Two Classes of Constacyclic Codes With Variable Parameters $[(q^m-1)/r, k, d]$

Zhonghua Sun, Cunsheng Ding, and Xiaoqiang Wang

***Abstract*— Constacyclic codes over finite fields are a family of linear codes and contain cyclic codes as a subclass. Constacyclic codes are related to many areas of mathematics and outperform cyclic codes in several aspects. Hence, constacyclic codes are of theoretical importance. On the other hand, constacyclic codes are important in practice, as they have rich algebraic structures and may have efficient decoding algorithms. In this paper, two classes of constacyclic codes are constructed using a general construction of constacyclic codes with cyclic codes. The first class of constacyclic codes is motivated by the punctured Dilix cyclic codes and the second class is motivated by the punctured generalised Reed-Muller codes. The two classes of constacyclic codes contain optimal linear codes. The parameters of the two classes of constacyclic codes are analysed and some open problems are presented in this paper.**

***Index Terms*— Constacylic codes, punctured Dilix cyclic codes, punctured generalised Reed-Muller codes.**

I. Introduction and Motivations

A. The State-of-the-Art of Constacyclic Codes Over Finite Fields

CONSTACYCLIC codes over finite fields are an important class of linear codes due to their performance and applications. Akre [1] and Aydin [3] et al. found some new constacyclic codes that improve the minimum distance of currently best known linear codes. Danev [17], Fang [24], Sun [56], Wang [62] and Zhou [66] et al. constructed several infinite classes of distance-optimal constacyclic codes. Constacyclic codes can also be MDS codes with flexible parameters [16], [26], [33], [44]. On the other hand, constacyclic codes have important applications in the construction of symbol-pair codes [14], [31], [38], locally repairable codes [13], [59] and quantum codes [15], [30], [39], [60], [61], [65].

Manuscript received 6 September 2022; revised 27 September 2023; accepted 1 October 2023. Date of publication 9 October 2023; date of current version 26 December 2023. The work of Zhonghua Sun was supported by the National Natural Science Foundation of China under Grant 62002093 and Grant U21A20428. The work of Cunsheng Ding was supported by the Hong Kong Research Grants Council under Grant 16301522. The work of Xiaoqiang Wang was supported by the National Natural Science Foundation of China under Grant 12001175. An earlier version of this paper was presented in part at WAIFI 2022 [DOI: 10.1007/978-3-031-22944-2_7]. *(Corresponding author: Zhonghua Sun.)*

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).

Xiaoqiang Wang is with the Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China (e-mail: waxiqq@163.com).

Communicated by V. Skachek, Associate Editor for Coding and Decoding.
Digital Object Identifier 10.1109/TIT.2023.3322990

The algebraic structure of constacyclic codes over finite fields has been studied in [4], [8], [9], [11], [12], [23], [25], [41], [45], [50], [51], [52], [53], [54]. Several classes of distance-optimal constacyclic codes with small distances have been constructed in [17], [24], [56], [62], [66]. The weight distributions of several classes of constacyclic codes have been determined in [35], [36], [49], [54], [57], [58], [63]. Although constacyclic codes are of theoretical importance, very limited results on λ-constacyclic codes with $\lambda \neq 1$ are known in the literature, while there are a lot of references on cyclic codes.

B. Motivations and Objectives

By definition, cyclic codes are a proper subclass of constacyclic codes and constacyclic codes are a proper subclass of linear codes (see Section II-A for their definitions). Clearly, cyclic codes have a better algebraic structure than λ-constacyclic codes with $\lambda \neq 1$ and constacyclic codes have a better algebraic structure than other linear codes. A better algebraic structure may mean a better decoding algorithm. Then the following two questions are interesting and good motivations for studying constacyclic codes.

Question 1: Is a given linear code over $\mathrm{GF}(q)$ monomially-equivalent to a cyclic code over $\mathrm{GF}(q)$?

Question 2: Is a given linear code over $\mathrm{GF}(q)$ monomially-equivalent to a λ-constacyclic code over $\mathrm{GF}(q)$ with $\lambda \neq 1$?

For example, the Hamming code of length $(q^m-1)/(q-1)$ over $\mathrm{GF}(q)$ is monomially-equivalent to a cyclic code over $\mathrm{GF}(q)$ when $\gcd(m, q-1) = 1$ [28, Theorem 5.1.4], and is always monomially-equivalent to a contacyclic code over $\mathrm{GF}(q)$ [24], [57]. This shows that the Hamming code is attractive. Notice that the two questions above are open for most linear codes.

Recall that cyclic codes have a better algebraic structure. Then one would ask why we would study constacyclic codes. Below is a list of motivations for studying λ-constacyclic codes with $\lambda \neq 1$:

- There does not exist a cyclic code over $\mathrm{GF}(q)$ with parameters $[n, k, d]$ for certain q, n, k and d; but there is a λ-constacyclic codes over $\mathrm{GF}(q)$ with parameters $[n, k, d]$ and $\lambda \neq 1$ [26], [33].
- The best $[n, k]$ constacyclic code over $\mathrm{GF}(q)$ has a much better error-correcting capability than the best $[n, k]$ cyclic code over $\mathrm{GF}(q)$ for certain q, n and k (see [17], [56] and the references therein).
- Constacyclic codes can do many things that cyclic codes cannot do. For example, the Hamming code of length

$(q^m-1)/(q-1)$ can always be constructed by a constacyclic code, but cannot be constructed by a cyclic code when $\gcd(q-1,m)\neq 1$.

- Cyclic self-dual codes of length n over $\mathrm{GF}(q)$ exist if and only if n is even and $q=2^s$ with a positive integer s [29]; but negacyclic self-dual codes of length n over $\mathrm{GF}(q)$ exist if and only if $n=2^a n'$ with an odd integer n' and $q\not\equiv -1 \pmod{2^{a+1}}$ [9].

The original binary Reed-Muller codes were introduced by Reed and Muller in 1954 [42], [48]. They are called geometric codes, as all the minimum weight codewords of the r-th order Reed-Muller code $\mathcal{R}_2(r,m)$ are the incidence vectors of all the $(m-r)$-flats in the affine geometry $\mathrm{AG}(m,\mathrm{GF}(2))$ and they generate $\mathcal{R}_2(r,m)$ [2]. The automorphism group of $\mathcal{R}_2(r,m)$ is known to be the general affine group $\mathrm{GA}_m(\mathrm{GF}(2))$ which is triply transitive on $\mathrm{GF}(2)^m$. Hence, the binary Reed-Muller codes support 3-designs. It was later discovered that the binary Reed-Muller codes become cyclic codes if they are punctured in a special coordinate position. These properties show that the original Reed-Muller codes are very interesting in theory. For more information on Reed-Muller codes, the reader is referred to [2], [6], [7], [18], [22], [34], [37] and the references therein. Binary Reed-Muller codes are also interesting in practice as they have efficient decoding algorithms [48]. The binary Reed-Muller codes and their punctured codes were later generalised to codes over $\mathrm{GF}(q)$ for general q. In 2018, the binary Reed-Muller codes were generalised into another type of linear codes [19], which were called *Dilix codes* for the purpose of distinguishing the two types of generalisations [21, Chapter 6]. The Dilix codes have also interesting properties and are extended cyclic codes by definition. In other words, if the Dilix codes are punctured in the last coordinate, the punctured Dilix codes are cyclic. A recent result by Yardi and Pellikaan [64] shows that any linear code can be obtained by a sequence of puncturing and/or shortening of some cyclic code. Motivated by the interesting properties of the punctured generalized Reed-Muller codes and punctured Dilix codes, we will construct and analyse two classes of constacyclic codes which are obtained from the punctured generalized Reed-Muller codes and the punctured Dilix codes. In particular, a new infinite class of distance-optimal constacyclic codes and a new infinite class of distance-almost-optimal constacyclic codes are obtained, and a new infinite class of negacyclic self-dual codes of length $n=(q^m-1)/2$ over $\mathrm{GF}(q)$ with minimum distance $d>\sqrt{n}$ is presented in this paper.

C. The Organisation of This Paper

The rest of this paper is organized as follows. Section II recalls some basic results about linear codes and constacyclic codes, which will be needed later. Section III introduces a general construction of constacyclic codes of length $(q^m-1)/r$ with cyclic codes of length q^m-1. Section IV introduces the first class of constacyclic codes and analyses the parameters of these codes. Section V introduces the second class of constacyclic codes and analyses the parameters of these codes. Section VI concludes this paper and makes concluding remarks.

II. Preliminaries

A. Constacyclic Codes and Cyclic Codes

Let q be a prime power, $\mathrm{GF}(q)$ be the finite field with q elements, and let $\mathrm{GF}(q)^*$ denote the multiplicative group of $\mathrm{GF}(q)$. By an $[n,k,d]$ linear code $\mathcal{C}$ over $\mathrm{GF}(q)$ we mean a k-dimensional linear subspace of $\mathrm{GF}(q)^n$ with minimum distance d. For a linear code $\mathcal{C}$ of length n over $\mathrm{GF}(q)$, we use $\dim(\mathcal{C})$ and $d(\mathcal{C})$ to denote its dimension and minimum Hamming distance, respectively. Let A_i denote the number of codewords with Hamming weight i in $\mathcal{C}$. The *weight enumerator* of $\mathcal{C}$ is defined as $1+A_1z+\cdots+A_nz^n$. The sequence $(1,A_1,\ldots,A_n)$ is called the *weight distribution* of $\mathcal{C}$. If the number of nonzero A_i in the sequence $(A_1,A_2,\ldots,A_n)$ equals t, then $\mathcal{C}$ is called a t-weight code.

Let $\lambda\in\mathrm{GF}(q)^*$ and let $\mathrm{ord}(\lambda)$ denote the order of λ in $\mathrm{GF}(q)^*$. We say that a linear code $\mathcal{C}$ of length n is λ-*constacyclic* if $(c_0,c_1,\ldots,c_{n-1})\in\mathcal{C}$ implies

$$(\lambda c_{n-1},c_0,c_1,\ldots,c_{n-2})\in\mathcal{C}.$$

By definition, 1-constacyclic codes are the classical cyclic codes. Hence, cyclic codes form a subclass of constacyclic codes. In other words, constacyclic codes are a generalisation of the classical cyclic codes.

Let Φ be the mapping from $\mathrm{GF}(q)^n$ to the quotient ring $\mathrm{GF}(q)[x]/\langle x^n-\lambda\rangle$ defined by

$$\Phi((c_0,c_1,\ldots,c_{n-1}))=\sum_{i=0}^{n-1}c_ix^i.$$

It is well known that every ideal of the ring $\mathrm{GF}(q)[x]/\langle x^n-\lambda\rangle$ is *principal* and a linear code $\mathcal{C}\subset\mathrm{GF}(q)^n$ is λ-constacyclic if and only if $\Phi(\mathcal{C})$ is an ideal of $\mathrm{GF}(q)[x]/\langle x^n-\lambda\rangle$. Consequently, we will identify $\mathcal{C}$ with $\Phi(\mathcal{C})$ for any λ-constacyclic code $\mathcal{C}$. Let $\mathcal{C}=\langle g(x)\rangle$ be a λ-constacyclic code of length n over $\mathrm{GF}(q)$, 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 $\mathcal{C}$. The dual code of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined by

$$\mathcal{C}^\perp=\{\mathbf{b}\in\mathrm{GF}(q)^n:\mathbf{b}\mathbf{c}^T=0,\ \forall\ \mathbf{c}\in\mathcal{C}\},$$

where $\mathbf{b}\mathbf{c}^T$ denotes the standard inner product of the two vectors $\mathbf{b}$ and $\mathbf{c}$. Constacyclic codes and their duals have the following relation, which is a fundamental result.

Lemma 3 [33]: The dual code of an $[n,k]$ λ-constacyclic code $\mathcal{C}$ generated by $g(x)$ is an $[n,n-k]$ λ^{-1}-constacyclic code $\mathcal{C}^\perp$ generated by $\widehat{h}(x)=h_0^{-1}x^k h(x^{-1})$, where $h(x)=(x^n-\lambda)/g(x)$ is the check polynomial of $\mathcal{C}$ and h_0 is the coefficient of x^0 in $h(x)$.

B. Cyclotomic Cosets

Let n be a positive integer with $\gcd(q,n)=1$, r be a positive divisor of $q-1$, and let λ be an element of $\mathrm{GF}(q)$ with order r. To deal with λ-constacyclic codes of length n over $\mathrm{GF}(q)$, we have to study the factorization of $x^n-\lambda$ over

$\mathrm{GF}(q)$. To this end, we need to introduce q-cyclotomic cosets modulo rn.

Let $\mathbb{Z}_{rn} = \{0, 1, 2, \cdots, rn-1\}$ be the ring of integers modulo rn. For any $i \in \mathbb{Z}_{rn}$, the *q-cyclotomic coset of i modulo rn* is defined by

$$C_i^{(q,rn)} = \{i, iq, iq^2, \cdots, iq^{\ell_i - 1}\} \bmod rn \subseteq \mathbb{Z}_{rn},$$

where ℓ_i is the smallest positive integer such that

$$i \equiv iq^{\ell_i} \pmod{rn},$$

and is the *size* of the q-cyclotomic coset $C_i^{(q,rn)}$. The smallest integer in $C_i^{(q,rn)}$ is called the *coset leader* of $C_i^{(q,rn)}$. Let $\Gamma_{(q,rn)}$ be the set of all the coset leaders. We have then

$$C_i^{(q,rn)} \cap C_j^{(q,rn)} = \emptyset$$

for any two distinct elements i and j in $\Gamma_{(q,rn)}$, and

$$\bigcup_{i \in \Gamma_{(q,rn)}} C_i^{(q,rn)} = \mathbb{Z}_{rn}.$$

Let $\mathrm{ord}_{rn}(q)$ denote the multiplicative order of q modulo rn and let $m = \mathrm{ord}_{rn}(q)$. It is easily seen that there is a primitive element α of $\mathrm{GF}(q^m)$ such that $\beta = \alpha^{(q^m-1)/rn}$ and $\beta^n = \lambda$. Then β is a primitive rn-th root of unity in $\mathrm{GF}(q^m)$. 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

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

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

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

Define

$$\Gamma_{(q,rn,r)}^{(1)} = \{i : i \in \Gamma_{(q,rn)},\ i \equiv 1 \pmod{r}\}.$$

Then

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

Lemma 4 [57]: Let n be a positive integer with $\gcd(q, n) = 1$ and let r be a positive divisor of $q-1$. If $\mathrm{ord}_n(q) = \ell$, then $\mathrm{ord}_{rn}(q) = \frac{r}{\gcd((q^\ell - 1)/n, r)}\ell$, which is the size ℓ_1 of $C_1^{(q,rn)}$, and the size ℓ_i of each q-cyclotomic coset $C_i^{(q,rn)}$ is a divisor of $\mathrm{ord}_{rn}(q)$.

C. The Trace Representation of Constacyclic Codes

For any positive integer m, let $\mathrm{Tr}_{q^m/q}$ denote the trace function from $\mathrm{GF}(q^m)$ to $\mathrm{GF}(q)$. The trace representation of λ-constacyclic codes is documented below (see [23], [49], [58, Theorem 1]).

Lemma 5: Let $\lambda \in \mathrm{GF}(q)^*$ with $\mathrm{ord}(\lambda) = r$. Let n be a positive integer such that $\gcd(n, q) = 1$. Let $m = \mathrm{ord}_{rn}(q)$ and let $\beta \in \mathrm{GF}(q^m)$ be a primitive rn-th root of unity such that $\beta^n = \lambda$. Let $\mathcal{C}$ be a λ-constacyclic code of length n over $\mathrm{GF}(q)$ with check polynomial $\prod_{j=1}^{s} \mathbb{M}_{\beta^{i_j}}(x)$, where $C_{i_a}^{(q,r\ n)} \cap C_{i_b}^{(q,rn)} = \emptyset$ for $a \neq b$. Then $\mathcal{C}$ has the trace representation

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

where $m_j = |C_{i_j}^{(q,rn)}|$.

Lemma 5 is very useful in determining the parameters and weight distributions of some constacyclic codes. We will make use of this lemma later in this paper.

D. The BCH Bound for Constacyclic Codes

The following lemma documents the BCH bound for constacyclic codes over finite fields, which is a generalization of the BCH bound of cyclic codes.

Lemma 6 ([33, Lemma 4] The BCH Bound for Constacyclic Codes): Let $\lambda \in \mathrm{GF}(q)^*$ with $\mathrm{ord}(\lambda) = r$. Let n be a positive integer such that $\gcd(n, q) = 1$. Let $\mathcal{C}$ be a λ-constacyclic code of length n over $\mathrm{GF}(q)$ with generator polynomial $g(x)$. Let $\beta \in \mathrm{GF}(q^m)$ be a primitive rn-th root of unity such that $\beta^n = \lambda$. If there are integers e, h, δ with $\gcd(e, n) = 1$ and $2 \leq \delta \leq n$ such that

$$g(\beta^{1+reh}) = g(\beta^{1+re(h+1)}) = \cdots = g(\beta^{1+re(h+\delta-2)}) = 0,$$

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

E. Some Bounds of Linear Codes

We now recall two bounds on linear codes, which will be needed later.

Lemma 7 (Sphere Packing Bound [28]): Let $\mathcal{C}$ be an $[n, k, d]$ code over $\mathrm{GF}(q)$. Then

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

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

The following lemma is the sphere packing bound for linear codes with an even minimum distance.

Lemma 8 [24]: Let $\mathcal{C}$ be an $[n, k, d]$ code over $\mathrm{GF}(q)$, where d is an even integer. Then

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

F. Automorphism Groups and Equivalence of Linear Codes

Two linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be *permutation-equivalent* if there is a permutation of coordinates which sends $\mathcal{C}_1$ to $\mathcal{C}_2$. This permutation could be described employing a *permutation matrix*, which is a square matrix with exactly one 1 in each row and column and 0s elsewhere. The set of coordinate permutations that map a code $\mathcal{C}$ to itself forms a group, which is referred to as the *permutation automorphism group* of $\mathcal{C}$ and denoted by $\mathrm{PAut}(\mathcal{C})$.

A *monomial matrix* over $\mathrm{GF}(q)$ is a square matrix having exactly one nonzero element of $\mathrm{GF}(q)$ in each row and column. A monomial matrix M can be written either in the form DP or the form PD_1, where D and D_1 are diagonal matrices and P is a permutation matrix.

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two linear codes of the same length over $\mathrm{GF}(q)$. Then $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be *monomially-equivalent* if there is a nomomial matrix over $\mathrm{GF}(q)$ such that $\mathcal{C}_2 = \mathcal{C}_1 M$. Monomial equivalence and permutation equivalence are precisely the same for binary codes. If $\mathcal{C}_1$ and $\mathcal{C}_2$ are monomially-equivalent, then they have the same weight distribution. The set of monomial matrices that map $\mathcal{C}$ to itself forms the group $\mathrm{MAut}(\mathcal{C})$, which is called the *monomial automorphism group* of $\mathcal{C}$. By definition, we have $\mathrm{PAut}(\mathcal{C}) \subseteq \mathrm{MAut}(\mathcal{C})$. Two linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of the same length over $\mathrm{GF}(q)$ are said to be *scalar-equivalent* if there is an invertible diagonal matrix D over $\mathrm{GF}(q)$ such that $\mathcal{C}_2 = \mathcal{C}_1 D$.

Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be *equivalent* if there is a monomial matrix M and an automorphism γ of $\mathrm{GF}(q)$ such that $\mathcal{C}_1 = \mathcal{C}_2 M\gamma$. All three are the same if the codes are binary; monomial equivalence and equivalence are the same if the field considered has a prime number of elements.

The *automorphism group* of $\mathcal{C}$, denoted by $\mathrm{Aut}(\mathcal{C})$, is the set of maps of the form $M\gamma$, where M is a monomial matrix and γ is a field automorphism, that map $\mathcal{C}$ to itself. In the binary case, $\mathrm{PAut}(\mathcal{C})$, $\mathrm{MAut}(\mathcal{C})$ and $\mathrm{Aut}(\mathcal{C})$ are the same. If q is a prime, $\mathrm{MAut}(\mathcal{C})$ and $\mathrm{Aut}(\mathcal{C})$ are identical. In general, we have

$$\mathrm{PAut}(\mathcal{C}) \subseteq \mathrm{MAut}(\mathcal{C}) \subseteq \mathrm{Aut}(\mathcal{C}).$$

In this paper, we consider the monomial equivalence of linear codes. Two monomially-equivalent codes have the same parameters and weight distribution. If a linear code $\mathcal{C}$ is monomially-equivalent to a constacyclic code $\mathcal{C}_2$, we prefer $\mathcal{C}_2$ to $\mathcal{C}$ as constacyclic codes have a better algebraic structure than general linear codes.

