Applicable Algebra in Engineering, Communication and Computing (2024) 35:291–314
https://doi.org/10.1007/s00200-022-00550-x

ORIGINAL PAPER

Constructing and expressing Hermitian self-dual cyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

Yuan Cao[1,3] · Yonglin Cao[1] · Fang-Wei Fu[2] · Fanghui Ma[1]

Received: 26 October 2021 / Accepted: 15 March 2022 / Published online: 19 April 2022

Abstract

Let p be an odd prime and m and s positive integers, with m even. Let further $\mathbb{F}_{p^m}$ be the finite field of p^m elements and $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ ($u^2 = 0$). Then R is a finite chain ring of p^{2m} elements, and there is a Gray map from R^N onto $\mathbb{F}_{p^m}^{2N}$ which preserves distance and orthogonality, for any positive integer N. It is an interesting approach to obtain self-dual codes of length $2N$ over $\mathbb{F}_{p^m}$ by constructing self-dual codes of length N over R. In particular, it has been shown that one of the key problems in constructing self-dual repeated-root cyclic codes over R is to find an effective way to present precisely Hermitian self-dual cyclic codes of length p^s over R. But so far, only the number of these codes has been determined in literature. In this paper, we give an efficient way of constructing all distinct Hermitian self-dual cyclic codes of length p^s over R by using column vectors of Kronecker products of matrices with specific types. Furthermore, we provide an explicit expression to present precisely all these Hermitian self-dual cyclic codes, using binomial coefficients.

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

✉ Yonglin Cao
ylcao@sdut.edu.cn

Yuan Cao
yuancao@sdut.edu.cn

Fang-Wei Fu
fwfu@nankai.edu.cn

Fanghui Ma
fhma@sdut.edu.cn

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

[2] Chern Institute of Mathematics and LPMC, and Tianjin Key Laboratory of Network and Data Security Technology, Nankai University, Tianjin 300071, China

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

Mathematics Subject Classification 94B15 · 94B05 · 11T71

1 Introduction

The class of self-dual codes is an interesting topic in coding theory due to their connections to other fields of mathematics such as lattices, cryptography, invariant theory, block designs, etc. In many instances, self-dual codes have been found by the following steps:

1. Find a self-dual code over a ring, say $\mathcal{C}$;
2. Map the code $\mathcal{C}$ onto a code over a subring (subfield, etc.) through a map that preserves duality.

In this research direction, many results have been presented in the literature (see [4, 5, 23–27, 30–32, 34], for examples).

We first review some necessary concepts and notations. Let Γ be a commutative finite ring with identity $1 \neq 0$, and $\Gamma^\times$ be the multiplicative group of invertible elements of Γ. Let N be a positive integer and set

$$\Gamma^N = \{(a_0, a_1, \ldots, a_{N-1}) \mid a_j \in \Gamma,\ j = 0, 1, \ldots, N-1\}.$$

Then Γ^N is a free Γ-module of rank N with componentwise addition and scalar multiplication by the elements of Γ. A *code* of length N over Γ is a nonempty subset $\mathcal{C}$ of Γ^N. A code $\mathcal{C}$ is said to be *linear* if $\mathcal{C}$ is an Γ-submodule of Γ^N, i.e., $\xi + \eta, c\xi \in \mathcal{C}$ for all $\xi, \eta \in \mathcal{C}$ and $c \in \Gamma$. All codes in this paper are assumed to be linear.

Let σ be a ring automorphism on Γ of multiplicative order 2. Let $\xi = (a_0, a_1, \ldots, a_{N-1}), \eta = (b_0, b_1, \ldots, b_{N-1}) \in \Gamma^N$. Then the *Euclidean inner product* and the *Hermitian inner product* of ξ and η is defined by

$$[\xi, \eta]_E = \sum_{j=0}^{N-1} a_j b_j$$

and

$$[\xi, \eta]_H = \sum_{j=0}^{N-1} a_j \cdot \sigma(b_j),$$

respectively.

Let $\mathcal{C}$ be a linear code of length N over Γ. The *Euclidean dual code* (resp. *Hermitian dual code*) is defined by

$$\mathcal{C}^{\perp_E} = \{\xi \in \Gamma^N \mid [\xi, \eta]_E = 0,\ \forall \eta \in \mathcal{C}\}$$

$$(\text{resp. } \mathcal{C}^{\perp_H} = \{\xi \in \Gamma^N \mid [\xi, \eta]_H = 0,\ \forall \eta \in \mathcal{C}\}).$$

If $\mathcal{C}^{\perp_E} = \mathcal{C}$ (resp. $\mathcal{C}^{\perp_H} = \mathcal{C}$), $\mathcal{C}$ is called an *Euclidean self-dual code* (resp. *Hermitian self-dual code*) over Γ. In general, it is difficult to construct all Euclidean (Hermitian) self-dual codes of arbitrary length over Γ. To make such construction feasible, an effective way of constructing self-dual codes is the use of linear codes with some specific algebraic structures.

Let $\gamma \in \Gamma^{\times}$. The linear code $\mathcal{C}$ is said to be γ-*constacyclic* if

$$(\gamma c_{N-1}, c_0, c_1, \ldots, c_{N_2}) \in \mathcal{C},\ \forall (c_0, c_1, \ldots, c_{N-1}) \in \mathcal{C}.$$

In particular, $\mathcal{C}$ is called a *cyclic code* (resp. *negacyclic code*) if $\gamma = 1$ (resp. $\gamma = -1$).

Let $\frac{\Gamma[x]}{\langle x^N - \gamma \rangle} = \{\sum_{j=0}^{N-1} a_j x^j \mid a_j \in \Gamma,\ j = 0, 1, \ldots, N-1\}$ in which the arithmetic is done modulo $x^N - \gamma$. As usual, we can regard γ-constacyclic codes of length N over Γ with ideals of the ring $\frac{\Gamma[x]}{\langle x^N - \gamma \rangle}$ under the Γ-linear isomorphism from Γ^N onto $\frac{\Gamma[x]}{\langle x^N - \gamma \rangle}$ defined by:

$$(a_0, a_1, \ldots, a_{N-1}) \mapsto a_0 + a_1 x + \ldots + a_{N-1} x^{N-1}$$

for all $a_j \in \Gamma$ and $j = 0, 1, \ldots, N-1$. Moreover, let $\text{char}(\Gamma)$ be the characteristic of Γ. Then ideals of $\frac{\Gamma[x]}{\langle x^N - \gamma \rangle}$ are called *simple-root* γ-*constacyclic codes* when $\gcd(\text{char}(\Gamma), N) = 1$, and *repeated-root* γ-*constacyclic codes* otherwise.

In this paper, let $\mathbb{F}_{p^m}$ be the finite field of p^m elements, where p is a prime number, and set

$$R = \mathbb{F}_{p^m}[u]/\langle u^2 \rangle = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} = \{a + bu \mid a, b \in \mathbb{F}_{p^m}\}\ (u^2 = 0).$$

Then R is a finite chain ring and every invertible element in R is of the form: $a + bu$, where $a, b \in \mathbb{F}_{p^m}$ and $a \neq 0$. Now, we illustrate how to obtain self-dual codes over $\mathbb{F}_{p^m}$ from self-dual codes over R:

Assume that p is odd. Then $p^m \equiv 1 \pmod 4$ for any positive integer m when $p \equiv 1 \pmod 4$; and $p^m \equiv 1 \pmod 4$ for any even positive integer m when $p \equiv 3 \pmod 4$. Now, we let $\mathbb{F}_{p^m}$ be the finite field satisfying $p^m \equiv 1 \pmod 4$, let ζ be a primitive element of $\mathbb{F}_{p^m}$ and set $\sqrt{-1} = \zeta^{\frac{p^m-1}{4}} \in \mathbb{F}_{p^m}$. We define a map $\phi : R \mapsto \mathbb{F}_{p^m}^2$ by

$$\phi(\xi) = (b, \sqrt{-1}(a+b)),\ \forall \xi = a + bu \in R \text{ where } a, b \in \mathbb{F}_{p^m},$$

and extend this map to a Gray map from R^N onto $\mathbb{F}_{p^m}^{2N}$ by:

$$\phi(\xi_0, \xi_1, \ldots, \xi_{N-1}) = (\phi(\xi_0), \phi(\xi_1), \ldots, \phi(\xi_{N-1})),\ \forall \xi_i \in R.$$

Then we know the following conclusions (cf. [11]):

1. If $\mathcal{C}$ is an Euclidean self-dual code of length N over R, $\phi(\mathcal{C})$ is an Euclidean self-dual code of length $2N$ over $\mathbb{F}_{p^m}$. Moreover, the Hamming weight (distance) distribution of $\phi(\mathcal{C})$ is the same as the Lee weight (distance) distribution of $\mathcal{C}$.

2. If $\mathcal{C}$ is a cyclic code of length N over R, $\phi(\mathcal{C})$ is a 2-quasi-cyclic code of length $2N$ over $\mathbb{F}_{p^m}$.

Hence it is feasible to construct self-dual codes from constacyclic codes over R. There are many studies on constacyclic codes of length N over rings $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, for various prime p, positive integer m and some positive integer N. See [1, 3, 5–8, 12–22, 36], for example.

Kim and Lee [33] found all the dual codes of cyclic codes over the ring $\mathbb{Z}_p[u]/\langle u^3\rangle$ of length p^k for every prime p, completely determined the generators of all the cyclic self-dual codes over the ring $\mathbb{Z}_2[u]/\langle u^3\rangle$ of length 2^k and obtained a mass formula for counting these self-dual cyclic self-dual codes.

In particular, the following results about self-dual and repeated-root cyclic (negacyclic) codes over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ have been obtained:

- The formulas to count *the number of Euclidean self-dual cyclic codes and Hermitian self-dual cyclic codes with length* p^s *over* R, respectively, were given by Choosuwan et al. [13].
- Dinh et al. determined *the number of Euclidean self-dual cyclic codes of length* p^s *over* R by [21, Corollary 4.17].
- *A clear discriminant condition for the Euclidean self-duality of any cyclic code and negacyclic code of length* $p^s n$ *over* R was provided ([7, Theorem 5.3]), for any positive integer n satisfying $\gcd(p, n) = 1$.
- Let $p = 2$ and $R = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$. *An efficient method for the construction of all distinct Euclidean self-dual cyclic codes with length* 2^s *over* R and *a calculation method to obtain all distinct Euclidean self-dual cyclic codes of length* $2^s n$ *over* R was given in [9] and [10], respectively.

However, the methods used in [9] and [10] require that the characteristic of the finite field $\mathbb{F}_{2^m}$ is 2 and can not be applied when the characteristic is odd. The paper [10] gives a constructive algorithm to get all distinct Euclidean self-dual cyclic codes of arbitrary even length over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ but not an explicit expression to present all these self-dual cyclic codes.

From now on, let p be an odd prime and let $n > 1$ be an integer satisfying $\gcd(p, n) = 1$. Using the discrete Fourier Transform and an argument paralleling to the one used in [28, Proposition 4.5], we see that all Euclidean self-dual cyclic codes of length $p^s n$ over R can be determined by the following three classes of codes:

1. Euclidean self-dual cyclic codes (and negacyclic codes) of length p^s over R. This class of codes has been completely determined in [11].
2. Hermitian self-dual cyclic codes of length p^s over Galois extension rings of R with even degrees.
3. Cyclic codes of length p^s over Galois extension rings of R and their Euclidean dual codes. This work has been done, see Lemma 2 of this paper or [7, Corollary 7.1].

In order to give an explicit expression for all Euclidean self-dual cyclic codes of length $p^s n$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, we need to determine the codes of Class 2.

- In [11], for any integer $m \geq 1$, the key idea is to present all distinct Euclidean self-dual cyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ by solving one class of homogeneous system of linear equations over the finite field $\mathbb{F}_{p^m}$.
- Here, for any even integer $m \geq 2$, in order to express explicitly all Hermitian self-dual cyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, we need to solve two classes of homogeneous system of linear equations over the subfield $\mathbb{F}_{p^{\frac{m}{2}}}$ of $\mathbb{F}_{p^m}$ and represent precisely their solutions by use of binomial coefficients.

