Several Families of Ternary Negacyclic Codes and Their Duals

Zhonghua Sun and Cunsheng Ding

***Abstract*— Constacyclic codes contain cyclic codes as a subclass and have nice algebraic structures. Constacyclic codes have theoretical importance, as they are connected to a number of areas of mathematics and outperform cyclic codes in several aspects. Negacyclic codes are a subclass of constacyclic codes and are distance-optimal in many cases. However, compared with the extensive study of cyclic codes, negacyclic codes are much less studied. In this paper, several families of ternary negacyclic codes and their duals are constructed and analysed. These families of negacyclic codes and their duals contain distance-optimal codes and have very good parameters in general. The duals of three families of ternary negacyclic codes presented in this paper are distance-optimal.**

***Index Terms*— Cyclic code, negacyclic code, linear code.**

I. Introduction and Motivations

A. Constacyclic Codes

FOR a given prime power q, let $\mathrm{GF}(q)$ denote the finite field with q elements, and let $\mathrm{GF}(q)^*$ denote the multiplicative group of $\mathrm{GF}(q)$. A q-ary $[n, k, d]$ linear code $\mathcal{C}$ is a k-dimensional linear subspace of $\mathrm{GF}(q)^n$ with minimum distance d. Let $\lambda \in \mathrm{GF}(q)^*$. A q-ary linear code $\mathcal{C}$ of length n is said to be λ-*constacyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$. Let

$$\Phi: \ \mathrm{GF}(q)^n \to \mathrm{GF}(q)[x]/(x^n - \lambda)$$
$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}.$$

It is known each ideal of the quotient ring $\mathrm{GF}(q)[x]/(x^n - \lambda)$ is *principal* and a q-ary linear code $\mathcal{C}$ of length n is λ-constacyclic if and only if $\Phi(\mathcal{C})$ is an ideal of the quotient ring $\mathrm{GF}(q)[x]/(x^n - \lambda)$. Due to this fact, we will identify $\Phi(\mathcal{C})$ with $\mathcal{C}$ for any λ-constacyclic code $\mathcal{C}$. Let $\mathcal{C} = (g(x))$ be a q-ary λ-constacyclic code of length n, where $g(x)$ is monic and has the smallest degree. Then $g(x)$ is called the *generator polynomial* and $h(x) = (x^n - \lambda)/g(x)$ is referred to as the *check polynomial* of $\mathcal{C}$. A q-ary λ-constacyclic code $\mathcal{C}$ is said to be *irreducible* if its check polynomial is irreducible over $\mathrm{GF}(q)$. By definition, a 1-constacyclic code is a *cyclic code*. In particular, (-1)-constacyclic codes are called *negacyclic* codes. Hence, cyclic codes form a subclass of constacyclic codes. Further information on constacyclic codes can be found in [1], [3], [4], [8], [9], [10], [11], [24], [26], [27], [28], [30], [32], [35], [36], [37], [38], [39], [42], [43], and [45] and the references therein.

Manuscript received 19 February 2023; revised 30 August 2023; accepted 29 December 2023. Date of publication 4 January 2024; date of current version 23 April 2024. The work of Zhonghua Sun was supported by the National Natural Science Foundation of China under Grant 62002093 and Grant 12171134. The work of Cunsheng Ding was supported by the Hong Kong Research Grants Council under Grant 16301522. *(Corresponding author: Cunsheng Ding.)*

Zhonghua Sun is with the School of Mathematics, Hefei University of Technology, Hefei, Anhui 230601, China (e-mail: sunzhonghuas@163.com).

Cunsheng Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong, China (e-mail: cding@ust.hk).

Communicated by S. R. Ghorpade, Associate Editor for Coding and Decoding.

Digital Object Identifier 10.1109/TIT.2024.3349996

TABLE I
THE BEST TERNARY CYCLIC CODES AND TERNARY NEGACYCLIC CODES

Best cyclic codes	Best negacyclic codes	Best linear codes
$[10, 4, 4]$	$[10, 4, 6]$	$[10, 4, 6]$
$[10, 6, 2]$	$[10, 6, 4]$	$[10, 6, 4]$
$[14, 6, 4]$	$[14, 6, 6]$	$[14, 6, 6]$
$[14, 8, 2]$	$[14, 8, 5]$	$[14, 8, 5]$
$[20, 10, 6]$	$[20, 10, 7]$	$[20, 10, 7]$
$[20, 12, 4]$	$[20, 12, 5]$	$[20, 12, 6]$
$[20, 16, 2]$	$[20, 16, 3]$	$[20, 16, 3]$

B. Motivations and Objectives

Negacyclic codes over finite fields are a subclass of constacyclic codes, and were first studied by Berlekamp [1] for correcting errors measured in the Lee metric. Therefore, the history of negacyclic codes goes back to 1966. In the past 56 years, some works on the application of negacyclic codes in quantum codes were done (see [15], [21], [22], [23], [34], [45]). However, only a few references about theoretical results of negacyclic codes have appeared in the literature [1], [2], [9], [31], [36], [44]. Hence, very limited results on the parameters of negacyclic codes over finite fields are known in the literature.

Negacyclic codes have similar algebraic structures as cyclic codes. With the help of Magma, we found that the best ternary negacyclic code of certain length and dimension has a better error-correcting capability than the best ternary cyclic code of the same length and dimension. Some examples of such code parameters are given in Table I. Therefore, it is very interesting to study ternary negacyclic codes. This is the main motivation of studying ternary negacyclic codes in this paper. The objectives of this paper are the following:

1) Construct and analyse several families of ternary negacyclic codes.
2) Study parameters of the duals of these ternary negacyclic codes.

C. The Organisation of This Paper

The rest of this paper is organized as follows. In Section II, we present some auxiliary results. In Section III, we prove a general result for negacyclic codes of even length.

In Section IV, we study the parameters of the first family of ternary negacyclic codes and their duals. In Section V, we investigate the parameters of the second family of ternary negacyclic codes and their duals. In Section VI, we analyse the parameters of the third family of ternary negacyclic codes and their duals. In Section VII, we study the parameters of the fourth family of ternary negacyclic codes. These families of negacyclic codes and their duals have very good parameters. In Section VIII, we conclude this paper and make some concluding remarks.

II. Preliminaries

Throughout this section, let q be an odd prime power, $\mathrm{GF}(q)$ be the finite field with q elements and n be a positive integer with $\gcd(n, q) = 1$. For a linear code $\mathcal{C}$, we use $\dim(\mathcal{C})$ and $d(\mathcal{C})$ to denote its dimension and minimum Hamming distance, respectively.

A. Cyclotomic Cosets

To deal with q-ary negacyclic codes of length n, we need to define q-cyclotomic cosets modulo $2n$.

Let $\mathbb{Z}_{2n} = \{0, 1, 2, \cdots, 2n-1\}$ be the ring of integers modulo $2n$. For any integer i, let $i \bmod 2n$ denote the unique integer s such that $0 \le s \le 2n-1$ and $i - s$ is divisible by $2n$ throughout this paper. For any $i \in \mathbb{Z}_{2n}$, the *q-cyclotomic coset of i modulo $2n$* is defined by

$$C_i^{(q,2n)} = \left\{iq^j \bmod 2n : 0 \le j \le \ell_i - 1\right\} \subseteq \mathbb{Z}_{2n},$$

where ℓ_i is the smallest positive integer such that $i \equiv iq^{\ell_i} \pmod{2n}$, and is the *size* of the q-cyclotomic coset. The smallest integer in $C_i^{(q,2n)}$ is called the *coset leader* of $C_i^{(q,2n)}$. Let $\Gamma_{(q,2n)}$ be the set of all the coset leaders. We have then $C_i^{(q,2n)} \cap C_j^{(q,2n)} = \emptyset$ for any two distinct elements i and j in $\Gamma_{(q,2n)}$, and $\bigcup_{i\in\Gamma_{(q,2n)}} C_i^{(q,2n)} = \mathbb{Z}_{2n}$.

Let $m = \mathrm{ord}_{2n}(q)$ be the order of q modulo $2n$. Let α be a primitive element of $\mathrm{GF}(q^m)$ and let $\beta = \alpha^{(q^m-1)/2n}$. Then β is a primitive $2n$-th root of unity in $\mathrm{GF}(q^m)$ and $\beta^n = -1$. The *minimal polynomial* $\mathbb{M}_{\beta^i}(x)$ of β^i over $\mathrm{GF}(q)$ is the monic polynomial of the smallest degree over $\mathrm{GF}(q)$ with β^i as a zero. We have

$$\mathbb{M}_{\beta^i}(x) = \prod_{j\in C_i^{(q,2n)}} (x - \beta^j) \in \mathrm{GF}(q)[x],$$

which is irreducible over $\mathrm{GF}(q)$. It then follows that

$$x^{2n} - 1 = \prod_{i\in\Gamma_{(q,2n)}} \mathbb{M}_{\beta^i}(x).$$

Define $\Gamma_{(q,2n)}^{(1)} = \left\{i : i \in \Gamma_{(q,2n)},\ i \equiv 1 \pmod 2\right\}$. Then

$$x^n + 1 = \prod_{i\in\Gamma_{(q,2n)}^{(1)}} \mathbb{M}_{\beta^i}(x).$$

B. Zeros, BCH Bound and Trace Representation of Negacyclic Codes

Let $\mathcal{C}$ be a q-ary negacyclic code of length n with generator polynomial $g(x)$. Then there is a subset $\Gamma \subseteq \Gamma_{(q,2n)}^{(1)}$ such that $g(x) = \prod_{i\in\Gamma} \mathbb{M}_{\beta^i}(x)$. Let $T = \cup_{i\in\Gamma} C_i^{(q,2n)}$. The elements in the *zero set* $\mathcal{Z}(\mathcal{C}) := \left\{\beta^i :\ i \in T\right\}$ are called the *zeros* of the negacyclic code $\mathcal{C}$ and the elements in the set

$$\left\{\beta^i :\ i \in \mathbb{Z}_{2n}\backslash T \text{ and } i \text{ is odd}\right\}$$

are the *nonzeros* of $\mathcal{C}$. It is easily seen that

$$\dim(\mathcal{C}) = n - |\mathcal{Z}(\mathcal{C})|.$$

The minimum distance of the negacyclic code $\mathcal{C}$ has the following lower bound.

Lemma 1 (The BCH bound for negacyclic codes [24, Lemma 4]): Let $\mathcal{C}$ be a q-ary negacyclic code of length n with zero set $\mathcal{Z}(\mathcal{C})$. If there are odd integer b, integer e with $\gcd(e, n) = 1$, integer δ with $2 \le \delta \le n$ and integer h such that

$$\left\{\beta^{b+2ei} : h \le i \le h + \delta - 2\right\} \subseteq \mathcal{Z}(\mathcal{C}),$$

then $d(\mathcal{C}) \ge \delta$.

The trace representation of negacyclic codes is documented below (see, e.g., [10], [38], [43, Theorem 1]).

Lemma 2: Let n be a positive integer such that $\gcd(n, q) = 1$. Let $m = \mathrm{ord}_{2n}(q)$ and $\beta \in \mathrm{GF}(q^m)$ be a primitive $2n$-th root of unity. Let $\mathcal{C}$ be the q-ary negacyclic code of length n with check polynomial $\prod_{j=1}^{s} \mathbb{M}_{\beta^{i_j}}(x)$, where $C_{i_a}^{(q,2n)} \cap C_{i_b}^{(q,2\ n)} = \emptyset$ for $a \ne b$. Then $\mathcal{C}$ has the trace representation

$$\{(\sum_{j=1}^{s} \mathrm{Tr}_{q^{m_j}/q}(a_j\beta^{-ti_j}))_{t=0}^{n-1}\ :\ a_j \in \mathrm{GF}(q^{m_j}),\ 1 \le j \le s\},$$

where $m_j = |C_{i_j}^{(q,2n)}|$ and $\mathrm{Tr}_{q^m/q}$ denotes the trace function from $\mathrm{GF}(q^m)$ to $\mathrm{GF}(q)$.

C. The Duals of Negacyclic Codes

Let $\mathcal{C}$ be a q-ary linear code of length n. Then its *dual code*, denoted by $\mathcal{C}^\perp$, is defined by

$$\mathcal{C}^\perp = \{(c_0, c_1, \ldots, c_{n-1}) \in \mathrm{GF}(q)^n :\ \sum_{i=0}^{n-1} c_i b_i = 0,\ \forall\ (b_0, b_1, \ldots, b_{n-1}) \in \mathcal{C}\}.$$

Similar to classical cyclic codes, the dual codes of negacyclic codes are also negacyclic codes. Let

$$f(x) = f_0 + f_1 x + \cdots + f_t x^t \in \mathrm{GF}(q)[x],$$

where $f_0 f_t \ne 0$ and t is a positive integer. The *reciprocal polynomial* of $f(x)$, denoted by $\widehat{f}(x)$, is defined by $\widehat{f}(x) = f_0^{-1} x^t f(x^{-1})$. Negacyclic codes and their duals have the following relation, which is a fundamental result.

Lemma 3: [24] Let $\mathcal{C}$ be a q-ary negacyclic code of length n generated by $g(x)$. Then the dual code of $\mathcal{C}$ is the q-ary negacyclic code of length n generated by $\widehat{h}(x)$, where $h(x) = (x^n + 1)/g(x)$.

D. Bounds of Linear Codes

We recall the following two bounds on linear codes, which will be needed in the sequel.

Lemma 4: (Sphere Packing Bound [17]) Let $\mathcal{C}$ be a q-ary $[n, k, d]$ linear code. Then

$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i}(q-1)^i \le q^{n-k},$$

where $\lfloor \cdot \rfloor$ is the floor function.

The following lemma is the sphere packing bound for even minimum distances.

Lemma 5: [11] Let $\mathcal{C}$ be a q-ary $[n, k, d]$ linear code, where d is an even integer. Then

$$\sum_{i=0}^{(d-2)/2} \binom{n-1}{i}(q-1)^i \le q^{n-1-k}.$$

A q-ary $[n, k, d]$ linear code is said to be *distance-optimal* if there is no q-ary $[n, k, d']$ linear code with $d' > d$. A q-ary $[n, k, d]$ linear code is said to be *dimension-optimal* if there is no q-ary $[n, k', d]$ linear code with $k' > k$. A q-ary $[n, k, d]$ linear code is said to be *length-optimal* if there is no q-ary $[n', k, d]$ linear code with $n' < n$. A linear code is said to be *optimal* if it is distance-optimal, dimension-optimal or length-optimal.

E. Several Equivalences of Linear Codes

In this paper, we will need the following notions:

- The permutation automorphism group of a linear code $\mathcal{C}$ denoted by $\mathrm{PAut}(\mathcal{C})$ and the permutation equivalence of two linear codes over a finite field.
- The monomial automorphism group of a linear code $\mathcal{C}$ denoted by $\mathrm{MAut}(\mathcal{C})$ and the monomial equivalence of two linear codes over a finite field.
- The automorphism group of a linear code $\mathcal{C}$ denoted by $\mathrm{Aut}(\mathcal{C})$ and the equivalence of two linear codes over a finite field.

For the definitions of these concepts, the reader is referred to [6, Section 2.8] or [17, Chapter 1]. Two q-ary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be *scalar-equivalent* if there is an invertible diagonal matrix $\mathbf{D}$ over $\mathrm{GF}(q)$ such that $\mathcal{C}_2 = \mathcal{C}_1\mathbf{D}$.

When n is an odd positive integer, let

$$\begin{aligned} \psi: \ \mathrm{GF}(q)[x]/(x^n+1) &\to \mathrm{GF}(q)[x]/(x^n-1), \\ c(x) &\mapsto c(-x). \end{aligned}$$

It is easily checked that ψ is a ring isomorphism. Define $\psi(\mathcal{C}) = \{\psi(\mathbf{c}) : \ \mathbf{c} \in \mathcal{C}\}$. Then we have the following result.

Theorem 6: [2] Let n be an odd positive integer. Then $\mathcal{C}$ is a q-ary negacyclic code of length n if and only if $\psi(\mathcal{C})$ is a q-ary cyclic code of length n. Furthermore, the negacyclic code $\mathcal{C}$ is scalar-equivalent to the cyclic code $\psi(\mathcal{C})$.

Table I shows that there are distance-optimal negacyclic codes that are not scalar-equivalent to cyclic codes. Although a negacyclic code $\mathcal{C}$ of odd length n is scalar-equivalent to a cyclic code $\psi(\mathcal{C})$, it is still valuable to study $\mathcal{C}$, as the parameters of the cyclic code $\psi(\mathcal{C})$ may still be open in the literature.

