On $Z_pZ_p^k$-additive codes and their duality

Minjia Shi, Rongsheng Wu, and Denis S. Krotov, Member, IEEE

Abstract—In this paper, two different Gray-like maps from $Z_p^n \times Z_p^k$, where $p$ is prime, to $Z_p^{n+\beta}$, $n = \alpha + \beta p^{m-1}$, denoted by $\varphi$ and $\Phi$, respectively, are presented. We have determined the connection between the weight enumerators among the image codes under these two mappings. We show that if $C$ is a $Z_pZ_p^k$-additive code, and $C^{\perp}$ is its dual, then the weight enumerators of the image $p$-ary codes $\varphi(C)$ and $\Phi(C^{\perp})$ are formally dual. This is a partial generalization of [D. S. Krotov, On $Z_pZ_p^k$-dual binary codes, IEEE Trans. Inform. Theory 53 (2007), 1532–1537, arXiv:math/0509225], and the result is generalized to odd characteristic $p$ and mixed alphabet. Additionally, a construction of 1-perfect additive codes in the mixed $Z_pZ_{p^2}\ldots Z_{p^k}$ alphabet is given.

Index Terms—Dual codes, Gray map, linear codes, MacWilliams identity, two-weight codes, 1-perfect codes.

I. INTRODUCTION

Quaternary codes have attracted people’s attention since the 80th, due to their relationship to some well-known nonlinear binary codes [11], [15], [16]. It was shown in [11] that some good nonlinear codes, including the Kerdock codes, can be viewed as the image codes of $Z_4$ cyclic codes under the so-called Gray mapping. In [9], the Gray map was generalized to construct new $Z_{p^k}$-linear codes, such as the generalized Kerdock codes and Delsarte-Goethals codes. The definition of the generalized Gray map can be found in Section II, i.e., $\varphi_k$ for the special case $p = 2$. However, it is worth noting that if $C$ is a linear code over $Z_{p^k}$, then it can be proved that the weight enumerators of $\varphi_k(C)$ and $\varphi_k(C^{\perp})$ do not in general satisfy the MacWilliams identity, i.e., are not formally dual. On the positive side, in [13], it was introduced another generalization of the Gray map, which can be viewed as dual to $\varphi_k$ in some sense. It was shown that the weight distributions of the image codes under these two generalized Gray mappings satisfy the MacWilliams identity.

Additive codes (mixed alphabet codes) were first defined by Delsarte in 1973 in terms of association schemes [8]. In the following 1997, the translation invariant propelinear codes were first introduced by Rifà and Pujol [17]. As follows from Delsarte’s results, any abelian binary propelinear codes has the form $Z_4^n \times Z_4^k$ for some nonnegative integers $\gamma$ and $\delta$. In general, a $Z_2Z_4$-additive code is defined to be a subgroup of $Z_2^n \times Z_4^k$; this is a generalization of the usual binary linear codes and quaternary linear codes. Later, the structure and properties of $Z_2Z_4$-additive codes have been intensely studied, including generator matrix, duality, kernel and rank, see [3]–[5], [9]. In [18], perfect $Z_2Z_4$-additive codes were shown to be potentially useful in the steganography, for hiding information; this application can be considered as a partial motivation for further researches in the area of additive codes, including our current results. Furthermore, $Z_2Z_4$-additive codes were generalized to $Z_2Z_{2^t}$-additive codes in [11], these codes are meaningful because they provided good binary codes via Gray maps. Then, the structure and the duality of $Z_{p^k}Z_{p^k}$-additive codes were discussed in [2]. Note that the last two papers mentioned considered additive codes in the Lee metric space. We study another generalization of the $Z_2Z_4$-additive codes, related to the homogeneous metric and the metric that can be considered as dual to homogeneous.

In the present paper, we introduce two generalized Gray maps on $Z_pZ_{p^k}$ (see Section III the definitions of $\varphi$ and $\Phi$), and prove that if $C$ is a $Z_pZ_{p^k}$-additive code and $C^{\perp}$ is its dual, then the images $\varphi(C)$ and $\Phi(C^{\perp})$ are formally dual, i.e., satisfy the MacWilliams identity. The result has a nature extension to the mixed $Z_pZ_{p^2}\ldots Z_{p^k}$ alphabet, see Remark III.7.

It should be mentioned that, while the $Z_2Z_4$-linear binary codes are known as a partial case of the propelinear codes [17], in general the $p$-ary codes obtained by the Gray map from $Z_pZ_{p^k}$-additive codes are not proven to be propelinear even for the case $k = 2$. The study of this question is an interesting topic for further research.

