J. Algebra Comb. Discrete Appl.
11(2) • 139–150

Received: 19 September 2023
Accepted: 18 January 2024

Journal of Algebra Combinatorics Discrete Structures and Applications

Self-orthogonal and quantum codes over chain rings

Research Article

Maryam Bajalan*, Mina Moeini , Bahattin Yildiz

Abstract: In this paper, we investigate the Gray images of codes over chain rings, leading to the derivation of infinite families of self-orthogonal linear codes over the residue field $\mathbb{F}_q$. We determine the parameters of optimal self-orthogonal and divisible linear codes. Additionally, we study the Gray images of quasi-twisted codes, resulting in some self-orthogonal Griesmer quasi-cyclic codes. Finally, we employ the CSS construction to derive some quantum codes based on self-orthogonal linear codes.

2020 MSC: 94B15, 13B25

Keywords: Gray map, Self-orthogonal code, Quantum code, Quasi-twisted code, Griesmer code

1. Introduction

In recent decades, codes over rings have gathered considerable attention, enriching classical coding theory traditionally defined over finite fields. One of the groundbreaking work in this direction was [9], where Hammons et al. defined the Gray map $\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ by $\phi(x_0 + 2x_1) = (x_1, x_0 + x_1)$, a mapping that preserves distance when $\mathbb{Z}_4$ is equipped with the Lee metric and $\mathbb{F}_2^2$ with the Hamming metric. They showed that some well-known non-linear binary codes, such as Kerdock and Preparata codes, can be obtained as the Gary images of linear codes over $\mathbb{Z}_4$.

The idea of defining a Gray map over a ring was generalized in subsequent works by many different researchers. For example, Carlet extended the above Gray map to an isometry between $\mathbb{Z}_{2^k}$ and a subset of $\mathbb{F}_2^{2^{k-1}}$; see [3]. Using the tensor product, Greferath and Schmidt generalized the mentioned Gray map to an arbitrary finite chain ring; see [8]. They also constructed a ternary non-linear code as the Gray

* *This author is supported by the Bulgarian Ministry of Education and Science, Scientific Programme "Enhancing the Research Capacity in Mathematical Sciences (PIKOM)", No. DO1-67/05.05.2022.*
Maryam Bajalan (Corresponding Author); Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Acad. G. Bonchev Str. Bl. 8, 1113, Sofia, Bulgaria (email: maryam.bajalan@math.bas.bg).
Mina Moeini; Department of Mathematics, Faculty of Mathematical Sciences, Malayer University, Malayer, Iran (email: m.moeini80@gmail.com).
Bahattin Yildiz; Director of Security Research, LG Electronics, Santa Clara, CA 95054, USA (email: bahattinyildiz@gmail.com).

image of a linear code over $\mathbb{Z}_9$. Ling and Blackford introduced a Gray map for $\mathbb{Z}_{p^{k+1}}$ with an algebraic structure, generalizing Carlet's definition; see [13]. Subsequently, Jitman and Udomkavanich generalized this idea to all finite chain rings; see [10].

All the Gray maps defined in [3, 8, 10, 13] have two common properties. The first property is that, under a specific condition, the Gray image of the mentioned rings corresponds to the first-order generalized Reed-Muller codes. The second property is that these Gray maps are distance-preserving mappings from the ring with the homogeneous distance to the field with the Hamming distance. The homogeneous weight, which generalizes the weight used in the aforementioned works, was first introduced by Constantinescu and Heise over the ring $\mathbb{Z}_m$ in [5], and it was further studied over chain rings in [8]. It was also described over Frobenius rings in [6]. The homogeneous weight over rings is an alternative to the Hamming weight over finite fields. Primitive generalized Reed-Muller codes over the field $\mathbb{F}_q$, which is equivalent to Reed-Muller codes in the special case when $q = 2$, were first introduced by Kasami et al. in [11], These codes were also extensively examined by Assmus and Key in [1].

Let R be an arbitrary chain ring with the maximal ideal $\langle\gamma\rangle$, nilpotency index e, and residue field $\mathbb{F}_q$. In this work, we prove that the Gray image of R^n is a self-orthogonal linear code if either $e \geqslant 4$ in the case $q = 2$ or $e \geqslant 3$ in the case $q \geqslant 3$. Moreover, for the special chain ring $\mathbb{F}_q[\gamma]/\langle\gamma^e\rangle$, the Gray image of any R-linear code is a self-orthogonal linear code. This presents a significant advantage in constructing self-orthogonal codes over $\mathbb{F}_q$ by just taking the Gray image of linear codes over the ring extension. A linear $[n, k]$ code is optimal if it has the highest minimum distance among all $[n, k]$ linear codes. In section 3, some optimal self-orthogonal linear codes are tabulated. A code is divisible if the weights of all its codewords are divisible by an integer $\delta > 1$. A significant property of codes equipped with the homogeneous weight is that they are divisible. This makes the tabulated codes in Section 3 more special because they are not only optimal and self-orthogonal but also divisible.

We describe the Gray images of quasi-twisted codes over chain rings and present some theoretical results. Subsequently, by applying these theoretical results, we construct many self-orthogonal Griesmer quasi-cyclic codes. These codes are obtained as the Gray images of a particular class of quasi-twisted codes over a chain ring, offering a construction for codes that might otherwise be challenging to build.

Quantum error-correcting codes were first introduced by Shor and independently by Stean; see [16, 18]. Later, Calderbank, Shor and Stean presented a method to construct quantum error-correcting codes from classical linear codes, known as the CSS construction; see [2, 17]. The CSS construction allows the derivation of quantum error-correcting codes from self-orthogonal codes over finite fields.

The rest of the paper is organized as follows. In Section 2, the fundamental concepts of chain rings and the Gray map defined on them are presented. Additionally, the section provides preliminaries on the first-order generalized Reed-Muller codes. In Section 3, certain conditions are imposed on chain rings to ensure that the Gray images defined on these chain rings are self-orthogonal. The section concludes with a table presenting optimal self-orthogonal codes. In Section 4, a theoretical discussion on quasi-twisted codes over chain rings and their Gray images is presented. In Section 5, some self-orthogonal Griesmer quasi-cyclic codes as the Gray image of quasi-twisted codes are tabulated. In Section 6, employing the CSS construction, some quantum codes are derived from the self-orthogonal Gray images of codes over chain rings.