The present paper is organized as follows. In Sect. 2, we review some known results for cyclic codes and their Euclidean dual codes of length p^s over the ring $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and give an explicit description for Hermitian self-dual cyclic codes of length p^s over R, where m is even. In Sect. 3, we represent all distinct Hermitian self-dual cyclic codes of length p^s over R, using column vectors of Kronecker products of matrices with specific types. On this basis, we provide an explicit expression to present precisely all these Hermitian self-dual cyclic codes, using binomial coefficients. In Sect. 4, we list all distinct Hermitian self-dual cyclic codes of length 3^s over $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m}$ for $s = 1, 2, 3$ and all distinct Hermitian self-dual cyclic codes of length 5^2 over $\mathbb{F}_{5^m} + u\mathbb{F}_{5^m}$. Section 5 concludes the paper.

2 Preliminaries

This section begins with necessary notations and conclusions for the finite field $\mathbb{F}_{p^m}$ and the ring $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ ($u^2 = 0$). Then we do the following:

1. Give a necessary and sufficient condition for a code over R to be Hermitian self-dual (Lemma 1).
2. Review some known results for the representation of cyclic codes and their Euclidean dual codes of length p^s over R (Lemma 2).
3. Give an explicit description for all Hermitian self-dual cyclic codes of length p^s over R (Theorem 1).

Let p be an odd prime number, m and s be positive integers with $2|m$. We let ζ be a primitive element of $\mathbb{F}_{p^m}$. Then $\zeta \in \mathbb{F}_{p^m}$ and $\mathrm{ord}(\zeta) = p^m - 1 = (p^{\frac{m}{2}})^2 - 1$. This implies $\mathrm{ord}(\zeta^{p^{\frac{m}{2}}-1}) = p^{\frac{m}{2}} + 1$ and $\mathrm{ord}(\zeta^{p^{\frac{m}{2}}+1}) = p^{\frac{m}{2}} - 1$.

By [29, Corollary 2.1] or [2], every automorphism of the finite chain ring $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ is given by:

$$\sigma_{i,\varepsilon} : a + bu \mapsto a^{p^i} + \varepsilon b^{p^i} u \ (\forall a, b \in \mathbb{F}_{p^m}),$$

where $0 \le i \le m-1$ and $\varepsilon \in \mathbb{F}_{p^m}^{\times}$. Obviously, the automorphism $\sigma_{i,\varepsilon}$ has multiplicative order 2 if and only if: $i \ne 0$ and for any $a, b \in \mathbb{F}_{p^m}$,

$$a^{p^{2i}} + \varepsilon \cdot \varepsilon^{p^i} b^{p^{2i}} u = (a^{p^i})^{p^i} + \varepsilon(\varepsilon b^{p^i})^{p^i} u = \sigma_{i,\varepsilon}^2(a + bu) = a + bu.$$

These conditions are equivalent to $\varepsilon^{p^i+1} = 1$ and $a^{p^{2i}} = a$. Therefore, the number of ring automorphisms on R with multiplicative order 2 is $p^{\frac{m}{2}} + 1$ and all these ring automorphisms are given by: $\sigma_{\frac{m}{2},\zeta^{j(p^{\frac{m}{2}}-1)}}$, where $0 \le j \le p^{\frac{m}{2}}$.

In this paper, we adopt the following notation:

- Assume $2|m$ and set $q = p^{\frac{m}{2}}$. Then

  $$\mathbb{F}_{p^m} = \mathbb{F}_{q^2} = \{0\} \cup \{\zeta^i \mid 0 \le i \le q^2 - 2\} \text{ and } R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}.$$

- Let $\mathbb{F}_q$ be the subfield of $\mathbb{F}_{q^2}$ with q elements. Then

  $$\mathbb{F}_q = \{a \in \mathbb{F}_{q^2} \mid a^q = a\} = \{0\} \cup \{(\zeta^{q+1})^j \mid j = 0, 1, \ldots, q-2\}.$$

- Set $\sigma = \sigma_{\frac{m}{2},1}$. Then $\sigma(a + bu) = a^q + b^q u,\ \forall a, b \in \mathbb{F}_{q^2}$.
- For any vector $\alpha = (a_0, a_1, \ldots, a_{N-1})$, where $a_i \in R$ for all integers $i = 0, 1, \ldots, N-1$, we let $\alpha(x) = \sum_{i=0}^{N-1} a_i x^i \in R[x]$ and define

  $$\sigma(\alpha) = (\sigma(a_0), \sigma(a_1), \ldots, \sigma(a_{N-1})),\ \sigma(\alpha(x)) = \sum_{i=0}^{N-1} \sigma(a_i) x^i.$$

- Let the Hermitian inner product $[-,-]_H$, Hermitian dual codes and Hermitian self-dual codes be defined the same as in Sect. 1 by setting $\sigma = \sigma_{\frac{m}{2},1}$.

First, we give a preliminarily criterion for Hermitian self-dual codes of length N over R:

Lemma 1 *Let $\mathcal{C}$ be a linear code of length N over R. Then $\mathcal{C}$ is Hermitian self-dual if and only if $\mathcal{C}^{\perp_E} = \sigma(\mathcal{C}) = \{\sigma(\alpha) \mid \alpha \in \mathcal{C}\}$.*

Proof Let $\alpha = (a_0, a_1, \ldots, a_{N-1})$, $\beta = (b_0, b_1, \ldots, b_{N-1}) \in R^N$. As $\sigma(\beta) = (\sigma(b_0), \sigma(b_1), \ldots, \sigma(b_{N-1}))$, by the definitions of $[-,-]_E$ and $[-,-]_H$, we have

$$[\alpha, \sigma(\beta)]_E = \sum_{i=0}^{N-1} a_i \cdot \sigma(b_i) = [\alpha, \beta]_H.$$

This implies that $[\alpha, \sigma(\beta)]_E = 0$ if and only if $[\alpha, \beta]_H = 0$.

Now, let $\mathcal{C}^{\perp_E}$ and $\mathcal{C}^{\perp_H}$ be the Euclidean dual code and Hermitian dual code of $\mathcal{C}$, respectively. Then we have

$$[\mathcal{C}, \mathcal{C}^{\perp_E}]_E := \{[\alpha, \beta]_E \mid \alpha \in \mathcal{C},\ \beta \in \mathcal{C}^{\perp_E}\} = \{0\}$$

and $|\mathcal{C}||\mathcal{C}^{\perp_E}| = |R|^N$. Set $\sigma(\mathcal{C}^{\perp_E}) = \{\sigma(\beta) \mid \beta \in \mathcal{C}^{\perp_E}\} \subseteq R^N$. Since σ is a ring automorphism on R of order 2, we have that $|\sigma(\mathcal{C}^{\perp_E})| = |\mathcal{C}^{\perp_E}|$ and

$$[\mathcal{C}, \sigma(\mathcal{C}^{\perp_E})]_H = [\mathcal{C}, \sigma(\sigma(\mathcal{C}^{\perp_E}))]_E = [\mathcal{C}, \mathcal{C}^{\perp_E}]_E = \{0\}.$$

As R is a finite chain ring, we conclude that $\mathcal{C}^{\perp_H} = \sigma\left(\mathcal{C}^{\perp_E}\right)$. From this, we deduce that $\mathcal{C}$ is Hermitian self-dual if and only if $\sigma\left(\mathcal{C}^{\perp_E}\right) = \mathcal{C}^{\perp_H} = \mathcal{C}$. Then by $\sigma^{-1} = \sigma$, the latter condition is equivalent to $\mathcal{C}^{\perp_E} = \sigma(\sigma\left(\mathcal{C}^{\perp_E}\right)) = \sigma(\mathcal{C})$. □

In order to determine all Hermitian self-dual cyclic codes of length p^s over R, by Lemma 1, we need to determine every cyclic code $\mathcal{C}$ and its Euclidean dual code $\mathcal{C}^{\perp_E}$ over R first. Let the ring

$$\mathcal{R} = \frac{R[x]}{\langle x^{p^s} - 1\rangle} = \left\{ \sum_{j=0}^{p^s-1} b_j x^j \mid b_j \in R, 0 \le j \le p^s - 1 \right\}$$

in which the arithmetic is done modulo $x^{p^s} - 1$. As noted in Sect. 1, we regard cyclic codes of length p^s over R as ideals of the ring $\mathcal{R}$.

For any $f(x), g(x) \in \mathcal{R}$, let

$$\langle f(x), g(x)\rangle = \{a(x)f(x) + b(x)g(x) \mid a(x), b(x) \in \mathcal{R}\}$$

be the ideal of $\mathcal{R}$ generated by $f(x)$ and $g(x)$. The following conclusion follows directly from [7, Corollary 7.1].

Lemma 2 *For any positive integers m and l: $1 \le l \le p^s - 1$, let $x^{-1} = x^{p^s-1}$ (mod $(x-1)^l$). Then every cyclic code $\mathcal{C}$ over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ of length p^s and its Euclidean dual code $\mathcal{C}^{\perp_E}$ are given by the following five cases*:

I. $(p^m)^{p^s - \lceil \frac{p^s}{2} \rceil} = p^{\frac{p^s-1}{2}m}$ *codes*:

$\mathcal{C} = \langle (x-1)b(x) + u\rangle$ with $|\mathcal{C}| = p^{p^s m}$; $\mathcal{C}^{\perp_E} = \langle (x-1)\cdot x^{-1}b(x^{-1}) + u\rangle$,

where $b(x) \in (x-1)^{\frac{p^s-1}{2}} \cdot \frac{\mathbb{F}_{p^m}[x]}{\langle (x-1)^{p^s-1}\rangle}$.

II. $\sum_{k=1}^{p^s-1} p^{(p^s-k-\lceil \frac{1}{2}(p^s-k)\rceil)m}$ *codes*:

$\mathcal{C} = \langle (x-1)^{k+1}b(x) + u(x-1)^k\rangle$ with $|\mathcal{C}| = p^{(p^s-k)m}$;

$\mathcal{C}^{\perp_E} = \langle (x-1)\cdot x^{-1}b(x^{-1}) + u, (x-1)^{p^s-k}\rangle$,

where $b(x) \in (x-1)^{\lceil \frac{p^s-k}{2}\rceil - 1} \cdot \frac{\mathbb{F}_{p^m}[x]}{\langle (x-1)^{p^s-k-1}\rangle}$ and $1 \le k \le p^s - 1$.

III. $p^s + 1$ *codes*:

$$\mathcal{C} = \langle (x-1)^k \rangle \text{ with } |\mathcal{C}| = p^{2(p^s-k)m};\ \mathcal{C}^{\perp_E} = \langle (x-1)^{p^s-k} \rangle,$$

where $0 \le k \le p^s$.

IV. $\sum_{t=1}^{p^s-1} p^{(t-\lceil \frac{t}{2} \rceil)m}$ *codes*:

$$\mathcal{C} = \langle (x-1)b(x) + u, (x-1)^t \rangle \text{ with } |\mathcal{C}| = p^{(2\cdot p^s - t)m};$$
$$\mathcal{C}^{\perp_E} = \langle (x-1)^{p^s-t+1} \cdot x^{-1}b(x^{-1}) + u(x-1)^{p^s-t} \rangle,$$

where $b(x) \in (x-1)^{\lceil \frac{t}{2} \rceil - 1} \cdot \frac{\mathbb{F}_{p^m}[x]}{\langle (x-1)^{t-1} \rangle}$ and $1 \le t \le p^s - 1$.

