European Journal of Mathematics (2020) 6:1424–1437
https://doi.org/10.1007/s40879-019-00378-9

RESEARCH ARTICLE

A note on self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$

Parinyawat Choosuwan[1] · **Somphong Jitman**[2] · **Patanee Udomkavanich**[3]

Received: 30 May 2019 / Revised: 25 September 2019 / Accepted: 6 October 2019 /
Published online: 15 October 2019

Abstract

Self-dual cyclic codes over rings and their generalizations have become of interest due to their rich algebraic structures and wide applications. Cyclic and self-dual cyclic codes over the ring $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ have been quite well studied, where p is a prime, k is a positive integer, and $u^2=0$. We focus on negacyclic codes over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$, where p is an odd prime and k is a positive integer. An alternative and explicit algebraic characterization of negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ is presented. Based on this result, representation and enumeration of self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ are given under both the Euclidean and Hermitian inner products.

Keywords Negacyclic codes · Self-dual codes · Codes over rings · Euclidean inner product · Hermitian inner product

Mathematics Subject Classification 94B05 · 94B15 · 13B25 · 94B60

P. Choosuwan was partially supported by the Faculty of Science and Technology, Rajamangala University of Technology Thanyaburi (RMUTT). S. Jitman was supported by the Thailand Research Fund and Silpakorn University under Research Grant RSA6280042.

✉ Somphong Jitman
sjitman@gmail.com

Parinyawat Choosuwan
parinyawat_c@rmutt.ac.th

Patanee Udomkavanich
pattanee.u@chula.ac.th

1 Department of Mathematics and Computer Science, Faculty of Science and Technology, Rajamangala University of Technology Thanyaburi (RMUTT), Khlong Luang, Pathum Thani 12110, Thailand

2 Department of Mathematics, Faculty of Science, Silpakorn University, Mueang, Nakhon Pathom 73000, Thailand

3 Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Pathumwan, Bangkok 10330, Thailand

1 Introduction

Self-dual cyclic and negacyclic codes over finite fields have been extensively studied for both theoretical and practical reasons. Codes over finite rings have been of interest since it was proven that some binary non-linear codes such as the Kerdock, Preparata, and Goethal codes are the Gray images of linear codes over $\mathbb{Z}_4$ (see [9]). Cyclic codes, negacyclic codes and their generalizations have extensively been studied over $\mathbb{Z}_{p^r}$, Galois rings, $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ with $u^2 = 0$ and finite chain rings (see [1–8,10,11,13–16] and references therein).

Recently, a lot attention has been paid to families of negacyclic and self-dual codes over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$, and there is a significant progress on these topics (see [3,6–8,14]). In [3], characterization and presentation of negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ have been established. Later, the algebraic structure of negacyclic codes of lengths $2p^s$ and $4p^s$ over the ring $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ has been studied in [6–8,14]. Subsequently, properties of Euclidean duals of negacyclic codes and Euclidean self-dual negacyclic codes of lengths $2p^s$ and $4p^s$ over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ have been studied in [8,14] and [6,7], respectively. To the best of our knowledge, a complete characterization and enumeration of self-dual negacyclic codes of length p^s have not been explicitly given so far.

Using a method which is a modification of the one in [13], the algebraic structure and number of cyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ have been presented in [2]. In *loc. cit.*, a complete characterization and enumeration of self-dual cyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ have been given under both the Euclidean and Hermitian inner products.

In this paper, we focus on negacyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ which makes sense only in the case where p is an odd prime and k is a positive integer. Throughout, assume that p is an odd prime and k is a positive integer. It is not difficult to verify that the map

$$\omega\colon \left(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}\right)[x]/\langle x^{p^s} - 1\rangle \to \left(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}\right)[x]/\langle x^{p^s} + 1\rangle$$

defined by

$$f(x) + \langle x^{p^s} - 1\rangle \mapsto f(-x) + \langle x^{p^s} + 1\rangle$$

is a ring isomorphism. Hence, the results on cyclic codes and self-dual cyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ in [2] can be carried over to negacyclic codes and self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$. Here, an alternative and direct method to study negacyclic codes and self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ is given. Characterization and enumeration of negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ are given by extending the techniques used in [2,10,12,13]. Furthermore, characterization of self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ is established under both the Euclidean and Hermitian inner products. Based on this characterization, enumeration of such self-dual codes is provided as well.

The paper is organized as follows. In Sect. 2, some basic results on the ring $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ are recalled. The characterization and enumeration of negacyclic codes of length p^s

over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ are provided in Sect. 3. In Sect. 4, the characterization and enumeration of self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ are discussed.

2 Preliminaries

In this section, some definitions and basic properties of negacyclic codes over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ are recalled. For a prime p and positive integer k, denote by $\mathbb{F}_{p^k}$ the finite field of order p^k. The set $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k} := \{a+ub : a, b \in \mathbb{F}_{p^k}\}$ forms a commutative chain ring with identity, where addition and multiplication are defined as in the usual polynomial ring over $\mathbb{F}_{p^k}$ with indeterminate u together with the condition $u^2 = 0$. In the case where k is even, the map $\widetilde{\cdot} : \mathbb{F}_{p^k}+u\mathbb{F}_{p^k} \to \mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ defined by

$$\widetilde{\alpha} = a^{p^{k/2}} + ub^{p^{k/2}} \tag{1}$$

for all $\alpha = a+ub \in \mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ is a ring automorphism. For more details concerning properties of $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$, we refer the reader to [3].

A *linear code* of length n over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ is defined to be an $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})$-submodule of the $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})$-module $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})^n$.

