Two Classes of Constacyclic Codes with Variable Parameters

Cunsheng Ding[1](✉) , Zhonghua Sun[2] , and Xiaoqiang Wang[3]

[1] Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China
cding@ust.hk

[2] School of Mathematics, Hefei University of Technology, Hefei 230601, Anhui, China

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

Abstract. Constacyclic codes over finite fields are a family of linear codes and contain cyclic codes as a subclass. Constacyclic codes are closely 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 extended abstract, 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 extended abstract.

Keywords: Constacyclic code · Cyclic code · Dilix code · Generalised Reed-Muller code · Projective Reed-Muller code

1 Introduction and Motivations

1.1 Constacyclic Codes and Cyclic Codes

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

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

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

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 $\mathcal{C} \subseteq \mathrm{GF}(q)^n$ 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 over $\mathrm{GF}(q)$, where $g(x)$ is monic and has the smallest degree. Then $g(x)$ is called the *generator poly-nomial* and $h(x) = (x^n - \lambda)/g(x)$ is referred to as the *check polynomial* of $\mathcal{C}$. The dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ is a λ^{-1}-constacyclic code generated by the reciprocal polyno-mial of the check polynomial $h(x)$ of $\mathcal{C}$. 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. For more information on constacyclic codes over finite fields, the reader is referred to [5–9, 13, 18, 20, 21, 24, 25, 27, 30–32, 35] and the references therein.

1.2   Motivations and Objectives

By definition, cyclic codes are a proper subclass of constacyclic codes and con-stacyclic codes are a proper subclass of linear codes. 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 alge-braic 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 $\gcd(m, q-1) = 1$, and is always monomially-equivalent to a contacyclic code over $\mathrm{GF}(q)$. This shows that the Hamming code is attractive. Notice that the two questions 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 $[n, k, d]$.

– The best $[n,k]$ constacyclic code over $\mathrm{GF}(q)$ has a better error-correcting capability than the best $[n,k]$ cyclic code over $\mathrm{GF}(q)$ for certain q, n and k.
– 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 as a constacyclic code, but cannot be constructed as a cyclic code when $\gcd(q - 1, m) \neq 1$.

The original binary Reed-Muller codes were introduced by Reed and Muller in 1954 [26,29]. 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. Binary Reed-Muller codes are also interesting in practice as they have efficient decoding algorithms [29]. 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 [10], which were called *Dilix codes* for the purpose of distinguishing the two types of generalisations [11, 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. Motivated by the punctured generalized Reed-Muller codes and punctured Dilix codes, the objective of this extended abstract is to construct and analyse two classes of constacyclic codes.

2   Preliminaries

Throughout this extended abstract, we fix the following notation, unless it is stated otherwise:

– q is a prime power.
– $m \geq 2$ is an integer.
– r is a positive divisor of $q - 1$.
– $N = q^m - 1$.

For a linear code $\mathcal{C}$, we use $\dim(\mathcal{C})$ and $d(\mathcal{C})$ to denote its dimension and minimum Hamming distance, respectively. For a linear code $\mathcal{C} \subset \mathrm{GF}(q)^n$, let A_i denote the number of codewords with Hamming weight i in $\mathcal{C}$. The *weight enumerator* of $\mathcal{C}$ defined as $1 + A_1 z + \cdots + A_n z^n$. 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.

2.1   The Hamming Weight and q-weight of Nonnegative Integers

Let $N = q^m - 1$. For each $i \in Z_N$, let the q-adic expansion of i be $i = \sum_{j=0}^{m-1} i_j q^j$, where $0 \le i_j \le q - 1$. 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 $\sum_{j=0}^{m-1} i_j$.

2.2   Cyclotomic Cosets

Let q be a prime power, 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 $m = \mathrm{ord}_{rn}(q)$. 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 $x^n - \lambda = \prod_{i \in \Gamma_{(q,rn,r)}^{(1)}} \mathbb{M}_{\beta^i}(x)$.