V. $\sum_{k=1}^{p^s-2} \sum_{t=1}^{p^s-k-1} p^{(t-\lceil \frac{t}{2} \rceil)m}$ *codes*:

$$\mathcal{C} = \langle (x-1)^{k+1}b(x) + u(x-1)^k, (x-1)^{k+t} \rangle \text{ with } |\mathcal{C}| = p^{(2\cdot p^s - 2k - t)m};$$
$$\mathcal{C}^{\perp_E} = \langle (x-1)^{p^s-k-t+1} \cdot x^{-1}b(x^{-1}) + u(x-1)^{p^s-k-t}, (x-1)^{p^s-k} \rangle,$$

where $b(x) \in (x-1)^{\lceil \frac{t}{2} \rceil - 1} \cdot \frac{\mathbb{F}_{p^m}[x]}{\langle (x-1)^{t-1} \rangle}$, $1 \le t \le p^s - k - 1$ and $1 \le k \le p^s - 2$.

Using Lemma 1, we can give an explicit description for the Hermitian self-dual codes which are cyclic codes listed by Lemma 2.

First, as $|\frac{R[x]}{\langle x^{p^s}-1 \rangle}| = |R^{p^s}| = |R|^{p^s} = (p^{p^s m})^2 = q^{4p^s}$, every Hermitian self-dual cyclic code $\mathcal{C}$ of length p^s over R must contain $|\mathcal{C}| = q^{2p^s}$ codewords. From this, we deduce that there is no Hermitian self-dual codes in Cases II, III and IV of Lemma 2. Hence we only need to consider the following two cases:

(†) Let $\mathcal{C} = \langle (x-1)b(x) + u \rangle$ be a code in Case I, where $b(x) \in (x-1)^{\frac{p^s-1}{2}} \cdot \frac{\mathbb{F}_{q^2}[x]}{\langle (x-1)^{p^s-1} \rangle}$. Then by $\sigma(c) = c^q = c$ for all $c \in \mathbb{F}_q$, we have

$$\sigma(\mathcal{C}) = \langle \sigma((x-1)b(x) + u) \rangle = \langle (x-1) \cdot \sigma(b(x)) + u \rangle.$$

From this, by Lemma 1 and $\mathcal{C}^{\perp_E} = \langle (x-1) \cdot x^{-1}b(x^{-1}) + u \rangle$, we deduce that the code $\mathcal{C}$ is a Hermitian self-dual code if and only if $\sigma(b(x)) = x^{-1}b(x^{-1})$ in the ring $\frac{\mathbb{F}_{q^2}[x]}{\langle (x-1)^{p^s-1} \rangle}$, i.e., $\sigma(b(x)) - x^{-1}b(x^{-1}) \equiv 0 \pmod{(x-1)^{p^s-1}}$.

(‡) Let $\mathcal{C} = \langle (x-1)^{k+1}b(x) + u(x-1)^k, (x-1)^{k+t} \rangle$ be a code in Case V, where $b(x) \in (x-1)^{\lceil \frac{t}{2} \rceil - 1} \cdot \frac{\mathbb{F}_{q^2}[x]}{\langle (x-1)^{t-1} \rangle}$, $1 \le t \le p^s - k - 1$ and $1 \le k \le p^s - 2$. Then $\sigma(\mathcal{C}) = \left\langle (x-1)^{k+1} \cdot \sigma(b(x)) + u(x-1)^k, (x-1)^{k+t} \right\rangle$. From this, by Lemma 1, $|\mathcal{C}| = q^{2(2\cdot p^s - 2k - t)}$ and

$$\mathcal{C}^{\perp_E} = \langle (x-1)^{p^s-k-t+1} \cdot x^{-1}b(x^{-1}) + u(x-1)^{2^s-k-t}, (x-1)^{2^s-k} \rangle,$$

we deduce that $\mathcal{C}^{\perp_H} = \mathcal{C}$ if and only if: $2 \cdot p^s - 2k - t = p^s$ and $b(x)$ satisfies $\sigma(b(x)) = x^{-1}b(x^{-1})$ in the ring $\frac{\mathbb{F}_{q^2}[x]}{\langle (x-1)^{t-1} \rangle}$. The latter is equivalent to

$$\sigma(b(x)) - x^{-1}b(x^{-1}) \equiv 0 \pmod{(x-1)^{t-1}}.$$

The former is equivalent to that $t = p^s - 2k$, $\left\lceil \frac{t}{2} \right\rceil = \frac{p^s-2k}{2} = \frac{p^s-1}{2} - k + 1$ and $1 \le k \le \frac{p^s-1}{2}$.

Summing up the above discussion, we obtain an explicit description for all Hermitian self-dual cyclic codes of length p^s over R:

Theorem 1 *All distinct Hermitian self-dual cyclic codes of length p^s over $R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$ are given by*:

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

where $0 \le k \le \frac{p^s-1}{2}$, *and* $b(x) = \sum_{i=\frac{p^s-1}{2}-k}^{p^s-2k-2} b_i(x-1)^i$ *with* $b_i \in \mathbb{F}_{q^2}$, *for all* $\frac{p^s-1}{2} - k \le i \le p^s - 2k - 2$, *satisfying the following condition*:

$$\sigma(b(x)) - x^{-1} b(x^{-1}) \equiv 0 \pmod{(x-1)^{p^s-2k-1}}. \tag{1}$$

Proof By $(x-1)^{p^s} = x^{p^s} - 1 = 0$ in $\mathcal{R} = \frac{R[x]}{\langle x^{p^s}-1 \rangle}$, the two cases (†) and (‡) can be combined into one case below:

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

where $t = p^s - 2k$, $0 \le k \le \frac{p^s-1}{2}$ and $b(x) \in (x-1)^{\lceil \frac{t}{2} \rceil - 1} \cdot \frac{\mathbb{F}_{q^2}[x]}{\langle (x-1)^{t-1} \rangle}$ satisfying Equation (1). As $\left\lceil \frac{t}{2} \right\rceil - 1 = \left\lceil \frac{p^s-2k}{2} \right\rceil - 1 = \frac{p^s+1}{2} - k - 1 = \frac{p^s-1}{2} - k$, we get

$$(x-1)^{\lceil \frac{t}{2} \rceil - 1} \cdot \frac{\mathbb{F}_{q^2}[x]}{\langle (x-1)^{t-1} \rangle} = (x-1)^{\frac{p^s-1}{2}-k} \cdot \frac{\mathbb{F}_{q^2}[x]}{\langle (x-1)^{p^s-2k-1} \rangle}.$$

Hence there is a unique vector $(b_{\frac{p^s-1}{2}-k}, b_{\frac{p^s-1}{2}-k+1}, \ldots, b_{p^s-2k-2}) \in \mathbb{F}_{q^2}^{\frac{p^s-1}{2}-k}$ such that $b(x) = \sum_{i=\frac{p^s-1}{2}-k}^{p^s-2k-2} b_i(x-1)^i$ and $b(x)$ satisfies Equation (1). □ □

Using Theorem 1, in order to present explicitly all Hermitian self-dual cyclic codes of length p^s over $\mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$, we only need to find the solutions $b(x)$ to the congruence relation (1) above.

3 Hermitian self-dual cyclic codes of length p^s over $\mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$

In this section, we give an explicit construction and representation for all distinct Hermitian self-dual cyclic codes of length p^s over $\mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$.

We introduce the necessary notation. Let $A = (a_{ij})$ and B be matrices over $\mathbb{F}_{p^m}$ of sizes $k \times t$ and $l \times v$ respectively. The *Kronecker product* of A and B is defined by $A \otimes B = (a_{ij}B)$, which is a matrix over $\mathbb{F}_{p^m}$ of size $kl \times tv$. Let A^{tr} be the transpose of A in this paper.

For any positive integer $\lambda \le s$, we define a $p^\lambda \times p^\lambda$ lower triangular matrix G_{p^λ} over $\mathbb{F}_p$ as follows (cf. [11]):

$$G_{p^\lambda} = \begin{pmatrix} g_{1,1}^{(p^\lambda)} & 0 & \cdots & 0 \\ g_{2,1}^{(p^\lambda)} & g_{2,2}^{(p^\lambda)} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ g_{p^\lambda,1}^{(p^\lambda)} & g_{p^\lambda,2}^{(p^\lambda)} & \cdots & g_{p^\lambda,p^\lambda}^{(p^\lambda)} \end{pmatrix} (\mathrm{mod}\ p),$$

where for any integers $i, j, 1 \le i, j \le p^\lambda$, we let

$$g_{i,j}^{(p^\lambda)} = (-1)^{j-1} \begin{pmatrix} p^\lambda - j \\ i - j \end{pmatrix}, \text{ with } \begin{pmatrix} p^\lambda - j \\ i - j \end{pmatrix} = 0 \text{ if } i < j. \tag{2}$$

Then by [11, Proposition 2 and Theorem 1 (ii)], we have the following:

Lemma 3 *Let λ be any positive integer and set $G_{p^0} = 1$.*

(i) *The matrix G_{p^λ} has the Kronecker product structure as follows*: $G_{p^\lambda} = G_p \otimes G_{p^{\lambda-1}}$, *i.e.*,

$$G_{p^\lambda} = \begin{pmatrix} g_{1,1}^{(p)} G_{p^{\lambda-1}} & 0 & \cdots & 0 \\ g_{2,1}^{(p)} G_{p^{\lambda-1}} & g_{2,2}^{(p)} G_{p^{\lambda-1}} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ g_{p,1}^{(p)} G_{p^{\lambda-1}} & g_{p,2}^{(p)} G_{p^{\lambda-1}} & \cdots & g_{p,p}^{(p)} G_{p^{\lambda-1}} \end{pmatrix},$$

where $g_{i,i}^{(p)} = (-1)^{i-1} \begin{pmatrix} p - i \\ i - i \end{pmatrix} = (-1)^{i-1}$ for all integers $i, 1 \le i \le p$.

(ii) *Let $1 \le l \le p^s - 1$ and assume that λ is the least positive integer such that $1 \le l \le p^\lambda$. Let G_l be the submatrix of size $l \times l$ in the upper left corner of G_{p^λ} defined by*

$$\begin{pmatrix} G_l & 0 \\ * & * \end{pmatrix} = G_{p^\lambda}. \tag{3}$$

Then G_l is a lower triangular matrix over $\mathbb{F}_p$ satisfying

$$G_l^2 = I_l, \ \mathrm{rank}(G_l - I_l) = \left\lfloor \frac{l}{2} \right\rfloor \text{ and } \mathrm{rank}(G_l + I_l) = \left\lceil \frac{l}{2} \right\rceil.$$

(iii) *Let $x^{-1} = x^{p^s-1}\ (mod\ (x-1)^l)$. For any $B_l = (b_0, b_1, \ldots, b_{l-1})^{\mathrm{tr}} \in \mathbb{F}_{q^2}^l$, we set $b(x) = \sum_{i=0}^{l-1} b_i (x-1)^i$. Then*

$$x^{-1} b(x^{-1}) \equiv (1, (x-1), \ldots, (x-1)^{l-1})(G_l B_l)\ (\mathrm{mod}\ (x-1)^l).$$

For any fixed integer $l, 1 \le l \le p^s - 1$, we assume that λ is the least positive integer such that $1 \le l \le p^\lambda$. Let G_l be the matrix defined by Equation (3). In this paper, we mark the rows of the matrices $G_l + I_l$ and $G_l - I_l$ from top to bottom in turn: 1st row, 2nd row, …, lth row; and mark the columns of $G_l + I_l$ and $G_l - I_l$ from left to right

in turn: 1st column, 2nd column, …, lth column. Moreover, we adopt the following notation:

- Let $Y_j^{[1,l]}$ be the jth column vector of the matrix $G_l + I_l$. Then $Y_j^{[1,l]} \in \mathbb{F}_p^l$ for all $j = 1, 2, \ldots, l$ and $G_l + I_l = (Y_1^{[1,l]}, Y_2^{[1,l]}, \ldots, Y_l^{[1,l]})$.
- For any integers δ and j, where $\lceil \frac{\delta}{2} \rceil + 1 \le j \le \lceil \frac{l}{2} \rceil$ and $0 \le \delta < l \le p^s - 1$, define the truncated vector $Y_{2j-1}^{[\delta+1,l]}$ of $Y_{2j-1}^{[1,l]}$ by

$$Y_{2j-1}^{[\delta+1,l]} = \begin{pmatrix} g_{\delta+1,2j-1} \\ g_{\delta+2,2j-1} \\ \vdots \\ g_{l,2j-1} \end{pmatrix}, \text{ if } Y_{2j-1}^{[1,l]} = \left(\begin{array}{c} g_{1,2j-1} \\ \vdots \\ g_{\delta,2j-1} \\ \hline g_{\delta+1,2j-1} \\ g_{\delta+2,2j-1} \\ \vdots \\ g_{l,2j-1} \end{array}\right).$$

