Covering codes and extremal problems from invariant sets under permutations

Emerson L. Monte Carmelo
Departamento de Matemática, Universidade Estadual de Maringá, Brazil

Abstract

Let \( c_q(n, R) \) denote the minimum cardinality of a subset \( H \) in \( \mathbb{F}_q^n \) such that every word in this space differs in at most \( R \) coordinates from a scalar multiple of a vector in \( H \), where \( q \) is a prime power. In order to explore symmetries of such coverings, a few properties of invariant sets under certain permutations are investigated. New classes of upper bounds on \( c_q(n, R) \) are obtained, extending previous results. Let \( K_q(n, R) \) denote the minimum cardinality of an \( R \)-covering code in the \( n \)-dimensional space over an alphabet with \( q \) symbols. As another application, a very-known upper bound on \( K_q(n, R) \) is improved under certain conditions. Moreover, two extremal problems are discussed by using tools from graph theory.

© 2012 Elsevier B.V. All rights reserved.

1. Introduction

1.1. Covering codes

For our purpose, covering codes are described when the alphabet is a finite field \( \mathbb{F}_q \). Given two vectors \( x = (x_1, \ldots, x_n) \) and \( y = (y_1, \ldots, y_n) \) in \( \mathbb{F}_q^n \), the Hamming distance \( d(x, y) \) between \( x \) and \( y \) is the number of coordinates in which \( x \) and \( y \) differ, that is,

\[
d(x, y) = |\{i : x_i \neq y_i\}|.
\]

In this metric space, the ball centered at \( x \) and radius \( R \) corresponds to the set

\[
B(x, R) = \{ y \in \mathbb{F}_q^n : d(x, y) \leq R \},
\]

where \( 0 \leq R \leq n \). A set \( C \) is an \( R \)-covering of \( \mathbb{F}_q^n \) when

\[
\bigcup_{c \in C} B(c, R) = \mathbb{F}_q^n.
\]

The number \( K_q(n, R) \) denotes the minimum cardinality of an \( R \)-covering of \( \mathbb{F}_q^n \). The determination of these numbers seems to be a great challenge of combinatorial coding theory. Indeed, covering codes have been extensively investigated since the...
1.2. Short covering codes

Some similar problems with algebraic constraints have been investigated; for instance, see the contributions [6,26]. In particular, a new concept of covering has arisen when the center $h$ is extended to the line that contains all the scalar multiples of $h$, according to [18]. For a vector $h$ in $\mathbb{F}_q^n$, let

$$E(h, R) = \bigcup_{\alpha \in \mathbb{F}_q} B(\alpha \cdot h, R),$$

where $\alpha \cdot h$ denotes the multiplication of $h$ by the scalar $\alpha$. A subset $H$ in $\mathbb{F}_q^n$ is an $R$-short covering of $\mathbb{F}_q^n$ when

$$\bigcup_{h \in H} E(h, R) = \mathbb{F}_q^n.$$  \hfill (2)

The number $c_q(n, R)$ is defined as the minimum cardinality of an $R$-short covering of $\mathbb{F}_q^n$.

Note that $H$ is an $R$-short covering if and only if

$$\mathbb{F}_q \cdot H = \{\alpha \cdot h : \alpha \in \mathbb{F}_q \text{ and } h \in H\}$$

is an $R$-covering of $\mathbb{F}_q^n$. It is worth emphasizing a difference. While a minimum covering does not have necessarily any algebraic property, a short covering $H$ always generates a classical covering $\mathbb{F}_q \cdot H$, which is invariant under scalar multiplication.

Some of the motivations for studying short covering codes are mentioned now. Short coverings provide us a way to store coverings using less memory than the classical ones. The distinct behavior of short covering seems to be interesting on theoretical viewpoints: results have been obtained in connection with group theory, finite ring theory, combinatorial number theory (sum-free sets and product-free sets), graph theory (dominating set, weighted graphs), and local search (tabu search), according to [15–20]. Moreover, results on short covering codes might enable us to bring record-breaking on the classical codes. Indeed, the work [16] explores a new upper bound on $K_q(n, R)$ from short covering code, which yields $K_5(10, 7) = 9$ from the value $c_5(10, 7) = 2$.

1.3. Statements of some results

The first part of this work concerns with covering codes. Some constructions of short covering codes are established. As a goal of this work, a new exact class of short coverings is established below, extending the previous number $c_5(10, 7) = 2$.

**Theorem 1.** For any positive integer $r$ and any prime power $q$ such that $q \geq r + 3$, we have

$$c_q(qr, qr - r - 1) = 2.$$ 

On the other hand, a closer look reveals that most upper bounds on $K_q(n, R)$ have been focused on particular instances and have been obtained by computer search in the past 20 years, according to the updated tables by Kerlé [12]. Sometimes structural property is imposed on the code (codes with certain automorphism) in order to reduce the search space (see [7,23], for instance). Even in this case, constructions are based on computer local search methods like tabu search, simulated annealing, or other computational approach. The most studied cases correspond to the small parameters, namely $q \leq 5$, $n \leq 33$, and $R \leq 10$.