2. Preliminaries

A finite commutative ring R with identity $1 \neq 0$ is called a finite chain ring if its ideals are linearly ordered by inclusion. Obviously, every chain ring has a unique maximal ideal, denoted by $\langle\gamma\rangle$. The nilpotency index of a finite chain ring is the smallest positive integer e such that $\gamma^e = 0$. All ideals of R can be expressed as

$$R = \langle\gamma^0\rangle \supseteq \langle\gamma^1\rangle \supseteq \cdots \supseteq \langle\gamma^{e-1}\rangle \supseteq \langle\gamma^e\rangle = 0.$$

Assume that the residue field $R/\langle\gamma\rangle$ is denoted by $\mathbb{F}_q$, where $q = p^m$, p is a prime number and m is

a positive integer. Consider $R^\times$ as the multiplicative group of units of R. There is an element ξ of $R^\times$ with multiplicative order $q-1$ such that every element of $x \in R$ can be written uniquely as

$$x = x_0 + x_1\gamma + x_2\gamma^2 + \cdots + x_{e-1}\gamma^{e-1},$$

where $x_i \in \mathcal{T}$ and $\mathcal{T} = \{0, 1, \xi, \ldots, \xi^{q-2}\}$ is the Teichmüller set of R. Clearly, $x \in R^\times$ if and only if $x_0 \neq 0$. So $|\langle\gamma^j\rangle| = q^{e-j}$ for some $j \in \{0, 1, \ldots, e-1\}$. Galois rings, especially $\mathbb{Z}_q$, and the quasi-Galois ring $\mathbb{F}_q[\gamma]/\langle\gamma^e\rangle$, are examples of chain rings.

A linear code of length n over R is an R-submodule of R^n. According to [14], any linear code C over R is permutation equivalent to a code with the following generator matrix

$$G = \begin{pmatrix} I_{k_0} & B_{0,1} & B_{0,2} & B_{0,3} & \ldots & B_{0,e-1} & B_{0,e} \\ 0 & \gamma_1 I_{k_1} & \gamma_1 B_{1,2} & \gamma_1 B_{1,3} & \ldots & \gamma_1 B_{1,e-1} & \gamma_1 B_{1,e} \\ 0 & 0 & \gamma_1^2 I_{k_2} & \gamma_1^2 B_{2,3} & \ldots & \gamma_1^2 B_{2,e-1} & \gamma_1^2 B_{2,e} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & \gamma_1^{e-1} I_{k_{e-1}} & \gamma_1^{e-1} B_{e-1,e} \end{pmatrix}.$$

Immediately, a code C with the given generator matrix has cardinality

$$|C| = q^{\sum_{i=0}^{e-1}(e-i)k_i}.$$

Recall that a free linear code over R is a free R-submodule. The code C is free if and only if $k_i = 0$ for all $i = 2, 3, \ldots, e-1$. Let $^-\colon R \to \mathbb{F}_q$ be the natural projection map, which can be extended naturally to a projection from R^n onto $\mathbb{F}_q^n$. We define $\overline{C} = \{\overline{x} | x \in C\}$. The Hamming distance between $x, y \in C$, denoted by $d(C)$ or simply d, is the number of coordinates in which x and y differ from one another. If C is a free linear code then $d(C) = d(\overline{C})$; see [14].

2.1. Gray map

The definition of the Gray map over chain rings used in this paper is based on the approach introduced in a recent paper [10], outlined as follows.

Let

$$\varepsilon = \xi_0(\varepsilon) + \xi_1(\varepsilon)p + \cdots + \xi_{m-1}(\varepsilon)p^{m-1}$$

be the p-adic representation of $\varepsilon \in \mathbb{Z}_{p^m}$, where $\xi_i(\varepsilon) \in \{0, 1, \ldots, p-1\}$ for all $i \in \{0, \ldots, m-1\}$. Let α be a fixed primitive element of $\mathbb{F}_{p^m}$. Corresponding to every ϵ, consider α_ε as

$$\alpha_\varepsilon = \xi_0(\varepsilon) + \xi_1(\varepsilon)\alpha + \cdots + \xi_{m-1}(\varepsilon)\alpha^{m-1}.$$

Moreover, let

$$w = \tilde{\xi}_0(w) + \tilde{\xi}_1(w)p^m + \cdots + \tilde{\xi}_{e-2}(w)p^{m(e-2)}$$

be the p-adic representation of $w \in Z_{p^{m(e-1)}}$, where $\tilde{\xi}_i(w) \in \{0, 1, \ldots, p^m - 1\}$. Now the Gray map $\phi : R \to \mathbb{F}_q^{q^{e-1}}$ is defined as

$$\phi(x) = (b_0, b_1, \ldots, b_{q^{e-1}-1})$$

for all $x = x_0 + x_1\gamma + \cdots + x_{e-1}\gamma^{e-1} \in R$, where

$$b_{wp^m+\varepsilon} = \alpha_\varepsilon \overline{x}_0 + \sum_{l=1}^{e-2} \alpha_{\tilde{\xi}_{l-1}(w)} \overline{x}_l + \overline{x}_{e-1} \tag{1}$$

for all $w \in \{0, \ldots, p^{m(e-1)} - 1\}$ and $\varepsilon \in \{0, \ldots, p^m - 1\}$.

Example 2.1.