- Let $\xi_j^{[1,l]}$ be the jth column vector of the matrix $G_l - I_l$. Then $\xi_j^{[1,l]} \in \mathbb{F}_p^l$ for all $j = 1, 2, \ldots, l$ and $G_l - I_l = (\xi_1^{[1,l]}, \xi_2^{[1,l]}, \ldots, \xi_l^{[1,l]})$.
- For any integers δ and t, where $\lfloor \frac{\delta}{2} \rfloor + 1 \le t \le \lfloor \frac{l}{2} \rfloor$ and $0 \le \delta < l \le p^s - 1$, define the truncated vector $\xi_{2t}^{[\delta+1,l]}$ of $\xi_{2t}^{[1,l]}$ by

$$\xi_{2t}^{[\delta+1,l]} = \begin{pmatrix} h_{\delta+1,2t} \\ h_{\delta+2,2t} \\ \vdots \\ h_{l,2t} \end{pmatrix}, \text{ if } \xi_{2t}^{[1,l]} = \left(\begin{array}{c} h_{1,2t} \\ \vdots \\ h_{\delta,2t} \\ \hline h_{\delta+1,2t} \\ h_{\delta+2,2t} \\ \vdots \\ h_{l,2t} \end{array}\right).$$

Lemma 4 *Using the notation above, we have the following conclusions*:

(i) ([11, *Theorem* 1 (*iv*) *and its proof*]) *The set* $\{Y_{2j-1}^{[1,l]} \mid j = 1, 2, \ldots, \lceil \frac{l}{2} \rceil\}$ *is a maximal* $\mathbb{F}_q$*-linearly independent system of the vectors* $Y_1^{[1,l]}, Y_2^{[1,l]}, \ldots, Y_l^{[1,l]}$.

(ii) ([11, *Theorem* 2 *and its proof*]) *The set* $\{Y_{2j-1}^{[\delta+1,l]} \mid \lceil \frac{\delta}{2} \rceil + 1 \le j \le \lceil \frac{l}{2} \rceil\}$ *is a linear independent subset of* $\mathbb{F}_q^{l-\delta}$ *containing* $\lceil \frac{l}{2} \rceil - \lceil \frac{\delta}{2} \rceil$ *vectors*.

(iii) *The set* $\{\xi_{2t}^{[1,l]} \mid t = 1, 2, \ldots, \lfloor \frac{l}{2} \rfloor\}$ *is a maximal* $\mathbb{F}_q$*-linear independent system of* $\xi_1^{[1,l]}, \xi_2^{[1,l]}, \ldots, \xi_l^{[1,l]}$.

(iv) *The set* $\{\xi_{2t}^{[\delta+1,l]} \mid \lfloor \frac{\delta}{2} \rfloor + 1 \le t \le \lfloor \frac{l}{2} \rfloor\}$ *is a linear independent subset of* $\mathbb{F}_q^{l-\delta}$ *containing* $\lfloor \frac{l}{2} \rfloor - \lfloor \frac{\delta}{2} \rfloor$ *vectors*.

Proof (iii) By Lemma 3.1 (ii), we have $\operatorname{rank}(G_l - I_l) = \lfloor \frac{l}{2} \rfloor$. This implies that $\lfloor \frac{l}{2} \rfloor$ is the rank of the vectors $\xi_1^{[1,l]}, \xi_2^{[1,l]}, \ldots, \xi_l^{[1,l]}$. From this, by

$$\begin{pmatrix} (\xi_1^{[1,l]}, \ldots, \xi_l^{[1,l]}) & 0 \\ * & * \end{pmatrix} = \begin{pmatrix} G_l - I_l & 0 \\ * & * \end{pmatrix} = G_{p^\lambda} - I_{p^\lambda}$$

and $G_{p^\lambda} - I_{p^\lambda} = \begin{pmatrix} 0 & & & & & \\ * & -2 & & & & \\ * & * & 0 & & & \\ \vdots & \vdots & \vdots & \ddots & & \\ * & * & * & \ldots & -2 & \\ * & * & * & \ldots & * & 0 \end{pmatrix}$, we deduce that the subset of vectors $\{\xi_{2t}^{[1,l]} \mid t = 1, 2, \ldots, \lfloor \frac{l}{2} \rfloor\}$ is a maximal $\mathbb{F}_q$-linear independent system of $\xi_1^{[1,l]}, \xi_2^{[1,l]}, \ldots, \xi_l^{[1,l]}$.

(iv) By the proof of (iii), we have

$$\xi_{2t}^{[1,l]} = \begin{pmatrix} \mathbf{0}_{(2t-1)\times 1} \\ -2 \\ h_{2t+1,2t} \\ \vdots \\ h_{l,2t} \end{pmatrix} \text{ for all } 1 \le t \le \left\lfloor \frac{l}{2} \right\rfloor. \tag{4}$$

Let t be an integer satisfying $2t - 1 \ge \delta$, i.e., $t \ge \lfloor \frac{\delta}{2} \rfloor + 1$. Then

$$\xi_{2t}^{[\delta+1,l]} = \begin{pmatrix} \mathbf{0}_{(2t-1-\delta)\times 1} \\ -2 \\ h_{2t+1,2t} \\ \vdots \\ h_{l,2t} \end{pmatrix} \in \mathbb{F}_q^{l-\delta},$$

where $\mathbf{0}_{(2t-1-\delta)\times 1}$ is the zero matrix of size $(2t - 1 - \delta) \times 1$, for all $\lfloor \frac{\delta}{2} \rfloor + 1 \le t \le \lfloor \frac{l}{2} \rfloor$. From these, we deduce that the set $\{\xi_{2t}^{[\delta+1,l]} \mid \lfloor \frac{\delta}{2} \rfloor + 1 \le t \le \lfloor \frac{l}{2} \rfloor\}$ is a linear independent subset of $\mathbb{F}_q^{l-\delta}$ containing $\lfloor \frac{l}{2} \rfloor - \lfloor \frac{\delta}{2} \rfloor$ vectors. □

Using the notation in Sect. 2, 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: $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q$, $\forall \alpha \in \mathbb{F}_{q^2}$. For any $a \in \mathbb{F}_q$, let

$$\mathrm{Tr}^{-1}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a) = \{\alpha \in \mathbb{F}_{q^2} \mid \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q = a\}.$$

Then $|\mathrm{Tr}^{-1}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(0)| = q$ (cf. [35, Corollary 7.17 (i)]). Further, since $q = p^{\frac{m}{2}}$ is odd, we have $\mathbb{F}_q \cap \mathrm{Tr}^{-1}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(0) = \{0\}$.

The following notation plays a key role in this paper:

• Let w be a fixed nonzero element in $\mathrm{Tr}^{-1}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(0)$. For example, we can choose $w = \zeta^{\frac{q+1}{2}}$. Then $w^q = -w$ and $\{1, w\}$ is a basis of the $\mathbb{F}_q$-linear space $\mathbb{F}_{q^2}$. This implies

$$\mathbb{F}_{q^2} = \{c + dw \mid c, d \in \mathbb{F}_q\}. \tag{5}$$

By [13, Corollary 25], the number of all distinct Hermitian self-dual cyclic codes of length p^s over R is given by: $\mathrm{NH}(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}, p^s)=\frac{q^{\frac{p^s-1}{2}+1}-1}{q-1}$. Now, we give an efficient construction for these Hermitian self-dual codes:

Theorem 2 *Using the notation above, all* $\frac{q^{\frac{p^s-1}{2}+1}-1}{q-1}$ *Hermitian self-dual cyclic codes of length* p^s *over* $R=\mathbb{F}_{q^2}+u\mathbb{F}_{q^2}$ *are given by the following three cases*:

I. 1 code: $\langle u(x-1)^{\frac{p^s-1}{2}}, (x-1)^{\frac{p^s+1}{2}}\rangle$.

II. q codes: $\langle (x-1)^{\frac{p^s+1}{2}}(-2)cw+u(x-1)^{\frac{p^s-3}{2}}, (x-1)^{\frac{p^s+3}{2}}\rangle$, where $c\in\mathbb{F}_q$.

III. For each integer k, $0\le k\le \frac{p^s-1}{2}-2$, there are exactly $q^{\frac{p^s-1}{2}-k}$ codes:

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

where $b(x)=\sum_{i=0}^{\frac{p^s-3}{2}-k} b_i(x-1)^i$ *and* $b_0, b_1, \ldots, b_{\frac{p^s-3}{2}-k}\in\mathbb{F}_{q^2}$ *are given by*:

$$(b_0, b_1, \ldots, b_{\frac{p^s-3}{2}-k})^{\mathrm{tr}} = \sum_{\lceil\frac{p^s-1-2k}{4}\rceil+1\le j\le\frac{p^s-1}{2}-k} a_{2j-1}\Upsilon_{2j-1}^{[\frac{p^s-1}{2}-k+1, p^s-2k-1]} + \sum_{\lfloor\frac{p^s-1-2k}{4}\rfloor+1\le t\le\frac{p^s-1}{2}-k} c_{2t}\cdot w\xi_{2t}^{[\frac{p^s-1}{2}-k+1, p^s-2k-1]},$$

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

$$\left\lceil\frac{p^s-1-2k}{4}\right\rceil+1\le j\le\frac{p^s-1}{2}-k,\ \left\lfloor\frac{p^s-1-2k}{4}\right\rfloor+1\le t\le\frac{p^s-1}{2}-k,$$

respectively.

Proof *Case I*. Obviously, the code $\langle u(x-1)^{\frac{p^s-1}{2}}, (x-1)^{\frac{p^s+1}{2}}\rangle$ is a Hermitian self-dual cyclic code of length p^s over R.

Case II. When $k=\frac{p^s-1}{2}-1=\frac{p^s-3}{2}$, one can easily verify that

$$\langle (x-1)^{\frac{p^s+1}{2}}b(x)+u(x-1)^{\frac{p^s-3}{2}}, (x-1)^{\frac{p^s+3}{2}}\rangle,$$

is Hermitian self-dual if and only if $b(x)=(-2)c_2w$, where $c_2\in\mathbb{F}_q$.

Case III. Let k be any fixed integer, $0\le k\le\frac{p^s-1}{2}-2=\frac{p^s-3}{2}-1$, and we assume

$$b_i=b_{i,0}+b_{i,1}w\in\mathbb{F}_{q^2},\ \text{ where }\ b_{i,0}, b_{i,1}\in\mathbb{F}_q,\ i=0,1,\ldots,\frac{p^s-3}{2}-k.$$

Then by $b_i\in\mathbb{F}_{q^2}$ and $w^q=-w$ where $q=p^{\frac{m}{2}}$, it follows that

$$\sigma(b_i) = b_i^q = b_{i,0}^q + b_{i,1}^q w^q = b_{i,0} - b_{i,1} w,\ 0 \le i \le \frac{p^s-3}{2} - k.$$

We set $\widehat{b}(x) = (x-1)^{\frac{p^s-1}{2}-k} b(x)$, where $b(x) = \sum_{i=0}^{\frac{p^s-3}{2}-k} b_i (x-1)^i$. This implies $\widehat{b}(x) = \sum_{i=\frac{p^s-1}{2}-k}^{p^s-2k-2} b_i (x-1)^i$.