The manuscript is organized as follows. Section II fixes some notations and definitions for this paper, we introduce two generalized Gray-like maps on $Z_pZ_{p^k}$. In addition, we describe the connection between these two mappings. The main results are given in Section III where we establish the MacWilliams identity between the image codes $\varphi(C)$ and $\Phi(C^{\perp})$ (Theorem III.6). Section IV gives a construction of 1-perfect additive codes in the mixed $Z_pZ_{p^2}\ldots Z_{p^k}$ alphabet with a special distance, such that the $\Phi$-image is a perfect code over $Z_p$.
II. Preliminaries

A. Linear Codes

Let $p$ be an odd prime number. Denote by $\mathbb{Z}_p$ and $\mathbb{Z}_{p^k}$ the rings of integers modulo $p$ and $p^k$, respectively. The Hamming weight of $x = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$, denoted by $\text{wt}(x)$, is the number of indices $i$ where $x_i \neq 0$. A linear code $C$ of length $n$ over the ring $\mathbb{Z}_p$ is a $\mathbb{Z}_p$-submodule of $\mathbb{Z}_p^n$. If the cardinality of the code $C$ is $M$, and its (minimum) distance, denoted by $d$, is defined as the minimum Hamming weight of its nonzero elements, then it is sometimes referred to as an $(n, M, d)$ code over $\mathbb{Z}_p$. The weight enumerator of the code $C$ is defined by $W_C(X, Y) = \sum_{c \in C} X^{\text{wt}(c)} Y^{n-\text{wt}(c)}$, a homogeneous polynomial of degree $n$ in two variables. From now on, we will focus on $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive codes. A $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive code is a $\mathbb{Z}_{p^k}$-submodule of $\mathbb{Z}_p^n \times \mathbb{Z}_{p^k}^n$. Throughout this paper we use calligraphic symbols like $\mathcal{C}$ to denote codes in the mixed $\mathbb{Z}_p\mathbb{Z}_{p^k}$ alphabet (even if the $\mathbb{Z}_p$ part is empty), and we use standard symbols like $C$ to denote codes over $\mathbb{Z}_p$.

Let $c = (v|w) \in \mathbb{Z}_p^n \times \mathbb{Z}_{p^k}^n$. For $l \in \mathbb{Z}_{p^k}$, where $l$ can be expressed as $l = l_0 + l_1 p + \cdots + l_{k-1} p^{k-1}$, and $0 \leq l_i \leq p-1$, we have

$$l c = (l_0 v|l w).$$

The inner product between $(v_1|w_1)$ and $(v_2|w_2)$ in $\mathbb{Z}_p^n \times \mathbb{Z}_{p^k}^n$ can be written as follows:

$$\langle (v_1|w_1), (v_2|w_2) \rangle = p^{k-1} \langle v_1, v_2 \rangle + \langle w_1, w_2 \rangle \in \mathbb{Z}_{p^k},$$

where $\langle \cdot, \cdot \rangle$ denotes the usual inner product

$$\langle (x_0, \ldots, x_{n-1}), (y_0, \ldots, y_{n-1}) \rangle = x_0 y_0 + \cdots + x_{n-1} y_{n-1}.$$

Note that the result of the inner product $(v_1, v_2)$ is from $\mathbb{Z}_{p^k}$, and multiplication of its value by $p^{k-1}$ should be formally understood as the natural homomorphism from $\mathbb{Z}_p$ into $\mathbb{Z}_{p^k}$.

The dual code $\mathcal{C}^\perp$ of a $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive code $\mathcal{C}$ is defined in the standard way by

$$\mathcal{C}^\perp = \{ (x|y) \in \mathbb{Z}_p^n \times \mathbb{Z}_{p^k}^n : \langle (x|y), (v|w) \rangle = 0 \text{ for all } (v|w) \in \mathcal{C} \}.$$

Readily, the dual code is also a $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive code.

B. Gray Maps

In this subsection, we will introduce two different Gray-like functions $\varphi$ and $\Phi$ from $\mathbb{Z}_p^n \times \mathbb{Z}_{p^k}^n$ to $\mathbb{Z}_{p^k}^n$, $n = \alpha + \beta p^{k-1}$. The first Gray-like map $\varphi$ corresponds to the homogeneous metric over $\mathbb{Z}_{p^k}$, and the second function $\Phi$ can be regarded as the dual of the first case (in general, $\Phi$ is a multi-valued function; so, formally it is a map from $\mathbb{Z}_p^n \times \mathbb{Z}_{p^k}^n$ to the set of subsets of $\mathbb{Z}_{p^k}^n$). More details are given as follows.

Let $P$ be the linear code over $\mathbb{Z}_p$ with the generator matrix $A$ in the form $\{I_p\}$, where $I$ denotes the all-1 vector of length $p^{k-1}$ and the columns of the matrix $B$ are all different vectors in $\mathbb{Z}_{p^k}^{p-1}$. Then $P$ is a linear two-weight code of size $p^k$ with nonzero weights $(p-1)p^{k-2}$ and $p^{k-1}$. Arrange the codewords in $P = \{c_0, c_1, \ldots, c_{p^k-1}\}$ in such a way that $c_0 = (0, \ldots, 0)$ and for all $i$, $0 \leq i \leq p^k - 1$, and $j$, $0 \leq j \leq p - 1$, the codeword $c_{i+jp^k-1} - c_i$ has the form $(j, j, \ldots, j)$.