1. *For $R = \mathbb{Z}_4$, the Gray map $\phi : R \to \mathbb{F}_2^2$ coincides with the classical Gray map $\phi(x_0 + 2x_1) = (x_1, x_0 + x_1)$.*
2. *For the quasi-Galois ring $R = \mathbb{F}_2[\gamma]/\langle\gamma^3\rangle$, the Gray map $\phi : R \to \mathbb{F}_2^4$ is $\phi(x_0 + x_1\gamma + x_2\gamma^2) = (x_2, x_0 + x_2, x_1 + x_2, x_0 + x_1 + x_2)$.*

The Gray map described above can be extended to $\mathbb{R}^n$ in a coordinate-wise manner. In [8], the homogeneous weight of an element $x \in R$, denoted by $w_{\text{hom}}(x)$, is defined as follows:

$$w_{\text{hom}}(x) = \begin{cases} q^{e-1} & x \in \gamma^{e-1}R\backslash\{0\}, \\ q^{e-2}(q-1) & x \in R\backslash\gamma^{e-1}R, \\ 0 & x = 0. \end{cases}$$

The homogeneous weight can naturally extend to $\mathbb{R}^n$ in a coordinate-wise manner. The homogeneous distance between two vectors x, y in R^n is defined by $w_{\text{hom}}(x - y)$. The minimum homogeneous distance of a code C, denoted by $d_{\text{hom}}(C)$ or simply d_{hom}, is the minimum value of $w_{\text{hom}}(x-y)$ for any two distinct $x, y \in C$. A code is called divisible if all its codewords have weights that are divisible by an integer $\delta > 1$. Clearly, codes over chain rings equipped with the homogeneous weight are divisible by $\delta = q^{e-2}$ for all $e \geqslant 3$.

Proposition 2.2. *[8] The Gray map ϕ is an isometry from (R^n, d_{hom}) to $(\mathbb{F}_q^{nq^{e-1}}, d)$, where d denotes the Hamming distance on $\mathbb{F}_q^{nq^{e-1}}$.*

2.2. 1^{st} order generalized Reed-Muller codes

Our description of 1^{st} order generalized Reed-Muller (1^{st} GRM) codes is based on [11]. Let α be a primitive element of $\mathbb{F}_{q^m}$, $m(q-1) > 1$ and $n = q^m - 1$. Let G' be the matrix

$$G' = \begin{pmatrix} a_{00} & a_{01} & a_{02} & \dots & a_{0,n-1} \\ a_{10} & a_{11} & a_{12} & \dots & a_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m-1,0} & a_{m-1,1} & a_{m-1,2} & \dots & a_{m-1,n-1} \end{pmatrix},$$

where $0 \leqslant j \leqslant q^{m-2}$, $a_{ij} \in \mathbb{F}_q$ and $\alpha^j = \sum_{i=0}^{m-1} a_{ij}\alpha^i$. The 1^{st} GRM (or extended 1^{st} GRM), denoted by $\mathcal{R}_q(1, m)$, has a generator matrix obtained from G' by adding a column of $0s$ and a row of $1s$. In fact, the generator matrix of $\mathcal{R}_q(1, m)$ can be viewed as a matrix with the following structure: the first row is all one vector and the other rows construct a matrix with all possible q-ary m-tuples as the columns. It is proved that the dimension of the code $\mathcal{R}_q(1, m)$ is $k = m + 1$ and the minimum Hamming distance is $d = q^{m-1}(q - 1)$. Moreover, the minimum distance of the dual code for the 1^{st} GRM code, denoted by $d^\perp$, is given by $d^\perp = (R + 1)q^Q$, where R is the remainder and Q the quotient from dividing 2 by $q - 1$; see [1, 11].

3. The Gray image of codes over chain rings

In this section, we study the properties of the Gray image of a linear code C over the chain ring R. In the following, $\mathcal{C}$ will always denote $\phi(C)$. Note that $\mathcal{C}$ is a divisible code of length nq^{e-1} over the alphabet $\mathbb{F}_q$. Let $\mathcal{C}^\perp$ denote the dual code of $\mathcal{C}$ concerning the standard inner product. We say $\mathcal{C}$ is self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^\perp$.
The next theorem gives an upper and lower bound on the minimum Hamming distance for $\mathcal{C}$.

Theorem 3.1. *Let C be a free linear code over R with the minimum Hamming distance $d(C)$. Then*

$$q^{e-2}(q-1)d(C) \leqslant d_{hom}(C) = d(\mathcal{C}) \leqslant q^{e-1}d(C).$$

Proof. Since $d(C) = d(\overline{C})$, there exists $x \in C$ such that $d(\overline{x}) = d(C)$. So x has exactly $d(C)$ unit coordinates, meaning $d(C)$ coordinates of $\gamma^{e-1}x \in C$ are in $\gamma^{e-1}R$ and the rest are zero. Therefore $w_{hom}(\gamma^{e-1}x) = q^{e-1}d(C)$, giving the upper bound. On the other hand, for every codeword $x \in C$ we have $d(\overline{x}) \geqslant d(\overline{C}) = d(C)$, which means x has at least $d(C)$ unit coordinates. Thus, the homogeneous weight of C is at least $d(C)q^{e-2}(q-1)$, giving the left-hand side inequality. □

Define the matrix A in such a way that the coefficients of $\overline{x}_0, \overline{x}_1, ..., \overline{x}_{e-1}$ in the definition of b_i in (1) form its i^{th} column, i.e.

$$A = \begin{pmatrix} \alpha_{\varepsilon_0} & \alpha_{\varepsilon_1} & \alpha_{\varepsilon_2} & \dots & \alpha_{\varepsilon_{q^{e-1}-1}} \\ \alpha_{\tilde{\xi}_0}(w_0) & \alpha_{\tilde{\xi}_0}(w_1) & \alpha_{\tilde{\xi}_0}(w_2) & \dots & \alpha_{\tilde{\xi}_0}(w_{q^{e-1}-1}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{\tilde{\xi}_{e-3}}(w_0) & \alpha_{\tilde{\xi}_{e-3}}(w_1) & \alpha_{\tilde{\xi}_{e-3}}(w_2) & \dots & \alpha_{\tilde{\xi}_{e-3}}(w_{q^{e-1}-1}) \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix}.$$