The *Euclidean inner product* on $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})^n$ is defined by

$$\langle \boldsymbol{a}, \boldsymbol{b}\rangle_{\mathrm{E}} := \sum_{i=0}^{n-1} \alpha_i \beta_i$$

for all $\boldsymbol{a} = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ and $\boldsymbol{b} = (\beta_0, \beta_1, \ldots, \beta_{n-1})$ in $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})^n$. In addition, if k is even, the *Hermitian inner product* on $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})^n$ is defined to be

$$\langle \boldsymbol{a}, \boldsymbol{b}\rangle_{\mathrm{H}} := \sum_{i=0}^{n-1} \alpha_i \widetilde{\beta_i}$$

for all $\boldsymbol{a} = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ and $\boldsymbol{b} = (\beta_0, \beta_1, \ldots, \beta_{n-1})$ in $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})^n$. The *Euclidean dual* of a linear code C of length n over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ is defined to be

$$C^{\perp_{\mathrm{E}}} := \left\{\boldsymbol{a} \in \left(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}\right)^n : \langle \boldsymbol{a}, \boldsymbol{b}\rangle_{\mathrm{E}} = 0 \text{ for all } \boldsymbol{b} \in C\right\}.$$

Similarly, if k is even, the *Hermitian dual* of C is defined as

$$C^{\perp_{\mathrm{H}}} := \left\{\boldsymbol{a} \in \left(\mathbb{F}_{p^k}+u\mathbb{F}\right)^n : \langle \boldsymbol{a}, \boldsymbol{b}\rangle_{\mathrm{H}} = 0 \text{ for all } \boldsymbol{b} \in C\right\}.$$

A linear code C is said to be *Euclidean self-dual* (resp., *Hermitian self-dual*) if $C = C^{\perp_{\mathrm{E}}}$ (resp., $C = C^{\perp_{\mathrm{H}}}$).

In the case where p is odd, $-1 \neq 1$ in $\mathbb{F}_{p^k}$. Then we have the following concepts. A linear code C of length n over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ is called a *negacyclic code* if C is invariant under the negacyclic shift, i.e., $(-c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$ for all

$(c_0, c_1, \ldots, c_{n-1}) \in C$. It is well known that there exists a one-to-one correspondence between the negacyclic codes of length n over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ and the ideals in the quotient ring $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^n + 1\rangle$. Precisely, a negacyclic code C of length n can be represented by the ideal

$$\left\{\sum_{i=0}^{n-1} c_i x^i : (c_0, c_1, \ldots, c_{n-1}) \in C\right\}$$

in $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^n + 1\rangle$.

Here, we focus on negacyclic and self-dual negacyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$. For convenience, denote by $\mathrm{N}(p^k, n)$, $\mathrm{NE}(p^k, n)$ and $\mathrm{NH}(p^k, n)$ the number of negacyclic codes, the number of Euclidean self-dual negacyclic codes, and the number of Hermitian self-dual negacyclic codes of length n over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, respectively.

3 Negacyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$

In this section, the characterization and enumeration of negacyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ are given. By extending techniques used for cyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ in [2], the algebraic structure and presentation of negacyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ can be derived in terms of ideals in $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1\rangle$. Since the proofs are quite straightforwardly extended from [2], they will be omitted.

First, we note that the map $\mu: (\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1\rangle \to \mathbb{F}_{p^k}[x]/\langle x^{p^s} + 1\rangle$ defined by

$$\mu(f(x)) = f(x) \pmod{u}$$

is a surjective ring homomorphism.

For each negacyclic code C in $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1\rangle$ and $i \in \{0, 1\}$, let

$$\mathrm{Tor}_i(C) = \left\{\mu(v(x)) : v(x) \in \left(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}\right)[x]/\langle x^{p^s} + 1\rangle \text{ and } u^i v(x) \in C\right\}.$$

For each $i \in \{0, 1\}$, $\mathrm{Tor}_i(C)$ is called the ith *torsion code* of C. The codes $\mathrm{Tor}_0(C) = \mu(C)$ and $\mathrm{Tor}_1(C)$ are sometimes called the *residue* and *torsion codes* of C, respectively. It is not difficult to see that for each $i \in \{0, 1\}$, $c(x) \in \mathrm{Tor}_i(C)$ if and only if $u^i(c(x) + uz(x)) \in C$ for some $z(x) \in \mathbb{F}_{p^k}[x]/\langle x^{p^s} + 1\rangle$. Consequently, $\mathrm{Tor}_0(C) \subseteq \mathrm{Tor}_1(C)$ are ideals in $\mathbb{F}_{p^k}[x]/\langle x^{p^s} + 1\rangle$, i.e., they are negacyclic codes of length p^s over $\mathbb{F}_{p^k}$. We note that every ideal in $\mathbb{F}_{p^k}[x]/\langle x^{p^s} + 1\rangle$ is of the form $\langle (x+1)^i\rangle$ for some $0 \leqslant i \leqslant p^s$ and its $\mathbb{F}_{p^m}$-dimension is p^{s-i}.

Proposition 3.1 ([2, Proposition 5]) *Let C be an ideal in $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1\rangle$ and let $i \in \{0, 1\}$. Then the following statements hold:*

(i) *$\mathrm{Tor}_i(C)$ is an ideal of $\mathbb{F}_{p^k}[x]/\langle x^{p^s} + 1\rangle$ and $\mathrm{Tor}_i(C) = \langle (x+1)^{T_i}\rangle$ for some $0 \leqslant T_i \leqslant p^s$.*

(ii) *If* $\mathrm{Tor}_i(C) = \langle (x+1)^{T_i} \rangle$, *then* $|\mathrm{Tor}_i(C)| = (p^k)^{p^s - T_i}$.
(iii) $|C| = |\mathrm{Tor}_0(C)| \cdot |\mathrm{Tor}_1(C)| = (p^k)^{2p^s - (T_0 + T_1)}$.