**Example II.1.** Let $p = k = 3$. From the description above, the generator matrix $A$ has the form as follows:

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\
0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2
\end{pmatrix}$$

and the weight enumerator of the code $P$ with the generator matrix $A$ is given by

$$W_C(X, Y) = X^9 + 24X^3Y^6 + 2Y^9.$$

**Definition 1.** Define the Gray map $\varphi_k$ from $\mathbb{Z}_{p^k}^n$ to $\mathbb{Z}_p^{p^k-1}$ as

$$\varphi_k(x_1, x_2, \ldots, x_n) = (c_{x_1}, c_{x_2}, \ldots, c_{x_n}),$$

where $x_i \in \mathbb{Z}_{p^k}$, $c_{x_i} \in \mathbb{Z}_{p^k-1}$ and $1 \leq i \leq n$.

Then the weight function $wt^*$ is defined by:

$$wt^*(x) = \begin{cases} 
0 & \text{if } x = 0, \\
p^{k-1} & \text{if } x \in p^{-k-1}\mathbb{Z}_{p^k}\backslash\{0\}, \\
(p-1)p^{k-2} & \text{otherwise}.
\end{cases}$$

The definition of the weight function here is consistent with the homogeneous metric introduced in [7], and we know this weight function can be expressed by a character sum $\Omega^2$. The corresponding distance $d^*$ on $\mathbb{Z}_p^{p^k-1}$ is defined as follows:

$$d^*(x, y) = \sum_{i=1}^{n} wt^*(y_i - x_i),$$

where $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}_p^{p^k}$.

It is easy to check that the mapping $\varphi_k$ is an isometric embedding of $(\mathbb{Z}_{p^k}^n, d^*)$ into $(\mathbb{Z}_p^{p^k-1}, d_H)$, where $d_H$ denotes the usual Hamming distance. If $C$ is a code with parameters $(n, M, d^*)$ over $\mathbb{Z}_{p^k}$, then the image code $C = \varphi_k(C)$ is a code with parameters $(p^{k-1}n, M, d_H)$ over $\mathbb{Z}_p$. Then, we define the Gray-like map $\varphi$ for elements $(v|w) \in \mathbb{Z}_p^n \times \mathbb{Z}_{p^k}^n$ by $\varphi((v|w)) = (\varphi_k(v|w))$.

Next, we introduce another Gray map from its dual side. Let the code $D$ be the dual to the linear code $P$ with the parity-check matrix $A$ introduced above. If $p$ is odd, then any two columns of $A$ are linearly independent and $A$ has three columns that are linearly dependent; so, the dual code $D$ is a linear code with parameters $(p^{k-1}p^{k-1}, p^{k-1}k, 3)$ over $\mathbb{Z}_p$. If $p = 2$, then $D$ is a binary $(2^{k-1}, 2^{2k-2} - k, 4)$ extended Hamming code. Consider all the cosets of the linear code $D$, write as $D_i$ for $i = 0, 1, \ldots, p^k - 1$. Then the set $\{D = D_0, D_1, \ldots, D_{p^k-1}\}$ forms a partition of $\mathbb{Z}_p^{p^k-1}$. Additionally, we require the sum of all coordinates of a codeword of $D_i$ to be equal to $i \mod p$ (for every coset, this sum is a constant, because $(1, \ldots, 1)$ is a row of $A$; so, this condition can be satisfied by an appropriate enumeration of the cosets).

**Definition 2.** Define the Gray map $\Phi_k$ from $\mathbb{Z}_{p^k}^n$ to the set of subsets of $\mathbb{Z}_p^{p^k-1}$ by

$$\Phi_k((x_1, x_2, \ldots, x_n)) = D_{x_1} \times D_{x_2} \times \cdots \times D_{x_n},$$

where $x_i \in \mathbb{Z}_{p^k}$, $1 \leq i \leq n$.
where \( x_i \in \mathbb{Z}_{p^k}, D_0, D_1, \ldots, D_{p^k-1} \) are the cosets of \( D \), ordered as described above.

For \( x \in \mathbb{Z}_{p^k} \), the weight function \( wt^\circ \) is defined as follows:

\[
wt^\circ(x) = \begin{cases} 
0 & \text{if } x = 0, \\
1 & \text{if } p \nmid x, \\
2 & \text{if } p | x, \text{ and } x \neq 0.
\end{cases}
\]

The corresponding distance \( d^\circ \) on \( \mathbb{Z}_{p^k}^n \) is defined as follows:

\[
d^\circ(x, y) = \sum_{i=1}^{n} wt^\circ(y_i - x_i),
\]

where \( x = (x_1, x_2, \ldots, x_n) \), \( y = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}_{p^k}^n \).

The map \( \Phi_k \) introduced here is not an isometric embedding of \( (\mathbb{Z}_{p^k}^n, d^\circ) \) into \( (\mathbb{Z}_p^{p^k-1}n, d_H) \), but still carry some partial isometric properties. If a code \( C \) with parameters \((n, |C|, d^\circ)\) over \( \mathbb{Z}_{p^k} \), then the image code

\[
\Phi_k(C) = \bigcup_{c \in C} \Phi_k(c)
\]

is a code with parameters \((p^{k-1}n, |C|, p^{(p^k-1-k)n}, d^\circ)\) over \( \mathbb{Z}_p \), where \( d^\circ = \min\{3, d^\circ\} \) for odd \( p \) and \( d^\circ = \min\{4, d^\circ\} \) in the case \( p = 2 \).