For example, if $R = \mathbb{F}_3[\gamma]/\langle\gamma^3\rangle$ is a quasi-Galois ring, then the matrix A is given by

$$A = \begin{pmatrix} 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

and if $R = \mathbb{F}_4[\gamma]/\langle\gamma^3\rangle$ is a quasi-Galois ring, then the matrix A is given by

$$A = \begin{pmatrix} 0 & 1 & \alpha & 1+\alpha & 0 & 1 & \alpha & 1+\alpha & 0 & 1 & \alpha & 1+\alpha & 0 & 1 & \alpha & 1+\alpha \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha & \alpha & \alpha & \alpha & 1+\alpha & 1+\alpha & 1+\alpha & 1+\alpha \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Let $e \geqslant 3$ in the case $q = 2$, $e \geqslant 2$ in the case $q = 3$, and e is arbitrary in other cases. In all cases, we have $m(q-1) > 1$, where $m = e-1$. From the definition of the 1^{st} GRM codes, it is evident that A is equivalent to the generator matrix of the code $\mathcal{R}_q(1, m)$. For $x = x_0 + x_1\gamma + \cdots + x_{e-1}\gamma^{e-1} \in R$, we have $\phi(x) = (\overline{x}_0, \overline{x}_1, ..., \overline{x}_{e-1})A$, which means $\phi(x)$ can be expressed as a linear combination of the rows A. Hence, the Gray image $\phi : R \to \mathbb{F}_q^{q^{e-1}}$ is the 1^{st} GRM in all cases.

Remark 3.2. *The map ϕ is not linear in general. For example, in the case of $R = \mathbb{Z}_{p^m}$, the assumption of linearity implies that*

$$0 = \overbrace{\phi(1) + \cdots + \phi(1)}^{p \text{ times}} = \phi(p) = (0, 1, 0, \dots, 0)A \neq 0,$$

which is a contradiction. However, it is clear that ϕ is linear over the quasi-Galois ring $R = \mathbb{F}_q[\gamma]/\langle\gamma^e\rangle$, which implies $\mathcal{C} = \phi(R)$ is always linear.

3.1. Self-orthogonal codes

Theorem 3.3. *Suppose that $R = \mathbb{F}_q[\gamma]/\langle\gamma^e\rangle$ is a quasi-Galois ring with one of the following conditions:*

1. *$q = 2$ and $e \geqslant 4$.*
2. *$q \geqslant 3$ and $e \geqslant 3$.*

Then $\mathcal{C} = \phi(R)$ is a self-orthogonal code with parameters $[q^{e-1}, e, q^{e-2}(q-1)]$.

Proof. The preceding discussion precisely gives the parameters of $\mathcal{C}$. Assume that $1 \leqslant i \leqslant e-1$ and A_i denotes the rows of A. It is easily seen that

- for all i such that $i \neq e-1$ we have $A_iA_i = \frac{q^{e-1}}{q}(\alpha_{\varepsilon_0}^2 + \alpha_{\varepsilon_1}^2 + \cdots + \alpha_{\varepsilon_{q-1}}^2)$,
- for all i, j such that $i \neq j$ and $i, j \neq e-1$ we have $A_iA_j = \frac{q^{e-1}}{q^2}(\alpha_{\varepsilon_0} + \alpha_{\varepsilon_1} + \cdots + \alpha_{\varepsilon_{q-1}})^2$,
- for all i, j such that $i \neq j$ and either $i = e-1$ or $j = e-1$ we have $A_iA_j = \frac{q^{e-1}}{q}(\alpha_{\varepsilon_0} + \alpha_{\varepsilon_1} + \cdots + \alpha_{\varepsilon_{q-1}})$,
- $A_{e-1}A_{e-1} = q^{e-1}$.

Hence, if one of the conditions (1) or (2) holds, we get $AA^t = 0$, where t denotes the transpose of the matrix A. Let $x = x_0 + x_1\gamma + \cdots + x_{e-1}\gamma^{e-1} \in R$. Then, for each $y = y_0 + y_1\gamma + \cdots + y_{e-1}\gamma^{e-1} \in R$ we have

$$\begin{aligned}\phi(x)\phi(y) &= ((\overline{x}_0, \ldots, \overline{x}_{e-1})A)((\overline{y}_0, \ldots, \overline{y}_{e-1})A)^t \\ &= (\overline{x}_0, \ldots, \overline{x}_{e-1})AA^t(\overline{y}_0, \ldots, \overline{y}_{e-1})^t \\ &= 0,\end{aligned}$$

implying that $\phi(x) \in (\phi(R))^{\perp}$. We have proved that $\mathcal{C} \subseteq \mathcal{C}^{\perp}$. □

Corollary 3.4. *Under the conditions of the previous theorem, $\mathcal{C} = \phi(R^n)$ is a self-orthogonal code with parameters $[nq^{e-1}, e, nq^{e-2}(q-1)]$.*

From now on, we denote the quasi-Galois ring $R = \mathbb{F}_q[\gamma]/\langle\gamma^e\rangle$ by $R_{\gamma,e,q}$ when q and e satisfy one of the following conditions:

1. $q = 2$ and $e \geqslant 4$.
2. $q \geqslant 3$ and $e \geqslant 3$.

Theorem 3.5. *Let the linear code C of length p over the quasi-Galois ring $R = R_{\gamma,e,q}$ be generated by vectors*

$$\{(1, 1, \ldots, 1), (0, \gamma^{e-1}, 2\gamma^{e-1}, \ldots, (p-1)\gamma^{e-1})\},$$

where $q = p^m$, p is a prime number and m is a positive integer. Then, $\mathcal{C} = \phi(C)$ is a self-orthogonal linear code with parameters $[pq^{e-1}, e+1, (p-1)q^{e-1}]$.

Proof. Every codeword of C has a homogeneous weight equal to either $pq^{e-2}(q-1)$ or $(p-1)q^{e-1}$. We have

$$pq^{e-2}(q-1) \geqslant p^{m(e-1)}(p-1) = q^{e-1}(p-1).$$

Now use Corollary 3.4. □

In the next two theorems, let C' be an arbitrary code over $\mathbb{F}_q$ with parameters $[n, k, d]$ and the generator matrix $[I_k|A]$. We aim to construct some self-orthogonal codes over $\mathbb{F}_q$ by using the existing code C'.