With the notations given in Proposition 3.1, for each $i \in \{0, 1\}$, $T_i(C) := T_i$ is called the ith-*torsional degree* of C. Since $\mathrm{Tor}_0(C) \subseteq \mathrm{Tor}_1(C)$, we have $0 \leqslant T_1(C) \leqslant T_0(C) \leqslant p^s$. Moreover, if $u(x+1)^t \in C$, then $t \geqslant T_1(C)$.

Next, we focus on negacyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, or equivalently, ideals in $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1 \rangle$.

Theorem 3.2 ([2, Theorem 8]) *Let C be an ideal in $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1 \rangle$, $T_0 := T_0(C)$, and $T_1 := T_1(C)$. Then*

$$C = \langle f_0(x), f_1(x) \rangle,$$

where

$$f_0(x) = \begin{cases} (x+1)^{T_0} + u(x+1)^t h(x) & \text{if } T_0 < p^s, \\ 0 & \text{if } T_0 = p^s, \end{cases}$$

and

$$f_1(x) = \begin{cases} u(x+1)^{T_1} & \text{if } T_1 < p^s, \\ 0 & \text{if } T_1 = p^s, \end{cases}$$

with $h(x) \in \mathbb{F}_{p^k}[x]/\langle x^{p^s} + 1 \rangle$ is either zero or a unit with $t + \deg(h(x)) < T_0$. Moreover, $(f_0(x), f_1(x))$ is unique in the sense that if there exists a pair $(g_0(x), g_1(x))$ of polynomials satisfying the above conditions, then $f_0(x) = g_0(x)$ and $f_1(x) = g_1(x)$.

For each ideal C in $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1 \rangle$, denote by $C = \langle\langle f_0(x), f_1(x) \rangle\rangle$ the *unique representation* of the ideal C obtained in Theorem 3.2.

In order to determine the number of ideals in $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1 \rangle$, the definition and some properties of the annihilator of an ideal in $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1 \rangle$ are revisited. For an ideal C in $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1 \rangle$, the *annihilator* of C is defined to be $\mathrm{Ann}(C) = \{f(x) \in (\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1 \rangle : f(x)g(x) = 0 \text{ for all } g(x) \in C\}$. The following properties can be derived easily (cf. results for $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} - 1 \rangle$ in [10, Theorems 12–13]).

Theorem 3.3 *Let C be an ideal of $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1 \rangle$. Then the following statements hold:*

(i) $\mathrm{Ann}(C)$ *is an ideal of* $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1 \rangle$.
(ii) *If* $|C| = (p^k)^d$, *then* $|\mathrm{Ann}(C)| = (p^k)^{(2 \cdot p^s - d)}$.
(iii) $\mathrm{Ann}(\mathrm{Ann}(C)) = C$.

Theorem 3.4 *Let $\mathcal{I}$ denote the set of ideals of $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1 \rangle$, and let $\mathcal{A} = \{C \in \mathcal{I} : T_0(C) + T_1(C) \leqslant p^s\}$ and $\mathcal{A}' = \{C \in \mathcal{I} : T_0(C) + T_1(C) \geqslant p^s\}$. Then the map $\phi \colon \mathcal{A} \to \mathcal{A}'$ defined by $C \mapsto \mathrm{Ann}(C)$ is a bijection.*

In view of Theorem 3.4, it suffices to focus on the ideals in $\mathcal{A}$. For each $C = \langle\langle f_0(x), f_1(x)\rangle\rangle$ in $\mathcal{A}$, if $f_0(x) = 0$, then $T_0(C) = p^s$ and $T_1(C) = 0$. Hence, the only ideal in $\mathcal{A}$ with $f_0(x) = 0$ is of the form $\langle\langle 0, u\rangle\rangle$. Under the assumption that $f_0(x) \neq 0$, the following two results can be obtained (cf. [10, Theorems 14–15] for cyclic codes).

Theorem 3.5 *Let* $\langle\langle (x+1)^{i_0} + u(x+1)^t h(x), u(x+1)^{i_1}\rangle\rangle$ *be the representation of an ideal in* $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$*. Then it is a representation of an ideal in* $\mathcal{A}$ *if and only if* i_0, i_1, t *are integers and* $h(x) \in \mathbb{F}_{p^k}[x]/\langle x^{p^s}+1\rangle$ *such that* $0 \leqslant i_0 < p^s$*,* $0 \leqslant i_1 \leqslant \min\{i_0, p^s - i_0\}$*,* $t \geqslant 0$*,* $t + \deg(h(x)) < i_1$*, and* $h(x)$ *is either zero or a unit in* $\mathbb{F}_{p^k}[x]/\langle x^{p^s}+1\rangle$*.*

Since every polynomial $\sum_{i=0}^{m} a_i(x+1)^i$ in $\mathbb{F}_{p^k}[x]/\langle x^{p^s}+1\rangle$ is either 0 or $(x+1)^t h(x)$, where $h(x)$ is a unit in $\mathbb{F}_{p^k}[x]/\langle x^{p^s}+1\rangle$ and $0 \leqslant t \leqslant m - \deg(h(x))$, Theorem 3.5 can be rewritten as follows.