In spite of the fact that the case $q \geq 6$ is also interesting (see [14]), the literature for large $q$ is significantly poorer. One of these few results states that $K_q(qr, qr - r - 1) \leq 2q$ for any $q$ such that $q \geq r + 3$, obtained by Östergård [22, Theorem 6]. As the second goal, our approach can be applied to the classical coverings too, improving this very-known upper bound under certain condition.

**Corollary 2.** For any positive integer $r$ and any prime power $q$ such that $q \geq r + 3$, the following bound holds

$$K_q(qr, qr - r - 1) \leq 2q - 1.$$ 

In order to obtain both results above, a new method based on invariant set under suitable permutation is discussed. For this purpose, we need to introduce the concept of $\gamma$-path, which plays a central role in this research.

The second part of this work has a combinatorial approach. Indeed, two extremal problems arise naturally from the concept of $\gamma$-path. As another goal of this work, these problems are solved by using tools from graph theory.

The remaining text is organized as follows. Some results on invariant sets under a permutation are investigated in Section 2. In Section 3, invariant sets are used to construct three classes of short covering codes, and the concept of
equivalence among short codes is discussed in Section 4. The previous results are applied to improve a known upper bound on classical covering codes in Section 5. Finally, we discuss two combinatorial problems in Section 6.

2. The main tool: invariant sets

As usual, the family $S_Ω$ of all permutations of a finite set $Ω$ is called the symmetric group on $Ω$. Given a nonempty subset $Δ$ of $Ω$ and a permutation $γ ∈ S_Ω$, write $γ(Δ) = \{γ(a) : a ∈ Δ\}$. We say that $Δ$ is setwise invariant (or simply invariant) under $γ$ if $γ(Δ) = Δ$. In the special case where $Δ = \{a\}$, we also say that $γ$ fixes $a$, that is, $γ(a) = a$.

Given $r$, with $2 ≤ r ≤ |Ω|$, a permutation $γ$ in $S_Ω$ is called an $r$-cycle if there are $r$ distinct points $a_1, . . . , a_r$ in $Ω$ such that: $γ(a_i) = a_{i+1}$ for $1 ≤ i ≤ r − 1$, $γ(a_r) = a_1$, and $γ$ leaves all others points fixed. By convention, any 1-cycle $(a)$ denotes the identity in $S_Ω$. A well-known result is stated below, whose proof can be found in [10].

Lemma 3. Every permutation is a product of disjoint cycles. This decomposition is unique up to the order of the cycles.

2.1. Paths

New concepts are introduced.

Definition 1. Let $γ$ be a permutation on the set $Ω$. A $γ$-path is simply a finite sequence $(a_1, . . . , a_m)$ of elements in $Ω$ which are generated by the recursive relation $a_{i+1} = γ(a_i)$, where $1 ≤ i ≤ m − 1$.

Definition 2. Let $Δ$ be a subset of $Ω$, the $γ$-path $(a_1, . . . , a_m)$ crosses $Δ$ (or is a $γ$-path crossing $Δ$, or passes although $Δ$) if it satisfies the properties:

- the set $\{a_2, . . . , a_{m-1}\}$ is contained in $Δ$;
- both extremal points $a_1$ and $a_m$ do not belong to $Δ$.

Definition 3. Given a permutation $γ$ in $S_Ω$ and a subset $Δ$ of $Ω$, let $c(γ, Δ)$ denote the number of $γ$-paths that cross $Δ$.

Example 4. Consider the permutation

$$γ = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 4 & 2 & 5 & 1 & 0 & 3 & 6 \end{pmatrix}$$

on $Ω = \{0, 1, 2, 3, 4, 5, 6\}$. There are two $γ$-paths crossing the set $\{1, 3, 6\}$, namely, $(4, 1, 4)$ and $(0, 6, 3, 5)$, thus $c(γ, \{1, 3, 6\}) = 2$. Note that $c(γ, \{0, 1, 3\}) = 3$, because the $γ$-paths $(4, 1, 4), (6, 3, 5),$ and $(5, 0, 6)$ cross the set $\{0, 1, 3\}$.

Proposition 5. Let $Δ$ be a nonempty subset of $Ω$ and let $γ$ be a permutation in $S_Ω$. The following numbers are equal.

1. $c(γ, Δ)$.
2. $|D_Δ|$, where $D_Δ = \{a ∈ Δ : γ(a) ∈ Δ\}$.

Proof. We first prove that each element $a$ in $D_Δ$ generates exactly one $γ$-path crossing $Δ$. Let $a_1 = a$ and consider the sequence given by $a_{i+1} = γ(a_i)$ for any $i$. By construction, $a_1 ∉ Δ$ but $a_2 ∈ Δ$. We claim that there is an index $i$ such that $a_i ∉ Δ$ and $i ≥ 3$. By absurd, suppose $a_i ∈ Δ$ for any $i ≥ 2$. Because $Ω$ is a finite set, there would be two distinct indices, say $h > k$, such that $a_h = a_k$. By applying $γ^{−1}$ recursively, we obtain

$$a_1 = (γ^{−1} k^{−1}(a_k)) = (γ^{−1} k^{−1}(a_h)) = a_{h−k+1},$$

thus $a_1 ∈ Δ$, which produces a contradiction. Define $m$ as the minimum index $i$ such that $a_i ∉ Δ$. Hence $(a_1, . . . , a_m)$ is a $γ$-path crossing $Δ$. Conversely, each $γ$-path $(a_1, . . . , a_m)$ crossing $Δ$ is associated to $a_1 ∈ D_Δ$. Since this correspondence is bijective, the statement follows.