Theorem 3.6. *Let $R = R_{\gamma,e,q}$ be a quasi-Galois ring. If C is a linear code of length n over R generated by $[\gamma^{e-1}I_k|\gamma^{e-1}A]$, then $\mathcal{C} = \phi(C)$ is a self-orthogonal linear code with parameters $[q^{e-1}n, k, q^{e-1}d]$.*

Proof. All codewords of C have the homogeneous weight $q^{e-1}d$. Moreover, self-orthogonality follows from Theorem 3.3. □

Theorem 3.7. *Let $R = R_{\gamma,e,q}$ be a quasi-Galois ring. If C is a linear code generated by $[I_k|B]$ such that B is a matrix over $R\backslash\langle\gamma\rangle$ and $\overline{B} = A$, then $\mathcal{C} = \phi(C)$ is a self-orthogonal linear code with parameters $[q^{e-1}n, ke, q^{e-2}(q-1)d]$.*

Proof. Every codeword of C has the homogeneous weight equal to either $q^{e-2}(q-1)d$ or $q^{e-1}d$. Hence $d_{hom}(C) = q^{e-2}(q-1)d$. Moreover, self-orthogonality follows from Theorem 3.3. □

Example 3.8. *We applied the above theorems and corollary to present some optimal (see Marcus Grassl's table in [7]) self-orthogonal codes in Table 1. In Table I, $[I_k|A]$ is considered as an arbitrary $[n,k,d]$-linear code over $\mathbb{F}_q$ and C is the code constructed in Theorem 3.6. In Table II, C is the code constructed in Theorem 3.5. Finally, Table III arises from Corollary 3.4.*

Table 1. Optimal self-orthogonal linear codes

Table I			Table II		Table III		
R	$[I_k\|A]$	$\phi(C)$	R	$\phi(C)$	R	n	$\phi(R^n)$
$R_{\gamma,4,2}$	$[16,5,8]$	$[128,5,64]$	$R_{\gamma,8,2}$	$[256,9,128]$	$R_{\gamma,4,2}$	$1 \le n \le 6$	$[8n,4,4n]$
$R_{\gamma,5,2}$	$[3,2,2]$	$[48,2,32]$	$R_{\gamma,7,2}$	$[128,8,64]$	$R_{\gamma,5,2}$	$1 \le n \le 6$	$[16n,5,8n]$
$R_{\gamma,6,2}$	$[7,3,4]$	$[224,3,128]$	$R_{\gamma,3,3}$	$[27,4,18]$	$R_{\gamma,6,2}$	$1 \le n \le 8$	$[32n,6,16n]$
$R_{\gamma,3,3}$	$[3,2,2]$	$[27,2,18]$	$R_{\gamma,4,3}$	$[81,5,54]$	$R_{\gamma,3,3}$	$1 \le n \le 6$	$[9n,3,6n]$
$R_{\gamma,4,3}$	$[4,2,3]$	$[108,2,81]$	$R_{\gamma,5,3}$	$[243,6,81]$	$R_{\gamma,4,3}$	$1 \le n \le 9$	$[27n,4,18n]$
$R_{\gamma,3,4}$	$[5,2,4]$	$[80,2,64]$	$R_{\gamma,3,5}$	$[125,4,100]$	$R_{\gamma,3,4}$	$1 \le n \le 8$	$[16n,3,12n]$

4. Quasi-twisted codes and their images

Denote the standard right shift operator on R^n by T. For a unit $\lambda \in R^\times$, the λ-shift operator T_λ on R^n is defined as $T_\lambda(a_0,\dots,a_{n-1}) = (\lambda a_{n-1}, a_0, a_1, \dots, a_{n-2})$. Recall that a linear code C of length n over R is called cyclic if $T(C) = C$, and λ-constacyclic if $T_\lambda(C) = C$. Suppose that $n = ml$. A linear code C of length n over R is called l-quasi-cyclic (l-QC) if $T^l(C) = C$, and (λ, l)-quasi-twisted ((λ,l)-QT) if $T_\lambda^l(C) = C$. Obviously QT-codes can be considered as a generalization of all cyclic, constacyclic and QC codes.

Remark 4.1. *Suppose that ϕ is the Gray map from R^n to $\mathbb{F}_q^{q^{e-1}}$ and $\lambda \in R^\times$. Then ϕ has the following properties:*

1. $\phi \circ T = T^{q^{e-1}} \circ \phi$.
2. $\phi \circ T_\lambda \cong T_\lambda^{q^{e-1}} \circ \phi$, *where $\cong$ denotes permutation equivalence.*

Proof. Using the definitions yields the part (1)(similar to subsection 4.1 in [19]). It is well-known that the unit element λ can be expressed as $\lambda = \lambda_0 + \lambda_1\gamma$, where $\lambda_0, \lambda_1 \in \mathbb{F}_q$ and $\lambda_0 \neq 0$. Hence, $a \in \gamma^{e-1}R\backslash\{0\}$ if and only if $\lambda a \in \gamma^{e-1}R\backslash\{0\}$, meaning $w_{\hom}(a) = w_{\hom}(\lambda a)$. Therefore, for any element $a = (a_0,\dots,a_{n-1}) \in R^n$, $\phi(\lambda a)$ is permutation equivalent to $\phi(a)$. So, we have $\phi \circ T_\lambda \cong T_\lambda^{q^{e-1}} \circ \phi$. □

Applying Lemma 4.1, the following theorem is straightforward.

Theorem 4.2.

