Cryptography and Communications (2022) 14:1117–1143
https://doi.org/10.1007/s12095-022-00579-2

On the construction of self-dual cyclic codes over $\mathbb{Z}_4$ with arbitrary even length

Yuan Cao[1,2] · Yonglin Cao[1] · San Ling[3] · Guidong Wang[1]

Received: 8 December 2021 / Accepted: 27 March 2022 / Published online: 21 April 2022

Abstract
Self-dual codes over the ring $\mathbb{Z}_4$ are related to combinatorial designs and unimodular lattices. First, we discuss briefly how to construct self-dual cyclic codes over $\mathbb{Z}_4$ of arbitrary even length. Then we focus on solving one key problem of this subject: for any positive integers k and m such that m is even, we give a direct and effective method to construct all distinct Hermitian self-dual cyclic codes of length 2^k over the Galois ring GR(4,m). This then allows us to provide explicit expressions to accurately represent all these Hermitian self-dual cyclic codes in terms of binomial coefficients. In particular, several numerical examples are presented to illustrate our applications.

Keywords Hermitian self-dual code · Cyclic code · Galois ring · Kronecker product of matrices · Binomial coefficient

Mathematics Subject Classification (2010) 94B15 · 94B05 · 11T71

✉ Yonglin Cao
ylcao@sdut.edu.cn

Yuan Cao
yuancao@sdut.edu.cn

San Ling
lingsan@ntu.edu.sg

Guidong Wang
hbuwgd@163.com

[1] School of Mathematics and Statistics, Shandong University of Technology, Zibo, Shandong 255091, China

[2] Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China

[3] School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Republic of Singapore

1 Introduction

The class of self-dual codes is closely related to other fields of mathematics, such as lattices, cryptography, invariant theory, block designs, etc. In particular, self-dual codes over $\mathbb{Z}_4$ are related to combinatorial designs and unimodular lattices (cf. [2, 6, 8, 23, 25–28]). The construction of self-dual codes over $\mathbb{Z}_4$ is an interesting topic in coding theory.

In general, the construction of optimal self-dual codes requires computer searches. To reduce the search field, self-dual codes can be constructed from linear codes with some special algebraic structures, such as cyclic codes, constacyclic codes and quasi-cyclic codes, etc.

The study of cyclic codes over finite rings started to attract much attention in the 1990s, when it was observed that some good nonlinear codes over $\mathbb{F}_2$ can be viewed as binary images of linear cyclic codes over $\mathbb{Z}_4$ under a Gray map [24]. In particular, [24] motivated the study of cyclic and negacyclic codes over Galois rings (see, for example, [1, 3–5, 15, 30, 35, 40, 44, 47, 48]). Using the Gray map from $\mathbb{Z}_4$ onto $\mathbb{F}_2^2$, defined by: $0\mapsto 00$, $1\mapsto 01$, $2\mapsto 11$, $3\mapsto 10$, binary formally self-dual codes can be obtained from self-dual codes over $\mathbb{Z}_4$ with good parameters. The construction of self-dual codes over $\mathbb{Z}_4$ and other rings has since become a research topic of much interest (cf. [31, 34, 36, 43]).

Cyclic codes were initially studied where their length is relatively prime to the characteristic of the ring. The structure of this class of cyclic codes over rings was studied in [7, 15, 35, 39, 40] and certain special generating sets for these codes were determined therein. Cyclic codes (resp. negacyclic codes) whose length is not relatively prime to the characteristic of the ring are called repeated-root cyclic codes (resp. negacyclic codes). The first study for this latter class of cyclic codes was done in [1], where the generators for cyclic codes over $\mathbb{Z}_4$ of length 2^e were determined. Then the generators for cyclic codes over $\mathbb{Z}_4$ of length $2n$ were presented in [4], where n is odd. Repeated-root cyclic and negacyclic codes are also interesting as they allow very simple syndrome-forming and decoding circuitry and, in some cases (see [38, 41]), they are maximum distance separable. A partial list of references for the theory of repeated-root cyclic codes includes [14, 16–21, 32, 33, 37, 41, 42, 45, 49].

Another important reason for studying cyclic codes over $\mathbb{Z}_4$ of even length is that there are more self-dual codes among them than there are among cyclic codes over $\mathbb{Z}_4$ of odd length. For example: the numbers of self-dual cyclic codes over $\mathbb{Z}_4$ of length 23, 22 and 20 are equal to 3, 33 and 63, respectively; the numbers of self-dual cyclic codes over $\mathbb{Z}_4$ of length 25, 26 and 28 are equal to 1, 65 and 339, respectively. In fact, some good binary self-dual codes or formally self-dual codes can be obtained from self-dual cyclic codes over $\mathbb{Z}_4$ of even length. Here is a simple example: there is only one binary self-dual cyclic code of length 8 and its basic parameters are [8,4,2]. However, there are 3 self-dual cyclic codes over $\mathbb{Z}_4$ of length 4, and two of them give binary self-dual codes having optimal parameters [8,4,4] by the Gray map defined above.

Now, we briefly review some main results on the determination of self-dual cyclic codes of even length over $\mathbb{Z}_4$ in the literature. A concatenated structure and an explicit representation for all distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$ and $4n$ were given by [9, 10], for any positive odd integer n. For length $2^k n$, where $k \geq 3$, using the methods in [9, 10] will result in complex representations.

Let $k,n \geq 3$ be any integers such that n is odd. Using the standard Discrete Fourier Transform decomposition, which may be viewed as an extension of the approaches in [4] and [21], and by [22, Theorem 3.2 and Corollary 3.3] and [29, Lemma 4.3 and Proposition

4.5], the problem of determining all (Euclidean) self-dual cyclic codes of length $2^k n$ over $\mathbb{Z}_4$ can be translated into solving the following three problems (see Section 2 of this paper for details):

(♭) Determining all cyclic codes and their Euclidean dual codes of length 2^k over a Galois extension ring of $\mathbb{Z}_4$, say GR(4,m), where $m \geq 1$.
(♮) Constructing and expressing explicitly all Euclidean self-dual cyclic codes of length 2^k over GR(4,m).
(♯) Constructing and expressing explicitly all Hermitian self-dual cyclic codes of length 2^k over GR(4,m), where m is an even positive integer.

So far, several results on the three problems have been obtained:

For Problem (♭): All cyclic codes and their Euclidean dual codes over GR(4,m) of length 2^k have been determined by [22, Lemma 2.4 (iv), Proposition 2.5 and Theorem 5.3] and [32, 33].
For Problem (♮): The number of Euclidean self-dual cyclic codes over GR(4,m) of length 2^k was determined by [33, Corollary 3.5]. Then explicit expressions for all distinct Euclidean self-dual cyclic codes over GR(4,m) of length 2^k were given in [11], using binomial coefficients.
For Problem (♯): The number $N_{\mathrm{H}}\big(\mathrm{GR}(4,m),2^k\big)$ of all Hermitian self-dual cyclic codes over GR(4,m) of length 2^k was determined by [29, Theorem 3.4]: $N_{\mathrm{H}}\big(\mathrm{GR}(4,m),2^k\big) = \frac{\left(2^{\frac{m}{2}}\right)^{2^{k-1}+1}-1}{2^{\frac{m}{2}}-1}$, where m is even.
However, to the best of our knowledge, there are no general results on the construction and explicit representation of all distinct Hermitian self-dual cyclic codes over GR(4,m) *of length* 2^k.

In order to represent explicitly all Euclidean self-dual cyclic codes of length $2^k n$ over $\mathbb{Z}_4$, we need to solve Problem (♯) completely. This is the main contribution of this current work.

The paper is organised as follows. In Section 2, we discuss briefly how to construct Euclidean self-dual cyclic codes over $\mathbb{Z}_4$ of length $2^k n$, for any positive odd integer n. In Section 3, we introduce necessary notation for the Galois ring GR(4,m) and Hermitian dual codes over GR(4,m). In Section 4, we give a direct and effective approach to construct precisely all distinct Hermitian self-dual cyclic codes over GR(4,m) of length 2^k by Theorem 1. This then allows us to provide an explicit expression to accurately represent all these Hermitian self-dual cyclic codes by Theorem 2, using binomial coefficients. In Section 5, we prove Theorem 1 in detail. As an application, we give explicitly all distinct Hermitian self-dual cyclic codes of length 2^k over GR(4,m), for the cases of $k = 3,4,5$, in Section 6. Section 7 concludes the paper.

2 Constructing self-dual cyclic codes over $\mathbb{Z}_4$ of length $2^k n$

In this section, we describe how to construct all distinct Euclidean self-dual cyclic codes over $\mathbb{Z}_4$ of length $2^k n$, where n is an odd positive integer.

As in [22] and [29, Section 4], define the ring $\mathcal{R} = \frac{\mathbb{Z}_4[u]}{\langle u^{2^k}-1\rangle}$. Then we have a $\mathbb{Z}_4$-module isomorphism $\Phi : \mathcal{R}^n \to \frac{\mathbb{Z}_4[x]}{\langle x^{2^k n}-1\rangle}$ defined by: for any $c_i(u) = \sum_{j=0}^{2^k-1} c_{i,j}u^j \in \mathcal{R}$ with $c_{i,j} \in \mathbb{Z}_4$, $i = 0,1,\ldots,n-1$, let

$$\Phi(c_0(u), c_1(u), \ldots, c_{n-1}(u)) = \sum_{i=0}^{n-1}\sum_{j=0}^{2^k-1} c_{i,j}x^{i+jn}.$$

Let M be the the multiplicative order of 2 modulo n and let ζ be a primitive n th root of unity in the Galois ring GR(4,M). We define the Discrete Fourier Transform of

$$c(x) = \sum_{i=0}^{n-1}\sum_{j=0}^{2^k-1} c_{i,j}x^{i+jn} \in \frac{\mathbb{Z}_4[x]}{\langle x^{2^k n}-1\rangle}$$

as the vector $(\widehat{c}_0, \widehat{c}_1, \ldots, \widehat{c}_{n-1}) \in \left(\frac{\mathrm{GR}(4,M)[u]}{\langle u^{2^k}-1\rangle}\right)^n$ with

$$\widehat{c}_h = \sum_{i=0}^{n-1}\sum_{j=0}^{2^k-1} c_{i,j}\zeta^{hi}u^{n'i+j},\ 0 \le h \le n-1,$$

where $nn' \equiv 1 \pmod{2^k}$, and define the Mattson-Solomon polynomial of $c(Z)$ to be $\widehat{c}(Z) = \sum_{h=0}^{n-1}\widehat{c}_{n-h \pmod n}Z^h$. By [22, Lemma 3.1] or [29, Lemma 4.1], we have the following

$$c(x) = \Phi\Big(\big(1, u^{-n'}, u^{-2n'}, \ldots, u^{-(n-1)n'}\big) \star \frac{1}{n}\big(\widehat{c}(1), \widehat{c}(\zeta), \ldots, \widehat{c}\big(\zeta^{n-1}\big)\big)\Big),$$

where $\star$ indicates the componentwise multiplication.

For any integer h, $0 \le h \le n-1$, denote by $S_2(h)$ the 2-cyclotomic coset modulo n containing h, i.e., $S_2(h) = \{h2^i \pmod n | i = 0,1,\ldots\}$. The 2-cyclotomic coset $S_2(h)$ is said to be self-inverse if $S_2(-h) = S_2(h)$. Set $J_0 = I_0 = \{0\}$. Let I_1 be the union of all self-inverse 2-cyclotomic cosets modulo n excluding I_0 and set $I_2 = \{0,1,\ldots,n-1\} \setminus (I_0 \cup I_1)$. The set I_2 is the union of pairs of 2-cyclotomic cosets of the form $S_2(h) \cup S_2(-h)$, where $h \notin I_0 \cup I_1$. Let J_1 and J_2 be complete sets of representatives of 2-cyclotomic cosets in I_1 and I_2, respectively. Without loss of generality, we assume that J_2 is chosen such that $h \in J_2$ if and only if $n - h \in J_2$. For any $h \in J_0 \cup J_1 \cup J_2$, denote by m_h the size of $S_2(h)$. Then m_h is even for all $h \in J_1$.

By [22, Theorem 3.2 and Corollary 3.3] or [29, Lemma 4.3], we know that $\frac{\mathbb{Z}_4[x]}{\langle x^{2^k n}-1\rangle} \cong \prod_{h\in J_0\cup J_1\cup J_2} \frac{\mathrm{GR}(4,m_h)[x]}{\langle x^{2^k}-1\rangle}$ via the following ring isomorphism

$$c(x) \mapsto (\widehat{c}_h)_{h\in J_0\cup J_1\cup J_2}.$$

Then every Euclidean self-dual cyclic code $\mathcal{C}$ over $\mathbb{Z}_4$ of length $2^k n$ can be constructed as follows (cf. [29, Proposition 4.5]):

$$\mathcal{C} \cong C_0 \times \prod_{j\in J_1} C_j \times \prod_{h\in J_2} C_h,$$

where

- C_0 is a Euclidean self-dual cyclic code over $\mathbb{Z}_4$ of length 2^k,

$\diamondsuit$ C_j is a Hermitian self-dual cyclic code of length 2^k over the Galois ring GR(4,m_j) for all $j \in J_1$,
$\diamondsuit$ C_h is a cyclic code of length 2^k over the Galois ring GR(4,m_h) and $C_{n-h} = C_h^{\perp_E}$, where $C_h^{\perp_E}$ is the Euclidean dual of C_h, for all $h \in J_2$.

In the following sections, we focus on the problem of constructing Hermitian self-dual cyclic code of length 2^k over the Galois ring GR(4,m).

3 Preliminaries

In this section, we introduce the notation needed in the following sections.

Let $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ in which the arithmetic is done modulo 4, and let $\mathbb{Z}_2 = \{0, 1\}$ in which the arithmetic is done modulo 2. In this paper, we regard $\mathbb{Z}_2$ as a subset of $\mathbb{Z}_4$, although $\mathbb{Z}_2$ is not a subfield of the ring $\mathbb{Z}_4$. In that sense, we have that $2\mathbb{Z}_2 = \{0, 2\} \subseteq \mathbb{Z}_4$, and each element a in $\mathbb{Z}_4$ has a unique 2-adic expansion: $a = b_0 + 2b_1$, where $b_0, b_1 \in \mathbb{Z}_2$.