As an immediate consequence, the existence of $γ$-path crossing $Δ$ is characterized as follows.

Corollary 6. The following statements are equivalent.

1. There is a $γ$-path crossing $Δ$.
2. $c(γ, Δ) > 0$.
3. $Δ$ is not an invariant set under $γ$.
2.2. Invariant sets under a linear operator

We consider here the particular case $\Omega = \mathbb{F}_q$ for our purpose. Let $\omega$ be an arbitrary element with order $r$ in the cyclic group $\mathbb{F}_q^*$, where $1 \leq r \leq q - 1$. The symbol $\sigma = \sigma_\omega$ denotes the nonsingular linear operator of $\mathbb{F}_q$ given by $\sigma(x) = \omega x$ for any $x \in \mathbb{F}_q$.

**Lemma 7.** Let $\sigma = \sigma_\omega$ be the linear operator described above. The following statements hold.

1. The set $\Delta$ is invariant under $\sigma_\omega$ if and only if $\Delta$ is a union of pairwise disjoint subsets $\Delta_i$, where each $\Delta_i$ is a coset of $[\omega]$ or $\Delta_i = \{0\}$.
2. Consider the linear operator $\sigma_\xi : x \mapsto \xi x$, where $\xi$ denotes a generator of the cyclic group $\mathbb{F}_q^*$. The only invariant sets under $\sigma_\xi$ are: $\{0\}, \mathbb{F}_q^*$, and $\mathbb{F}_q$.

**Proof.** Let us prove the first part. Beside the sets $\{0\}, \mathbb{F}_q^*$, and $\mathbb{F}_q$, note that the coset $b[\omega]$ is an invariant set under $\sigma$ for any $b$ other than $0$, and therefore any union of cosets is also an invariant set under $\sigma$. The converse is proved as follows. Suppose there is a setwise invariant set $\Delta$ other than $\{0\}, \mathbb{F}_q^*$, and $\mathbb{F}_q$. Pick an arbitrary element $b_1$ in $\Delta$. Since $\Delta$ is invariant, the element $\sigma^n(b_1) = b_1\omega^n$ also belongs to $\Delta$ for each $n$, thus

$$b_1[\omega] = \{ b_1, b_1\omega, \ldots, b_1\omega^{r-1} \}$$

is a subset of $\Delta$. If $b_1[\omega] = \Delta$, the statement follows. Otherwise, pick an element $b_2$ in $\Delta - b_1[\omega]$. By assumption, the coset $b_2[\omega] \subset \Delta$. Since $b_2 \notin b_1[\omega]$, the cosets $b_1[\omega]$ and $b_2[\omega]$ are disjoint. Repeat the procedure described above until we find a partition of $\Delta$ into cosets such that

$$\Delta = \bigcup_{i=1}^k b_i[\omega].$$

The second part follows from the first part and the fact that any coset is always $\mathbb{F}_q^*$.

3. From invariant sets to short covering codes

Given a vector $x$ in $\mathbb{F}_q^n$ and an element $a$ in $\mathbb{F}_q$, $s_a(x)$ denotes the number of coordinates of $x$ equal to $a$. The equality below is trivial but useful:

$$\sum_{a \in \mathbb{F}_q} s_a(x) = n. \quad (3)$$

Suitable constructions of short covering codes enable us to state new upper bounds, as described in next results. Their proofs are based on the characterizations of invariant sets under permutation given in Section 2.

3.1. First construction

**Proposition 8.** For any positive integer $r$ and any prime power $q$, with $q \geq r + 4$, the bound below holds

$$c_q(qr - 1, qr - r - 2) \leq 3.$$

**Proof.** Let $n = qr - 1$ and $R = qr - r - 2$. Let $\xi$ denote a generator of $\mathbb{F}_q^*$. Define the vectors

$$h_1 = (1, 1, \ldots, 1; 1, 1, \ldots, 1),$$
$$h_2 = (1, 1, \ldots, 1; \xi, \xi, \ldots, \xi),$$
$$h_3 = (\xi, \xi, \ldots, \xi; 1, 1, \ldots, 1),$$

where the changes of the symbols in $h_2$ and $h_3$ happen in the the last $r + 1$ coordinates.

We need to prove that $H = \{h_1, h_2, h_3\}$ is an $R$-short covering of $\mathbb{F}_q^n$. Indeed, take an arbitrary vector $x$ in $\mathbb{F}_q^n$.

Case 1: Suppose there is a symbol $a$ such that $s_a(x) \geq r + 1$. Hence $x$ and $a \cdot h_1$ disagree at most in $R$ coordinates, that is, $x \in E(h_1, R)$.

Case 2: Otherwise, $s_a(x) \leq r$ for any $a$ in $\mathbb{F}_q$. The equality in (3) implies the next statement.