1. *If C is a cyclic code of length n over R, then $\phi(C)$ is a q^{e-1}-QC code of length $q^{e-1}n$.*
2. *If C is a l-QC code of length n over R, then $\phi(C)$ is a $q^{e-1}l$-QC code of length $q^{e-1}n$.*
3. *If C is a λ-constacyclic code of length n over R, then $\phi(C)$ is equivalent to a q^{e-1}-QC code of length $q^{e-1}n$.*
4. *If C is a (λ, l)-QT code of length n over R, then $\phi(C)$ is equivalent to a $q^{e-1}l$-QC code of length $q^{e-1}n$.*

4.1. One-generator QT codes

By the correspondence between vectors in R^m and polynomials of degree m, it is well-known that a cyclic code of length m over R can be considered as an ideal in $R_m = R[x]/\langle x^m - 1\rangle$, a λ-constacyclic code of length m as an ideal in $R_{m,\lambda} = R[x]/\langle x^m - \lambda\rangle$, an l-QC code of length $n = ml$ as an R_m-submodule in R_m^l, and finally, a (λ, l)-QT code of length $n = ml$ as an $R_{m,\lambda}$-submodule in $R_{m,\lambda}^l$. We know that R_m and $R_{m,\lambda}$ are both principal ideal rings. Therefore, any λ-constacylic code (and any cyclic code as a particular case) is generated by a polynomial, namely $a(x) = a_0 + a_1x + \ldots + a_{m-1}x^{m-1} \in R_{m,\lambda}$, and has a generator matrix in the following form

$$G = \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & a_{m-1} \\ \lambda a_{m-1} & a_0 & a_1 & \ldots & a_{m-2} \\ \lambda a_{m-2} & \lambda a_{m-1} & a_0 & \ldots & a_{m-3} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ \lambda a_1 & \lambda a_2 & \lambda a_3 & \ldots & a_0 \end{pmatrix}.$$

In some contexts, this matrix is called λ-twistulant or λ-circulant. Generally,, R_m^l and $R_{m,\lambda}^l$ are not principal ideal rings. This complicates the study of QT-codes (and QC codes as particular cases), prompting most literature to focus on a special case, namely the one-generator QT codes. A QT code C is called one-generator if it is generated by a single element $\underline{a}(x) = (a^{(1)}(x), \ldots, a^{(l)}(x)) \in R_{m,\lambda}^l$ as an $R_{m,\lambda}$-submodule of $R_{m,\lambda}^l$, i.e.,

$$C = \langle \underline{a}(x)\rangle = \{(a^{(1)}(x)g(x), \ldots, a^{(l)}(x)g(x)) \,|\, g(x) \in R_{m,\lambda}\}.$$

As a result, the generator matrix of C is in the form $[G_1|G_2|\ldots G_l]$, where each G_i is an λ-twistulant matrix of size $m \times m$ related to the polynomial $a^{(i)}(x)$.

The following theorem, which has a cyclic version in [15], can be easily obtained.

Theorem 4.3. *Let $C = \langle g(x)\rangle$ be a λ-constacyclic code of length m over the chain ring R, where $g(x)$ is a monic polynomial with $\deg g(x) = m - k$. Then C is a free code of rank k if and only if $g(x)|x^m - \lambda$.*

By Theorem 4.3, the following theorem can be proven similarly to Theorem 4.12 in [19].

Theorem 4.4. *Suppose that C is a one-generator QT-code generated by the polynomial $\underline{a}(x) = (a^{(1)}(x)g(x), \ldots, a^{(l)}(x)g(x))$, where $g(x)$ is a monic polynomial in $R_{m,\lambda}$ such that $x^m - \lambda = g(x)h(x)$ for some monic polynomial $h(x)$ in $R_{m,\lambda}$, and $a^{(i)}(x)$ is relatively prime to $h(x)$ for all $i = 1, \ldots, l$. Then C is a free code of rank $m - \deg g(x)$ and $\phi(C)$ is of rank $e(m - \deg g(x))$.*

By Theorem 3.1, the following theorem can be proven similarly to Corollary 4.14. in [19].

Theorem 4.5. *Let C be a (λ, l)-QT code of length $n = ml$ over the chain ring R with a generator $\underline{a}(x) = (a^{(1)}(x), \ldots, a^{(l)}(x))$. If the number of unit coefficients of $a^{(i)}(x)$ is d_i for $i = 1, \ldots, l$, then $d_{hom}(C) \leqslant q^{e-1}(d_1 + \cdots + d_l)$.*

5. Griesmer codes

Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ with the parameters $[n, k, d]$. The Griesmer bound, a lower bound on the length, is defined as $n \geqslant \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$, where $\lceil x \rceil$ denotes the ceiling function, i.e., the smallest integer greater than or equal to x. Linear codes meeting this bound are called Griesmer codes.

Theorem 5.1. *Suppose that R is a quasi-Galois ring and $g(x) = 1 + x + x^2 + \cdots + x^{m-1} \in R_{m,\lambda}$. Let C be a one-generator QT-code of length $n = ml$ generated by $\underline{a}(x) = (g(x), \ldots, g(x))$. Then*

1. *$\phi(C)$ is a $q^{e-1}l$-QC code with parameters $[q^{e-1}n, e, q^{e-2}(q-1)n]$.*
2. *For all $n < q$, $\phi(C)$ is a Griesmer code.*

Proof. We have $x^m - 1 = (x-1)g(x)$. Then, by Theorem 4.4, the dimension of $\phi(C)$ is e. Since C is the repetition code of length n, the minimum distance of $\phi(C)$ can be computed easily, which completes the proof of the statement (1). To prove the statement (2), note that if $n < q$, we have $\lceil \frac{q-1}{q} n \rceil = n$. So

$$\begin{aligned}\left\lceil \frac{q^{e-2}(q-1)n}{q^0} \right\rceil + \cdots + \left\lceil \frac{q^{e-2}(q-1)n}{q^{e-1}} \right\rceil &= (q-1)n(q^{e-2} + q^{e-3} + \cdots + q + 1) + \left\lceil \frac{q-1}{q} n \right\rceil \\ &= (q-1)n\left(\frac{1-q^{e-1}}{1-q}\right) + n \\ &= q^{e-1}n,\end{aligned}$$

and hence $\phi(C)$ meets the Griesmer bound (note that if $n \geqslant q$, then there are q, r such that $n = kq + r$, and so $\lceil \frac{q-1}{q} n \rceil = n - k$, and hence we do not have Griesmer code). □