Define $\overline{a} = b_0 = a \pmod 2$, and let $\overline{a}(z) = \sum_{i=0}^{d} \overline{a}_i z^i \in \mathbb{Z}_2[z]$, for any $a(z) = \sum_{i=0}^{d} a_i z^i \in \mathbb{Z}_4[z]$. Then the map $^-$ is a surjective homomorphism of rings from $\mathbb{Z}_4[z]$ onto $\mathbb{Z}_2[z]$. A monic polynomial $a(z)$ in $\mathbb{Z}_4[z]$ of positive degree is said to be *basic irreducible* if $\overline{a}(z)$ is an irreducible polynomial in $\mathbb{Z}_2[z]$. From now on, we adopt the following notation:

Let m be an arbitrary even positive integer, set $q = 2^{\frac{m}{2}}$ and let $\varsigma(z)$ be a fixed monic basic irreducible polynomial in $\mathbb{Z}_4[z]$ of degree m.
Let $R = \frac{\mathbb{Z}_4[z]}{\langle \varsigma(z) \rangle} = \{\sum_{i=0}^{m-1} a_i z^i \mid a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}_4\}$ in which the arithmetic is done modulo $\varsigma(z)$. Then R is a Galois ring of characteristic 4 and $4^m = q^4$ elements, i.e., $R =$ GR(4,m) (cf. [46, Theorem 14.1]).
Let $\mathbb{F}_{q^2} = \mathbb{F}_{2^m} = \frac{\mathbb{Z}_2[z]}{\langle \overline{\varsigma}(z) \rangle} = \left\{ \sum_{i=0}^{m-1} b_i z^i \mid b_0, b_1, \ldots, b_{m-1} \in \mathbb{Z}_2 \right\}$ in which the arithmetic is done modulo $\overline{\varsigma}(z)$. Then $\mathbb{F}_{q^2}$ is a finite field of q^2 elements.
Let $\mathbb{F}_q = \{\xi \in \mathbb{F}_{q^2} \mid \xi^q = \xi\} \subseteq \mathbb{F}_{q^2}$. Then $\mathbb{F}_q$ is the unique subfield of $\mathbb{F}_{q^2}$ with q elements (cf. [46, Theorem 6.18]). In particular, $\mathbb{F}_2 = \mathbb{Z}_2$.

As we have regarded $\mathbb{Z}_2$ as a subset of $\mathbb{Z}_4$, we will regard $\mathbb{F}_{q^2}$ as a subset of R in the natural way, though $\mathbb{F}_{q^2}$ is not a subfield of R. In this sense, we have $2 \cdot 1 = 2 \in R$, where $2 \in \mathbb{Z}_4 \subseteq R$ and $1 \in \mathbb{Z}_2 \subseteq \mathbb{F}_{q^2}$.
Let $\alpha = \sum_{i=0}^{m-1} a_i z^i \in R$, where $a_i = b_{i0} + 2b_{i1} \in \mathbb{Z}_4$ with $b_{i0}, b_{i1} \in \mathbb{Z}_2$, for all $i = 0,1,\ldots,m-1$. Then α can be uniquely expressed as: $\alpha = \beta_0 + 2\beta_1$, where $\beta_j = \sum_{i=0}^{m-1} b_{ij} z^i \in \mathbb{F}_{q^2}$ for $j = 0, 1$. Define

$$\overline{\alpha} = \beta_0 = \sum_{i=0}^{m-1} \overline{a}_i z^i, \ \forall \alpha \in R.$$

Then the map $^-$ is a surjective homomorphism of rings from R onto $\mathbb{F}_{q^2}$ with the following kernel:

$$2R = 2\mathbb{F}_{q^2} = \left\{2\beta \mid \beta \in \mathbb{F}_{q^2}\right\} \subset R \text{ and } |2R| = |\mathbb{F}_{q^2}| = q^2. \tag{1}$$

Here, we emphasize that $\mathbb{F}_{q^2}$ is only regarded as a subset of R, but $\mathbb{F}_{q^2}$ is not a subfield of R. Then we have $\mathbb{F}_{q^2} = \overline{R} = \{\overline{\alpha} \mid \alpha \in R\}$.

As $2^m = q^2$ and R is a Galois ring of characteristic 4 and 4^m elements, by [46, Theorem 14.8], we can choose a fixed invertible element ζ of R with multiplicative order $q^2 - 1$. From now on, we let

$$\mathcal{T} = \{0\} \cup \left\{\zeta^i \mid i = 0, 1, \ldots, q^2 - 2 = 2^m - 2\right\}.$$

By [46, Theorem 14.8]), each element α of R has a unique 2-adic expansion: $\alpha = t_0 + 2t_1$, where $t_0, t_1 \in \mathcal{T}$. This implies $\overline{R} = \overline{\mathcal{T}}$, $2R = 2\mathcal{T}$ and $|2R| = |\mathcal{T}| = q^2$. Then by (1), we have $\overline{\mathcal{T}} = \mathbb{F}_{q^2}$ and $2\mathcal{T} = 2\mathbb{F}_{q^2}$. Moreover, we let

$$\mathcal{T}_0 = \{0\} \cup \left\{ \left(\zeta^{q+1}\right)^i \mid i = 0, 1, \ldots, q - 2 = 2^{\frac{m}{2}} - 2 \right\} \subseteq \mathcal{T}.$$

As the multiplicative order of ζ^{q+1} is $\frac{q^2-1}{q+1} = q - 1$, we see that $|\mathcal{T}_0| = q$ and $\mathcal{T}_0 = \{\xi \in \mathcal{T} \mid \xi^q = \xi\}$. Hence the subset R_0 of R, defined by

$$R_0 = \left\{t_0 + 2t_1 \mid t_0, t_1 \in \mathcal{T}_0\right\},$$

is the unique Galois subring of R with $q^2 = 4^{\frac{m}{2}}$ elements. Therefore, R is a Galois extension ring of R_0 with degree 2. Moreover, by $\overline{\mathcal{T}} = \mathbb{F}_{q^2}$ we have

$$\overline{\mathcal{T}}_0 = \left\{\overline{\xi} \mid \overline{\xi}^q = \overline{\xi},\ \overline{\xi} \in \overline{\mathcal{T}} = \mathbb{F}_{q^2}\right\} = \mathbb{F}_q,$$

where $\mathbb{F}_q$ is the subfield of $\mathbb{F}_{q^2}$ with q elements. From now on, we define the map $\phi : R \to R$ by

$$\phi(t_0 + 2t_1) = t_0^q + 2t_1^q \ (\forall t_0, t_1 \in \mathcal{T}).$$

By [46, Theorem 14.30], we know that ϕ is the *generalized Frobenius automorphism* of R over R_0 with multiplicative order 2 satisfying

$$\phi(a) = a,\ \forall a \in R_0.$$

Especially, by $\mathbb{F}_q = \overline{\mathcal{T}}_0 \subset \overline{\mathcal{T}}$, it follows that $c^q = c$ for all $c \in \mathbb{F}_q$.

Now, let $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ be the trace function from $\mathbb{F}_{q^2}$ onto $\mathbb{F}_q$ defined by:

$$\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q \ \left(\forall \alpha \in \mathbb{F}_{q^2}\right),$$

and set $\mathrm{Tr}^{-1}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(c) = \left\{\alpha \in \mathbb{F}_{q^2} \mid \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = c\right\}$ for any $c \in \mathbb{F}_q$. Then for any $\alpha \in \mathbb{F}_{q^2}$, we know that $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = 0$ if and only if $\alpha \in \mathbb{F}_q$. This implies $\mathrm{Tr}^{-1}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(0) = \mathbb{F}_q$. Moreover, for any element $c \in \mathbb{F}_q$, we have $|\mathrm{Tr}^{-1}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(c)| = q$ (cf. [46, Corollary 7.17]).

The following lemma is one of the key results for this paper.

Lemma 1 Using the notation above, let w be a fixed element of the finite field $\mathbb{F}_{q^2}$ satisfying $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(w) = 1$, i.e., $w + w^q = 1$. Then

(i) $\mathbb{F}_{q^2} = \{a + bw \mid a, b \in \mathbb{F}_q\}$.
(ii) For any $a, b \in \mathbb{F}_q$, we have $(a + bw)^q = (a + b) + bw$.

(iii) Let $c \in \mathbb{F}_{q^2}$. We regard $2c$ as an element of the Galois ring R. Then we have $\phi(2 \cdot c) = 2 \cdot c^q$. In particular, we have that $\phi(2 \cdot c) = 2 \cdot c$ if $c \in \mathbb{F}_q$.

Proof (i) By $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(w) = 1$, we see that $w \notin \mathbb{F}_q$. Since $\mathbb{F}_{q^2}$ is an $\mathbb{F}_q$-linear space of dimension 2, the set $\{1,w\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^2}$. Therefore, $\mathbb{F}_{q^2} = \{a + bw \mid a, b \in \mathbb{F}_q\}$.

(ii) By $w + w^q = 1$, we have $w^q = 1 + w$. As $q = 2^{\frac{m}{2}}$ and $a, b \in \mathbb{F}_q$, we have $a^q = a$ and $b^q = b$. Therefore, in the finite field $\mathbb{F}_{q^2}$, we have $(a + bw)^q = a^q + b^q w^q = a + b(1 + w) = (a + b) + bw$.

(iii) As we regard $\mathbb{F}_{q^2}$ as a subset of the Galois ring R, the element $c \in \mathbb{F}_{q^2}$ has a unique 2-adic expansion $c = t_0 + 2t_1$, where $t_0, t_1 \in \mathcal{T}$. This implies $2c = 2t_0$. From this and by the definition of ϕ, we deduce that $\phi(2c) = 2t_0^q$.

On the other hand, by $c = t_0 + 2t_1$ and $4 = 0$ in $\mathbb{Z}_4 \subset R$, we have $c^2 = t_0^2 + 4(t_0 t_1 + t_2^2) = t_0^2$. From this and by $q = 2^{\frac{m}{2}}$, we obtain $c^q = t_0^q$.

As stated above, we conclude that $\phi(2c) = 2t_0^q = 2c^q$. □

At the end of this section, we emphasize that the element w and the subset $\mathbb{F}_q$ of the Galois ring GR(4,m) play important roles in the construction and representation of Hermitian self-dual cyclic codes of length 2^k over GR(4,m). Specifically, the element w and subset $\mathbb{F}_q$ can be constructed as follows:

1. Choose a monic basic irreducible polynomial $\varsigma(z)$ in $\mathbb{Z}_4[z]$ of degree m, say $\varsigma(z) = \sum_{i=0}^{m-1} \varsigma_i z^i + z^m$, where $\varsigma_i \in \mathbb{Z}_4$ for all $i = 0,1,\ldots,m-1$.
Then $\overline{\varsigma}(z) = \sum_{i=0}^{m-1} \overline{\varsigma}_i z^i + z^m$ is an irreducible polynomial in $\mathbb{Z}_2[z]$.
2. Set the Galois ring $R = \mathrm{GR}(4, m) = \{\sum_{i=0}^{m-1} a_i z^i \mid a_i \in \mathbb{Z}_4,\ i = 0, 1, \ldots,\ m-1\}$ in which $z^m = -\sum_{i=0}^{m-1} \varsigma_i z^i = 3\sum_{i=0}^{m-1} \varsigma_i z^i$.
Set the finite field $\mathbb{F}_{q^2} = \{\sum_{i=0}^{m-1} b_i z^i \mid b_i \in \mathbb{Z}_2,\ i = 0, 1, \ldots, m-1\}$ in which $z^m = \sum_{i=0}^{m-1} \overline{\varsigma}_i z^i$.
3. Choose a primitive element ζ of the finite field $\mathbb{F}_{q^2}$. Then ζ^{q+1} is a primitive element of the subfield $\mathbb{F}_q \subset \mathbb{F}_{q^2}$. Hence

$$\mathbb{F}_q = \{0\} \cup \left\{\zeta^{l(q+1)} \mid l = 0, 1, \ldots, q-2\right\} \pmod{\overline{\varsigma}(z)}.$$

4. Select a fixed $w \in \mathbb{F}_{q^2}$ such that $w + w^q \equiv 1 \pmod{\overline{\varsigma}(z)}$ in $\mathbb{Z}_2[z]$. Then

$$\mathbb{F}_{q^2} = \{\alpha + w\beta \mid \alpha, \beta \in \mathbb{F}_q\} \pmod{\overline{\varsigma}(z)}$$

and $R = \{\xi + 2\eta \mid \xi, \eta \in \mathbb{F}_{q^2}\}$. Here we regard $\mathbb{F}_{q^2}$ as a subset of R.

Finally, we give two examples to describe the above constructions:

Example 1 Let $m = 2$. Then $q = 2$. Choose $\varsigma(z) = z^2 + z + 1$. Therefore,

- $R = \mathrm{GR}(4, 2) = \{a_0 + a_1 z \mid a_0, a_1 \in \mathbb{Z}_4\}$ in which $z^2 = 3 + 3z$.
  $\mathbb{F}_4 = \{b_0 + b_1 z \mid b_0, b_1 \in \mathbb{Z}_2\} = \{0, 1, z, 1 + z\}$ in which $z^2 = 1 + z$.
- $\zeta = z$ is a primitive element of $\mathbb{F}_4$. Then $\zeta^{q+1} = z^3 = 1$ is a primitive element of $\mathbb{F}_2$. Hence $\mathbb{F}_2 = \{0, 1\}$.
- Let $w = z$. Then $w^2 + w \equiv 1 \pmod{z^2 + z + 1}$ in $\mathbb{Z}_2[z]$. Hence $\mathbb{F}_4 = \{\alpha + z\beta \mid \alpha, \beta \in \mathbb{F}_2\}$.

Example 2 Let $m = 4$. Then $q = 4$. Choose $\varsigma(z) = z^4 + z^3 + 1$. We have the following:

- $R = \mathrm{GR}(4,4) = \{a_0 + a_1 z + a_2 z^2 + a_3 z^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Z}_4\}$ in which $z^4 = 3 + 3z^3$.
  $\mathbb{F}_{16} = \{b_0 + b_1 z + b_2 z^2 + b_3 z^3 \mid b_0, b_1, b_2, b_3 \in \mathbb{Z}_2\}$ in which $z^4 = 1 + z^3$.
- $\zeta = 1 + z + z^2$ is a primitive element of the finite field $\mathbb{F}_{16}$.
  $\zeta^{q+1} = (1 + z + z^2)^5 = 1 + z + z^3$ is a primitive element of $\mathbb{F}_4$. Hence $\mathbb{F}_4 = \{0, 1, \zeta^{q+1}, (\zeta^{q+1})^2\} \pmod{z^4 + z^3 + 1}$, i.e.,

$$\mathbb{F}_4 = \left\{0, 1, 1 + z + z^3, z + z^3\right\}.$$

- Let $w = z^2 + z^3$. Then $w^2 + w \equiv 1 \pmod{z^4 + z^3 + 1}$ in $\mathbb{Z}_2[z]$. Hence

$$\mathbb{F}_{16} = \left\{\alpha + \left(z^2 + z^3\right)\beta \mid \alpha, \beta \in \mathbb{F}_4\right\}.$$

4 Hermitian self-dual cyclic codes of length 2^k over GR(4,*m*)

In this section, we give an explicit representation for every Hermitian self-dual cyclic code over GR(4,*m*) of length 2^k. To do this, we first review necessary concepts and facts for Euclidean and Hermitian self-dual codes.