From now on, we adopt the following notation:

- $X_{p^s-2k-1} = (1, (x-1), (x-1)^2, \ldots, (x-1)^{p^s-2k-2})$.
- Let $\mathbf{0}_{\frac{p^s-1}{2}-k}$ be the zero vector in $\mathbb{F}_{q^2}^{\frac{p^s-1}{2}-k}$ and define vectors $B_{p^s-2k-1,0}$ and $B_{p^s-2k-1,1}$ in $\mathbb{F}_q^{p^s-2k-1}$ by: $B_{p^s-2k-1,\lambda} = \begin{pmatrix} \mathbf{0}_{\frac{p^s-1}{2}-k} \\ b_{0,\lambda} \\ b_{1,\lambda} \\ \vdots \\ b_{\frac{p^s-3}{2}-k,\lambda} \end{pmatrix},\ \lambda = 0, 1.$
- Set $B_{p^s-2k-1} = \begin{pmatrix} \mathbf{0}_{\frac{p^s-1}{2}-k} \\ b_0 \\ b_1 \\ \vdots \\ b_{\frac{p^s-3}{2}-k} \end{pmatrix} = B_{p^s-2k-1,0} + wB_{p^s-2k-1,1} \in \mathbb{F}_{q^2}^{p^s-2k-1}$.
- Let $\mathcal{V}_0$ and $\mathcal{V}_1$ be the solution spaces of the following homogeneous system of linear equations over $\mathbb{F}_q$:

$$(G_{p^s-2k-1} - I_{p^s-2k-1})Y = 0 \ \text{ and } \ (G_{p^s-2k-1} + I_{p^s-2k-1})Y = 0,$$

respectively, where $Y = (y_1, y_2, \ldots, y_{p^s-2k-1})^{\mathrm{tr}}$.

Using the above notation, we have

$$\widehat{b}(x) = X_{p^s-2k-1} B_{p^s-2k-1} = X_{p^s-2k-1}(B_{p^s-2k-1,0} + wB_{p^s-2k-1,1}).$$

This implies

$$\begin{aligned} \sigma(\widehat{b}(x)) =& X_{p^s-2k-1} \cdot \sigma\left(B_{p^s-2k-1,0} + wB_{p^s-2k-1,1}\right) \\ =& X_{p^s-2k-1} \cdot \left(B_{p^s-2k-1,0} - wB_{p^s-2k-1,1}\right). \end{aligned}$$

On the other hand, by Lemma 3 (iii), it follows that

$$\begin{aligned} x^{-1} b(x^{-1}) \equiv& X_{p^s-2k-1} \cdot \left(G_{p^s-2k-1} B_{p^s-2k-1}\right) \\ \equiv& X_{p^s-2k-1} \cdot \left(G_{p^s-2k-1} B_{p^s-2k-1,0} + wG_{p^s-2k-1} B_{p^s-2k-1,1}\right) \end{aligned}$$

(mod $(x-1)^{p^s-2k-1}$). Now, let $\mathcal{C}_{b(x)}$ be the cyclic code of length p^s over R defined by:

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

By Theorem 1, we see that $\mathcal{C}_{b(x)}$ is a Hermitian self-dual cyclic code if and only if $\widehat{b}(x)$ satisfies: $\sigma(\widehat{b}(x)) \equiv x^{-1}\widehat{b}(x^{-1})\ (\bmod\ (x-1)^{p^s-2k-1})$. Obviously, the latter condition is equivalent to

$$B_{p^s-2k-1,0} - wB_{p^s-2k-1,1} = G_{p^s-2k-1}B_{p^s-2k-1,0} + wG_{p^s-2k-1}B_{p^s-2k-1,1}.$$

By Equation (5), $\{1, w\}$ is a basis of the $\mathbb{F}_q$-linear space $\mathbb{F}_{q^2}$. Hence the above condition is equivalent to $\begin{cases} (G_{p^s-2k-1} - I_{p^s-2k-1})B_{p^s-2k-1,0} = 0; \\ (G_{p^s-2k-1} + I_{p^s-2k-1})B_{p^s-2k-1,1} = 0, \end{cases}$ i.e.,

$$B_{p^s-2k-1,0} \in \mathcal{V}_0 \ \text{ and } \ B_{p^s-2k-1,1} \in \mathcal{V}_1. \tag{6}$$

Using the notation of Equation (3), we set $l = p^s - 2k - 1$. Then l is even, since p is odd. By Lemma 3 (ii), we have $G^2_{p^s-2k-1} = I_{p^s-2k-1}$ and that

$$\operatorname{rank}\left(G_{p^s-2k-1} \pm I_{p^s-2k-1}\right) = \frac{p^s-2k-1}{2} = \frac{p^s-1}{2} - k.$$

This implies

$$\dim_{\mathbb{F}_q}(\mathcal{V}_\lambda) = (p^s-2k-1) - \frac{p^s-2k-1}{2} = \frac{p^s-1}{2} - k, \ \lambda = 0, 1.$$

Therefore, we have the following conclusions:

◇ By $G^2_{p^s-2k-1} = I_{p^s-2k-1}$, it follows that

$$\left(G_{p^s-2k-1} + I_{p^s-2k-1}\right)\left(G_{p^s-2k-1} - I_{p^s-2k-1}\right) = 0.$$

This implies $\left(G_{p^s-2k-1} + I_{p^s-2k-1}\right)\xi_i^{[1,p^s-2k-1]} = 0$ for all integers $i = 1, 2, \ldots, p^s - 2k - 1$. Hence all column vectors of the matrix $G_{p^s-2k-1} - I_{p^s-2k-1}$: $\xi_i^{[1,p^s-2k-1]}$, $1 \le i \le p^s - 2k - 1$, are solution vectors of the homogeneous system of linear equation $(G_{p^s-2k-1} + I_{p^s-2k-1})Y = 0$, i.e., $\xi_i^{[1,p^s-2k-1]} \in \mathcal{V}_1$ for all $i = 1, 2, \ldots, p^s - 2k - 1$.

Since $l = p^s - 2k - 1$ is even, we have $\lfloor \frac{l}{2} \rfloor = \frac{p^s-1}{2} - k$. Then by Lemma 4 (iii), we know that $\{\xi_{2t}^{[1,p^s-2k-1]} \mid 1 \le t \le \frac{p^s-1}{2} - k\}$ is a maximal $\mathbb{F}_q$-linear independent system of $\xi_1^{[1,p^s-2k-1]}, \xi_2^{[1,p^s-2k-1]}, \ldots, \xi_{p^s-2k-1}^{[1,p^s-2k-1]}$. From this and by $\dim_{\mathbb{F}_q}(\mathcal{V}_1) = \frac{p^s-1}{2} - k$, we deduce that $\{\xi_{2t}^{[1,p^s-2k-1]} \mid 1 \le t \le \frac{p^s-1}{2} - k\}$ is an $\mathbb{F}_q$-basis of $\mathcal{V}_1$. Since $B_{p^s-2k-1,1} \in \mathcal{V}_1$ by Equation (6), there is a unique vector $(c_2, c_4, \ldots, c_{p^s-2k-1}) \in \mathbb{F}_q^{\frac{p^s-1}{2}-k}$ such that

$$B_{p^s-2k-1,1} = \sum_{t=1}^{\frac{p^s-1}{2}-k} c_{2t}\xi_{2t}^{[1,p^s-2k-1]}.$$

Then from $B_{p^s-2k-1,1} = \begin{pmatrix} \mathbf{0}_{\frac{p^s-1}{2}-k} \\ b_{0,1} \\ b_{1,1} \\ \vdots \\ b_{\frac{p^s-3}{2}-k,1} \end{pmatrix}$ and Equation (4), we deduce that $c_{2t} = 0$ for all integers t: $1 \le t \le \left\lfloor \frac{p^s-1-2k}{4} \right\rfloor$. Hence

$$(b_{0,1}, b_{1,1}, \ldots, b_{\frac{p^s-3}{2}-k,1})^{\mathrm{tr}} = \sum_{\lfloor \frac{p^s-1-2k}{4} \rfloor + 1 \le t \le \frac{p^s-1}{2}-k} c_{2t} \xi_{2t}^{[\frac{p^s-1}{2}-k+1, p^s-2k-1]},$$

where $c_{2t} \in \mathbb{F}_q$ arbitrary, for all integers t: $\lfloor \frac{p^s-1-2k}{4} \rfloor + 1 \le t \le \frac{p^s-1}{2} - k$.

◇ Similarly, from $\left(G_{p^s-2k-1} - I_{p^s-2k-1}\right)\left(G_{p^s-2k-1} + I_{p^s-2k-1}\right) = 0$, Equation (4) and Lemma 4 (i), we deduce that

$$(b_{0,0}, b_{1,0}, \ldots, b_{\frac{p^s-3}{2}-k,0})^{\mathrm{tr}} = \sum_{\lceil \frac{p^s-1-2k}{4} \rceil + 1 \le j \le \frac{p^s-1}{2}-k} a_{2j-1} Y_{2j-1}^{[\frac{p^s-1}{2}-k+1, p^s-2k-1]},$$

where $a_{2j-1} \in \mathbb{F}_q$ arbitrary, for all integers j: $\lceil \frac{p^s-1-2k}{4} \rceil + 1 \le j \le \frac{p^s-1}{2} - k$.

As stated above, we conclude that

$$\begin{aligned}
&(b_0, b_1, \ldots, b_{\frac{p^s-3}{2}-k})^{\mathrm{tr}} \\
&= (b_{0,0}, b_{1,0}, \ldots, b_{\frac{p^s-3}{2}-k,0})^{\mathrm{tr}} + w(b_{0,1}, b_{1,1}, \ldots, b_{\frac{p^s-3}{2}-k,1})^{\mathrm{tr}} \\
&= \sum_{\lceil \frac{p^s-1-2k}{4} \rceil + 1 \le j \le \frac{p^s-1}{2}-k} a_{2j-1} Y_{2j-1}^{[\frac{p^s-1}{2}-k+1, p^s-2k-1]} \\
&\quad + \sum_{\lfloor \frac{p^s-1-2k}{4} \rfloor + 1 \le t \le \frac{p^s-1}{2}-k} c_{2t} \cdot w \xi_{2t}^{[\frac{p^s-1}{2}-k+1, p^s-2k-1]}.
\end{aligned}$$

Moreover, by (ii) and (iv) of Lemma 4 and $\lceil \frac{p^s-1-2k}{4} \rceil + \lfloor \frac{p^s-1-2k}{4} \rfloor = \frac{p^s-1}{2} - k$, the number of all column vectors $(b_0, b_1, \ldots, b_{\frac{p^s-3}{2}-k})^{\mathrm{tr}}$ determined above is equal to $q^{(\frac{p^s-1}{2}-k)-\lceil \frac{p^s-1-2k}{4} \rceil} \cdot q^{(\frac{p^s-1}{2}-k)-\lfloor \frac{p^s-1-2k}{4} \rfloor} = q^{\frac{p^s-1}{2}-k}$.

Summing up the conclusions of the above three cases, we have constructed $\sum_{k=0}^{\frac{p^s-1}{2}} q^{\frac{p^s-1}{2}-k} = \frac{q^{\frac{p^s-1}{2}+1}-1}{q-1}$ distinct Hermitian self-dual cyclic codes of length p^s over R. As $\mathrm{NH}(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}, p^s) = \frac{q^{\frac{p^s-1}{2}+1}-1}{q-1}$, we have obtained all distinct Hermitian self-dual cyclic codes of length p^s over R. □ □

Moreover, by Equations (2), (3) and the definitions for the following vectors

$$Y_{2j-1}^{[\frac{p^s-1}{2}-k+1, p^s-2k-1]} \text{ and } \xi_{2t}^{[\frac{p^s-1}{2}-k+1, p^s-2k-1]},$$

we can provide an explicit expression for all distinct Hermitian self-dual cyclic codes of length p^s over $\mathbb{F}_{q^2}+u\mathbb{F}_{q^2}$, using binomial coefficients.

Theorem 3 *All distinct* $\frac{q^{\frac{p^s-1}{2}+1}-1}{q-1}$ *Hermitian self-dual cyclic codes of length* p^s *over* $R=\mathbb{F}_{q^2}+u\mathbb{F}_{q^2}$ *are given by the following three cases*:

I. 1 code: $\langle u(x-1)^{\frac{p^s-1}{2}}, (x-1)^{\frac{p^s+1}{2}}\rangle$.

II. q codes: $\langle (x-1)^{\frac{p^s+1}{2}}(-2)cw + u(x-1)^{\frac{p^s-3}{2}}, (x-1)^{\frac{p^s+3}{2}}\rangle$, where $c\in\mathbb{F}_q$.