G. Some Basic Notation

From now on, we fix the following notation, unless it is stated otherwise:

- q is a prime power.
- $m \geq 2$ is an integer.
- $r \geq 2$ is a divisor of $q-1$.
- $N = q^m - 1$.
- $\lambda \in \mathrm{GF}(q)^*$ with $\mathrm{ord}(\lambda) = r$.
- β is a primitive element of $\mathrm{GF}(q^m)$ such that $\beta^{(q^m-1)/r} = \lambda$.

H. The Hamming Weight and q-Weight of Nonnegative Integers

For each $0 \leq i \leq N$, let the q-adic expansion of i be

$$i = \sum_{j=0}^{m-1} i_j q^j,$$

where $0 \leq i_j \leq q-1$. The *Hamming weight* of i, denoted by $\mathtt{wt}(i)$, is defined to be the Hamming weight of the vector $(i_0, i_1, \ldots, i_{m-1})$. The *$q$-weight* of i, denoted by $\mathtt{wt}_q(i)$, is defined to be $\sum_{j=0}^{m-1} i_j$. The two kinds of weights will be used later.

I. The Projective Reed-Muller Codes

A point of the projective geometry $\mathrm{PG}(m-1, \mathrm{GF}(q))$ is given in homogeneous coordinates by $(x_1, x_2, \ldots, x_m)$ where all x_i are in $\mathrm{GF}(q)$ and are not all zero. Each point of $\mathrm{PG}(m-1, \mathrm{GF}(q))$ has $q-1$ coordinate representations, as $(ax_1, ax_2, \ldots, ax_m)$ and $(x_1, x_2, \ldots, x_m)$ generate the same 1-dimensional subspace of $\mathrm{GF}(q)^m$ for any nonzero $a \in \mathrm{GF}(q)$.

Let $\mathrm{GF}(q)[x_1, x_2, \ldots, x_m]$ be the set of polynomials in m indeterminates over $\mathrm{GF}(q)$, which is a linear space over $\mathrm{GF}(q)$. Let $A(q, m, h)$ be the subspace of

$$\mathrm{GF}(q)[x_1, x_2, \ldots, x_m]$$

generated by all the homogeneous polynomials of degree h. Let $n = (q^m - 1)/(q-1)$ and let $\{\mathbf{x}^1, \mathbf{x}^2, \cdots, \mathbf{x}^n\}$ be a set of projective points in $\mathrm{PG}(m-1, \mathrm{GF}(q))$. Then the *$h$-th order projective Reed-Muller code* $\mathrm{PRM}(q, m, h)$ of length n is defined by

$$\begin{aligned}\mathrm{PRM}(q, m, h) = \{&\big(f(\mathbf{x}^1), f(\mathbf{x}^2), \ldots, f(\mathbf{x}^n)\big) : \\ &f(x_1, x_2, \ldots, x_m) \in A(q, m, h)\}.\end{aligned}$$

The code $\mathrm{PRM}(q, m, h)$ depends on the choice of the set $\{\mathbf{x}^1, \mathbf{x}^2, \cdots, \mathbf{x}^n\}$ of coordinate representatives of the point set in $\mathrm{PG}(m-1, \mathrm{GF}(q))$, but is unique up to monomial equivalence (in fact, up to scalar equivalence). The parameters of $\mathrm{PRM}(q, m, h)$ and $\mathrm{PRM}(q, m, h)^\perp$ are known and documented in the following theorems [5], [34], [55].

Theorem 9: Let $m \geq 2$ and $1 \leq h \leq (m-1)(q-1)$. Then the linear code $\mathrm{PRM}(q, m, h)$ has length $n = (q^m-1)/(q-1)$ and minimum distance $(q-v)q^{m-2-u}$, where $h - 1 = u(q-1) + v$ and $0 \leq v < q-1$. Furthermore,

$$\begin{aligned}&\dim(\mathrm{PRM}(q, m, h)) \\ &= \sum_{\substack{t \equiv h \pmod{q-1} \\ 0 < t \leq h}} \left(\sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{t - jq + m - 1}{t - jq} \right).\end{aligned}$$

Theorem 10: Let $m \geq 2$ and $1 \leq h \leq (m-1)(q-1)$. If $h \not\equiv 0 \pmod{q-1}$, then

$$\mathrm{PRM}(q, m, h)^\perp = \mathrm{PRM}(q, m, (m-1)(q-1) - h).$$

By Theorem 9 and definition, $\mathrm{PRM}(q, m, 1)$ is monomially-equavalent to the Simplex code. The weight distribution of $\mathrm{PRM}(q, m, 2)$ was settled in [37]. It was pointed out in [7], [55] that the code $\mathrm{PRM}(q, m, h)$ is not cyclic in general, but is equivalent to a cyclic code if $\gcd(m, q-1) = 1$ or $h \equiv 0 \pmod{q-1}$. Later in this paper, we will compare some newly constructed constacyclic codes with the projective Reed-Muller codes. This explains why we introduced the projective Reed-Muller codes here. We will need the following theorem later.

Theorem 11 [37]: Let $m \geq 2$. Then the weight distribution of $\mathrm{PRM}(q, m, 2)$ is given by

$$A_0 = 1,$$
$$A_{q^{m-1}} = q^m - 1 + \sum_{j=1}^{\lfloor (m-1)/2 \rfloor} q^{j^2+j} \frac{\prod_{i=m-2j}^{m}(q^i-1)}{\prod_{i=1}^{j}(q^{2i}-1)},$$
$$A_{q^{m-1}-\tau q^{m-1-j}} = \frac{q^{j^2}(q^j+\tau)}{2} \frac{\prod_{i=m-2j+1}^{m}(q^i-1)}{\prod_{i=1}^{j}(q^{2i}-1)},$$

$1 \leq j \leq \lfloor m/2 \rfloor$, $\tau \in \{1, -1\}$, and $A_h = 0$ for other h.

J. The Nonprimitive Reed-Muller Codes

Let $\ell = (q-1)h + \ell_0 < (q-1)m$, where $0 \leq \ell_0 \leq q-2$ and $\ell_0 \equiv 0 \pmod r$. Let $\mathrm{P}(q, m, r, \ell)$ be the linear subspace of $\mathrm{GF}(q)[x_1, x_2, \ldots, x_m]$, which is spanned by all monomials $x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}$ satisfying the following three conditions:

1) $0 \leq i_j \leq q-1$ for $1 \leq j \leq m$,
2) $\sum_{j=1}^{m} i_j \equiv 0 \pmod r$,
3) $\sum_{j=1}^{m} i_j \leq \ell$.

Let β be a primitive element of $\mathrm{GF}(q^m)$ and let

$$\mathbb{M}_\beta(x) = \sum_{i=0}^{m-1} \epsilon_i x^i + x^m,$$

where $\epsilon_i \in \mathrm{GF}(q)$. Let

$$\mathbf{M} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -\epsilon_0 & -\epsilon_1 & -\epsilon_2 & \cdots & -\epsilon_{m-1} \end{pmatrix}$$

be the companion matrix of $\mathbb{M}_\beta(x)$. Let $n = (q^m-1)/r$ and $\mathbf{e} = (1, 0, \ldots, 0)$. Then the *nonprimitive generalized Reed-Muller code* $\mathrm{NGRM}(q, m, r, h)$ of length n is defined by

$$\mathrm{NGRM}(q, m, r, h) = \{\big(f(\mathbf{e}), f(\mathbf{eM}), \ldots, f(\mathbf{eM}^{n-1})\big) : f(x_1, x_2, \ldots, x_m) \in \mathrm{P}(q, m, r, \ell)\}.$$

In particular, when $r = q-1$, it is easily verified that

$$\{\mathbf{e}, \mathbf{eM}, \cdots, \mathbf{eM}^{n-1}\}$$

is the set of projective points in $\mathrm{PG}(m-1, \mathrm{GF}(q))$. Then the code $\mathrm{NGRM}(q, m, q-1, h)$ is also called the *h-th order projective generalized Reed-Muller code* $\mathrm{PGRM}(q, m, h)$ of length n.

Theorem 12 [18]: Let $\ell = (q-1)h + \ell_0 < (q-1)m$, where $0 \leq \ell_0 \leq q-2$ and $\ell_0 \equiv 0 \pmod r$. Then the minimum weight of $\mathrm{NGRM}(q, m, r, h)$ is $\frac{(q-\ell_0)q^{m-h-1}-1}{r}$ and

$$\dim(\mathrm{NGRM}(q, m, r, h)) = |\{0 \leq j \leq (q^m-1)/r : \mathtt{wt}_q(jr) \leq \ell\}|. \quad (1)$$

Note that the minimum distance of $\mathrm{NGRM}(q, m, r, h)$ is known to be $\frac{(q-\ell_0)q^{m-h-1}-1}{r}$. But the expression in (1) is not specific, and no specific formula for $\dim(\mathrm{NGRM}(q, m, r, h))$ is known. Later we will compare the codes $\mathrm{NGRM}(q, m, r, h)$ with the constacyclic codes presented in this paper. To this end, we present the following example.

Example 13: The parameters of the codes $\mathrm{NGRM}(3, 4, 2, h)$ for $0 \leq h \leq 3$ are given below:

$$[40, 1, 40], \ [40, 11, 13], \ [40, 30, 4], \ [40, 40, 1].$$

K. The Punctured Dilix Codes

In this subsection, we outline a type of cyclic codes, called *punctured Dilix codes* [19]. Let β be a primitive element of $\mathrm{GF}(q^m)$. For any $1 \leq h \leq m$, we define a polynomial

$$\omega_{(q,m,h)}(x) = \prod_{\substack{1 \leq a \leq n-1 \\ 1 \leq \mathtt{wt}(a) \leq h}} (x - \beta^a).$$

Since $\mathtt{wt}(a)$ is a constant function on each q-cyclotomic coset modulo q^m-1, $\omega_{(q,m,h)}(x)$ is a polynomial over $\mathrm{GF}(q)$. By definition, $\omega_{(q,m,h)}(x)$ is a divisor of $x^{q^m-1}-1$. Let $\Omega(q, m, h)$ denote the cyclic code over $\mathrm{GF}(q)$ with length q^m-1 and generator polynomial $\omega_{(m,q,h)}(x)$.

Theorem 14 [19]: Let $m \geq 2$ and $1 \leq h \leq m-1$. Then $\Omega(q, m, h)$ has parameters

$$\left[q^m - 1, q^m - \sum_{i=0}^{h} \binom{m}{i} (q-1)^i, d \geq (q^{h+1}-1)/(q-1)\right].$$

Later we will use the codes $\Omega(q, m, h)$ to construct some constacyclic codes. This explains why we introduced the punctured Dilix codes $\Omega(q, m, h)$ here.

III. A General Construction of Constacyclic Codes of Length $(q^m-1)/r$ With Cyclic Codes of Length q^m-1

In this section, we present a general construction of constacyclic codes of length $(q^m-1)/r$ with cyclic codes of length q^m-1 over $\mathrm{GF}(q)$, where $r > 1$ is a divisor of $q-1$. Throughout this section, let $n = (q^m-1)/r$, where m is an integer with $m \geq 2$. Define $N = rn = q^m - 1$. Let β be a primitive element of $\mathrm{GF}(q^m)$ and $\lambda = \beta^n$. Then λ is an element of $\mathrm{GF}(q)^*$ with order r.

Let $\mathcal{C}$ be a cyclic code of length N over $\mathrm{GF}(q)$ with generator polynomial

$$g(x) = \prod_{i \in D(\mathcal{C})} (x - \beta^i),$$

where $D(\mathcal{C})$ is the union of some q-cyclotomic cosets modulo N and is called the *defining set* of $\mathcal{C}$ with respect to the primitive element β of $\mathrm{GF}(q^m)$. Put

$$\underline{D}(\mathcal{C}) = \{i \in D(\mathcal{C}) : i \equiv 1 \pmod r\}.$$

If $\underline{D}(\mathcal{C}) = \emptyset$, define $\underline{g}(x) = 1$. If $\underline{D}(\mathcal{C}) \neq \emptyset$, define

$$\underline{g}(x) = \prod_{i \in \underline{D}(\mathcal{C})} (x - \beta^i).$$

Then the following hold:

1) $\underline{g}(x)$ is a polynomial over $\mathrm{GF}(q)$.
2) $\underline{g}(x) = \gcd(g(x), x^n - \lambda)$.

Let $\underline{\mathcal{C}}$ denote the λ-constacyclic code of length n over $\mathrm{GF}(q)$ with generator polynomial $\underline{g}(x)$. By definition, $\underline{\mathcal{C}}$ is constructed from the given cyclic code $\mathcal{C}$. In particular, the following hold:

1) If $(x^n-\lambda) \mid g(x)$, i.e., $\underline{D}(\mathcal{C}) = \Gamma^{(1)}_{(q,N,r)}$, then $\underline{\mathcal{C}} = \{\mathbf{0}\}$.
2) If $\gcd(g(x), x^n-\lambda) = 1$, i.e., $\underline{D}(\mathcal{C}) = \emptyset$, then $\underline{\mathcal{C}} = \mathrm{GF}(q)^n$.

This general construction produces a nontrivial code only when $\underline{D}(\mathcal{C}) \notin \{\emptyset, \Gamma^{(1)}_{(q,N,r)}\}$.

By definition,

$$\dim(\mathcal{C}) = N - \deg(g) = N - |D(\mathcal{C})|$$

and

$$\dim(\underline{\mathcal{C}}) = n - \deg(\underline{g}) = n - |\underline{D}(\mathcal{C})|.$$

Hence, it may not be easy to determine $\dim(\underline{\mathcal{C}})$ even if $\dim(\mathcal{C})$ is known. However, this may be possible in some special cases. It is clear that

$$x^{rn}-1 = \prod_{i=0}^{r-1}(x^n-\lambda^i),$$

and $\gcd(x^n-\lambda^i, x^n-\lambda^j) = 1$ for $0 \le i \ne j \le r-1$. For a given $g(x) \mid (x^N-1)$, let $\underline{g}_i(x) = \gcd(g(x), x^n-\lambda^i)$. Then $\underline{g}_1(x) = \underline{g}(x)$. Let $\mathrm{Ind}(\mathcal{C}) = \{i : \underline{g}_i(x) \ne 1, 0 \le i \le r-1\}$, then

$$g(x) = \prod_{i \in \mathrm{Ind}(\mathcal{C})} \underline{g}_i(x).$$

Theorem 15: Assume that $\gcd(g(x), x^n-\lambda) \ne 1$ and $\gcd(g(x), x^n-\lambda) \ne x^n-\lambda$. Then the following hold:

1) $d(\mathcal{C}) \le |\mathrm{Ind}(\mathcal{C})| \cdot d(\underline{\mathcal{C}})$.
2) If $1 \le |\mathrm{Ind}(\mathcal{C})| \le r-1$, then $2 \le d(\mathcal{C}) \le |\mathrm{Ind}(\mathcal{C})|+1$.
3) The code $\underline{\mathcal{C}} = \{c(x) \pmod{x^n-\lambda} : c(x) \in \mathcal{C}\}$.

Proof: 1) For any $\underline{c}(x) \in \underline{\mathcal{C}}$, we have

$$c(x) := \underline{c}(x) \prod_{i \in \mathrm{Ind}(\mathcal{C}) \setminus \{1\}} (x^n-\lambda^i) \in \mathcal{C}.$$

Since $\prod_{i \in \mathrm{Ind}(\mathcal{C})\setminus\{1\}}(x^n-\lambda^i)$ can be expanded as a sum of the form $\sum a_i x^{ni}$, we have

$$\mathtt{wt}(c(x)) = \mathtt{wt}(\underline{c}(x)) \cdot \mathtt{wt}\left(\prod_{i \in \mathrm{Ind}(\mathcal{C})\setminus\{1\}} (x^n-\lambda^i)\right).$$

Consequently,

$$\begin{aligned} &d(\mathcal{C}) \\ &\le \min\left\{\mathtt{wt}\left(\underline{c}(x) \prod_{i \in \mathrm{Ind}(\mathcal{C})\setminus\{1\}} (x^n-\lambda^i)\right) : 0 \ne \underline{c}(x) \in \underline{\mathcal{C}}\right\} \\ &\le |\mathrm{Ind}(\mathcal{C})| \cdot d(\underline{\mathcal{C}}). \end{aligned}$$

2) If $1 \le |\mathrm{Ind}(\mathcal{C})| \le r-1$, then $0 \ne \prod_{i \in \mathrm{Ind}(\mathcal{C})}(x^n-\lambda^i) \in \mathcal{C}$. Note that

$$\mathtt{wt}\left(\prod_{i \in \mathrm{Ind}(\mathcal{C})} (x^n-\lambda^i)\right) \le |\mathrm{Ind}(\mathcal{C})|+1,$$

we have $d(\mathcal{C}) \le |\mathrm{Ind}(\mathcal{C})|+1$.

3) Let $\mathrm{Res}(\mathcal{C}) = \{c(x) \pmod{x^n-\lambda} : \ c(x) \in \mathcal{C}\}$. Let $c(x) \in \mathcal{C}$, then there is $\underline{c}(x) \in \mathrm{GF}(q)[x]/\langle x^n-\lambda\rangle$ such that

$$\underline{c}(x) \equiv c(x) \pmod{x^n-\lambda}.$$

Clearly,

$$\gcd(c(x), x^n-\lambda) = \gcd(\underline{c}(x), x^n-\lambda).$$

Then $\underline{g}(x)$ divides $\underline{c}(x)$. It follows that $\underline{c}(x) \in \underline{\mathcal{C}}$. Consequently, $\mathrm{Res}(\mathcal{C}) \subseteq \underline{\mathcal{C}}$.

Let $\underline{c}(x) \in \underline{\mathcal{C}}$. It is easily verified that

$$\gcd\left(\frac{x^n-\lambda}{\underline{g}(x)}, \frac{g(x)}{\underline{g}(x)}\right) = 1.$$

Then there are $a_1(x)$ and $a_2(x)$ such that

$$a_1(x)\frac{x^n-\lambda}{\underline{g}(x)} + a_2(x)\frac{g(x)}{\underline{g}(x)} = 1.$$

It follows that

$$a_2(x)\frac{g(x)}{\underline{g}(x)}\underline{c}(x) = \underline{c}(x) - a_1(x)\frac{x^n-\lambda}{\underline{g}(x)}\underline{c}(x).$$

Note that $\underline{g}(x) \mid \underline{c}(x)$, we have $g(x) \mid \frac{g(x)}{\underline{g}(x)}\underline{c}(x)$ and

$$(x^n-\lambda) \mid \frac{x^n-\lambda}{\underline{g}(x)}\underline{c}(x).$$

Therefore,

$$c(x) := a_2(x)\frac{g(x)}{\underline{g}(x)}\underline{c}(x) \in \mathcal{C}$$

and $c(x) \equiv \underline{c}(x) \pmod{x^n-\lambda}$. Consequently, $\underline{\mathcal{C}} \subseteq \mathrm{Res}(\mathcal{C})$. The desired conclusion follows. ∎

The third conclusion of Theorem 15 shows that there is no clear connection between $d(\underline{\mathcal{C}})$ and $d(\mathcal{C})$ in general.

Example 16: Let $(q,m,r) = (3,4,2)$. Then $n = (q^m-1)/2 = 40$ and $N = 80$. Let β be a primitive element of $\mathrm{GF}(3^4)$ with $\beta^4-\beta^3-1=0$.

1) Let $\mathcal{C}$ be the cyclic code of length N over $\mathrm{GF}(q)$ with generator polynomial $g(x) = \mathbb{M}_\beta(x)$, then $\underline{\mathcal{C}}$ is the negacyclic code of length n over $\mathrm{GF}(q)$ with generator polynomial $\underline{g}(x) = \mathbb{M}_\beta(x)$. Clearly, $\mathrm{Ind}(\mathcal{C}) = \{1\}$. Then $\mathcal{C}$ has parameters $[80, 76, 2]$ and $\underline{\mathcal{C}}$ has parameters $[40, 36, 3]$. It is clear that $d(\mathcal{C}) < d(\underline{\mathcal{C}})$.
2) Let $\mathcal{C}$ be the cyclic code of length N over $\mathrm{GF}(q)$ with generator polynomial $g(x) = (x-1)\mathbb{M}_\beta(x)$, then $\underline{\mathcal{C}}$ is the negacyclic code of length n over $\mathrm{GF}(q)$ with generator polynomial $\underline{g}(x) = \mathbb{M}_\beta(x)$. Clearly, $\mathrm{Ind}(\mathcal{C}) = \{0,1\}$. Then $\mathcal{C}$ has parameters $[80, 75, 3]$ and $\underline{\mathcal{C}}$ has parameters $[40, 36, 3]$. It is clear that $d(\mathcal{C}) = d(\underline{\mathcal{C}})$.
3) Let $\mathcal{C}$ be the cyclic code of length N over $\mathrm{GF}(q)$ with generator polynomial $g(x) = (x^n-1)\mathbb{M}_\beta(x)$, then $\underline{\mathcal{C}}$ is the negacyclic code of length n over $\mathrm{GF}(q)$ with generator polynomial $\underline{g}(x) = \mathbb{M}_\beta(x)$. Clearly, $\mathrm{Ind}(\mathcal{C}) = \{0,1\}$. Then $\mathcal{C}$ has parameters $[80, 36, 6]$ and $\underline{\mathcal{C}}$ has parameters $[40, 36, 3]$. It is clear that $d(\mathcal{C}) = 2d(\underline{\mathcal{C}})$.