Theorem 3.6 *The expression* $\left\langle\!\left\langle (x+1)^{i_0} + u\sum_{j=0}^{i_1-1} h_j(x+1)^j, u(x+1)^{i_1}\right\rangle\!\right\rangle$ *represents an ideal in* $\mathcal{A}$ *if and only if* i_0 *and* i_1 *are integers such that* $0 \leqslant i_0 < p^s$*,* $0 \leqslant i_1 \leqslant \min\{i_0, p^s - i_0\}$*,* $i_0 + i_1 \leqslant p^s$*, and* $h_j \in \mathbb{F}_{p^k}$ *for all* $0 \leqslant j < i_1$*.*

Proposition 3.7 *Let* $0 \leqslant d \leqslant p^s$*. Then the number of distinct ideals in* $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$ *with* $T_0 + T_1 = d$ *is*

$$\frac{p^{k(K+1)} - 1}{p^k - 1},$$

where $K = \min\{\lfloor d/2\rfloor, p^s - \lfloor d/2\rfloor\}$*.*

Proof Let $T_1 = i_1$ and $i_0 := T_0 = d - T_1$ be fixed.

Case 1: $d < p^s$. Then $i_0 \leqslant i_0 + i_1 = T_0 + T_1 = d < p^s$. By Theorem 3.6, it follows that $C = \left\langle\!\left\langle (x+1)^{i_0} + u\sum_{j=0}^{i_1-1} h_j(x+1)^j, u(x+1)^{i_1}\right\rangle\!\right\rangle$. Then the choice for $\sum_{j=0}^{i_1-1} h_j(x+1)^j$ is $(p^k)^{i_1}$. By Theorem 3.6 again, we also have $T_1 \leqslant \min\{T_0, p^s - T_0\}$. Since $T_0 + T_1 = d$, we obtain that $T_1 \leqslant \lfloor d/2\rfloor \leqslant T_0$, and hence, $T_1 \leqslant \min\{\lfloor d/2\rfloor, p^s - T_0\} \leqslant \min\{\lfloor d/2\rfloor, p^s - \lfloor d/2\rfloor\}$. Now, vary T_1 from 0 to K, we obtain that there are $1 + p^k + \cdots + (p^k)^K = (p^{k(K+1)} - 1)/(p^k - 1)$ ideals with $T_0 + T_1 = d$.

Case 2: $d = p^s$. If $i_0 = p^s$, then the only ideal with $T_0 + T_1 = p^s$ is the ideal represented by $\langle\langle 0, u\rangle\rangle$. If $i_0 < p^s$, then we have $p^k + (p^k)^2 + \cdots + (p^k)^K$ ideals by arguments similar to those in Case 1. □

For a negacyclic code C in $\mathcal{A}$, we have $C \neq \mathrm{Ann}(C)$ whenever $T_0(C) + T_1(C) < p^s$. In the case where $T_0(C) + T_1(C) = p^s$, by Theorem 3.5, the annihilator of the negecyclic code $C = \langle\langle (x+1)^{i_0} + u(x+1)^t h(x), u(x+1)^{i_1}\rangle\rangle$ is of the form $\mathrm{Ann}(C) = \langle (x+1)^{i_0} - u(x+1)^t h(x), u(x+1)^{i_1}\rangle$. Since p is odd, then $C = \mathrm{Ann}(C)$ occurs only in the case $h(x) = 0$. By Proposition 3.7 and the bijection given in Theorem 3.4, we have

Corollary 3.8 *The number of negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ is*

$$\mathrm{N}(p^k, p^s) = 2\left(\sum_{d=0}^{p^s} \frac{p^{k(\min\{\lfloor d/2\rfloor, p^s-\lfloor d/2\rfloor\}+1)}-1}{p^k-1}\right)-1.$$

Proof From Theorem 3.4, the number of negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ is $|\mathcal{A}\cup\mathcal{A}'| = |\mathcal{A}|+|\mathcal{A}'|-|\mathcal{A}\cap\mathcal{A}'|$. The desired result follows immediately from the discussion above. □

4 Self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$

In this section, the characterization and enumeration of self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ are established under both the Euclidean and Hermitian inner products.

4.1 Euclidean self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$

We define a *conjugation* $\overline{\cdot}$ on $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$ to be the map that fixes $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ and sends x^l to x^{-l} for all $l\in\mathbb{Z}_{p^s}$. For each subset A of the ring $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$, we denote by $\overline{A}$ the set of polynomials $\overline{f(x)}$ for all $f(x)$ in A. The following result can be derived similarly to [10, Theorem 18].

Theorem 4.1 *Let C be an ideal in $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$. Then $C^{\perp_{\mathrm{E}}}=\overline{\mathrm{Ann}(C)}$.*

Theorem 4.2 *The Euclidean dual $C^{\perp_{\mathrm{E}}}$ of the ideal $C=\left\langle\!\left\langle (x+1)^{i_0}+u\sum_{j=0}^{i_1-1}h_j(x+1)^j, u(x+1)^{i_1}\right\rangle\!\right\rangle$ given in Theorem 3.6 is of the form*

$$C^{\perp_{\mathrm{E}}}=\left\langle\!\!\left\langle (x+1)^{p^s-i_1}-u(x+1)^{p^s-i_0-i_1}\sum_{r=0}^{i_1-1}\sum_{j=0}^{r}(-1)^{i_0-r}\binom{i_0-j}{r-j}h_j(x+1)^r,\ u(x+1)^{p^s-i_0}\right\rangle\!\!\right\rangle.$$

Proof From Theorem 3.6, it can be concluded that

$$\mathrm{Ann}(C)=\left\langle\!\!\left\langle (x+1)^{p^s-i_1}-u(x+1)^{p^s-i_0-i_1}\sum_{j=0}^{i_1-1}h_j(x+1)^j,\ u(x+1)^{p^s-i_0}\right\rangle\!\!\right\rangle.$$