III. A Theorem About Negacyclic Codes of Even Length

Let n be an even integer and $q \equiv 1 \pmod 4$, then there is a $\lambda \in \mathrm{GF}(q)^*$ such that $\lambda^2 = -1$. It follows that

$$x^n + 1 = (x^{n/2} - \lambda)(x^{n/2} + \lambda).$$

Let $e_1(x) = \frac{\lambda}{2}(x^{n/2} - \lambda)$ and $e_2(x) = -\frac{\lambda}{2}(x^{n/2} + \lambda)$. In the ring $R := \mathrm{GF}(q)[x]/(x^n+1)$, it is easily checked that $e_1(x) + e_2(x) = 1$, $e_1(x)^2 = e_1(x)$, $e_2(x)^2 = e_2(x)$ and $e_1(x)e_2(x) = 0$. Then R is the direct sum of the ideals generated by the $e_i(x)$, i.e., $R = e_1(x)R + e_2(x)R$. Furthermore,

$$e_1(x)R \cong \mathrm{GF}(q)[x]/(x^{n/2} + \lambda)$$

and $e_2(x)R \cong \mathrm{GF}(q)[x]/(x^{n/2} - \lambda)$. Let $\mathcal{C}$ be a q-ary negacyclic code of length n. We associate to $\mathcal{C}$ the following two q-ary linear codes:

$$\begin{aligned} \mathrm{Res}_1(\mathcal{C}) &= \left\{ c(x) \pmod{x^{n/2} + \lambda} : \ c(x) \in \mathcal{C} \right\}, \\ \mathrm{Res}_2(\mathcal{C}) &= \left\{ c(x) \pmod{x^{n/2} - \lambda} : \ c(x) \in \mathcal{C} \right\}. \end{aligned}$$

By definition, the code $\mathrm{Res}_1(\mathcal{C})$ (resp. $\mathrm{Res}_2(\mathcal{C})$) is a q-ary $(-\lambda)$-constacyclic (resp. λ-constacyclic) code of length $n/2$. Moreover, we have the following results.

Theorem 7: Let n be an even integer and $q \equiv 1 \pmod 4$. Let $\mathcal{C}$ be a q-ary negacyclic code of length n with generator polynomial $g(x)$. Then

$$\begin{aligned} \mathcal{C} &= e_1\mathrm{Res}_1(\mathcal{C}) + e_2\mathrm{Res}_2(\mathcal{C}) \\ &= \{e_1(x)c_1(x) + e_2(x)c_2(x) : \ c_1(x) \in \mathrm{Res}_1(\mathcal{C}), \\ &\quad c_2(x) \in \mathrm{Res}_2(\mathcal{C})\}. \end{aligned}$$

Furthermore, the following hold.

1) The code $\mathrm{Res}_1(\mathcal{C})$ is the q-ary $(-\lambda)$-constacyclic code of length $n/2$ with generator polynomial
$$g_1(x) = \gcd(g(x), x^{n/2} + \lambda).$$
2) The code $\mathrm{Res}_2(\mathcal{C})$ is the q-ary λ-constacyclic code of length $n/2$ with generator polynomial
$$g_2(x) = \gcd(g(x), x^{n/2} - \lambda).$$
3) $\dim(\mathcal{C}) = \dim(\mathrm{Res}_1(\mathcal{C})) + \dim(\mathrm{Res}_2(\mathcal{C}))$.
4) If $(x^{n/2} - \lambda) \mid g(x)$, then $d(\mathcal{C}) = 2 \cdot d(\mathrm{Res}_1(\mathcal{C}))$.
5) If $(x^{n/2} + \lambda) \mid g(x)$, then $d(\mathcal{C}) = 2 \cdot d(\mathrm{Res}_2(\mathcal{C}))$.
6) If $(x^{n/2} - \lambda) \nmid g(x)$ and $(x^{n/2} + \lambda) \nmid g(x)$, then
$$d(\mathcal{C}) = 2 \cdot \min\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\},$$
provided that
$$\begin{aligned} &2 \cdot \min\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\} \\ &\quad \le \max\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\}, \end{aligned}$$
and
$$\begin{aligned} &\max\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\} \le d(\mathcal{C}) \\ &\quad \le 2 \cdot \min\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\}, \end{aligned}$$
provided that
$$\begin{aligned} &2 \cdot \min\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\} \\ &\quad > \max\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\}. \end{aligned}$$

Proof: Firstly, we prove that $\mathrm{Res}_i(\mathcal{C})$ is the q-ary constacyclic code generated by $g_i(x)$. Let $\mathcal{D}$ be the q-ary $(-\lambda)$-constacyclic code of length $n/2$ with generator polynomial $g_1(x)$. Let $c_1(x) \in \mathrm{Res}_1(\mathcal{C})$, then there is $c(x) \in \mathcal{C}$ such that

$$c_1(x) \equiv c(x) \pmod{x^{n/2}+\lambda}.$$

It is clear that

$$\gcd(c(x), x^{n/2}+\lambda) = \gcd(c_1(x), x^{n/2}+\lambda).$$

Then $g_1(x)$ divides $c_1(x)$. It follows that $\mathrm{Res}_1(\mathcal{C}) \subseteq \mathcal{D}$. On the other hand, let $c_2(x) \in \mathcal{D}$, then $g_1(x)$ divides $c_2(x)$. Noting that $\gcd\left(\frac{x^{n/2}+\lambda}{g_1(x)}, \frac{g(x)}{g_1(x)}\right) = 1$, then there are $a_1(x)$ and $a_2(x)$ such that

$$a_1(x)\left(\frac{x^{n/2}+\lambda}{g_1(x)}\right) + a_2(x)\left(\frac{g(x)}{g_1(x)}\right) = 1.$$

It follows that

$$\begin{aligned} c(x) &:= a_2(x)\left(\frac{g(x)}{g_1(x)}\right)c_2(x) \\ &= c_2(x) - a_1(x)\left(\frac{x^{n/2}+\lambda}{g_1(x)}\right)c_2(x). \end{aligned}$$

Since $g_1(x) \mid c_2(x)$, we have $g(x) \mid c(x)$ and

$$c_2(x) \equiv c(x) \pmod{x^{n/2}+\lambda}.$$

Therefore, $c_2(x) \in \mathrm{Res}_1(\mathcal{C})$. It follows that $\mathcal{D} \subseteq \mathrm{Res}_1(\mathcal{C})$. Consequently, $\mathrm{Res}_1(\mathcal{C}) = \mathcal{D}$, i.e., $\mathrm{Res}_1(\mathcal{C})$ is the q-ary $(-\lambda)$-constacyclic code of length $n/2$ with generator polynomial $g_1(x)$. By a similar method, we can prove that $\mathrm{Res}_2(\mathcal{C})$ is the q-ary λ-constacyclic code of length $n/2$ with generator polynomial $g_2(x)$.

Secondly, we prove that $\mathcal{C} = e_1\mathrm{Res}_1(\mathcal{C}) + e_2\mathrm{Res}_2(\mathcal{C})$. Since $1 = e_1(x) + e_2(x)$, any $c(x) \in \mathcal{C}$ can be written uniquely in the form

$$\begin{aligned} c(x) &= e_1(x)c(x) + e_2(x)c(x) \\ &= e_1(x)c_1(x) + e_2(x)c_2(x), \end{aligned}$$

where $c_1(x) \equiv c(x) \pmod{x^{n/2}+\lambda} \in \mathrm{Res}_1(\mathcal{C})$ and

$$c_2(x) \equiv c(x) \pmod{x^{n/2}-\lambda} \in \mathrm{Res}_2(\mathcal{C}).$$

Therefore, $\mathcal{C} \subseteq e_1\mathrm{Res}_1(\mathcal{C}) + e_2\mathrm{Res}_2(\mathcal{C})$. On the other hand,

$$\dim(\mathrm{Res}_1(\mathcal{C})) = n/2 - \deg(g_1(x))$$

and $\dim(\mathrm{Res}_2(\mathcal{C})) = n/2 - \deg(g_2(x))$. It is easily checked that $g(x) = g_1(x)g_2(x)$. Then

$$\begin{aligned} \dim(\mathcal{C}) &= n - \deg(g(x)) \\ &= n - \deg(g_1(x)) - \deg(g_2(x)) \\ &= \dim(\mathrm{Res}_1(\mathcal{C})) + \dim(\mathrm{Res}_2(\mathcal{C})). \end{aligned}$$

Therefore,

$$\begin{aligned} |\mathcal{C}| &= |\mathrm{Res}_1(\mathcal{C})| \cdot |\mathrm{Res}_2(\mathcal{C})| \\ &= |e_1\mathrm{Res}_1(\mathcal{C}) + e_2\mathrm{Res}_2(\mathcal{C})|. \end{aligned}$$

Consequently, $\mathcal{C} = e_1\mathrm{Res}_1(\mathcal{C}) + e_2\mathrm{Res}_2(\mathcal{C})$.

Finally, we study the minimum distance of $\mathcal{C}$. Let

$$c(x) = e_1(x)c_1(x) + e_2(x)c_2(x) \in \mathcal{C}$$

and $c(x) \neq 0$, where $c_1(x) \in \mathrm{Res}_1(\mathcal{C})$ and $c_2(x) \in \mathrm{Res}_2(\mathcal{C})$ are not all 0. Noting that

$$c(x) = \frac{\lambda}{2}(c_1(x) - c_2(x))x^{n/2} + \frac{1}{2}(c_1(x) + c_2(x)),$$

we have

$$\mathtt{wt}(c(x)) = \mathtt{wt}(c_1(x) - c_2(x)) + \mathtt{wt}(c_1(x) + c_2(x)). \quad (1)$$

There are the following three cases.

- If $(x^{n/2}-\lambda) \mid g(x)$, then $\mathrm{Res}_2(\mathcal{C}) = \{\mathbf{0}\}$, i.e., $c_2(x) \equiv 0$. It follows from (1) that
$$\mathtt{wt}(c(x)) = 2 \cdot \mathtt{wt}(c_1(x)).$$
Therefore, $d(\mathcal{C}) = 2 \cdot d(\mathrm{Res}_1(\mathcal{C}))$.
- If $(x^{n/2}+\lambda) \mid g(x)$, then $\mathrm{Res}_1(\mathcal{C}) = \{\mathbf{0}\}$. i.e., $c_1(x) \equiv 0$. It follows from (1) that
$$\mathtt{wt}(c(x)) = 2 \cdot \mathtt{wt}(c_2(x)).$$
Therefore, $d(\mathcal{C}) = 2 \cdot d(\mathrm{Res}_2(\mathcal{C}))$.
- If $(x^{n/2}-\lambda) \nmid g(x)$ and $(x^{n/2}+\lambda) \nmid g(x)$, then $\mathrm{Res}_i(\mathcal{C}) \neq \{\mathbf{0}\}$ for $i \in \{1,2\}$. On one hand, if $c_1(x) = 0$ (resp. $c_2(x) = 0$), from (1), $\mathtt{wt}(c(x)) = 2 \cdot \mathtt{wt}(c_2(x))$ (resp. $\mathtt{wt}(c(x)) = 2 \cdot \mathtt{wt}(c_1(x))$). For any two elements a and b in $\mathrm{GF}(q)$, we have $a - b = 0$ and $a + b = 0$ if and only if $a = b = 0$, as q is odd. On the other hand, if $c_1(x) \neq 0$ and $c_2(x) \neq 0$, then
$$\begin{aligned} \mathtt{wt}(c(x)) &\geq \max\{\mathtt{wt}(c_1(x)), \mathtt{wt}(c_2(x))\} \\ &\geq \max\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\}. \end{aligned}$$
Combining the results above with the discussions of the two cases above, we have the following conclusions.
  - If
  $$\begin{aligned} &2 \cdot \min\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\} \\ &\quad \leq \max\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\} \end{aligned}$$
  we have
  $$d(\mathcal{C}) = 2 \cdot \min\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\}.$$
  - If
  $$\begin{aligned} &\max\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\} \\ &\quad < 2 \cdot \min\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\}, \end{aligned}$$
  we have
  $$\begin{aligned} &\max\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\} \leq d(\mathcal{C}) \\ &\quad \leq 2 \cdot \min\{d(\mathrm{Res}_1(\mathcal{C})), d(\mathrm{Res}_2(\mathcal{C}))\}. \end{aligned}$$

This completes the proof. ■

For two q-ary linear codes $\mathcal{C}_1, \mathcal{C}_2$ of length n, the $u+v|u-v$ *construction* (see [18]) is defined by

$$\mathcal{C}_1 \curlyvee \mathcal{C}_2 = \{(\mathbf{c}_1 + \mathbf{c}_2, \mathbf{c}_1 - \mathbf{c}_2) : \ \mathbf{c}_1 \in \mathcal{C}_1, \mathbf{c}_2 \in \mathcal{C}_2\}.$$

Theorem 7 shows that if n is even and $q \equiv 1 \pmod 4$, then the q-ary negacyclic code $\mathcal{C}$ of length n generated by $g(x)$ is scalar-equivalent to $\mathrm{Res}_1(\mathcal{C}) \curlyvee \mathrm{Res}_2(\mathcal{C})$.

Theorem 7 can be used to study a q-ary negacyclic code $\mathcal{C}$ of even length n via the study of the two associated constacyclic codes $\mathrm{Res}_1(\mathcal{C})$ and $\mathrm{Res}_2(\mathcal{C})$ of length $n/2$ if $q \equiv 1 \pmod 4$. Hence, it may be very useful in some cases. However, it cannot be used to study ternary negacyclic codes of even length.

IV. The First Family of Ternary Negacyclic Codes and Their Duals

In this section, let $\rho > 3$ be an odd prime. We will construct a family of ternary irreducible negacyclic codes of length 2ρ. To settle the value of $\mathrm{ord}_{4\rho}(3)$, we need the following two lemmas.

Lemma 8: [19] 3 is a quadratic residue of primes of the form $12\ell+1$ and $12\ell-1$. 3 is a quadratic nonresidue of primes of the form $12\ell+5$ and $12\ell-5$.

Lemma 9: Let $\rho > 3$ be an odd prime, then $\mathrm{ord}_{4\rho}(3) = \rho-1$ if and only if the one of the following conditions holds:

1) $\rho \equiv \pm 5 \pmod{12}$ and $\mathrm{ord}_\rho(3) = \rho - 1$.
2) $\rho \equiv -1 \pmod{12}$ and $\mathrm{ord}_\rho(3) = (\rho-1)/2$.

Proof: ($\Rightarrow$) Suppose $\mathrm{ord}_{4\rho}(3) = \rho - 1$. Let $\ell = \mathrm{ord}_\rho(3)$. It is clear that $\mathrm{ord}_\rho(3)$ divides $\mathrm{ord}_{4\rho}(3)$, i.e., $\ell \mid (\rho-1)$.

1) Suppose that ℓ is even. Then $4 \mid (3^\ell - 1)$. Noting that $\rho \mid (3^\ell - 1)$ and $\gcd(4, \rho) = 1$, we have $4\rho \mid (3^\ell - 1)$. It follows that $\mathrm{ord}_{4\rho}(3) = \rho - 1$ divides ℓ. Consequently, $\ell = \rho-1$. It then follows that 3 is a quadratic nonresidue of ρ. By Lemma 8, $\rho \equiv \pm 5 \pmod{12}$.
2) Suppose that ℓ is odd. It follows from $\ell \mid (\rho - 1)$ that $\ell \mid ((\rho-1)/2)$. Consequently, 3 is a quadratic residue of ρ. By Lemma 8, $\rho \equiv \pm 1 \pmod{12}$. We consider the following two cases:
   a) $\rho \equiv 1 \pmod{12}$: In this case, $(\rho-1)/2$ is even. It follows that $3^{(\rho-1)/2} \equiv 1 \pmod{4\rho}$, which contradicts the fact that $\mathrm{ord}_{4\rho}(3) = \rho - 1$.
   b) $\rho \equiv -1 \pmod{12}$: Noting that $4\rho \mid (3^{2\ell} - 1)$, we have $\mathrm{ord}_{4\rho}(3)$ divides 2ℓ, i.e., $((\rho-1)/2) \mid \ell$. Therefore, $\ell = (\rho-1)/2$.