Later in this paper, we will use this general construction to obtain two classes of λ-constacyclic codes of length $(q^m-1)/r$ over $\mathrm{GF}(q)$, where $r > 1$ and $r \mid (q-1)$.

IV. The First Class of Constacyclic Codes

We follow the previous notation. Throughout this section, let $r > 1$ and $r \mid (q-1)$. Let $n = (q^m-1)/r$, where m is an integer with $m \geq 2$. Define $N = rn = q^m - 1$. Then it follows from Lemma 4 that $\mathrm{ord}_n(q) = \mathrm{ord}_N(q) = m$. Let $\Gamma_{(q,N)}$ be the set of q-cyclotomic coset leaders modulo N and let

$$\Gamma^{(1)}_{(q,N,r)} = \{i : i \in \Gamma_{(q,N)},\ i \equiv 1 \pmod r\}.$$

Let β be a primitive element of $\mathrm{GF}(q^m)$ and let $\lambda = \beta^{(q^m-1)/r}$. Then $\lambda \in \mathrm{GF}(q)^*$ with $\mathrm{ord}(\lambda) = r$. Let ℓ be a positive integer with $1 \leq \ell \leq m$. Define

$$g'_{(q,m,r,\ell)}(x) = \prod_{\substack{i \in \Gamma^{(1)}_{(q,N,r)} \\ 1 \leq \mathtt{wt}(i) \leq \ell}} \mathbb{M}_{\beta^i}(x).$$

Let

$$D'_{(q,m,r,\ell)} = \bigcup_{\substack{i \in \Gamma^{(1)}_{(q,N,r)} \\ 1 \leq \mathtt{wt}(i) \leq \ell}} C^{(q,N)}_i.$$

Then $\{\beta^i : i \in D'_{(q,m,r,\ell)}\}$ is the set of all zeros of $g'_{(q,m,r,\ell)}(x)$. It is easily verified that $D'_{(q,m,r,\ell)}$ is invariant under the permutation $qy \mod N$ of $\mathbb{Z}_N$. Consequently, $g'_{(q,m,r,\ell)}(x)$ is over $\mathrm{GF}(q)$ and is a divisor of $x^n - \lambda$. Let $\mathcal{C}'(q,m,r,\ell)$ denote the λ-constacyclic code of length n over $\mathrm{GF}(q)$ with generator polynomial $g'_{(q,m,r,\ell)}(x)$. By definition, $g'_{(q,m,r,m)}(x) = x^n - \lambda$ and the code $\mathcal{C}'(q,m,r,m)$ is the zero code and $\mathcal{C}'(q,m,r,m)^\perp$ is the $[n,n,1]$ code $\mathrm{GF}(q)^n$ over $\mathrm{GF}(q)$. Hence, we will consider the code $\mathcal{C}'(q,m,r,\ell)$ only for $1 \leq \ell \leq m-1$, and call $D'_{(q,m,r,\ell)}$ the *defining set* of $\mathcal{C}'(q,m,r,\ell)$ with respect to the primitive element β of $\mathrm{GF}(q^m)$.

To settle the dimension of this code $\mathcal{C}'(q,m,r,\ell)$, we need the following lemma.

Lemma 17: Let t be a positive integer and let q be a prime power. Then the number of solutions $(x_1, x_2, \ldots, x_t)$ with $1 \leq x_i \leq q-1$ to the equation $x_1 + x_2 + \cdots + x_t \equiv 1 \pmod r$ is equal to $\frac{(q-1)^t}{r}$.

Proof: For any $(x_1, x_2, \ldots, x_{t-1})$ with $1 \leq x_i \leq q-1$, let $a = x_1 + x_2 + \cdots + x_{t-1}$, then the equation $x_1 + x_2 + \cdots + x_t \equiv 1 \pmod r$ is equivalent to $x_t \equiv 1 - a \pmod r$. For any a, the number of solutions x_t with $1 \leq x_t \leq q-1$ to the equation $x_t \equiv 1 - a \pmod r$ is equal to $(q-1)/r$. The desired conclusion follows. ∎

Theorem 18: Let $1 \leq \ell \leq m-1$. Then

$$\dim(\mathcal{C}'(q,m,r,\ell)) = \frac{q^m - \sum_{i=0}^{\ell} \binom{m}{i}(q-1)^i}{r}$$

and

$$d(\mathcal{C}'(q,m,r,\ell)) \geq \left\lfloor \frac{q^{\ell+1} - 1 - 2(q-1)}{r(q-1)} \right\rfloor + 2. \tag{2}$$

Proof: Let i be an integer with $1 \leq i \leq q^m - 2$. Let the q-adic expression of i be

$$i = \sum_{j=0}^{m-1} i_j q^j, \quad 0 \leq i_j \leq q-1.$$

Then $i \equiv \sum_{j=0}^{m-1} i_j \pmod r$. It then follows from Lemma 17 that the number of i with $1 \leq i \leq q^m - 2$ such that $\mathtt{wt}(i) = t$ and $i \equiv 1 \pmod r$ is $\binom{m}{t}\frac{(q-1)^t}{r}$. Consequently,

$$\deg(g'_{(q,m,r,\ell)}(x)) = \sum_{i=1}^{\ell} \binom{m}{i} \frac{(q-1)^i}{r}.$$

Thus,

$$\begin{aligned}\dim(\mathcal{C}'(q,m,r,\ell)) &= \frac{q^m - 1}{r} - \sum_{i=1}^{\ell} \binom{m}{i} \frac{(q-1)^i}{r} \\ &= \frac{q^m - \sum_{i=0}^{\ell} \binom{m}{i}(q-1)^i}{r}.\end{aligned}$$

We now prove the lower bound on the minimum distance of the code $\mathcal{C}'(q,m,r,\ell)$. It is straightforward to verify that every integer a with $1 \leq a \leq \frac{q^{\ell+1}-1}{q-1} - 1$ has Hamming weight $\mathtt{wt}(a) \leq \ell$. It then follows from the definition of the code $\mathcal{C}'(q,m,r,\ell)$ that β^i is a zero of $\mathcal{C}'(q,m,r,\ell)$ for each i in the set

$$\left\{1 + rj : 0 \leq j \leq \left\lfloor \frac{q^{\ell+1} - 1 - 2(q-1)}{r(q-1)} \right\rfloor \right\}.$$

The desired lower bound then follows from the BCH bound for constacyclic codes (see Lemma 6). ∎

Next we study the dual code of the constacyclic code $\mathcal{C}'(q,m,r,\ell)$. We have the following theorem.

Theorem 19: Let $q \geq 3$, $r > 1$ and $r \mid (q-1)$. Let $1 \leq \ell \leq m-1$. Then

$$\dim(\mathcal{C}'(q,m,r,\ell)^\perp) = \frac{\sum_{i=1}^{\ell} \binom{m}{i}(q-1)^i}{r}$$

and

$$d(\mathcal{C}'(q,m,r,\ell)^\perp) \geq q^{m-\ell}. \tag{3}$$

Proof: The desired dimension of $\mathcal{C}'(q,m,r,\ell)^\perp$ follows from the dimension of $\mathcal{C}'(q,m,r,\ell)$. Note that $(\beta^{-1})^n = \lambda^{-1}$ and β^{-1} is a primitive element of $\mathrm{GF}(q^m)$. By Lemma 3, the dual code $\mathcal{C}'(q,m,r,\ell)^\perp$ is a λ^{-1}-constacyclic code of length $n = (q^m-1)/r$ over $\mathrm{GF}(q)$ with generator polynomial

$$\prod_{\substack{i \in \Gamma^{(1)}_{(q,N,r)} \\ \mathtt{wt}(i) > \ell}} \mathbb{M}_{(\beta^{-1})^i}(x).$$

Let

$$D(q,m,r,\ell) = \{i \in \mathbb{Z}_N : \mathtt{wt}(i) \geq \ell + 1,\ i \equiv 1 \pmod r\},$$

then

$$\bigcup_{\substack{i \in \Gamma^{(1)}_{(q,N,r)} \\ \mathtt{wt}(i) > \ell}} C^{(q,N)}_i = D(q,m,r,\ell).$$

Let

$$B := \left\{1 + rj : \frac{q^m - 1}{r} - q^{m-\ell} + 1 \leq j \leq \frac{q^m - 1}{r} - 1\right\}.$$

It is easily checked that $\mathtt{wt}(i) \geq \ell + 1$ and $i \equiv 1 \pmod r$ for all $i \in B$. Hence, B is a subset of $D(q,m,r,\ell)$. Consequently, $(\beta^{-1})^i$ is a zero of $\mathcal{C}'(q,m,r,\ell)^\perp$ for each $i \in B$. Note that

$$\left(\frac{q^m - 1}{r} - 1\right) - \left(\frac{q^m - 1}{r} - q^{m-\ell} + 1\right) + 1 = q^{m-\ell} - 1.$$

The desired conclusion then follows from the BCH bound for constacyclic codes (see Lemma 6). ∎

An interesting fact about the family of constacyclic codes $\mathcal{C}'(q,m,r,\ell)$ is the following.

Corollary 20: Let $m \geq 2$ and $r = q-1$. Then the constacyclic code $\mathcal{C}'(q,m,r,1)$ over $\mathrm{GF}(q)$ has parameters

$$[(q^m-1)/(q-1), (q^m-1)/(q-1)-m, 3]$$

and is monomially-equivalent to the Hamming code. In addition, $\mathcal{C}'(q,m,r,1)^\perp$ has parameters

$$\left[(q^m-1)/(q-1), m, q^{m-1}\right]$$

and is monomially-equivalent to the Simplex code.

Proof: The desired dimension of the code $\mathcal{C}'(q,m,q-1,1)$ follows from Theorem 18. It follows from Lemma 7 that $d(\mathcal{C}'(q,m,q-1,1)) \leq 4$. It then follows from Lemma 8 that

$$d(\mathcal{C}'(q,m,q-1,1)) \neq 4.$$

Again by Theorem 18, $d(\mathcal{C}'(q,m,q-1,1)) \geq 3$. Consequently, $d(\mathcal{C}'(q,m,q-1,1)) = 3$. Hence, $\mathcal{C}'(q,m,q-1,1)$ has the same parameters as the Hamming code of length $(q^m-1)/(q-1)$ over $\mathrm{GF}(q)$. It is well known that all linear codes over $\mathrm{GF}(q)$ with parameters

$$[(q^m-1)/(q-1), (q^m-1)/(q-1)-m, 3]$$

are unique up to monomial equivalence. Therefore, $\mathcal{C}'(q,m,q-1,1)$ is monomially-equivalent to the Hamming code and $\mathcal{C}'(q,m,q-1,1)^\perp$ is monomially-equivalent to the Simplex code. ∎

Corollary 21: Let $m \geq 2$. Let q be an odd prime power and $r = (q-1)/2$. Then the constacyclic code $\mathcal{C}'(q,m,r,1)$ over $\mathrm{GF}(q)$ has parameters

$$[2(q^m-1)/(q-1), 2(q^m-1)/(q-1)-2m, 4]$$

and is distance-optimal with respect to the Sphere Packing bound. The dual code $\mathcal{C}'(q,m,r,1)^\perp$ has the following properties:

- When $m \geq 3$ is odd and q is an odd prime, $\mathcal{C}'(q,m,r,1)^\perp$ has parameters

  $$\left[2(q^m-1)/(q-1), 2m, 2q^{m-1}-q^{(m-1)/2}\right],$$

  and the weight distribution of $\mathcal{C}'(q,m,r,1)^\perp$ is given in Table I.
- When $m \geq 2$ is even and q is an odd prime, $\mathcal{C}'(q,m,r,1)^\perp$ has parameters

  $$\left[2(q^m-1)/(q-1), 2m, 2q^{m-1}-(q-1)q^{(m-2)/2}\right],$$

  and the weight distribution of $\mathcal{C}'(q,m,r,1)^\perp$ is given in Table II.

Proof: The desired dimension of the code $\mathcal{C}'(q,m,r,1)$ follows from Theorem 18. It follows from Lemma 7 that $[2(q^m-1)/(q-1), 2(q^m-1)/(q-1)-2m, d \geq 5]$ linear codes over $\mathrm{GF}(q)$ do not exist. Therefore, $d(\mathcal{C}'(q,m,r,1)) \leq 4$. Again by Theorem 18, $d(\mathcal{C}'(q,m,r,1)) \geq 4$. Consequently, $d(\mathcal{C}'(q,m,r,1)) = 4$, and $\mathcal{C}'(q,m,r,1)$ is distance-optimal with respect to the Sphere Packing bound.

TABLE I

WEIGHT DISTRIBUTION OF THE CODE $\mathcal{C}'(q,m,r,1)^\perp$ FOR ODD m

Weight ω	No. of codewords A_ω
0	1
$2q^{m-1}-q^{(m-1)/2}$	$q^{(m-1)/2}(q^{(m-1)/2}+1)(q^m-1)$
$2q^{m-1}$	$(q^m-1)(q^m-2q^{m-1}+1)$
$2q^{m-1}+q^{(m-1)/2}$	$q^{(m-1)/2}(q^{(m-1)/2}-1)(q^m-1)$

TABLE II

WEIGHT DISTRIBUTION OF THE CODE $\mathcal{C}'(q,m,r,1)^\perp$ FOR EVEN m

Weight ω	No. of codewords A_ω
0	1
$2q^{m-1}-(q-1)q^{(m-2)/2}$	$\frac{(q^{(m-2)/2}+1)(q^{m/2}-1)(q^m-1)}{q^2-1}$
$2q^{m-1}-2q^{(m-2)/2}$	$\frac{(q^{m/2}+1)^2(q-1)(q^m-1)}{4(q+1)}$
$2q^{m-1}-q^{(m-2)/2}$	$q^{(m-2)/2}(q^{m/2}+1)(q^m-1)$
$2q^{m-1}$	$\frac{(q^{m+1}-3q^m+q+1)(q^m-1)}{2(q-1)}$
$2q^{m-1}+q^{(m-2)/2}$	$q^{(m-2)/2}(q^{m/2}-1)(q^m-1)$
$2q^{m-1}+2q^{(m-2)/2}$	$\frac{(q^{m/2}-1)^2(q-1)(q^m-1)}{4(q+1)}$
$2q^{m-1}+(q-1)q^{(m-2)/2}$	$\frac{(q^{(m-2)/2}-1)(q^{m/2}+1)(q^m-1)}{q^2-1}$

It is easily checked that the generator polynomial of $\mathcal{C}'(q,m,r,1)$ is $\mathbb{M}_\beta(x)\mathbb{M}_{\beta^{(q+1)/2}}(x)$. By Lemma 5, the code $\mathcal{C}'(q,m,r,1)^\perp$ has the trace representation

$$\mathcal{C}'(q,m,r,1)^\perp = \{\mathbf{c}(a_1,a_2) : a_1,a_2 \in \mathrm{GF}(q^m)\},$$

where

$$\mathbf{c}(a_1,a_2) = (\mathrm{Tr}_{q^m/q}(a_1\beta^i + a_2\beta^{(\frac{q+1}{2})i}))_{i=0}^{n-1}.$$

Define

$$\mathcal{EC}'(q,m,r,1)^\perp = \{\widetilde{\mathbf{c}}(a_1,a_2) : a_1,a_2 \in \mathrm{GF}(q^m)\},$$

where

$$\widetilde{\mathbf{c}}(a_1,a_2) = (\mathrm{Tr}_{q^m/q}(a_1\beta^i + a_2\beta^{(\frac{q+1}{2})i}))_{i=0}^{q^m-2}.$$

It is easily verified that $\mathcal{EC}'(q,m,r,1)^\perp$ is the cyclic code of length q^m-1 over $\mathrm{GF}(q)$ with check polynomial

$$\mathbb{M}_{\beta^{-1}}(x)\mathbb{M}_{\beta^{-(q+1)/2}}(x).$$

For each $(a_1,a_2) \in \mathrm{GF}(q^m)^2$, we have

$$\widetilde{\mathbf{c}}(a_1,a_2) = (\mathbf{c}(a_1,a_2) \| \lambda\cdot\mathbf{c}(a_1,a_2) \| \cdots \| \lambda^{\frac{q-3}{2}}\cdot\mathbf{c}(a_1,a_2)),$$

where $\lambda = \beta^n \in \mathrm{GF}(q)^*$ and $\|$ denotes the concatenation of vectors. It follows that the constacyclic code $\mathcal{C}'(q,m,r,1)^\perp$ has weight distribution $W(z)$ if and only if the cyclic code $\mathcal{EC}'(q,m,r,1)^\perp$ has weight distribution $W(z^{(q-1)/2})$. When q is an odd prime, the weight distribution of $\mathcal{EC}'(q,m,r,1)^\perp$ was determined in [40]. The desired result follows. ∎

Let $n = 2(q^m-1)/(q-1)$, where q is an odd prime power and $m \geq 2$. Any constacyclic code over $\mathrm{GF}(q)$ with parameters $[n, n-2m, 4]$ is optimal with respect to the Sphere Packing bound. Fang et al. constructed constacyclic codes with the same parameters as their counterparts in Corollary 21 using the q-polynomial approach [24]. The contribution of

Corollary 21 is to solve the weight distribution of the dual codes of this class of optimal codes

Example 22: Let $(q,m,r,\ell)=(5,2,2,1)$. Let β be the primitive element of $\mathrm{GF}(5^2)$ with $\beta^2+4\beta+2=0$. Then the constacyclic code $\mathcal{C}'(5,2,2,1)$ over $\mathrm{GF}(5)$ has parameters $[12,8,4]$ and is distance-optimal. The dual code $\mathcal{C}'(5,2,2,1)^\perp$ has parameters $[12,4,6]$ and weight enumerator $1+8z^6+144z^8+144z^9+168z^{10}+96z^{11}+64z^{12}$.

Example 23: Let $(q,m,r,\ell)=(5,3,2,1)$. Let β be the primitive element of $\mathrm{GF}(5^3)$ with $\beta^3+3\beta+3=0$. Then the constacyclic code $\mathcal{C}'(5,3,2,1)$ over $\mathrm{GF}(5)$ has parameters $[62,56,4]$ and is distance-optimal. The dual code $\mathcal{C}'(5,3,2,1)^\perp$ has parameters $[62,6,45]$ and weight enumerator $1+3720z^{45}+9424z^{50}+2480z^{55}$. Moreover, the code $\mathcal{C}'(5,3,2,1)^\perp$ has the best parameters known [27].

Corollary 24: Let $m\geq 2$. Let q be a prime power with $q\equiv 1 \pmod 3$, and let $r=(q-1)/3>1$. Then the constacyclic code $\mathcal{C}'(q,m,r,1)$ over $\mathrm{GF}(q)$ has parameters

$$[3(q^m-1)/(q-1), 3(q^m-1)/(q-1)-3m, 5\leq d\leq 6].$$

Proof: The desired dimension of the code $\mathcal{C}'(q,m,r,1)$ follows from Theorem 18. It follows from Lemma 7 that

$$d(\mathcal{C}'(q,m,r,1))\leq 6.$$

Again by Theorem 18, $d(\mathcal{C}'(q,m,r,1))\geq 5$. The desired result follows. ∎

Let $n=3(q^m-1)/(q-1)$, where $q\equiv 1 \pmod 3$ and $m\geq 2$. By the Sphere Packing bound, an $[n,n-3m,d\geq 7]$ linear code over $\mathrm{GF}(q)$ does not exist. Therefore, the constacyclic code constructed by Corollary 24 is optimal in the sense that the error-correction ability is maximal for the fixed length n and the fixed dimension $n-3m$.

Example 25: Let $(q,m,r,\ell)=(7,2,2,1)$. Let β be the primitive element of $\mathrm{GF}(7^2)$ with $\beta^2+6\beta+3=0$. Then the constacyclic code $\mathcal{C}'(7,2,2,1)$ over $\mathrm{GF}(7)$ has parameters $[24,18,5]$ and has the best parameters known [27].