Similarly, we define the Gray-like map \( \Phi \) for the elements \((v|w)\) of \( \mathbb{Z}_p^\alpha \times \mathbb{Z}_p^\beta \) and for the subsets \( C \) of \( \mathbb{Z}_p^\alpha \times \mathbb{Z}_p^\beta \):

\[
\Phi((v|w)) = \{v\} \times \Phi_k(w), \quad \Phi(C) = \bigcup_{(v|w) \in C} \Phi((v|w)).
\]

**III. \( \mathbb{Z}_p \)-Duality for Image Codes**

In this section, we determine the weight relationship between the image codes \( \varphi(C) \) and \( \Phi(C^\perp) \) under the maps \( \varphi \) and \( \Phi \), respectively. For this purpose, we have to start with the weight distributions of the cosets of the linear code \( C \). We first observe that \( D \) satisfies the hypothesis of the following proposition.

**Proposition III.1.** Let \( d \) be the Hamming distance of a code \( C \), and let \( s \) be the number of nonzero Hamming weights of its dual.

(i) [8 Theorem 5.13] If \( 2s - 1 \leq d \leq 2s + 1 \), then the weight distribution of a coset of \( C \) depends only on its minimum weight.

(ii) [8 Theorem 5.10] The minimum weight of a coset of \( C \) cannot be larger than \( s \).

Therefore, the cosets of \( D \) have only 3 different weight distributions. Trivially, the coset \( D_0 = D \) has a word of weight 0. All other cosets \( D_i, p | i \), have minimum weight 2, because their words are orthogonal to the all-zero word and by Proposition III.1(ii). The remaining cosets \( D_i, p \nmid i \), have minimum weight 1, because their number coincides with the number of weight-1 words.

**Lemma III.2.** Let the linear code \( D \) be introduced in Section II and let \( \{D = D_0, D_1, \ldots, D_{p^k-1}\} \) be the coset partition of \( \mathbb{Z}_p^{p^k-1} \) introduced above. Then

- the weight enumerator of \( D_0 \) satisfies the identity
  \[
  \frac{1}{|D_0|} W_{D_0}(X + (p-1)Y, X - Y) = X^{p^{k-1}} + (p-1)Y^{p^{k-1}} + (p - p)X^{p^{k-1}}Y^{(p-1)p^{k-2}};
  \]
- if \( i \equiv 0 \mod p \) and \( i \neq 0 \), then
  \[
  \frac{1}{|D_i|} W_{D_i}(X + (p-1)Y, X - Y) = X^{p^{k-1}} + (p-1)Y^{p^{k-1}} - pX^{p^{k-1}}Y^{(p-1)p^{k-2}};
  \]
- if \( i \not\equiv 0 \mod p \), then
  \[
  \frac{1}{|D_i|} W_{D_i}(X + (p-1)Y, X - Y) = X^{p^{k-1}} - Y^{p^{k-1}}.
  \]

**Proof.** The weight enumerator of \( D_0 \) is easy to obtain from the MacWilliams identity, since its dual \( P \) is a two-weight code. For the rest cases, let \( H \) be a linear code of length \( p^{k-1} \) with the generator matrix containing the all-1 vector over \( \mathbb{Z}_p \) as the only row. Denote the dual of \( H \) by \( H^\perp \). We know that the weight enumerator of \( H^\perp \) is

\[
W_{H^\perp}(X, Y) = \frac{1}{|H|} W_H(X + (p-1)Y, X - Y) = X^{(p + 1)Y^{p^{k-1}} + (p - 1)(X-Y)^{p^{k-1}}}.
\]

On the other hand, we know

\[
W_{D_i}(X, Y) = \frac{1}{p^k} \left( X^{(p + 1)Y^{p^{k-1}} + (p - 1)(X-Y)^{p^{k-1}}} \right)
\]

and

\[
\begin{align*}
X^{(p + 1)Y^{p^{k-1}} + (p - 1)(X-Y)^{p^{k-1}}} - p(X + (p-1)Y)^{p^{k-1}}(X-Y)^{(p-1)p^{k-2}}.
\end{align*}
\]

Then, by a simple variable substitutions, we obtain the result directly. The remaining case follows from the fact that \( \mathbb{Z}_p^{p^k-1}\).}

**The complete weight enumerator of a \( \mathbb{Z}_p\mathbb{Z}_p \)-additive code \( C \) is**

\[
W_C(X_i, Y_j; \ i = 0, 1, \ldots, p - 1, \ j = 0, 1, \ldots, p^k - 1) = \sum_{(v|w) \in C} \left( \prod_{i=1}^{\alpha} X_{v_i} \right) \left( \prod_{j=1}^{\beta} Y_{w_j} \right),
\]

Then, we define the polynomial \( SW_C(X, S, Y, Z, T) \) obtained from \( W_C \) by