Using the notation of Section 2, let k be any fixed positive integer and assume $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{2^k-1}), \beta = (\beta_0, \beta_1, \ldots, \beta_{2^k-1}) \in R^{2^k}$. We let $\phi(\beta) = (\phi(\beta_0), \phi(\beta_1), \ldots, \phi(\beta_{2^k-1}))$. Recall that the *Euclidean inner product* $[\alpha,\beta]_E$ and the *Hermitian inner product* $[\alpha,\beta]_H$ of α and β are defined by

$$[\alpha, \beta]_E = \sum_{i=0}^{2^k-1} \alpha_i \beta_i \in R \text{ and } [\alpha, \beta]_H = \sum_{i=0}^{2^k-1} \alpha_i \cdot \phi(\beta_i) = [\alpha, \phi(\beta)]_E,$$

respectively. Then both $[-,-]_E$ and $[-,-]_H$ are nondegenerate bilinear quadratic forms on R^{2^k}.

Let $\mathcal{C}$ be a linear code over R of length 2^k. Then the *Euclidean dual code* $\mathcal{C}^{\perp_E}$ and the *Hermitian dual code* $\mathcal{C}^{\perp_H}$ of $\mathcal{C}$ are defined by

$$\mathcal{C}^{\perp_E} = \left\{\beta \in R^{2^k} \mid [\alpha, \beta]_E = 0, \ \forall \alpha \in \mathcal{C}\right\}$$

and

$$\mathcal{C}^{\perp_H} = \left\{\beta \in R^{2^k} \mid [\alpha, \beta]_H = 0, \ \forall \alpha \in \mathcal{C}\right\},$$

respectively. Both $\mathcal{C}^{\perp_E}$ and $\mathcal{C}^{\perp_H}$ are also linear codes over R of length 2^k. As R is a Galois ring, we have $|\mathcal{C}||\mathcal{C}^{\perp_H}| = |\mathcal{C}||\mathcal{C}^{\perp_E}| = |R|^{2^k}$, and so $|\mathcal{C}^{\perp_H}| = |\mathcal{C}^{\perp_E}|$.

In particular, $\mathcal{C}$ is said to be *Hermitian self-dual* (resp. *Euclidean self-dual*) if $\mathcal{C}^{\perp_H} = \mathcal{C}$ (resp. $\mathcal{C}^{\perp_E} = \mathcal{C}$). It is well known that the number of codewords in each Hermitian (Euclidean) self-dual code over the Galois ring R of length 2^k is equal to $\left(|R|^{2^k}\right)^{\frac{1}{2}} = \left((4^m)^{2^k}\right)^{\frac{1}{2}} = (2^m)^{2^k} = (q^2)^{2^k}$.

In this paper, we write $\phi(\mathcal{C}) = \{\phi(\alpha) \mid \alpha \in \mathcal{C}\} \subseteq R^{2^k}$. As ϕ is a ring automorphism on R of multiplicative order 2, by the definition of inner products $[-,-]_E$ and $[-,-]_H$, we conclude that

$$|\phi(\mathcal{C}^{\perp_H})| = |\mathcal{C}^{\perp_H}| = |\mathcal{C}^{\perp_E}| \text{ and } [\mathcal{C}, \phi(\mathcal{C}^{\perp_H})]_E = [\mathcal{C}, \mathcal{C}^{\perp_H}]_H = \{0\}.$$

The latter implies $\phi(\mathcal{C}^{\perp_H}) \subseteq \mathcal{C}^{\perp_E}$, and hence $\phi(\mathcal{C}^{\perp_H}) = \mathcal{C}^{\perp_E}$. Therefore,

$$\mathcal{C}^{\perp_H} = \mathcal{C} \Longleftrightarrow \phi(\mathcal{C}) = \phi(\mathcal{C}^{\perp_H}) \Longleftrightarrow \phi(\mathcal{C}) = \mathcal{C}^{\perp_E}. \tag{2}$$

Next, we review the notation and some known results for Kronecker products of matrices of specific types. These are key to the constructions in this paper. In the following, set $q = 2^{\frac{m}{2}}$ and let the field $\mathbb{F}_q$ be the same as that defined in Section 2.

Let $A = (a_{ij})$ and B be matrices over $\mathbb{F}_q$ of sizes $s \times t$ and $l \times v$ respectively. We denote by A^{tr} the transpose of A. Recall that the *Kronecker product* of A and B is defined by $A \otimes B = (a_{ij}B)$, which is a matrix over $\mathbb{F}_q$ of size $sl \times tv$. Then we define

$$G_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ G_{2^\lambda} = G_2 \otimes G_{2^{\lambda-1}} = \begin{pmatrix} G_{2^{\lambda-1}} & 0 \\ G_{2^{\lambda-1}} & G_{2^{\lambda-1}} \end{pmatrix} \text{ for all } \lambda \geq 2. \tag{3}$$

For any integers l and s, where $1 \leq l \leq 2^\lambda$ and $1 \leq s \leq 2^{\lambda-1}$, we denote by I_l the identity matrix of order l and adopt the following notation:

- Let G_l be the submatrix of size $l \times l$ in the upper left corner of G_{2^λ} and define $M_l = I_l + G_l$, i.e.,

$$\begin{pmatrix} G_l & 0 \\ * & * \end{pmatrix} = G_{2^\lambda} \text{ and } \begin{pmatrix} M_l & 0 \\ * & * \end{pmatrix} = I_{2^\lambda} + G_{2^\lambda}. \tag{4}$$

  Then M_l is a matrix over $\mathbb{F}_2$ of size $l \times l$ and $M_{2^\lambda} = I_{2^\lambda} + G_{2^\lambda}$.
- We label the rows of the matrix M_l from top to bottom as: 0th row, 1st row, …, $(l-1)$st row; and label the columns of M_l from left to right as: 1st column, 2nd column, …, l th column.

  For $l = 2s-1$, we denote by $Y_j^{[0,2s-1)}$ the j th column vector of the matrix M_{2s-1}, for all $j = 1,2,\ldots,2s-1$. Then $Y_j^{[0,2s-1)} \in \mathbb{F}_2^{2s-1}$ and

$$M_{2s-1} = \left(Y_1^{[0,2s-1)}, Y_2^{[0,2s-1)}, \ldots, Y_{2s-1}^{[0,2s-1)}\right).$$

- For any vector $\alpha^{[0,2s-1)} \in \mathbb{F}_q^{2s-1}$, define its truncated vector $\alpha^{[s-1,2s-1)}$ by

$$\alpha^{[s-1,2s-1)} = \begin{pmatrix} g_{s-1} \\ g_s \\ \vdots \\ g_{2s-2} \end{pmatrix} \in \mathbb{F}_q^s, \text{ when } \alpha^{[0,2s-1)} = \left(\begin{array}{c} g_0 \\ \vdots \\ g_{s-2} \\ \hline g_{s-1} \\ \vdots \\ g_{2s-2} \end{array}\right). \tag{5}$$

- Let $\varepsilon_{2s-1}^{(2s-1)} = (0, \ldots, 0, 1)^{\text{tr}} \in \mathbb{F}_2^{2s-1}$.

The solution space of the homogeneous linear equations with coefficient matrix M_l is determined by the following lemma, when l is odd.

Lemma 2 (cf. [11, Theorem 1]) For any positive integer s, let $\mathcal{S}_{2s-1}$ be the solution space for the homogeneous linear equations over $\mathbb{F}_q$:

$$M_{2s-1}Y = \mathbf{0}, \text{ where } Y = (y_0, y_1, y_2, \dots, , y_{2s-2})^{\mathrm{tr}}.$$

Then we have the following conclusions:

(i) $\dim_{\mathbb{F}_q}(\mathcal{S}_{2s-1}) = s$ and the following s column vectors:

$$Y_1^{[0,2s-1)}, Y_3^{[0,2s-1)}, \dots, Y_{2s-3}^{[0,2s-1)}, \varepsilon_{2s-1}^{(2s-1)}$$

form a basis of the $\mathbb{F}_q$-linear space $\mathcal{S}_{2s-1}$.

(ii) $\mathcal{S}_{2s-1} = \left\{ \sum_{i=1}^{s-1} a_{2i-1} Y_{2i-1}^{[0,2s-1)} + a_{2s-2}\varepsilon_{2s-1}^{(2s-1)} \mid a_{2i-1} \in \mathbb{F}_q \text{ for all } 1 \le i \le s-1, \text{ and } a_{2s-2} \in \mathbb{F}_q \right\}$.

To determine Hermitian self-dual cyclic codes over GR(4,m) of length 2^k, the following conclusion plays an essential role.

Lemma 3 Using the notation above, we set

$$\mathcal{S}_{2s-1}^{[s-1]} = \left\{ (b_{s-1}, b_s, \dots, b_{2s-2})^{\mathrm{tr}} \mid (0, \dots, 0, b_{s-1}, b_s, \dots, b_{2s-2})^{\mathrm{tr}} \in \mathcal{S}_{2s-1} \right\}.$$

Then $\mathcal{S}_{2s-1}^{[s-1]}$ is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^s$. Moreover, we have that $\dim_{\mathbb{F}_q}\left(\mathcal{S}_{2s-1}^{[s-1]}\right) = \lceil \frac{s+1}{2} \rceil$ and an $\mathbb{F}_q$-basis of $\mathcal{S}_{2s-1}^{[s-1]}$ is given by:

$$\left\{ Y_{2i-1}^{[s-1,2s-1)} \mid \lfloor \frac{s+1}{2} \rfloor \le i \le s-1 \right\} \cup \left\{ \varepsilon_s^{(s)} = (0, \dots, 0, 1)^{\mathrm{tr}} \right\}.$$

Therefore, we have $|\mathcal{S}_{2s-1}^{[s-1]}| = q^{\lceil \frac{s+1}{2} \rceil}$ and

$$\mathcal{S}_{2s-1}^{[s-1]} = \left\{ \sum_{\lfloor \frac{s+1}{2} \rfloor \le i \le s-1} a_{2i-1} Y_{2i-1}^{[s-1,2s-1)} + a_{2s-2}\varepsilon_s^{(s)} \mid a_{2i-1}, a_{2s-2} \in \mathbb{F}_q, \lfloor \frac{s+1}{2} \rfloor \le i \le s-1 \right\}.$$

Proof By (3) and (4), we see that M_{2s-1} is a strictly lower triangle matrix and its column vectors $Y_1^{[0,2s-1)}, Y_2^{[0,2s-1)}, \dots, Y_{2s-1}^{[0,2s-1)}$ satisfy the following properties: $Y_{2s-1}^{[0,2s-1)} = \mathbf{0}_{2s-1}$, and

$$Y_{2i-1}^{[0,2s-1)} = \begin{pmatrix} \mathbf{0}_{2i-1} \\ 1 \\ * \\ * \\ \vdots \\ * \end{pmatrix}, \ Y_{2i}^{[0,2s-1)} = \begin{pmatrix} \mathbf{0}_{2i-1} \\ 0 \\ 0 \\ * \\ \vdots \\ * \end{pmatrix}, \ \forall i = 1, 2, \dots, s-1, \tag{6}$$

where $\mathbf{0}_t$ is the zero column vector of length t for any integer $t \ge 0$. Hence

$$Y_{2i-1}^{[0,2s-1)} = \begin{pmatrix} \mathbf{0}_{s-1} \\ Y_{2i-1}^{[s-1,2s-1)} \end{pmatrix}, \ \forall i : \left\lfloor \frac{s+1}{2} \right\rfloor \le i \le s-1.$$

From this and by Lemma 2 (i), we deduce that $\dim_{\mathbb{F}_q}\left(\mathcal{S}_{2s-1}^{[s-1]}\right) = \left\lceil \frac{s+1}{2} \right\rceil$, and $\mathcal{S}_{2s-1}^{[s-1]} = \left\{ \sum_{\lfloor \frac{s+1}{2} \rfloor \le i \le s-1} a_{2i-1} Y_{2i-1}^{[s-1,2s-1)} + a_{2s-2}\epsilon_s^{(s)} \mid a_{2i-1}, a_{2s-2} \in \mathbb{F}_q, \lfloor \frac{s+1}{2} \rfloor \le i \le s-1 \right\}$ by Lemma 2 (ii).

□

In this paper, cyclic codes of length 2^k over the Galois ring $R = \mathrm{GR}(4,m)$ are identified with ideals of the following ring

- $\frac{R[x]}{\langle x^{2^k}-1\rangle} = R[x]/\langle x^{2^k}-1\rangle = \left\{ \sum_{i=0}^{2^k-1} a_i x^i \mid a_0, a_1, \ldots, a_{2^k-1} \in R \right\}$ in which the arithmetic is done modulo the polynomial $x^{2^k}-1$,

under the identification map $\theta : R^{2^k} \to \frac{R[x]}{\langle x^{2^k}-1\rangle}$ defined by

$$\theta : (a_0, a_1, \ldots, a_{2^k-1}) \mapsto a_0 + a_1 x + \ldots + a_{2^k-1} x^{2^k-1}$$

for all $a_i \in R$ and $i = 0,1,\ldots,2^k-1$. Further, we set

- $\frac{\mathbb{F}_{q^2}[x]}{\langle x^{2^k}-1\rangle} = \mathbb{F}_{q^2}[x]/\langle x^{2^k}-1\rangle = \left\{ \sum_{i=0}^{2^k-1} b_i x^i \mid b_0, b_1, \ldots, b_{2^k-1} \in \mathbb{F}_{q^2} \right\}$ in which the arithmetic is done modulo $x^{2^k}-1$.

As we have regarded $\mathbb{F}_{q^2}$ as a subset of R, we will regard $\frac{\mathbb{F}_{q^2}[x]}{\langle x^{2^k}-1\rangle}$ as a subset of $\frac{R[x]}{\langle x^{2^k}-1\rangle}$ in the natural way, though $\frac{\mathbb{F}_{q^2}[x]}{\langle x^{2^k}-1\rangle}$ is not a subring of $\frac{R[x]}{\langle x^{2^k}-1\rangle}$. In that sense, each element ξ of $\frac{R[x]}{\langle x^{2^k}-1\rangle}$ has a unique 2-adic expansion:

$$\xi = \xi_0 + 2\xi_1, \text{ where } \xi_0, \xi_1 \in \mathbb{F}_{q^2}[x]/\langle x^{2^k}-1\rangle.$$

This implies $2 \cdot \frac{R[x]}{\langle x^{2^k}-1\rangle} = 2 \cdot \frac{\mathbb{F}_{q^2}[x]}{\langle x^{2^k}-1\rangle} = \left\{ 2\xi_0 \mid \xi_0 \in \frac{\mathbb{F}_{q^2}[x]}{\langle x^{2^k}-1\rangle} \right\} \subset \frac{R[x]}{\langle x^{2^k}-1\rangle}$. Here we only regard $\frac{\mathbb{F}_{q^2}[x]}{\langle x^{2^k}-1\rangle}$ as a subset of $\frac{R[x]}{\langle x^{2^k}-1\rangle}$.