2.3   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 by 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 PAut($\mathcal{C}$).

A *monomial matrix* over GF(q) is a square matrix having exactly one nonzero element of 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 GF(q). Then $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be *monomially-equivalent* if there is a monomial matrix over 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 MAut($\mathcal{C}$), which is called the *monomial automorphism group* of $\mathcal{C}$. By definition, we have PAut($\mathcal{C}$) $\subseteq$ MAut($\mathcal{C}$). Two linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of the same length over GF(q) are said to be *scalar-equivalent* if there is an invertible diagonal matrix D over 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 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 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, PAut($\mathcal{C}$), MAut($\mathcal{C}$) and Aut($\mathcal{C}$) are the same. If q is a prime, MAut($\mathcal{C}$) and Aut($\mathcal{C}$) are identical. In general, we have

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

In this extended abstract, 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 $\mathcal{C}_1$, we prefer $\mathcal{C}_1$ to $\mathcal{C}$ as constacyclic codes have a better algebraic structure than general linear codes.

2.4   The Projective Reed-Muller Codes

Let q be a power of a prime p and let $m \geq 2$. A point of the projective geometry PG($m-1$, GF(q)) is given in homogeneous coordinates by $(x_1, x_2, \ldots, x_m)$ where all x_i are in GF(q) and are not all zero. Each point of PG($m-1$, GF(q)) has $q-1$ coordinate representations, as $(ax_1, x_2, ..., ax_m)$ and $(x_1, x_2, ..., x_m)$ generate the same 1-dimensional subspace of GF(q)^m for any nonzero $a \in$ GF(q).

Let GF(q)$[x_1, x_2, \ldots, x_m]$ be the set of polynomials in m indeterminates over GF(q), which is a linear space over GF(q). Let $A(q, m, h)$ be the subspace of GF(q)$[x_1, x_2, \ldots, x_m]$ generated by all the homogeneous polynomials of degree h. Let $\{\mathbf{x}^1, \mathbf{x}^2, \cdots, \mathbf{x}^n\}$ be a set of projective points in PG($m-1$, GF(q)), where $n = (q^m - 1)/(q - 1)$. Then, the *h-th order projective Reed-Muller code* PRM(q, m, h) of length n is defined by

$$\text{PRM}(q, m, h) = \left\{ \left(f(\mathbf{x}^1), f(\mathbf{x}^2), \ldots, f(\mathbf{x}^n) \right) : f \in A(q, m, h) \right\}.$$

The code $\text{PRM}(q, m, h)$ 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 $\text{PG}(m - 1, \text{GF}(q))$, but is unique up to monomial equivalence (in fact, up to scalar equivalence). The parameters of $\text{PRM}(q, m, h)$ are known and documented in the following theorem [3,19,34].

Theorem 1. *Let $m \geq 2$ and $1 \leq h \leq (m - 1)(q - 1)$. Then the linear code $\text{PRM}(q, m, h)$ 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,*

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

By Theorem 1 and definition, $\text{PRM}(q, m, 1)$ is monomially-equivalent to the Simplex code. The weight distribution of $\text{PRM}(q, m, 2)$ was settled in [22]. It was pointed out in [4] that the code $\text{PRM}(q, m, h)$ is not cyclic in general, but could be cyclic or quasi-cyclic under special conditions. Later in this extended abstract, 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.

2.5 Projective Generalized Reed-Muller Codes

For an integer $h \geq 0$, let $\text{PP}(q, m, h)$ be the linear subspace of $\text{GF}(q)[x_1, x_2, \ldots, x_m]$, which is spanned by all monomials $x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}$ satisfying the following two conditions:

1. $\sum_{j=1}^{m} i_j \equiv 0 \pmod{q - 1}$,
2. $\sum_{j=1}^{m} i_j \leq h(q - 1)$.

Each $a \in \text{GF}(q)$ is viewed as the constant function $f_a(x_1, x_2, \ldots, x_m) \equiv a$.