III. For each integer k, $0\le k\le \frac{p^s-1}{2}-2$, there are exactly $q^{\frac{p^s-1}{2}-k}$ codes given by:

$$\langle (x-1)^{\frac{p^s+1}{2}} b_k(x) + u(x-1)^k, (x-1)^{p^s-k}\rangle,$$

where

$$b_k(x)=\sum_{\rho=0}^{\frac{p^s-3}{2}-k}\gamma_\rho(x-1)^\rho+\sum_{j=\lceil\frac{p^s-1-2k}{4}\rceil+1}^{\frac{p^s-1}{2}-k}a_{2j-1}(x-1)^{2j-2-\frac{p^s-1}{2}+k}$$
$$-\sum_{t=\lfloor\frac{p^s-1-2k}{4}\rfloor+1}^{\frac{p^s-1}{2}-k}c_{2t}w(x-1)^{2t-1-\frac{p^s-1}{2}+k}$$

with

$$\gamma_\rho=\sum_{j=\lceil\frac{p^s-1-2k}{4}\rceil+1}^{\frac{p^s-1}{2}-k}a_{2j-1}\binom{p^s+1-2j}{\frac{p^s+1}{2}-k+1+\rho-2j}$$
$$-\sum_{t=\lfloor\frac{p^s-1-2k}{4}\rfloor+1}^{\frac{p^s-1}{2}-k}c_{2t}w\binom{p^s-2t}{\frac{p^s+1}{2}-k+\rho-2t}$$

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

$$\left\lceil\frac{p^s-1-2k}{4}\right\rceil+1\le j\le\frac{p^s-1}{2}-k,\ \left\lfloor\frac{p^s-1-2k}{4}\right\rfloor+1\le t\le\frac{p^s-1}{2}-k,$$

respectively.

Proof By the notation at the beginning of this section and the notation in Lemma 4, we have the following:

✓ $(Y_1^{[1,p^s-2k-1]}, Y_2^{[1,p^s-2k-1]},\ldots,Y_{p^s-2k-1}^{[1,p^s-2k-1]})=G_{p^s-2k-1}+I_{p^s-2k-1}$ and

$$Y_{2j-1}^{[\frac{p^s-1}{2}-k+1,p^s-2k-1]}=\begin{pmatrix} g_{\frac{p^s-1}{2}-k+1,2j-1} \\ g_{\frac{p^s-1}{2}-k+2,2j-1} \\ \vdots \\ g_{p^s-2k-1,2j-1} \end{pmatrix};$$

✓ $(\xi_1^{[1,p^s-2k-1]},\xi_2^{[1,p^s-2k-1]},\ldots,\xi_{p^s-2k-1}^{[1,p^s-2k-1]})=G_{p^s-2k-1}-I_{p^s-2k-1}$ and

$$\xi_{2t}^{[\frac{p^s-1}{2}-k+1,p^s-2k-1]}=\begin{pmatrix} h_{\frac{p^s-1}{2}-k+1,2t} \\ h_{\frac{p^s-1}{2}-k+2,2t} \\ \vdots \\ h_{p^s-2k-1,2t} \end{pmatrix}.$$

From these, by Equations (2) and (3), $(-1)^{(2j-1)-1}=1$ and $(-1)^{2t-1}=-1$, we deduce the following conclusions.

(†) For any integer $j, \lceil\frac{p^s-1-2k}{4}\rceil+1\le j\le\frac{p^s-1}{2}-k$, we have the following:

◇ When $0\le\rho\le\frac{p^s-3}{2}-k$ and $\rho\ne 2j-2-\frac{p^s-1}{2}+k$,

$$\begin{aligned} g_{\frac{p^s-1}{2}-k+1+\rho,2j-1} &= \begin{pmatrix} p^s-(2j-1) \\ \frac{p^s-1}{2}-k+1+\rho-(2j-1) \end{pmatrix} \\ &= \begin{pmatrix} p^s+1-2j \\ \frac{p^s+1}{2}-k+1+\rho-2j \end{pmatrix}. \end{aligned}$$

◇ When $\rho=2j-2-\frac{p^s-1}{2}+k$,

$$g_{\frac{p^s-1}{2}-k+1+\rho,2j-1}=\begin{pmatrix} p^s+1-2j \\ \frac{p^s+1}{2}-k+1+\rho-2j \end{pmatrix}+1.$$

(‡) For any integer $t, \lfloor\frac{p^s-1-2k}{4}\rfloor+1\le t\le\frac{p^s-1}{2}-k$, we have the following:

◇ When $0\le\rho\le\frac{p^s-3}{2}-k$ and $\rho\ne 2t-1-\frac{p^s-1}{2}+k$,

$$\begin{aligned} h_{\frac{p^s-1}{2}-k+1+\rho,2t} &= (-1)^{2t-1}\begin{pmatrix} p^s-2t \\ \frac{p^s-1}{2}-k+1+\rho-2t \end{pmatrix} \\ &= -\begin{pmatrix} p^s-2t \\ \frac{p^s+1}{2}-k+\rho-2t \end{pmatrix}. \end{aligned}$$

◇ When $\rho=2t-1-\frac{p^s-1}{2}+k$,

$$h_{\frac{p^s-1}{2}-k+1+\rho,2t}=-\begin{pmatrix} p^s-2t \\ \frac{p^s+1}{2}-k+\rho-2t \end{pmatrix}-1.$$

Then the explicit expressions for all distinct Hermitian self-dual cyclic codes of length p^s over $\mathbb{F}_{q^2}+u\mathbb{F}_{q^2}$ can be deduced directly from Theorem 2. Here, we omit these details. □

4 Applications

In this section, using Theorem 3, we list all distinct Hermitian self-dual cyclic codes of length 3^s over the ring $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m}$ for the cases $s = 1, 2, 3$ and all distinct Hermitian self-dual cyclic codes of length 5^2 over $\mathbb{F}_{5^m} + u\mathbb{F}_{5^m}$, respectively, for any even positive integer m.

(†) Using the notation of Section 2 and by Equation (1), we assume that $\mathbb{F}_{3^m} = \{a + bw \mid a, b \in \mathbb{F}_{3^{\frac{m}{2}}}\}$, where $0 \neq w \in \mathbb{F}_{3^m}$ satisfies $w^{3^{\frac{m}{2}}} = -w$ and $\mathbb{F}_{3^{\frac{m}{2}}}$ is the subfield of $\mathbb{F}_{3^m}$ with $3^{\frac{m}{2}}$ elements.

(i) Let $s = 1$. By Theorem 2, all $\mathrm{NH}(\mathbb{F}_{3^m} + u\mathbb{F}_{3^m}, 3) = 1 + 3^{\frac{m}{2}}$ Hermitian self-dual cyclic codes of length 3 over $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m}$ are the following:

$$\langle u(x-1), (x-1)^2\rangle; \langle (x-1)^2 \cdot cw + u\rangle \text{ where } c \in \mathbb{F}_{3^{\frac{m}{2}}}.$$

(ii) Let $s = 2$. By Theorem 3, all $\mathrm{NH}(\mathbb{F}_{3^m} + u\mathbb{F}_{3^m}, 9) = 1 + 3^{\frac{m}{2}} + (3^{\frac{m}{2}})^2 + (3^{\frac{m}{2}})^3 + (3^{\frac{m}{2}})^4$ Hermitian self-dual cyclic codes of length 3^2 over $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m}$ are given by the following five cases:

▷ 1 code: $\langle u(x-1)^4, (x-1)^5\rangle$.

▷ $3^{\frac{m}{2}}$ codes: $\langle (x-1)^5 \cdot cw + u(x-1)^3, (x-1)^6\rangle$, where $c \in \mathbb{F}_{3^{\frac{m}{2}}}$.

▷ $(3^{\frac{m}{2}})^2$ codes: $\langle (x-1)^5 \cdot b_2(x) + u(x-1)^2, (x-1)^7\rangle$, where $b_2(x) = 2a_3 + c_4w(x-1)$ and $a_3, c_4 \in \mathbb{F}_{3^{\frac{m}{2}}}$.

▷ $(3^{\frac{m}{2}})^3$ codes: $\langle (x-1)^5 \cdot b_1(x) + u(x-1), (x-1)^8\rangle$, where $b_1(x) = c_4w + (2a_5 + c_4w)(x-1) + (a_5 + 2c_4w + c_6w)(x-1)^2$ and $a_5, c_4, c_6 \in \mathbb{F}_{3^{\frac{m}{2}}}$.

▷ $(3^{\frac{m}{2}})^4$ codes: $\langle (x-1)^5 \cdot b_0(x) + u\rangle$, where $b_0(x) = 2a_5 + (a_5 + c_6w)(x-1) + 2a_7(x-1)^2 + (a_5 + 2a_7 + c_8w)(x-1)^3$ and $a_5, a_7, c_6, c_8 \in \mathbb{F}_{3^{\frac{m}{2}}}$.

(iii) Let $s = 3$. By Theorem 3, all $\mathrm{NH}(\mathbb{F}_{3^m} + u\mathbb{F}_{3^m}, 27) = \sum_{k=0}^{13}(3^{\frac{m}{2}})^k = \frac{(3^{\frac{m}{2}})^{14}-1}{3^{\frac{m}{2}}-1}$ Hermitian self-dual cyclic codes of length 3^3 over $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m}$ are given by the following:

- 1 code: $\langle u(x-1)^{13}, (x-1)^{14}\rangle$.
- $\sum_{i=1}^{13}(3^{\frac{m}{2}})^i$ codes: for each integer k, $0 \leq k \leq 12$, there are $(3^{\frac{m}{2}})^{13-k}$ codes given by:

$$\langle (x-1)^{14}b_k(x) + u(x-1)^k, (x-1)^{27-k}\rangle,$$

where

$$b_{12}(x) = c_2w; b_{11}(x) = 2a_3 + c_4w(x-1);$$
$$b_{10}(x) = c_4w + (2a_5 + c_4w)(x-1) + (a_5 + 2c_4w + c_6w)(x-1)^2;$$
$$b_9(x) = 2a_5 + (a_5 + c_6w)(x-1) + 2a_7(x-1)^2 + (a_5 + 2a_7 + c_8w)(x-1)^3;$$

