Several families of irreducible constacyclic and cyclic codes

Zhonghua Sun · Xiaoqiang Wang · Cunsheng Ding

Received: 28 October 2022 / Revised: 16 April 2023 / Accepted: 2 May 2023 / Published online: 16 May 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract
In this paper, several families of irreducible constacyclic codes over finite fields and their duals are studied. The weight distributions of these irreducible constacyclic codes and the parameters of their duals are settled. Several families of irreducible constacyclic codes with a few weights and several families of optimal constacyclic codes are constructed. As by-products, a family of \([2n, (n - 1)/2, d \geq 2(\sqrt{n} + 1)]\) irreducible cyclic codes over \(GF(q)\) and a family of \([{(q - 1)n, (n - 1)/2, d \geq (q - 1)(\sqrt{n} + 1)}]\) irreducible cyclic codes over \(GF(q)\) are presented, where \(n\) is a prime such that \(\text{ord}_{2n}(q) = (n - 1)/2\) and \(\text{ord}_{(q-1)n}(q) = (n - 1)/2\), respectively. The results in this paper complement earlier works on irreducible constacyclic and cyclic codes over finite fields.

Keywords Constacyclic code · Irreducible constacyclic code · Irreducible cyclic code · Weight distribution

Mathematics Subject Classification 94B05 · 94B15

Communicated by G. Ge.

Xiaoqiang Wang and Cunsheng Ding have contributed equally to this work.

Zhonghua Sun
sunzhonghuas@163.com

Xiaoqiang Wang
waxiqq@163.com

Cunsheng Ding
cding@ust.hk

1 School of Mathematics, Hefei University of Technology, Hefei 230601, Anhui, China
2 Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, Hubei, China
3 Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China
1 Introduction and motivations

1.1 Constacyclic codes and cyclic codes

Let GF\((q)\) denote the finite field with \(q\) elements, and let GF\((q)^*\) denote the multiplicative group of GF\((q)\). An \([n, k, d]\) code \(C\) over GF\((q)\) is a \(k\)-dimensional linear subspace of GF\((q)^n\) with minimum distance \(d\). Let \(\lambda \in \text{GF}(q)^*\). A linear code \(C\) of length \(n\) is said to be \(\lambda\)-constacyclic if \((c_0, c_1, \ldots, c_{n-1}) \in C\) implies \((\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C\). Let \(\Phi\) be the mapping from GF\((q)^n\) to the quotient ring GF\((q)[x]/(x^n - \lambda)\) defined by

\[
\Phi(c_0, c_1, \ldots, c_{n-1}) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}.
\]

It is known that every ideal of GF\((q)[x]/(x^n - \lambda)\) is principal and a linear code \(C \subseteq \text{GF}(q)^n\) is \(\lambda\)-constacyclic if and only if \(\Phi(C)\) is an ideal of GF\((q)[x]/(x^n - \lambda)\). Due to this, we will identify \(C\) with \(\Phi(C)\) for any \(\lambda\)-constacyclic code \(C\). Let \(C = (g(x))\) be a \(\lambda\)-constacyclic code over 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 \(C\). A \(\lambda\)-constacyclic code \(C\) over GF\((q)\) is said to be irreducible if its check polynomial is irreducible over GF\((q)\). The dual code \(C^\perp\) of \(C\) is generated by the reciprocal polynomial of the check polynomial \(h(x)\) of \(C\). 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, the reader is referred to [2–6, 10, 16–18, 20, 21, 23, 28–30] and the references therein.

For a linear code \(C \subseteq \text{GF}(q)^n\), let \(A_i\) denote the number of codewords with Hamming weight \(i\) in \(C\). The weight enumerator of \(C\) is 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 \(C\). If the number of nonzero \(A_j\) in the sequence \((A_1, A_2, \ldots, A_n)\) equals \(N\), then \(C\) is called an \(N\)-weight code. The weight distribution of a code contains important information on its error detection and correction with respect to some algorithms [15]. It is well known that determining the weight distribution of a linear code is a difficult work in general, and there are a lot of references on the weight distribution of cyclic codes. For the weight distribution of irreducible cyclic codes, the reader is referred to [9] and the references therein.