Let $\{\mathbf{x}^1, \mathbf{x}^2, \ldots, \mathbf{x}^n\}$ be the set of projective points in $\text{PG}(m - 1, \text{GF}(q))$, where $n = \frac{q^m - 1}{q - 1}$. Then, the *h-th order projective generalized Reed-Muller code* $\text{PGRM}(q, m, h)$ of length n is defined by

$$\text{PGRM}(q, m, h) = \left\{ \left(f(\mathbf{x}^1), f(\mathbf{x}^2), \ldots, f(\mathbf{x}^n) \right) : f \in \text{PP}(q, m, h) \right\}.$$

Theorem 2. *Let $0 \leq h \leq m - 1$. Then, the minimum weight of $\text{PGRM}(q, m, h)$ is $\frac{q^{m-h} - 1}{q - 1}$ and*

$$\dim(\text{PGRM}(q, m, h)) = \left| \left\{ 0 \leq j \leq \frac{q^m - 1}{q - 1} : \text{wt}_q(j(q - 1)) \leq h(q - 1) \right\} \right|. \quad (1)$$

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

Example 1. The parameters of the codes PGRM$(3, 4, h)$ for $0 \leq h \leq 3$ are given below.

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

2.6 The Punctured Dilix Codes

In this subsection, we outline a type of cyclic codes, called *punctured Dilix codes* [10]. Let m be a positive integer and let $N = q^m - 1$, where q is a prime power. Let β be a primitive element of GF(q^m). For any $1 \leq h \leq m$, we define a polynomial

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

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

Theorem 3. *[10] Let $m \geq 2$ and $1 \leq h \leq m-1$. Then $\Omega(q, m, h)$ has parameters $[N, k, d \geq (q^{h+1} - 1)/(q - 1)]$, where*

$$k = q^m - \sum_{i=0}^{h} \binom{m}{i} (q - 1)^i.$$

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.

3 A General Construction of Constacyclic Codes of Length $\frac{q^m - 1}{r}$ with Cyclic Codes of Length $q^m - 1$

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

Let $\mathcal{C}$ be a cyclic code of length N over 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 GF(q^m). Put

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

If $\underline{D}(\mathcal{C}) = \emptyset$, then define $\underline{g}(x) = 1$. If $\underline{D}(\mathcal{C}) \neq \emptyset$, then 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 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 GF(q) with generator polynomial $\underline{g}(x)$. By definition, $\underline{\mathcal{C}}$ is constructed from the given cyclic code $\mathcal{C}$.
    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. By definition, there is no clear connection between $d(\underline{\mathcal{C}})$ and $d(\mathcal{C})$ in general.
    Later in this extended abstract, we will use this general construction to obtain two classes of λ-constacyclic codes of length $(q^m - 1)/(q-1)$ over GF(q). Specifically, we will consider only the special case $r = q - 1$ in this extended abstract.

Example 2. Let $q > 2$ be a prime power and let $m \geq 2$ and $r = q - 1$. Let β be a primitive element of GF(q^m) and $\lambda = \beta^{(q^m-1)/(q-1)}$. Let $\mathcal{C}$ denote the cyclic code of length $N = q^m - 1$ with generator polynomial $g(x) = \mathbb{M}_\beta(x)\mathbb{M}_{\beta^{q+1}}(x)$. It is easily seen that $\underline{D}(\mathcal{C}) = C_1^{(q,N)}$ and $\underline{g}(x) = \mathbb{M}_\beta(x)$. Then the λ-constacyclic code $\underline{\mathcal{C}}$ is the Hamming code and $\underline{\mathcal{C}}^\perp$ is the Simplex code.