$b_8(x) = c_6w + 2a_7(x-1) + (2a_7 + c_8w)(x-1)^2 + (a_7 + 2a_9 + 2c_6w + 2c_8w)$
$(x-1)^3 + c_{10}w(x-1)^4$;
$b_7(x) = 2a_7 + (2a_7 + c_8w)(x-1) + (a_7 + 2a_9 + 2c_8w)(x-1)^2 + c_{10}w(x-1)^3$
$+(2a_{11} + c_{10}w)(x-1)^4 + (a_{11} + 2c_{10}w + c_{12}w)(x-1)^5$;
$b_6(x) = c_8w + (2a_9 + 2c_8w)(x-1) + c_{10}w(x-1)^2 + (2a_{11} + c_{10}w)(x-1)^3$
$+(a_{11} + 2c_{10}w + c_{12}w)(x-1)^4 + (2a_{13} + c_{10}w)(x-1)^5 + (2a_{11} + 2a_{13}$
$+2c_{10}w + c_{14}w)(x-1)^6$;
$b_5(x) = 2a_9 + c_{10}w(x-1) + (2a_{11} + c_{10}w)(x-1)^2 + (a_{11} + 2c_{10}w + c_{12}w)$
$(x-1)^3 + (2a_{13} + c_{10}w)(x-1)^4 + (2a_{11} + 2a_{13} + 2c_{10}w + c_{14}w)(x-1)^5$
$+(2a_{11} + a_{13} + 2a_{15} + c_{10}w + c_{12}w + 2c_{14}w)(x-1)^6 + (a_{13} + 2c_{10}w$
$+c_{16}w)(x-1)^7$;
$b_4(x) = c_{10}w + (2a_{11} + c_{10}w)(x-1) + (a_{11} + 2c_{10}w + c_{12}w)(x-1)^2 + (2a_{13}$
$+c_{10}w)(x-1)^3 + (2a_{11} + 2a_{13} + 2c_{10}w + c_{14}w)(x-1)^4 + (2a_{11} + a_{13}$
$+2a_{15} + c_{10}w + c_{12}w + 2c_{14}w)(x-1)^5 + (a_{13} + 2c_{10}w + c_{16}w)(x-1)^6$
$+(a_{11} + 2a_{13} + 2a_{17} + c_{10}w + 2c_{14}w + c_{16}w)(x-1)^7 + (a_{11} + a_{13} + a_{15}$
$+a_{17} + 2c_{10}w + 2c_{12}w + 2c_{14}w + 2c_{16}w + c_{18}w)(x-1)^8$;
$b_3(x) = 2a_{11} + (a_{11} + c_{12}w)(x-1) + 2a_{13}(x-1)^2 + (2a_{11} + 2a_{13} + c_{14}w)$
$(x-1)^3 + (2a_{11} + a_{13} + 2a_{15} + c_{12}w + 2c_{14}w)(x-1)^4 + (a_{13} + c_{16}w)$
$(x-1)^5 + (a_{11} + 2a_{13} + 2a_{17} + 2c_{14}w + c_{16}w)(x-1)^6 + (a_{11} + a_{13} + a_{15}$
$+a_{17} + 2c_{12}w + 2c_{14}w + 2c_{16}w + c_{18}w)(x-1)^7 + 2a_{19}(x-1)^8 + (a_{11}$
$+2a_{19} + c_{20}w)(x-1)^9$;
$b_2(x) = c_{12}w + 2a_{13}(x-1) + (2a_{13} + c_{14}w)(x-1)^2 + (a_{13} + 2a_{15} + c_{12}w$
$+2c_{14}w)(x-1)^3 + (a_{13} + c_{16}w)(x-1)^4 + (2a_{13} + 2a_{17} + 2c_{14}w + c_{16}w)$
$(x-1)^5 + (a_{13} + a_{15} + a_{17} + 2c_{12}w + 2c_{14}w + 2c_{16}w + c_{18}w)(x-1)^6$
$+2a_{19}(x-1)^7 + (2a_{19} + c_{20}w)(x-1)^8 + (a_{19} + 2a_{21} + 2c_{12}w + 2c_{20}w)$
$(x-1)^9 + (a_{13} + 2a_{19} + c_{22}w)(x-1)^{10}$;
$b_1(x) = 2a_{13} + (2a_{13} + c_{14}w)(x-1) + (a_{13} + 2a_{15} + 2c_{14}w)(x-1)^2 + (a_{13}$
$+c_{16}w)(x-1)^3 + (2a_{13} + 2a_{17} + 2c_{14}w + c_{16}w)(x-1)^4 + (a_{13} + a_{15} + a_{17}$
$+2c_{14}w + 2c_{16}w + c_{18}w)(x-1)^5 + 2a_{19}(x-1)^6 + (2a_{19} + c_{20}w)(x-1)^7$
$+(a_{19} + 2a_{21} + 2c_{20}w)(x-1)^8 + (a_{13} + 2a_{19} + c_{22}w)(x-1)^9 + (2a_{13}$
$+a_{19} + 2a_{23} + 2c_{14}w + c_{20}w + c_{22}w)(x-1)^{10} + (a_{13} + a_{15} + 2a_{19} + 2a_{21}$
$+a_{19} + 2a_{23} + 2c_{14}w + c_{20}w + c_{22}w)(x-1)^{10} + (a_{13} + a_{15} + 2a_{19} + 2a_{21}$
$+a_{23} + 2c_{14}w + c_{20}w + 2c_{22}w + c_{24}w)(x-1)^{11}$;
$b_0(x) = c_{14}w + (2a_{15} + 2c_{14}w)(x-1) + c_{16}w(x-1)^2 + (2a_{17} + 2c_{14}w + c_{16}w)$
$(x-1)^3 + (a_{15} + a_{17} + 2c_{14}w + 2c_{16}w + c_{18}w)(x-1)^4 + 2a_{19}(x-1)^5$
$+(2a_{19} + c_{20}w)(x-1)^6 + (a_{19} + 2a_{21} + 2c_{20}w)(x-1)^7 + (2a_{19} + c_{22}w)$
$(x-1)^8 + (a_{19} + 2a_{23} + 2c_{14}w + c_{20}w + c_{22}w)(x-1)^9 + (a_{15} + 2a_{19}$
$+2a_{21} + a_{23} + 2c_{14}w + c_{20}w + 2c_{22}w + c_{24}w)(x-1)^{10} + (a_{19} + 2a_{25}$
$+2c_{16}w + 2c_{22}w)(x-1)^{11} + (a_{17} + 2a_{19} + a_{23} + 2a_{25} + 2c_{14}w + c_{16}w$
$+2c_{20}w + c_{22}w + c_{26}w)(x-1)^{12}$,

and $a_{2j-1}, c_{2t} \in \mathbb{F}_{3^{\frac{m}{2}}}$, for all integers j, t: $2 \le j \le 13$ and $1 \le t \le 13$.

Remark 1 (♭) Let $m = 2$. Then $z^2 + 1$ is an irreducible polynomial in $\mathbb{F}_3[z]$. We set

$$\mathbb{F}_9 = \{a + bw \mid a, b \in \mathbb{F}_3\}$$

in which $w^2 + 1 = 0$. Then $w^3 = -w$ in $\mathbb{F}_9$. Therefore, we have $\frac{3^{14}-1}{3-1} = 2391484$ Hermitian self-dual cyclic codes of length 27 over $\mathbb{F}_9 + u\mathbb{F}_9$. In particular, all these Hermitian self-dual cyclic codes can be obtained from the case (iii) above, by setting:

$$a_{2j-1}, c_{2t} \in \mathbb{F}_3,\ \forall j, t :\ 2 \le j \le 13,\ 1 \le t \le 13.$$

(♮) Let $m = 4$. Then $z^4 + z^3 + z^2 + z + 1$ is an irreducible polynomial in $\mathbb{F}_3[z]$. We set

$$\mathbb{F}_{3^4} = \{a + b\alpha + c\alpha^2 + d\alpha^3 \mid a, b, c, d \in \mathbb{F}_3\}$$

in which $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$. Then $\mathrm{ord}(1 + 2\alpha + \alpha^2) = 8$, and

$$\begin{aligned}\diamond\ \mathbb{F}_9 =& \{0\} \cup \{(1 + 2\alpha + \alpha^2)^i \mid 0 \le i \le 7\}\\ =& \{0, 1, 2, 1 + 2\alpha + \alpha^2, \alpha + 2\alpha^2, 1 + \alpha + 2\alpha^2, 2 + \alpha + 2\alpha^2, 2\alpha + \alpha^2,\\ & 2 + 2\alpha + \alpha^2\}.\end{aligned}$$

$\diamond$ Let $w = 1 + \alpha$. Then $w^9 = -w$ in $\mathbb{F}_{3^4}$.

Therefore, we have $\frac{9^{14}-1}{9-1} = 2859599056870$ Hermitian self-dual cyclic codes of length 27 over $\mathbb{F}_{81} + u\mathbb{F}_{81}$. In particular, all these Hermitian self-dual cyclic codes can be obtained from the case (iii) above, by setting:

$$w = 1 + \alpha \ \text{ and } \ a_{2j-1}, c_{2t} \in \mathbb{F}_9,\ \forall j, t :\ 2 \le j \le 13,\ 1 \le t \le 13..$$

(♯) Using the notation of Section 2 and by Equation (1), we assume $\mathbb{F}_{5^m} = \{a + bw \mid a, b \in \mathbb{F}_{5^{\frac{m}{2}}}\}$, where $0 \ne w \in \mathbb{F}_{5^m}$ satisfies $w^{5^{\frac{m}{2}}} = -w$ and $\mathbb{F}_{5^{\frac{m}{2}}}$ is the subfield of $\mathbb{F}_{5^m}$ with $5^{\frac{m}{2}}$ elements..

By Theorem 3, all $\mathrm{NH}(\mathbb{F}_{5^m} + u\mathbb{F}_{5^m}, 25) = \sum_{k=0}^{12}(5^{\frac{m}{2}})^k = \frac{(5^{\frac{m}{2}})^{13}-1}{5^{\frac{m}{2}}-1}$ Hermitian self-dual cyclic codes of length 5^2 over $\mathbb{F}_{5^m} + u\mathbb{F}_{5^m}$ are the following:

- 1 code: $\langle u(x-1)^{12}, (x-1)^{13}\rangle$.
- $\sum_{i=1}^{12}(5^{\frac{m}{2}})^i$ codes: For each integer k, $0 \le k \le 11$, there are $(5^{\frac{m}{2}})^{12-k}$ codes given by:

  $$\langle (x-1)^{13} b_k(x) + u(x-1)^k, (x-1)^{25-k}\rangle,$$

  where

  $$\begin{aligned}&b_{11}(x) = 3c_2w;\ b_{10}(x) = 2a_3 + (2a_3 + 3c_4w)(x-1);\\ &b_9(x) = 3c_4w + (2a_5 + 4c_4w)(x-1) + 3c_6w(x-1)^2;\\ &b_8(x) = 2a_5 + 3c_6w(x-1) + (2a_7 + c_6w)(x-1)^2 + (3a_7 + 4c_6w + 3c_8w)(x-1)^3\\ &;\end{aligned}$$

$$b_7(x) = 3c_6w + (2a_7 + c_6w)(x-1) + (3a_7 + 4c_6w + 3c_8w)(x-1)^2 + (3a_7 + 2a_9 + c_6w + 3c_8w)(x-1)^3 + (a_7 + a_9 + 4c_6w + 4c_8w + 3c_{10}w)(x-1)^4$$

; $b_6(x) = 2a_7 + (3a_7 + 3c_8w)(x-1) + (3a_7 + 2a_9 + 3c_8w)(x-1)^2 + (a_7 + a_9 + 4c_8w + 3c_{10}w)(x-1)^3 + 2a_{11}(x-1)^4 + (3a_7 + 4a_{11} + 3c_{12}w)(x-1)^5$;

$b_5(x) = 3c_8w + (2a_9 + 3c_8w)(x-1) + (a_9 + 4c_8w + 3c_{10}w)(x-1)^2 + 2a_{11}(x-1)^3 + (4a_{11} + 3c_{12}w)(x-1)^4 + (a_{11} + 2a_{13} + 2c_8w + 2c_{12}w)(x-1)^5 + (3a_9 + 4a_{11} + 2a_{13} + 4c_8w + 2c_{12}w + 3c_{14}w)(x-1)^6$;

$b_4(x) = 2a_9 + (a_9 + 3c_{10}w)(x-1) + 2a_{11}(x-1)^2 + (4a_{11} + 3c_{12}w)(x-1)^3 + (a_{11} + 2a_{13} + 2c_{12}w)(x-1)^4 + (3a_9 + 4a_{11} + 2a_{13} + 2c_{12}w + 3c_{14}w)(x-1)^5 + (3a_9 + a_{11} + a_{13} + 2a_{15} + 2c_{10}w + 4c_{12}w + 4c_{14}w)(x-1)^6 + (2a_{11} + 3c_{16}w)(x-1)^7$;

$b_3(x) = 3c_{10}w + 2a_{11}(x-1) + (4a_{11} + 3c_{12}w)(x-1)^2 + (a_{11} + 2a_{13} + 2c_{12}w)(x-1)^3 + (4a_{11} + 2a_{13} + 2c_{12}w + 3c_{14}w)(x-1)^4 + (a_{11} + a_{13} + 2a_{15} + 2c_{10}w + 4c_{12}w + 4c_{14}w)(x-1)^5 + (2a_{11} + 3c_{16}w)(x-1)^6 + (3a_{11} + 2a_{17} + 3c_{12}w + c_{16}w)(x-1)^7 + (2a_{11} + 2a_{13} + 3a_{17} + 4c_{12}w + 4c_{16}w + 3c_{18}w)(x-1)^8$;