**Claim 1.** There are $q - 1$ symbols such that $s_a(x) = r$ and there is one symbol with $s_a(x) = r - 1$.

The vector $x$ can be written as $x = (u; v)$, where $u \in \mathbb{F}_q^r$ and $v \in \mathbb{F}_q^{r+1}$. Let $\Delta$ be the set formed by the symbols in the vector $u$. By Claim 1, we have $2 \leq |\Delta| \leq r + 1$. By Lemma 7, the set $\Delta$ is not invariant under the linear operator $\sigma_\xi$. Take a path $(a_1, \ldots, a_m)$ crossing $\Delta$ (the existence of such path is a consequence of Corollary 6). We claim that $a_1 \neq a_m$; otherwise, the set $(a_1, \ldots, a_{m-1})$ would be an invariant set with at most $q - 2$ elements, which contradicts the second part of Lemma 7. Since $a_1 \neq a_m$ holds, Claim 1 implies $s_{a_1}(x) = r$ or $s_{a_m}(x) = r$. 
• If \( s_{a_1}(x) = r \), then \( d(x, a_1, h_2) \leq R \), and therefore \( x \in E(h_2, R) \).
• If \( s_{a_m}(x) = r \), then \( d(x, a_{m-1}, h_2) \leq R \), that is, \( x \in E(h_3, R) \).

The proof is complete \( \square \)

3.2. Second construction

**Theorem 9.** For any positive integer \( r \) and for any prime power \( q \), with \( q \geq 3 \), we have

\[ c_q(qr, qr - r - 1) \leq 3. \]

**Proof.** Let \( R = qr - r - 1 \). Since \( q > 2 \), pick any element \( \omega \) in \( \mathbb{F}_q \setminus \{0, 1\} \), and choose the following vectors in \( \mathbb{F}_q^{qr} \):

\[
\begin{align*}
  h_1 &= (1, 1, \ldots, 1, 1), \\
  h_2 &= (1, 1, \ldots, 1, \omega), \\
  h_3 &= (1, 1, \ldots, 1, 0).
\end{align*}
\]

We claim that \( H = H_2 = \{h_1, h_2, h_3\} \) is an \( R \)-short covering of \( \mathbb{F}_q^{qr} \). Consider \( x \) an arbitrary vector in \( \mathbb{F}_q^{qr} \).

Case 1: Suppose there is a symbol \( a \in \mathbb{F}_q \) such that \( s_a(x) \geq r + 1 \). It is easy to see that \( d(x, a, h_1) \leq R \), thus \( x \in E(h_1, R) \).

Case 2: Otherwise, \( s_a(x) \leq r \) for each \( a \in \mathbb{F}_q \). Eq. (3) implies \( s_a(x) = r \) for any \( a \in \mathbb{F}_q \). Pick the symbol in the last coordinate of \( x \), say \( a = x_{qr} \), and take the linear operator \( \sigma = \sigma_a \) on \( \mathbb{F}_q \). We analyze the behavior of the set \( \Delta = \{a\} \) under \( \sigma_a \).

Case 2.1: If \( \Delta \) is invariant under \( \sigma_a \), then Lemma 7 implies \( a = 0 \). In this case, we have \( d(x, h_3) = R \), because \( x \) and \( h_3 \) coincide in the last coordinate and \( s_1(x) = r \). Thus \( x \in E(h_3, R) \).

Case 2.2: If \( \Delta \) is not invariant under \( \sigma_a \). By Corollary 6, there is a \( \sigma \)-path of type \( (a_1, a, a_2) \) crossing \( \Delta \). Note that \( a_3 = \omega a \) and \( a = \omega a_1 \). Since \( x \) and \( a_1 \cdot h_2 \) coincide in the last coordinate (\( \sigma_a(a_1) = a \)) and \( s_{a_1}(x) = r \), we obtain \( d(x, a_1, h_2) = R \). Therefore \( x \in E(h_2, R) \). \( \square \)

**Remark 1.** The bound above cannot be improved for all instances. Indeed, the upper bound is sharp at least for the class \( c_3(3n, 2n - 1) = 3 \) for any positive integer \( n \), according to [16]. See another application of Theorem 9 in Corollary 15.

3.3. Third construction

Let us report the following result.

**Theorem 10** ([18]). We have \( n \geq (t - 1)q + 1 \) if and only if

\[ c_q(n, n - t) = 1. \]

A slight refinement of Theorem 9 under certain assumption is described by Theorem 1.

**Proof of Theorem 1.** The lower bound comes from Theorem 10. For the upper bound, let \( n = qr \) and \( R = qr - r - 1 \). Choose the following vectors in \( \mathbb{F}_q^n \):

\[
\begin{align*}
  k &= (1, 1, \ldots, 1, 1, \ldots, 1) \\
  h &= (1, 1, \ldots, 1, \xi, \ldots, \xi),
\end{align*}
\]

where \( \xi \) denotes a generator of \( \mathbb{F}_q^r \) that appears in the last \( r + 1 \) coordinates of \( h \). We claim that \( H = H_2 = \{k, h\} \) is an \( R \)-short covering of \( \mathbb{F}_q^n \). It is enough to prove that \( \mathbb{F}_q \cdot H \) is an \( R \)-covering of \( \mathbb{F}_q^n \). Pick an arbitrary vector \( x \in \mathbb{F}_q^n \).