Let $\Omega(q,m,\ell)$ denote the punctured Dilix code constructed in [19] (see also Section II-K). Theorem 18 tells us that

$$\dim(\Omega(q,m,r,\ell))=r\cdot\dim(\mathcal{C}'(q,m,r,\ell)).$$

Experimental data indicates that the lower bound in (2) is good in general. But the following problem is worth of investigation.

Open Problem 26: Determine the minimum distance of $\mathcal{C}'(q,m,r,\ell)$ or improve the lower bound in (2) for $2\leq\ell\leq m-1$.

Experimental data shows that the lower bound in (3) is quite away from the true minimum distance.

Open Problem 27: Determine the minimum distance of $\mathcal{C}'(q,m,r,\ell)^\perp$ or improve the lower bound in (3) for $2\leq\ell\leq m-1$.

Example 28: Let $(q,m,r,\ell)=(3,4,2,1)$. Let β be the primitive element of $\mathrm{GF}(3^4)$ with $\beta^4+2\beta^3+2=0$. Then the constacyclic code $\mathcal{C}'(3,4,2,1)$ over $\mathrm{GF}(3)$ has parameters $[40,36,3]$ and $\mathcal{C}'(3,4,2,1)^\perp$ has parameters $[40,4,27]$. The former is a perfect code and the latter meets the Griesmer bound.

Example 29: Let $(q,m,r,\ell)=(3,4,2,2)$. Let β be the primitive element of $\mathrm{GF}(3^4)$ with $\beta^4+2\beta^3+2=0$. Then the constacyclic code $\mathcal{C}'(3,4,2,2)$ over $\mathrm{GF}(3)$ has parameters $[40,24,8]$ and $\mathcal{C}'(3,4,2,2)^\perp$ has parameters $[40,16,12]$. The best ternary code known of length 40 and dimension 24 has minimum distance 9 [27].

Example 30: Let $(q,m,r,\ell)=(3,4,2,3)$. Let β be the primitive element of $\mathrm{GF}(3^4)$ with $\beta^4+2\beta^3+2=0$. Then the constacyclic code $\mathcal{C}'(3,4,2,3)$ over $\mathrm{GF}(3)$ has parameters $[40,8,21]$ and has the best parameters known [27], and $\mathcal{C}'(3,4,2,3)^\perp$ has parameters $[40,32,4]$.

Example 31: Let $(q,m,r,\ell)=(4,3,3,2)$. Let β be the primitive element of $\mathrm{GF}(4^3)$ with $\beta^6+\beta^4+\beta^3+\beta+1=0$. Then the constacyclic code $\mathcal{C}'(4,3,3,2)$ over $\mathrm{GF}(4)$ has parameters $[21,9,8]$ and $\mathcal{C}'(4,3,3,2)^\perp$ has parameters $[21,12,6]$.

The forgoing examples demonstrate that the constacyclic code $\mathcal{C}'(q,m,r,\ell)$ over $\mathrm{GF}(q)$ and its dual $\mathcal{C}'(q,m,r,\ell)^\perp$ may be optimal or have the best parameters known sometimes. Below we explain some connection and difference among the code $\mathcal{C}'(q,m,q-1,\ell)$, the projective Reed-Muller codes and the nonprimitive generalized Reed-Muller codes.

By Corollary 20, $\mathcal{C}'(q,m,q-1,1)^\perp$ is monomially-equivalent to $\mathrm{PRM}(q,m,1)$, as both codes are monomially-equivalent to the Simplex code. This is one connection between the codes $\mathcal{C}'(q,m,q-1,\ell)$ and the projective Reed-Muller codes. Consider now all the projective codes $\mathrm{PRM}(3,4,\ell)$ for all ℓ with $1\leq\ell\leq 6$. It follows from Theorem 9 that

$$\begin{aligned}
d(\mathrm{PRM}(3,4,1)) &= 27,\\
d(\mathrm{PRM}(3,4,2)) &= 18,\\
d(\mathrm{PRM}(3,4,3)) &= 9,\\
d(\mathrm{PRM}(3,4,4)) &= 6,\\
d(\mathrm{PRM}(3,4,5)) &= 3,\\
d(\mathrm{PRM}(3,4,6)) &= 2.
\end{aligned}$$

By Example 29, $d(\mathcal{C}'(3,4,2,2))=8$ and $d(\mathcal{C}'(3,4,2,2)^\perp)=12$. This means that both $\mathcal{C}'(3,4,2,2)$ and $\mathcal{C}'(3,4,2,2)^\perp$ cannot be monomially-equivalent to a code $\mathrm{PRM}(3,4,\ell)$ for all ℓ with $1\leq\ell\leq 6$. Hence, the two families of codes $\mathcal{C}'(q,m,q-1,\ell)$ and $\mathrm{PRM}(q,m,\ell)$ are different in general. Notice that $\mathcal{C}'(q,m,q-1,\ell)$ and the punctured Dilix code $\Omega(q,m,\ell)$ are not monomially-equivalent when $q>2$, as they have different lengths.

Compared with parameters of the codes $\mathrm{NGRM}(3,4,2,\ell)$ in Example 13, both $\mathcal{C}'(3,4,2,2)$ and $\mathcal{C}'(3,4,2,2)^\perp$ cannot be monomially-equivalent to a code $\mathrm{NGRM}(3,4,2,\ell)$ for all ℓ with $0\leq\ell\leq 3$. Hence, the class of codes $\mathcal{C}'(q,m,q-1,\ell)$ and the class of codes $\mathrm{NGRM}(q,m,q-1,\ell)$ are different.

V. The Second Class of Constacyclic Codes

We follow the previous notation. Throughout this section, let $r>1$ and $r\mid(q-1)$. Let $n=(q^m-1)/r$, where m is an integer with $m\geq 2$. Define $N=rn=q^m-1$, then it follows from Lemma 4 that $\mathrm{ord}_n(q)=\mathrm{ord}_N(q)=m$. Let $\Gamma_{(q,N)}$ be the set of q-cyclotomic coset leaders modulo N and let

$$\Gamma^{(1)}_{(q,N,r)}=\{i: i\in\Gamma_{(q,N)},\ i\equiv 1 \pmod r\}.$$

Recall that $r \mid (q-1)$, we have $\mathtt{wt}_q(i) \equiv i \pmod r$. Then $\mathtt{wt}_q(i) \equiv 1 \pmod r$ for $i \in \Gamma^{(1)}_{(q,N,r)}$.

A. Definition and Basic Properties of the Constacyclic Codes

Let β be a primitive element of $\mathrm{GF}(q^m)$ and let $\lambda = \beta^{(q^m-1)/r}$. Then $\lambda \in \mathrm{GF}(q)^*$ with $\mathrm{ord}(\lambda) = r$. Let ℓ be an integer with $0 \le \ell < (q-1)m - 1$. Define

$$g_{(q,m,r,\ell)}(x) = \prod_{\substack{i \in \Gamma^{(1)}_{(q,N,r)} \\ \mathtt{wt}_q(i) < (q-1)m-\ell}} \mathbb{M}_{\beta^i}(x).$$

Let

$$D_{(q,m,r,\ell)} = \bigcup_{\substack{i \in \Gamma^{(1)}_{(q,N,r)} \\ \mathtt{wt}_q(i) < (q-1)m-\ell}} C_i^{(q,N)}.$$

Note that $\mathtt{wt}_q(i) \equiv i \pmod r$. It is easily checked that

$$D_{(q,m,r,\ell)} = \{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) < (q-1)m - \ell,\ \mathtt{wt}_q(i) \equiv 1 \pmod r\}.$$

By definition, $\{\beta^i : i \in D_{(q,m,r,\ell)}\}$ is the set of all zeros of $g_{(q,m,r,\ell)}(x)$. It is easily verified that $D_{(q,m,r,\ell)}$ is invariant under the permutation $qy \bmod N$ of $\mathbb{Z}_N$. Consequently, $g_{(q,m,r,\ell)}(x)$ is over $\mathrm{GF}(q)$ and is a divisor of $x^n - \lambda$. Let $\mathcal{C}(q,m,r,\ell)$ denote the λ-constacyclic code of length n over $\mathrm{GF}(q)$ with generator polynomial $g_{(q,m,r,\ell)}(x)$. We call $D_{(q,m,r,\ell)}$ the *defining set* of $\mathcal{C}(q,m,r,\ell)$ with respect to the primitive element β of $\mathrm{GF}(q^m)$.

Theorem 32: Let $0 \le \ell = r\ell_1 + \ell_0 < m(q-1) - 1$, where $0 \le \ell_0 \le r-1$. If $\ell_1 = 0$ and $0 \le \ell_0 \le r-2$, then $\mathcal{C}(q,m,r,\ell) = \{\mathbf{0}\}$. Otherwise,

$$\mathcal{C}(q,m,r,\ell) = \mathcal{C}(q,m,r,r\ell_2 + r - 1),$$

where

$$\ell_2 = \begin{cases} \ell_1 & \text{if } \ell_0 = r-1, \\ \ell_1 - 1 & \text{if } \ell_0 \ne r-1. \end{cases}$$

Proof: Since $r \mid (q-1)$, we have

$$(q-1)m - \ell \equiv 1 \pmod r$$

if and only if $\ell \equiv r-1 \pmod r$. If $\ell_1 = 0$ and $0 \le \ell_0 \le r-2$, i.e., $0 \le \ell \le r-2$. Then $(q-1)m - \ell \le (q-1)m - r + 2$. In this case, $D_{(q,m,r,\ell)} = \{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) \equiv 1 \pmod r\}$, i.e., $g_{(q,m,r,\ell)}(x) = x^n - \lambda$. Consequently, $\mathcal{C}(q,m,r,\ell) = \{\mathbf{0}\}$. If $\ell \ge r-1$ and $\ell_0 < r-1$, then $\mathtt{wt}_q(i) < (q-1)m - \ell$ with $\mathtt{wt}_q(i) \equiv 1 \pmod r$ if and only if

$$\begin{aligned} \mathtt{wt}_q(i) &\le (q-1)m - (r\ell_1 + r - 1) \\ &< (q-1)m - (r\ell_1 + r - 1) + r \end{aligned}$$

with $\mathtt{wt}_q(i) \equiv 1 \pmod r$. The desired conclusion follows. ∎

It follows from Theorem 32 that the class of λ-constacyclic codes $\mathcal{C}(q,m,r,\ell)$ contains only the following distinct codes

$$\mathcal{C}(q,m,r,r\ell_1 + r - 1),\ 0 \le \ell_1 \le \left(\frac{q-1}{r}\right) m - 2.$$

To determine the dimension of the λ-constacyclic code $\mathcal{C}(q,m,r,\ell)$, we need the following lemma.

Lemma 33 [55]: The number of ways one can place t objects in m cells such that no cell contains more than s objects is

$$N(t,m,s) = \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{t - j(s+1) + m - 1}{t - j(s+1)}.$$

The dimension of the λ-constacyclic code $\mathcal{C}(q,m,r,\ell)$ is documented in the next theorem.

Theorem 34: Let $\ell = r\ell_1 + r - 1$, where $0 \le \ell_1 \le (\frac{q-1}{r})m - 2$. Then

$$\begin{aligned} &\dim(\mathcal{C}(q,m,r,\ell)) \\ &= \sum_{\substack{t \equiv r-1 \pmod r \\ 0 < t \le \ell}} \left(\sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{t - jq + m - 1}{t - jq} \right) \\ &= \sum_{t=0}^{\ell_1} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{tr + r - 1 - jq + m - 1}{tr + r - 1 - jq}. \end{aligned} \tag{4}$$

Proof: Define

$$H(q,m,r,\ell) = \{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) \ge (q-1)m - \ell,\ \mathtt{wt}_q(i) \equiv 1 \pmod r\}.$$

By definition, $\dim(\mathcal{C}(q,m,r,\ell)) = |H(q,m,r,\ell)|$. We now determine $|H(q,m,r,\ell)|$.

For each $i \in \mathbb{Z}_N$, $i \equiv 1 \pmod r$ if and only if $N - i \equiv r-1 \pmod r$. Furthermore, $\mathtt{wt}_q(N-i) = (q-1)m - \mathtt{wt}_q(i)$. Consequently, $\mathtt{wt}_q(i) \ge (q-1)m - \ell$ if and only if

$$\mathtt{wt}_q(N-i) \le \ell.$$

We then deduce that

$$\begin{aligned} &|H(q,m,r,\ell)| \\ &= |\{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) \le \ell,\ \mathtt{wt}_q(i) \equiv r-1 \pmod r\}|. \end{aligned} \tag{5}$$

From Lemma 33, the number of ways of picking t objects from a set of m objects, under the restriction that no objects can be chosen more than $q-1$ times, is equal to

$$N(t,m,q-1) = \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{t - jq + m - 1}{t - jq}.$$

The desired dimension then follows from (5). ∎

The formula in (4) looks complicated. The following theorem documents a upper bound on the dimension of the code $\mathcal{C}(q,m,r,\ell)$.

Theorem 35: Let $\ell = r\ell_1 + r - 1$, where $0 \le \ell_1 \le (\frac{q-1}{r})m - 2$. Let $\ell_2 = \lceil \frac{\ell+1}{q-1} \rceil$. Then

$$\dim(\mathcal{C}(q,m,r,\ell)) \le \frac{q^m - \sum_{t=0}^{m-\ell_2} \binom{m}{t} (q-1)^t}{r}.$$

Proof: Recall

$$D_{(q,m,r,\ell)} = \{i \in \mathbb{Z}_N : 1 \le \mathtt{wt}_q(i) < (q-1)m - \ell,\ i \equiv 1 \pmod r\}.$$

Note that $(q-1)m-\ell=(q-1)m-r\ell_1-r+1$. Then by definition,

$$\begin{aligned}
&D_{(q,m,r,\ell)}\\
=&\{i\in\mathbb{Z}_N: 1\le \mathtt{wt}_q(i)\le (q-1)m-r\ell_1-2r+1,\\
&\quad i\equiv 1 \pmod r\}\\
\supseteq&\{i\in\mathbb{Z}_N: 1\le \mathtt{wt}_q(i)\le (q-1)(m-\ell_2),\ i\equiv 1 \pmod r\}\\
\supseteq&\{i\in\mathbb{Z}_N: 1\le \mathtt{wt}(i)\le m-\ell_2,\ i\equiv 1 \pmod r\}.
\end{aligned}$$

It then follows from Lemma 17 that

$$\begin{aligned}
&|D_{(q,m,r,\ell)}|\\
\ge&|\{i\in\mathbb{Z}_N: 1\le \mathtt{wt}(i)\le m-\ell_2,\ i\equiv 1 \pmod r\}|\\
=&\sum_{t=1}^{m-\ell_2}\binom{m}{t}|\{(x_1,x_2,\ldots,x_t)\in\{1,2,\cdots,q-1\}^t:\\
&\qquad x_1+x_2+\cdots+x_t\equiv 1 \pmod r\}|\\
=&\sum_{t=1}^{m-\ell_2}\binom{m}{t}\frac{(q-1)^t}{r}.
\end{aligned}$$

Consequently,

$$\begin{aligned}
\dim(\mathcal{C}(q,m,r,\ell)) &= \frac{q^m-1}{r}-|D_{(q,m,r,\ell)}|\\
&\le \frac{q^m-\sum_{t=0}^{m-\ell_2}\binom{m}{t}(q-1)^t}{r}.
\end{aligned}$$

The desired conclusion follows. ∎

In order to determine the minimum distance of the λ-constacyclic code $\mathcal{C}(q,m,r,\ell)$, we will give another form of this code.

Let β be a primitive element of $\mathrm{GF}(q^m)$ and let

$$\mathbb{M}_\beta(x)=\sum_{i=0}^{m-1}\epsilon_i x^i+x^m,$$

where $\epsilon_i\in\mathrm{GF}(q)$. Since $\mathbb{M}_\beta(x)$ is the minimal polynomial of β over $\mathrm{GF}(q)$, $\epsilon_0\neq 0$. Let

$$\mathbf{M}=\begin{pmatrix}
0 & 1 & 0 & \cdots & 0\\
0 & 0 & 1 & \cdots & 0\\
\vdots & \vdots & \vdots & \ddots & \vdots\\
0 & 0 & 0 & \cdots & 1\\
-\epsilon_0 & -\epsilon_1 & -\epsilon_2 & \cdots & -\epsilon_{m-1}
\end{pmatrix}$$

be the companion matrix of $\mathbb{M}_\beta(x)$. Note that $n=(q^m-1)/r$ and $\beta^n=\lambda$, then $\mathbf{M}^n=\lambda\mathbf{E}$, where $\mathbf{E}$ is the identity matrix of order m. Furthermore,

$$\mathrm{GF}(q)^m=\{\mathbf{0}\}\cup\{\mathbf{e}\mathbf{M}^i: 0\le i\le q^m-2\},\tag{6}$$

where $\mathbf{0}=(0,0,\ldots,0)$ and $\mathbf{e}=(1,0,\ldots,0)$. It is clear that $\{1,\beta,\cdots,\beta^{m-1}\}$ is a basis for $\mathrm{GF}(q^m)$ as a vector space over $\mathrm{GF}(q)$. Let $\overline{\beta}=(1,\beta,\ldots,\beta^{m-1})$, then

$$\begin{aligned}
\mathbf{M}\overline{\beta}^T&=(\beta,\beta^2,\ldots,\beta^{m-1},-\sum_{j=0}^{m-1}\epsilon_j\beta^j)^T\\
&=(\beta,\beta^2,\ldots,\beta^{m-1},\beta^m)^T\\
&=\beta\cdot\overline{\beta}^T.
\end{aligned}$$

It follows that $\mathbf{M}^i\overline{\beta}^T=\beta^i\cdot\overline{\beta}^T$ for $0\le i\le q^m-2$. Therefore, $\beta^i=(\mathbf{e}\mathbf{M}^i,\overline{\beta})$ for $0\le i\le q^m-2$, where $(\cdot,\cdot)$ denotes the inner product of two vectors. It follows that the mapping $\mathbf{0}\mapsto 0$, $\mathbf{e}\mathbf{M}^i\mapsto\beta^i=(\mathbf{e}\mathbf{M}^i,\overline{\beta})$ is an isomorphism between the vector space structures of $\mathrm{GF}(q)^m$ and $\mathrm{GF}(q^m)$. Let

$$r-1\le\ell<(q-1)m-1$$

with $\ell\equiv r-1 \pmod r$, and let $M(q,m,r,\ell)$ be the linear subspace of $\mathrm{GF}(q)[x_1,x_2,\ldots,x_m]$, which is spanned by all monomials $x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}$ satisfying the following three conditions:

1) $0\le i_j\le q-1$ for $1\le j\le m$,
2) $\sum_{j=1}^m i_j\equiv r-1 \pmod r$,
3) $\sum_{j=1}^m i_j\le\ell$.

Define

$$\begin{aligned}
\mathcal{GC}(q,m,r,\ell)=\{&\mathbf{c}_f=(f(\mathbf{e}),f(\mathbf{e}\mathbf{M}),\ldots,f(\mathbf{e}\mathbf{M}^{n-1})):\\
&f(x_1,x_2,\ldots,x_m)\in M(q,m,r,\ell)\}.
\end{aligned}$$

Below we will prove that $\mathcal{GC}(q,m,r,\ell)=\mathcal{C}(q,m,r,\ell)$. For this purpose, we need the following two lemmas.

Lemma 36 [18]: Let

$$f(x_1,x_2,\ldots,x_m)\in\mathrm{GF}(q)[x_1,x_2,\ldots,x_m],$$

then we have the following:

1) If $f(\mathbf{P})=0$ for all $\mathbf{P}\in\mathrm{GF}(q)^m$, then $f\equiv 0$.
2) If $\deg(f)<(q-1)m$, then $\sum_{\mathbf{P}\in\mathrm{GF}(q)^m}f(\mathbf{P})=0$.

Lemma 37: Let $f(x_1,x_2,\ldots,x_m)\in M(q,m,r,\ell)$, then the following hold:

1) Let $0\le i\le n-1$ and $0\le j\le r-1$, then

$$f(\mathbf{e}\mathbf{M}^{jn+i})=\lambda^{-j}\cdot f(\mathbf{e}\mathbf{M}^i).$$

2) If $f(\mathbf{e}\mathbf{M}^i)=0$ for all $0\le i\le n-1$, then $f\equiv 0$.