($\Leftarrow$) Let $\ell' = \mathrm{ord}_{4\rho}(3)$. Notice that $\phi(4\rho) = 2(\rho-1)$, where ϕ is the Euler totient function. Then ℓ' divides $2(\rho - 1)$. According to the primitive root theorem, $\ell' \neq 2(\rho-1)$. Therefore, $\ell' \leq \rho-1$. It is clear that $\mathrm{ord}_\rho(3) \mid \ell'$. We consider the following two cases:

1) Suppose that $\mathrm{ord}_\rho(3) = \rho - 1$. Then $\ell' = \rho - 1$.
2) Suppose that $\rho \equiv -1 \pmod{12}$ and $\mathrm{ord}_\rho(3) = (\rho - 1)/2$. Noting that $\mathrm{ord}_3(\rho)$ divides ℓ' and $\ell' \leq \rho-1$, then $\ell' = \rho-1$ or $(\rho-1)/2$. In this case, $(\rho-1)/2$ is odd, $\gcd(3^{(\rho-1)/2}-1, 4) = 2$. It follows that $\ell' \neq (\rho-1)/2$. Therefore, $\ell' = \rho - 1$.

This completes the proof. ■

Throughout the rest of this section, let ρ be an odd prime such that $\rho \equiv \pm 5 \pmod{12}$ and $\mathrm{ord}_\rho(3) = \rho - 1$ and let $n = 2\rho$. By Lemma 9, $\mathrm{ord}_{4\rho}(3) = \rho - 1$. By assumption,

$$C_1^{(3,4\rho)} = \{3^i \bmod 4\rho : 0 \leq i \leq \rho - 2\}.$$

It is clear that $C_\rho^{(3,4\rho)} = \{\rho, 3\rho\}$ and all elements in both $C_1^{(3,4\rho)}$ and $C_\rho^{(3,4\rho)}$ are odd. Let h be any integer from

$$\{2i+1 : 0 \leq i \leq 2\rho-1\} \setminus (C_1^{(3,4\rho)} \cup C_\rho^{(3,4\rho)}).$$

Noting that $\gcd(h, 4\rho) = 1$, we have

$$|C_h^{(3,4\rho)}| = |C_1^{(3,4\rho)}| = \rho - 1.$$

Then $C_1^{(3,4\rho)}$, $C_h^{(3,4\rho)}$ and $C_\rho^{(3,4\rho)}$ form a partition of

$$\{2i+1 : 0 \leq i \leq 2\rho - 1\}.$$

Let α be a primitive element of $\mathrm{GF}(3^m)$, where $m = \rho-1$. Put $\beta = \alpha^{(3^{\rho-1}-1)/4\rho}$. By definition, $\beta^{2\rho} = -1$. Let $\mathbb{M}_{\beta^i}(x)$ denote the minimal polynomial of β^i over $\mathrm{GF}(3)$. It is easily seen that $\mathbb{M}_{\beta^\rho}(x) = x^2 + 1$ and

$$x^n + 1 = \mathbb{M}_{\beta^\rho}(x)\mathbb{M}_\beta(x)\mathbb{M}_{\beta^h}(x).$$

Let $\mathcal{C}(\rho)$ denote the ternary negacyclic code of length 2ρ with check polynomial $\mathbb{M}_\beta(x)$. Then $\dim(\mathcal{C}(\rho)) = \rho - 1$. By definition, $\mathcal{C}(\rho)$ is irreducible. By Lemma 2, the code $\mathcal{C}(\rho)$ has the trace representation

$$\mathcal{C}(\rho) = \left\{\mathbf{c}(a) = \left(\mathrm{Tr}_{3^m/3}(a\theta^i)\right)_{i=0}^{2\rho-1} : \ a \in \mathrm{GF}(3^m)\right\}, \quad (2)$$

where $\theta = \beta^{-1}$. The dual code $\mathcal{C}(\rho)^\perp$ has the trace representation

$$\mathcal{C}(\rho)^\perp = \{\mathbf{c}(a,b) = \left(\mathrm{Tr}_{3^2/3}(a\beta^{\rho i}) + \mathrm{Tr}_{3^m/3}(b\beta^{hi})\right)_{i=0}^{2\rho-1} : \ a \in \mathrm{GF}(3^2), \ b \in \mathrm{GF}(3^m)\}.$$

Associated with the irreducible negacyclic code $\mathcal{C}(\rho)$ is the following code over $\mathrm{GF}(3^2)$:

$$\overline{\mathcal{C}}(\rho) = \left\{\overline{\mathbf{c}}(a) = \left(\mathrm{Tr}_{3^m/3^2}(a\theta^{2i})\right)_{i=0}^{\rho-1} : \ a \in \mathrm{GF}(3^m)\right\}.$$

Note that θ^2 is a primitive 2ρ-th root of unity and $\theta^{2\rho} = -1$. It follows from Lemma 2 that $\overline{\mathcal{C}}(\rho)$ is the 3^2-ary negacyclic code of length ρ with check polynomial $\mathbb{M}_{\beta^2}(x)$. It is easily verified that the dual code $\overline{\mathcal{C}}(\rho)^\perp$ has the trace representation

$$\overline{\mathcal{C}}(\rho)^\perp = \{\overline{\mathbf{c}}(a,b) = \left(a(-1)^i + \mathrm{Tr}_{3^m/3^2}(b\beta^{2hi})\right)_{i=0}^{\rho-1} : \ a \in \mathrm{GF}(3^2), \ b \in \mathrm{GF}(3^m)\}.$$

We first prove the following theorem.

Theorem 10: Let notation be the same as before. The 3^2-ary negacyclic code $\overline{\mathcal{C}}(\rho)$ has parameters

$$[\rho, (\rho-1)/2, d \geq \sqrt{\rho} + 1],$$

and $\overline{\mathcal{C}}(\rho)^\perp$ has parameters $\left[\rho, (\rho+1)/2, d \geq \sqrt{\rho}\right]$.

Proof: Suppose $\mathrm{ord}_{2\rho}(3^2) = \ell$. Since $4\rho \mid (3^{\rho-1} - 1)$, we have $2\rho \mid (3^{\rho-1} - 1)$. It follows that $\ell \mid ((\rho-1)/2)$. On the other hand, since $2\rho \mid (3^{2\ell} - 1)$ and $4 \mid (3^{2\ell} - 1)$, we have $4\rho \mid (3^{2\ell} - 1)$. It then follows that $\mathrm{ord}_{4\rho}(3) \mid 2\ell$, i.e., $((\rho-1)/2) \mid \ell$. Therefore, $\ell = (\rho-1)/2$. According to [42, Theorem 26], the irreducible negacyclic code $\overline{\mathcal{C}}(\rho)$ has parameters

$$[\rho, (\rho-1)/2, d \geq \sqrt{\rho} + 1],$$

and $\overline{\mathcal{C}}(\rho)^\perp$ has parameters $[\rho, (\rho+1)/2, d \geq \sqrt{\rho}]$. This completes the proof. ■

Theorem 11: Let notation be the same as before. Then the ternary negacyclic code $\mathcal{C}(\rho)$ has parameters $[2\rho, \rho-1, d]$, where $d \geq d(\overline{\mathcal{C}}(\rho)) \geq \sqrt{\rho} + 1$.

Proof: It is clear that $\dim(\mathcal{C}(\rho)) = \mathrm{ord}_{4\rho}(3) = \rho - 1$. Now we prove that $d(\mathcal{C}(\rho)) \geq d(\overline{\mathcal{C}}(\rho))$. Since $\gcd(2, \rho) = 1$, we deduce that $\{2i + \rho j : \ 0 \leq i \leq \rho-1, \ 0 \leq j \leq 1\}$ is a complete set of residues modulo 2ρ. It then follows that

$$\begin{aligned} & \{0, 1, \cdots, 2\rho - 1\} \\ = \ & \{2i : \ 0 \leq i \leq \rho - 1\} \cup \{2i + \rho : \ 0 \leq i \leq (\rho-1)/2\} \\ & \cup \{2i + \rho - 2\rho : \ (\rho+1)/2 \leq i \leq \rho - 1\}. \end{aligned}$$

For any codeword $\mathbf{c}(a) = \left(\mathrm{Tr}_{3^m/3}(a\theta^i)\right)_{i=0}^{2\rho-1} \in \mathcal{C}(\rho)$, it is easily checked that $\mathbf{c}(a)$ is permutation-equivalent to

$$\begin{aligned}&\Big(\left(\mathrm{Tr}_{3^m/3}(a\theta^{2i}), \mathrm{Tr}_{3^m/3}(a\theta^{2i+\rho})\right)_{i=0}^{(\rho-1)/2} \|\\ &\left(\mathrm{Tr}_{3^m/3}(a\theta^{2i}), \mathrm{Tr}_{3^m/3}(a\theta^{2i+\rho-2\rho})\right)_{i=(\rho+1)/2}^{\rho-1}\Big)\\ =&\Big(\left(\mathrm{Tr}_{3^m/3}(a\theta^{2i}), \mathrm{Tr}_{3^m/3}(a\theta^{2i+\rho})\right)_{i=0}^{(\rho-1)/2} \|\\ &\left(\mathrm{Tr}_{3^m/3}(a\theta^{2i}), -\mathrm{Tr}_{3^m/3}(a\theta^{2i+\rho})\right)_{i=(\rho+1)/2}^{\rho-1}\Big),\end{aligned}$$

where $\|$ denotes the concatenation of vectors. It then follows that the code $\mathcal{C}(\rho)$ is monomial-equivalent to

$$\widetilde{\mathcal{C}}(\rho) = \{\widetilde{\mathbf{c}}(a) : a \in \mathrm{GF}(3^m)\}, \tag{3}$$

where

$$\widetilde{\mathbf{c}}(a) = \left(\left(\mathrm{Tr}_{3^m/3}(a\theta^{2i}), \mathrm{Tr}_{3^m/3}(a\theta^{2i+\rho})\right)\right)_{i=0}^{\rho-1}.$$

For any $a \in \mathrm{GF}(3^m)^*$, it follows from (3) that

$$\begin{aligned}&\rho - \mathtt{wt}(\widetilde{\mathbf{c}}(a))\\ \le&\left|\{0 \le i \le \rho-1 : \mathrm{Tr}_{3^m/3}(a\theta^{2i}) = \mathrm{Tr}_{3^m/3}(a\theta^{2i+\rho}) = 0\}\right|\\ =&\frac{1}{9}\sum_{i=0}^{\rho-1}\sum_{x_1\in\mathrm{GF}(3)}\zeta_3^{x_1\mathrm{Tr}_{3^m/3}(a\theta^{2i})}\sum_{x_2\in\mathrm{GF}(3)}\zeta_3^{x_2\mathrm{Tr}_{3^m/3}(a\theta^{2i+\rho})}\\ =&\frac{1}{9}\sum_{i=0}^{\rho-1}\sum_{(x_1,x_2)\in\mathrm{GF}(3)^2}\zeta_3^{\mathrm{Tr}_{3^m/3}((x_1+x_2\theta^\rho)a\theta^{2i})},\end{aligned} \tag{4}$$

where $\zeta_3 = e^{2\pi\sqrt{-1}/3}$. Noting that $\mathrm{ord}(\theta^\rho) = 4$, we have $\theta^\rho \in \mathrm{GF}(3^2)\backslash\mathrm{GF}(3)$. It is easy to verify that

$$\{x_1 + x_2\theta^\rho : \ x_1,\ x_2 \in \mathrm{GF}(3)\} = \mathrm{GF}(3^2). \tag{5}$$

It follows from (4) and (5) that

$$\begin{aligned}\mathtt{wt}(\widetilde{\mathbf{c}}(a)) &\ge \rho - \frac{1}{9}\sum_{i=0}^{\rho-1}\sum_{x\in\mathrm{GF}(3^2)}\zeta_3^{\mathrm{Tr}_{3^m/3}(xa\theta^{2i})}\\ &= \rho - \frac{1}{9}\sum_{i=0}^{\rho-1}\sum_{x\in\mathrm{GF}(3^2)}\zeta_3^{\mathrm{Tr}_{3^2/3}(x\mathrm{Tr}_{3^m/3^2}(a\theta^{2i}))}\\ &= \left|\{0 \le i \le \rho-1 :\ \mathrm{Tr}_{3^m/3^2}(a\theta^{2i}) \ne 0\}\right|\\ &= \mathtt{wt}(\overline{\mathbf{c}}(a)) \ge d(\overline{\mathcal{C}}(\rho)).\end{aligned}$$

Therefore, $d(\mathcal{C}(\rho)) \ge d(\overline{\mathcal{C}}(\rho))$. The desired result follows. ■

Theorem 12: Let notation be the same as before. Then the ternary negacyclic code $\mathcal{C}(\rho)^\perp$ has parameters

$$\left[2\rho, \rho+1, d^\perp\right],$$

where $d^\perp \ge d(\overline{\mathcal{C}}(\rho)^\perp) \ge \sqrt{\rho}$.

Proof: The dimension of the code $\mathcal{C}(\rho)^\perp$ follows from $\dim(\mathcal{C}(\rho)) = \rho-1$. Now we prove that $d(\mathcal{C}(\rho)^\perp) \ge d(\overline{\mathcal{C}}(\rho)^\perp)$. It is similarly verified that the code $\mathcal{C}(\rho)^\perp$ is monomial-equivalent to

$$\begin{aligned}\Big\{\widetilde{\mathbf{c}}(a,b) = \Big(&\left(\mathrm{Tr}_{3^2/3}(a\beta^{\rho 2i}) + \mathrm{Tr}_{3^m/3}(b\beta^{h2i}),\right.\\ &\left.\mathrm{Tr}_{3^2/3}(a\beta^{\rho(2i+\rho)}) + \mathrm{Tr}_{3^m/3}(b\beta^{h(2i+\rho)})\right)\Big)_{i=0}^{\rho-1} :\\ &a \in \mathrm{GF}(3^2),\ b \in \mathrm{GF}(3^m)\Big\}.\end{aligned} \tag{6}$$

For any $(a, b) \in (\mathrm{GF}(3^2) \times \mathrm{GF}(3^m))\backslash(0,0)$, it follows from (6) that

$$\begin{aligned}&\mathtt{wt}(\widetilde{\mathbf{c}}(a,b))\\ \ge&\rho - |\{0 \le i \le \rho-1 : \mathrm{Tr}_{3^2/3}(a\beta^{\rho 2i}) + \mathrm{Tr}_{3^m/3}(b\beta^{h2i}) = 0,\\ &\mathrm{Tr}_{3^2/3}(a\beta^{\rho(2i+\rho)}) + \mathrm{Tr}_{3^m/3}(b\beta^{h(2i+\rho)}) = 0\}|\\ =&\rho - \frac{1}{9}\sum_{i=0}^{\rho-1}\sum_{x_1\in\mathrm{GF}(3)}\zeta_3^{x_1(\mathrm{Tr}_{3^2/3}(a\beta^{\rho 2i})+\mathrm{Tr}_{3^m/3}(b\beta^{h2i}))}\\ &\sum_{x_2\in\mathrm{GF}(3)}\zeta_3^{x_2(\mathrm{Tr}_{3^2/3}(a\beta^{\rho(2i+\rho)})+\mathrm{Tr}_{3^m/3}(b\beta^{h(2i+\rho)}))}\\ =&\rho - \frac{1}{9}\sum_{i=0}^{\rho-1}\sum_{(x_1,x_2)\in\mathrm{GF}(3)^2}\zeta_3^{f(a,b,x_1,x_2,i)},\end{aligned} \tag{7}$$

where

$$f(a,b,x_1,x_2,i) = \mathrm{Tr}_{3^2/3}((x_1+x_2\beta^{\rho^2})a(-1)^i) + \mathrm{Tr}_{3^m/3}((x_1+x_2\beta^{h\rho})b\beta^{h2i})$$

and $\zeta_3 = e^{2\pi\sqrt{-1}/3}$. Noting that ρ and h are odd, we have $\rho \equiv h \pmod 4$ or $\rho \equiv -h \pmod 4$. If $\rho \equiv h \pmod 4$, then $\beta^{h\rho} = \beta^{\rho^2} = (-1)^{\frac{\rho-1}{2}}\beta^\rho$. It follows from (7) that

$$\begin{aligned}&\mathtt{wt}(\widetilde{\mathbf{c}}(a,b))\\ &\ge \rho - \frac{1}{9}\sum_{i=0}^{\rho-1}\sum_{x\in\mathrm{GF}(3^2)}\zeta_3^{\mathrm{Tr}_{3^2/3}(xa(-1)^i)+\mathrm{Tr}_{3^m/3}(xb\beta^{h2i})}\\ &= \rho - \frac{1}{9}\sum_{i=0}^{\rho-1}\sum_{x\in\mathrm{GF}(3^2)}\zeta_3^{\mathrm{Tr}_{3^2/3}(x(a(-1)^i+\mathrm{Tr}_{3^m/3^2}(b\beta^{h2i})))}\\ &= \left|\{0 \le i \le \rho-1 :\ a(-1)^i + \mathrm{Tr}_{3^m/3^2}(b\beta^{h2i}) \ne 0\}\right|\\ &= \mathtt{wt}(\overline{\mathbf{c}}(a,b)) \ge d(\overline{\mathcal{C}}(\rho)^\perp).\end{aligned} \tag{8}$$