4   The First Class of Constacyclic Codes

We follow the previous notation. Throughout this section, let $n = \frac{q^m-1}{q-1}$, where m is an integer with $m \geq 2$. Define $N = rn = q^m - 1$, where $r = q - 1$. Then it is easily seen 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

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

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

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

Let

$$D'_{(q,m,\ell)} = \bigcup_{\substack{i \in \Gamma^{(1)}_{(q,N,q-1)} \\ 1 \le \mathtt{wt}(i) \le \ell}} C_i^{(q,N)}.$$

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

Theorem 4. *Let $1 \le \ell \le m-1$. Then*

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

and

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

Theorem 5. *Let $1 \le \ell \le m-1$ and $q \ge 3$. Then*

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

and

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

Corollary 1. *Let $m \ge 2$. Then the constacyclic code $\mathcal{C}'(q,m,1)$ has parameters*

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

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

Let $\Omega(q,m,\ell)$ denote the punctured Dilix code constructed in [10] (see also Sect. 2.6). Theorem 4 tells us that

$$\dim(\Omega(q,m,\ell)) = (q-1)\dim(\mathcal{C}'(q,m,\ell)).$$

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

Open Problem 6. *Determine the minimum distance of* $\mathcal{C}'(q, m, \ell)$ *or improve the lower 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 7. *Determine the minimum distance of* $\mathcal{C}'(q, m, \ell)^{\perp}$ *or improve the lower bound in* (3) *for* $2 \leq \ell \leq m - 1$.

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

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

Example 5. Let $(q, m, \ell) = (3, 4, 3)$. Let β be the primitive element of $\mathrm{GF}(3^4)$ with $\beta^4 + 2\beta^3 + 2 = 0$. Then the code $\mathcal{C}'(q, m, \ell)$ has parameters $[40, 8, 21]$ and has the best parameters known [16], and $\mathcal{C}'(q, m, \ell)^{\perp}$ has parameters $[40, 32, 4]$.

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

By Corollary 1, $\mathcal{C}'(q, m, 1)^{\perp}$ 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 $\mathcal{C}'(q, m, \ell)$ 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 1 that

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

By Example 4, $d(\mathcal{C}'(3, 4, 2)) = 8$ and $d(\mathcal{C}'(3, 4, 2)^{\perp}) = 12$. This means that both $\mathcal{C}'(3, 4, 2)$ and $\mathcal{C}(3, 4, 2)^{\perp}$ 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 $\mathcal{C}'(q, m, \ell)$ and $\mathrm{PRM}(q, m, \ell)$ are different in general. Notice that $\mathcal{C}'(2, m, \ell)$ and the punctured Dilix code $\Omega(2, m, \ell)$ are identical. But $\mathcal{C}'(q, m, \ell)$ 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 PGRM$(3, 4, \ell)$ in Example 1, both $\mathcal{C}'(3, 4, 2)$ and $\mathcal{C}'(3, 4, 2)^\perp$ cannot be monomially-equivalent to a code PGRM$(3, 4, \ell)$ for all ℓ with $0 \leq \ell \leq 3$. Hence, the class of codes $\mathcal{C}'(q, m, \ell)$ and the class of codes PGRM(q, m, ℓ) are different.

5   The Second Class of Constacyclic Codes

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

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

5.1   Definition and Basic Properties of the Constacyclic Codes

Let β be a primitive element of $\text{GF}(q^m)$ and let $\lambda = \beta^{(q^m-1)/(q-1)}$. Then λ is a primitive element of $\text{GF}(q)$. Let ℓ be a positive integer with $0 \leq \ell < (q-1)m-1$. Define

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

Let

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

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

Lemma 1. *Let $m \geq 2$ and $q \geq 3$. Then $\mathcal{C}(q, m, \ell) = \{\mathbf{0}\}$ for all ℓ with $1 \leq \ell \leq q - 3$. Furthermore, $\mathcal{C}(q, m, (q-1)u + q - 2) = \mathcal{C}(q, m, (q-1)(u+1) + v)$ for all $0 \leq u \leq m - 2$ and $0 \leq v \leq q - 3$.*