Case 1: Suppose there is a symbol \( a \in \mathbb{F}_q \) such that \( s_a(x) \geq r + 1 \). Thus \( x \) and \( a \cdot k \) disagree at most in \( R \) coordinates, and therefore \( d(x, a \cdot k) \leq R \).

Case 2: Otherwise, \( s_a(x) \leq r \) for any \( a \in \mathbb{F}_q \). An application of Eq. (3) yields \( s_a(x) = r \) for any \( a \) in \( \mathbb{F}_q \). The vector \( x \) can be decomposed into \( x = (u, v) \), where \( u \in \mathbb{F}_q^R \) and \( v \in \mathbb{F}_q^{r+1} \). Let \( \Delta \) be the set formed by the symbols that appear in the vector \( v \). Thus \( 2 \leq |\Delta| \leq r + 1 \), with \( r + 1 < q - 1 \). By Lemma 7, this set \( \Delta \) is not setwise invariant under the linear operator \( \sigma : x \mapsto \xi x \). By Corollary 6, there is a \( \sigma \)-path \( (a_1 = a, a_2, \ldots, a_m) \) crossing \( \Delta \). A closer look reveals that \( d(x, a \cdot h) \leq R \).

Indeed, both \( x \) and \( a \cdot h \) have exactly \( r \) symbols \( a \) (among the first \( R \) coordinates), because \( a \notin \Delta \) and \( s_{a_1}(x) = r \). Moreover, \( \sigma(a) = \xi a \) appears at least in one of the coordinates of \( v \) (among the last \( r + 1 \) coordinates of \( x \)). Therefore \( H = \{k, h\} \) is an \( R \)-short covering of \( \mathbb{F}_q^n \). \( \square \)

**Remark 2.** A few remarks are reported below.

• **Theorem 1** generalizes the previous result \( c_q(q, q - 2) = 2 \) for any prime power \( q \geq 4 \), by Mendes et al. [16].

• In contrast with the previous result, the computation of the corresponding number \( K_q(q, q - 2) \) still remains an open problem for arbitrary \( q \). Their exact values were only determined for \( q \leq 10 \), according to Haas et al. [9].

• The hypothesis \( q \geq r + 3 \) is essential, because the result cannot be extended to arbitrary \( q \). Note that \( c_3(3, 1) = 3 \); see [18].

• Both **Theorems 1** and **10** yield \( c_5(5, 3) = 2 \).
4. Equivalence on short coverings

A concept of equivalence on short covering is described now.

Given a prime power $q$, let $D_q$ denote the direct product of $n$ copies of $L_n$, where $L_n$ is the group of nonsingular linear operators of $F_q$. As usual, $S_n$ denotes the symmetric group of degree $n$. For each $\alpha \in S_n$, each $\sigma = (\sigma_1, \ldots, \sigma_n) \in D_q$ and each $h = (h_1, \ldots, h_n) \in F_q^n$, define

$$h^{(\alpha, \sigma)} = ((h_{(1)\alpha^{-1}})^{\sigma_1}, \ldots, (h_{(n)\alpha^{-1}})^{\sigma_n}).$$

This action of group is called the wreath product of $(F_q^n)$ by $S_n$; see details in [25].

**Definition 4 ([18]).** Consider $H$ and $L$ subsets of $F_q^n$. We say that $H$ and $L$ are $F_q$-equivalent if and only if there is a pair $(\alpha, \sigma)$, with $\alpha \in S_n$ and $\sigma = (\sigma_1, \ldots, \sigma_n) \in D_q$, such that

$$L = H^{(\alpha, \sigma)} = \{h^{(\alpha, \sigma)} | h \in H\}.$$

**Proposition 11.** Let $H_\omega$ and $H_{\omega'}$ be the short coverings constructed in Theorem 9 by using the elements $\omega$ and $\omega'$, respectively. The sets $H_\omega$ and $H_{\omega'}$ are $F_q$-equivalent if and only if $\omega = \omega'$ or $\omega\omega' = 1$.

**Proof.** If $H_\omega$ and $H_{\omega'}$ are $F_q$-equivalent, then there exists a permutation $\alpha$ in $S_q$ and there is $\sigma = (\sigma_1, \ldots, \sigma_q) \in D_q$ such that $H_{\omega'} = H^{(\alpha, \sigma)}$. A look on the last coordinate reveals that $\sigma_q((1, \omega)) = (1, \omega')$. If $\sigma_q(1) = 1$, then $\sigma_q$ corresponds to the identity function, that is, $\omega = \omega'$. Otherwise, $\sigma_q(1) = \omega'$, and therefore $\sigma_q(\omega) = 1$. Since $\sigma_q(\omega) = \omega, \sigma_q(1) = \omega, \omega'$, we obtain $\omega' = 1$. On the other hand, we can take $\alpha$ the identity function in $S_q$ and define $\sigma = (\sigma_1, \ldots, \sigma_q) \in D_q$ as follows

$$\sigma_i(x) = \begin{cases} x & \text{if } 1 \leq i < qr - 1 \\ \omega x & \text{if } i = qr. \end{cases}$$

Thus $H_{\omega'} = H^{(\alpha, \sigma)}$, and the converse is complete. \qed

**Proposition 12.** Let $H_\xi$ and $H_{\xi'}$ be the short coverings constructed in Theorem 1 by the elements $\xi$ and $\xi'$, respectively. The sets $H_\xi$ and $H_{\xi'}$ are $F_q$-equivalent if and only if $\xi = \xi'$ or $\xi\xi' = 1$.