If $\rho \equiv -h \pmod 4$, then $\beta^{h\rho} = \beta^{3\rho^2} = (-1)^{\frac{\rho+1}{2}}\beta^\rho$. Note that

$$\begin{aligned}&\mathrm{Tr}_{3^2/3}((x_1+x_2\beta^{\rho^2})a(-1)^i)\\ =&\ \mathrm{Tr}_{3^2/3}((x_1^3+x_2^3\beta^{3\rho^2})a^3(-1)^i)\\ =&\ \mathrm{Tr}_{3^2/3}((x_1+x_2\beta^{3\rho^2})a^3(-1)^i).\end{aligned}$$

It then follows from (7) that

$$\begin{aligned}&\mathtt{wt}(\widetilde{\mathbf{c}}(a,b))\\ &\ge \rho - \frac{1}{9}\sum_{i=0}^{\rho-1}\sum_{x\in\mathrm{GF}(3^2)}\zeta_3^{\mathrm{Tr}_{3^2/3}(xa^3(-1)^i)+\mathrm{Tr}_{3^m/3}(xb\beta^{h2i})}\\ &= \mathtt{wt}(\overline{\mathbf{c}}(a^3,b)) \ge d(\overline{\mathcal{C}}(\rho)^\perp).\end{aligned} \tag{9}$$

Combining Equations (8) and (9), we deduce that $d(\mathcal{C}(\rho)) \ge d(\overline{\mathcal{C}}(\rho)^\perp)$. The desired result follows. ■

The lower bounds on $d(\mathcal{C}(\rho))$ and on $d(\mathcal{C}(\rho)^\perp)$ documented in Theorems 11 and 12 are close to the square-root bound. The experimental data in Table II shows that the minimum distances of the codes $\mathcal{C}(\rho)$ (resp. $\mathcal{C}(\rho)^\perp$) and $\overline{\mathcal{C}}(\rho)$ (resp. $\overline{\mathcal{C}}(\rho)^\perp$) are very close to each other.

Note that the length of the code $\mathcal{C}(\rho)$ is even, the code $\mathcal{C}(\rho)$ is not known to be scalar-equivalent or permutation-equivalent to a ternary cyclic code. The negacyclic code $\mathcal{C}(\rho)$ and its dual

TABLE II
THE CODES $\overline{\mathcal{C}}(\rho)$, $\mathcal{C}(\rho)$ AND THEIR DUAL

ρ	$\overline{\mathcal{C}}(\rho)$	$\overline{\mathcal{C}}(\rho)^\perp$	$\mathcal{C}(\rho)$	$\mathcal{C}(\rho)^\perp$
5	$[5,2,4]$	$[5,3,3]$	$[10,4,6]$	$[10,6,4]$
7	$[7,3,5]$	$[7,4,4]$	$[14,6,6]$	$[14,8,5]$
17	$[17,8,8]$	$[17,9,7]$	$[34,16,12]$	$[34,18,10]$
19	$[19,9,10]$	$[19,10,9]$	$[38,18,10]$	$[38,20,9]$
29	$[29,14,12]$	$[29,15,11]$	$[58,28,18]$	$[58,30,16]$
31	$[31,15,12]$	$[31,16,11]$	$[62,30,14]$	$[62,32,12]$
43	$[43,21,16]$	$[43,22,15]$	$[86,42,18]$	$[86,44,16]$

are exceptionally good in general and are much better than the best cyclic codes with the same length and dimension. The authors are not aware of any family of ternary linear codes that outperforms this class of negacyclic codes $\mathcal{C}(\rho)$. The example codes below justify this claim.

Example 13: Let $\rho = 5$ and let β be the primitive 4ρ-th root of unity with $\beta^4 + \beta^3 + 2\beta + 1 = 0$. Then the negacyclic code $\mathcal{C}(\rho)$ has parameters $[10, 4, 6]$, and $\mathcal{C}(\rho)^\perp$ has parameters $[10, 6, 4]$. These two negacyclic codes are distance-optimal [14]. The best ternary cyclic code of length 10 and dimension 4 has minimum distance 4, and the best ternary cyclic code of length 10 and dimension 6 has minimum distance 2 [5].

Example 14: Let $\rho = 7$ and let β be the primitive 4ρ-th root of unity with $\beta^6+2\beta^5+2\beta^3+2\beta+1 = 0$. Then the negacyclic code $\mathcal{C}(\rho)$ has parameters $[14, 6, 6]$, and $\mathcal{C}(\rho)^\perp$ has parameters $[14, 8, 5]$. These two negacyclic codes are distance-optimal [14]. The best ternary cyclic code of length 14 and dimension 6 has minimum distance 4, and the best ternary cyclic code of length 14 and dimension 8 has minimum distance 2 [5].

Example 15: Let $\rho = 17$ and let β be the primitive 4ρ-th root of unity with $\beta^{16} + 2\beta^{15} + 2\beta^{12} + 2\beta^{11} + 2\beta^{10} + 2\beta^6+\beta^5+2\beta^4+\beta+1 = 0$. Then the negacyclic code $\mathcal{C}(\rho)$ has parameters $[34, 16, 12]$ and $\mathcal{C}(\rho)^\perp$ has parameters $[34, 18, 10]$. These two negacyclic codes are distance-optimal [14]. The best ternary cyclic code of length 34 and dimension 16 has minimum distance 4, and the best ternary cyclic code of length 34 and dimension 18 has minimum distance 2 [5].

Example 16: Let $\rho = 19$ and let β be the primitive 4ρ-th root of unity with $\beta^{18} + 2\beta^{17} + 2\beta^{14} + \beta^{13} + 2\beta^{11} + \beta^{10} + 2\beta^9 + \beta^8 + 2\beta^7 + \beta^5 + 2\beta^4 + 2\beta + 1 = 0$. Then the negacyclic code $\mathcal{C}(\rho)$ has parameters $[38, 18, 10]$. The best ternary code known of length 38 and dimension 18 has minimum distance 12 [14]. The best ternary cyclic code of length 38 and dimension 18 has minimum distance 4 [5]. The dual code $\mathcal{C}(\rho)^\perp$ has parameters $[38, 20, 9]$. The best ternary code known of length 38 and dimension 20 has minimum distance 10 [14]. The best ternary cyclic code of length 38 and dimension 20 has minimum distance 2 [5].

Example 17: Let $\rho = 29$ and let β be the primitive 4ρ-th root of unity with $\beta^{28} + 2\beta^{27} + 2\beta^{25} + \beta^{23} + 2\beta^{22} + \beta^{21} + 2\beta^{19} + 2\beta^{17} + \beta^{15} + 2\beta^{14} + 2\beta^{13} + \beta^{11} + \beta^9 + 2\beta^7 + 2\beta^6 + 2\beta^5 + \beta^3 + \beta + 1 = 0$. Then the negacyclic code $\mathcal{C}(\rho)$ has parameters $[58, 28, 18]$, and has the best parameters known [14]. The best ternary cyclic code of length 58 and dimension 28 has minimum distance 4 [5]. The dual code $\mathcal{C}(\rho)^\perp$ has parameters $[58, 30, 16]$, and has the best parameters known [14]. The best ternary cyclic code of length 58 and dimension 30 has minimum distance 2 [5].

Example 18: Let $\rho = 31$ and let β be the primitive 4ρ-th root of unity with $\beta^{30} + \beta^{29} + 2\beta^{27} + \beta^{26} + 2\beta^{25} + 2\beta^{24} + \beta^{23} + 2\beta^{22} + \beta^{21} + \beta^{20} + 2\beta^{19} + \beta^{18} + \beta^{17} + 2\beta^{16} + \beta^{15} + 2\beta^{14} + \beta^{13} + \beta^{12} + 2\beta^{11} + \beta^{10} + \beta^9 + 2\beta^8 + \beta^7 + 2\beta^6 + 2\beta^5 + \beta^4 + 2\beta^3 + \beta + 1 = 0$. Then the negacyclic code $\mathcal{C}(\rho)$ has parameters $[62, 30, 14]$. The best ternary code known of length 62 and dimension 30 has minimum distance 18 [14]. The best ternary cyclic code of length 62 and dimension 30 has minimum distance 4 [5]. The dual code $\mathcal{C}(\rho)^\perp$ has parameters $[62, 32, 12]$. The best ternary code known of length 62 and dimension 32 has minimum distance 16 [14]. The best ternary cyclic code of length 62 and dimension 32 has minimum distance 2 [5].

V. THE SECOND FAMILY OF TERNARY NEGACYCLIC CODES AND THEIR DUALS

Let $\ell \geq 2$ be an integer, and let n be a positive divisor of $3^\ell+1$ and $2n > 3^{\lceil \ell/2 \rceil}+1$. Let β be a primitive $2n$-th root of unity, then $\beta^n = -1$. Let $\mathbb{M}_\beta(x)$ be the minimum polynomial of β over GF(3). Let $\mathcal{C}(\ell)$ denote the ternary negacyclic code of length n with check polynomial $\mathbb{M}_\beta(x)$. To settle the dimension of the negacyclic code $\mathcal{C}(\ell)$, we need the following lemma.

Lemma 19: Let notation be the same as before. Then $\mathrm{ord}_{2n}(3) = 2\ell$.

Proof: It is clear that $\mathrm{ord}_{2n}(3) \mid 2\ell$.

1) If $\mathrm{ord}_{2n}(3) \leq \ell/2$, we have $2n \leq 3^{\ell/2} - 1$, a contradiction.
2) If $\mathrm{ord}_{2n}(3) = (2\ell)/3$, then $3 \mid \ell$, and n divides
$$\gcd\left((3^{2\ell/3} - 1)/2, 3^\ell + 1\right).$$
Noting that
$$\gcd\left((3^{2\ell/3} - 1)/2, 3^\ell + 1\right) = 3^{\ell/3} + 1,$$
we have $n \leq 3^{\ell/3} + 1$, a contradiction.
3) If $\mathrm{ord}_{2n}(3) = \ell$, then n divides
$$\gcd\left((3^\ell - 1)/2, 3^\ell + 1\right).$$
Noting that
$$\begin{aligned}\gcd\left((3^\ell - 1)/2, 3^\ell + 1\right) &= \gcd\left((3^\ell - 1)/2, 2\right)\\ &= \gcd(\ell, 2),\end{aligned}$$
we have $n \leq 2$, a contradiction.

This completes the proof. ∎

Theorem 20: Let $n = (3^\ell+1)/2$, where $\ell \geq 2$ is an integer. Then the negacyclic code $\mathcal{C}(\ell)$ has parameters
$$[n, 2\ell, d \geq (3^{\ell-1} + 1)/2],$$
and the code $\mathcal{C}(\ell)^\perp$ has parameters $[n, n - 2\ell, 5]$.

Proof: By Lemma 19, $\dim(\mathcal{C}(\ell)) = \mathrm{ord}_{2n}(3) = 2\ell$. Consequently, $\dim(\mathcal{C}(\ell)^\perp) = n - 2\ell$. It is easily verified that

$$C_1^{(3,2n)} = \left\{1, 3, \cdots, 3^{\ell-1}, 2n - 3^{\ell-1}, 2n - 3^{\ell-2}, \cdots, 2n-1\right\}.$$

Let $H = \left\{2i+1 : (3^{\ell-1}+1)/2 \le i \le 3^{\ell-1}-1\right\}$. Then

$$H \subseteq \{1+2i : \ 0 \le i \le n-1\} \backslash C_1^{(3,2n)},$$

and β^i is a zero of $\mathcal{C}(\ell)$ for each $i \in H$. The desired lower bound then follows from Lemma 1. Notice that $-3, -1, 1, 3 \in C_1^{(3,2n)}$, from Lemma 1, $d(\mathcal{C}(\ell)^\perp) \ge 5$. It follows from Lemma 5 that $d(\mathcal{C}(\ell)^\perp) \le 5$. Therefore, $d(\mathcal{C}(\ell)^\perp) = 5$. This completes the proof. ∎

The code $\mathcal{C}(\ell)^\perp$ is a ternary negacyclic BCH code with designed distance 2, and its parameters were studied in [36]. Theorem 20 gives a lower bound on the minimum distance of the code $\mathcal{C}(\ell)$. When ℓ is even, $n = (3^\ell+1)/2$ is odd, then the ternary negacyclic code $\mathcal{C}(\ell)$ of length n is scalar-equivalent to a ternary cyclic code of length n. In other words, Theorem 20 can produce ternary cyclic codes with good parameters.

Example 21: Let $\ell = 3$, then $n = (3^\ell+1)/2 = 14$. Let β be the primitive $2n$-th root of unity with $\beta^6+2\beta^5+2\beta^3+2\beta+1 = 0$. Then the negacyclic code $\mathcal{C}(\ell)$ has parameters $[14, 6, 6]$ and $\mathcal{C}(\ell)^\perp$ has parameters $[14, 8, 5]$. These two negacyclic codes are distance-optimal [14]. The best ternary cyclic code of length 14 and dimension 6 has minimum distance 4, and the best ternary cyclic code of length 14 and dimension 8 has minimum distance 2 [5].

Example 22: Let $\ell = 4$, then $n = (3^\ell+1)/2 = 41$. Let β be the primitive $2n$-th root of unity with $\beta^8+2\beta^6+2\beta^5+2\beta^3+2\beta^2+1 = 0$. Then the negacyclic code $\mathcal{C}(\ell)$ has parameters $[41, 8, 22]$, and has the best parameters known [14]. The dual code $\mathcal{C}(\ell)^\perp$ has parameters $[41, 33, 5]$, and is distance-optimal.

Example 23: Let $\ell = 5$, then $n = (3^\ell+1)/2 = 122$. Let β be the primitive $2n$-th root of unity with $\beta^{10}+2\beta^9+2\beta^8+2\beta^7+\beta^6+\beta^5+\beta^4+2\beta^3+2\beta^2+2\beta+1 = 0$. Then the negacyclic code $\mathcal{C}(\ell)$ has parameters $[122, 10, 71]$. The best ternary code known of length 122 and dimension 10 has minimum distance 72 [14]. The dual code $\mathcal{C}(\ell)^\perp$ has parameters $[122, 112, 5]$, and is distance-optimal.

Theorem 24: Let $n = (3^\ell+1)/4$, where $\ell \ge 5$ is an odd integer. Then the negacyclic code $\mathcal{C}(\ell)$ has parameters

$$[n, 2\ell, d \ge (3^{\ell-1}-1)/4],$$

and the code $\mathcal{C}(\ell)^\perp$ has parameters $[n, n-2\ell, 5 \le d^\perp \le 6]$.

Proof: By Lemma 19, $\dim(\mathcal{C}(\ell)) = \mathrm{ord}_{2n}(3) = 2\ell$. Consequently, $\dim(\mathcal{C}(\ell)^\perp) = n - 2\ell$. It is easily verified that

$$C_1^{(3,2n)} = \left\{1, 3, \cdots, 3^{\ell-2}, 2n-3^{\ell-1}, 3^{\ell-1}, 2n-3^{\ell-2}, \cdots, 2n-1\right\}.$$

Let

$$H = \left\{2i+1 : (3^{\ell-1}+3)/4 \le i \le (3^{\ell-1}-3)/2\right\}.$$

Then $H \subseteq \{1+2i : \ 0 \le i \le n-1\} \backslash C_1^{(3,2n)}$, and β^i is a zero of $\mathcal{C}(\ell)$ for each $i \in H$. The desired lower bound then follows from Lemma 1. Notice that $-3, -1, 1, 3 \in C_1^{(3,2n)}$, from Lemma 1, $d(\mathcal{C}(\ell)^\perp) \ge 5$. It follows from Lemma 4 that $d(\mathcal{C}(\ell)^\perp) \le 6$. This completes the proof. ∎

Note that $3^\ell + 1 \equiv 4 \pmod 8$ for ℓ being odd, then $n = (3^\ell+1)/4$ is odd. In this case, the ternary negacyclic code $\mathcal{C}(\ell)$ of length n is scalar-equivalent to a ternary cyclic code of length n. Therefore, Theorem 24 can produce ternary cyclic codes with good parameters.