For any polynomial $b(x) = \sum_{i=0}^{2^k-1} b_i x^i \in \frac{R[x]}{\langle x^{2^k}-1\rangle}$, where $b_i \in R$ for all i, we define $\phi(b(x)) = \sum_{i=0}^{2^k-1} \phi(b_i) x^i$. Then ϕ is an automorphism of multiplicative order 2 on the ring $\frac{R[x]}{\langle x^{2^k}-1\rangle}$. By Lemma 1 (iii), we have that

$$\phi(2b(x)) = 2b(x), \text{ if } b_i \in \mathbb{F}_q \text{ for all } i = 0, 1, \ldots, 2^k-1.$$

Let $\mathcal{C}$ be an ideal of the ring $\frac{R[x]}{\langle x^{2^k}-1\rangle}$. We set $\phi(\mathcal{C}) = \{\phi(b(x)) \mid b(x) \in \mathcal{C}\}$, which is an ideal of $\frac{R[x]}{\langle x^{2^k}-1\rangle}$ as well. Hence ϕ introduces a bijection $\mathcal{C} \mapsto \phi(\mathcal{C})$ on the set of ideals in $\frac{R[x]}{\langle x^{2^k}-1\rangle}$.

Let $f(x), g(x) \in \frac{R[x]}{\langle x^{2^k}-1\rangle}$. In this paper, we denote by $\langle f(x), g(x)\rangle$ the ideal of the ring $\frac{R[x]}{\langle x^{2^k}-1\rangle}$ generated by $f(x)$ and $g(x)$, i.e.,

$$\langle f(x), g(x)\rangle = \left\{ a(x)f(x) + b(x)g(x) \mid a(x), b(x) \in R[x]/\langle x^{2^k}-1\rangle \right\}.$$

Now, using the notation above and in Section 2, we determine all distinct Hermitian self-dual cyclic codes of length 2^k over the Galois ring $R = \mathrm{GR}(4,m)$ by the following theorem. Its detailed proof is given in Section 4.

Theorem 1 For any positive integer k, we have the following:

$\diamond$ If $k=1$, there are $1+2^{\frac{m}{2}}$ Hermitian self-dual cyclic codes of length 2 over R:

$$\langle 2\rangle,\ \langle (x-1)+2(b_0+w)\rangle \text{ where } b_0\in\mathbb{F}_q.$$

$\diamond$ If $k=2$, there are $1+2^{\frac{m}{2}}+2^m$ Hermitian self-dual cyclic codes of length 2^2 over R:
$\langle 2\rangle$;
$\langle (x-1)^3+2b_0, 2(x-1)\rangle$, where $b_0\in\mathbb{F}_q$;
$\langle (x-1)^2+2(b_0+w+b_1(x-1))\rangle$, where $b_0,b_1\in\mathbb{F}_q$.

$\diamond$ Let $k\geq 3$ and set $q=2^{\frac{m}{2}}$. Then all distinct Hermitian self-dual cyclic codes of length 2^k over R are given by the following four cases:

I. 1 code: $\langle 2\rangle$.
II. q codes: $\langle (x-1)^{2^{k-1}}+2b_0, 2(x-1)\rangle$ where $b_0\in\mathbb{F}_q$.
III. For every integer s, $2\leq s\leq 2^{k-1}-1$, there are q^s codes:

$$\langle (x-1)^{2^k-s}+2(x-1)^{(2^{k-1}-1)-s}+2b_s(x), 2(x-1)^s\rangle$$

in which $b_s(x)=\sum_{j=0}^{s-1}(b_{j,0}+wb_{j,1})(x-1)^j$ is determined by:

$$\begin{pmatrix} b_{0,1}\\ b_{1,1}\\ \vdots\\ b_{s-1,1}\end{pmatrix}=\sum_{\lceil\frac{s+1}{2}\rceil\leq t\leq s-1} c_{2t-1}Y_{2t-1}^{[s-1,2s-1)},$$

$$\begin{pmatrix} b_{0,0}\\ b_{1,0}\\ \vdots\\ b_{s-1,0}\end{pmatrix}=\begin{pmatrix} \widehat{c}_s\\ \widehat{c}_{s+1}\\ \vdots\\ \widehat{c}_{2s-1}\end{pmatrix}+\sum_{\lfloor\frac{s+1}{2}\rfloor\leq i\leq s-1} a_{2i-1}Y_{2i-1}^{[s-1,2s-1)}+a_{2s-2}\begin{pmatrix}0\\ \vdots\\ 0\\ 1\end{pmatrix},$$

where

$$\widehat{c}_j=\begin{cases} c_{2t-1}, & \text{if } j=2t-1 \text{ and } \lceil\frac{s+1}{2}\rceil\leq t\leq s-1;\\ 0, & \text{otherwise,}\end{cases}$$

and $c_{2t-1}, a_{2i-1}, a_{2s-2}\in\mathbb{F}_q$, for all integers t and i: $\lceil\frac{s+1}{2}\rceil\leq t\leq s-1$ and $\lfloor\frac{s+1}{2}\rfloor\leq i\leq s-1$.

IV. $q^{2^{k-1}}$ codes:

$$\langle (x-1)^{2^{k-1}}+2b(x)\rangle,$$

where

$$b(x)=(c_0+w)+\sum_{j=1}^{2^{k-2}-1}(a_j+c_j+a_jw)x^j+c_{2^{k-2}}x^{2^{k-2}}+\sum_{j=1}^{2^{k-2}-1}(c_j+a_jw)x^{2^{k-1}-j}$$

and $a_i, c_i, c_0, c_{2^{k-2}}\in\mathbb{F}_q$, for all $i=1,2,\ldots,2^{k-2}-1$.

Hence the number $N_{\mathrm{H}}(\mathrm{GR}(4,m),2^k)$ of all Hermitian self-dual cyclic codes of length 2^k over R is $N_{\mathrm{H}}(\mathrm{GR}(4,m),2^k)=\sum_{s=0}^{2^{k-1}}(2^{\frac{m}{2}})^s=\frac{(2^{\frac{m}{2}})^{2^{k-1}+1}-1}{2^{\frac{m}{2}}-1}$.

Remark 1

(i) The formula for the number of Hermitian self-dual cyclic codes of length 2^k over GR(4,m) has been given in [29, Theorem 3.4].
(ii) In Theorem 1, $b(x)$ is expressed as a polynomial in x in Case IV, while $b_s(x)$ is expressed as a polynomial in $x-1$ in case III.

Finally, we give an explicit expression for every Hermitian self-dual cyclic code of length 2^k over GR(4,m). For any integers K and t satisfying $1 \le t \le K$, let $\binom{K}{t}$ be the binomial coefficient defined by

$$\binom{K}{t} = \frac{K!}{(K-t)!\,t!} = \frac{K\cdot(K-1)\cdot\ldots\cdot(K-t+1)}{1\cdot 2\cdot\ldots\cdot t}.$$

Then by [13, Proposition 2], we have

$$G_{2^k} = \begin{pmatrix} g_{1,1}^{(2^k)} & g_{1,2}^{(2^k)} & \cdots & g_{1,2^k}^{(2^k)} \\ g_{2,1}^{(2^k)} & g_{2,2}^{(2^k)} & \cdots & g_{2,2^k}^{(2^k)} \\ \cdots & \cdots & \cdots & \cdots \\ g_{2^k,1}^{(2^k)} & g_{2^k,2}^{(2^k)} & \cdots & g_{2^k,2^k}^{(2^k)} \end{pmatrix} (\mathrm{mod}\ 2),$$

where

$$g_{i,j}^{(2^k)} = \binom{2^k-j}{i-j} \text{ if } i \ge j, \text{ and } \binom{2^k-j}{i-j} = 0 \text{ if } i < j. \tag{7}$$

From this, by (4) and (5), we have the following conclusion:

Theorem 2 For any integer $k \ge 3$, all distinct Hermitian self-dual cyclic codes of length 2^k over GR(4,m) are given by the following four cases:

I. 1 code: $\langle 2\rangle$.
II. q codes: $\langle (x-1)^{2^{k-1}} + 2b_0, 2(x-1)\rangle$, where $b_0 \in \mathbb{F}_q$.
III. For each integer s: $2 \le s \le 2^{k-1}-1$, there are q^s codes:

$$\langle (x-1)^{2^k-s} + 2(x-1)^{(2^{k-1}-1)-s} + 2b_s(x), 2(x-1)^s\rangle,$$

where

$$\begin{aligned} b_s(x) = & \sum_{\lfloor \frac{s+1}{2}\rfloor \le i \le s-1} \sum_{\nu=1}^{2(s-i)} a_{2i-1}\binom{2^k-2i+1}{\nu}(x-1)^{2i-1-s+\nu} \\ & + a_{2s-2}(x-1)^{s-1} + \sum_{\lceil \frac{s+1}{2}\rceil \le t \le s-1} c_{2t-1}(x-1)^{2t-1-s} \\ & + \sum_{\lceil \frac{s+1}{2}\rceil \le t \le s-1} \sum_{\nu=1}^{2(s-t)} c_{2t-1} w \binom{2^k-2t+1}{\nu}(x-1)^{2t-1-s+\nu} \end{aligned}$$

and $c_{2t-1}, a_{2i-1}, a_{2s-2} \in \mathbb{F}_q$, for all integers t and i satisfying

$$\left\lceil \frac{s+1}{2} \right\rceil \le t \le s-1 \text{ and } \left\lfloor \frac{s+1}{2} \right\rfloor \le i \le s-1.$$

IV. $q^{2^{k-1}}$ codes: $\langle (x-1)^{2^{k-1}} + 2b(x) \rangle$, where

$$b(x) = (c_0 + w) + \sum_{j=1}^{2^{k-2}-1} (a_j + c_j + a_j w)x^j + c_{2^{k-2}} x^{2^{k-2}} + \sum_{j=1}^{2^{k-2}-1} (c_j + a_j w)x^{2^{k-1}-j}$$

and $a_i, c_i, c_0, c_{2^{k-2}} \in \mathbb{F}_q$, for all $i = 1,2,\ldots,2^{k-2}-1$.

Proof Obviously, we only need to prove the conclusion in Case III. For any integer s, $2 \le s \le 2^{k-1}-1$, let $j \in \{i,t\}$, where $\lfloor \frac{s+1}{2} \rfloor \le i \le s-1$ and $\lceil \frac{s+1}{2} \rceil \le t \le s-1$. By the definition for the truncated vector $Y_{2j-1}^{[s-1,2s-1)}$ (see (5)) and (7), we have $Y_{2j-1}^{[s-1,2s-1)} = \begin{pmatrix} g_{s-1,2j-1} \\ g_{s,2j-1} \\ \vdots \\ g_{2s-2,2j-1} \end{pmatrix}$ in which $g_{s-1+\gamma,2j-1}$ satisfies the following conditions:

($\diamondsuit$) If $0 \le \gamma < 2j-1-s$, $g_{s-1+\gamma,2j-1} = \begin{pmatrix} 2^k-(2j-1) \\ s+\gamma-(2j-1) \end{pmatrix} = 0$.

($\diamondsuit$) If $\gamma = 2j-1-s$, $g_{s-1+\gamma,2j-1} = \begin{pmatrix} 2^k-(2j-1) \\ s+\gamma-(2j-1) \end{pmatrix} + 1 = 0$.

($\diamondsuit$) If $\gamma = 2j-1-s+\nu$, where $1 \le \nu \le 2(s-j)$,

$$g_{s-1+\gamma,2j-1} = \begin{pmatrix} 2^k-(2j-1) \\ \nu \end{pmatrix} = \begin{pmatrix} 2^k-2j+1 \\ \nu \end{pmatrix}.$$

From these and by Theorem 1, we deduce the conclusions in Case III directly. Here, we omit the trivial verification process.
□

5 Proof of Theorem 1

In this section, we prove Theorem 1. To save space, we will refer directly to some of the results in the literature later in this paper.

Lemma 4 (cf. [11, Lemma 1]) We have $(x-1)^{2^k} = 2(x-1)^{2^{k-1}}$ in $\frac{R[x]}{\langle x^{2^k}-1 \rangle}$.

Lemma 5 (cf. [11, Lemma 2]) Let s be an integer: $1 \le s \le 2^{k-1}$. For any vector $\underline{b} = (b_0, b_1, \ldots, b_{s-1})^{\mathrm{tr}} \in \mathbb{F}_{q^2}^s$, we set $b(x) = \sum_{j=0}^{s-1} b_j (x-1)^j$, and let $\mathcal{C}_{\underline{b}}$ be the ideal of $\frac{R[x]}{\langle x^{2^k}-1 \rangle}$ generated by $(x-1)^{2^k-s} + 2b(x)$ and $2(x-1)^s$, i.e.,

$$\mathcal{C}_{\underline{b}} = \langle (x-1)^{2^k-s} + 2b(x), 2(x-1)^s \rangle. \tag{8}$$

Then we have the following:

(i) The ideal $\mathcal{C}_{\underline{b}}$ is a cyclic code of length 2^k over R containing $(|R|^{2^k})^{\frac{1}{2}}$ codewords.
(ii) We have $\mathcal{C}_{\underline{b}} \ne \mathcal{C}_{\underline{c}}$, for any $\underline{b}, \underline{c} \in \mathbb{F}_{q^2}^s$ satisfying $\underline{b} \ne \underline{c}$.

As $x^{2^k}=1$ in the rings $\frac{R[x]}{\langle x^{2^k}-1\rangle}$ and $\frac{\mathbb{F}_{q^2}[x]}{\langle x^{2^k}-1\rangle}$, we have $x^{-l}=x^{2^k-l}$ for all integers l, $1\le l\le 2^k-1$. Here is the key conclusion for proving Theorem 1:

Lemma 6 Using the notation of Lemma 5, if $b(x)$ satisfies the following congruence relation in the ring $\mathbb{F}_{q^2}[x]$:

$$\phi(b(x))+x^{-s}b(x^{-1})\equiv(x-1)^{2^{k-1}-s}\ (\mathrm{mod}\ (x-1)^s), \tag{9}$$

where $\phi(b(x))=\sum_{j=0}^{s-1}b_j^q(x-1)^j\in\mathbb{F}_{q^2}[x]$, the code $\mathcal{C}_{\underline{b}}$ defined by (8) is a Hermitian self-dual cyclic code of length 2^k over R.