- substituting \( X \) for \( X_0, Y \) for \( Y_0 \),
Let $\omega_1$ and $\omega_2$ be the complex numbers $e^{2\pi i/p}$ and $e^{2\pi i/p^k}$, respectively. For a complex-valued function $f$ defined on $\mathbb{Z}_p^{\alpha} \times \mathbb{Z}_p^{\beta}$, denote
\[
\hat{f}(z) = \sum_{u \in \mathbb{Z}_p^{\alpha} \times \mathbb{Z}_p^{\beta}} \omega_2^{(z,u)} f(u), \quad z \in \mathbb{Z}_p^{\alpha} \times \mathbb{Z}_p^{\beta}.
\]
Here $\omega_2^{(z',z'')}$ can be written as $\omega_2^{(u',z')} \omega_2^{(u'',z'')}$, where $u', z' \in \mathbb{Z}_p^{\alpha}$ and $u'', z'' \in \mathbb{Z}_p^{\beta}$. The function $\hat{f}$ is called the Fourier transform of $f$.

**Lemma III.3.** Let $C$ be an additive code in $\mathbb{Z}_p^{\alpha} \times \mathbb{Z}_p^{\beta}$, and let $C^\perp$ be its dual. Then for every complex-valued function $f$ on $\mathbb{Z}_p^{\alpha} \times \mathbb{Z}_p^{\beta}$,
\[
\sum_{u \in C} \omega_2^{(u,z)} f(u) = \frac{1}{|C|} \sum_{u \in C} \hat{f}(u).
\]

**Proof.** We have
\[
\sum_{u \in C} \omega_2^{(u,z)} f(u) = \sum_{u \in C} \sum_{z' \in \mathbb{Z}_p^{\alpha} \times \mathbb{Z}_p^{\beta}} \omega_2^{(u,z')} f(u) = \sum_{z \in \mathbb{Z}_p^{\alpha} \times \mathbb{Z}_p^{\beta}} f(z) \sum_{u \in C} \omega_2^{(u,z)}.
\]
If $z \in C^\perp$, then $\langle u, z \rangle = 0$ for all $u \in C$. Hence, the inner sum $\sum_{u \in C} \omega_2^{(u,z)}$ is equal to $|C|$. On the other hand, if $z \notin C^\perp$, then there exists $u_0 \in C$ such that $\langle u_0, z \rangle = \lambda \neq 0$. Since $C$ is an $\mathbb{Z}_p^{\alpha} \mathbb{Z}_p^{\beta}$-additive code, for the inner sum $\sum_{u \in C} \omega_2^{(u,z)}$, we have
\[
\sum_{u \in C} \omega_2^{(u,z)} = \sum_{u \in C} \omega_2^{(u+u_0,z)} = \omega_2^{(u_0,z)} \sum_{u \in C} \omega_2^{(u,z)}.
\]
Since $\omega_2^{(u_0,z)} \neq 1$, the inner sum is zero. Therefore,
\[
\sum_{u \in C} \hat{f}(u) = |C| \sum_{z \in C^\perp} f(z).
\]
Then the result follows. \(\square\)

Let $z = (z', z'') \in \mathbb{Z}_p^{\alpha} \times \mathbb{Z}_p^{\beta}$ and
\[
f(z) = \prod_{i=0}^{p-1} X_i^{w_i(z')} \prod_{j=0}^{p^k-1} Y_j^{w_j(z'')},
\]
where $w_i(z')$ (respectively, $w_j(z'')$) denotes the number of $i$ (respectively, $j$) in $z'$ (respectively, $z''$). By computing the Fourier transform $\hat{f}(z)$ of $f(z)$, and according to Lemma III.3 we find that the complete weight enumerator $W_{C^\perp}$ satisfies the MacWilliams identity
\[
W_{C^\perp}(X_i, Y_j; i = 0, 1, \ldots, p-1, \ j = 0, 1, \ldots, p^k-1) = \frac{1}{|C|} W_C \left( \sum_{t=0}^{p^k-1} \sum_{s=0}^{p-1} \omega_2^{(z',z'')} X_i^{w_i(z')} Y_j^{w_j(z''); i = 0, 1, \ldots, p-1, \ j = 0, 1, \ldots, p^k-1} \right).
\]
• $SW_0$ equals $X$.
• $SW_i$ equals $S$ for $i \neq 0$.
• $SW_0$ equals $Y$.
• $SW_i$ equals $Z$ if $p \nmid i$, and
• $SW_i$ equals $T$ if $p \mid i$ and $i \neq 0$.

On the other hand, according to the definition of the map $\Phi$ introduced in Section II, the image $\Phi(e)$ contributes $SW_{x_1} \ldots SW_{x_n} W_{D_{x_1}}(X, Y) \ldots W_{D_{x_n}}(X, Y)$ to $W_C(X, Y)$. From Lemma III.2, we know that $W_{D_i}(X, Y)$ equals $W_{D_0}(X, Y)$ if $p \nmid i$, and $W_{D_i}(X, Y)$ equals $W_{D_p}(X, Y)$ if $p \mid i$ and $i \neq 0$. The desired result follows.