This lemma shows that this class of constacyclic codes $\mathcal{C}(q, m, \ell)$ contain only the following distinct nonzero codes:

$$\mathcal{C}(q, m, (q-1)u + q - 2), \quad 0 \leq u \leq m - 2.$$

Theorem 8. *Let $m \geq 2$, $q \geq 3$ and $0 \leq u \leq m-2$. Then $\mathcal{C}(q, m, (q-1)u+q-2)$ is monomially-equivalent to $\mathrm{PRM}(q, m, (q-1)u+q-2)$. Consequently,*

$$\dim(\mathcal{C}(q, m, (q-1)u+q-2)) = \sum_{\substack{t \equiv q-2 \pmod{q-1} \\ 0 < t \leq (q-1)u+q-2}} \left(\sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{t-jq+m-1}{t-jq} \right),$$

and

$$d(\mathcal{C}(q, m, (q-1)u+q-2)) = 3q^{m-2-u}.$$

The main contribution of this section is Theorem 8, which shows that the projective Reed-Muller code $\mathrm{PRM}(q, m, \ell)$ has a constacyclic code construction when $\ell = (q-1)u + q - 2$ for any u with $0 \leq u \leq m - 2$ up to monomial equivalence. However, the following question is still open.

Open Problem 9. *Is $\mathrm{PRM}(q, m, \ell)$ monomially-equivalent to a constacyclic code when $\ell \not\equiv q - 2 \pmod{q - 1}$ and $q - 2 \leq \ell \leq (m - 1)(q - 1)$?*

5.2   Some Special Cases of the Code $\mathcal{C}(q, m, \ell)$

In this subsection, we study the code $\mathcal{C}(q, m, \ell)$ in some special cases. The code is very interesting in some special cases.

Corollary 2. *Let $q \geq 3$ and $m \geq 2$. Then $\mathcal{C}(q, m, (q-1)(m-2)+q-2)$ has parameters*

$$\left[\frac{q^m - 1}{q - 1}, \frac{q^m - 1}{q - 1} - m, 3 \right]$$

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

$$\left[\frac{q^m - 1}{q - 1}, m, q^{m-1} \right]$$

and is monomially-equivalent to the Simplex code.

Corollary 3. *Let $m \geq 2$. Then $\mathcal{C}(4, m, 2)$ has parameters*

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

and $\mathcal{C}(4, m, 2)^{\perp}$ has parameters

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

The following four examples show that $\mathcal{C}(4, m, 2)$ is a $(m + 1)$-weight code for even m and m-weight code for odd m.

Example 6. Let $(q, m, \ell) = (4, 2, 2)$. Let β be the primitive element of $\mathrm{GF}(4^2)$ with $\beta^4 + \beta + 1 = 0$. Then $\mathcal{C}(4, 2, 2)$ has parameters $[5, 3, 3]$ and weight enumerator $1 + 30z^3 + 15z^4 + 18z^5$. Furthermore, $\mathcal{C}(4, 2, 2)^\perp$ has parameters $[5, 2, 4]$. Both codes are MDS and optimal.

Example 7. Let $(q, m, \ell) = (4, 3, 2)$. Let β be the primitive element of $\mathrm{GF}(4^3)$ with $\beta^6 + \beta^4 + \beta^3 + \beta + 1 = 0$. Then $\mathcal{C}(4, 3, 2)$ has parameters $[21, 6, 12]$ and weight enumerator
$$1 + 630z^{12} + 3087z^{16} + 378z^{20}.$$
Notice that the code $\mathcal{C}(4, 3, 2)$ is distance-optimal [16]. Furthermore, $\mathcal{C}(4, 3, 2)^\perp$ has parameters $[21, 15, 4]$ and is almost-distance optimal [16].

Example 8. Let $(q, m, \ell) = (4, 3, 5)$. Let β be the primitive element of $\mathrm{GF}(4^3)$ with $\beta^6 + \beta^4 + \beta^3 + \beta + 1 = 0$. Then the code $\mathcal{C}(q, m, \ell)$ has parameters $[21, 18, 3]$ and is distance-optimal [16], and $\mathcal{C}(q, m, \ell)^\perp$ has parameters $[21, 3, 16]$ and is distance-optimal [16].