Example 25: Let $\ell = 5$, then $n = (3^\ell+1)/4 = 61$. Let β be the primitive $2n$-th root of unity with $\beta^{10}+\beta^8+\beta^7+\beta^5+\beta^3+\beta^2+1 = 0$. Then the negacyclic code $\mathcal{C}(\ell)$ has parameters $[61, 10, 31]$. The best ternary code known of length 61 and dimension 10 has minimum distance 32 [14]. The dual code $\mathcal{C}(\ell)^\perp$ has parameters $[61, 51, 5]$ and has the best parameters known [14].

Theorem 26: Let $n = 3^\ell + 1$, where $\ell \ge 2$ is an integer. Then the negacyclic code $\mathcal{C}(\ell)$ has parameters

$$[n, 2\ell, d \ge (3^\ell+3)/2],$$

and the code $\mathcal{C}(\ell)^\perp$ has parameters $[n, n-2\ell, d^\perp]$, where

$$d^\perp = \begin{cases} 3 & \text{if } \ell \text{ is odd,} \\ 4 & \text{if } \ell \text{ is even.} \end{cases}$$

Proof: By Lemma 19, $\dim(\mathcal{C}(\ell)) = \mathrm{ord}_{2n}(3) = 2\ell$. Consequently, $\dim(\mathcal{C}(\ell)^\perp) = n - 2\ell$. It is easily verified that

$$3^{\ell+i} \equiv 3^\ell - (3^i - 1) \pmod{2n}$$

for any $1 \le i \le \ell - 1$. Therefore,

$$C_1^{(3,2n)} = \left\{1, 3, \cdots, 3^{\ell-1}, 3^\ell - (3^{\ell-1}-1), \cdots, 3^\ell - 2, 3^\ell\right\}.$$

Let $H = \left\{2i+1 : (3^\ell+1)/2 \le i \le 3^\ell\right\}$. Then

$$H \subseteq \{1+2i : \ 0 \le i \le n-1\} \backslash C_1^{(3,2n)},$$

and β^i is a zero of $\mathcal{C}(\ell)$ for each $i \in H$. The desired lower bound then follows from Lemma 1.

Now we consider the minimum distance of $\mathcal{C}(\ell)^\perp$. It follows from Lemma 4 that $d(\mathcal{C}(\ell)^\perp) \le 4$. Note that $1, 3 \in C_1^{(3,2n)}$, by Lemma 1, $d(\mathcal{C}(\ell)^\perp) \ge 3$. We now consider the following two cases.

1) If m is odd, then $4 \mid n$. Let $\eta = \beta^{-(n/4)}$, then $\eta \in \mathrm{GF}(3^2) \backslash \mathrm{GF}(3)$. Consequently, there exist $a_0, a_1 \in \mathrm{GF}(3)$ such that $\mathbb{M}_\eta(x) = x^2 + a_1 x + a_0$. It follows that $x^{\frac{n}{2}} + a_1 x^{\frac{n}{4}} + a_0 \in \mathcal{C}(\ell)^\perp$. Therefore, $d(\mathcal{C}(\ell)^\perp) = 3$.
2) If m is even, then $n/2$ is odd. If $d(\mathcal{C}(\ell)^\perp) = 3$, then there exist $a_0, a_1 \in \mathrm{GF}(3)^*$ and $1 \le i_0 < i_1 \le n-1$ such that

$$a_1\beta^{-i_1} + a_0\beta^{-i_0} = 1. \tag{10}$$

Raising both sides of (10) to the (3^m+1)-th power, we have

$$(-1)^{i_1} + a_1a_0[(-1)^{i_1}\beta^{i_1-i_0} + (-1)^{i_0}\beta^{i_0-i_1}] + (-1)^{i_0} = 1. \tag{11}$$

It follows that $(-1)^{i_1}\beta^{i_1-i_0} + (-1)^{i_0}\beta^{i_0-i_1} \in \mathrm{GF}(3)$, which is equivalent to

$$[(-1)^{i_1}\beta^{i_1-i_0} + (-1)^{i_0}\beta^{i_0-i_1}]^3$$

$$\begin{aligned}&= (-1)^{i_1}\beta^{i_1-i_0} + (-1)^{i_0}\beta^{i_0-i_1}\\ \Leftrightarrow &(-1)^{i_0}\beta^{3(i_0-i_1)}(\beta^{2(i_1-i_0)}-1)\\ &[(-1)^{(i_1-i_0)}\beta^{4(i_1-i_0)}-1] = 0. \qquad (12)\end{aligned}$$

Note that $(-1)^{i_0}\beta^{3(i_0-i_1)} \neq 0$, it follows from (12) that $\beta^{2(i_1-i_0)} = 1$ or $\beta^{4(i_1-i_0)} = (-1)^{i_1-i_0}$.

a) If $\beta^{2(i_1-i_0)} = 1$, we have $n \mid (i_1 - i_0)$, which contradicts the fact that $0 < i_1 - i_0 < n$.

b) If $\beta^{4(i_1-i_0)} = (-1)^{i_1-i_0}$, we have $n \mid 4(i_1 - i_0)$. Since $n/2$ is odd, $(n/2) \mid (i_1 - i_0)$. Notice that $0 < i_1 - i_0 < n$, then $i_1 - i_0 = n/2$. Consequently, $\beta^{4(i_1-i_0)} = \beta^{2n} = 1 = (-1)^{i_1-i_0} = -1$, a contradiction.

Therefore, $d(\mathcal{C}(\ell)^\perp) = 4$.

This completes the proof. ∎

Example 27: Let $\ell = 2$, then $n = 3^\ell + 1 = 10$. Let β be the primitive $2n$-th root of unity with $\beta^4 + \beta^3 + 2\beta + 1 = 0$. Then the negacyclic code $\mathcal{C}(\ell)$ has parameters $[10, 4, 6]$ and $\mathcal{C}(\ell)^\perp$ has parameters $[10, 6, 4]$. These two negacyclic codes are distance-optimal [14]. The best ternary cyclic code of length 10 and dimension 4 has minimum distance 4, and the best ternary cyclic code of length 10 and dimension 6 has minimum distance 2 [5].

Example 28: Let $\ell = 3$, then $n = 3^\ell + 1 = 28$. Let β be the primitive $2n$-th root of unity with $\beta^6 + 2\beta^5 + 2\beta + 2 = 0$. Then the negacyclic code $\mathcal{C}(\ell)$ has parameters $[28, 6, 15]$ and is distance-optimal [14]. The code $\mathcal{C}(\ell)^\perp$ has parameters $[28, 22, 3]$ and is distance-almost-optimal. The best ternary cyclic code of length 28 and dimension 6 has minimum distance 12, and the best ternary cyclic code of length 28 and dimension 22 has minimum distance 2 [5].

Example 29: Let $\ell = 4$, then $n = 3^\ell+1 = 82$. Let β be the primitive $2n$-th root of unity with $\beta^8+2\beta^7+2\beta^6+\beta^5+\beta^4+2\beta^3+2\beta^2+\beta+1 = 0$. Then the negacyclic code $\mathcal{C}(\ell)$ has parameters $[82, 8, 48]$. The best ternary code known of length 82 and dimension 8 has minimum distance 49 [14]. The code $\mathcal{C}(\ell)^\perp$ has parameters $[82, 74, 4]$ and is distance-optimal.

VI. The Third Family of Ternary Negacyclic Codes and Their Duals

Let $m \geq 3$ be an integer, and let n be a positive divisor of $(3^m - 1)/2$ and $n > (3^{\lfloor m/2 \rfloor} + 1)/2$. Let β be a primitive $2n$-th root of unity, then $\beta^n = -1$. Let $\mathbb{M}_\beta(x)$ be the minimum polynomial of β over GF(3). Let $\mathcal{C}(m)$ denote the ternary negacyclic code of length n with check polynomial $\mathrm{lcm}(\mathbb{M}_\beta(x), \mathbb{M}_{\beta^{2n-1}}(x))$, where lcm denotes the least common multiple of the minimal polynomials. To settle the dimension of the negacyclic code $\mathcal{C}(m)$, we need the following lemma.

Lemma 30: Let notation be the same as before. Then $\mathrm{ord}_{2n}(3) = m$ and

$$\mathrm{lcm}(\mathbb{M}_\beta(x), \mathbb{M}_{\beta^{2n-1}}(x)) = \mathbb{M}_\beta(x)\mathbb{M}_{\beta^{2n-1}}(x).$$

Proof: It is clear that $\mathrm{ord}_{2n}(3)$ divides m.

1) If $\mathrm{ord}_{2n}(3) < m$ and m is even, we have $2n \leq 3^{m/2}-1$, a contradiction.

2) If $\mathrm{ord}_{2n}(3) < m$ and m is odd, then

$$\mathrm{ord}_{2n}(3) \leq m/3 \leq (m-1)/2.$$

Consequently, $2n \leq 3^{(m-1)/2} - 1$, a contradiction.

Therefore, $\mathrm{ord}_{2n}(3) = m$. It is easy to see that

$$\mathrm{lcm}(\mathbb{M}_\beta(x), \mathbb{M}_{\beta^{2n-1}}(x)) = \mathbb{M}_\beta(x)\mathbb{M}_{\beta^{2n-1}}(x)$$

if and only if $2n - 1 \notin C_1^{(3,2n)}$. Suppose $2n - 1 \in C_1^{(3,2n)}$, then there is $0 \leq \ell \leq m - 1$ such that $3^\ell \equiv -1 \pmod{2n}$. It follows that $2n \mid \gcd(3^\ell + 1, 3^m - 1)$. Notice that

$$\gcd(3^\ell + 1, 3^m - 1) = \begin{cases} 2 & \text{if } \frac{m}{\gcd(\ell,m)} \text{ is odd,} \\ 3^{\gcd(\ell,m)} + 1 & \text{if } \frac{m}{\gcd(\ell,m)} \text{ is even.} \end{cases}$$

Since $2n > 2$, from $2n \mid \gcd(3^\ell + 1, 3^m - 1)$, we have m is even and $\gcd(\ell, m) \leq m/2$. Consequently, $2n \leq 3^{m/2} + 1$, a contradiction. This completes the proof. ∎

Theorem 31: Let $n = (3^m - 1)/2$, where $m \geq 3$ is an integer. Then the negacyclic code $\mathcal{C}(m)$ has parameters

$$[n, 2m, d \geq (3^{m-1} - 1)/2],$$

and the code $\mathcal{C}(m)^\perp$ has parameters $[n, n - 2m, 5]$.

Proof: It is easily checked that $|C_1^{(3,2n)}| = |C_{2n-1}^{(3,2n)}|$. By Lemma 30, $|C_1^{(3,2n)}| = |C_{2n-1}^{(3,2n)}| = m$. It follows that $\dim(\mathcal{C}(m)) = 2m$ and $\dim(\mathcal{C}(m)^\perp) = n-2m$. On one hand,

$$\begin{aligned}&C_1^{(3,2n)} \cup C_{2n-1}^{(3,2n)}\\ =&\left\{1, 3, \cdots, 3^{m-1}\right\} \cup \left\{2n-1, 2n-3, \cdots, 2n-3^{m-1}\right\}.\end{aligned}$$

Let $H = \left\{2i + 1 : (3^{m-1} + 1)/2 \leq i \leq 3^{m-1} - 2\right\}$, then

$$H \subseteq \{1 + 2i :\ 0 \leq i \leq n - 1\} \backslash (C_1^{(3,2n)} \cup C_{2n-1}^{(3,2n)}),$$

and β^i is a zero of $\mathcal{C}(m)$ for each $i \in H$. The desired lower bound then follows from Lemma 1. On the other hand, $-3, -1, 1, 3 \in C_1^{(3,2n)} \cup C_{2n-1}^{(3,2n)}$, from Lemma 1, $d(\mathcal{C}(m)^\perp) \geq 5$. It follows from Lemma 5 that $d(\mathcal{C}(m)^\perp) \leq 5$. This completes the proof. ∎

The negacyclic code $\mathcal{C}(m)^\perp$ was studied in [9]. Theorem 31 gives a lower bound on the minimum distance of the code $\mathcal{C}(m)$. When m is odd, $n = (3^m-1)/2$ is odd, then the ternary negacyclic code $\mathcal{C}(m)$ of length n is scalar-equivalent to a ternary cyclic code of length n. In other words, Theorem 31 can produce ternary cyclic codes with good parameters.

Example 32: Let $m = 3$, then $n = (3^m - 1)/2 = 13$. Let β be the primitive $2n$-th root of unity with $\beta^3 + 2\beta + 1 = 0$. Then the negacyclic code $\mathcal{C}(m)$ has parameters $[13, 6, 6]$ and $\mathcal{C}(m)^\perp$ has parameters $[13, 7, 5]$. These two negacyclic codes are distance-optimal [14].

Example 33: Let $m = 4$, then $n = (3^m - 1)/2 = 40$. Let β be the primitive $2n$-th root of unity with $\beta^4 + 2\beta^3 + 2 = 0$. Then the negacyclic code $\mathcal{C}(m)$ has parameters $[40, 8, 21]$ and has the best parameters known [14]. The code $\mathcal{C}(m)^\perp$ has parameters $[40, 32, 5]$, and is distance-optimal. The best ternary cyclic code of length 40 and dimension 8 has minimum distance 20, and the best ternary cyclic code of length 40 and dimension 32 has minimum distance 4 [5].

Example 34: Let $m = 5$, then $n = (3^m-1)/2 = 121$. Let β be the primitive $2n$-th root of unity with $\beta^5+2\beta+1 = 0$. Then the negacyclic code $\mathcal{C}(m)$ has parameters $[121, 10, 71]$. The best ternary code known of length 121 and dimension 10 has minimum distance 72 [14]. The code $\mathcal{C}(m)^\perp$ has parameters $[121, 111, 5]$, and is distance-optimal.

Theorem 35: Let $n = (3^m - 1)/4$, where $m \geq 4$ is an even integer. Then the negacyclic code $\mathcal{C}(m)$ has parameters

$$[n, 2m, d \geq (3^{m-1} + 1)/4],$$

and the code $\mathcal{C}(m)^\perp$ has parameters $[n, n-2m, 5 \leq d^\perp \leq 6]$, and $d^\perp = 5$ if $m \equiv 0 \pmod 4$.

Proof: By Lemma 30, $\deg(\mathrm{lcm}(\mathbb{M}_\beta(x), \mathbb{M}_{\beta^{2n-1}}(x))) = 2m$. Then $\dim(\mathcal{C}(m)) = 2m$ and $\dim(\mathcal{C}(m)^\perp) = n - 2m$. It is easily checked that

$$\begin{aligned} &C_1^{(3,2n)} \cup C_{2n-1}^{(3,2n)} \\ &= \left\{1, 3, \cdots, 3^{m-1}\right\} \cup \left\{2n-1, 2n-3, \cdots, 2n-3^{m-1}\right\}. \end{aligned}$$

Let $H = \left\{2i+1 : (3^{m-1}+1)/4 \leq i \leq (3^{m-1}-3)/2\right\}$, then

$$H \subseteq \{1 + 2i : \ 0 \leq i \leq n-1\} \backslash (C_1^{(3,2n)} \cup C_{2n-1}^{(3,2n)}),$$

and β^i is a zero of $\mathcal{C}(m)$ for each $i \in H$. The desired lower bound then follows from Lemma 1.