Now, we introduce the main result of this section.

**Theorem III.6.** Let $C$ be an additive code in $\mathbb{Z}_p^r \times \mathbb{Z}_{p^k}^s$, and let $C^\perp$ be the dual of $C$. Denote $C = \varphi(C)$ and $C^\perp = \Phi(C^\perp)$. Then we have

$$W_C(X, Y) = \frac{1}{|C^\perp|} W_{C^\perp}(X + (p-1)Y, X - Y).$$

**Proof.** From Lemmas III.2 and III.4 we have

$$W_C(X, Y) = \frac{1}{|C^\perp|} SW_{C^\perp}(X + (p-1)Y, X - Y),$$

$$= \frac{1}{|C^\perp|} \left( \frac{p^k}{|p^k - 1|} \right)^\alpha SW_{C^\perp}(X + (p-1)Y, X - Y),$$

$$= \frac{1}{|C^\perp|} \left( \frac{p^k}{|p^k - 1|} \right)^\alpha W_{D_0}(X + (p-1)Y, X - Y),$$

$$= \frac{1}{|C^\perp|} \left( \frac{p^k}{|p^k - 1|} \right)^\beta W_{D_1}(X + (p-1)Y, X - Y),$$

$$= \frac{1}{|C^\perp|} \left( \frac{p^k}{|p^k - 1|} \right)^\beta W_{D_p}(X + (p-1)Y, X - Y).$$

We know that $|C^\perp| \left( \frac{p^k}{|p^k - 1|} \right)^\beta = |C^\perp|$, and according to Lemma III.3 we have

$$SW_{C^\perp}(X + (p-1)Y, X - Y),$$

$$W_{D_0}(X + (p-1)Y, X - Y),$$

$$W_{D_1}(X + (p-1)Y, X - Y),$$

$$W_{D_p}(X + (p-1)Y, X - Y) = W_{C^\perp}(X + (p-1)Y, X - Y).$$

This completes the proof.

**Remark III.7.** Theorem III.6 can be extended to more general case. Let $C$ be an additive code in $\mathbb{Z}_{p^a_1}^{r_1} \times \mathbb{Z}_{p^a_2}^{r_2} \times \cdots \times \mathbb{Z}_{p^a_k}^{r_k}$, and $C^\perp$ be its dual. Let $C = \varphi(C)$ and $C^\perp = \Phi(C^\perp)$. Then we have

$$W_C(X, Y) = \frac{1}{|C^\perp|} W_{C^\perp}(X + (p-1)Y, X - Y).$$

Note that, for given $v = (v_1|v_2|\ldots|v_k)$ and $u = (u_1|u_2|\ldots|u_k)$ from $C \subseteq \mathbb{Z}_{p^a_1}^{r_1} \times \mathbb{Z}_{p^a_2}^{r_2} \times \cdots \times \mathbb{Z}_{p^a_k}^{r_k}$, where $v_i, u_i \in \mathbb{Z}_{p^a_i}$, the inner product is defined by

$$\langle v, u \rangle = p^{k-1}\langle v_1, u_1 \rangle + p^{k-2}\langle v_2, u_2 \rangle + \cdots + \langle v_k, u_k \rangle, (1)$$

and the Gray-like maps $\varphi$ and $\Phi$ are defined by

$$\varphi(v) = (\varphi_1(v_2), \ldots, \varphi_k(v_k))$$

and

$$\Phi(v) = (\varphi_1(v_1) \times \varphi_2(v_2) \times \cdots \times \varphi_k(v_k)).$$

**IV. ADDITIVE 1-PERFECT CODES**

**Definition 3.** A set $C$ of vertices of a finite metric space is called an $e$-perfect code if every vertex is at distance $e$ or less from exactly one element of $C$; in other words, if every ball of radius $e$ contains exactly one codeword.

In this section, we characterize the additive 1-perfect codes in the mixed $\mathbb{Z}_p^r \mathbb{Z}_{p^2}^s \ldots \mathbb{Z}_{p^k}^t$ alphabet, $p$ prime, with the distance $d^*$ defined as in Section III. Once we have the inner product (1), we can define additive codes with the help of check matrices.

**Theorem IV.1.** Assume that $A$ is a matrix with rows from $\mathbb{Z}_p^r \times \mathbb{Z}_{p^2}^s \times \cdots \times \mathbb{Z}_{p^k}^t$ such that the first $\gamma_1 \geq 0$ rows are of order $p$, the next $\gamma_2 \geq 0$ rows are of order $p^2$, and so on; the last $\gamma_k > 0$ rows are of order $p^k$. Assume that all the rows are linearly independent. The additive code $C \subseteq \mathbb{Z}_p^r \times \mathbb{Z}_{p^2}^s \times \cdots \times \mathbb{Z}_{p^k}^t$ defined by the check matrix $A$ is a 1-perfect code with respect to the distance $d^*$ if and only if for every $i$ from 1 to $k$,

(i) $\alpha_i = p^{\gamma_1}p^{2\gamma_2} \ldots p^{(i-1)\gamma_{i-1}}(p^{\gamma_{i,k}} - p^{(i-1)\gamma_i})/(p^i - p^{i-1})$, where $\gamma_{i,k} = \gamma_i + \cdots + \gamma_k$;

(ii) the order of each of $\alpha_i$ columns of $A$ corresponding to $\mathbb{Z}_{p^i}$ is $p^i$;

(iii) the $\alpha_i$ columns of the matrix $A$ corresponding to $\mathbb{Z}_{p^i}$ are mutually non-collinear.