**Proof.** The proof is similar to that given in the previous proposition. \qed

5. From short coverings to classical covering codes

A useful relationship between the function $c$ and $K$ is described below.

**Theorem 13 ([18]).** For any prime power $q$ and for any $R$ such that $0 \leq R \leq n$, the inequalities hold

$$c_q(n, R) + 1 \leq K_q(n, R) \leq (q - 1)c_q(n, R) + 1.$$

Note that both inequalities are tight at least for $q = 2$, since $c_2(n, R) = K_2(n, R) - 1$. This relationship constitutes a systematic way to translate bounds, as illustrated below.

**Corollary 14.** The optimal bound $c_q(4, 2) = 3$ holds.

**Proof.** Theorem 13 applied to the instance $q = 5, n = 4, R = 2$ yields $c_5(4, 2) \geq 3$, because $K_5(4, 2) = 11$ (see [9,22] or updated tables in [12]). The sharp bound $c_5(4, 2) = 3$ follows as a consequence of Proposition 8. \qed

**Corollary 15.** We have $c_q(8, 5) = 3$.

**Proof.** The upper bound is an application of Theorem 9. The lower bound is derived by applying Theorem 13 to $K_4(8, 5) = 8$, by Kéri and Östergård [13]. \qed

In another direction, we now discuss the impact of the previous results on the number $K_q(n, R)$.

**Proof of Corollary 2.** An immediate application of Theorems 1 and 13 produces the proof. \qed

**Example 16.** A particular construction of Theorem 1 yields that the set

$$H = \{1111111111, 1111111222\}$$

is a sharp 7-short covering of $F_S^{10}$. By using Theorem 13, the nine vectors in $F_5 \cdot H$ produce an optimal 7-covering of $F_S^{10}$. 

---

Remark 3. A few consequences of Corollary 2 are listed below.

1. Corollary 2 improves the classical bound $K_q( qr, qr − r − 1) ≤ 2q$, by Östergård [22, Theorem 6].
2. The sharp upper bound $K_q(10, 7) = 9$ in [16] is a special case of Corollary 2 (see Example 16). The lower bound $K_q(10, 7) ≥ 9$ was obtained by Haas et al. [9].
3. Corollary 2 yields alternative proofs for both upper bounds
   $$K_q(4, 2) = 7 \text{ and } K_q(5, 3) = 9$$
   (see tables in [5] or [12]). The previous constructions in [21] were based on $s$-surjective matrices in the context of mixed covering codes.
4. Corollary 2 emphasizes the strong relationships between $c_q(n, R)$ and $K_q(n, R)$.

Theorem 17. The inequality below is due to Bhandari and Durairajan [2].

$$K_q(n_1 + n_2, R_1 + R_2 + 1) \geq \min \{K_q(n_1, R_1), K_q(n_2, R_2)\} .$$

Example 18. Near-optimal bounds can be determined too, for instance,

$$11 ≤ K_q(14, 11) ≤ 13 \text{ and } 12 ≤ K_q(16, 13) ≤ 15 .$$

The upper bounds follow from Corollary 2. On the other hand, the lower bounds are derived by combining Theorem 17 and the numbers $K_q(7, 5) = 11$ and $K_q(8, 6) = 12$, by Kéri and Östergård [14].

6. Extremal problems

Let us consider the permutation on the general case $Ω$. Invariant sets and cyclic factors are closely associated, more precisely.

Lemma 19. Take the factorization of $γ = γ_1 · · · γ_s$ into pairwise disjoint cycles. The statements are equivalent.

1. $Δ$ is a minimal invariant set under $γ$.
2. $Δ$ is formed by the elements in one of the cycles $γ_i$, where $1 ≤ i ≤ s$.

Proof. Let $Δ = \{a_1, . . . , a_m\}$ be the elements of the cycle $γ_i$. Since this set is invariant under $γ$, it remains proving that $Δ$ is minimal. Let $I'$ be a subset of $Δ$ and suppose that an element $a_j$ belongs to $I'$, where $1 ≤ j ≤ m$. If the set $I'$ is invariant under $γ$, then any power $γ^j(a_i)$ always belongs to $I'$. Since these powers generate the set $Δ$, we conclude $I' = Δ$.

Conversely, suppose that $Δ$ is an invariant set under $γ$ and $a_i ∈ Δ$. By Lemma 3, each $a_i$ belongs to one cycle $γ_i$, for some $i$ with $1 ≤ i ≤ s$. Because $Δ$ is an invariant set under $γ$, any element of the cycle $γ_i$ also belongs to $Δ$. These sets should be equal, since $Δ$ is minimal. □

How many invariant sets under $γ$ are there? Let $d(γ)$ denote this number. The computation of $d(γ)$ depends on the well-known decomposition of $γ$ into cycles, as described below.