Notice that $-3, -1, 1, 3 \in C_1^{(3,2n)} \cup C_{2n-1}^{(3,2n)}$, by Lemma 1, $d(\mathcal{C}(m)^\perp) \geq 5$. It follows from Lemma 4 that $d(\mathcal{C}(m)^\perp) \leq 6$. If $m \equiv 0 \pmod 4$, 5 divides n. Let $\eta = \beta^{n/5}$, then $\mathrm{ord}(\eta) = 10$ and $\eta \in \mathrm{GF}(3^4) \backslash \mathrm{GF}(3^2)$. Then $\mathbb{M}_\eta(x) = \mathbb{M}_{\eta^{-1}}(x)$ and $\deg(\mathbb{M}_\eta(x)) = 4$. It follows that there exist $a_0, a_1, a_2, a_3 \in \mathrm{GF}(3)$ such that

$$\begin{aligned} &\eta^4 + c_3\eta^3 + c_2\eta^2 + c_1\eta + c_0 \\ &= \eta^{-4} + c_3\eta^{-3} + c_2\eta^{-2} + c_1\eta^{-1} + c_0 \\ &= 0 \end{aligned}$$

Therefore,

$$c(x) = x^{(4n)/5} + c_3x^{(3n)/5} + c_2x^{(2n)/5} + c_1x^{n/5} + c_0 \in \mathcal{C}(m)^\perp.$$

We then deduce that $d(\mathcal{C}(m)^\perp) \leq 5$. The desired conclusion then follows. ■

Example 36: Let $m = 4$, then $n = (3^m - 1)/4 = 20$. Let β be the primitive $2n$-th root of unity with $\beta^4 + 2\beta^3 + \beta^2 + 1 = 0$. Then the negacyclic code $\mathcal{C}(m)$ has parameters $[20, 8, 8]$. The best ternary code known of length 20 and dimension 8 has minimum distance 9 [14]. The code $\mathcal{C}(m)^\perp$ has parameters $[20, 12, 5]$. The best ternary code known of length 20 and dimension 12 has minimum distance 6 [14]. The best ternary cyclic code of length 20 and dimension 8 has minimum distance 8, and the best ternary cyclic code of length 20 and dimension 12 has minimum distance 4 [5].

Example 37: Let $m = 6$, then $n = (3^m - 1)/4 = 182$. Let β be the primitive $2n$-th root of unity with $\beta^6 + \beta^5 + 2\beta^3 + 1 = 0$. Then the negacyclic code $\mathcal{C}(m)$ has parameters $[182, 12, 104]$. The best ternary code known of length 182 and dimension 12 has minimum distance 105 [14]. The code $\mathcal{C}(m)^\perp$ has parameters $[182, 170, 5]$, and has the best parameters known [14].

VII. The Fourth Family of Ternary Negacyclic Codes and Their Duals

Let $m \geq 2$ be an integer. Let $n = (3^m - 1)/2$ and $N = 2n = 3^m - 1$. For any i with $0 \leq i \leq N-1$, we have the following 3-adic expansion $i = \sum_{j=0}^{m-1} i_j 3^j$, where $0 \leq i_j \leq 2$. The 3-weight $\mathtt{wt}_3(i)$ of i is defined by $\mathtt{wt}_3(i) = \sum_{j=0}^{m-1} i_j$. It is easy to see that $\mathtt{wt}_3(i)$ is a constant on each cyclotomic coset $C_j^{(3,N)}$ and $\mathtt{wt}_3(i) \equiv i \pmod 2$. Let $\Gamma_{(3,N)}$ be the set of 3-cyclotomic coset leaders modulo N and let

$$\Gamma_{(3,N)}^{(1)} = \{i : \ i \in \Gamma_{(3,N)}, \ i \equiv 1 \pmod 2\}.$$

Let β be a primitive element of $\mathrm{GF}(3^m)$, then

$$\begin{aligned} x^n + 1 &= \prod_{i \in \Gamma_{(3,N)}^{(1)}} \mathbb{M}_{\beta^i}(x) \\ &= \prod_{\substack{i \in \Gamma_{(3,N)}^{(1)}, \\ \mathtt{wt}_3(i) \equiv 1 \pmod 4}} \mathbb{M}_{\beta^i}(x) \prod_{\substack{i \in \Gamma_{(3,N)}^{(1)}, \\ \mathtt{wt}_3(i) \equiv 3 \pmod 4}} \mathbb{M}_{\beta^i}(x). \end{aligned}$$

For each $j \in \{1, 3\}$, define

$$g_{(j,m)}(x) = \prod_{\substack{i \in \Gamma_{(3,N)}^{(1)}, \\ \mathtt{wt}_3(i) \equiv j \pmod 4}} \mathbb{M}_{\beta^i}(x).$$

Then $g_{(j,m)}(x)$ is a polynomial over $\mathrm{GF}(3)$. Let $\mathcal{C}_{(j,m)}$ be the ternary negacyclic code of length n with generator polynomial $g_{(j,m)}(x)$.

For any positive integer m, let

$$\begin{aligned} S_j(m) = \{&(i_0, i_1, \ldots, i_{m-1}) \in \{0, 1, 2\}^m : \\ &i_0 + i_1 + \cdots + i_{m-1} \equiv j \pmod 4\}, \end{aligned}$$

where $j \in \{0, 1, 2, 3\}$. It is easy to verify that

$$\begin{aligned} &\bigcup_{\substack{i \in \Gamma_{(3,N)}^{(1)}, \\ \mathtt{wt}_3(i) \equiv j \pmod 4}} C_i^{(3,N)} \\ &= \left\{1 \leq i \leq N-1 : \ \mathtt{wt}_3(i) \equiv j \pmod 4\right\}, \end{aligned}$$

and $\deg(g_{(j,m)}(x)) = |S_j(m)|$ for $j = \{1, 3\}$. To settle the dimension of the negacyclic code $\mathcal{C}_{(j,m)}$, we need the following lemma.

Lemma 38: Let notation be the same as before. The following hold.

1) If $m \geq 2$ is even, then $|S_0(m)| = \frac{3^m + 1 + 2(-1)^{m/2}}{4}$, $|S_1(m)| = |S_3(m)| = \frac{3^m - 1}{4}$, and
$$|S_2(m)| = \frac{3^m + 1 + 2(-1)^{(m-2)/2}}{4}.$$
2) If $m \geq 3$ is odd, then $|S_0(m)| = |S_2(m)| = \frac{3^m + 1}{4}$, $|S_1(m)| = \frac{3^m - 1 + 2(-1)^{(m-1)/2}}{4}$ and
$$|S_3(m)| = \frac{3^m - 1 + 2(-1)^{(m+1)/2}}{4}.$$

Proof: It is easy to verify that

$$\begin{aligned} &|S_1(m)| + |S_3(m)| \\ &= |\{\bar{i} \in \{0, 1, 2\}^m : \ i_0 + i_1 + \cdots + i_{m-1} \equiv 1 \pmod 2\}| \\ &= |\{\bar{i} \in \{0, 1, 2\}^m : \ |\{0 \leq j \leq m-1 : i_j = 1\}| \text{ is odd}\}| \end{aligned}$$

$$= \sum_{i \text{ is odd}} \binom{m}{i} 2^{m-i},$$

where $\bar{i} = (i_0, i_1, \ldots, i_{m-1})$. Clearly,

$$\begin{aligned}(2+1)^m &= \sum_{i \text{ is odd}} \binom{m}{i} 2^{m-i} + \sum_{i \text{ is even}} \binom{m}{i} 2^{m-i},\\ (2-1)^m &= \sum_{i \text{ is odd}} (-1)^i \binom{m}{i} 2^{m-i} + \\ &\quad \sum_{i \text{ is even}} (-1)^i \binom{m}{i} 2^{m-i}.\end{aligned}$$

Therefore,

$$|S_1(m)| + |S_3(m)| = \sum_{i \text{ is odd}} \binom{m}{i} 2^{m-i} = (3^m - 1)/2. \quad (13)$$

Consequently,

$$\begin{aligned}&|S_0(m)| + |S_2(m)|\\ &= |\{\bar{i} \in \{0,1,2\}^m : \ i_0 + i_1 + \cdots + i_{m-1} \equiv 0 \pmod 2\}|\\ &= (3^m + 1)/2, \qquad (14)\end{aligned}$$

where $\bar{i} = (i_0, i_1, \ldots, i_{m-1})$.

Recall $N = 3^m - 1$, we consider the following cases.

1) Suppose that $m \geq 2$ is even. It is easy to verify that $i \in S_1(m)$ if and only if $N - i \in S_3(m)$. Then

$$\psi_1 : \ S_1(m) \to S_3(m), \ i \mapsto N - i$$

is a bijection. Therefore, $|S_1(m)| = |S_3(m)|$. It follows from (13) that

$$|S_1(m)| = |S_3(m)| = (3^m - 1)/4.$$

Clearly, $|S_0(2)| = 2$. Suppose $m \geq 4$, then

$$\begin{aligned}|S_0(m)| &= |S_0(m-1)| + |S_2(m-1)| + |S_3(m-1)|\\ &= \frac{3^{m-1}+1}{2} + |S_3(m-1)|\\ &= \frac{3^{m-1}+1}{2} + |S_1(m-2)| + |S_2(m-2)|\\ &\qquad + |S_3(m-2)|\\ &= \frac{3^{m-1}+1}{2} + \frac{3^{m-2}-1}{2} + \frac{3^{m-2}+1}{2}\\ &\qquad - |S_0(m-2)|\\ &= \frac{5 \cdot 3^{m-2}+1}{2} - |S_0(m-2)|.\end{aligned}$$

Using recursion, we deduce that

$$\begin{aligned}|S_0(m)| &= \sum_{i=1}^{(m-2)/2} (-1)^{i-1} \left(\frac{5 \cdot 3^{m-2i}+1}{2} \right)\\ &\qquad + (-1)^{(m-2)/2} |S_0(2)|\\ &= \frac{3^m + 1 + 2(-1)^{m/2}}{4}. \qquad (15)\end{aligned}$$

It follows from (14) and (15) that

$$|S_2(m)| = \frac{3^m + 1 + 2(-1)^{(m-2)/2}}{4}.$$

2) Suppose that $m \geq 3$ is odd. It is easy to check that $i \in S_0(m)$ if and only if $N - i \in S_2(m)$. Then

$$\psi_2 : \ S_0(m) \to S_2(m), \ i \mapsto N - i$$

is a bijection. Therefore, $|S_0(m)| = |S_2(m)|$. It follows from (14) that

$$|S_0(m)| = |S_2(m)| = (3^m + 1)/4.$$

Note that

$$\begin{aligned}|S_1(m)| &= |S_0(m-1)| + |S_1(m-1)| + |S_3(m-1)|\\ &= |S_0(m-1)| + \frac{3^{m-1}-1}{2}\\ &= \frac{3^{m-1}+1+2(-1)^{(m-1)/2}}{4} + \frac{3^{m-1}-1}{2}\\ &= \frac{3^m - 1 + 2(-1)^{(m-1)/2}}{4}. \qquad (16)\end{aligned}$$

It follows from (13) and (16) that

$$|S_3(m)| = \frac{3^m - 1 + 2(-1)^{(m+1)/2}}{4}.$$

This completes the proof. ■

To lower bound the minimum distance of the negacyclic code $\mathcal{C}_{(j,m)}$, we need the following lemmas.

Lemma 39: Let $1 \leq s \leq m$ be a positive integer. The following hold.

1) For any $0 \leq i \leq 3^s - 1$, $\mathtt{wt}_3(3^s - 1 - i) = 2s - \mathtt{wt}_3(i)$.
2) For any $1 \leq i \leq 3^s$, $\mathtt{wt}_3((3^s - 1)i) = 2s$.
3) For any $0 \leq i \leq 2 \cdot 3^s - 1$,

$$\mathtt{wt}_3(2 \cdot 3^s - 1 - i) = 2s + 1 - \mathtt{wt}_3(i).$$

4) Suppose $i = i_a 3^a + \cdots + i_b 3^b$, where $0 \leq a \leq b \leq m-1$, $i_j \in \{0,1,2\}$ and $i_a \neq 0$. Then

$$\mathtt{wt}_3(i-1) = 2a + \mathtt{wt}_3(i) - 1.$$

Proof: 1. Let the 3-adic expansion of i be $i = \sum_{j=0}^{s-1} i_j 3^j$, then

$$3^s - 1 - i = \sum_{j=0}^{s-1} (2 - i_j) 3^j.$$

It follows that $\mathtt{wt}_3(3^s - 1 - i) = 2s - \mathtt{wt}_3(i)$.

2. For any $1 \leq i \leq 3^s$,

$$\begin{aligned}(3^s - 1)i &= (i-1)3^s + 3^s - i\\ &= (i-1)3^s + 3^s - 1 - (i-1).\end{aligned}$$

It follows that

$$\begin{aligned}\mathtt{wt}_3((3^s - 1)i) &= \mathtt{wt}_3(i-1) + \mathtt{wt}(3^s - 1 - (i-1))\\ &= \mathtt{wt}_3(i-1) + 2s - \mathtt{wt}_3(i-1)\\ &= 2s.\end{aligned}$$

3. If $0 \leq i \leq 3^s - 1$, $2 \cdot 3^s - 1 - i = 3^s + 3^s - 1 - i$. It follows that

$$\begin{aligned}\mathtt{wt}_3(2 \cdot 3^s - 1 - i) &= 1 + \mathtt{wt}_3(3^s - 1 - i)\\ &= 2s + 1 - \mathtt{wt}_3(i).\end{aligned}$$

If $i = 3^s + j$, where $0 \le j \le 3^s - 1$, then $2 \cdot 3^s - 1 - i = 3^s - 1 - j$. Consequently,

$$\begin{aligned}\mathtt{wt}_3(2 \cdot 3^s - 1 - i) &= 2s - \mathtt{wt}_3(j) \\ &= 2s - (\mathtt{wt}_3(i) - 1) \\ &= 2s + 1 - \mathtt{wt}_3(i).\end{aligned}$$

4. Clearly,

$$\begin{aligned} i - 1 &= i_a 3^a - 1 + \sum_{a<j\le b} i_j 3^j \\ &= 2 \sum_{0\le j\le a-1} 3^j + (i_a - 1)3^a + \sum_{a<j\le b} i_j 3^j.\end{aligned}$$

It follows that $\mathtt{wt}_3(i-1) = 2a + \mathtt{wt}_3(i) - 1$. This completes the proof. ■

Lemma 40: Let $m \ge 5$ and $m \equiv 1 \pmod 4$. Let $h = (m-1)/2$. Then

$$\left\{3^{m-1} + (3^h - 1)i : \ -2 \le i \le 3^h + 3\right\} \subseteq S_1(m).$$

Proof: If $i \in \{-1, -2\}$, it is easily verified that $\mathtt{wt}_3(3^{m-1} + (3^h - 1)i) = m$. If $i = 0$,

$$\mathtt{wt}_3(3^{m-1} + (3^h - 1)i) = 1.$$

If $1 \le i \le 3^h$, $1 \le (3^h - 1)i < 3^{m-1}$. It follows that

$$\begin{aligned}\mathtt{wt}_3(3^{m-1} + (3^h - 1)i) &= 1 + \mathtt{wt}_3((3^h - 1)i) \\ &= 1 + 2h \\ &= m,\end{aligned}$$

where the second equation follows from Result 2 of Lemma 39. If $i \in \{1, 2, 3\}$,

$$3^{m-1} + (3^h - 1)(3^h + i) = 2 \cdot 3^{m-1} + (i-1)3^h - i.$$

Then $\mathtt{wt}_3(3^{m-1} + (3^h - 1)(3^h + 1)) = 2m - 1 \equiv 1 \pmod 4$ and $\mathtt{wt}_3(3^{m-1} + (3^h - 1)(3^h + i)) = m$ for each $i \in \{2, 3\}$. In summary,

$$\mathtt{wt}_3(3^{m-1} + (3^h - 1)i) \equiv 1 \pmod 4$$

for any $-2 \le i \le 3^h + 3$. This completes the proof. ■

Lemma 41: Let $m \ge 5$ and $m \equiv 1 \pmod 4$. Let $h = (m-1)/2$. Then

$$\left\{2 \cdot 3^{h-1} - 1 + (3^h - 1)i : \ 0 \le i \le 2 \cdot 3^{h-1}\right\} \subseteq S_3(m).$$

Proof: For any $0 \le i \le 2 \cdot 3^{h-1} - 1$,

$$2 \cdot 3^{h-1} - 1 + (3^h - 1)i = i \cdot 3^h + 2 \cdot 3^{h-1} - 1 - i.$$

It follows that

$$\begin{aligned}&\mathtt{wt}_3(2 \cdot 3^{h-1} - 1 + (3^h - 1)i) \\ &= \mathtt{wt}_3(i) + \mathtt{wt}_3(2 \cdot 3^{h-1} - 1 - i) \\ &= \mathtt{wt}_3(i) + 2(h-1) + 1 - \mathtt{wt}_3(i) \\ &= m - 2,\end{aligned}$$

where the second equation follows from Result 3 of Lemma 39. It is easily verified that

$$\begin{aligned}&\mathtt{wt}_3(2 \cdot 3^{h-1} - 1 + (3^h - 1) \cdot 2 \cdot 3^{h-1}) \\ &= \mathtt{wt}_3(2 \cdot 3^{2h-1} - 1) = 2(2h-1) + 1 = 2m - 3.\end{aligned}$$

Therefore, $\mathtt{wt}_3(2 \cdot 3^{h-1} - 1 + (3^h - 1)i) \equiv 3 \pmod 4$ for any $0 \le i \le 2 \cdot 3^{h-1}$. This completes the proof. ■

Lemma 42: Let $m \ge 7$ and $m \equiv 3 \pmod 4$. Let $h = (m-3)/2$. Then

$$\left\{2 \cdot 3^h - 1 + (3^{h+2} - 1)i : \ 0 \le i \le 2 \cdot 3^h + 2\right\} \subseteq S_1(m).$$

Proof: Similar to Lemma 41, for any $0 \le i \le 2 \cdot 3^h - 1$,

$$\begin{aligned}&\mathtt{wt}_3(2 \cdot 3^h - 1 + (3^{h+2} - 1)i) \\ &= \mathtt{wt}_3(i) + \mathtt{wt}_3(2 \cdot 3^h - 1 - i) \\ &= \mathtt{wt}_3(i) + 2h + 1 - \mathtt{wt}(i) = m - 2.\end{aligned}$$

It is easily verified that

$$\mathtt{wt}_3(2 \cdot 3^h - 1 + (3^{h+2} - 1) \cdot 2 \cdot 3^h) = 2m - 1$$

and

$$\mathtt{wt}_3(2 \cdot 3^h - 1 + (3^{h+2} - 1)(2 \cdot 3^h + i)) = m + 2$$

for each $i \in \{1, 2\}$. In summary,

$$\mathtt{wt}_3(2 \cdot 3^h - 1 + (3^{h+2} - 1)i) \equiv 1 \pmod 4$$

for any $0 \le i \le 2 \cdot 3^h + 2$. This completes the proof. ■

Lemma 43: Let $m \ge 7$ and $m \equiv 3 \pmod 4$. Let $h = (m-1)/2$. Then $\left\{3^{m-1} + (3^h - 1)i : \ 1 \le i \le 3^h\right\} \subseteq S_3(m)$.