Corollary 5.2. *Suppose that $R = R_{\gamma,e,q}$ and $g(x) = 1 + x + x^2 + \cdots + x^{m-1} \in R_{m,\lambda}$. Let C be a one-generator QT-code of length $n = ml$ generated by $\underline{a}(x) = (g(x), \ldots, g(x))$. If $n < q$, then $\phi(C)$ is a self-orthogonal Griesmer $q^{e-1}l$-QC code with parameters $[q^{e-1}n, e, q^{e-2}(q-1)n]$.*

Example 5.3. *All codes in Table 2 are self-orthogonal Geriesmer $q^{e-1}l$-QC codes, arising from Corollary 5.2. The code labelled with $*$ appears in Chen's table; see [4].*

Table 2. **Self-orthogonal Geriesmer $q^{e-1}l$-QC codes**

	$q=2,e=4$	$q=3,e=3$	$q=3,e=4$	$q=4,e=3$	$q=4,e=4$	$q=5,e=3$	$q=7,e=3$
$[n,k,d]$	$[8n,4,4n]$	$[9n,3,6n]$	$[27n,4,18n]$	$[16n,3,12n]$	$[64n,4,48n]$	$[25n,3,20n]$	$[49n,3,42n]$
$n=1$	$[8,4,4]$	$[9,3,6]$	$[27,4,18]$	$[16,3,12]$	$[64,4,48]$	$[25,3,20]$	$[49,3,42]$
$n=2$		$[18,3,12]$	$[54,4,36]$	$[32,3,24]$	$[128,4,96]$	$[50,3,40]$	$[98,3,84]$
$n=3$				$[48,3,36]^*$	$[192,4,144]$	$[75,3,60]$	$[147,3,126]$
$n=4$						$[100,3,80]$	$[196,3,168]$
$n=5$							$[245,3,210]$
$n=6$							$[294,3,252]$

Theorem 5.4. *Let $q = p$ and C be the linear code over $R = R_{\gamma,e,q}$ constructed in Theorem 3.5. Then $\phi(C)$ is a self-orthogonal Griesmer code with parameters $[q^e, e+1, (q-1)q^{e-1}]$.*

Proof. We have

$$\left\lceil \frac{(q-1)q^{e-1}}{q^0} \right\rceil + \cdots + \left\lceil \frac{(q-1)q^{e-1}}{q^e} \right\rceil = (q-1)(q^{e-1} + q^{e-2} + \cdots + q + 1) + \left\lceil \frac{q-1}{q} \right\rceil$$
$$= (q-1)\left(\frac{1-q^e}{1-q}\right) + 1$$
$$= q^e,$$

which gives the result. □

Example 5.5. *Self-orthogonal Geriesmer codes in Table 3 are constructed by Theorem 5.4.*

Table 3. Self-orthogonal Geriesmer codes

q/e	3	4	5
2		$[16, 5, 8]$	$[32, 6, 16]$
3	$[27, 4, 18]$	$[81, 5, 54]$	$[243, 6, 162]$
5	$[125, 4, 100]$	$[625, 5, 500]$	

6. Quantum codes

Let $\mathbb{C}^q$ be a q-dimensional vector space, representing the state of a quantum mechanical system. A q-ary quantum error-correcting code of length n and dimension k is a k-dimensional subspace of the n-fold tensor product $\mathbb{C}^q \otimes \ldots \otimes \mathbb{C}^q$. It is called an $[[n, k, d]]$-linear code if $d = 2t + 1$, where t is the maximum number of errors that the code can correct. For more information about quantum error-correcting codes, readers may refer to [12].

Theorem 6.1. (*CSS Construction; see [2, 17]*) *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two linear codes over the field $\mathbb{F}_q$ with parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$, respectively, such that $\mathcal{C}_2 \subseteq \mathcal{C}_1$. Then, there exists a quantum code with parameters $[[n, k_1 - k_2, \min\{d_1, d_2^{\perp}\}]]$, where $d_2^{\perp}$ denotes the Hamming distance of the dual code $\mathcal{C}_2^{\perp}$.*

Corollary 6.2. *Let $\mathcal{C}$ be a self-orthogonal $[n, k, d]$-linear code over the field $\mathbb{F}_q$. Then, there exists a quantum error-correcting code with parameters $[[n, n - 2k, d^{\perp}]]$, where $d^{\perp}$ denotes the Hamming distance of $\mathcal{C}^{\perp}$.*

Theorem 6.3. *There exists a family of quantum error-correcting codes with parameters $[[q^{e-1}, q^{e-1} - 2e, d^{\perp}]]$, where $d^{\perp} = 4$ in the case $q = 2$ and $d^{\perp} = 3$ in the case $q \geqslant 3$.*

Proof. If $R = R_{\gamma,e,q}$, then according to Theorem 3.3, the codes $\mathcal{C} = \phi(R)$ is self-orthogonal with parameters $[q^{e-1}, e, q^{e-2}(q-1)]$. On the other hand, $\mathcal{C}$ is a 1^{th} GRM code. So $d^{\perp} = (R+1)q^Q$, where $2 = (q-1)Q + R$ and $0 \leqslant R < q - 1$. Then, $d^{\perp} = 4$ in the case $q = 2$ and $d^{\perp} = 3$ in the case $q \geqslant 3$. Now we apply Corollary 6.2. □

Theorem 6.4. *If $n \geqslant 2$, then there exists a family of quantum error-correcting codes with parameters $[[q^{e-1}n, q^{e-1}n - 2e, 2]]$.*