1.2 Motivations and objectives

Constacyclic codes over finite fields are of theoretical importance as they are closely related to a number of areas of mathematics such as algebra, algebraic geometry, graph theory, combinatorial designs and number theory. The following remarks show that constacyclic codes have advantages over cyclic codes.

1. MDS cyclic codes over GF\((q)\) with length \(q + 1\) and even dimension do not exist [12], but MDS constacyclic codes over GF\((q)\) with length \(q + 1\) and even dimension do exist [16].
2. The Hamming code over GF\((q)\) with parameters \([(q^m - 1)/(q - 1), (q^m - 1)/(q - 1) - m, 3]\), here and hereafter denoted by Hamming\((q, m)\), is a perfect code. The dual of a Hamming code is the Simplex code, denoted by Simplex\((q, m)\). The Simplex code is a one-weight code and is optimal in the sense that it meets the Griesmer bound. If \(\gcd(m, q - 1) = 1\), the Hamming code Hamming\((q, m)\) is monomially-equivalent to the dual code of a cyclic code over GF\((q)\), and the Simplex code Simplex\((q, m)\) is monomially-equivalent to a cyclic code over GF\((q)\). However, this conclusion is not true.
when \( \gcd(q - 1, m) > 1 \). For example, the \([4, 2, 3]\) ternary Hamming code documented in [14, Example 5.1.6] is not monomially-equivalent to a ternary cyclic code. But there is an irreducible \( \lambda \)-constacyclic code over \( \text{GF}(q) \) which is monomially-equivalent to the Simplex code Simplex \((q, m)\), and its dual code is monomially-equivalent to the Hamming code Hamilton \((q, m)\) [11, 13], where \( \lambda \) is a primitive element of \( \text{GF}(q) \).

3. Any \([q^2 + 1, 4, q^2 - q]\) code over \( \text{GF}(q) \) is called an \textit{ovoid code}. Ovoid codes are two-weight codes, and are optimal in the sense that they meet the Griesmer bound. The dual code of a \([q^2 + 1, 4, q^2 - q]\) ovoid code has parameters \([q^2 + 1, q^2 - 3, 4]\) and is distance-optimal. Ovoid codes and their duals can be employed to construct 3-designs and inversive planes [8, Chapter 13]. Some subfield codes of ovoid codes are optimal [7]. It is known that an ovoid code corresponds to an ovoid in the projective space \( \text{PG}(3, \text{GF}(q)) \). So far the elliptic quadrics and the Tits ovoids are the only known two families of ovoids up to equivalence. The elliptic quadric in \( \text{PG}(3, \text{GF}(2^m)) \) can be constructed with an irreducible cyclic code over \( \text{GF}(2^m) \) [1, 8]. However, the elliptic quadric in \( \text{PG}(3, \text{GF}(p^m)) \) for odd \( p \) cannot be constructed with any cyclic code over \( \text{GF}(p^m) \), but can be constructed with an irreducible constacyclic code [8, Chapter 13].

The above remarks show that constacyclic codes can do certain things that cyclic codes cannot. Therefore, it is very interesting to study constacyclic codes.

Constacyclic codes over finite fields are a subclass of the \textit{pseudo-cyclic codes} over finite fields defined in [24, Section 8.10], and were studied under the name of pseudo-cyclic codes. Negacyclic codes over finite fields are a subclass of constacyclic codes, and were first studied by Berlekamp [2] for correcting errors measured in the Lee metric. Therefore, the history of constacyclic codes goes back to 1966. In the past 56 years, only a few references on irreducible constacyclic codes have appeared in the literature [13, 17, 18, 25–28, 30, 31]. It was shown in [25] that the weight distributions of irreducible constacyclic codes can be described in terms of the Gaussian periods of certain order \( L \). However, Gaussian periods have been evaluated only for a few orders \( L \). Hence, very limited results on the parameters and weight distributions of irreducible constacyclic codes over finite fields are known in the literature.

The objectives of this paper are the following:

1. Study parameters of some families of irreducible constacyclic codes.
2. Study parameters of the dual of these irreducible constacyclic codes.