Proof Let $b(x)$ satisfy (9). By Lemma 5 (i), we know that $\mathcal{C}_{\underline{b}}$ is a cyclic code of length 2^k over R containing $(2^m)^{2^k}=(|R|^{2^k})^{\frac{1}{2}}$ codewords. Moreover, by Lemma 1 (iii) and $\phi(a)=a$ for all $a\in R_0$, it follows that

$$\begin{aligned}\phi(\mathcal{C}_{\underline{b}}) &= \langle\phi((x-1)^{2^k-s}+2b(x)),\phi(2(x-1)^s)\rangle\\ &= \langle(x-1)^{2^k-s}+2\phi(b(x)),2(x-1)^s\rangle.\end{aligned}$$

For any ideal $\mathcal{D}$ of the ring $\frac{R[x]}{\langle x^{2^k}-1\rangle}$, recall that the annihilator $\mathrm{Ann}(\mathcal{D})$ of $\mathcal{D}$ is defined by

$$\mathrm{Ann}(\mathcal{D})=\Big\{a(x)\in R[x]/\langle x^{2^k}-1\rangle\mid a(x)c(x)=0,\ \forall c(x)\in\mathcal{D}\Big\}.$$

Let $\chi:\frac{R[x]}{\langle x^{2^k}-1\rangle}\to\frac{R[x]}{\langle x^{2^k}-1\rangle}$ be the conjugate map defined by

$$\chi(a(x))=a(x^{-1})=a_0+\sum_{i=1}^{2^k-1}a_ix^{2^k-i},\ \forall a(x)=\sum_{i=0}^{2^k-1}a_ix^i\ \text{where}\ a_i\in R.$$

Then it is well known that (cf. [32, Theorem 4.1])

$$\mathcal{C}_{\underline{b}}^{\perp_E}=\chi(\mathrm{Ann}(\mathcal{C}_{\underline{b}}))=\Big\{\chi(a(x))\mid a(x)\in\mathrm{Ann}(\mathcal{C}_{\underline{b}})\Big\}.$$

Since $b(x)$ satisfies (9), there exists $g(x)\in\frac{\mathbb{F}_{q^2}[x]}{\langle x^{2^k}-1\rangle}$ such that

$$x^{-s}b(x^{-1})=\phi(b(x))+(x-1)^{2^{k-1}-s}+g(x)(x-1)^s.$$

This implies $2x^{-s}b(x^{-1})=2(\phi(b(x))+(x-1)^{2^{k-1}-s})+g(x)\cdot 2(x-1)^s$ in $\frac{R[x]}{\langle x^{2^k}-1\rangle}$. As x is invertible in $\frac{R[x]}{\langle x^{2^k}-1\rangle}$, by $-2=2$ in $\mathbb{Z}_4\subset R$, it follows that

$$\begin{aligned}\chi(\mathcal{C}_{\underline{b}}) &= \langle\chi((x-1)^{2^k-s}+2b(x)),\chi(2(x-1)^s)\rangle\\ &= \langle(x^{-1}-1)^{2^k-s}+2b(x^{-1}),2(x^{-1}-1)^s\rangle\\ &= \langle(-1)^{2^k-s}x^{-(2^k-s)}(x-1)^{2^k-s}+2b(x^{-1}),2x^{-s}(x-1)^s\rangle\\ &= \langle(x-1)^{2^k-s}+2x^{-s}b(x^{-1}),2(x-1)^s\rangle\\ &= \langle(x-1)^{2^k-s}+2(\phi(b(x))+(x-1)^{2^{k-1}-s})+g(x)\cdot 2(x-1)^s,2(x-1)^s\rangle\\ &= \langle(x-1)^{2^k-s}+2(\phi(b(x))+(x-1)^{2^{k-1}-s}),2(x-1)^s\rangle.\end{aligned}$$

Moreover, by Lemma 4, we have that

$$(x-1)^{2^k-s}\cdot 2(x-1)^s=2(x-1)^{2^k}=2\cdot 2(x-1)^{2^{k-1}}=0.$$

Similarly, as $2^k - 2s \geq 2^k - 2 \cdot 2^{k-1} = 0$, we obtain

$$(x-1)^{2(2^k-s)} = (x-1)^{2^k}(x-1)^{2^k-2s} = 2(x-1)^{2^{k-1}}(x-1)^{2^k-2s},$$

and hence

$$\begin{aligned}
&\big((x-1)^{2^k-s} + 2\phi(b(x))\big)\big((x-1)^{2^k-s} + 2\big(\phi(b(x)) + (x-1)^{2^{k-1}-s}\big)\big)\\
&= (x-1)^{2(2^k-s)} + 2(x-1)^{2^k-s} \cdot \big(\phi(b(x)) + \phi(b(x)) + (x-1)^{2^{k-1}-s}\big)\\
&= 2(x-1)^{2^{k-1}+2^k-2s} + 2(x-1)^{2^k-s} \cdot (x-1)^{2^{k-1}-s}\\
&= 0.
\end{aligned}$$

From these, we deduce that $\phi(\mathcal{C}_{\underline{b}}) \cdot \chi(\mathcal{C}_{\underline{b}}) = \{0\}$. Since R is a Galois ring and $|\chi(\mathcal{C}_{\underline{b}})| = |\phi(\mathcal{C}_{\underline{b}})| = |\mathcal{C}_{\underline{b}}| = (|R|^{2^k})^{\frac{1}{2}}$, we conclude that $\mathrm{Ann}(\phi(\mathcal{C}_{\underline{b}})) = \chi(\mathcal{C}_{\underline{b}})$.

As $\chi^{-1} = \chi$, we have $(\phi(\mathcal{C}_{\underline{b}}))^{\perp_E} = \chi(\mathrm{Ann}(\phi(\mathcal{C}_{\underline{b}}))) = \chi^2(\mathcal{C}_{\underline{b}}) = \mathcal{C}_{\underline{b}}$. This implies $\phi(\mathcal{C}_{\underline{b}}) = \mathcal{C}_{\underline{b}}^{\perp_E}$. From this and by the condition in (2) of Section 2, we conclude that $\mathcal{C}_{\underline{b}}$ is a Hermitian self-dual code.

Finally, by the definition of ϕ and Lemma 1 (iii), it follows that

$$\begin{aligned}
2\phi(b(x)) &= \phi(2b(x)) = \phi\left(\sum_{j=0}^{s-1} 2b_j(x-1)^j\right) = \sum_{j=0}^{s-1} \phi(2b_j)\phi\big((x-1)^j\big)\\
&= \sum_{j=0}^{s-1} 2b_j^q(x-1)^j = 2\left(\sum_{j=0}^{s-1} b_j^q(x-1)^j\right).
\end{aligned}$$

This implies $\phi(b(x)) = \sum_{j=0}^{s-1} b_j^q(x-1)^j \pmod 2$.

□

By $-1 = 1$ in the finite field $\mathbb{F}_2 \subset \mathbb{F}_{q^2}$, we have the following conclusion.

Lemma 7 ([12, Theorem 1 (ii) and its proof]) Let l be an integer satisfying $1 \leq l \leq 2^k - 1$, and let G_l be the matrix defined by (4). Let $B_l = (b_0, b_1, \ldots, b_{l-1})^{\mathrm{tr}} \in \mathbb{F}_{q^2}^l$ and set $\beta(x) = \sum_{j=0}^{l-1} b_j(x-1)^j$. Then we have

$$x^{-1}\beta(x^{-1}) \equiv (1, (x-1), (x-1)^2, \ldots, (x-1)^{l-1})(G_l B_l) \pmod{(x-1)^l},$$

where $x^{-1} = x^{2^k-1} \pmod{(x-1)^l}$.

Lemma 8 Let $k \geq 3$ be any fixed integer. For any integer s, $2 \leq s \leq 2^{k-1} - 1$, we set

$$\rho_s(x) = (x-1)^{(2^{k-1}-1)-s}.$$

Then $\rho_s(x)$ satisfies (9) in Lemma 6, i.e.,

$$\phi(\rho_s(x)) + x^{-s}\rho_s(x^{-1}) \equiv (x-1)^{2^{k-1}-s} \pmod{(x-1)^s}.$$

Proof As $\phi(a) = a$ for all $a \in \mathbb{Z}_4 \subseteq R_0$, we have $\phi(\rho_s(x)) = \rho_s(x)$. Then by [11, Lemma 5]:

$$\rho_s(x) + x^{-s}\rho_s(x^{-1}) \equiv (x-1)^{2^{k-1}-s} \pmod{(x-1)^s},$$

we conclude that $\phi(\rho_s(x)) + x^{-s}\rho_s(x^{-1}) \equiv (x-1)^{2^{k-1}-s} \pmod{(x-1)^s}$.
□

We are now ready to prove Theorem 1 in Section 3. It is obvious that $\langle 2 \rangle = 2 \cdot \frac{R[x]}{\langle x^{2^k}-1 \rangle}$ is a trivial Hermitian self-dual cyclic code of length 2^k over R for any positive integer k. Then we only need to determine the nontrivial codes.

Case 1: $k = 1$.

In this case, by [29, Theorem 3.4], there are $2^{\frac{m}{2}}$ nontrivial Hermitian self-dual cyclic codes of length 2 over R. As $1 \le s \le 2^{k-1} = 1$, we have $s = 1$.

Let $b(x) = b_0 + w$, where $b_0 \in \mathbb{F}_q$ and $q = 2^{\frac{m}{2}}$. Then we have $\phi(b(x)) = b_0 + 1 + w$, $(x-1)^{2^{k-1}-s} = (x-1)^0 = 1$ and $x^{-1}b(x^{-1}) = x^{-1}(b_0 + w) \equiv b_0 + w \pmod{x-1}$. From these, we deduce that

$$\phi(b(x)) + x^{-1}b(x^{-1}) \equiv (b_0 + 1 + w) + b_0 + w = (x-1)^{2^{k-1}-s} \pmod{x-1}.$$

Then by Lemma 6, we conclude that $\langle (x-1) + 2b(x), 2(x-1) \rangle$ is a nontrivial Hermitian self-dual cyclic code of length 2 over R, for any $b_0 \in \mathbb{F}_q$.

Moreover, by Lemma 5, all these cyclic codes are distinct from each other. Further, by $2(x-1) = 2((x-1) + 2b(x)) \in \langle (x-1) + 2b(x) \rangle$, it follows that $\langle (x-1) + 2b(x), 2(x-1) \rangle = \langle (x-1) + 2b(x) \rangle$.

Therefore, all Hermitian self-dual cyclic codes of length 2 over R have been given in Theorem 1.

Case 2: $k \ge 2$.

As $1 \le s \le 2^{k-1}$, we have two cases for nontrivial Hermitian self-dual cyclic codes of length 2^k over R: when $s = 1$ and when $2 \le s \le 2^{k-1}$.

(i) Let $s = 1$. For any $b_0 \in \mathbb{F}_q$, set $b(x) = b_0$. Then $\phi(b(x)) = b_0$. As $x \equiv 1 \pmod{x-1}$, we get $x^{-1} \equiv 1 \pmod{x-1}$. By $k \ge 2$, we have $2^{k-1} - 1 \ge 1$. This implies $(x-1)^{2^{k-1}-1} \equiv 0 \pmod{x-1}$. From these, we deduce that

$$\phi(b(x)) + x^{-1}b(x^{-1}) \equiv b_0 + b_0 = 0 \equiv (x-1)^{2^{k-1}-1} \pmod{x-1}.$$

Then by Lemma 6, $\langle (x-1)^{2^{k-1}} + 2b(x), 2(x-1)^s \rangle$ is a nontrivial Hermitian self-dual cyclic code of length 2^k over R. Therefore, by Lemma 5, we obtain q distinct nontrivial Hermitian self-dual cyclic codes of length 2^k over R: $\langle (x-1)^{2^{k-1}} + 2b_0, 2(x-1) \rangle$, where $b_0 \in \mathbb{F}_q$.

(ii) Let $2 \le s \le 2^{k-1}$. We further split this case into two subcases: when $k = 2$ and when $k \ge 3$.

(ii-1) Let $k = 2$. Then we have $s = 2$, which is the only case. For any $b_0, b_1 \in \mathbb{F}_q$, set $b(x) = b_0 + w + b_1(x-1)$. Then we have that $\phi(b(x)) = b_0 + 1 + w + b_1(x-1) = 1 + b(x)$ and $(x-1)^{2^{2-1}-2} = 1$. Further, by $q = 2^{\frac{m}{2}}$, we have $(x-1)^2 = x^2 - 1$. This implies $x^2 \equiv 1$ and $x^{-1} \equiv x \pmod{(x-1)^2}$, and hence $x^{-2}b(x^{-1}) \equiv b(x) \pmod{(x-1)^2}$. From these, we deduce that

$$\phi(b(x)) + x^{-2}b(x^{-1}) \equiv 1 + b(x) + b(x) = (x-1)^{2^{2-1}-2} \pmod{(x-1)^2}.$$

Therefore, by Lemmas 6 and 5, we obtain q^2 distinct nontrivial Hermitian self-dual cyclic codes of length 2^k over R:

$$\begin{aligned}&\langle (x-1)^2+2(b_0+w+b_1(x-1)), 2(x-1)^2\rangle\\ =\ &\langle (x-1)^2+2(b_0+w+b_1(x-1))\rangle,\end{aligned}$$

where $b_0, b_1 \in \mathbb{F}_q$, since $2(x-1)^2 = 2((x-1)^2+2(b_0+w+b_1(x-1)))$.

Now, by Lemma 5, we have obtained $q+q^2$ distinct nontrivial Hermitian self-dual cyclic codes of length 2^2 over R given by Case (i) and Case (ii-1).

Moreover, by [29, Theorem 3.4], $q+q^2$ is the number of all nontrivial Hermitian self-dual cyclic codes of length 2^2 over R. Hence all Hermitian self-dual cyclic codes of length 2^2 over R have been given in Theorem 1.