Example 9. Let $(q, m, \ell) = (4, 3, 4)$. Let β be the primitive element of $\mathrm{GF}(4^3)$ with $\beta^6 + \beta^4 + \beta^3 + \beta + 1 = 0$. Then the code $\mathcal{C}(q, m, \ell)$ has parameters $[21, 6, 12]$ and is distance-optimal [16], and $\mathcal{C}(q, m, \ell)^\perp$ has parameters $[21, 15, 4]$.

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

5.3 The Difference Between the Codes $\mathcal{C}(q, m, \ell)$ and the Codes PGRM(q, m, h)

According to Theorem 2, $\mathcal{C}(3, 4, 5)$ has minimum distance 3. By Example 1, none of the codes PGRM$(3, 4, h)$ for $0 \leq h \leq 3$ has minimum distance 3. Consequently, the class of codes $\mathcal{C}(q, m, \ell)$ and the class of codes PGRM(q, m, h) are different.

6 Summary and Concluding Remarks

The main contributions of this extended abstract are the constructions and analyses of the two classes of constacyclic codes $\mathcal{C}'(q, m, \ell)$ and $\mathcal{C}(q, m, \ell)$. The codes are interesting in theory as they contain optimal codes and codes with best-known parameters and they are constacyclic. In addition, the codes $\mathcal{C}'(q, m, \ell)$ are new, and the codes $\mathcal{C}(q, m, \ell)$ give a costacyclic-code construction of some projective Reed-Muller codes. It would be very interesting to settle the open problems presented in this extended abstract and determine the automorphism groups of the first class of constacyclic codes $\mathcal{C}'(q, m, \ell)$.

References

1. Abdukhalikov, K., Ho, D.: Extended cyclic codes, maximal arcs and ovoids. Des. Codes Crypt. **89**(10), 2283–2294 (2021). https://doi.org/10.1007/s10623-021-00915-2

2. Assmus, E.F., Jr., Key, J.D.: Polynomial codes and finite geometries. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, vol. II, pp. 1269–1343. Elsevier, Amsterdam (1998)

3. Ballet, S., Rolland, R.: On low weight codewords of generalized affine and projective Reed-Muller codes. Des. Codes Cryptogr. **73**, 271–297 (2014)

4. Berger, T.P., de Maximy, L.: Cyclic projective reed-muller codes. In: Boztaş, S., Shparlinski, I.E. (eds.) AAECC 2001. LNCS, vol. 2227, pp. 77–81. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45624-4_8

5. Blackford, E.R.: Negacyclic codes for the Lee metric. In: Proceedings of the Conference on Combinatorial Mathematics and its Applications, pp. 298–316. Chapel Hill, NC (1968)

6. Chen, B., Dinh, H.Q., Fan, Y., Ling, S.: Polyadic constacyclic codes. IEEE Trans. Inf. Theory **61**(9), 4895–4904 (2015)

7. Chen, B., Fan, Y., Lin, L., Liu, H.: Constacyclic codes over finite fields. Finite Fields Appl. **18**, 1217–1231 (2012)

8. Dahl, C., Pedersen, J.P.: Cyclic and pseudo-cyclic MDS codes of length $q + 1$. J. Comb. Theory Ser. A **59**, 130–133 (1992)

9. Danev, D., Dodunekov, S., Radkova, D.: A family of constacyclic ternary quasi-perfect codes with covering radius 3. Des. Codes Cryptogr. **59**, 111–118 (2011)

10. Ding, C., Li, C., Xia, Y.: Another generalization of the Reed-Muller codes. Finite Fields Appl. **53**, 147–174 (2018)

11. Ding, C., Tang, C.: Designs from Linear Codes, 2nd edn. World Scientific, Singapore (2022)

12. Ding, P., Key, J.D.: Subcodes of the projective generalized Reed-Muller codes spanned by minimum-weight vectors. Des. Codes Cryptogr. **26**, 197–211 (2002)