Proof: Similar to Lemma 40, for any $1 \le i \le 3^h$,

$$\mathtt{wt}_3(3^{m-1} + (3^h - 1)i) = m \equiv 3 \pmod 4.$$

This completes the proof. ■

Based on the foregoing lemmas, the main results of this section are given in the next theorem.

Theorem 44: Let $m \ge 5$ be odd. Then the negacyclic code $\mathcal{C}_{(1,m)}$ has parameters

$$\left[\frac{3^m - 1}{2}, \ \frac{3^m - 1 + 2(-1)^{(m+1)/2}}{4}, \ d \ge d(m)\right],$$

where

$$d(m) = \begin{cases} 3^{(m-1)/2} + 7 & \text{if } m \equiv 1 \pmod 4, \\ 2 \cdot 3^{(m-3)/2} + 4 & \text{if } m \equiv 3 \pmod 4. \end{cases}$$

The negacyclic code $\mathcal{C}_{(1,m)}^{\perp} = \mathcal{C}_{(3,m)}$ and has parameters

$$\left[\frac{3^m - 1}{2}, \ \frac{3^m - 1 + 2(-1)^{(m-1)/2}}{4}, \ d^{\perp} \ge d^{\perp}(m)\right],$$

where

$$d^{\perp}(m) = \begin{cases} 2 \cdot 3^{(m-3)/2} + 2 & \text{if } m \equiv 1 \pmod 4, \\ 3^{(m-1)/2} + 1 & \text{if } m \equiv 3 \pmod 4. \end{cases}$$

Proof: It is clear that

$$\dim(\mathcal{C}_{(1,m)}) = n - |S_1(m)| = |S_3(m)|.$$

The desired dimension of $\mathcal{C}_{(1,m)}$ then follows from Lemma 38. We now prove the lower bound on the minimum distance of the code $\mathcal{C}_{(1,m)}$. We consider the following two cases.

1) Suppose that $m \equiv 1 \pmod 4$, then

$$\gcd(3^{(m-1)/2} - 1, 3^m - 1) = 2.$$

Let

$$H=\{3^{m-1}+(3^{(m-1)/2}-1)i: -2\le i\le 3^{(m-1)/2}+3\},$$

by Lemma 40, β^i is a zero of $\mathcal{C}_{(1,m)}$ for each $i\in H$. The desired lower bound on d then follows from the BCH bound on negacyclic codes.

2) Suppose that $m\equiv 3 \pmod 4$, then

$$\gcd(3^{(m+1)/2}-1,3^m-1)=2.$$

Let $h=(m-3)/2$ and

$$H=\{2\cdot 3^h-1+(3^{h+2}-1)i: 0\le i\le 2\cdot 3^h+2\},$$

by Lemma 42, β^i is a zero of $\mathcal{C}_{(1,m)}$ for each $i\in H$. The desired lower bound on d then follows from the BCH bound on negacyclic codes.

It follows from Lemma 39 that $\mathtt{wt}_3(N-i)=2m-\mathtt{wt}_3(i)$. Therefore, $\mathtt{wt}_3(N-i)\equiv \mathtt{wt}_3(i) \pmod 4$ for odd i. It follows that $\widehat{g_{(j,m)}}(x)=g_{(j,m)}(x)$ for $j\in\{1,3\}$. By definition, $\mathcal{C}_{(3,m)}=(g_{(3,m)}(x))$ and

$$\mathcal{C}_{(1,m)}^{\perp}=(\widehat{g_{(3,m)}}(x))=(g_{(3,m)}(x)).$$

Hence, $\mathcal{C}_{(1,m)}^{\perp}=\mathcal{C}_{(3,m)}$.

The desired dimension of $\mathcal{C}_{(3,m)}$ then follows from Lemma 38. We now prove the lower bound on the minimum distance of the code $\mathcal{C}_{(3,m)}$. We consider the following two cases.

1) Suppose that $m\equiv 1 \pmod 4$, then

$$\gcd(3^{(m-1)/2}-1,3^m-1)=2.$$

Let $h=(m-3)/2$ and

$$H=\left\{2\cdot 3^h-1+(3^{h+1}-1)i:\ 0\le i\le 2\cdot 3^h\right\},$$

by Lemma 41, β^i is a zero of $\mathcal{C}_{(3,m)}$ for each $i\in H$. The desired lower bound on $d^{\perp}$ then follows from the BCH bound on negacyclic codes.

2) Suppose that $m\equiv 3 \pmod 4$, then

$$\gcd(3^{(m-1)/2}-1,3^m-1)=2.$$

Let

$$H=\left\{3^{m-1}+(3^{(m-1)/2}-1)i:\ 1\le i\le 3^{(m-1)/2}\right\},$$

by Lemma 43, β^i is a zero of $\mathcal{C}_{(3,m)}$ for each $i\in H$. The desired lower bound on $d^{\perp}$ then follows from the BCH bound on negacyclic codes.

This completes the proof. ■

Since m is odd, $n=(3^m-1)/2$ is odd. Then the ternary negacyclic code $\mathcal{C}_{(i,m)}$ of length n is scalar-equivalent to a ternary cyclic code of length n. Studying these negacyclic codes are still valuable due to the following facts.

- Firstly, our experimental data shows that this family of negacyclic codes have very good parameters in general and contain distance-optimal codes. For example, when $m=3$, the negacyclic code $\mathcal{C}_{(1,m)}$ has parameters $[13,7,5]$, and $\mathcal{C}_{(3,m)}$ has parameters $[13,6,6]$. These two negacyclic codes are distance-optimal.
- Secondly, the ternary cyclic codes that are scalar-equivalent to these negacyclic codes $\mathcal{C}_{(i,m)}$ have not been studied in the literature.

Finally, we compare the family of ternary negacyclic codes $\mathcal{C}_{(1,m)}$ with the family of ternary projective Reed-Muller codes (see [41]). The parameters of the ternary projective Reed-Muller codes of length 13 are given below:

$$[13,3,9],\quad [13,6,6],\quad [13,10,3],\quad [13,12,2].$$

Notice that the negacyclic code $\mathcal{C}_{(1,3)}$ has parameters $[13,7,5]$. The family of codes $\mathcal{C}_{(1,m)}$ and the ternary projective Reed-Muller codes are different in general.

When $m\ge 2$ is even, for any $1\le i\le N-1$,

$$\mathtt{wt}_3(N-i)=2m-\mathtt{wt}_3(i)\equiv -\mathtt{wt}_3(i) \pmod 4.$$

It follows that $\widehat{g_{(1,m)}}(x)=g_{(3,m)}(x)$. By definition,

$$\mathcal{C}_{(1,m)}=(g_{(1,m)}(x))$$

and $\mathcal{C}_{(3,m)}=(g_{(3,m)}(x))$. Then $\mathcal{C}_{(1,m)}$ and $\mathcal{C}_{(3,m)}$ have the same parameters. Notice that $x^n+1=g_{(1,m)}(x)g_{(3,m)}(x)$. Then both $\mathcal{C}_{(1,m)}$ and $\mathcal{C}_{(3,m)}$ are self-dual codes. To estimate the minimum distance of the negacyclic code $\mathcal{C}_{(j,m)}$, we need the following lemmas.

Lemma 45: Let $m\ge 4$ and $m\equiv 0 \pmod 4$. Let $h=(m-2)/2$. Then

$$\left\{3^{m-1}+(3^h-1)i:\ 1\le i\le 3^h\right\}\subseteq S_3(m).$$

Proof: Similar to Lemma 40, for any $1\le i\le 3^h$,

$$\mathtt{wt}_3(3^{m-1}+(3^h-1)i)=m-1\equiv 3 \pmod 4.$$

This completes the proof. ■

Lemma 46: Let $m\ge 6$ and $m\equiv 2 \pmod 4$. Let $h=m/2$. Then

$$\{[2\cdot 3^{h+2}-3^{h-1}+6+(n-1-3^{h+1})i] \bmod N:\\ 1\le i\le (3^{h-1}+11)/2\}\subseteq S_3(m).$$

Proof: It is easily verified that the desired result holds for $m=6$. Suppose $m\ge 10$ and $m\equiv 2 \pmod 4$, then $h\ge 5$ is odd, and

$$\begin{aligned}\frac{3^{h-1}+11}{2}&=\frac{3^{h-1}-1}{2}+6\\ &\equiv h-1+6 \pmod 2\\ &\equiv 0 \pmod 2.\end{aligned}$$

We consider the following two cases.

1) Suppose $1\le i\le \frac{3^{h-1}+11}{2}$ is odd, then $\frac{3^{h-1}+11}{2}-i$ is odd. Consequently, $\mathtt{wt}_3(\frac{3^{h-1}+11}{2}-i)$ is odd. Recall $N=2n$, we get that

$$\begin{aligned}&2\cdot 3^{h+2}-3^{h-1}+6+(n-1-3^{h+1})i\\ &\equiv 2\cdot 3^{h+2}-3^{h-1}+6+n-i-i3^{h+1} \pmod N\\ &=\left(\frac{3^{h-1}-1}{2}-i+6\right)3^{h+1}+\\ &\quad 3^h+\frac{3^{h-1}-1}{2}-i+6.\end{aligned}$$

It follows that

$$\begin{aligned}&\mathtt{wt}_3([2\cdot 3^{h+2}-3^{h-1}+6+(n-1-3^{h+1})i] \bmod N)\\ =&\ 2\cdot \mathtt{wt}_3\left(\frac{3^{h-1}-1}{2}-i+6\right)+1\\ \equiv&\ 3 \pmod 4).\end{aligned}$$

2) Suppose $1\le i\le \frac{3^{h-1}+11}{2}$ is even. If $i=2$,

$$\begin{aligned}&2\cdot 3^{h+2}-3^{h-1}+6+(n-1-3^{h+1})i] \bmod N\\ =&\ (3^3+2\cdot 3+2)3^{h-1}+3+1.\end{aligned}$$

Then

$$\begin{aligned}&\mathtt{wt}_3([2\cdot 3^{h+2}-3^{h-1}+6+(n-1-3^{h+1})i] \bmod N)\\ =&\ 7\equiv 3 \pmod 4).\end{aligned}$$

If $i=4$,

$$\begin{aligned}&[2\cdot 3^{h+2}-3^{h-1}+6+(n-1-3^{h+1})i] \bmod N\\ =&\ (3^2+2\cdot 3+2)3^{h-1}+2.\end{aligned}$$

Then

$$\begin{aligned}&\mathtt{wt}_3([2\cdot 3^{h+2}-3^{h-1}+6+(n-1-3^{h+1})i] \bmod N)\\ =&\ 7\equiv 3 \pmod 4).\end{aligned}$$

If $i\ge 6$ is even, then $i-6\ge 0$ is even and $\mathtt{wt}_3(i-6)$ is even. It is easily verified that

$$\begin{aligned}&2\cdot 3^{h+2}-3^{h-1}+6+(n-1-3^{h+1})i\\ \equiv&\ 2\cdot 3^{h+2}-3^{h-1}+6+2n-i-i3^{h+1} \pmod N)\\ =&\ (3^{h-1}-i+5)3^{h+1}+2\cdot 3^h+2\cdot 3^{h-1}-i+5.\end{aligned}$$

It follows that

$$\begin{aligned}&\mathtt{wt}_3([2\cdot 3^{h+2}-3^{h-1}+6+(n-1-3^{h+1})i] \bmod N)\\ =&\ \mathtt{wt}_3(3^{h-1}-i+5)+2+\mathtt{wt}_3(2\cdot 3^{h-1}-i+5)\\ =&\ 2(h-1)-\mathtt{wt}_3(i-6)+2+2(h-1)+\\ &\ 1-\mathtt{wt}_3(i-6)\\ =&\ 3+4(h-1)-2\cdot\mathtt{wt}_3(i-6)\\ \equiv&\ 3 \pmod 4).\end{aligned}$$

This completes the proof. ■

Theorem 47: Let $m\ge 4$ be even. Then $\mathcal{C}_{(1,m)}$ and $\mathcal{C}_{(3,m)}$ have the same parameters, and are ternary

$$[(3^m-1)/2,(3^m-1)/4,d\ge d(m)]$$

self-dual codes, where

$$d(m)=\begin{cases}3^{(m-2)/2}+3 & \text{if } m\equiv 0 \pmod 4),\\ \frac{3^{(m-2)/2}+15}{2} & \text{if } m\equiv 2 \pmod 4).\end{cases}$$

Proof: It is clear that we only need to prove the lower bound on the minimum distance of the code $\mathcal{C}_{(3,m)}$. We consider the following two cases.

1) Suppose $m\equiv 0 \pmod 4)$, then

$$\gcd(3^{(m-2)/2}-1,3^m-1)=2.$$

Let

$$H=\left\{3^{m-1}+(3^{(m-2)/2}-1)i:\ 1\le i\le 3^{(m-2)/2}\right\},$$

by Lemma 45, β^i is a zero of $\mathcal{C}_{(3,m)}$ for each $i\in H$. By the negacyclic BCH bound,

$$d(\mathcal{C}_{(3,m)})\ge 3^{(m-2)/2}+1.$$

According to [17, Theorem 1.4.5],

$$d(\mathcal{C}_{(3,m)})\equiv 0 \pmod 3).$$

Therefore, $d(\mathcal{C}_{(3,m)})\ge 3^{(m-2)/2}+3$.

2) Suppose $m\equiv 2 \pmod 4)$, then $(m+2)/2$ is even, and $n-1-3^{(m+2)/2}\equiv 2 \pmod 4)$. Notice that

$$\begin{aligned}&\gcd(2(n-1-3^{(m+2)/2}),2n)\\ =&\ \gcd(2\cdot 3^{(m+2)/2}+2,3^m-1)\end{aligned}$$

and $\gcd(3^{(m+2)/2}+1,3^m-1)=2$, then

$$\gcd(n-1-3^{(m+2)/2},2n)=2.$$

Let

$$\begin{aligned}&H=\\ &\{[2\cdot 3^{(m+4)/2}-3^{(m-2)/2}+6+(n-1-3^{(m+2)/2})i]\\ &\bmod N:\ 1\le i\le (3^{(m-2)/2}+11)/2\},\end{aligned}$$

by Lemma 46, β^i is a zero of $\mathcal{C}_{(3,m)}$ for each $i\in H$. By the negacyclic BCH bound,

$$d(\mathcal{C}_{(3,m)})\ge (3^{(m-2)/2}+13)/2.$$

According to [17, Theorem 1.4.5],

$$d(\mathcal{C}_{(3,m)})\equiv 0 \pmod 3).$$

Therefore, $d(\mathcal{C}_{(3,m)})\ge (3^{(m-2)/2}+15)/2$.