Proof: 1) Suppose

$$f(x_1,x_2,\ldots,x_m)=\sum c_{i_1,i_2,\cdots,i_m}x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}.$$

It follows from $\mathbf{M}^n=\lambda\mathbf{E}$ that $\mathbf{e}\mathbf{M}^{jn+i}=\lambda^j\mathbf{e}\mathbf{M}^i$. Note that $\sum_{k=1}^m i_k\equiv r-1 \pmod r$ and $\mathrm{ord}(\lambda)=r$, then

$$(\lambda^j)^{i_1+i_2+\cdots+i_m}=\lambda^{-j}.$$

Consequently,

$$f(\mathbf{e}\mathbf{M}^{jn+i})=f(\lambda^j\mathbf{e}\mathbf{M}^i)=\lambda^{-j}\cdot f(\mathbf{e}\mathbf{M}^i).$$

2) Let $\mathbf{P}\in\mathrm{GF}(q)^m\backslash\{\mathbf{0}\}$, it follows from (6) that there are $0\le i\le n-1$ and $0\le j\le r-1$ such that $\mathbf{P}=\mathbf{e}\mathbf{M}^{jn+i}$. Then $f(\mathbf{P})=\lambda^{-j}\cdot f(\mathbf{e}\mathbf{M}^i)=0$. Note that $f(\mathbf{0})=0$. Therefore, $f(\mathbf{P})=0$ for all $\mathbf{P}\in\mathrm{GF}(q)^m$. By the first conclusion of Lemma 36, we have $f\equiv 0$. The desired conclusion follows. ∎

Theorem 38: Let $q>2$ be a prime power and $m\ge 2$ be an integer. Let $r>1$ with $r\mid(q-1)$, and let $r-1\le\ell<(q-1)m-1$ with $\ell\equiv r-1 \pmod r$. Then $\mathcal{GC}(q,m,r,\ell)=\mathcal{C}(q,m,r,\ell)$.

Proof: Firstly, we prove that $\mathcal{GC}(q,m,r,\ell)$ is a λ-constacyclic code of length n over $\mathrm{GF}(q)$. For any

$$f(\mathbf{x})\in M(q,m,r,\ell),$$

let $g(\mathbf{x}) = \lambda \cdot f(\mathbf{x}\mathbf{M}^{n-1})$. It is easily verified that

$$g(\mathbf{x}) \in M(q, m, r, \ell).$$

By Lemma 37,

$$\begin{aligned} g(\mathbf{e}\mathbf{M}^i) &= \lambda \cdot f(\mathbf{e}\mathbf{M}^{n+i-1}) \\ &= \lambda \cdot \lambda^{-1} \cdot f(\mathbf{e}\mathbf{M}^{i-1}) \\ &= f(\mathbf{e}\mathbf{M}^{i-1}) \end{aligned}$$

for $1 \le i \le n-1$. Therefore,

$$\mathbf{c}_g = (\lambda \cdot f(\mathbf{e}\mathbf{M}^{n-1}), f(\mathbf{e}), \ldots, f(\mathbf{e}\mathbf{M}^{n-2})) \in \mathcal{GC}(q, m, r, \ell).$$

It follows that $\mathcal{GC}(q, m, r, \ell)$ is a λ-constacyclic code of length n over $\mathrm{GF}(q)$.

Secondly, we prove that

$$\dim(\mathcal{GC}(q, m, r, \ell)) = \dim(\mathcal{C}(q, m, r, \ell)).$$

By the second conclusion of Lemma 37, the evaluations of all monomials

$$\left\{ x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} : \sum_{k=1}^{m} i_k \equiv r-1 \pmod r, \quad 0 \le i_k \le q-1, \ \sum_{k=1}^{m} i_k \le \ell \right\}$$

give linearly independent codewords. It follows that

$$\begin{aligned} &\dim(\mathcal{GC}(q, m, r, \ell)) \\ =&|\{(i_1, i_2, \ldots, i_m) \in \{0, 1, \cdots, q-1\}^m : \\ &\sum_{k=1}^{m} i_k \equiv r-1 \pmod r, \ \sum_{k=1}^{m} i_k \le \ell\}| \\ =&|\{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) \equiv r-1 \pmod r, \ \mathtt{wt}_q(i) \le \ell\}|. \end{aligned}$$

The desired dimension then follows from Theorem 34.

Finally, we prove that $\mathcal{GC}(q, m, r, \ell) \subseteq \mathcal{C}(q, m, r, \ell)$. Let $g(x)$ be the generator polynomial of $\mathcal{GC}(q, m, r, \ell)$. Then we only need to prove $g_{(q,m,r,\ell)}(x) \mid g(x)$. Suppose that $i = \sum_{l=0}^{m-1} i_l q^l$, $\mathtt{wt}_q(i) < (q-1)m - \ell$ and $\mathtt{wt}_q(i) \equiv 1 \pmod r$. For any $f(x_1, x_2, \ldots, x_m) \in M(q, m, r, \ell)$, let

$$c_f(x) = \sum_{j=0}^{n-1} f(\mathbf{e}\mathbf{M}^j) x^j$$

be the polynomial corresponding to the codeword

$$\mathbf{c}_f \in \mathcal{GC}(q, m, r, \ell).$$

For each $1 \le t \le r-1$, by Lemma 37,

$$\begin{aligned} \sum_{j=0}^{n-1} f(\mathbf{e}\mathbf{M}^{tn+j})(\beta^i)^{tn+j} &= \sum_{j=0}^{n-1} f(\mathbf{e}\mathbf{M}^j)\lambda^{-t}(\beta^i)^{tn+j} \\ &= \sum_{j=0}^{n-1} f(\mathbf{e}\mathbf{M}^j)(\beta^i)^j \\ &= c_f(\beta^i). \end{aligned}$$

Then we have

$$\begin{aligned} c_f(\beta^i) &= \sum_{j=0}^{n-1} f(\mathbf{e}\mathbf{M}^j)(\beta^i)^j \\ &= \frac{1}{r} \sum_{j=0}^{rn-1} f(\mathbf{e}\mathbf{M}^j)(\beta^i)^j \\ &= \frac{1}{r} \sum_{j=0}^{q^m-2} f(\mathbf{e}\mathbf{M}^j)(\beta^j)^i \\ &= \frac{1}{r} \sum_{j=0}^{q^m-2} f(\mathbf{e}\mathbf{M}^j)[(\mathbf{e}\mathbf{M}^j, \overline{\beta})]^i \\ &= \frac{1}{r} \sum_{j=0}^{q^m-2} f(\mathbf{e}\mathbf{M}^j)[(\mathbf{e}\mathbf{M}^j, \overline{\beta})]^{\sum_{l=0}^{m-1} i_l q^l} \\ &= \frac{1}{r} \sum_{j=0}^{q^m-2} f(\mathbf{e}\mathbf{M}^j) \prod_{l=0}^{m-1} [(\mathbf{e}\mathbf{M}^j, \overline{\beta})^{q^l}]^{i_l}. \end{aligned}$$

For $\overline{e}M^j = (x_1, x_2, \ldots, x_m) \in \mathrm{GF}(q)^m$,

$$\begin{aligned} h(\mathbf{e}\mathbf{M}^j) :&= \prod_{l=0}^{m-1} [(\mathbf{e}\mathbf{M}^j, \overline{\beta})^{q^l}]^{i_l} \\ &= \prod_{l=0}^{m-1} [x_1 + x_2\beta^{q^l} + \cdots + x_m\beta^{(m-1)q^l}]^{i_l} \end{aligned}$$

is a homogenous polynomial of degree $\mathtt{wt}_q(i)$ in indeterminates x_j. It is clear that

$$\deg(fh) < \ell + (q-1)m - \ell = (q-1)m$$

and $f(\mathbf{0})h(\mathbf{0}) = 0$. It follows from Lemma 36 that

$$\begin{aligned} &\sum_{j=0}^{q^m-2} f(\mathbf{e}\mathbf{M}^j) \prod_{l=0}^{m-1} [(\mathbf{e}\mathbf{M}^j, \overline{\beta})^{q^l}]^{i_l} \\ &= \sum_{\mathbf{P} \in \mathrm{GF}(q)^m} f(\mathbf{P}) \prod_{l=0}^{m-1} [(\mathbf{P}, \overline{\beta})^{q^l}]^{i_l} \\ &= 0. \end{aligned}$$

Therefore, β^i is a root of $g(x)$. It follows that $g_{(q,m,r,\ell)}(x)$ divides $g(x)$. This completes the proof. ∎

It is hard to settle the minimum distance of the constacyclic code $\mathcal{C}(q, m, r, \ell)$. Below we develop some bounds on $d(\mathcal{C}(q, m, r, \ell))$.

Theorem 39: Let $\ell = (q-1)\ell_1 + \ell_0 < (q-1)m - 1$, where $0 \le \ell_0 \le q-2$ and $\ell_0 \equiv r-1 \pmod r$. Then

$$\frac{(q-\ell_0)q^{m-\ell_1-1} - 2}{r} + 1 \le d(\mathcal{C}(q, m, r, \ell)) \le \frac{(q-\ell_0+r-2)q^{m-\ell_1-1}}{r}. \quad (7)$$

Proof: By definition, we have

$$(q-1)m - \ell = (q-1)(m-\ell_1-1) + q - 1 - \ell_0.$$

Let H be the smallest integer with $\mathtt{wt}_q(H) = (q-1)m - \ell$. Then

$$\begin{aligned} H &= (q-1-\ell_0)q^{m-\ell_1-1} + \sum_{i=0}^{m-\ell_1-2} (q-1)q^i \\ &= (q-\ell_0)q^{m-\ell_1-1} - 1. \end{aligned}$$

It is easily verified that every integer u with $0 < u < H$ satisfies $\mathtt{wt}_q(u) < (q-1)m - \ell$. Define

$$B = \left\{ 1 + rj : 0 \le j \le \frac{(q-\ell_0)q^{m-\ell_1-1} - 2}{r} - 1 \right\}.$$

Then B is a subset of $\{1, 2, \cdots, H-r\}$ and β^i is a zero of $\mathcal{C}(q, m, r, \ell)$ for each $i \in B$. The desired lower bound then follows from Lemma 6.

Let

$$\mathcal{D}(q, m, r, \ell) = \{\widetilde{\mathbf{c}}_f = (f(\mathbf{eM}^i))_{i=0}^{rn-1} : f(x_1, x_2, \ldots, x_m) \in M(q, m, r, \ell)\}.$$

For any $f(x_1, x_2, \ldots, x_m) \in M(q, m, r, \ell)$, it follows from Lemma 37 that

$$\widetilde{\mathbf{c}}_f = (\mathbf{c}_f \parallel \lambda^{-1}\mathbf{c}_f \parallel \cdots \parallel \lambda^{-(r-1)}\mathbf{c}_f),$$

where $\mathbf{c}_f = (f(\mathbf{eM}^i))_{i=0}^{n-1}$ and $\parallel$ denotes the concatenation of vectors. By Theorem 38, we have

$$d(\mathcal{C}(q, m, r, \ell)) = \frac{1}{r} \cdot d(\mathcal{D}(q, m, r, \ell)).$$

Let

$$f(x_1, \ldots, x_m) = \prod_{i=1}^{\ell_1} [1 - x_i^{(q-1)}] \cdot x_{\ell_1+1}^{r-1} \cdot \prod_{i=1}^{\frac{\ell_0-r+1}{r}} [x_{\ell_1+1}^r - \omega^{ri}],$$

where ω is a primitive element of $\mathrm{GF}(q)$. It is easily verified that $\deg(f) = (q-1)\ell_1 + \ell_0$ and $f \in M(q, m, r, \ell)$. Clearly, $f(x_1, x_2, \ldots, x_m)$ is zero in $\mathrm{GF}(q)^m$ unless

$$x_i = 0 \text{ for } i = 1, 2, \cdots, \ell_1,$$
$$x_{\ell_1+1} \notin \{0\} \cup \left\{ \lambda^j \omega^i : 1 \le i \le \frac{\ell_0 - r + 1}{r},\ 0 \le j \le r-1 \right\}. \tag{8}$$

For any $1 \le i, i' \le \frac{\ell_0-r+1}{r}$, $0 \le j, j' \le r-1$, if $\lambda^{j'}\omega^{i'} = \lambda^j\omega^i$, then $\omega^{i-i'} = \lambda^{j'-j}$. It follows that $\omega^{r(i-i')} = 1$. Then we have $(q-1)/r$ divides $i - i'$. Note that

$$0 \le |i - i'| \le \frac{\ell_0 - 2r + 1}{r} < \frac{q-1}{r}.$$

Therefore, $i = i'$. Consequently, $j = j'$. That is to say, there are $[q - r(\frac{\ell_0-r+1}{r}) - 1]q^{m-1-\ell_1}$ vectors in $\mathrm{GF}(q)^m \backslash \{\mathbf{0}\}$ satisfying both equations in (8) and

$$\mathtt{wt}(\mathbf{c}_f) = (q - \ell_0 + r - 2)q^{m-1-\ell_1}.$$

It follows that

$$d(\mathcal{D}(q, m, r, \ell)) \le (q - \ell_0 + r - 2)q^{m-1-\ell_1}.$$

The desired upper bound follows. ∎

If $r = 2$ or $\ell_1 = m-1$, it is easily verified that the upper and lower bounds in (7) are equal. Therefore, we have following two conclusions.

Corollary 40: Let $\ell = (q-1)(m-1) + \ell_0$, where $m \ge 2$, $0 \le \ell_0 \le q-2$ and $\ell_0 \equiv r-1 \pmod r$. Then

$$d(\mathcal{C}(q, m, r, \ell)) = \frac{q - \ell_0 + r - 2}{r}.$$

Corollary 41: Let q be an odd prime power and $r = 2$. Let $r - 1 \le \ell = (q-1)\ell_1 + \ell_0 < (q-1)m - 1$, where $m \ge 2$, $0 \le \ell_0 \le q-2$ and $\ell_0 \equiv r-1 \pmod r$. Then

$$d(\mathcal{C}(q, m, r, \ell)) = \left(\frac{q - \ell_0}{2}\right) q^{m-1-\ell_1}.$$

Example 42: Let $(q, m, r, \ell) = (3, 3, 2, 3)$. Let β be the primitive element of $\mathrm{GF}(3^3)$ with $\beta^3 + 2\beta + 1 = 0$. Then the constacyclic code $\mathcal{C}(3, 3, 2, 3)$ over $\mathrm{GF}(3)$ has parameters $[13, 10, 3]$ and is distance-optimal.

Example 43: Let $(q, m, r, \ell) = (5, 2, 2, 3)$. Let β be the primitive element of $\mathrm{GF}(5^2)$ with $\beta^2 + 4\beta + 2 = 0$. Then the constacyclic code $\mathcal{C}(5, 2, 2, 3)$ over $\mathrm{GF}(5)$ has parameters $[12, 6, 5]$. Furthermore, $\mathcal{C}(5, 2, 2, 3)$ is self-dual and almost-distance optimal.

For ℓ with $r - 1 \le \ell \le (q-1)(m-1) - 1$ and $\ell \equiv r - 1 \pmod r$, we will give an improved bound on the minimum distance of the code $\mathcal{C}(q, m, r, \ell)$. To this end, we consider the subcode of the λ-constacyclic code $\mathcal{C}(q, m, r, \ell)$. Let $\widetilde{M}(q, m, r, \ell)$ be the linear subspace of $\mathrm{GF}(q)[x_1, x_2, \ldots, x_m]$, which is spanned by all monomials $x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}$ satisfying the following three conditions:

1) $0 \le i_j \le q-1$ for $1 \le j \le m$,
2) $\sum_{j=1}^m i_j \equiv \ell \pmod{q-1}$,
3) $\sum_{j=1}^m i_j \le \ell$.

It is easily verified that $\widetilde{M}(q, m, r, \ell) \subseteq M(q, m, r, \ell)$. In the special case $r = q-1$, $\widetilde{M}(q, m, r, \ell) = M(q, m, r, \ell)$. Associated with the λ-constacyclic code $\mathcal{C}(q, m, r, \ell)$ are the following two codes over $\mathrm{GF}(q)$:

$$\widetilde{\mathcal{C}}(q, m, r, \ell) = \{\widetilde{\mathbf{c}}_f = (f(\mathbf{e}), f(\mathbf{eM}), \ldots, f(\mathbf{eM}^{n-1})) : f(x_1, x_2, \ldots, x_m) \in \widetilde{M}(q, m, r, \ell)\},$$

and

$$\mathrm{P}(\widetilde{\mathcal{C}}(q, m, r, \ell)) = \{\overline{\mathbf{c}}_f = (f(\mathbf{e}), f(\mathbf{eM}), \ldots, f(\mathbf{eM}^{\overline{n}-1})) : f(x_1, x_2, \ldots, x_m) \in \widetilde{M}(q, m, r, \ell)\},$$

where $\overline{n} = (q^m - 1)/(q-1)$. In the special case $r = q-1$, $\mathcal{C}(q, m, r, \ell)$, $\widetilde{\mathcal{C}}(q, m, r, \ell)$ and $\mathrm{P}(\widetilde{\mathcal{C}}(q, m, r, \ell))$ are identical.

Theorem 44: Let $q > 2$ be a prime power and $m \ge 2$ be an integer. Let $r > 1$ with $r \mid (q-1)$, and let $r - 1 \le \ell \le (q-1)(m-1) - 1$ with $\ell \equiv r-1 \pmod r$. Then the following hold:

1) The linear code $\widetilde{\mathcal{C}}(q, m, r, \ell)$ is a λ-constacyclic code of length $(q^m - 1)/r$ over $\mathrm{GF}(q)$.
2) The λ-constacyclic code $\widetilde{\mathcal{C}}(q, m, r, \ell) \subseteq \mathcal{C}(q, m, r, \ell)$. In the special case $r = q-1$, $\widetilde{\mathcal{C}}(q, m, r, \ell) = \mathcal{C}(q, m, r, \ell)$.
3) If $r = q-1$, the λ-constacyclic code

$$\widetilde{\mathcal{C}}(q, m, r, \ell) = \mathrm{P}(\widetilde{\mathcal{C}}(q, m, r, \ell)).$$

If $r < q-1$, the λ-constacyclic code

$$\widetilde{\mathcal{C}}(q, m, r, \ell) = \{(\overline{\mathbf{c}}_f \| \omega^\ell \cdot \overline{\mathbf{c}}_f \| \cdots \| \omega^{(\frac{q-1}{r}-1)\ell} \cdot \overline{\mathbf{c}}_f) : \overline{\mathbf{c}}_f \in \mathrm{P}(\widetilde{\mathcal{C}}(q, m, r, \ell))\},$$

where $\omega = \beta^{\overline{n}}$ is a primitive element of $\mathrm{GF}(q)$.

Proof: 1) The proof is similar to Theorem 38, and the details are omitted here.

2) Note that $\widetilde{M}(q,m,r,\ell) \subseteq M(q,m,r,\ell)$ and

$$\widetilde{M}(q,m,r,\ell) = M(q,m,r,\ell)$$

for $r = q-1$. The desired result follows.

3) If $r = q-1$, the desired result is obvious. If $r < q-1$, since β is a primitive element of $\mathrm{GF}(q^m)$, $\omega := \beta^{\overline{n}}$ is a primitive element of $\mathrm{GF}(q)$. Therefore, $\mathbf{M}^{\overline{n}} = \omega\mathbf{E}$. It follows that $\mathbf{e}\mathbf{M}^{j\overline{n}+i} = \omega^j \mathbf{e}\mathbf{M}^i$ for any $0 \le j \le \frac{q-1}{r} - 1$, $0 \le i \le \overline{n}-1$. Let $f(x_1,x_2,\ldots,x_m) \in \widetilde{M}(q,m,r,\ell)$, then

$$f(\mathbf{e}\mathbf{M}^{j\overline{n}+i}) = f(\omega^j \mathbf{e}\mathbf{M}^i) = \omega^{j\ell} \cdot f(\mathbf{e}\mathbf{M}^i).$$

Let

$$\widetilde{\mathbf{c}}_f = (f(\mathbf{e}), f(\mathbf{e}\mathbf{M}), \ldots, f(\mathbf{e}\mathbf{M}^{n-1}))$$

be the codeword corresponding to the polynomial

$$f(x_1,x_2,\ldots,x_m).$$

Then

$$\widetilde{\mathbf{c}}_f = (\overline{\mathbf{c}}_f \| \omega^{\ell} \cdot \overline{\mathbf{c}}_f \| \cdots \| \omega^{(\frac{q-1}{r}-1)\ell} \cdot \overline{\mathbf{c}}_f).$$

The third desired result follows. ∎

Below we will prove that the code $\mathrm{P}(\widetilde{\mathcal{C}}(q,m,r,\ell))$ is scalar-equivalent to the projective Reed-Muller code $\mathrm{PRM}(q,m,\ell)$.

