;} \\ H_{(i_s, j_s)} \cup \{(j_s, i_t)\} \cup H_{(i_t, j_t)}, & j_s, j_t \text{ are both Type III.} \end{cases}$$

Define σ to be the permutation $\left(F_{j_1}, F_{j_d}, F_{j_{(d-1)}}, \cdots, F_{j_2}\right) \in \mathcal{S}_n$, i.e, 1 is mapped to the first element of F_{j_1} (note that F_{j_1} is an ordered set), 2 is mapped to the second element of F_{j_1}, and so on. Then we have

$$A_c(\sigma) = G_{j_1, j_d} \cup G_{j_d, j_{(d-1)}} \cup G_{j_{(d-1)}, j_{(d-2)}} \cup G_{j_{(d-2)}, j_{(d-3)}} \cup \cdots \cup G_{j_2, j_1}. \qquad (5.3)$$

Since $A_c(\sigma)$ does not contain $G_{j_s, j_{(s+1)}}$ for all $1 \leq s \leq d$, we have $A_c(\epsilon) \backslash A_c(\sigma) = D_J$.

Finally, let J' be a subset of d elements that is different from J. Assume that σ' is obtained in the same way from J'. As $A_c(\sigma) \backslash A_c(\epsilon) = D_J \neq D_{J'} = A_c(\sigma') \backslash A_c(\epsilon)$, we must have $A_c(\sigma) \neq A_c(\sigma')$, i.e., $\overline{\sigma'} \neq \overline{\sigma}$. This completes the proof. □

Using the lower bound given in Lemma 10, we can show that our cyclic block permutation codes given in Sect. 3 break the Gilbert–Varshamov bound for constant number d.

Corollary 4 *For a constant number $d \geq 4$, we have*

$$\frac{M_C(n,d)}{M_{GV}(n,d)} = \Omega_d(n).$$

Proof By Corollary 1 and Lemma 10, we have

$$\frac{M_C(n,d)}{M_{GV}(n,d)} = \frac{V(d-1)}{p^{d-2}} = \frac{|\bigcup_{i=0}^{d-1} \mathrm{SP}_c(\overline{\epsilon}, i)|}{p^{d-2}} \geq \frac{|\mathrm{SP}_c(\overline{\epsilon}, d-1)|}{p^{d-2}} \geq \frac{\binom{n}{d-1}}{(2n)^{d-2}} = \Omega_d(n),$$

where p is the minimum prime number larger than n. Note that we applied the famous Bertrand–Chebyshev theorem[2] here, since p above is the least prime no less than n and there must exist at least one prime number between n and $2n$. □

6 Future directions

In this section, we give some possible future directions of improving the constructions of permutation codes under several related metrics. For the block permutation metric d_B, we have already known that our new metric d_C (cyclic block permutation metic) satisfies that $d_B(\sigma, \tau)+1 \geq d_C(\overline{\sigma}, \overline{\tau}) \geq d_B(\sigma, \tau)-1$. However, we have not studied the exact relationship between these two metrics. A further study for this relationship is meaningful since it may directly help us to gain an even better constructions of block permutation codes using our modified algebraic-geometric method. Also, we still curious about whether our methods in this paper can be transferred into constructing better permutation codes under other related metrics (e.g. Generalized Kendall's τ-metric). Last but not least, in Sect. 5, a rough estimation of a related combinatorial problem is given in Lemma 10. However, can we solve this combinatorial problem with an exact formula?

Acknowledgements The author thanks professor Chaoping Xing, for patiently and carefully instructing him to rewrite this paper in a more reasonable way. Since this work was done by the author when he was an undergraduate student in Sichuan University, the author also thanks professor Qifan Zhang, for his guidance during the last several years. Meanwhile, the author thanks Zixiang Xu for generously introducing this topic to him as well as discussing and giving useful suggestions about Sect. 5, Siyi Yang for some useful advice in explicitly constructing systematic block permutation codes. Last but not least, the author thanks professor Zeyu Guo for kindly helping him revise this paper and two anonymous reviewers for giving their useful advice.