This completes the proof. ■

Example 48: Let $m=4$, then $n=(3^m-1)/2=40$. Let β be the primitive $2n$-th root of unity with $\beta^4+2\beta^3+2=0$. Then both $\mathcal{C}_{(1,m)}$ and $\mathcal{C}_{(3,m)}$ are ternary $[40,20,9]$ self-dual codes. The best ternary self-dual code known of length 40 and dimension 20 has minimum distance 12 [12]. Ternary cyclic self-dual codes do not exist [20].

When $m\ge 2$ is even, the two negacyclic codes $\mathcal{C}_{(1,m)}$ and $\mathcal{C}_{(3,m)}$ are interesting, as they are self-dual codes and have good minimum distances. For example, when $m=2$, these two negacyclic codes are ternary $[4,2,3]$ self-dual codes. According to [20], ternary cyclic self-dual codes do not exist.

VIII. Summary and Concluding Remarks

The main contributions of this paper are the constructions and analyses of several families of ternary negacyclic codes. These ternary negacyclic codes are very interesting in theory as they contain distance-optimal codes and codes with best known parameters (see the code examples presented in this paper). In addition, the duals of three families of these ternary negacyclic codes are distance-optimal. A summary of the main specific contributions of this paper goes as follows.

1) A family of ternary irreducible negacyclic codes $\mathcal{C}(\rho)$ with parameters $[2\rho,\rho-1,d\ge\sqrt{\rho}+1]$ was constructed in Section IV (see Theorems 11 and 12). The dual code $\mathcal{C}(\rho)^{\perp}$ has parameters $[2\rho,\rho+1,d^{\perp}\ge\sqrt{\rho}]$. The authors are not aware of any family of ternary codes that can

outperform this family of negacyclic codes in terms of the error-correcting capability when the length and dimension are fixed.

2) A family of ternary irreducible negacyclic codes $\mathcal{C}(\ell)$ with parameters $\left[(3^\ell+1)/2, 2\ell, d \geq (3^{\ell-1}+1)/2\right]$ was constructed in Section V. Moreover, the dual code $\mathcal{C}(\ell)^\perp$ has parameters $\left[(3^\ell+1)/2, (3^\ell+1)/2-2\ell, 5\right]$ and is distance-optimal (see Theorem 20).
3) A family of ternary irreducible negacyclic codes $\mathcal{C}(\ell)$ with parameters $\left[(3^\ell+1)/4, 2\ell, d \geq (3^{\ell-1}-1)/4\right]$ was constructed in Section V. Moreover, the dual code $\mathcal{C}(\ell)^\perp$ has parameters
$$\left[(3^\ell+1)/4, (3^\ell+1)/4-2\ell, 5 \leq d^\perp \leq 6\right]$$
and is distance-almost-optimal (see Theorem 24).
4) A family of ternary irreducible negacyclic codes $\mathcal{C}(\ell)$ with parameters $\left[3^\ell+1, 2\ell, d \geq (3^\ell+3)/2\right]$ was constructed in Section V (see Theorem 26). Examples 27, 28, and 29 show that the code could be much better than the best ternary cyclic code with the same length and dimension and could be distance-optimal. In addition, we have the following:
   - If ℓ is odd, the dual code $\mathcal{C}(\ell)^\perp$ has parameters $[3^\ell+1, 3^\ell+1-2\ell, 3]$, and is distance-almost-optimal.
   - If ℓ is even, the dual code $\mathcal{C}(\ell)^\perp$ has parameters $[3^\ell+1, 3^\ell+1-2\ell, 4]$, and is distance-optimal.
5) A family of ternary negacyclic codes $\mathcal{C}(m)$ with parameters $\left[(3^m-1)/2, 2m, d \geq (3^{m-1}-1)/2\right]$ was constructed in Section VI (see Theorem 31). Examples 32 and 33 show that the code could be distance-optimal or could have the best known parameters. Moreover, the dual code $\mathcal{C}(m)^\perp$ has parameters
$$[(3^m-1)/2, (3^m-1)/2-2m, 5]$$
and is distance-optimal.
6) A family of ternary negacyclic codes $\mathcal{C}(m)$ with parameters $\left[(3^m-1)/4, 2m, d \geq (3^{m-1}+1)/4\right]$ was constructed in Section VI (see Theorem 35). Examples 36 and 37 show that the code could be much better than the best ternary cyclic code with the same length and dimension. Moreover, the dual code $\mathcal{C}(m)^\perp$ has parameters $\left[(3^m-1)/4, (3^m-1)/4-2m, d^\perp\right]$, where $5 \leq d^\perp \leq 6$, and $d^\perp = 5$ if $m \equiv 0 \pmod 4$, and $\mathcal{C}(m)^\perp$ is distance-almost-optimal.
7) A family of ternary negacyclic codes $\mathcal{C}_{(1,m)}$ with parameters
$$\left[\frac{3^m-1}{2}, \frac{3^m-1+2(-1)^{(m+1)/2}}{4}, d \geq d(m)\right]$$
was constructed in Section VII (see Theorem 44), where $m \geq 5$ is odd and
$$d(m) = \begin{cases} 3^{(m-1)/2}+7 & \text{if } m \equiv 1 \pmod 4, \\ 2\cdot 3^{(m-3)/2}+4 & \text{if } m \equiv 3 \pmod 4. \end{cases}$$
The dual code $\mathcal{C}_{(1,m)}^\perp$ has parameters
$$\left[\frac{3^m-1}{2}, \frac{3^m-1+2(-1)^{(m-1)/2}}{4}, d^\perp \geq d^\perp(m)\right],$$
where
$$d^\perp(m) = \begin{cases} 2\cdot 3^{(m-3)/2}+2 & \text{if } m \equiv 1 \pmod 4, \\ 3^{(m-1)/2}+1 & \text{if } m \equiv 3 \pmod 4. \end{cases}$$
The codes $\mathcal{C}_{(1,m)}$ and $\mathcal{C}_{(1,m)}^\perp$ have very good parameters in general.
8) A family of ternary negacyclic self-dual codes $\mathcal{C}_{(1,m)}$ with parameters
$$[(3^m-1)/2, (3^m-1)/4, d \geq d(m)]$$
was constructed in Section VII (see Theorem 47), where $m \geq 4$ is even, and
$$d(m) = \begin{cases} 3^{(m-2)/2}+3 & \text{if } m \equiv 0 \pmod 4, \\ \frac{3^{(m-2)/2}+15}{2} & \text{if } m \equiv 2 \pmod 4. \end{cases}$$

It is very difficult to construct an infinite family of ternary negacyclic codes with parameters
$$[n, k \in \{(n\pm 2)/2, n/2\}, d \geq \sqrt{n}]$$
such that the minimum distances $d^\perp$ of the dual codes also satisfy $d^\perp \geq \sqrt{n}$. In this paper, we constructed three infinite families of ternary negacyclic codes with parameters
$$[n, k \in \{(n\pm 2)/2, n/2\}, d]$$
and a nearly square-root bound on d (see Theorems 12, 44 and 47).

Some families of ternary negacyclic codes presented in this paper have odd lengths. So these ternary negacyclic codes are scalar-equivalent to some ternary cyclic codes. Therefore, this paper has produced some families of ternary cyclic codes with good parameters, which were not studied in the literature. Notice that most families of ternary negacyclic codes presented in this paper have even lengths, and they have a much better error-correcting capability compared with ternary cyclic codes with the same length and dimension.

Acknowledgment

The authors are very grateful to the associate editor, Prof. Sudhir Ghorpade, and the reviewers for their comments and suggestions that much improved the quality of this article.

References

[1] E. R. Berlekamp, "Negacyclic codes for the Lee metric," in *Proc. Conf. Combinat. Math. Appl.*, Chapel Hill, NC, USA, 1968, pp. 298–316.
[2] T. Blackford, "Negacyclic duadic codes," *Finite Fields Appl.*, vol. 14, no. 4, pp. 930–943, Nov. 2008.
[3] B. Chen, H. Q. Dinh, Y. Fan, and S. Ling, "Polyadic constacyclic codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4895–4904, Sep. 2015.
[4] B. Chen, Y. Fan, L. Lin, and H. Liu, "Constacyclic codes over finite fields," *Finite Fields Their Appl.*, vol. 18, no. 6, pp. 1217–1231, Nov. 2012.
[5] C. Ding, *Codes From Difference Sets*. Singapore: World Scientific, 2015.
[6] C. Ding and C. Tang, *Designs From Linear Codes*, 2nd ed. Singapore: World Scientific, 2022.
[7] C. Ding and J. Yang, "Hamming weights in irreducible cyclic codes," *Discrete Math.*, vol. 313, no. 4, pp. 434–446, Feb. 2013.
[8] C. Dahl and J. P. Pedersen, "Cyclic and pseudo-cyclic MDS codes of length q+1," *J. Combinat. Theory, Ser. A*, vol. 59, no. 1, pp. 130–133, 1992.

[9] D. Danev, S. Dodunekov, and D. Radkova, "A family of constacyclic ternary quasi-perfect codes with covering radius 3," *Des., Codes Cryptogr.*, vol. 59, nos. 1–3, pp. 111–118, Apr. 2011.

[10] X. Dong and S. Yin, "The trace representation of λ-constacyclic codes over $\mathbb{F}_q$," *J. Liaoning Normal Univ.*, vol. 33, pp. 129–131, Jan. 2010.

[11] W. Fang, J. Wen, and F.-W. Fu, "A q-polynomial approach to constacyclic codes," *Finite Fields Their Appl.*, vol. 47, pp. 161–182, Sep. 2017.

[12] P. Gaborit. *Table of Self-Dual Codes Over GF(3)*. Accessed: Aug. 30, 2023. [Online]. Available: https://www.unilim.fr/pages_perso/philippe.gaborit/SD/GF3/GF3.htm

[13] J. Georgiades, "Cyclic (q +1,k)-codes of odd order q and even dimension k are not optimal," *Atti Sem. Mat. Fis. Univ. Modena*, vol. 30, no. 2, pp. 284–285, 1983.

[14] M. Grassl. *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*. Accessed: Aug. 30, 2023. [Online]. Available: http://www.codetables.de

[15] G. Guo, R. Li, Y. Liu, and J. Wang, "A family of negacyclic BCH codes of length $n = \frac{q^{2m}-1}{2}$," *Cryptogr. Commun.*, vol. 12, pp. 187–203, Mar. 2020.

[16] Z. Heng and C. Ding, "A construction of q-ary linear codes with irreducible cyclic codes," *Des., Codes Cryptogr.*, vol. 87, no. 5, pp. 1087–1108, May 2019.

[17] W. C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[18] G. Hughes, "Constacyclic codes, cocycles and a u+v|u−v construction," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 674–680, Mar. 2000.

[19] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, vol. 84, 2nd ed. Berlin, Germany: Springer-Verlag, 1990.

[20] Y. Jia, S. Ling, and C. Xing, "On self-dual cyclic codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2243–2251, Apr. 2011.

[21] X. Kai and S. Zhu, "New quantum MDS codes from negacyclic codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1193–1197, Feb. 2013.

[22] X. Kai, S. Zhu, and Y. Tang, "Quantum negacyclic codes," *Phys. Rev. A, Gen. Phys.*, vol. 88, no. 1, Jul. 2013, Art. no. 012326.

[23] X. Kai, P. Li, and S. Zhu, "Construction of quantum negacyclic BCH codes," *Int. J. Quantum Inf.*, vol. 16, no. 7, Oct. 2018, Art. no. 1850059.

[24] A. Krishna and D. V. Sarwate, "Pseudocyclic maximum-distance-separable codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 4, pp. 880–884, Jul. 1990.

[25] T. Kølve, *Codes for Error Detection*. Singapore: World Scientfic, 2007.

[26] Y. Liu, R. Li, L. Lv, and Y. Ma, "A class of constacyclic BCH codes and new quantum codes," *Quantum Inf. Process.*, vol. 16, no. 3, p. 66, Feb. 2017.

[27] F. Li, Q. Yue, and F. Liu, "The weight distribution of constacyclic codes," *Adv. Math. Commun.*, vol. 11, no. 3, pp. 471–480, Aug. 2017.

[28] F. Li and Q. Yue, "The primitive idempotents and weight distributions of irreducible constacyclic codes," *Des., Codes Cryptogr.*, vol. 86, no. 4, pp. 771–784, Apr. 2018.

[29] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1997.

[30] J. Mi and X. Cao, "Constructing MDS Galois self-dual constacyclic codes over finite fields," *Discrete Math.*, vol. 344, no. 6, Jun. 2021, Art. no. 112388.

[31] B. Pang, S. Zhu, and Z. Sun, "On LCD negacyclic codes over finite fields," *J. Syst. Sci. Complex.*, vol. 31, no. 4, pp. 1065–1077, Aug. 2018.

[32] J. P. Pedersen and C. Dahl, "Classification of pseudo-cyclic MDS codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 365–370, Mar. 1991.

[33] W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*, 2nd ed. Cambridge, MA, USA: MIT Press, 1972.

[34] J. Wang, R. Li, Y. Liu, and G. Guo, "Some negacyclic BCH codes and quantum codes," *Quantum Inf. Process.*, vol. 19, no. 2, p. 74, Jan. 2020.

[35] L. Wang, Z. Sun, and S. Zhu, "Hermitian dual-containing narrow-sense constacyclic BCH codes and quantum codes," *Quantum Inf. Process.*, vol. 18, no. 10, p. 323, Sep. 2019.

[36] X. Wang, Z. Sun, and C. Ding, "Two families of negacyclic BCH codes," *Des., Codes Cryptogr.*, vol. 91, no. 7, pp. 2395–2420, Jul. 2023.

[37] J. Wolfmann, "Projective two-weight irreducible cyclic and constacyclic codes," *Finite Fields Appl.*, vol. 14, no. 2, pp. 351–360, Apr. 2008.

[38] A. Sharma and S. Rani, "Trace description and Hamming weights of irreducible constacyclic codes," *Adv. Math. Commun.*, vol. 12, no. 1, pp. 123–141, 2018.

[39] Z. Shi and F.-W. Fu, "The primitive idempotents of irreducible constacyclic codes and LCD cyclic codes," *Cryptography Commun.*, vol. 12, no. 1, pp. 29–52, Jan. 2020.

[40] M. Singh, "Weight distributions of all irreducible μ-constacyclic codes of length ℓ^n," 2018, *arXiv:1806.10600v1*.

[41] A. B. Sorensen, "Projective Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 6, pp. 1567–1576, Nov. 1991.

[42] Z. Sun, X. Wang, and C. Ding, "Several families of irreducible constacyclic and cyclic codes," *Des., Codes Cryptogr.*, vol. 91, no. 9, pp. 2821–2843, Sep. 2023.

[43] Z. Sun, S. Zhu, and L. Wang, "A class of constacyclic BCH codes," *Cryptogr. Commun.*, vol. 12, no. 2, pp. 265–284, Mar. 2020.

[44] Y. Zhou, X. Kai, S. Zhu, and J. Li, "On the minimum distance of negacyclic codes with two zeros," *Finite Fields Appl.*, vol. 55, pp. 134–150, Jan. 2019.

[45] S. Zhu, Z. Sun, and P. Li, "A class of negacyclic BCH codes and its application to quantum codes," *Des., Codes Cryptogr.*, vol. 86, no. 10, pp. 2139–2165, Oct. 2018.

Zhonghua Sun received the M.S. and Ph.D. degrees from the Hefei University of Technology in 2016 and 2019, respectively. He was a Post-Doctoral Fellow from February 2021 to January 2022 and a Visiting Scholar from July 2023 to August 2023 with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology. He is currently with the Hefei University of Technology. His major research interests include coding theory.

Cunsheng Ding was born in Shaanxi, China, in 1962. He received the M.Sc. degree from the Northwestern Telecommunications Engineering Institute, Xi'an, China, in 1988, and the Ph.D. degree from the University of Turku, Turku, Finland, in 1997.

From 1988 to 1992, he was a Lecturer in mathematics with Xidian University, Xi'an. He was an Assistant Professor in computer science with the National University of Singapore. He joined The Hong Kong University of Science and Technology in 2000, where he is currently a Professor in computer science and engineering. He has coauthored six research monographs. His research interests include combinatorial designs, cryptography, and coding theory.

Dr. Ding co-received the State Natural Science Award of China in 1989. He served as a guest editor or an editor for ten journals.