Let T be the mapping from $\mathrm{GF}(q)[x_1,x_2,\ldots,x_m]$ to the quotient ring

$$\mathrm{GF}(q)[x_1,x_2,\ldots,x_m]/\langle x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle$$

defined by

$$T(\sum c_{i_1,i_2,\ldots,i_m} x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}) = \sum c_{i_1,i_2,\ldots,i_m} x_1^{i'_1} x_2^{i'_2} \cdots x_m^{i'_m}$$

where these i'_j satisfy the following conditions:

1) If $i_j = 0$, then $i'_j = 0$.
2) If $i_j > 0$, then $1 \le i'_j \le q-1$ and $i'_j \equiv i_j \pmod{q-1}$.

For each $a \in \mathrm{GF}(q)$, $a^q = a$. It follows that $a^{i_j} = a^{i'_j}$. Consequently, $f(\mathbf{x}) = T(f)(\mathbf{x})$ for any $\mathbf{x} \in \mathrm{GF}(q)^m$.

Recall that $A(q,m,\ell)$ denotes the subspace of

$$\mathrm{GF}(q)[x_1,x_2,\ldots,x_m]$$

generated by all the homogeneous polynomials of degree ℓ, where $\ell < (q-1)m$.

Lemma 45: Let $q > 2$ be a prime power, $m \ge 2$ be an integer and $\overline{n} = (q^m-1)/(q-1)$. Then $\{\mathbf{e}\mathbf{M}^i : 0 \le i \le \overline{n}-1\}$ is the set of points in $\mathrm{PG}(m-1,\mathrm{GF}(q))$.

Proof: Suppose there are $0 \le i < j \le \overline{n}-1$ such that $\mathbf{e}\mathbf{M}^i = \gamma \cdot \mathbf{e}\mathbf{M}^j$, where $\gamma \in \mathrm{GF}(q)^*$. Then

$$\begin{aligned}\beta^i &= (\mathbf{e}\mathbf{M}^i, \overline{\beta}) \\ &= (\gamma \cdot \mathbf{e}\mathbf{M}^j, \overline{\beta}) \\ &= \gamma \cdot (\mathbf{e}\mathbf{M}^j, \overline{\beta}) \\ &= \gamma \cdot \beta^j.\end{aligned}$$

It follows that $\beta^{j-i} \in \mathrm{GF}(q)^*$, which deduces that $\overline{n} \mid (j-i)$, a contradiction. Therefore, any two distinct elements in the set $\{\mathbf{e}\mathbf{M}^i : 0 \le i \le \overline{n}-1\}$ are linearly independent over $\mathrm{GF}(q)$. The desired result follows. ∎

According to Lemma 45, the projective Reed-Muller code $\mathrm{PRM}(q,m,\ell)$ is scalar-equivalent to the code

$$\begin{aligned}\widehat{\mathcal{C}}(q,m,\ell) = \{&\widehat{\mathbf{c}}_f = (f(\mathbf{e}), f(\mathbf{e}\mathbf{M}), \ldots, f(\mathbf{e}\mathbf{M}^{\overline{n}-1})) : \\ &f(x_1,x_2,\ldots,x_m) \in A(q,m,\ell)\},\end{aligned}$$

where $\overline{n} = (q^m-1)/(q-1)$.

Theorem 46: Let $q > 2$ be a prime power and $m \ge 2$ be an integer. Let $r > 1$ with $r \mid (q-1)$, and let $r-1 \le \ell \le (q-1)(m-1)-1$ with $\ell \equiv r-1 \pmod{r}$. Then the following hold.

1) The code $\mathrm{P}(\widetilde{\mathcal{C}}(q,m,r,\ell))$ over $\mathrm{GF}(q)$ has dimension

$$\sum_{\substack{t \equiv \ell \pmod{q-1} \\ 0<t\le\ell}} \left(\sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{t-jq+m-1}{t-jq} \right).$$

2) The projective Reed-Muller code $\mathrm{PRM}(q,m,\ell)$ over $\mathrm{GF}(q)$ is scalar-equivalent to the code $\mathrm{P}(\widetilde{\mathcal{C}}(q,m,r,\ell))$. In particular, if $r = q-1$, the code $\mathrm{PRM}(q,m,\ell)$ is scalar-equivalent to the λ-constacyclic code $\mathcal{C}(q,m,r,\ell)$.

3) Let $\ell = (q-1)\ell_1 + \ell_0$, where $\ell_1 \ge 0$ and $0 < \ell_0 < q-1$, then the code $\mathrm{P}(\widetilde{\mathcal{C}}(q,m,r,\ell))$ has minimum distance

$$(q-\ell_0+1)q^{m-2-\ell_1}.$$

4) The λ-constacyclic code $\widetilde{\mathcal{C}}(q,m,r,\ell)$ over $\mathrm{GF}(q)$ has parameters $[n,k,d]$, where

$$\begin{aligned}n &= (q^m-1)/r, \\ k &= \sum_{\substack{t \equiv \ell \pmod{q-1} \\ 0<t\le\ell}} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{t-jq+m-1}{t-jq}, \\ d &= \left(\frac{q-1}{r}\right)(q-\ell_0+1)q^{m-2-\ell_1}.\end{aligned}$$

Proof: 1) Similar to Theorem 38, one can prove that

$$\begin{aligned}&\dim(\mathrm{P}(\widetilde{\mathcal{C}}(q,m,r,\ell))) \\ &= |\{(i_1,i_2,\ldots,i_m) \in \{0,1,\cdots,q-1\}^m : \\ &\quad \sum_{k=1}^{m} i_k \equiv \ell \pmod{q-1}, \sum_{k=1}^{m} i_k \le \ell\}|.\end{aligned}$$

The remaining proofs are similar to Theorem 34, and details are omitted here.

2) We claim that $\widehat{\mathcal{C}}(q,m,\ell) = \mathrm{P}(\widetilde{\mathcal{C}}(q,m,r,\ell))$. It follows from Theorem 9 and Result 1 that

$$\dim(\widehat{\mathcal{C}}(q,m,\ell)) = \dim(\mathrm{P}(\widetilde{\mathcal{C}}(q,m,r,\ell))).$$

Therefore, in order to prove the desired conclusion, we only need to prove $\widehat{\mathcal{C}}(q,m,\ell) \subseteq \mathrm{P}(\widetilde{\mathcal{C}}(q,m,r,\ell))$. Let

$$f(x_1,x_2,\ldots,x_m) \in A(q,m,\ell)$$

and let

$$\widehat{\mathbf{c}}_f = (f(\mathbf{e}), f(\mathbf{e}\mathbf{M}), \ldots, f(\mathbf{e}\mathbf{M}^{\overline{n}-1}))$$

be the codeword corresponding to the polynomial

$$f(x_1,x_2,\ldots,x_m).$$

Since $f(\mathbf{x}) = T(f)(\mathbf{x})$ for any $\mathbf{x} \in \mathrm{GF}(q)^m$, we have

$$\widehat{\mathbf{c}}_f = (T(f)(\mathbf{e}), T(f)(\mathbf{eM}), \ldots, T(f)(\mathbf{eM}^{n-1})).$$

If

$$f(x_1, \ldots, x_m) = \sum c_{i_1,i_2,\ldots,i_m} x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \in A(q, m, \ell),$$

then $T(f) = \sum c_{i_1,i_2,\ldots,i_m} x_1^{i'_1} x_2^{i'_2} \cdots x_m^{i'_m}$ where $i'_j = i_j = 0$ or $1 \le i'_j \le q-1$ and such that $i'_j \equiv i_j \pmod{q-1}$. It is clear that

$$\sum_{j=1}^{m} i'_j \equiv \sum_{j=1}^{m} i_j \equiv \ell \pmod{q-1},$$

and $\deg(T(f)) \le \ell$. Therefore, $T(f) \in \widetilde{M}(q, m, r, \ell)$. It follows that

$$\widehat{\mathbf{c}}_f = (T(f)(\mathbf{e}), T(f)(\mathbf{eM}), \ldots, T(f)(\mathbf{eM}^{n-1})) \in \mathrm{P}(\widetilde{\mathcal{C}}(q, m, r, \ell)).$$

Consequently, $\widehat{\mathcal{C}}(q, m, \ell) \subseteq \mathrm{P}(\widetilde{\mathcal{C}}(q, m, r, \ell))$. This proves the claim.

Note that the code $\mathrm{PRM}(q, m, \ell)$ is scalar-equivalent to the code $\widehat{\mathcal{C}}(q, m, \ell)$, and $\mathrm{P}(\widetilde{\mathcal{C}}(q, m, r, \ell)) = \mathcal{C}(q, m, r, \ell)$ for $r = q-1$. The desired result follows.

3) The desired result follows from Result 2 and Theorem 9.

4) By Result 3 of Theorem 44,

$$\dim(\widetilde{\mathcal{C}}(q, m, r, \ell)) = \dim(\mathrm{P}(\widetilde{\mathcal{C}}(q, m, r, \ell)))$$

and

$$d(\widetilde{\mathcal{C}}(q, m, r, \ell)) = \left(\frac{q-1}{r}\right) \cdot d(\mathrm{P}(\widetilde{\mathcal{C}}(q, m, r, \ell))).$$

The desired result follows from Result 1 and Result 3. ∎

Note that $\widetilde{\mathcal{C}}(q, m, r, \ell) \subseteq \mathcal{C}(q, m, r, \ell)$, we have

$$d(\mathcal{C}(q, m, r, \ell)) \le d(\widetilde{\mathcal{C}}(q, m, r, \ell)).$$

By Result 4 of Theorem 46, we can improve the upper bound in (7).

Theorem 47: Let $r > 2$ and $r \mid (q-1)$. Let $\ell = (q-1)\ell_1 + \ell_0 \le (q-1)(m-1)-1$, where $\ell_1 \le m-2$, $0 \le \ell_0 \le q-2$ and $\ell_0 \equiv r-1 \pmod{r}$. Then

$$\frac{(q-\ell_0)q^{m-\ell_1-1}-2}{r} + 1 \le d(\mathcal{C}(q, m, r, \ell)) \le \left(\frac{q-1}{r}\right)(q-\ell_0+1)q^{m-2-\ell_1}. \quad (9)$$

When $r = q-1$, the minimum distance of the code $\mathcal{C}(q, m, r, \ell)$ just takes the upper bound in (9).

Corollary 48: Let $q \ge 3$ be a prime power and $r = q-1$. Let $\ell = (q-1)\ell_1 + q - 2$, where $0 \le \ell_1 \le m-2$. Then the code $\mathcal{C}(q, m, q-1, \ell)$ over $\mathrm{GF}(q)$ is scalar-equivalent to the projective Reed-Muller code $\mathrm{PRM}(q, m, \ell)$ over $\mathrm{GF}(q)$. Furthermore, $d(\mathcal{C}(q, m, q-1, \ell)) = 3 \cdot q^{m-2-\ell_1}$.

Proof: When $r = q-1$, $\mathcal{C}(q, m, r, \ell) = \mathrm{P}(\widetilde{\mathcal{C}}(q, m, r, \ell))$. The desired result follows directly from Theorem 46. ∎

Corollary 48 shows that the constacyclic code

$$\mathcal{C}(q, m, q-1, (q-1)\ell_1 + q - 2)$$

is scalar-equivalent to the projective Reed-Muller code

$$\mathrm{PRM}(q, m, (q-1)\ell_1 + q - 2),$$

where $0 \le \ell_1 \le m-2$. Although the two codes

$$\mathcal{C}(q, m, q-1, (q-1)\ell_1 + q - 2)$$

and $\mathrm{PRM}(q, m, (q-1)\ell_1 + q - 2)$ are scalar-equivalent, the former is more interesting, as the former is a constacyclic code but the later is a linear code.

Example 49: Let $(q, m, r, \ell) = (3, 4, 2, 1)$. Let β be the primitive element of $\mathrm{GF}(3^4)$ with $\beta^4 + 2\beta^3 + 2 = 0$. Then the constacyclic code $\mathcal{C}(3, 4, 2, 1)$ over $\mathrm{GF}(3)$ has parameters $[40, 4, 27]$ and is distance-optimal.

When $\ell_1 = m-2$ and $\ell_0 = r-1$, it is easily verified that the upper and lower bounds in (9) are equal. Then we have the following conclusion.

Corollary 50: Let $\ell = (q-1)(m-2)+r-1$, where $m \ge 2$. Then

$$d(\mathcal{C}(q, m, r, \ell)) = \frac{(q-1)(q-r+2)}{r}.$$

The following problem is interesting and worth of investigation.

Open Problem 51: Let $q \ge 7$ and $m \ge 2$. Let r be a divisor of $q-1$ and $2 < r < q-1$. Let $\ell = r\ell_1 + r - 1$, where $1 \le \ell_1 \le (\frac{q-1}{r})m - 3$. Determine the minimum distance of the code $\mathcal{C}(q, m, r, \ell)$ or improve the lower bound in (7).

We have the following results about the dual code of the constacyclic code $\mathcal{C}(q, m, r, \ell)$.

Theorem 52: Let $\ell = r\ell_1 + r - 1$, where $0 \le \ell_1 \le (\frac{q-1}{r})m - 2$. Then the dual code $\mathcal{C}(q, m, r, \ell)^\perp$ of the constacyclic code $\mathcal{C}(q, m, r, \ell)$ is the λ^{-1}-constacyclic code of length $(q^m-1)/r$ over $\mathrm{GF}(q)$ with generator polynomial

$$g^\perp_{(q,m,r,\ell)}(x) = \prod_{\substack{i \in \Gamma^{(r-1)}_{(q,N,r)} \\ \mathtt{wt}_q(i) \le \ell}} \mathbb{M}_{\beta^i}(x),$$

where $\Gamma^{(r-1)}_{(q,N,r)} = \{i \in \Gamma_{(q,N)} : \mathtt{wt}_q(i) \equiv r-1 \pmod{r}\}$. In particular, if $r = 2$, then

$$\mathcal{C}(q, m, r, \ell)^\perp = \mathcal{C}(q, m, r, (q-1)m - \ell - r).$$

Proof: It is clear that

$$x^n - \lambda = \prod_{i \in \Gamma^{(1)}_{(q,N,r)}} \mathbb{M}_{\beta^i}(x) = \prod_{\substack{i \in \Gamma^{(1)}_{(q,N,r)} \\ \mathtt{wt}_q(i) < (q-1)m-\ell}} \mathbb{M}_{\beta^i}(x) \prod_{\substack{i \in \Gamma^{(1)}_{(q,N,r)} \\ \mathtt{wt}_q(i) \ge (q-1)m-\ell}} \mathbb{M}_{\beta^i}(x).$$

It follows that the generator polynomial of $\mathcal{C}(q, m, r, \ell)^\perp$ is

$$g^\perp_{(q,m,r,\ell)}(x) := \prod_{\substack{i \in \Gamma^{(1)}_{(q,N,r)} \\ \mathtt{wt}_q(i) \ge (q-1)m-\ell}} \widehat{\mathbb{M}_{\beta^i}}(x) = \prod_{\substack{i \in \Gamma^{(1)}_{(q,N,r)} \\ \mathtt{wt}_q(i) \ge (q-1)m-\ell}} \mathbb{M}_{\beta^{N-i}}(x),$$

where $\widehat{\mathbb{M}_{\beta^i}(x)}$ denotes the reciprocal polynomial of $\mathbb{M}_{\beta^i}(x)$. Since $r \mid N$, $i \equiv 1 \pmod r$ if and only if $N - i \equiv r - 1 \pmod r$. Note that

$$\mathtt{wt}_q(N-i) = (q-1)m - \mathtt{wt}_q(i),$$

then $\mathtt{wt}_q(i) \geq (q-1)m - \ell$ if and only if $\mathtt{wt}_q(N-i) \leq \ell$. Therefore,

$$g^{\perp}_{(q,m,r,\ell)}(x) = \prod_{\substack{i \in \Gamma^{(r-1)}_{(q,N,r)} \\ \mathtt{wt}_q(i) \leq \ell}} \mathbb{M}_{\beta^i}(x).$$

When $r = 2$, it is clear that

$$g^{\perp}_{(q,m,r,\ell)}(x) = g_{(q,m,r,(q-1)m-\ell-r)}(x).$$

This completes the proof. ∎

Theorem 53: Let $r > 1$ and $r \mid (q-1)$. Let $\ell = r\ell_1 + r - 1$, where $0 \leq \ell_1 \leq (\frac{q-1}{r})m - 2$. Then

$$\dim(\mathcal{C}(q,m,r,\ell)^{\perp}) = \frac{q^m-1}{r} - \sum_{t=0}^{\ell_1}\sum_{j=0}^{m}(-1)^j \binom{m}{j}\binom{tr+r-1-jq+m-1}{tr+r-1-jq}$$

and

$$d(\mathcal{C}(q,m,r,\ell)^{\perp}) \geq \left\lfloor \left(\frac{\ell_0'+1}{r}\right) q^{\ell_1'} \right\rfloor + 1, \tag{10}$$

where ℓ_0', ℓ_1' such that $\ell = (q-1)\ell_1' + \ell_0'$ and $0 \leq \ell_0' \leq q-2$.

Proof: The desired conclusion on the dimension of the dual code follows from Theorem 34. Below we prove the lower bound on the minimum distance of the dual code.

Suppose $\ell = (q-1)\ell_1' + \ell_0'$, where $0 \leq \ell_0' \leq q-2$. Let H be the smallest integer with $\mathtt{wt}_q(H) = \ell$. Then

$$H = \ell_0' q^{\ell_1'} + \sum_{i=0}^{\ell_1'-1}(q-1)q^i = (\ell_0'+1)q^{\ell_1'} - 1.$$

It is easily verified that every integer u with $0 < u \leq H$ satisfies $\mathtt{wt}_q(u) \leq \ell$. Define

$$B = \left\{ r - 1 + rj : 0 \leq j \leq \left\lfloor \left(\frac{\ell_0'+1}{r}\right) q^{\ell_1'} \right\rfloor - 1 \right\}.$$

Then β^i is a zero of $g^{\perp}_{(q,m,r,\ell)}(x)$ for each $i \in B$. The desired bound then follows from Lemma 6. This completes the proof. ∎

When $r = 2$ or $q-1$, the minimum distance of $\mathcal{C}(q,m,r,\ell)^{\perp}$ can be completely determined.

Theorem 54: Let q be an odd prime power and $r = 2$. Let $1 \leq \ell = (q-1)\ell_1 + \ell_0 < (q-1)m - 1$, where $m \geq 2$, $0 \leq \ell_0 \leq q-2$ and $\ell_0 \equiv r - 1 \pmod r$. Then

$$d(\mathcal{C}(q,m,r,\ell)^{\perp}) = \begin{cases} \left(\frac{3+\ell_0}{2}\right) q^{\ell_1} & \text{if } \ell_0 < q-2, \\ q^{\ell_1+1} & \text{if } \ell_0 = q-2. \end{cases}$$

Proof: By Theorem 52,

$$\mathcal{C}(q,m,r,\ell)^{\perp} = \mathcal{C}(q,m,r,(q-1)m-\ell-r).$$

Note that

$$(q-1)m - \ell - r = (q-1)(m-\ell_1-1) + q - 3 - \ell_0.$$

If $\ell_0 < q-2$, by Corollary 41,

$$d(\mathcal{C}(q,m,r,\ell)^{\perp}) = [(3+\ell_0)/2]q^{\ell_1}.$$

If $\ell_0 = q-2$, by Corollary 41,

$$d(\mathcal{C}(q,m,r,\ell)^{\perp}) = q^{\ell_1+1}.$$

This completes the proof. ∎

Theorem 55: Let $q > 2$ be a prime power and $r = q-1$. Let $\ell = (q-1)\ell_1 + q - 2$, where $0 \leq \ell_1 \leq m-2$. Then

$$d(\mathcal{C}(q,m,r,\ell)^{\perp}) = q^{\ell_1+1}.$$

Proof: By Corollary 48, the code $\mathcal{C}(q,m,q-1,\ell)$ is scalar-equivalent to $\mathrm{PRM}(q,m,\ell)$. It follows that the code $\mathcal{C}(q,m,q-1,\ell)^{\perp}$ is scalar-equivalent to $\mathrm{PRM}(q,m,\ell)^{\perp}$. It then follows from Theorem 10 that

$$\mathrm{PRM}(q,m,\ell)^{\perp} = \mathrm{PRM}(q,m,(m-1)(q-1)-\ell).$$

Thereby,

$$d(\mathcal{C}(q,m,r,\ell)) = d(\mathrm{PRM}(q,m,(m-1)(q-1)-\ell)).$$

Note that $(m-1)(q-1) - \ell - 1 = (m-2-\ell_1)(q-1)$, by Theorem 9,

$$d(\mathrm{PRM}(q,m,(m-1)(q-1)-\ell)) = q^{\ell_1+1}.$$

This completes the proof. ∎

B. Some Special Cases of the Constacyclic Code $\mathcal{C}(q,m,r,\ell)$

In this subsection, we will study the code $\mathcal{C}(q,m,r,\ell)$ in some special cases. We do have the dimension formula of the code $\mathcal{C}(q,m,r,\ell)$ in Theorem 34, which may not be easily simplified. Instead, we will determine the generator or check polynomial of $\mathcal{C}(q,m,r,\ell)$ and will then know the dimension of the code without using Theorem 34.