$b_2(x) = 2a_{11} + (4a_{11} + 3c_{12}w)(x-1) + (a_{11} + 2a_{13} + 2c_{12}w)(x-1)^2 + (4a_{11} + 2a_{13} + 2c_{12}w + 3c_{14}w)(x-1)^3 + (a_{11} + a_{13} + 2a_{15} + 4c_{12}w + 4c_{14}w)(x-1)^4 + (2a_{11} + 3c_{16}w)(x-1)^5 + (3a_{11} + 2a_{17} + 3c_{12}w + c_{16}w)(x-1)^6 + (2a_{11} + 2a_{13} + 3a_{17} + 4c_{12}w + 4c_{16}w + 3c_{18}w)(x-1)^7 + (3a_{11} + 4a_{13} + 3a_{17} + 2a_{19} + 4c_{12}w + 3c_{14}w + c_{16}w + 3c_{18}w)(x-1)^8 + (2a_{11} + 2a_{13} + 2a_{15} + a_{17} + a_{19} + 3c_{12}w + 3c_{14}w + 4c_{16}w + 4c_{18}w + 3c_{20}w)(x-1)^9$;

$b_1(x) = 3c_{12}w + (2a_{13} + 2c_{12}w)(x-1) + (2a_{13} + 2c_{12}w + 3c_{14}w)(x-1)^2 + (a_{13} + 2a_{15} + 4c_{12}w + 4c_{14}w)(x-1)^3 + 3c_{16}w(x-1)^4 + (2a_{17} + 3c_{12}w + c_{16}w)(x-1)^5 + (2a_{13} + 3a_{17} + 4c_{12}w + 4c_{16}w + 3c_{18}w)(x-1)^6 + (4a_{13} + 3a_{17} + 2a_{19} + 4c_{12}w + 3c_{14}w + c_{16}w + 3c_{18}w)(x-1)^7 + (2a_{13} + 2a_{15} + a_{17} + a_{19} + 3c_{12}w + 3c_{14}w + 4c_{16}w + 4c_{18}w + 3c_{20}w)(x-1)^8 + (2a_{21} + 4c_{16}w)(x-1)^9 + (a_{17} + 4a_{21} + 4c_{12}w + c_{16}w + 3c_{22}w)(x-1)^{10}$;

$b_0(x) = 2a_{13} + (2a_{13} + 3c_{14}w)(x-1) + (a_{13} + 2a_{15} + 4c_{14}w)(x-1)^2 + 3c_{16}w(x-1)^3 + (2a_{17} + c_{16}w)(x-1)^4 + (2a_{13} + 3a_{17} + 4c_{16}w + 3c_{18}w)(x-1)^5 + (4a_{13} + 3a_{17} + 2a_{19} + 3c_{14}w + c_{16}w + 3c_{18}w)(x-1)^6 + (2a_{13} + 2a_{15} + a_{17} + a_{19} + 3c_{14}w + 4c_{16}w + 4c_{18}w + 3c_{20}w)(x-1)^7 + (2a_{21} + 4c_{16}w)(x-1)^8 + (a_{17} + 4a_{21} + c_{16}w + 3c_{22}w)(x-1)^9 + (a_{13} + 3a_{17} + a_{21} + 2a_{23} + 4c_{16}w + 4c_{18}w + 2c_{22}w)(x-1)^{10} + (2a_{13} + 3a_{17} + a_{19} + 4a_{21} + 2a_{23} + 4c_{14}w + c_{16}w + 3c_{18}w + 2c_{22}w + 3c_{24}w)(x-1)^{11}$,

and $a_{2j-1}, c_{2t} \in \mathbb{F}_{5^{\frac{m}{2}}}$, for all integers j and t: $2 \le j \le 12$ and $1 \le t \le 12$.

Remark 2 Let $m = 2$. Then $z^2 + z + 1$ is irreducible in $\mathbb{F}_5[z]$. We set $\mathbb{F}_{25} = \{a + b\beta \mid a, b \in \mathbb{F}_5\}$ in which $\beta^2 + \beta + 1 = 0$. Let $w = 1 + 2\beta$. Then $w^5 = -w$ in $\mathbb{F}_{25}$. Therefore, we have $\frac{5^{13}-1}{5-1} = 305175781$ Hermitian self-dual cyclic codes of

length 25 over $\mathbb{F}_{25} + u\mathbb{F}_{25}$. All these codes can be obtained precisely from the above expressions, by setting:

$$w = 1 + 2\beta \text{ and } a_{2j-1}, c_{2t} \in \mathbb{F}_5, \ \forall j, t : \ 2 \le j \le 12, \ 1 \le t \le 12.$$

Remark 3 The correctness of the results in this section has been verified by computer.

5 Conclusion and further work

For any odd prime p, even positive integer m and positive integer s, using binomial coefficients, we have provided an explicit expression to present precisely all distinct Hermitian self-dual cyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ $(u^2 = 0)$. For concrete odd prime p, even positive integer m and positive integer s, one can obtain these Hermitian self-dual cyclic codes easily, using the expression provided and computer.

A natural extension of this work is to construct and express all distinct Euclidean self-dual cyclic codes of length $p^k n$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ explicitly, for any odd prime p and arbitrary positive integers m, s, n satisfying $\gcd(p, n) = 1$ and $n > 1$. Another interesting question is to study the self-dual 2-quasi-cyclic codes over $\mathbb{F}_{p^m}$ which are derived from self-dual cyclic codes codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$.

Acknowledgements This research was supported in part by the National Natural Science Foundation of China (Grant Nos. 12071264, 11801324, 11671235, 61971243), the Shandong Provincial Natural Science Foundation, China (Grant Nos. ZR2021QA047, ZR2018BA007), the Scientific Research Foundation for the PhD of Shandong University of Technology (Grant No. 417037), the Scientific Research Fund of Hubei Provincial Key Laboratory of Applied Mathematics (Hubei University) (Grant Nos. HBAM201906), the IC Program of Shandong Institutions of Higher Learning For Youth Innovative Talents and the Nankai Zhide Foundation.

References

1. Abualrub, T., Siap, I.: Constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. J. Franklin Inst. **346**(5), 520–529 (2009)
2. Alkhamees, Y.: The determination of the group of automorphisms of a finite chain ring of characteristic p. The Quarterly Journal of Mathematics **42**(1), 387–391 (1991)
3. Amerra, M.C.V., Nemenzo, F.R.: On $(1 - u)$-cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$. Appl. Math. Lett. **21**(11), 1129–1133 (2008)
4. Betsumiya, K., Ling, S., Nemenzo, F.R.: Type II codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$. Discrete Math. **275**(1–3), 43–65 (2004)
5. Bonnecaze, A., Udaya, P.: Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Trans. Inform. Theory **45**(4), 1250–1255 (1999)
6. Cao, Y.: On constacyclic codes over finite chain rings. Finite Fields Appl. **24**, 124–135 (2013)
7. Cao, Y., Cao, Y., Dinh, H.Q., Fu, F.-W., Gao, J., Sriboonchitta, S.: Constacyclic codes of length np^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Adv. Math. Commun. **12**(2), 231–262 (2018)
8. Cao, Y., Cao, Y., Fu, F.-W.: Matrix-product structure of constacyclic codes over finite chain rings $\mathbb{F}_{p^m}/\langle u^e \rangle$. Appl. Algebra in Engrg. Commun. Comput. **29**, 455–478 (2018)
9. 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**(7), 2077–2091 (2019)

10. Cao, Y., Cao, Y., Dinh, H.Q., Fu, F.-W., Ma, F.: Construction and enumeration for self-dual cyclic codes of even length over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$. Finite Fields Appl. **61**, 101598 (2020)
11. Cao, Y., Cao, Y., Dinh, H.Q., Jitman, S.: An efficient method to construct self-dual cyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Discrete Math. **343**(6), 111868 (2020)
12. Chen, B., Dinh, H.Q., Liu, H., Wang, L.: Constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Finite Fields Appl. **37**, 108–130 (2016)
13. Choosuwan P., Jitman S., Udomkavanich P.: Self-dual abelian codes in some nonprincipal ideal group algebras. Mathematical Problems in Engineering **2016**, article ID 9020173, 12 pages (2016)
14. 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)
15. 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)
16. Dinh, H.Q.: Repeated-root constacyclic codes of length $2p^s$. Finite Fields Appl. **18**(1), 133–143 (2012)
17. Dinh, H.Q.: Structure of repeated-root constacyclic codes of length $3p^s$ and their duals. Discrete Math. **313**(9), 983–991 (2013)
18. Dinh, H.Q., Wang, L., Zhu, S.: Negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Finite Fields Appl. **31**, 178–201 (2015)
19. Dinh, H.Q., Dhompongsa, S., Sriboonchitta, S.: On constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Discrete Math. **340**(4), 832–849 (2017)
20. Dinh H. Q., Sharma A., Rani S., Sriboonchitta S.: Cyclic and negacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. J. Algebra Appl. **17** (9), 1850173, 22 pages (2018)
21. Dinh, H.Q., Fan, Y., Liu, H., Liu, X., Sriboonchitta, S.: On self-dual constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Discrete Math. **341**(2), 324–335 (2018)
22. Dinh, H.Q., López-Permouth, S.R.: Cyclic and negacyclic codes over finite chain rings. IEEE Trans. Inform. Theory **50**(8), 1728–1744 (2004)
23. Dougherty, S.T., Gaborit, P., Harada, M., Solé, P.: Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Trans. Inform. Theory **45**(1), 32–45 (1999)
24. Dougherty, S.T., Kim, J.-L., Kulosman, H., Liu, H.: Self-dual codes over commutative Frobenius rings. Finite Fields Appl. **16**(1), 14–26 (2010)
25. Gulliver, T.A., Harada, M.: Construction of optimal Type IV self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Trans. Inform. Theory. **45**(7), 2520–2521 (1999)
26. Han, S., Lee, H., Lee, Y.: Construction of self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. Bull. Korean Math. Soc. **49**(1), 135–143 (2012)
27. Huffman, W.C.: On the decompostion of self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ with an automorphism of odd prime number. Finite Fields Appl. **13**(3), 682–712 (2007)
28. Jitman, S., Ling, S., Sangwisut, E.: On self-dual cyclic codes of length p^a over GR(p^2, s). Adv. Math. Commun. **10**(2), 255–273 (2016)
29. Jitman, S., Ling, S., Udomkavanich, P.: Skew constacyclic codes over finite chain rings. Adv. Math. Commun. **6**(1), 39–63 (2012)
30. Karadeniz, S., Yildiz, B., Aydin, N.: Extremal binary self-dual codes of lengths 64 and 66 from four-circulant constructions over $\mathbb{F}_2 + u\mathbb{F}_2$. Filomat **28**(5), 937–945 (2014)
31. Kaya, A., Yildiz, B., Siap, I.: New extremal binary self-dual codes from $\mathbb{F}_4 + u\mathbb{F}_4$-lifts of quadratic double circulant codes over $\mathbb{F}_4$. Finite Fields Appl. **35**, 318–329 (2015)
32. Kaya, A., Yildiz, B.: Various constructions for self-dual codes over rings and new binary self-dual codes. Discrete Math. **339**(2), 460–469 (2010)
33. Kim, B., Lee, Y.: Classification of self-dual cyclic codes over the chain ring $\mathbb{Z}_p[u]/\langle u^3\rangle$. Des. Codes Cryptogr. **88**, 2247–2273 (2020)
34. Ling, S., Solé, P.: Type II codes over $\mathbb{F}_4 + u\mathbb{F}_4$. Eur. J. Comb. **22**(7), 983–997 (2001)
35. Wan Z.-X.: Lectures on finite fields and Galois rings. World Scientific Pub Co Inc. (2003)
36. Zhao, W., Tang, X., Gu, Z.: All $\alpha + u\beta$-constacyclic codes of length np^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Finite Fields Appl. **50**, 1–16 (2018)