13. Dong, X., Yin, S.: The trace representation of λ-constacyclic codes over $\mathbb{F}_q$. J. Liaoning Normal Univ. (Nat. Sci. ed.) **33**, 129–131 (2010)

14. Fang, W., Wen, J., Fu, F.: A q-polynomial approach to constacyclic codes. Finite Fields Appl. **47**, 161–182 (2017)

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

16. Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. http://www.codetables.de

17. Huffman, W.C., Pless, V.: Fundamentals of Error Correcting Codes. Cambridge University Press, Cambridge (2003)

18. Krishna, A., Sarwate, D.V.: Pseudocyclic maximum-distance-separable codes. IEEE Trans. Inf. Theory **36**(4), 880–884 (1990)

19. Lachaud, G.: Projective reed-muller codes. In: Cohen, G., Godlewski, P. (eds.) Coding Theory 1986. LNCS, vol. 311, pp. 125–129. Springer, Heidelberg (1988). https://doi.org/10.1007/3-540-19368-5_13

20. Li, F., Yue, Q., Liu, F.: The weight distribution of constacyclic codes. Adv. Math. Commun. **11**(3), 471–480 (2017)

21. Li, F., Yue, Q.: The primitive idempotents and weight distributions of irreducible constacyclic codes. Des. Codes Cryptogr. **86**, 771–784 (2018)

22. Li, S.: On the weight distribution of second order Reed-Muller codes and their relatives. Des. Codes Cryptogr. **87**, 2447–2460 (2019)
23. Lidl, R., Niederreiter, H.: Finite Fields. Addison-Wesly, New York (1983)
24. Liu, Y., Li, R., Lv, L., Ma, Y.: A class of constacyclic BCH codes and new quantum codes. Quantum Inf. Process. **16**(3), 1–16 (2017). https://doi.org/10.1007/s11128-017-1533-y
25. Mi, J., Cao, X.: Constructing MDS Galois self-dual constacyclic codes over finite fields. Discret. Math. **334**(6), 1–15 (2021)
26. Muller, D.E.: Application of boolean algebra to switching circuit design and to error detection. IEEE Trans. Comput. **3**, 6–12 (1954)
27. Pedersen, J.P., Dahl, C.: Classification of pseudo-cyclic MDS codes. IEEE Trans. Inf. Theory **37**(2), 365–370 (1991)
28. Peterson, W.W., Weldon, E.J., Jr.: Error-Correcting Codes, 2nd edn. MIT Press, Cambridge (1972)
29. Reed, I.S.: A class of multiple-error-correcting codes and the decoding scheme. IRE Trans. Inf. Theory **4**, 38–49 (1954)
30. Wang, L., Sun, Z., Zhu, S.: Hermitian dual-containing narrow-sense constacyclic BCH codes and quantum codes. Quantum Inf. Process. **18**(10), 1–40 (2019). https://doi.org/10.1007/s11128-019-2440-1
31. Wolfmann, J.: Projective two-weight irreducible cyclic and constacyclic codes. Finite Fields Appl. **14**(2), 351–360 (2008)
32. Sharma, A., Rani, S.: Trace description and Hamming weights of irreducible constacyclic codes. Adv. Math. Commun. **12**(1), 123–141 (2018)
33. Shi, Z., Fu, F.: The primitive idempotents of irreducible constacyclic codes and LCD cyclic codes. Cryptogr. Commun. **12**, 29–52 (2020)
34. Sørensen, A.: Projective Reed-Muller codes. IEEE Trans. Inf. Theory **37**(6), 1567–1576 (1991)
35. Sun, S., Zhu, S., Wang, L.: A class of constacyclic BCH codes. Cryptogr. Commun. **12**, 265–284 (2020)
36. Zhu, S., Sun, Z., Li, P.: A class of negacyclic BCH codes and its application to quantum codes. Des. Codes Cryptogr. **86**(10), 2139–2165 (2018)