**Proof.** Only if. Assume that $C$ is a 1-perfect code. It is straightforward from the definition of a 1-perfect code that a codeword cannot have weight $1$ or $2$. Now (ii) is straightforward as if the $j$th column over $\mathbb{Z}_{p^i}$ has order smaller than $p^i$, then the word with $p^i$ in the $j$th position and $0$s in the other must be a codeword of weight 1 (in the case $i = 1$) or 2 (for $i > 1$), leading to a contradiction.

(iii) is also clear because if two columns $x$ and $y$ of maximal order are collinear, then $x = \kappa y$ for some $\kappa$ of order $p^i$ in $\mathbb{Z}_{p^i}$, which results in a weight-$2$ codeword with 1 in the position of $x$, $-\kappa$ in the position of $y$ and 0 in the other positions.

Let us prove (i). The total number of different possible columns of order $p^i$ over $\mathbb{Z}_{p^i}$ is $p^{\gamma_1}p^{2\gamma_2} \ldots p^{(i-1)\gamma_{i-1}}(p^{\gamma_{i,k}} - p^{(i-1)\gamma_i})$ (the first $\gamma_1 + \cdots + \gamma_i$ elements are arbitrary, with the restriction on order; the last $\gamma_{i+1} + \cdots + \gamma_k$ are arbitrary of order at most $p^i$, but there is at least one element of order exactly $p^i$). To obtain the maximum number of non-collinear columns, we divide this number by the number $p^i - p^{i-1}$ of elements of maximum order in $\mathbb{Z}_{p^i}$ and obtain the formula in (i). So, $\alpha_i$
cannot exceed this value. On the other hand, calculating the cardinality of a radius-1 ball $B$ gives

$$|B| = 1 + \sum_{i=1}^{k} (p^i - p^{i-1})\alpha_i$$

$$\leq 1 + \sum_{i=1}^{k} p^{\gamma_i} p^{2\gamma_2} \cdots p^{(i-1)\gamma_{i-1}} (p^{\gamma_i \cdot k} - p^{(i-1)\gamma_{i} \cdot k}) \quad (2)$$

$$= p^{\alpha_1} p^{2\alpha_2} \cdots p^{k\alpha_k}.$$  

From the definition of the 1-perfect code, $|B| \cdot |C|$ coincides with the size of the space; so, (2) is satisfied with equality. (i) follows.

If. From (ii) and (iii), it is easy to see that for different $\epsilon = 1$ from $Z_{p^1} \times Z_{p^2} \times \cdots \times Z_{p^k}$, the syndromes $A\epsilon$ are different. From (iii) and numerical considerations above, we see that $A\epsilon$ exhausts all possible nonzero syndromes from $Z_{p^1} \times Z_{p^2} \times \cdots \times Z_{p^k}$. It follows that for every $u$ from $Z_{p^1} \times Z_{p^2} \times \cdots \times Z_{p^k}$ there is unique $\epsilon$ of weight such that $A\epsilon = Au$; i.e., $u - \epsilon$ is a unique codeword at distance 1 from $u$. Hence, the code is 1-perfect, by the definition.

Corollary IV.2. For every integer $k > 0$, $\gamma_1 \geq 0, \ldots, \gamma_{k-1} \geq 0, \gamma_k > 0$, there exists an additive 1-perfect code in $Z_{p^1} \times Z_{p^2} \times \cdots \times Z_{p^k}$, where

$$\alpha_i = \gamma_i\cdot p^{2\gamma_{2}} \cdots p^{(i-1)\gamma_{i-1}} (p^{\gamma_i \cdot k} - p^{(i-1)\gamma_{i} \cdot k})/(p^i - p^{i-1})$$

Moreover, all 1-perfect codes in $Z_{p^1} \times Z_{p^2} \times \cdots \times Z_{p^k}$ are obtained from each other by monomial transformations, i.e., by permutations of coordinates within each of the $k$ groups and multiplication of each coordinate by a unit of the corresponding ring.

Example IV.3. Let $p = 3$, $k = 3$, $\gamma_1 = 1, \gamma_2 = 0, \gamma_3 = 1$. The following matrix is a check matrix of a 1-perfect code in $Z_3^4 \times Z_3^3 \times Z_3^2$:

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 0 & 3 & 6 & 0 & 9 & 18 \\
1 & 0 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}.$$ 

The size of a radius-1 ball is $1 + \alpha_1 \cdot (3-1) + \alpha_2 \cdot (3^2 - 1) + \alpha_3 \cdot (3^3 - 3^2) = 1 + 4 \cdot 2 + 3 \cdot 6 + 3 \cdot 18 = 81 = 3^4 \cdot 92 = 27^3$.