Theorem 56: Let $r > 1$ and $r \mid (q-1)$. Let $\ell = (q-1)m - r - 1$, where $m \geq 2$. Then the constacyclic code $\mathcal{C}(q,m,r,\ell)$ over $\mathrm{GF}(q)$ has parameters $[(q^m-1)/r, (q^m-1)/r - m, d]$, where

$$d = \begin{cases} 2 & \text{if } r < q-1, \\ 3 & \text{if } r = q-1. \end{cases}$$

Moreover, the dual code $\mathcal{C}(q,m,r,\ell)^{\perp}$ has parameters

$$[(q^m-1)/r, m, [(q-1)/r]q^{m-1}].$$

Proof: When $\ell = (q-1)m - r - 1$, we have

$$\begin{aligned} & D_{(q,m,r,\ell)} \\ &= \{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) < r+1,\ \mathtt{wt}_q(i) \equiv 1 \pmod r\} \\ &= \{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) = 1\} \\ &= C_1^{(q,N)}. \end{aligned}$$

By definition, we have $g_{(q,m,r,\ell)}(x) = \mathbb{M}_{\beta}(x)$. Then

$$\dim(\mathcal{C}(q,m,r,\ell)) = (q^m-1)/r - m.$$

Now consider the minimum distance of the code $\mathcal{C}(q,m,r,\ell)$. There are two cases.

1) $r < q-1$. Then $\ell = (q-1)(m-1)+q-2-r$. By Theorem 39, $d(\mathcal{C}(q,m,r,\ell)) = 2$.
2) $r = q-1$. Then $\ell = (q-1)(m-2)+(q-2)$. By Theorem 39, $d(\mathcal{C}(q,m,r,\ell)) \geq 3$. By the Sphere Packing bound, $d(\mathcal{C}(q,m,r,\ell)) \leq 3$. The desired result follows.

By Lemma 5, the trace representation of $\mathcal{C}(q,m,r,\ell)^\perp$ is given by

$$\mathcal{C}(q,m,r,\ell)^\perp = \{\mathbf{c}(a) = (\mathrm{Tr}_{q^m/q}(a\beta^i))_{i=0}^{n-1} : a \in \mathrm{GF}(q^m)\}.$$

For $a \in \mathrm{GF}(q^m)^*$,

$$\begin{aligned}
\mathtt{wt}(\mathbf{c}(a)) &= n - \frac{1}{q}\sum_{i=0}^{n-1}\sum_{x\in\mathrm{GF}(q)} \zeta_p^{\mathrm{Tr}_{q/p}(x\mathrm{Tr}_{q^m/q}(a\beta^i))} \\
&= n - \frac{1}{rq}\sum_{i=0}^{rn-1}\sum_{x\in\mathrm{GF}(q)} \zeta_p^{\mathrm{Tr}_{q/p}(x\mathrm{Tr}_{q^m/q}(a\beta^i))} \\
&= n - \frac{1}{rq}\sum_{x\in\mathrm{GF}(q)}\sum_{y\in\mathrm{GF}(q^m)^*} \zeta_p^{\mathrm{Tr}_{q^m/p}(axy)} \\
&= n - \frac{1}{rq}[q^m - 1 + (q-1)\sum_{y\in\mathrm{GF}(q^m)^*} \zeta_p^{\mathrm{Tr}_{q^m/p}(y)}] \\
&= n - \frac{1}{rq}[q^m - 1 - (q-1)] \\
&= (\frac{q-1}{r})q^{m-1}.
\end{aligned}$$

The desired minimum distance of the dual code then follows. ∎

Notice that the constacyclic code

$$\mathcal{C}(q,m,q-1,(q-1)(m-2)+q-2)$$

has parameters

$$[(q^m-1)/(q-1), (q^m-1)/(q-1)-m, 3]$$

and is monomially-equivalent to the Hamming code. The dual code $\mathcal{C}(q,m,(q-1)(m-2)+q-2)^\perp$ has parameters

$$\left[(q^m-1)/(q-1), m, q^{m-1}\right]$$

and is monomially-equivalent to the Simplex code.

Theorem 57: Let $r > 1$ and $r \mid (q-1)$. Let $\ell = (q-1)(m-1)+\ell_0$, where $m \geq 2$, $0 \leq \ell_0 < q-2$ and $\ell_0 \equiv r-1 \pmod r$. Then the constacyclic code $\mathcal{C}(q,m,r,\ell)$ over $\mathrm{GF}(q)$ has parameters

$$\left[\frac{q^m-1}{r}, \frac{q^m-1}{r} - \sum_{t=0}^{\frac{q-2-\ell_0}{r}-1}\binom{m+rt}{rt+1}, \frac{q-\ell_0+r-2}{r}\right].$$

Proof: When $\ell = (q-1)(m-1)+\ell_0$, we have

$$(q-1)m - \ell = q-1-\ell_0.$$

Then

$$\begin{aligned}
&D_{(q,m,r,\ell)} \\
&= \{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) < q-1-\ell_0,\ \mathtt{wt}_q(i) \equiv 1 \pmod r\} \\
&= \bigcup_{t=0}^{\frac{q-2-\ell_0}{r}-1} \{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) = rt+1\}.
\end{aligned}$$

It is easily checked that

$$|D_{(q,m,r,\ell)}| = \sum_{t=0}^{\frac{q-2-\ell_0}{r}-1}\binom{m+rt}{rt+1}.$$

The desired dimension follows. The desired minimum distance then follows from Corollary 40. ∎

Theorem 58: Let $r > 1$ and $r \mid (q-1)$. Let $\ell = (q-1)(m-2)+r-1$, where $m \geq 2$. Then the constacyclic code $\mathcal{C}(q,m,r,\ell)$ over $\mathrm{GF}(q)$ has parameters

$$\left[\frac{q^m-1}{r}, \frac{q^m-1}{r} - \kappa, \frac{(q-1)(q-r+2)}{r}\right],$$

where

$$\kappa = \begin{cases} \sum_{t=0}^{\frac{2(q-1-r)}{r}}\binom{m+rt}{rt+1} & \text{if } \frac{q+1}{2} \leq r \leq q-1, \\ \sum_{t=0}^{\frac{2(q-1-r)}{r}}\binom{m+rt}{rt+1} - m\sum_{t=\frac{q-1}{r}}^{\frac{2(q-1-r)}{r}}\binom{tr-q+m}{tr-q+1} & \text{if } 2 \leq r \leq \frac{q-1}{2}. \end{cases}$$

Proof: When $\ell = (q-1)(m-2)+r-1$, we have $(q-1)m - \ell = 2(q-1)-r+1$. Then

$$\begin{aligned}
&D_{(q,m,r,\ell)} \\
&= \{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) \leq 2(q-r)-1, \mathtt{wt}_q(i) \equiv 1 \pmod r\} \\
&= \bigcup_{t=0}^{\frac{2(q-1-r)}{r}} \{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) = rt+1\}.
\end{aligned}$$

When $(q+1)/2 \leq r \leq q-1$, we have $2(q-1)-2r+1 \leq q-2$. It is easily checked that

$$|D_{(q,m,r,\ell)}| = \sum_{t=0}^{\frac{2(q-1-r)}{r}}\binom{m+rt}{rt+1}.$$

When $2 \leq r \leq (q-1)/2$, we have

$$q \leq 2(q-1)-2r+1 < 2(q-1).$$

Clearly,

$$\begin{aligned}
&|D_{(q,m,r,\ell)}| \\
&= \sum_{t=0}^{\frac{q-1}{r}-1} |\{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) = rt+1\}| \\
&\quad + \sum_{t=\frac{q-1}{r}}^{\frac{2(q-1-r)}{r}} |\{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) = rt+1\}| \\
&= \sum_{t=0}^{\frac{q-1}{r}-1}\binom{m+rt}{rt+1} + \\
&\quad \sum_{t=\frac{q-1}{r}}^{\frac{2(q-1-r)}{r}}\left[\binom{m+rt}{rt+1} - m\binom{tr-q+m}{tr-q+1}\right] \\
&= \sum_{t=0}^{\frac{2(q-1-r)}{r}}\binom{m+rt}{rt+1} - m\sum_{t=\frac{q-1}{r}}^{\frac{2(q-1-r)}{r}}\binom{tr-q+m}{tr-q+1}.
\end{aligned}$$

The desired dimension follows. The desired minimum distance then follows from Corollary 50. ∎

Theorem 59: Let $q \geq 3$ and $m \geq 3$. Then the constacyclic code $\mathcal{C}(q, m, q-1, (q-1)(m-3)+q-2)$ over $\mathrm{GF}(q)$ has parameters

$$\left[(q^m-1)/(q-1), (q^m-1)/(q-1) - \binom{m+q-1}{q}, 3\cdot q\right],$$

and the dual code $\mathcal{C}(q, m, q-1, (q-1)(m-3)+q-2)^\perp$ has parameters

$$\left[(q^m-1)/(q-1), \binom{m+q-1}{q}, q^{m-2}\right].$$

Proof: Let $\ell = (q-1)(m-3)+q-2$. Note that

$$(q-1)m - \ell = 2(q-1)+1.$$

It is easy to see that

$$\begin{aligned} & D_{(q,m,q-1,\ell)} \\ = \ & \{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) < 2q-1, \ \mathtt{wt}_q(i) \equiv 1 \pmod{q-1}\} \\ = \ & \{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) = 1\} \cup \{i \in \mathbb{Z}_{q^m-1} : \mathtt{wt}_q(i) = q\}. \end{aligned}$$

Then

$$\begin{aligned} & |D_{(q,m,q-1,\ell)}| \\ = & |\{(i_0, i_1, \ldots, i_{m-1}) \in \Sigma_q^m : \sum_{j=0}^{m-1} i_j = 1\}| + \\ & |\{(i_0, i_1, \ldots, i_{m-1}) \in \Sigma_q^m : \sum_{j=0}^{m-1} i_j = q\}|, \end{aligned} \tag{11}$$

where $\Sigma_q^m = \{0, 1, \cdots, q-1\}^m$.

Clearly, we have

$$|\{(i_0, i_1, \ldots, i_{m-1}) \in \Sigma_q^m : \sum_{j=0}^{m-1} i_j = 1\}| = m. \tag{12}$$

It follows Lemma 33 that

$$\begin{aligned} & |\{(i_0, i_1, \ldots, i_{m-1}) \in \Sigma_q^m : \sum_{j=0}^{m-1} i_j = q\}| \\ = \ & N(q, m, q-1) \\ = \ & \binom{m+q-1}{q} - m. \end{aligned}$$

It then follows from (11) and (12) that

$$|D_{(q,m,q-1,\ell)}| = \binom{m+q-1}{q}.$$

The desired conclusion on the dimension of $\mathcal{C}(q, m, q-1, \ell)$ then follows. By Corollary 48,

$$d(\mathcal{C}(q, m, q-1, \ell)) = 3 \cdot q.$$

By Theorem 55, $d(\mathcal{C}(q, m, q-1, \ell))^\perp = q^{m-2}$. This completes the proof. ∎

Theorem 60: Let $q \geq 3$ and $m \geq 2$. Then the constacyclic code $\mathcal{C}(q, m, q-1, q-2)$ over $\mathrm{GF}(q)$ has parameters

$$\left[(q^m-1)/(q-1), \binom{m+q-3}{q-2}, 3\cdot q^{m-2}\right],$$

and the dual code $\mathcal{C}(q, m, q-1, q-2)^\perp$ has parameters

$$\left[(q^m-1)/(q-1), (q^m-1)/(q-1) - \binom{m+q-3}{q-2}, q\right].$$

Proof: Let $\ell = q-2$, then

$$\begin{aligned} D_{(q,m,q-1,\ell)} = \{i \in \mathbb{Z}_N : & \mathtt{wt}_q(i) < (q-1)m - (q-1) + 1, \\ & \mathtt{wt}_q(i) \equiv 1 \pmod{q-1}\}. \end{aligned}$$

It is easy to check that

$$\begin{aligned} & \{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) = (q-1)m - (q-1) + 1\} \\ = & \left\{N - (i_0 + i_1 q + \cdots + i_{m-1} q^{m-1}) : \sum_{k=0}^{m-1} i_k = q-2\right\}. \end{aligned}$$

It follows that

$$\begin{aligned} & |\{i \in \mathbb{Z}_N : \mathtt{wt}_q(i) = (q-1)m - (q-1) + 1\}| \\ = & \binom{q-2+m-1}{q-2} \\ = & \binom{m+q-3}{q-2}. \end{aligned}$$

Then

$$\dim(\mathcal{C}(q, m, q-1, q-2)) = \binom{m+q-3}{q-2},$$

and

$$\dim(\mathcal{C}(q, m, q-1, q-2)^\perp) = \frac{q^m-1}{q-1} - \binom{m+q-3}{q-2}.$$

The minimum distance of the code $\mathcal{C}(q, m, q-1, q-2)$ (resp. $\mathcal{C}(q, m, q-1, q-2)^\perp$) follows from Corollary 48 (resp. Theorem 55). This completes the proof. ∎

Notice that the constacyclic code $\mathcal{C}(4, m, 3, 2)$ over $\mathrm{GF}(4)$ and the code $\mathrm{PRM}(4, m, 2)$ over $\mathrm{GF}(4)$ are scalar-equivalent, they have the same weight distribution. The weight distribution of $\mathcal{C}(4, m, 3, 2)$ is the given in Theorem 11. The following four examples show that $\mathcal{C}(4, m, 3, 2)$ is a $(m+1)$-weight code for even m and m-weight code for odd m. This is consistent with the weight distribution of $\mathcal{C}(4, m, 3, 2)$, which is the same as the weight distribution of $\mathrm{PRM}(4, m, 2)$ documented in Theorem 11.

Example 61: Let $(q, m, q-1, \ell) = (4, 2, 3, 2)$. Let β be the primitive element of $\mathrm{GF}(4^2)$ with $\beta^4 + \beta + 1 = 0$. Then the constacyclic code $\mathcal{C}(4, 2, 3, 2)$ over $\mathrm{GF}(4)$ has parameters $[5, 3, 3]$ and weight enumerator $1 + 30z^3 + 15z^4 + 18z^5$. Furthermore, $\mathcal{C}(4, 2, 3, 2)^\perp$ has parameters $[5, 2, 4]$. Both codes are MDS and optimal.

Example 62: Let $(q, m, q-1, \ell) = (4, 3, 3, 2)$. Let β be the primitive element of $\mathrm{GF}(4^3)$ with $\beta^6 + \beta^4 + \beta^3 + \beta + 1 = 0$. Then the constacyclic code $\mathcal{C}(4, 3, 3, 2)$ over $\mathrm{GF}(4)$ has parameters $[21, 6, 12]$ and weight enumerator

$$1 + 630z^{12} + 3087z^{16} + 378z^{20}.$$

Notice that $\mathcal{C}(4, 3, 3, 2)$ is distance-optimal [27]. Furthermore, $\mathcal{C}(4, 3, 3, 2)^\perp$ has parameters $[21, 15, 4]$ and is almost-distance-optimal [27].

Example 63: Let $(q, m, q-1, \ell) = (4, 4, 3, 2)$. Let β be the primitive element of $\mathrm{GF}(4^4)$ with $\beta^8 + \beta^4 + \beta^3 + \beta^2 + 1 =$

0. Then the constacyclic code $\mathcal{C}(4,4,3,2)$ over GF(4) has parameters $[85,10,48]$ and weight enumerator

$$1+10710z^{48}+411264z^{60}+257295z^{64}+362880z^{68}+6426z^{80}.$$

Furthermore, $\mathcal{C}(4,4,3,2)^{\perp}$ has the best known parameters $[85,75,4]$ [27].

Example 64: Let $(q,m,q-1,\ell)=(4,5,3,2)$. Let β be the primitive element of GF(4^5) with $\beta^{10}+\beta^6+\beta^5+\beta^3+\beta^2+\beta+1=0$. Then the constacyclic code $\mathcal{C}(4,5,3,2)$ over GF(4) has parameters $[341,15,192]$ and weight enumerator $1+173910z^{192}+140241024z^{240}+809480463z^{256}+123742080z^{272}+104346z^{320}$. Furthermore, $\mathcal{C}(4,5,3,2)^{\perp}$ has parameters $[341,326,4]$.

Theorem 65: Let $q\geq 5$ be an odd prime power, $m\geq 2$, and $r=2$. Let $\ell=(q-1)(m-2)+\ell_0$, where $1\leq \ell_0\leq q-2$ and ℓ_0 is odd. Then the constacyclic code $\mathcal{C}(q,m,2,\ell)$ over GF(q) has parameters

$$[(q^m-1)/2,(q^m-1)/2-\kappa,[(q-\ell_0)/2]q],$$

where

$$\kappa=\begin{cases}\sum\limits_{t=0}^{\frac{2q-5-\ell_0}{2}}\binom{2t+m}{2t+1}-m\sum\limits_{t=\frac{q-1}{2}}^{\frac{2q-5-\ell_0}{2}}\binom{2t-q+m}{2t-q+1} & \text{if } \ell_0<q-2,\\ \sum\limits_{t=0}^{\frac{q-3}{2}}\binom{2t+m}{2t+1} & \text{if } \ell_0=q-2.\end{cases}$$

Moreover, the dual code $\mathcal{C}(q,m,2,\ell)^{\perp}$ has parameters

$$[(q^m-1)/2,\kappa,d],$$

where

$$d=\begin{cases}[(3+\ell_0)/2]q^{m-2} & \text{if } \ell_0<q-2,\\ q^{m-1} & \text{if } \ell_0=q-2.\end{cases}$$

Proof: Note that $(q-1)m-\ell=2(q-1)-\ell_0$. It is easy to see that

$$\begin{aligned}&D_{(q,m,2,\ell)}\\ &=\{i\in\mathbb{Z}_N:\mathtt{wt}_q(i)\leq 2q-4-\ell_0,\ \mathtt{wt}_q(i)\equiv 1 \pmod 2\}\\ &=\bigcup_{t=0}^{\frac{2q-5-\ell_0}{2}}\{i\in\mathbb{Z}_N:\mathtt{wt}_q(i)=2t+1\}.\end{aligned}$$

If $\ell_0=q-2$, then $2q-4-\ell_0=q-2$. It follows that

$$|D_{(q,m,2,\ell)}|=\sum_{t=0}^{\frac{2q-5-\ell_0}{2}}\binom{2t+m}{2t+1}.$$

If $\ell_0<q-2$, then $2q-4-\ell_0\geq q$. Consequently,

$$\begin{aligned}&|D_{(q,m,2,\ell)}|\\ &=\sum_{t=0}^{\frac{q-3}{2}}|\{i\in\mathbb{Z}_N:\mathtt{wt}_q(i)=2t+1\}|+\\ &\quad\sum_{t=\frac{q-1}{2}}^{\frac{2q-5-\ell_0}{2}}|\{i\in\mathbb{Z}_N:\mathtt{wt}_q(i)=2t+1\}|\\ &=\sum_{t=0}^{\frac{q-3}{2}}\binom{2t+m}{2t+1}+\sum_{t=\frac{q-1}{2}}^{\frac{2q-5-\ell_0}{2}}\left[\binom{2t+m}{2t+1}-m\binom{2t-q+m}{2t-q+1}\right]\\ &=\sum_{t=0}^{\frac{2q-5-\ell_0}{2}}\binom{2t+m}{2t+1}-m\sum_{t=\frac{q-1}{2}}^{\frac{2q-5-\ell_0}{2}}\binom{2t-q+m}{2t-q+1}.\end{aligned}$$

It follows that $\dim(\mathcal{C}(q,m,2,\ell))=n-|D_{(q,m,2,\ell)}|=n-\kappa$, and $\dim(\mathcal{C}(q,m,2,\ell)^{\perp})=\kappa$. The minimum distance of the code $\mathcal{C}(q,m,2,\ell)$ (resp. $\mathcal{C}(q,m,2,\ell)^{\perp}$) follows from Corollary 41 (resp. Theorem 54). This completes the proof. ∎

Theorem 66: Let q be an odd prime power, $m\geq 2$ be an integer and $q^m\equiv 1 \pmod 4$. Let $r=2$ and $\ell=\frac{(q-1)m}{2}-1$. Then the constacyclic code $\mathcal{C}(q,m,2,\ell)$ over GF(q) is a self-dual code with parameters $[(q^m-1)/2,(q^m-1)/4,d]$, where

$$d=\begin{cases}q^{m/2} & \text{if } m \text{ is even},\\ [(q+3)/4]q^{(m-1)/2} & \text{if } m \text{ is odd}.\end{cases}$$

Proof: If $q^m\equiv 1 \pmod 4$, then $\ell=\frac{(q-1)m}{2}-1$ is odd. It follows from Theorem 52 that $\mathcal{C}(q,m,2,\ell)^{\perp}=\mathcal{C}(q,m,2,\ell)$. We now consider the minimum distance of the code $\mathcal{C}(q,m,2,\ell)$. There are two cases.