By Theorem 4.1, it follows that $C^{\perp_{\mathrm{E}}}=\overline{\mathrm{Ann}(C)}$. Hence, $C^{\perp_{\mathrm{E}}}$ contains the elements $u(x+1)^{p^s-i_0}$ and

$$(x+1)^{p^s-i_1}-u(x+1)^{p^s-i_0-i_1}\sum_{j=0}^{i_1-1}h_j(x+1)^jx^{i_0-j}.$$

By writing $x = (x+1) - 1$ and applying the Binomial Theorem, it can be concluded that $C^{\perp_E}$ contains an element of the form

$$(x+1)^{p^s-i_1} - u(x+1)^{p^s-i_0-i_1} \sum_{j=0}^{i_1-1} \sum_{l=0}^{i_0-j} (-1)^{i_0-j-l} \binom{i_0-j}{l} h_j (x+1)^{l+j}.$$

Hence,

$$\left\langle\!\!\left\langle (x+1)^{p^s-i_1} - u(x+1)^{p^s-i_0-i_1} \sum_{j=0}^{i_1-1} \sum_{l=0}^{i_0-j} (-1)^{i_0-j-l} \binom{i_0-j}{l} h_j (x+1)^{l+j},\ (x+1)^{p^s-i_1} \right\rangle\!\!\right\rangle \subseteq C^{\perp_E}.$$

Comparing the cardinalities, the two sets are equal. Updating the indices, it follows that

$$C^{\perp_E} = \left\langle\!\!\left\langle (x+1)^{p^s-i_1} - u(x+1)^{p^s-i_0-i_1} \sum_{r=0}^{i_1-1} \sum_{j=0}^{r} (-1)^{i_0-r} \binom{i_0-j}{r-j} h_j (x+1)^{r},\ (x+1)^{p^s-i_1} \right\rangle\!\!\right\rangle$$

as desired. □

We note that, if $i_1 = 0$, then $C = \langle u \rangle$ is the only Euclidean self-dual ideal.

Assume that C is Euclidean self-dual. Then $C = C^{\perp_E}$ which implies that $|C| = (p^k)^{p^s}$ and $i_0 + i_1 = p^s$.

Assume that $i_1 \geqslant 1$. Since

$$C = \left\langle\!\!\left\langle (x+1)^{i_0} + u \sum_{j=0}^{i_1-1} h_j (x+1)^j,\ u(x+1)^{i_1} \right\rangle\!\!\right\rangle$$

is Euclidean self-dual in $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/\langle x^{p^s} + 1\rangle$, it follows that $p^s = i_0 + i_1$ and

$$-h_t = \sum_{j=0}^{t} (-1)^{i_0-t} \binom{i_0-j}{t-j} h_j \tag{2}$$

in $\mathbb{F}_{p^k}$ for all $0 \leqslant t \leqslant i_i - 1$ by Theorem 4.2.

Let $V(p^s, i_1)$ be an $(i_1 \times i_1)$-matrix defined by

$$V(p^s, i_1) = \begin{bmatrix} (-1)^{i_0}+1 & 0 & 0 & \cdots & 0 \\ (-1)^{i_0-1}\binom{i_0}{1} & (-1)^{i_0-1}+1 & 0 & \cdots & 0 \\ (-1)^{i_0-2}\binom{i_0}{2} & (-1)^{i_0-2}\binom{i_0-1}{1} & (-1)^{i_0-2}+1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (-1)^{i_0-i_1+1}\binom{i_0}{i_1-1} & (-1)^{i_0-i_1+1}\binom{i_0-1}{i_1-2} & (-1)^{i_0-i_1+1}\binom{i_0-2}{i_1-3} & \cdots & (-1)^{i_0+i_1-1}+1 \end{bmatrix}. \tag{3}$$

It is easily seen that the i_1 equations from (2) are equivalent to the matrix equation

$$V(p^s, i_1)\boldsymbol{h} = \boldsymbol{0}, \tag{4}$$

where $\boldsymbol{h} = (h_0, h_1, \ldots, h_{i_1-1})^{\mathrm{T}}$ and $\boldsymbol{0} = (0, 0, \ldots, 0)^{\mathrm{T}}$.

Hence, the ideal C in $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$ is Euclidean self-dual if and only if $p^s=i_0+i_1$ and $h_0,h_1,\ldots,h_{i_1-1}$ satisfy (4). Since $h_0=h_1=\cdots=h_{i_1-1}=0$ is a solution to (4), the corresponding ideal $\langle (x+1)^{p^s-i_1}, u(x+1)^{i_1}\rangle$ is a Euclidean self-dual negacyclic code in $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$. Hence, for a fixed first torsion degree $1\leqslant i_1\leqslant p^s$, a Euclidean self-dual ideal in $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$ always exists. By solving (4), all Euclidean self-dual ideals in $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$ can be constructed.

In order to determine the number of solutions to (4), or equivalently, the nullity of $V(p^s,i_1)$, we recall the $(i_1\times i_1)$-matrix $M(p^s,i_1)$ over $\mathbb{F}_{p^k}$ defined in [13] as

$$M(p^s,i_1)=\begin{bmatrix} (-1)^{i_0}+1 & 0 & 0 & \ldots & 0\\ (-1)^{i_0}\binom{i_0}{1} & (-1)^{i_0+1}+1 & 0 & \ldots & 0\\ (-1)^{i_0}\binom{i_0}{2} & (-1)^{i_0+1}\binom{i_0-1}{1} & (-1)^{i_0+2}+1 & \ldots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ (-1)^{i_0}\binom{i_0}{i_1-1} & (-1)^{i_0+1}\binom{i_0-1}{i_1-2} & (-1)^{i_0+2}\binom{i_0-2}{i_1-3} & \ldots & (-1)^{i_0+i_1-1}+1 \end{bmatrix}.$$

The nullity of $V(p^s,i_1)$ can be determined in terms of $M(p^s,i_1)$ as in the following theorem.