The following corollary provides an additive analogue of a one-weight linear code in the Hamming space, known as the simplex code.

Corollary IV.4. Under the assumption and notation of Corollary IV.2 the dual $\overline{C}^\perp$ of an additive 1-perfect code $C$ in $Z_{p^1} \times Z_{p^2} \times \cdots \times Z_{p^k}$ is an additive one-homogeneous-weight code with the non-zero homogeneous weight $p^{\gamma - 1}$, where $\gamma = 1\gamma_1 + 2\gamma_2 + \ldots + k\gamma_k$.

Proof. Applying the Gray map $\varphi$ to $C$ we get a code of length $n = (p^\gamma - 1)/(p - 1)$ size $p^{n-\gamma}$, and minimum distance $3$; i.e., a code with the same parameters as the Hamming code. From Remark III.7 it follows that $\Phi(C^\perp)$ has the same weight distribution as the dual of the Hamming code, which is a one-weight (simplex) code of non-zero weight $p^{\gamma - 1}$.

**References**

[1] I. Aydogdu and I. Siap, “The structure of $Z_2 Z_2^r$ -additive codes: Bounds on the minimum distance,” *Appl. Math. Inf. Sci.*, vol. 7, no. 6, pp. 2271–2278, 2013.

[2] I. Aydogdu and I. Siap, “$Z_2 Z_2^r$ -additive codes,” *Linear Multilinear Algebra*, vol. 63, no. 10, pp. 2089–2102, 2015, doi: 10.1080/03081087.2014.952728.

[3] J. Borges, S. T. Dougherty, and C. Fernández-Córdoba, “Characterization of linear codes,” *Adv. Math. Commun.*, vol. 6, no. 3, pp. 287–303, 2012, doi: 10.3934/amc.2012.6.287.

[4] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifa, and M. Villanueva, “$Z_2 Z_2^3$ -additive codes: Generator matrices and duality,” *Des. Codes Cryptography*, vol. 54, no. 2, pp. 167–179, 2010, doi: 10.1007/s10623-009-9316-9.

[5] J. Borges and J. Rifa, “A characterization of 1-perfect additive codes,” *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1688–1697, 1999, doi: 10.1109/18.771247.

[6] C. Carlet, “$Z_2^k$ -Linear codes,” *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1543–1547, 1998, doi: 10.1109/18.681528.

[7] I. Constantinescu and W. Heise, “A metric for codes over residue class rings of integers,” *Probl. Inf. Transm.*, vol. 33, no. 3, pp. 208–213, 1997, translated from *Probl. Peredachi Inf.*, vol. 33(3): 22–28, 1997.

[8] P. Delsarte, “An Algebraic Method for Construction of Linear Codes, ” *Philips Res. Rep.* vol. 13, 1958.

[9] C. Fernández-Córdoba, J. Pujol, and M. Villanueva, “$Z_2 Z_2^3$ -linear codes: Rank and kernel,” *Des. Codes Cryptography*, vol. 56, no. 1, pp. 43–59, 2010, doi: 10.1007/s10623-009-9340-9.

[10] C. Fernández-Córdoba, C. Vela, and M. Villanueva, “On $Z_2^x$ -linear Hadamard codes: Kernel and partial classification,” *Des. Codes Cryptography*, 2018, doi: 10.1007/s10623-018-0546-0.

[11] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, “The $Z_4$-linearity of Kerdock, Preparata, Goethals, and related codes,” *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 301–319, 1994, doi: 10.1109/18.121514.

[12] T. Honold, “Characterization of finite Frobenius rings,” *Arch. Math.*, vol. 76, no. 6, pp. 406–415, 2001, doi: 10.1007/PL00004651.

[13] D. S. Krotov, “$Z_2^k$ -Dual binary codes,” *IEEE Trans. Inf. Theory*, vol. 53, no. 4, pp. 1532–1537, 2007, doi: 10.1109/TIT.2007.892878.

[14] I. A. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, Netherlands: North Holland, 1977.

[15] A. A. Nechaev, “Trace-function in Galois ring and noise-stable codes,” in *Proc. V All-Union Symp. on Theory of Rings, Alg. and Mod.*, Novosibirsk, Russia, 1982, p. 97, in Russian.

[16] A. A. Nechaev, “Kerdock code in a cyclic form,” *Discrete Math. Appl.*, vol. 1, no. 4, pp. 365–384, 1991, doi: 10.1515/dma.1991.1.4.365.

[17] A. A. Nechaev, “Translation-invariant propelinear codes,” *IEEE Trans. Inf. Theory*, vol. 43, no. 2, pp. 590–598, 1997, doi: 10.1109/18.556115.

[18] H. Rifa-Pous, J. Rifa, and L. Ronquillo, “$Z_2 Z_2^r$ -Additive perfect codes in steganography,” *Adv. Math. Commun.*, vol. 5, no. 3, pp. 425–433, 2011, doi: 10.3934/amc.2011.5.425.