Proposition 20. Suppose the decomposition of $γ$ into $s$ cyclic factors. Then

$$d(γ) = 2^i − 1 .$$

Proof. Consider the complete factorization of $γ = γ_1 · · · γ_s$ into pairwise disjoint cycles. Each element $a$ in $\{1, 2, . . . , n\}$ is contained in exactly one minimal invariant set, denoted by $Min(a)$.

Let $C$ be an invariant set under $γ$. Note that $C ⊆ \bigcup_{a∈γ} Min(a)$. By the previous lemma, $Min(a) = \{\text{elements of } γ_i, \text{ where } a ∈ γ_i\}$. Therefore $C$ is partitioned into sets of type $Min(a)$, that is,

$$C = Min(a_{i_1}) ∪ · · · ∪ Min(a_{i_k})$$

for a suitable $k$ such that $1 ≤ k ≤ s$, where the elements $a_{i_k}$ belong to distinct minimal invariant sets. Moreover, a nonempty invariant set $C$ corresponds to a nonempty subset of indices $\{i_1, . . . , i_k\}$ in $\{1, . . . , s\}$, which can be chosen from $2^i − 1$ ways. □

Remark 4. Note that the previous proposition yields an alternative proof of the second part of Lemma 7. Indeed, the cyclic decomposition of $σ_4$ is written as $σ_4 = (0) · (1, 1, 1, 1)$. Hence there are 3 invariant sets under $σ_4$, as described in Lemma 7.

We go back to the path $γ$ illustrated in Example 4. What is the maximum number of $γ$-paths crossing $Δ$? The set $\{0, 1, 3\}$ in Example 4 implies that this number is at least 3. More generally, the following extremal problems arise naturally.
Problem 1. Given a permutation \( \gamma \) in \( S_n \), what is the maximum number \( g(\gamma) \) of \( \gamma \)-paths crossing \( \Delta \), where \( \Delta \) is a nonempty subset in \( \{1, \ldots, n\} \)? More formally,
\[
g(\gamma) = \max_{\Delta \subseteq \{1, \ldots, n\}} c(\gamma, \Delta).
\]

Problem 2. Given a subset \( \Delta \) of \( \{1, \ldots, n\} \), what is the maximum number of \( \gamma \)-paths crossing \( \Delta \), where \( \gamma \) is chosen among all permutations in \( S_n \)? Let \( h(\Delta) \) denote this number, that is,
\[
h(\Delta) = \max_{\gamma \in S_n} c(\gamma, \Delta).
\]

6.1. Reformulation via digraphs

In this section, permutation and invariant set are reformulated in terms of graph theory. The cyclic decomposition of a permutation corresponds to a decomposition of a digraph into suitable components. Given a permutation \( \gamma \in S_\Omega \), the directed graph (digraph) \( \mathcal{G}^* = \mathcal{G}^*(\gamma) \) is defined as follows:
1. each element of \( \Omega \) is also a vertex of \( \mathcal{G}^* \);
2. the edge \((a, b)\) belongs to \( \mathcal{G}^* \) iff \( \gamma(a) = b \), where \( a \neq b \).

Note that each point fixed by \( \gamma \) represents an isolated vertex in \( \mathcal{G}^* \). For convenience, the digraph \((\{a, b\}, \{(a, b), (b, a)\})\) induced by the 2-cycle \((a, b)\) is denoted by \( C_2 \). More generally, each cycle of size \( k \), \( k \geq 3 \), in the decomposition of \( \gamma \) is associated to a directed cycle of type \( C_k \). The \( \gamma \)-path \((a_1, \ldots, a_m)\) in \( S_\Omega \) corresponds to the direct path \((a_1, \ldots, a_m)\) in \( \mathcal{G}^*(\gamma) \). This way of looking at permutation differs slightly from the standard in the literature; see [1] for instance.

Example 21. Consider the following digraphs: \( g_1^* = ([2], \emptyset) \), \( g_2^* = ([1, 4], ([1, 4], (4, 1))) \), and
\[
g_2^* = ([3, 5, 6, 0], (3, 5), (5, 0), (0, 6), (6, 3)).
\]
The permutation \( \gamma \) in Example 4 corresponds to the direct graph \( g^* \), which is decomposed into \( g^* = g_1^* \cup g_2^* \cup g_3^* \). By deleting the order of edges and eventually the multiple edges, \( \gamma \) can be also reduced to the simple graph \( \tilde{g} \) formed by the union of \( K_1 \) (isolated vertex), \( K_2 \) (edge), and a copy of \( C_4 \).

6.2. Solutions of the problems

Given a subset \( W \) of the vertices of a simple graph \( G = (V, E) \), we say that \( W \) is an independent set if there is no edge between the vertices of \( W \). The independence number \( \alpha(G) \) denotes the maximum cardinality of an independent set \( W \) in \( G \); see details in [3]. It is easy to see that for any positive integer \( m \),
\[
\alpha(C_{2m}) = m \quad \text{and} \quad \alpha(C_{2m+1}) = m.
\]

We are ready to answer Problem 1.