Theorem 4.3 *Let i_1 be a positive integer such that $i_1\leqslant p^s$. Then the nullity of $V(p^s,i_1)$ is $\lfloor i_1/2\rfloor$.*

Proof First, we show that $V(p^s,i_1)$ and $M(p^s,i_1)$ have the same nullity. We consider the following two cases.

Case 1: i_1 is odd. Let $A=\mathrm{diag}(1,-1,\ldots,-1,1)$ be an $(i_1\times i_1)$-matrix over $\mathbb{F}_{p^s}$. It is not difficult to see that A is invertible and $AV(p^s,i_1)A=M(p^s,i_1)$.

Case 2: i_1 is even. Let $A=\mathrm{diag}(1,-1,\ldots,1,-1)$ be an $i_1\times i_1$ matrix over $\mathbb{F}_{p^s}$. It is not difficult to see that A is invertible and $AV(p^s,i_1)A=M(p^s,i_1)$.

From the two cases, the nullity of $V(p^s,i_1)$ and the nullity of $M(p^s,i_1)$ are equal. From [13, Proposition 3.3], the nullity of $M(p^s,i_1)$ is $\lfloor i_1/2\rfloor$. Hence, the nullity of $V(p^s,i_1)$ is $\lfloor i_1/2\rfloor$ as desired. □

Proposition 4.4 *Let $i_1>0$ and let κ be the nullity of $V(p^s,i_1)$ over $\mathbb{F}_{p^k}$. Then the number of Euclidean self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k}$ with first torsional degree i_1 is $(p^k)^\kappa$.*

From Theorem 3.6, we have $0\leqslant i_1\leqslant\lfloor p^s/2\rfloor$ since $i_0+i_1=p^s$.

Corollary 4.5 *Let k and s be positive integers and let p an odd prime. Then the number of Euclidean self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ is*

$$\mathrm{NE}(p^k,p^s)=\begin{cases} 2\left(\frac{(p^k)^{(p^s+1)/4}-1}{p^k-1}\right) & \text{if } p^s\equiv 3 \bmod 4,\\ 2\left(\frac{(p^k)^{(p^s-1)/4}-1}{p^k-1}\right)+(p^k)^{(p^s-1)/4} & \text{if } p^s\equiv 1 \bmod 4.\end{cases}$$

Proof From Theorem 4.3 and Proposition 4.4, the number of Euclidean self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ is $\sum_{i_1=0}^{\lfloor p^s/2\rfloor}(p^k)^{\lfloor i_1/2\rfloor}$. Note that $p^s\equiv 3 \bmod 4$ (resp., $p^s\equiv 1 \bmod 4$) if and only if $(p^s+1)/4$ (resp., $(p^s-1)/4$) is an integer. Hence, the results follow from a geometric sum. □

4.2 Hermitian self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$

Under the assumption that k is even, characterization and enumeration Hermitian self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$ are given. For a subset A of $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$, let

$$\widetilde{A}:=\left\{\sum_{i=0}^{p^s-1}\widetilde{a_i}x^i : \sum_{i=0}^{p^s-1}a_ix^i\in A\right\},$$

where $\widetilde{\cdot}$ is the automorphism defined in (1).

Based on the unique presentation of a negacyclic code given in Theorem 3.6, its Hermitian dual can be determined using Theorem 4.2 and the fact that $C^{\perp_{\mathrm{H}}}=\widetilde{C^{\perp_{\mathrm{E}}}}$.

Theorem 4.6 *The Hermitian dual $C^{\perp_{\mathrm{H}}}$ of the ideal $C=\left\langle\!\left\langle(x+1)^{i_0}+u\sum_{j=0}^{i_1-1}h_j(x+1)^j, u(x+1)^{i_1}\right\rangle\!\right\rangle$ given in Theorem 3.6 has the representation*

$$C^{\perp_{\mathrm{H}}}=\left\langle\!\!\left\langle(x+1)^{p^s-i_1}-u(x+1)^{p^s-i_0-i_1}\sum_{r=0}^{i_1-1}\sum_{j=0}^{r}(-1)^{i_0+r}\binom{i_0-j}{r-j}h_j^{p^{k/2}}(x+1)^r,\ u(x+1)^{p^s-i_0}\right\rangle\!\!\right\rangle.$$

If $i_1=0$, then it is not difficult to see that the ideal generated by u is the only Hermitian self-dual negacyclic code of length p^s over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$.

Assume that C is Hermitian self-dual. Then $C=C^{\perp_{\mathrm{H}}}$ implies that $|C|=(p^k)^{p^s}$ and $i_0+i_1=p^s$.

Assume that $i_1\geqslant 1$. Then, by Theorems 3.6 and 4.6, we have

$$-uh_t^{p^{k/2}}=u\sum_{j=0}^{t}(-1)^{i_0-t}\binom{i_0-j}{t-j}h_j$$

for all $0\leqslant t\leqslant i_1-1$.