(ii-2) Let $k \geq 3$ and $2 \leq s \leq 2^{k-1}$. For any integer $l \geq 2$, we set

$$X_l = (1, (x-1), (x-1)^2, \ldots, (x-1)^{l-1}).$$

Let $\underline{b} = (b_0, b_1, \ldots, b_{s-1})^{\mathrm{tr}}$, where $b_j = b_{j,0} + wb_{j,1} \in \mathbb{F}_{q^2}$ with $b_{j,0}, b_{j,1} \in \mathbb{F}_q$ for all $j = 0,1,\ldots,s-1$. Let $B_{s;(0)} = \begin{pmatrix} b_{0,0} \\ b_{1,0} \\ \vdots \\ b_{s-1,0} \end{pmatrix}$ and $B_{s;(1)} = \begin{pmatrix} b_{0,1} \\ b_{1,1} \\ \vdots \\ b_{s-1,1} \end{pmatrix}$, which are vectors in $\mathbb{F}_q^s$. Then we have $\underline{b} = B_{s;(0)} + wB_{s;(1)}$. Set

$$b(x) = b_0 + b_1(x-1) + \ldots + b_{s-1}(x-1)^{s-1} = X_s\underline{b} = X_s(B_{s;(0)} + wB_{s;(1)}).$$

By Lemma 1 (ii), we have $b_j^q = b_{j,0} + (1+w)b_{j,1} = (b_{j,0}+b_{j,1}) + wb_{j,1}$ for all j. Then it follows that

$$\begin{aligned}\phi(b(x)) &= \sum_{j=0}^{s-1} b_j^q (x-1)^j = \sum_{j=0}^{s-1} ((b_{j,0}+b_{j,1}) + wb_{j,1})(x-1)^j\\ &= X_s(B_{s;(0)} + B_{s;(1)} + wB_{s;(1)}) \pmod 2.\end{aligned}$$

By $2 \leq s \leq 2^{k-1}$, where $k \geq 3$, we have the following two cases: (‡) $2 \leq s \leq 2^{k-1}-1$, and (†) $s = 2^{k-1}$.

(‡) Let $2 \leq s \leq 2^{k-1}-1$. We adopt the following notation:

◇ Set $\widehat{b}(x) = \rho_s(x) + b(x)$, where $\rho_s(x) = (x-1)^{(2^{k-1}-1)-s}$ (see Lemma 8).

◇ Let $\mathcal{C}_{\widehat{b}(x)} = \langle (x-1)^{2^k-s} + 2\widehat{b}(x), 2(x-1)^s\rangle$, which is a cyclic code of length 2^k over R by Lemma 5. Then

$$\mathcal{C}_{\widehat{b}(x)} = \langle (x-1)^{2^k-s} + 2(x-1)^{(2^{k-1}-1)-s} + 2b(x), 2(x-1)^s\rangle.$$

Obviously, we have that $b(x) = \rho_s(x) + \widehat{b}(x)$, $\phi(\widehat{b}(x)) = \phi(b(x)) + \phi(\rho_s(x))$ and $x^{-s}\widehat{b}(x^{-1}) = x^{-s}b(x^{-1}) + x^{-s}\rho_s(x^{-1})$. Furthermore, by Lemma 8, we have that $\phi(\rho_s(x)) + x^{-s}\rho_s(x^{-1}) \equiv (x-1)^{2^{k-1}-s} \pmod{(x-1)^s}$. These imply

$$\begin{aligned}\phi(\widehat{b}(x)) + x^{-s}\widehat{b}(x^{-1}) &= \left(\phi(b(x)) + x^{-s}b(x^{-1})\right) + \left(\phi(\rho_s(x)) + x^{-s}\rho_s(x^{-1})\right)\\ &\equiv \left(\phi(b(x)) + x^{-s}b(x^{-1})\right) + (x-1)^{2^{k-1}-s} \pmod{(x-1)^s}.\end{aligned}$$

From this and by Lemma 6, we deduce that

$$\begin{aligned}
&\phi(b(x)) + x^{-s}b(x^{-1}) \equiv 0 \pmod{(x-1)^s} \\
\iff &\phi(\widehat{b}(x)) + x^{-s}\widehat{b}(x^{-1}) \equiv (x-1)^{2^{k-1}-s} \pmod{(x-1)^s} \\
\implies &(\mathcal{C}_{\widehat{b}(x)})^{\perp_H} = \mathcal{C}_{\widehat{b}(x)}.
\end{aligned}$$

From now on, we let

$$\beta(x) = (x-1)^{s-1}b(x) = X_{2s-1}\begin{pmatrix} \mathbf{0}_{s-1} \\ \underline{b} \end{pmatrix} = X_{2s-1}\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(0)} + wB_{s;(1)} \end{pmatrix},$$

where $\mathbf{0}_t$ is the zero column vector of length t, for any integer $t \geq 0$. Then we have $\phi(\beta(x)) = X_{2s-1}\left(\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(0)} \end{pmatrix} + \begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix} + w\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix}\right)$ and

$$x^{-1}\beta\left(x^{-1}\right) \equiv X_{2s-1}\left(G_{2s-1}\left(\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(0)} \end{pmatrix} + w\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix}\right)\right) \left(\mathrm{mod}\ (x-1)^{2s-1}\right)$$

by Lemma 7. On the other hand, we have

$$\phi(\beta(x)) = \phi((x-1)^{s-1}b(x)) = (x-1)^{s-1} \cdot \phi(b(x))$$

and $x^{-1}\beta(x^{-1}) = x^{-1}(x^{-1}-1)^{s-1}b(x^{-1}) = (x-1)^{s-1} \cdot x^{-s}b(x^{-1}) \pmod 2$. From these, we deduce that

$$\begin{aligned}
&\phi(b(x)) + x^{-s}b\left(x^{-1}\right) \equiv 0 \pmod{(x-1)^s} \\
\iff &\phi(\beta(x)) + x^{-1}\beta\left(x^{-1}\right) \equiv 0 \left(\mathrm{mod}\ (x-1)^{2s-1}\right) \\
\iff &\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(0)} \end{pmatrix} + \begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix} + w\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix} = G_{2s-1}\left(\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(0)} \end{pmatrix} + w\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix}\right) \\
\iff &\begin{cases} \begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix} + G_{2s-1}\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix} = 0; \\ \begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(0)} \end{pmatrix} + \begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix} + G_{2s-1}\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(0)} \end{pmatrix} = 0. \end{cases} \\
\iff &\begin{cases} M_{2s-1}\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix} = 0; \\ M_{2s-1}\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(0)} \end{pmatrix} = \begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix}, \end{cases}
\end{aligned}$$

where $M_{2s-1} = I_{2s-1} + G_{2s-1}$, by (4).

Using (4), (5) and (6) in Section 3, we can write

$$M_{2s-1} = \begin{pmatrix} M_{s-1} & 0 \\ * & \widetilde{M}_s \end{pmatrix},$$

where $\widetilde{M}_s = \left(Y_s^{[s-1,2s-1)}, Y_{s+1}^{[s-1,2s-1)}, \ldots, Y_{2s-1}^{[s-1,2s-1)}\right)$. Therefore, the matrices $B_{s;(1)}$ and $B_{s;(0)}$ satisfy the following matrix equations:

$$M_{2s-1}\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix} = 0 \text{ and } M_{2s-1}\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(0)} \end{pmatrix} = \begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix}, \tag{10}$$

if and only if $\widetilde{M}_s B_{s;(1)} = \mathbf{0}_s$ and $\widetilde{M}_s B_{s;(0)} = B_{s;(1)}$.

Now, by Lemmas 2 and 3 in Section 3, it follows that

$$\widetilde{M}_s B_{s;(1)} = \mathbf{0}_s \iff M_{2s-1}\begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix} = 0 \iff \begin{pmatrix} \mathbf{0}_{s-1} \\ B_{s;(1)} \end{pmatrix} \in \mathcal{S}_{2s-1}$$
$$\iff B_{s;(1)} \in \mathcal{S}_{2s-1}^{[s-1]}.$$

Therefore, $\mathcal{S}_{2s-1}^{[s-1]}$ is the solution space of the system of homogeneous linear equations $\widetilde{M}_s Y = \mathbf{0}_s$, where $Y = (y_0, y_1, \ldots, y_{s-1})^{\mathrm{tr}}$. By $\widetilde{M}_s B_{s;(0)} = B_{s;(1)}$, we see that $B_{s;(0)}$ is a solution vector of the following system of linear equations:

$$\widetilde{M}_s Y = B_{s;(1)}, \text{ where } B_{s;(1)} \in \mathcal{S}_{2s-1}^{[s-1]}. \tag{11}$$

As $2 \le s \le 2^{k-1} - 1$, we split this case into two subcases: when s is even and when s is odd.

(‡-1) Let s be even, where $2 \le s \le 2^{k-1} - 2$. Assume $B_{s;(1)} \in \mathcal{S}_{2s-1}^{[s-1]}$. Then by Lemma 3, the vector $B_{s;(1)}$ is uniquely expressed as

$$B_{s;(1)} = \sum_{\frac{s}{2} \le t \le s-1} c_{2t-1} Y_{2t-1}^{[s-1,2s-1)} + c_{2s-2}\varepsilon_s^{(s)}, \tag{12}$$

where $c_{2s-2}, c_{2t-1} \in \mathbb{F}_q$ for all integers t: $\frac{s}{2} \le t \le s-1$. Applying column elementary transformation to the augmented matrix of (11), from $\widetilde{M}_s = \left(Y_s^{[s-1,2s-1)}, Y_{s+1}^{[s-1,2s-1)}, \ldots, Y_{2s-1}^{[s-1,2s-1)}\right)$, we obtain

$$\left(\widetilde{M}_s \mid B_{s;(1)}\right) \overset{\text{column}}{\longrightarrow} \left(\widetilde{M}_s \mid c_{s-1} Y_{s-1}^{[s-1,2s-1)} + c_{2s-2}\varepsilon_s^{(s)}\right).$$

From this, by Lemma 3 and (6) in Section 3, we deduce that there are solutions to the linear equation system (11) if and only if $c_{s-1} = c_{2s-2} = 0$. Now, let this condition be satisfied. By (12), we have

$$B_{s;(1)} = \sum_{\frac{s}{2}+1 \le t \le s-1} c_{2t-1} Y_{2t-1}^{[s-1,2s-1)} = \widetilde{M}_s \underline{\widehat{c}} \text{ with } \underline{\widehat{c}} = \begin{pmatrix} \widehat{c}_s \\ \widehat{c}_{s+1} \\ \vdots \\ \widehat{c}_{2s-1} \end{pmatrix}, \tag{13}$$

and the components of $\underline{\widehat{c}}$ are defined by:

- $\widehat{c}_j = c_{2t-1}$, if $j = 2t - 1$ and $\frac{s}{2} + 1 \le t \le s - 1$;
- $\widehat{c}_j = 0$, otherwise.

Then the vector $\underline{\widehat{c}}$ is a solution of the linear equation system (11). Furthermore, since $\mathcal{S}_{2s-1}^{[s-1]}$ is the solution space of $\widetilde{M}_s Y = \mathbf{0}_s$, $\underline{\widehat{c}} + \mathcal{S}_{2s-1}^{[s-1]}$ must be the set of all solutions of 11), for any vector $B_{s,(1)}$ given by (13).

As stated above, we obtain the following $q^{\frac{s}{2}-1} q^{\frac{s}{2}+1} = q^s$ nontrivial Hermitian self-dual cyclic codes of length 2^k over R:

$$\mathcal{C}_{\widehat{b}(x)} = \langle (x-1)^{2^k - s} + 2(x-1)^{(2^{k-1}-1)-s} + 2b(x), 2(x-1)^s \rangle,$$

where $b(x) = X_s(B_{s;(0)} + wB_{s;(1)})$ is determined by

$$B_{s;(0)} \in \underline{\widehat{c}} + \mathcal{S}_{2s-1}^{[s-1]},\ B_{s;(1)} = \sum_{\frac{s}{2}+1 \le t \le s-1} c_{2t-1} Y_{2t-1}^{[s-1,2s-1)},$$

and $c_{2t-1} \in \mathbb{F}_q$ for all integers t: $\frac{s}{2} + 1 \le t \le s-1$.

(‡-2) Let s be odd, where $3 \le s \le 2^{k-1} - 1$. Assume $B_{s;(1)} \in \mathcal{S}_{2s-1}^{[s-1]}$. Then by Lemma 3, the vector $B_{s;(1)}$ is uniquely expressed as

$$B_{s;(1)} = \sum_{\frac{s+1}{2} \le t \le s-1} c_{2t-1} Y_{2t-1}^{[s-1,2s-1)} + c_{2s-2}\varepsilon_s^{(s)}, \tag{14}$$

where $c_{2s-2}, c_{2t-1} \in \mathbb{F}_q$ for all integers t: $\frac{s+1}{2} \le t \le s-1$. Applying column elementary transformation to the augmented matrix of (11), by $\widetilde{M}_s = (Y_s^{[s-1,2s-1)}, Y_{s+1}^{[s-1,2s-1)}, \ldots, Y_{2s-1}^{[s-1,2s-1)})$, we obtain

$$\left(\widetilde{M}_s \mid B_{s;(1)}\right) \overset{\text{column}}{\longrightarrow} \left(\widetilde{M}_s \mid c_{2s-2}\varepsilon_s^{(s)}\right).$$

From this, by Lemma 3 and (6) in Section 3, we deduce that there are solutions to the linear equation system (11) if and only if $c_{2s-2} = 0$. Now, let this condition be satisfied. By (14), we have

$$B_{s;(1)} = \sum_{\frac{s+1}{2} \le t \le s-1} C_{2t-1} Y_{2t-1}^{[s-1,2s-1)} = \widetilde{M}_s \underline{\widehat{c}} \text{ with } \underline{\widehat{c}} = \begin{pmatrix} \widehat{c}_s \\ \widehat{c}_{s+1} \\ \vdots \\ \widehat{c}_{2s-1} \end{pmatrix}, \tag{15}$$

and the components of $\underline{\widehat{c}}$ are defined by: $\widehat{c}_j = c_{2t-1}$, if $j = 2t-1$ and $\frac{s+1}{2} \le t \le s-1$; and $\widehat{c}_j = 0$, otherwise. Then the vector $\underline{\widehat{c}}$ is a solution of the linear equation system (11). Furthermore, since $\mathcal{S}_{2s-1}^{[s-1]}$ is the solution space of $\widetilde{M}_s Y = \mathbf{0}_s$, we conclude that $\underline{\widehat{c}} + \mathcal{S}_{2s-1}^{[s-1]}$ is the set of all solutions of (11), for any vector $B_{s,(1)}$ given by (15).

As stated above, we obtain the following $q^{\frac{s-1}{2}} q^{\frac{s+1}{2}} = q^s$ nontrivial Hermitian self-dual cyclic codes of length 2^k over R:

$$\mathcal{C}_{\widehat{b}(x)} = \langle (x-1)^{2^k - s} + 2(x-1)^{(2^{k-1}-1)-s} + 2b(x), 2(x-1)^s \rangle,$$

where $b(x) = X_s(\widehat{B}_{s;(0)} + wB_{s;(1)})$ is determined by

$$B_{s;(0)} \in \underline{\widehat{c}} + \mathcal{S}_{2s-1}^{[s-1]},\ B_{s;(1)} = \sum_{\frac{s+1}{2} \le t \le s-1} c_{2t-1} Y_{2t-1}^{[s-1,2s-1)},$$

and $c_{2t-1} \in \mathbb{F}_q$ for all integers t: $\frac{s+1}{2} \le t \le s-1$.