Theorem 22. Let \( \gamma \) be a permutation in \( S_n \) with \( t \) non-fixed points, and suppose that its decomposition (without 1-cycle) has \( r \) odd cycles, with \( r \geq 0 \). Then
\[
g(\gamma) = \frac{t - r}{2}.
\]

Proof. A simple computing reveals that \( t \) and \( r \) have the same parity. Consider the decomposition
\[
\gamma = \gamma_1 \cdots \gamma_{r-1} \gamma_{r+1} \cdots \gamma_s,
\]
where each \( \gamma_i \) is an \( n_i \)-cycle. Without loss of generality (because the product of disjoint cycles is abelian), suppose that the first \( r \) cycles are odd, that is: \( n_i = 2m_i \) for \( 1 \leq i \leq r \) and \( n_i = 2m_i \) for \( r + 1 \leq i \leq s \).

First part: pick an arbitrary \( \Delta \), we prove initially that the number of \( \gamma \)-paths crossing \( \Delta \) is at most \((t - r)/2\). We analyze the contribution of each component \( \gamma_i \), with \( 1 \leq i \leq s \). For each \( i \), denote \( D_i = \{a \notin \Delta : \gamma_i(a) \in \Delta\} \), thus \( |\gamma_i(D_i)| = |D_i| \). Regard now \( \gamma_i \) as a simple graph which is isomorphic to the cycle \( C_{n_i} \) of order \( n_i \). Since \( \gamma_i(D_i) \) is an independent set of \( C_{n_i} \), Eq. (4) implies that \( 2|D_i| \leq n_i \) if \( r + 1 \leq i \leq s \), and \( 2|D_i| + 1 \leq n_i \) if \( 1 \leq i \leq r \). Denote
\[
D = \bigcup_{i=1}^s D_i = \{a \in S_n - \Delta : \gamma(a) \in \Delta\},
\]
and write \( d = |D| \). Since the sets \( D_i \) are pairwise disjoint,
\[
2d + r \leq \sum_{i=1}^s n_i = t.
\]

By Proposition 5, the number of \( \gamma \)-paths crossing \( \Delta \) is at most \( d \), where \( d = (t - r)/2 \).
Second part: the bound \((t - r)/2\) may be reached by a suitable choice of \(\Delta\). Indeed, we have to construct a subset \(\Delta\) which induces \((t - r)/2\) \(\gamma\)-paths crossing \(\Delta\). We also consider the decomposition of \(\gamma\). For each \(i\), pick \(\Delta_i\) as a largest independent set in \(\gamma_i\) (it is possible because \(\gamma_i\) can be regard as a simple graph isomorphic to the cycle \(C_n_i\)). By Eq. (4), the inequality \(|\Delta_i| = m\) holds. The set \(\Delta = \bigcup_{i=1}^{\gamma} \Delta_i\) has exactly \(d = (t - r)/2\) paths, according to Proposition 5. \(\square\)

In the other direction, one of the tools to solve Problem 2 is the edge independence number. Consider a simple graph \(G = (V, E)\) and take a subset \(M\) of \(E\). We say that \(M\) is a matching of \(G\) if the edges in \(M\) are independent. The edge independence number of \(G\) is the largest cardinality \(\alpha'(G)\) of a matching of \(G\) (see [3]).

**Theorem 23.** Given a subset \(\Delta\) of \([1, \ldots, n]\), we have

\[
h(\Delta) = \min(|\Delta|, n - |\Delta|).
\]

**Proof.** Pick an arbitrary \(\gamma\) in \(S_n\). For each \(\gamma\)-path \((a_1, \ldots, a_m)\) crossing \(\Delta\), we select the edge \(\{a_1, a_2\}\) in the complete bipartite graph \(G(S_n - \Delta, \Delta)\) formed by the partition sets \(S_n - \Delta\) and \(\Delta\). The subset of edges

\[
M = \{\{a_1, a_2\} : (a_1, a_2, \ldots, a_m)\} \text{ is a } \gamma\text{-path crossing } \Delta\]

is constructed from the set of all \(\gamma\)-paths crossing \(\Delta\), and this correspondence is injective. Since \(M\) is a matching of \(G(S_n - \Delta, \Delta)\), the number of such paths is at most \(\alpha'(G(S_n - \Delta, \Delta))\).

Conversely, there is at least a permutation \(\gamma\) in \(S_n\) with exactly \(\alpha'(G(S_n - \Delta, \Delta))\) paths. Pick a maximal matching \(M\) in \(G(S_n - \Delta, \Delta)\). For each edge \(e_j = \{a_j, b_j\}\) in \(M\), consider the 2-cycle \(\gamma_j = \{a_j, b_j\}\), that is, \(\gamma_j(a_j) = b_j\) and \(\gamma_j(b_j) = a_j\). Now construct the permutation \(\gamma = \gamma_1 \cdots \gamma_M\), which is well-defined because \(M\) is a matching. Note that \(\gamma\) induces \(|M|\ \gamma\)-paths crossing \(\Delta\), namely, paths of type \(\{a_j, b_j, a_j\}\), where \(1 \leq j \leq |M|\). Since \(\alpha'(G(S_n - \Delta, \Delta)) = \min(|\Delta|, n - |\Delta|)\), the proof is complete. \(\square\)

**Acknowledgment**

We would like to thank I.N. Nakaoka for helpful comments.

**References**

12. K. Gé, Tables for bound on covering codes, hdpeg://www.sztaki.hu/-keri/