1) m is even. Then $\ell=(q-1)(m/2-1)+(q-2)$. By Corollary 41, $d(\mathcal{C}(q,m,2,\ell))=q^{m/2}$.
2) m is odd. Then $q\equiv 1 \pmod 4$. Consequently,
$$\ell=(q-1)[(m-1)/2]+(q-3)/2.$$
By Corollary 41, $d(\mathcal{C}(q,m,2,\ell))=[(q+3)/4]q^{(m-1)/2}$.

This completes the proof. ∎

Example 67: Let $(q,m,r,\ell)=(5,3,2,5)$. Let β be the primitive element of GF(5^3) with $\beta^3+3\beta+3=0$. Then the constacyclic code $\mathcal{C}(5,3,2,5)$ over GF(5) has parameters $[62,31,10]$ and is self-dual.

According to [28, Chapter 6], $d\geq\sqrt{n}$ is a good lower on the minimum distance of an infinite class of linear codes over GF(q) with length n and dimension $n/2$, where n is a positive even integer. To the best knowledge of the authors, known infinite classes of self-dual codes with unbounded length n and minimum distance $d\geq\sqrt{n}$ are the following:

1) The extended codes of odd-like quadratic residue codes [28].
2) The Pless symmetry codes [21], [43].
3) The generalized Reed-Muller code of order $[m(q-1)-1]/2$ is a self-dual code over GF(q) with parameters $[q^m,q^m/2,[(q+2)/2]q^{(m-1)/2}]$, where m is odd and $q=2^s$ with a positive integer s [2, Theorem 5.8, Theorem 5.25].

Therefore, Theorem 66 constructs a new class of self-dual codes of length $n=(q^m-1)/2$ over GF(q) with minimum distance $d>\sqrt{n}$. Below we will apply this class of self-dual codes to construct quantum codes. The quantum codes and classical linear codes have the following relationship. For more information on quantum codes, the reader is referred to [32], [46], [47] and the references therein.

Theorem 68 (CSS Construction): [32] If $\mathcal{C}$ is an $[n,k,d]$ linear code over GF(q) with $\mathcal{C}^{\perp}\subseteq\mathcal{C}$, then there exists an $[[n,2k-n,\geq d]]_q$ quantum code.

Using the negacyclic self-dual codes in Theorem 66 via the CSS construction in Theorem 68, we obtain the following quantum codes.

Corollary 69: Let q be an odd prime power, $m \geq 2$ be an integer and $q^m \equiv 1 \pmod 4$. Then there exists a quantum code with parameters $[[(q^m-1)/2, 0, \geq d]]_q$, where

$$d = \begin{cases} q^{m/2} & \text{if } m \text{ is even,} \\ [(q+3)/4]q^{(m-1)/2} & \text{if } m \text{ is odd.} \end{cases}$$

More examples of the code $\mathcal{C}(q, m, r, \ell)$ and its dual are the following.

Example 70: Let $(q, m, r, \ell) = (4, 3, 3, 5)$. Let β be the primitive element of $\mathrm{GF}(4^3)$ with $\beta^6 + \beta^4 + \beta^3 + \beta + 1 = 0$. Then the constacyclic code $\mathcal{C}(4, 3, 3, 5)$ over $\mathrm{GF}(4)$ has parameters $[21, 18, 3]$ and is distance-optimal [27], and $\mathcal{C}(4, 3, 3, 5)^{\perp}$ has parameters $[21, 3, 16]$ and is distance-optimal [27].

Example 71: Let $(q, m, r, \ell) = (4, 3, 3, 4)$. Let β be the primitive element of $\mathrm{GF}(4^3)$ with $\beta^6 + \beta^4 + \beta^3 + \beta + 1 = 0$. Then the constacyclic code $\mathcal{C}(4, 3, 3, 4)$ over $\mathrm{GF}(4)$ has parameters $[21, 6, 12]$ and is distance-optimal [27], $\mathcal{C}(4, 3, 3, 4)^{\perp}$ has parameters $[21, 15, 4]$.

Example 72: Let $(q, m, r, \ell) = (5, 3, 4, 3)$. Let β be the primitive element of $\mathrm{GF}(5^3)$ with $\beta^3 + 3\beta + 3 = 0$. Then the constacyclic code $\mathcal{C}(5, 3, 4, 3)$ over $\mathrm{GF}(5)$ has the best-known parameters $[31, 10, 15]$ [27] and $\mathcal{C}(5, 3, 4, 3)^{\perp}$ has parameters $[31, 21, 5]$.

Example 73: Let $(q, m, r, \ell) = (5, 3, 4, 7)$. Let β be the primitive element of $\mathrm{GF}(5^3)$ with $\beta^3 + 3\beta + 3 = 0$. Then the constacyclic code $\mathcal{C}(5, 3, 4, 7)$ over $\mathrm{GF}(5)$ has parameters $[30, 28, 3]$ and is distance-optimal [27], and $\mathcal{C}(5, 3, 4, 7)^{\perp}$ has parameters $[31, 3, 25]$ and is distance-optimal [27].

These examples above show that the code $\mathcal{C}(q, m, r, \ell)$ could be optimal in some cases. Thus, the code $\mathcal{C}(q, m, r, \ell)$ is interesting in terms of its error-correcting capability.

C. Some Differences Between the Codes $\mathcal{C}(q, m, r, \ell)$ and the Nonprimitive Generalized Reed-Muller Codes NGRM(q, m, r, h)

On one hand, by Corollary 41, the constacyclic code $\mathcal{C}(q, m, 2, \ell)$ over $\mathrm{GF}(q)$ has minimum distance

$$d_1 = [(q - \ell_0)/2]q^{m-1-\ell_1},$$

where $\ell = (q-1)\ell_1 + \ell_0$, $\ell_1 \geq 0$, $0 \leq \ell_0 \leq q - 2$ and $\ell_0 \equiv 1 \pmod 2$. According to Theorem 1, the code $\mathrm{NGRM}(q, m, r, h)$ has minimum distance

$$d_2 = \frac{(q-h_0)q^{m-1-h} - 1}{2},$$

where $(q-1)h + h_0 < (q-1)m$, $0 \leq h_0 \leq q-2$ and $h_0 \equiv 0 \pmod 2$. It is easily checked that $d_1 = d_2$ if and only if $\ell_1 = h = m - 1$ and $\ell_0 = h_0 + 1$. Consequently, the constacyclic code $\mathcal{C}(q, m, 2, \ell)$ and the nonprimitive generalized Reed-Muller codes $\mathrm{NGRM}(q, m, 2, h)$ are different in general.

On the other hand, by Corollary 48, the constacyclic code $\mathcal{C}(q, m, q-1, (q-1)\ell_1 + q - 2)$ over $\mathrm{GF}(q)$ has minimum distance $d_3 = 3 \cdot q^{m-2-\ell_1}$, where $0 \leq \ell_1 \leq m-2$. According to Theorem 1, the code $\mathrm{NGRM}(q, m, q-1, h)$ over $\mathrm{GF}(q)$ has minimum distance $d_4 = (q^{m-h} - 1)/(q-1)$, where $0 \leq h \leq m-1$. Note that $q \geq 3$, we have $d_3 \neq d_4$. Consequently, the constacyclic code $\mathcal{C}(q, m, q-1, (q-1)\ell_1 + q - 2)$ and the nonprimitive generalized Reed-Muller codes $\mathrm{NGRM}(q, m, q-1, h)$ are different.

VI. Summary and Concluding Remarks

The main contributions of this paper are the constructions and analysis of the two classes of constacyclic codes $\mathcal{C}'(q, m, r, \ell)$ and $\mathcal{C}(q, m, r, \ell)$ of length $n = (q^m - 1)/r$ over $\mathrm{GF}(q)$. These codes are quite interesting in theory as they contain optimal codes and codes with best known parameters (see the examples presented in this paper). An infinite class of distance-optimal constacyclic codes was obtained (see Corollary 21). A new infinite class of distance-almost-optimal constacyclic codes was constructed (see Corollary 24). A new infinite class of negacyclic self-dual codes of length $n = (q^m - 1)/2$ over $\mathrm{GF}(q)$ with minimum distance $d > \sqrt{n}$ was obtained (see Theorem 66). Since the codes presented in this paper are constacyclic, their efficient decoding algorithms may be obtained by modifying some efficient decoding algorithms of cyclic codes. For example, Boztas [10] discussed the encoding/decoding of constacyclic codes by means of a constacyclic DFT. Hence, the codes presented in this paper would also be interesting in practice.

The automorphism group of the code $\mathrm{PRM}(q, m, \ell)$ was settled in [6]. Hence, the automorphism group of the code $\mathcal{C}(q, m, r, \ell)$ is known when $r = q - 1$ but is open if $r < q - 1$. Note that $\mathcal{C}(q, 2, q-1, q-2)$ is MDS. It follows from Lemma 8 in [6] that the codewords of each fixed nonnzero weight in $\mathcal{C}(q, m, q-1, (q-1)\ell_1 + q - 2)$ support a 2-design for $m \geq 3$ and $0 \leq \ell_1 \leq m - 2$ [21]. Hence, the codes $\mathcal{C}(q, m, q-1, (q-1)\ell_1 + q - 2)$ are also interesting from the viewpoint of combinatorics.

The two classes of constacyclic codes $\mathcal{C}'(q, m, r, \ell)$ and $\mathcal{C}(q, m, r, \ell)$ treated in this paper are new in the sense that the parameters of some codes in the two classes are not covered by the codes available in the literature. The constacyclic code $\mathcal{C}(q, m, q-1, \ell_1(q-1) + q - 2)$ is scalar-equivalent to the linear code $\mathrm{PRM}(q, m, \ell_1(q-1) + q - 2)$ and gives a constacyclic-code construction of the code $\mathrm{PRM}(q, m, \ell_1(q-1) + q - 2)$. Hence, another contribution of this paper is the proof of the fact that the subclass of projective Reed-Muller codes $\mathrm{PRM}(q, m, \ell_1(q-1) + q - 2)$ are constacyclic up to equivalence. However, it is open if the code $\mathrm{PRM}(q, m, \ell)$ is monomially-equivalent to a constacyclic code when ℓ is not of the form $\ell = \ell_1(q-1) + q - 2$.

It would be very interesting to settle the open problems presented in this paper and determine the automorphism groups of the two classes of constacyclic codes.

Acknowledgment

The authors are very grateful to the associate editor, Prof. Vitaly Skachek, and the reviewers for their comments and suggestions that much improved the quality of this article. All the code examples in this article were computed with the Magma software package.

REFERENCES

[1] D. Akre, N. Aydin, M. Harrington, and S. Pandey, "A generalization of cyclic code equivalence algorithm to constacyclic codes," *Designs, Codes Cryptogr.*, vol. 91, no. 3, pp. 763–777, Mar. 2023.

[2] E. F. Assmus Jr. and J. D. Key, "Polynomial codes and finite geometries," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, pp. 1269–1343.

[3] N. Aydin and J. M. Murphree, "New linear codes from constacyclic codes," *J. Franklin Inst.*, vol. 351, no. 3, pp. 1691–1699, Mar. 2014.

[4] G. K. Bakshi and M. Raka, "A class of constacyclic codes over a finite field," *Finite Fields Appl.*, vol. 18, no. 2, pp. 362–377, Mar. 2012.

[5] S. Ballet and R. Rolland, "On low weight codewords of generalized affine and projective Reed–Muller codes," *Designs, Codes Cryptogr.*, vol. 73, no. 2, pp. 271–297, Nov. 2014.

[6] T. P. Berger, "Automorphism groups of homogeneous and projective Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 5, pp. 1035–1045, May 2002.

[7] T. P. Berger and L. de Maximy, "Cyclic projective Reed–Muller codes," in *Proc. Int. Symp. Appl. Algebra, Algebr. Algorithms, Error-Correcting Codes (AAECC)* (Lecture Notes in Computer Science), S. Boztas and I. E. Shparlinski, Eds. Berlin, Germany: Springer-Verlag, 2001, pp. 77–81.

[8] E. R. Berlekamp, "Negacyclic codes for the Lee metric," in *Proc. Conf. Combinat. Math. Appl.*, Chapel Hill, NC, USA, 1968, pp. 298–316.

[9] T. Blackford, "Negacyclic duadic codes," *Finite Fields Appl.*, vol. 14, no. 4, pp. 930–943, Nov. 2008.

[10] S. Boztas, "Constacyclic codes and constacyclic DFTs," in *Proc. IEEE Int. Symp. Inf. Theory*, Cambridge, MA, USA, Aug. 1998, p. 235.

[11] 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.

[12] B. Chen, Y. Fan, L. Lin, and H. Liu, "Constacyclic codes over finite fields," *Finite Fields Appl.*, vol. 18, no. 6, pp. 1217–1231, Nov. 2012.

[13] B. Chen, W. Fang, S. T. Xia, and F. W. Fu, "Constructions of optimal (r, δ) locally repairable codes via constacyclic codes," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5253–5263, Aug. 2019.

[14] B. Chen, L. Lin, and H. Liu, "Constacyclic symbol-pair codes: Lower bounds and optimal constructions," *IEEE Trans. Inf. Theory*, vol. 63, no. 12, pp. 7661–7666, Dec. 2017.

[15] B. Chen, S. Ling, and G. Zhang, "Application of constacyclic codes to quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1474–1484, Mar. 2015.

[16] C. Dahl and J. P. Pedersen, "Cyclic and pseudo-cyclic MDS codes of length $q+1$," *J. Comb. Theory A*, vol. 59, no. 1, pp. 130–133, Jan. 1992.

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

[18] P. Delsarte, J. M. Goethals, and F. J. MacWilliams, "On generalized Reed–Muller codes and their relatives," *Inf. Control*, vol. 16, no. 5, pp. 403–442, Jul. 1970.

[19] C. Ding, C. Li, and Y. Xia, "Another generalisation of the binary Reed–Muller codes and its applications," *Finite Fields Appl.*, vol. 53, pp. 144–174, Sep. 2018.

[20] C. Ding, Z. Sun, and X. Wang, "Two classes of constacyclic codes with variable parameters," in *Arithmetic Finite Field* (Lecture Notes in Computer Science), vol. 13638, S. Mesnager and Z. Zhou, Eds. Cham, Switzerland: Springer, 2022, pp. 127–141.

[21] C. Ding and C. Tang, *Designs from Linear Codes*, 2nd ed. Singapore: World Scientific, 2022.

[22] P. Ding and J. D. Key, "Subcodes of the projective generalized Reed–Muller codes spanned by minimum-weight vectors," *Des. Codes Cryptogr.*, vol. 26, nos. 1–3, pp. 197–211, Jun. 2002.

[23] X. Dong and S. Yin, "The trace representation of λ-constacyclic codes over $\mathbb{F}_{11}$," *J. Liaoning Normal Univ. Nat. Sci. Ed.*, vol. 33, no. 2, pp. 129–131, Jun. 2010.

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

[25] Y. Fu and H. Liu, "Galois self-orthogonal constacyclic codes over finite fields," *Designs, Codes Cryptogr.*, vol. 90, no. 11, pp. 2703–2733, Nov. 2022.

[26] J. Georgiades, "Cyclic $(q+1, k)$-codes of odd order q and even dimension k are not optimal," *Atti Sent. Mat. Fis. Univ. Modena*, vol. 30, pp. 284–285, 1982.

[27] M. Grassl. *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*. Accessed: Sep. 5, 2022. [Online]. Available: http://www.codetables.de

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

[29] 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.

[30] X. Kai, S. Zhu, and P. Li, "Constacyclic codes and some new quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2080–2086, Apr. 2014.

[31] X. Kai, S. Zhu, and P. Li, "A construction of new MDS symbol-pair codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 5828–5834, Nov. 2015.

[32] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892–4914, Nov. 2006.

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

[34] G. Lachaud, "Projective Reed–Muller codes," in *Coding Theory and Applications* (Lecture Notes in Computer Science), vol. 311. Berlin, Germany: Springer, 1988, pp. 125–129.

[35] 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.

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

[37] S. Li, "On the weight distribution of second order Reed–Muller codes and their relatives," *Designs, Codes Cryptogr.*, vol. 87, no. 10, pp. 2447–2460, Oct. 2019.

[38] S. Li and G. Ge, "Constructions of maximum distance separable symbol-pair codes using cyclic and constacyclic codes," *Designs, Codes Cryptogr.*, vol. 84, no. 3, pp. 359–372, Sep. 2017.

[39] 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, Mar. 2017.

[40] J. Luo and K. Feng, "Cyclic codes and sequences from generalized Coulter–Matthews function," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5345–5353, Dec. 2008.

[41] 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.

[42] D. E. Müller, "Application of Boolean algebra to switching circuit design and to error detection," *Trans. I.R.E. Prof. Group Electron. Comput.*, vol. EC-3, no. 3, pp. 6–12, Sep. 1954.

[43] V. Pless, "Symmetry codes over GF(3) and new five-designs," *J. Comb. Theory A*, vol. 12, no. 1, pp. 119–142, Jan. 1972.

[44] 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.

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

[46] F. R. F. Pereira, R. Pellikann, G. G. La Guardia, and F. M. de Assis, "Application of complementary dual AG codes to entanglement-assisted quantum codes," in *Proc. IEEE Int. Symp. Inform. Theory*, Paris, France, Jul. 2019, pp. 2559–2563.

[47] F. R. F. Pereira, R. Pellikaan, G. G. L. Guardia, and F. M. de Assis, "Entanglement-assisted quantum codes from algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 67, no. 11, pp. 7110–7120, Nov. 2021.

[48] I. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *IRE Prof. Group Inf. Theory*, vol. 4, no. 4, pp. 38–49, Sep. 1954.

[49] 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.

[50] M. Shi, X. Li, A. Neri, and P. Solé, "How many weights can a cyclic code have?" *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1449–1459, Mar. 2020.

[51] M. Shi, A. Neri, and P. Solé, "How many weights can a quasi-cyclic code have?" *IEEE Trans. Inf. Theory*, vol. 66, no. 11, pp. 6855–6862, Nov. 2020.

[52] M. Shi, L. Qian, L. Sok, and P. Solé, "On constacyclic codes over $\mathbb{Z}_4[u]/(u^2-1)$ and their Gray images," *Finite Fields Appl.*, vol. 45, pp. 86–95, May 2017.

[53] M. Shi and Y. Zhang, "Quasi-twisted codes with constacyclic constituent codes," *Finite Fields Appl.*, vol. 39, pp. 159–178, May 2016.

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

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

[56] Z. Sun, S. Huang, and S. Zhu, "Optimal quaternary Hermitian LCD codes and their related codes," *Designs, Codes Cryptogr.*, vol. 91, no. 4, pp. 1527–1558, Apr. 2023.

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

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

[59] Z. Sun, S. Zhu, and L. Wang, "Optimal constacyclic locally repairable codes," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 206–209, Feb. 2019.

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

[61] 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, Oct. 2019.

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

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

[64] A. Yardi and R. Pellikaan, "On shortened and punctured cyclic codes," 2017, *arXiv:1705.09859*.

[65] J. Yuan, S. Zhu, X. Kai, and P. Li, "On the construction of quantum constacyclic codes," *Designs, Codes Cryptogr.*, vol. 85, no. 1, pp. 179–190, Oct. 2017.

[66] 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.

Zhonghua Sun received the M.S. and Ph.D. degrees from the Hefei University of Technology, China, in 2016 and 2019, respectively. From 2021 to 2022, he was a Post-Doctoral Fellow with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology. From July 2023 to August 2023, he visited 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 of mathematics at Xidian University, Xi'an. He was an Assistant Professor of computer science with the National University of Singapore. In 2000, he joined The Hong Kong University of Science and Technology, Hong Kong, where he is currently a Professor of 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.

Xiaoqiang Wang received the B.S. degree in mathematics from Hubei Normal University, Huangshi, China, in 2012, the M.S. degree in applied mathematics from Hubei University, China, in 2015, and the Ph.D. degree in applied mathematics from Central China Normal University, China, in 2019. From 2017 to 2018, he visited the Department of Mathematical Sciences, Kent State University, Kent, OH, USA. From 2020 to 2021, he was a Post-Doctoral Fellow with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology. He is currently with Hubei University. His research interests include coding theory and cryptography.