(†) Let $s = 2^{k-1}$ and set

$$b(x) = (c_0 + w) + \sum_{j=1}^{2^{k-2}-1} (a_j + c_j + a_j w)x^j + c_{2^{k-2}} x^{2^{k-2}} + \sum_{j=1}^{2^{k-2}-1} (c_j + a_j w)x^{2^{k-1}-j},$$

where $a_i, c_j, c_0, c_{2^{k-2}} \in \mathbb{F}_q$, for all $i = 1,2,\ldots,2^{k-2} - 1$. As $q = 2^{\frac{m}{2}}$, we have $(x-1)^{2^{k-1}} = x^{2^{k-1}} - 1$. This implies $x^{2^{k-1}} \equiv 1$ and $x^{-j} \equiv x^{2^{k-1}-j} \pmod{(x-1)^{2^{k-1}}}$, and hence

$$\begin{aligned}\phi(b(x)) &= (c_0+1+w)+\sum_{j=1}^{2^{k-2}-1}(a_j+c_j+a_j(1+w))x^j\\ &\quad +c_{2^{k-2}}x^{2^{k-2}}+\sum_{j=1}^{2^{k-2}-1}(c_j+a_j(1+w))x^{2^{k-1}-j}\\ &= 1+(c_0+w)+\sum_{j=1}^{2^{k-2}-1}(a_j+c_j+w)x^{2^{k-1}-j}\\ &\quad +c_{2^{k-2}}x^{2^{k-2}}+\sum_{j=1}^{2^{k-2}-1}(c_j+a_jw)x^j\\ &\equiv 1+x^{-2^{k-1}}b(x^{-1})\ \left(\mathrm{mod}\ (x-1)^{2^{k-1}}\right).\end{aligned}$$

From this, we deduce that $\phi(b(x))+x^{-2^{k-1}}b(x^{-1})\equiv 1\,(\mathrm{mod}\,(x-1)^{2^{k-1}})$. Then by Lemmas 6 and 5, we obtain $q^{2\cdot(2^{k-2}-1)+2}=q^{2^{k-1}}$ distinct nontrivial Hermitian self-dual cyclic codes of length 2^k over R:

$$\langle (x-1)^{2^{k-1}}+2b(x),2(x-1)^{2^{k-1}}\rangle=\langle (x-1)^{2^{k-1}}+2b(x)\rangle,$$

where $a_i,c_i,c_0,c_{2^{k-2}}\in\mathbb{F}_q$, for all $i=1,\ldots,2^{k-2}-1$.

Summarizing the results above, we have constructed

$$1+q+\sum_{s=2}^{2^{k-1}-1}q^s+q^{2^{k-1}}=\frac{q^{2^{k-1}+1}-1}{q-1}$$

distinct Hermitian self-dual cyclic codes of length 2^k over R.

As the number of all Hermitian self-dual cyclic codes of length 2^k over R is $N_{\mathrm{H}}(\mathrm{GR}(4,m),2^k)=\frac{q^{2^{k-1}+1}-1}{q-1}$ (cf. [29, Theorem 3.4]), where $q=2^{\frac{m}{2}}$, the codes listed by Theorem 1 are exactly all the distinct Hermitian self-dual cyclic codes of length 2^k over R. Therefore, we have proved Theorem 1.

6 Applications

In this section, we list all distinct Hermitian self-dual cyclic codes of length 2^k over the Galois ring $R=\mathrm{GR}(4,m)$, where m is even, using Theorem 1 or Theorem 2. To save space, we only consider the cases $k=3,4,5$.

Example 3 All $1+q+q^2+q^3+q^4$ Hermitian self-dual cyclic codes of length 8 over R are given by the following four cases:

(i) 1 code: $\langle 2\rangle$.
(ii) q codes: $\langle (x-1)^7+2b_0,2(x-1)\rangle$, where $b_0\in\mathbb{F}_q$.
(iii) q^2+q^3 codes: $\langle (x-1)^{8-s}+2(x-1)^{3-s}+2b_s(x),2(x-1)^s\rangle$, where $s=2,3$ and

$b_2(x) = a_1 + (a_1 + a_2)(x-1), a_1, a_2 \in \mathbb{F}_q$;
$b_3(x) = c_3 + (a_3 + wc_3)(x-1) + a_4(x-1)^2, c_3, a_3, a_4 \in \mathbb{F}_q$.

(iv) q^4 codes: $\langle (x-1)^4 + 2b(x) \rangle$, where

$b(x) = (c_0 + w) + (a_1 + c_1 + wa_1)x + c_2x^2 + (c_1 + a_1w)x^3$ and $a_1, c_0, c_1, c_2 \in \mathbb{F}_q$.

Example 4 All $1 + \sum_{s=1}^{8} q^s$ Hermitian self-dual cyclic codes of length 16 over R are given by the following four cases:

(i) 1 code: $\langle 2 \rangle$.
(ii) q codes: $\langle (x-1)^{15} + 2b_0, 2(x-1) \rangle$, where $b_0 \in \mathbb{F}_q$.
(iii) $\sum_{s=2}^{7} q^s$ codes: $\langle (x-1)^{16-s} + 2(x-1)^{7-s} + 2b_s(x), 2(x-1)^s \rangle$,

where $s = 2,3,4,5,6,7$ and
$b_2(x), b_3(x)$ are the same as those in Example 3;

$$\begin{aligned}
b_4(x) &= a_3 + c_5(x-1) + (a_5 + wc_5)(x-1)^2 + (a_3 + a_5 + a_6 + wc_5)(x-1)^3, c_5, a_3, a_5, a_6 \in \mathbb{F}_q;\\
b_5(x) &= c_5 + (a_5 + wc_5)(x-1) + (c_7 + a_5 + wc_5)(x-1)^2 + (a_5 + a_7 + w(c_5 + c_7))(x-1)^3\\
&\quad + a_8(x-1)^4, c_5, c_7, a_5, a_7, a_8 \in \mathbb{F}_q;\\
b_6(x) &= a_5 + (c_7 + a_5)(x-1) + (a_5 + a_7 + wc_7)(x-1)^2 + c_9(x-1)^3 + (a_9 + wc_9)(x-1)^4\\
&\quad + (a_9 + a_{10} + wc_9)(x-1)^5, c_7, c_9, a_5, a_7, a_9, a_{10} \in \mathbb{F}_q;\\
b_7(x) &= c_7 + (a_7 + wc_7)(x-1) + c_9(x-1)^2 + (a_9 + wc_9)(x-1)^3 + (c_{11} + a_9 + wc_9)(x-1)^4\\
&\quad + (a_9 + a_{11} + w(c_9 + c_{11}))(x-1)^5 + (a_9 + a_{12} + wc_9)(x-1)^6, c_7, c_9, c_{11}, a_7, a_9, a_{11}, a_{12} \in \mathbb{F}_q.
\end{aligned}$$

(iv) q^8 codes: $\langle (x-1)^8 + 2b(x) \rangle$, where

$$b(x) = (c_0 + w) + \sum_{j=1}^{3} (a_j + c_j + a_jw)x^j + c_4x^4 + \sum_{j=1}^{3} (c_j + a_jw)x^{8-j}$$

and $a_i, c_i, c_0, c_4 \in \mathbb{F}_q$, for all $i = 1,2,3$.

Example 5 All $1 + \sum_{s=1}^{15} q^s$ Hermitian self-dual cyclic codes of length 32 over R are given by the following four cases:

(i) 1 code: $\langle 2 \rangle$.
(ii) q codes: $\langle (x-1)^{31} + 2b_0, 2(x-1) \rangle$, where $b_0 \in \mathbb{F}_q$.
(iii) $\sum_{s=2}^{15} q^s$ codes: $\langle (x-1)^{32-s} + 2(x-1)^{15-s} + 2b_s(x), 2(x-1)^s \rangle$, where $s = 2,3,4,5,6,7,8,9,10,11,12,13,14,15$ and

$b_2(x), b_3(x), b_4(x), b_5(x), b_6(x), b_7(x)$ are the same as those in Example 4;

$$
\begin{aligned}
b_8(x) &= a_7 + c_9(x-1) + (a_9 + c_9w)(x-1)^2 + (a_9 + c_{11} + c_9w)(x-1)^3 + (a_9 + a_{11} \\
&\quad + c_9w + c_{11}w)(x-1)^4 + (a_9 + c_{13} + c_9w)(x-1)^5 + (a_9 + a_{13} + c_9w \\
&\quad + c_{13}w)(x-1)^6 + (a_7 + a_9 + a_{11} + a_{13} + a_{14} + c_9w + c_{11}w + c_{13}w)(x-1)^7; \\
b_9(x) &= c_9 + (a_9 + c_9w)(x-1) + (a_9 + c_{11} + c_9w)(x-1)^2 + (a_9 + a_{11} + c_9w \\
&\quad + c_{11}w)(x-1)^3 + (a_9 + c_{13} + c_9w)(x-1)^4 + (a_9 + a_{13} + c_9w \\
&\quad + c_{13}w)(x-1)^5 + (a_9 + a_{11} + a_{13} + c_{15} + c_9w + c_{11}w + c_{13}w)(x-1)^6 \\
&\quad + (a_9 + a_{11} + a_{13} + a_{15} + c_9w + c_{11}w + c_{13}w + c_{15}w)(x-1)^7 + a_{16}(x-1)^8; \\
b_{10}(x) &= a_9 + (a_9 + c_{11})(x-1) + (a_9 + a_{11} + c_{11}w)(x-1)^2 + (a_9 + c_{13})(x-1)^3 \\
&\quad + (a_9 + a_{13} + c_{13}w)(x-1)^4 + (a_9 + a_{11} + a_{13} + c_{15} + c_{11}w + c_{13}w)(x-1)^5 \\
&\quad + (a_9 + a_{11} + a_{13} + a_{15} + c_{11}w + c_{13}w + c_{15}w)(x-1)^6 + c_{17}(x-1)^7 \\
&\quad + (a_{17} + c_{17}w)(x-1)^8 + (a_{17} + a_{18} + c_{17}w)(x-1)^9; \\
b_{11}(x) &= c_{11} + (a_{11} + c_{11}w)(x-1) + c_{13}(x-1)^2 + (a_{13} + c_{13}w)(x-1)^3 + (a_{11} + a_{13} \\
&\quad + c_{15} + c_{11}w + c_{13}w)(x-1)^4 + (a_{11} + a_{13} + a_{15} + c_{11}w + c_{13}w + c_{15}w)(x-1)^5 \\
&\quad + c_{17}(x-1)^6 + (a_{17} + c_{17}w)(x-1)^7 + (a_{17} + c_{19} + c_{17}w)(x-1)^8 + (a_{17} \\
&\quad + a_{19} + c_{17}w + c_{19}w)(x-1)^9 + (a_{17} + a_{20} + c_{17}w)(x-1)^{10}; \\
b_{12}(x) &= a_{11} + c_{13}(x-1) + (a_{13} + c_{13}w)(x-1)^2 + (a_{11} + a_{13} + c_{15} + c_{13}w)(x-1)^3 \\
&\quad + (a_{11} + a_{13} + a_{15} + c_{13}w + c_{15}w)(x-1)^4 + c_{17}(x-1)^5 + (a_{17} + c_{17}w)(x-1)^6 \\
&\quad + (a_{17} + c_{19} + c_{17}w)(x-1)^7 + (a_{17} + a_{19} + c_{17}w + c_{19}w)(x-1)^8 + (a_{17} + c_{21} \\
&\quad + c_{17}w)(x-1)^9 + (a_{17} + a_{21} + c_{17}w + c_{21}w)(x-1)^{10} + (a_{17} + a_{19} + a_{21} \\
&\quad + a_{22} + c_{17}w + c_{19}w + c_{21}w)(x-1)^{11}; \\
b_{13}(x) &= c_{13} + (a_{13} + c_{13}w)(x-1) + (a_{13} + c_{15} + c_{13}w)(x-1)^2 + (a_{13} + a_{15} + c_{13}w \\
&\quad + c_{15}w)(x-1)^3 + c_{17}(x-1)^4 + (a_{17} + c_{17}w)(x-1)^5 + (a_{17} + c_{19} + c_{17}w)(x-1)^6 \\
&\quad + (a_{17} + a_{19} + c_{17}w + c_{19}w)(x-1)^7 + (a_{17} + c_{21} + c_{17}w)(x-1)^8 + (a_{17} + a_{21} \\
&\quad + c_{17}w + c_{21}w)(x-1)^9 + (a_{17} + a_{19} + a_{21} + c_{23} + c_{17}w + c_{19}w + c_{21}w)(x-1)^{10} \\
&\quad + (a_{17} + a_{19} + a_{21} + a_{23} + c_{17}w + c_{19}w + c_{21}w + c_{23}w)(x-1)^{11} \\
&\quad + (a_{17} + a_{24} + c_{17}w)(x-1)^{12}; \\
b_{14}(x) &= a_{13} + (a_{13} + c_{15})(x-1) + (a_{13} + a_{15} + c_{15}w)(x-1)^2 + c_{17}(x-1)^3 + (a_{17} \\
&\quad + c_{17}w)(x-1)^4 + (a_{17} + c_{19} + c_{17}w)(x-1)^5 + (a_{17} + a_{19} + c_{17}w + c_{19}w)(x-1)^6 \\
&\quad + (a_{17} + c_{21} + c_{17}w)(x-1)^7 + (a_{17} + a_{21} + c_{17}w + c_{21}w)(x-1)^8 + (a_{17} + a_{19} \\
&\quad + a_{21} + c_{23} + c_{17}w + c_{19}w + c_{21}w)(x-1)^9 + (a_{17} + a_{19} + a_{21} + a_{23} + c_{17}w \\
&\quad + c_{19}w + c_{21}w + c_{23}w)(x-1)^{10} + (a_{17} + c_{25} + c_{17}w)(x-1)^{11} + (a_{17} + a_{25} \\
&\quad + c_{17}w + c_{25}w)(x-1)^{12} + (a_{17} + a_{19} + a_{25} + a_{26} + c_{17}w + c_{19}w + c_{25}w)(x-1)^{13}; \\
b_{15}(x) &= c_{15} + (a_{15} + c_{15}w)(x-1) + c_{17}(x-1)^2 + (a_{17} + c_{17}w)(x-1)^3 + (a_{17} + c_{19} \\
&\quad + c_{17}w)(x-1)^4 + (a_{17} + a_{19} + c_{17}w + c_{19}w)(x-1)^5 + (a_{17} + c_{21} + c_{17}w)(x-1)^6 \\
&\quad + (a_{17} + a_{21} + c_{17}w + c_{21}w)(x-1)^7 + (a_{17} + a_{19} + a_{21} + c_{23} + c_{17}w + c_{19}w \\
&\quad + c_{21}w)(x-1)^8 + (a_{17} + a_{19} + a_{21} + a_{23} + c_{17}w + c_{19}w + c_{21}w + c_{23}w)(x-1)^9 \\
&\quad + (a_{17} + c_{25} + c_{17}w)(x-1)^{10} + (a_{17} + a_{25} + c_{17}w + c_{25}w)(x-1)^{11} + (a_{17} + a_{19} \\
&\quad + a_{25} + c_{27} + c_{17}w + c_{19}w + c_{25}w)(x-1)^{12} + (a_{17} + a_{19} + a_{25} + a_{27} + c_{17}w \\
&\quad + c_{19}w + c_{25}w + c_{27}w)(x-1)^{13} + (a_{17} + a_{21} + a_{25} + a_{28} + c_{17}w + c_{21}w + c_{25}w)(x-1)^{14},
\end{aligned}
$$

and $a_i, c_{2t-1} \in \mathbb{F}_q$ for all integers i,t: $1 \le i \le 28$ and $2 \le t \le 14$.