References

1. Buzaglo S., Etzion T.: Bounds on the size of permutation codes with the Kendall τ-metric. IEEE Trans. Inf. Theory **61**(6), 3241–3250 (2015).
2. Buzaglo S., Yaakobi E., Etzion T., Bruck J.: Systematic error-correcting codes for permutations and multi-permutations. IEEE Trans. Inf. Theory **62**(6), 3113–3124 (2016).
3. Chee, Y.M., Van Khu, V.: Breakpoint analysis and permutation codes in generalized Kendall tau and Cayley metrics. In: 2014 IEEE International Symposium on Information Theory, Honolulu, June 29–July 4, 2014, pp. 2959–2963 (2014)
4. Chu W., Colbourn C., Dukes P.: Constructions for permutation codes in powerline communications. Des. Codes Cryptogr. **32**(1), 51–64 (2004).
5. Colbourn C., Klove T., Ling A.: Permutation arrays for powerline communication and mutually orthogonal Latin squares. IEEE Trans. Inf. Theory **50**(6), 1289–1291 (2004).
6. Deza M., Vanstone S.A.: Bounds for permutation arrays. J. Stat. Plan. Inference **2**(2), 197–209 (1978).

[2] Bertrand–Chebyshev theorem states that for any positive integer n, there exist at least one prime number p such that $n \leq p \leq 2n$.

7. Ding C., Fu F., Klove T., Wei V.: Constructions of permutation arrays. IEEE Trans. Inf. Theory **48**(4), 977–980 (2002).
8. Farnoud F., Skachek V., Milenkovic O.: Error-correction in flash memories via codes in the Ulam metric. IEEE Trans. Inf. Theory **59**(5), 3003–3020 (2013).
9. Frankl P., Deza M.: On the maximum number of permutations with given maximal or minimal distance. J. Comb. Theory Ser. A **22**(3), 352–360 (1977).
10. Fu F., Klove T.: Two constructions of permutation arrays. IEEE Trans. Inf. Theory **50**(5), 881–883 (2004).
11. Gölogluu, F., Lember, J., Riet, A., Skachek, V.: New bounds for permutation codes in Ulam metric. In: IEEE International Symposium on Information Theory, ISIT 2015, Hong Kong, June 14–19, 2015, pp. 1726–1730 (2015)
12. Hassanzadeh F.F., Milenkovic O.: Multipermutation codes in the Ulam metric for nonvolatile memories. IEEE J. Sel. Areas Commun. **32**(5), 919–932 (2014).
13. Jin L.: A construction of permutation codes from rational function fields and improvement to the Gilbert–Varshamov bound. IEEE Trans. Inf. Theory **62**(1), 159–162 (2016).
14. Myers A.: Counting permutations by their rigid patterns. J. Comb. Theory Ser. A **99**(2), 345–357 (2002).
15. Niederreiter H., Xing C.: Rational Points on Curves Over Finite Fields, LMS 285. Cambridge University Press, Cambridge (2001).
16. Smith D.H., Montemanni R.: A new table of permutation codes. Des. Codes Cryptogr. **63**(2), 241–253 (2012).
17. Stichtenoth H.: Algebraic Function Fields and Codes. GTM 254. Springer, New York (2009).
18. Tait, M., Vardy, A., Verstraëte, J.: Asymptotic improvement of the Gilbert–Varshamov bound on the size of permutation codes. CoRR. http://arxiv.org/abs/1311.4925 (2013)
19. Xing C.: Constructions of codes from residue rings of polynomials. IEEE Trans. Inf. Theory **48**(11), 2995–2997 (2002).
20. Xing C.: Linear codes from narrow ray class groups of algebraic curves. IEEE Trans. Inf. Theory **50**(3), 541–543 (2004).
21. Xu Z., Zhang Y., Ge G.: New theoretical bounds and constructions of permutation codes under block permutation metric. Des. Codes Cryptogr. **87**(11), 2625–2637 (2019).
22. Yang S., Schoeny C., Dolecek L.: Theoretical bounds and constructions of codes in the generalized Cayley metric. IEEE Trans. Inf. Theory **65**(8), 4746–4763 (2019).

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