Proof. If $R = R_{\gamma,e,q}$, then according to Corollary 3.4, $\mathcal{C} = \phi(R^n)$ is a self-orthogonal code with parameters $[nq^{e-1}, e, nq^{e-2}(q-1)]$. Assume that $d^{\perp} = 1$. Without loss of generality, there exists $0 \neq x = (x_0, 0, \ldots, 0) \in \phi(R^n)^{\perp}$ with the Hamming weight 1. On the other hand, $y = (1, 1, \ldots, 1) \in \phi(R^n)$ because $(0, 0, \ldots, 1) \in R^n$. Therefore, $0 = x \cdot y = x_0$, which is a contradiction. So $d^{\perp} \geqslant 2$. Now, let $d^{\perp} \geqslant 3$. Applying the sphere-packing bound on $\phi(R^n)^{\perp}$, we obtain $1 + q^{e-1}n(q-1) \leqslant q^e$. This implies $\frac{1}{q^{e-1}} + q \leqslant 2$, which is impossible with $q \geqslant 2$, $e \geqslant 2$ and $n \geqslant 2$. Therefore $d^{\perp} = 2$. Now, we apply Corollary 6.2. □

Example 6.5. *In Table 4 some examples of quantum codes with minimum distances* $2, 3$ *and* 4 *are presented. In Table I, quantum codes are constructed by Theorem 6.3 and in Table II, by Theorem 6.4.*

Table 4. Some quantum codes from our constructions

Table I			Table II			
R	$\phi(R)$	$[[n,k,d]]$	R	n	$\phi(R^n)$	$[[n,k,d]]$
$R_{\gamma,3,7}$	$[49,3,42]$	$[[49,43,3]]$	$R_{\gamma,3,3}$	3	$[27,3,18]$	$[[27,21,2]]$
$R_{\gamma,4,3}$	$[27,4,18]$	$[[27,19,3]]$	$R_{\gamma,3,5}$	2	$[50,3,40]$	$[50,44,2]$
$R_{\gamma,4,4}$	$[64,4,48]$	$[[64,56,3]]$	$R_{\gamma,3,7}$	2	$[98,3,84]$	$[[98,92,2]]$
$R_{\gamma,4,2}$	$[8,4,4]$	$[[8,0,4]]$	$R_{\gamma,4,3}$	2	$[54,4,36]$	$[[54,46,2]]$
$R_{\gamma,5,2}$	$[16,5,8]$	$[[16,6,4]]$	$R_{\gamma,3,4}$	2	$[32,3,24]$	$[[32,26,2]]$
$R_{\gamma,6,2}$	$[32,6,16]$	$[[32,20,4]]$	$R_{\gamma,4,2}$	2	$[16,4,8]$	$[[16,8,2]]$

7. Conclusion

In this paper, we have focused on the study of the Gray image ϕ (introduced by Jitman; see [10]) of codes over chain rings and its applications. We have presented a new interpretation of this Gray image associated with 1^{st} order generalized Reed-Muller codes. We have proved that the Gray image $\phi(R)$, where R is a chain ring satisfying in Theorem 3.3, is a self-orthogonal linear code. As a result, we have found a class of self-orthogonal linear codes over $\mathbb{F}_q$ with rather simple constructions. We have described the Gray image of quasi-twisted codes over chain rings. Then, we have constructed self-orthogonal Geriesmer quasi-cyclic codes as the Gray image of special quasi-twisted codes. Finally, we have derived some quantum codes by the CSS construction.

References

[1] E. F. Assmus, J. D. Key, Polynomial codes and finite geometries, Handbook of coding theory, (1998) 2(part 2) 1269–1343.

[2] A. R. Calderbank, P. W. Shor, Good quantum error-correcting codes exist, Physical Review A 54(2) (1996) 1098–1105.

[3] C. Carlet, $\mathbb{Z}_{2^k}$-linear codes, IEEE Transactions on Information Theory 44(4) (1998) 1543–1547.

[4] E. Z. Chen, Online database of Quasi-Twisted Codes, available online at `http://databases.cs.hkr.se/qtcodes/searchqc2.php?`

[5] I. Constantinescu, W. Heise, A metric for codes over residue class rings, Problemy Peredachi Informatsii 33(3) (1997) 22–28.

[6] M. Greferath, M. E. OâĂŹSullivan, On bounds for codes over Frobenius rings under homogeneous weights, Discrete Mathematics 289(1-3) (2004) 11-24.

[7] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, (2007), Online available at `http://www.codetables.de/`.

[8] M. Greferath, S. E. Schmidt, Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code, IEEE Transactions on Information Theory 45(7) (1999) 2522–2524.

[9] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Transactions on Information Theory 40(2) (1994) 301–319.

[10] S. Jitman, P. Udomkavanich, The Gray image of codes over finite chain rings, International Journal of Contemporary Mathematical Sciences 5(10) (2010) 449–458.
[11] T. Kasami, S. Lin, W. Peterson, New generalizations of the Reed-Muller codes part I: primitive codes. IEEE Transactions on Information Theory 14(2) (1968) 189–199.
[12] D. A. Lidar, T. A. Brun (Eds.), Quantum error correction, Cambridge University Press (2013).
[13] S. Ling, J. T. Blackford, $\mathbb{Z}_{(p^{k+1})}$-linear codes, IEEE Transactions on Information Theory 48(9) (2002) 2592–2605.
[14] G. Norton, A. Sălăgean, On the Hamming distance of linear codes over a finite chain ring, IEEE Transactions on Information Theory 46(3) (2000) 1060–1067.
[15] G. Norton, A. Sălăgean, On the structure of linear and cyclic codes over a finite chain ring, AAECC 10 (2000) 489–506.
[16] P. W. Shor, Scheme for reducing decoherence in quantum computer memory. Physical Review A 52(4) (1995) R2493–R2496.
[17] A. Steane, Multiple-particle interference and quantum error correction, Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences 452(1954) (1996) 2551–2577.
[18] A. M. Steane, Simple quantum error-correcting codes. Physical Review A 54(6) (1996) 4741.
[19] B. Yildiz, I. G. Kelebek, The homogeneous weight for R_k, related Gray map and new binary quasi-cyclic codes, Filomat 31(4) (2017) 885–897.