(iv) q^{16} codes: $\langle (x-1)^{16} + 2b(x) \rangle$, where

$$b(x) = (c_0 + w) + \sum_{j=1}^{7} (a_j + c_j + a_j w)x^j + c_8 x^8 + \sum_{j=1}^{7} (c_j + a_j w)x^{16-j}$$

and $a_i, c_i, c_0, c_8 \in \mathbb{F}_q$, for all $i = 1,2,3,4,5,6,7$.

Remark 2 Let the Galois rings GR(4,2) and GR(4,4) be constructed by Examples 1 and 2, respectively. Then by Examples 4 and 5, we obtain:

- ◇ 511 distinct Hermitian self-dual cyclic codes of length 16 over GR(4,2);
- ◇ 87381 distinct Hermitian self-dual cyclic codes of length 16 over GR(4,4);
- ◇ 131071 distinct Hermitian self-dual cyclic codes of length 32 over GR(4,2);
- ◇ 5726623061 distinct Hermitian self-dual cyclic codes of length 32 over GR(4,4).

Finally, we give an example of the construction of self-dual cyclic codes over $\mathbb{Z}_4$ of length 6. First, we have that $z^3-1=(z-1)(z^2+z+1)$, where $z-1$ and z^2+z+1 correspond to the 2-cyclotomic cosets modulo 3 $S_2(0)=\{0\}$ and $S_2(1)=\{1,2\}$ respectively. Obviously, $S_2(1)$ is self-inverse.

Let $\mathrm{GR}(4,2)=\frac{\mathbb{Z}_4[z]}{\langle z^2+z+1\rangle}$. As $\mathbb{Z}_4=\frac{\mathbb{Z}_4[z]}{\langle z-1\rangle}$, we have the following isomorphism of rings from $\mathbb{Z}_4\times\mathrm{GR}(4,2)$ onto $\frac{\mathbb{Z}_4[z]}{\langle z^3-1\rangle}$ defined by:

$$(b,a_0+a_1z)\mapsto 3(z^2+z+1)b+(z^2+z+2)(a_0+a_1z)\ (\mathrm{mod}\ z^3-1),$$

for all $b,a_0,a_1\in\mathbb{Z}_4$. Hence $\mathcal{C}$ is a self-dual cyclic code over $\mathbb{Z}_4$ of length 6 if and only if $\mathcal{C}\cong C_0\times C_1$, where C_0 (as an ideal of $\frac{\mathbb{Z}_4[y]}{\langle y^2-1\rangle}$) is an Euclidean self-dual cyclic code over $\mathbb{Z}_4$ of length 2 and C_1 (as an ideal of $\frac{\mathrm{GR}(4,2)[y]}{\langle y^2-1\rangle}$) is a Hermitian self-dual cyclic code over GR(4,2) of length 2.

By [11, Theorem 2] and Theorem 1 in Section 4, we give all 3 self-dual cyclic codes $\mathcal{C}$ over $\mathbb{Z}_4$ of length 6 by the following table:

C_0	C_1	$\mathcal{C}$ (as ideals of the ring $\frac{\mathbb{Z}_4[x]}{\langle x^6-1\rangle}$)
$\langle 2\rangle$	$\langle 2\rangle$	$\langle 2\rangle$
$\langle 2\rangle$	$\langle (y-1)+2z\rangle$	$\langle 2+x+3x^2+2x^3+x^4+x^5\rangle$
$\langle 2\rangle$	$\langle (y-1)+2(1+z)\rangle$	$\langle 2+x+x^2+2x^3+3x^4+x^5\rangle$

7 Conclusions and further work

For any positive integers m and k, where m is even, we have given a direct and effective approach to construct all distinct Hermitian self-dual cyclic codes of length 2^k over the Galois ring GR(4,m) precisely. In particular, using binomial coefficients, we have provided an explicit expression to accurately represent this class of Hermitian self-dual cyclic codes over GR(4,m).

Theoretically, using the results in [11, 22] and this paper, any self-dual cyclic code over $\mathbb{Z}_4$ of arbitrary even length can be constructed by the Discrete Fourier Transform decomposition given in [29]. This approach is, however, not easy to be implemented in practice.

A natural extension of this work will be to give directly an explicit representation for all self-dual cyclic codes over $\mathbb{Z}_4$ of length 2^kn, for any positive odd integer n. Moreover, it would be interesting to investigate the parameters of these codes and obtain good self-dual cyclic $\mathbb{Z}_4$-codes and formally self-dual binary codes, using the representations obtained.

Acknowledgements This research is supported in part by the National Natural Science Foundation of China (Grant Nos. 12071264, 11801324, 11671235), the Shandong Provincial Natural Science Foundation, China (Grant No. ZR2018BA007), Nanyang Technological University, Singapore (Grant No. 04INS000047C230GRT01), the IC Program of Shandong Institutions of Higher Learning For Youth Innovative Talents and the Scientific Research Fund of Hubei Provincial Key Laboratory of Applied Mathematics (Hubei University)(Grant Nos. HBAM201906).

Funding Not available.

References

1. Abualrub, T., Oehmke, R.: On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e. IEEE Trans. Inform. Theory **49**, 2126–2133 (2003)
2. Bachoc, C.: Application of coding theory to the construction of modular lattices. J. Combin. Theory Ser. A **78**, 92–119 (1997)
3. Blackford, T., Ray-Chaudhuri, D.K.: A transform approach to permutation groups of cyclic codes over Galois rings. IEEE Trans. Inform. Theory **46** (7), 2350–2358 (2000)
4. Blackford, T.: Cyclic codes over $\mathbb{Z}_4$ of oddly even length. Discret. Appl. Math. **128**, 27–46 (2003)
5. Blackford, T.: Negacyclic codes over $\mathbb{Z}_4$ of even length. IEEE Trans. Inform. Theory **49**(6), 1417–1424 (2003)
6. Bonnecaze, A., Rains, E., Solé, P.: 3-colored 5-designs and Z_4,-codes. J. Statist. Plann. Inference **86**(2), 349–368 (2000). Special issue in honor of Professor Ralph Stanton. MR 1768278 (2001g:05021)
7. Calderbank, A.R., Sloane, N.J.A.: Modular and p-adic cyclic codes. Des. Codes Cryptogr. **6**(1), 21–35 (1995)
8. Calderbank, A.R., Sloane, N.J.A.: Double circulant codes over $\mathbb{Z}_4$ and even unimodular lattices. J. Alg. Combin. **6**, 119–131 (1997)
9. Cao, Y., Cao, Y., Dougherty, S.T., Ling, S.: Construction and enumeration for self-dual cyclic codes over $\mathbb{Z}_4$ of oddly even length. Des. Codes Cryptogr. **87**, 2419–2446 (2019)
10. Cao, Y., Cao, Y., Fu, F.-W., Wang, G.: Self-dual cyclic codes over $\mathbb{Z}_4$ of length 4n. Appl. Algebra in Engrg. Comm. Comput. **33**, 21–51 (2022)
11. Cao, Y., Cao, Y., Ling, S., Wang, G.: An explicit expression for Euclidean self-dual cyclic codes of length 2^k over Galois ring GR(4,m). Finite Fields Appl. **72**, 101817 (2021)
12. Cao, Y., Cao, Y., Dinh, H.Q., Jitman, S.: An explicit representation and enumeration for self-dual cyclic codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ of length 2^s. Discrete Math. **342**, 2077–2091 (2019)
13. Cao, Y., Cao, Y., Dinh, H.Q., Jitman, S.: An efficient method to construct self-dual cyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Discret. Math. **343**, 111868 (2020)
14. Castagnoli, G., Massey, J.L., Schoeller, P.A., von Seemann, N.: On repeated-root cyclic codes. IEEE Trans. Inform. Theory **37**(2), 337–342 (1991)
15. Dinh, H.Q., López-Permouth, S.R.: Cyclic and negacyclic codes over finite chain rings. IEEE Trans. Inform. Theory **50**(8), 1728–1744 (2004)
16. Dinh, H.Q.: Negacyclic codes of length 2^s over Galois rings. IEEE Trans. Inform. Theory **51**(12), 4252–4262 (2005)
17. Dinh, H.Q.: Complete distances of all negacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$. IEEE Trans. Inform. Theory **53**(1), 147–161 (2007)
18. Dinh, H.Q.: On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. Finite Fields Appl. **14**(1), 22–40 (2008)
19. Dinh, H.Q.: Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Trans. Inform. Theory **55**(4), 1730–1740 (2009)
20. Dinh, H.Q.: Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. J. Algebra **324**(5), 940–950 (2010)
21. Dougherty, S.T., Park, Y.H.: On modular cyclic codes. Finite Fields Appl. **13**, 31–57 (2007)
22. Dougherty, S.T., Ling, S.: Cyclic codes over $\mathbb{Z}_4$ of even length. Des. Codes Cryptogr. **39**, 127–153 (2006)
23. Gaborit, P., Natividad, A.M., Solé, P.: Eisenstein lattices, Galois rings and quaternary codes. Int. J. Number Theory **2**, 289–303 (2006)
24. Hammons, Jr.A. R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inform. Theory **40**(2), 301–319 (1994)
25. Harada, M.: Self-dual $\mathbb{Z}_4$-codes and Hadamard matrices. Discret. Math. **245**, 273–278 (2002)

26. Harada, M., Kitazume, M., Munemasa, A., Venkov, B.: On some self-dual codes and unimodular lattices in dimension 48. Eur. J. Combin. **26**, 543–557 (2005)
27. Harada, M., Miezaki, T.: An optimal odd unimodular lattice in dimension 72. Arch. Math. **97**(6), 529–533 (2011)
28. Harada, M., Solé, P., Gaborit, P.: Self-dual codes over $\mathbb{Z}_4$ and unimodular lattices: a survey. In: Algebras and Combinatorics, Hong Kong, 1997, pp 255–275. Springer, Singapore (1999)
29. Jitman, S., Ling, S., Sangwisut, E.: On self-dual cyclic codes of length p^a over GR(p^2,s). Adv. Math. Commun. **10**, 255–273 (2016)
30. Kai, X., Zhu, S.: On the distance of cyclic codes of length 2^e over $\mathbb{Z}_4$. Discret. Math. **310**(1), 12–20 (2010)
31. Kaya, A., Yildiz, B.: Various constructions for self-dual codes over rings and new binary self-dual codes. Discret. Math. **339**, 460–469 (2016)
32. Kiah, H.M., Leung, K.H., Ling, S.: Cyclic codes over GR(p^2,m) of length p^k. Finite Fields Appl. **14**, 834–846 (2008)
33. Kiah, H.M., Leung, K.H., Ling, S.: A note on cyclic codes over GR(p^2,m) of length p^k. Des. Codes Cryptogr. **63**, 105–112 (2012)
34. Kiermaier, M.: There is no self-dual Z_4,-linear codes whose Gray image has the parameter (72, 2^{36}, 16). IEEE Trans. Inform. Theory **59**(6), 3384–3386 (2013)
35. Kanwar, P., López-Permouth, S.R.: Cyclic codes over the integers modulo p^m. Finite Fields Appl. **3**(4), 334–352 (1997)
36. Liu, H., Youcef, M.: Some repeated-root constacyclic codes over Galois rings. IEEE Trans. Inform. Theory **63**(10), 6247–6255 (2017)
37. López-Permouth, S.R., Szabo, S.: On the Hamming weight of repeated root cyclic and negacyclic codes over Galois rings. Adv. Math. Commun. **3**(4), 409–420 (2009)
38. Massey, J.L., Costello, D.J., Justesen, J.: Polynomial weights and code constructions. IEEE Trans. Inform. Theory **19**, 101 (1973)
39. Norton, G.H., Ana Sălăgean, A.: On the structure of linear and cyclic codes over a finite chain ring. Appl. Algebra Engrg. Comm. Comput. **10**(6), 489–506 (2000)
40. Pless, V.S., Qian, Z.: Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. IEEE Trans. Inform. Theory **42**(5), 1594–1600 (1996)
41. Roth, R.M., Seroussi, G.: On cyclic MDS codes of length q over GF(q). IEEE Trans. Inform. Theory **32**(2), 284–285 (1986)
42. Sălăgean, A.: Repeated-root cyclic and negacyclic codes over a finite chain ring. Discret. Appl. Math. **154**(2), 413–419 (2006)
43. Shi, M., Qian, L., Sok, L., Aydin, N., Solé, P.: On constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2-1\rangle$ and their Gray images. Finite Fields Appl. **45**, 86–95 (2017)
44. Vega, G., Wolfmann, J.: Some families of $\mathbb{Z}_4$-cyclic codes. Finite Fields Appl. **10**(4), 530–539 (2004)
45. van Lint, J.H.: Repeated-root cyclic codes. IEEE Trans. Inform. Theory **37**(2), 343–345 (1991)
46. Wan, Z.-X.: Lectures on finite fields and Galois rings. World Scientific Pub Co Inc (2003)
47. Wolfmann, J.: Negacyclic and cyclic codes over $\mathbb{Z}_4$. IEEE Trans. Inform. Theory **45**(7), 2527–2532 (1999)
48. Wolfmann, J.: Binary images of cyclic codes over $\mathbb{Z}_4$. IEEE Trans. Inform. Theory **47**(5), 1773–1779 (2001)
49. Zimmermann, K.-H.: On generalizations of repeated-root cyclic codes. IEEE Trans. Inform. Theory **42**(2), 641–649 (1996)