From the i_1 equations above and the definition of $V(p^s,i_1)$, we have

$$V(p^s,i_1)\boldsymbol{x}+\left(\boldsymbol{x}^{p^{k/2}}-\boldsymbol{x}\right)=\boldsymbol{0} \tag{5}$$

where $\boldsymbol{x}=(x_1,x_2,\ldots,x_{i_1})^{\mathrm{T}}$, $\boldsymbol{x}^{p^{k/2}}=(x_1^{p^{k/2}},x_2^{p^{k/2}},\ldots,x_{i_1}^{p^{k/2}})^{\mathrm{T}}$ and $\boldsymbol{0}=(0,0,\ldots,0)^{\mathrm{T}}$. It can be concluded that an ideal C in $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$ is Hermitian self-dual if and only if $p^s=i_0+i_1$ and $h_0,h_1,\ldots,h_{i_1-1}$ satisfy (5). Since $h_0=h_1=\cdots=h_{i_1-1}=0$ is a solution to (5), the corresponding ideal $\langle(x+1)^{p^s-i_1}, u(x+1)^{i_1}\rangle$ is a Hermitian self-dual negacyclic code in $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$.

Hence, for a fixed first torsion degree $1 \leqslant i_1 \leqslant p^s$, a Hermitian self-dual negacyclic code in $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$ always exists. By solving (5), all Hermitian self-dual negacyclic codes in $(\mathbb{F}_{p^k}+u\mathbb{F}_{p^k})[x]/\langle x^{p^s}+1\rangle$ can be constructed.

In order to determine the number of solutions to (5), we shall need some properties of $V(p^s, i_1)$. For integers i and j such that $1 \leqslant i, j \leqslant i_1$, let v_{ij} denote the entry in the ith row and the jth column of the matrix $V(p^s, i_1)$. For an integer l, $1 \leqslant l \leqslant j < i \leqslant i_1$, we have

$$v_{ij} = (-1)^{i_0-i+1}\binom{i_0-j+1}{i-j}$$

and

$$v_{ij}v_{jl} = (-1)^{i_0-i+1}\binom{i-l}{j-l}v_{il}.$$

The following two maps in [10] are key to determine the number of solutions to (5) in $\mathbb{F}_{p^k}^{i_1}$:

- The map $\Psi\colon \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ is defined by $\alpha \mapsto \alpha^{p^{k/2}} - \alpha$ for all $\alpha \in \mathbb{F}_{p^k}$.
- The trace map $\mathrm{Tr}\colon \mathbb{F}_{p^k} \to \mathbb{F}_{p^{k/2}}$ is defined by $\alpha \mapsto \alpha^{p^{k/2}} + \alpha$ for all $\alpha \in \mathbb{F}_{p^k}$.

From [10], we have that Ψ and Tr are $\mathbb{F}_{p^{k/2}}$-linear.

Lemma 4.7 ([10, Lemma 3.2]) *Let* Tr *and* Ψ *be defined as above. Then the following statements hold:*

- *For each* $\alpha \in \mathbb{F}_{p^k}$, $\Psi(\alpha) = 0$ *if and only if* $\alpha \in \mathbb{F}_{p^{k/2}}$.
- $\Psi \circ \mathrm{Tr} \equiv \mathrm{Tr} \circ \Psi$.
- *For each* $a \in \Psi(\mathbb{F}_{p^k})$, $|\Psi^{-1}(a)| = p^{k/2}$.
- *For each* $a \in \mathrm{Tr}(\mathbb{F}_{p^{k/2}})$, $|\mathrm{Tr}^{-1}(a)| = p^{k/2}$.

Similarly to [10, Proposition 3.3], we have

Proposition 4.8 *Let k and s be positive integers such that k is even, and let p be an odd prime. Let i_1 be a positive integer such that $i_1 \leqslant \lfloor p^s/2 \rfloor$. Then the number of solutions to (5) in $\mathbb{F}_{p^k}^{i_1}$ is $p^{ki_1/2}$.*

Proof From (3), the diagonal of $V(p^s, i_1)$ has two different presentations depending on the parity of i_1. Hence, the proof consists of two cases.

Case 1: i_1 is odd. Then $i_1 = 2\mu + 1$ for some non-negative integer μ. From (3), the matrix $V(p^s, i_1)$ can be written as

$$V(p^s, i_1) = \begin{bmatrix} 2 & 0 & 0 & 0 & \cdots & 0 & 0 \\ * & 0 & 0 & 0 & \cdots & 0 & 0 \\ * & * & 2 & 0 & \cdots & 0 & 0 \\ * & * & * & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ * & * & * & * & \cdots & 0 & 0 \\ * & * & * & * & \cdots & * & 2 \end{bmatrix},$$

where $*$ denotes an entry of the matrix $V(p^s, i_1)$ as defined in (3). It is easily seen that

$$\mathrm{Tr}(x_1) = 0, \tag{6}$$

$$\Psi(x_{2I}) = -\sum_{j=1}^{2i-1} v_{2i,j} x_j, \tag{7}$$

$$\mathrm{Tr}(x_{2i+1}) = -\sum_{j=1}^{2i} v_{2i+1,j} x_j \tag{8}$$

for all integers $1 \leqslant i \leqslant \mu$. We observe that (5) has a solution if and only if the right-hand sides of (6) and (8) are in $\mathbb{F}_{p^{k/2}}$ and the right-hand side of (7) is in $\Psi(\mathbb{F}_{p^k})$. In this case, it can be deduced that

$$x_1 \in \mathrm{Tr}^{-1}(0), \quad x_{2i} \in \Psi^{-1}\left(-\sum_{j=1}^{2i-1} v_{2i,j} x_j\right) \quad \text{and} \quad x_{2i+1} \in \mathrm{Tr}^{-1}\left(-\sum_{j=1}^{2i} v_{2i+1,j} x_j\right)$$

for all integers $1 \leqslant i \leqslant \mu$. Equivalently, the number of solutions to (5) is $p^{ki_1/2}$ by Lemma 4.7.

To reason the discussion above, by Lemma 4.7, it suffices to show that the images under Ψ of the right-hand sides of (6) and (8) are 0 and the image under the trace map Tr of the right-hand side of (7) is 0. We note that the image under Ψ of the right-hand sides of (6) is 0.

Let $1 \leqslant i \leqslant \mu$ be an integer. Using calculation similar to the one in [10, Equation (3.11)], it follows that

$$\mathrm{Tr}\left(-\sum_{j=1}^{2i-1} v_{2i,j} x_j\right) = -\sum_{j=1}^{2i-1} v_{2i,j} \mathrm{Tr}(x_j) = 0 \quad \text{in} \quad \mathbb{F}_{p^{k/2}}.$$

Using calculation similar to the one in [10, Equation (3.12)], it follows that

$$\Psi\left(-\sum_{j=1}^{2i} v_{2i+1,j} x_j\right) = -\sum_{j=1}^{2i} v_{2i+1,j} \Psi(x_j) = 0 \quad \text{in} \quad \mathbb{F}_{p^{k/2}}.$$

Case 2: i_1 is even. Then $i_1 = 2\mu$ for some positive integer μ. From (3), the matrix $V(p^s, i_1)$ can be written as

$$V(p^s, i_1) = \begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & 0 \\ * & 2 & 0 & 0 & \cdots & 0 \\ * & * & 0 & 0 & \cdots & 0 \\ * & * & * & 2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & * & \cdots & 2 \end{bmatrix},$$

where $*$ denotes an entry of the matrix $V(p^s, i_1)$ defined in (3). We see that

$$\Psi(x_{2i-1}) = -\sum_{j=1}^{2i-2} v_{2i-1,j}x_j, \tag{9}$$

$$\mathrm{Tr}(x_{2i}) = -\sum_{j=1}^{2i-1} v_{2i,j}x_j \tag{10}$$

for all integers $1 \leqslant i \leqslant \mu$.

We observe that (5) has a solution if and only if the right-hand side of (9) is in $\Psi(\mathbb{F}_{p^k})$ and the right-hand side of (10) is in $\mathbb{F}_{p^{k/2}}$. In this case, the number of solutions to (5) is $p^{ki_1/2}$ by Lemma 4.7. By Lemma 4.7 again, it is sufficient to show that the image under the trace map Tr of right-hand side of (9) and the image under the Ψ of right-hand side of (10) are 0. By using calculation similar to the one in Case 1, the proof is completed. □

Corollary 4.9 *Let k and s be positive integers such that k is even, and let p be an odd prime. Then the number of Hermitian self-dual negacyclic codes of length p^s over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ is*

$$\mathrm{NH}(p^k, p^s) = \sum_{i_1=0}^{\lfloor p^s/2 \rfloor} p^{ki_1/2} = \frac{(p^{k/2})^{\lfloor p^s/2\rfloor+1} - 1}{p^{k/2} - 1}.$$

Acknowledgements The authors would like to thank the anonymous referees for very helpful comments.

References

1. Cao, Y.: On constacyclic codes over finite chain rings. Finite Fields Appl. **24**, 124–135 (2013)
2. Choosuwan, P., Jitman, S., Udomkavanich, P.: Self-dual abelian codes in some nonprincipal ideal group algebras. Math. Probl. Eng. **2016**, # 9020173 (2016)
3. 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)
4. Dinh, H.Q.: Negacyclic codes of length 2^s over Galois rings. IEEE Trans. Inform. Theory **51**(12), 4252–4262 (2005)
5. Dinh, H.Q., López-Permouth, S.R.: Cyclic and negacyclic codes over finite chain rings. IEEE Trans. Inform. Theory **50**(8), 1728–1744 (2004)
6. Dinh, H.Q., Nguyen, B.T., Sriboonchitta, S.: Negacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and their duals. Discrete Math. **341**(4), 1055–1071 (2018)
7. 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. **9**, # 1850173 (2018)
8. 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)
9. Hammons Jr., A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. Inform. Theory **40**(2), 301–319 (1994)
10. Jitman, S., Ling, S., Sangwisut, E.: On self-dual cyclic codes of length p^a over $\mathrm{GR}(p^2, s)$. Adv. Math. Commun. **10**(2), 255–273 (2016)
11. Kai, X., Zhu, S.: Negacyclic self-dual codes over finite chain rings. Des. Codes Cryptogr. **62**(2), 161–174 (2012)

12. Kiah, H.M., Leung, K.H., Ling, S.: Cyclic codes over $\mathrm{GR}(p^2, m)$ of length p^k. Finite Fields Appl. **14**(3), 834–846 (2008)
13. Kiah, H.M., Leung, K.H., Ling, S.: A note on cyclic codes over $\mathrm{GR}(p^2, m)$ of length p^k. Des. Codes Cryptogr. **63**(1), 105–112 (2012)
14. Liu, X., Xu, X.: Cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Acta Math. Sci. Ser. B Engl. Ed. **34**(3), 829–839 (2014)
15. Sobhani, R., Esmaeili, M.: Cyclic and negacyclic codes over the Galois ring $\mathrm{GR}(p^2, m)$. Discrete Appl. Math. **157**(13), 2892–2903 (2009)
16. Wolfman, J.: Negacyclic and cyclic codes over $\mathbb{Z}_4$. IEEE Trans. Inform. Theory **45**(7), 2527–2532 (1999)