The main results of this paper are the following:

1. The weight distributions of several families of irreducible constacyclic codes and the parameters of their duals are settled (see Theorems 4 and 6 and their corollaries).
2. Several infinite families of optimal constacyclic codes are presented in this paper (see Theorem 4).
3. A family of \([2n, (n - 1)/2, d \geq 2(\sqrt{n} + 1)]\) irreducible cyclic codes over \( \text{GF}(q) \) and a family of \([((q - 1)n, (n - 1)/2, d \geq (q - 1)(\sqrt{n} + 1)]\) irreducible cyclic codes over \( \text{GF}(q) \) are constructed, where \( n \) is a prime such that \( \text{ord}_{2n}(q) = (n - 1)/2 \) and \( \text{ord}_{(q - 1)n}(q) = (n - 1)/2 \), respectively (see Theorems 8 and 10).

### 1.3 The organization of this paper

The rest of this paper is organized as follows. In Sect. 2, we present some auxiliary results. In Sect. 3, we associate three linear codes to an irreducible constacyclic code and establish relations among the four codes. In Sect. 4, we study the parameters of irreducible constacyclic
codes, and determine the weight distributions of some families of irreducible constacyclic codes. In Sect. 5, we present a family of \([2n, (n - 1)/2, d \geq 2(\sqrt{n} + 1)]\) irreducible cyclic codes. In Sect. 6, we document a family of \([(q - 1)n, (n - 1)/2, d \geq (q - 1)(\sqrt{n} + 1)]\) irreducible cyclic codes. In Sect. 7, we present the objective of studying the two families of constacyclic codes in Sects. 5 and 6. In Sect. 8, we conclude this paper and make some concluding remarks.

2 Preliminaries

2.1 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 \(\lambda\) be an element of \(\text{GF}(q)\) with order \(r\). To deal with \(\lambda\)-constacyclic codes of length \(n\) over \(\text{GF}(q)\), we have to study the factorization of \(x^n - \lambda\) over \(\text{GF}(q)\). To this end, we need to introduce \(q\)-cyclotomic cosets modulo \(rn\).

Let \(\mathbb{Z}_{rn} = \{0, 1, 2, \ldots, rn - 1\}\) 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

\[
C_i^{(q, rn)} = \{i, iq, iq^2, \ldots, iq^{\ell_i - 1}\} \mod rn \subseteq \mathbb{Z}_{rn},
\]

where \(\ell_i\) is the smallest positive integer such that \(i \equiv iq^{\ell_i} \pmod{rn}\), and is the size of the \(q\)-cyclotomic coset. 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 \(\bigcup_{i \in \Gamma_{(q, rn)}} C_i^{(q, rn)} = \mathbb{Z}_{rn}\).

For any positive integer \(N\) with \(\gcd(q, N) = 1\), let \(\text{ord}_N(q)\) denote the multiplicative order of \(q\) modulo \(N\). Let \(m = \text{ord}_n(q)\). It is easily seen that there is a primitive element \(\alpha\) of \(\text{GF}(q^m)\) such that \(\beta = \alpha^{(q^m - 1)/rn}\) and \(\beta^rn = \lambda\). Then \(\beta\) is a primitive \(rn\)-th root of unity in \(\text{GF}(q^m)\). The minimal polynomial \(M_{\beta^i}(x)\) of \(\beta^i\) over \(\text{GF}(q)\) is a monic polynomial of the smallest degree over \(\text{GF}(q)\) with \(\beta^i\) as a zero. We have \(M_{\beta^i}(x) = \prod_{j \in C_i^{(q, rn)}} (x - \beta^j) \in \text{GF}(q)[x]\), which is irreducible over \(\text{GF}(q)\). It then follows that \(x^{rn} - 1 = x^{rn} - \lambda^r = \prod_{i \in \Gamma_{(q, rn)}} M_{\beta^i}(x)\).

Define

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

Then \(x^n - \lambda = \prod_{i \in \Gamma_{(q, rn)}^{(1)}} M_{\beta_i}(x)\).

**Lemma 1** Let \(n\) be a positive integer with \(\gcd(q, n) = 1\) and let \(r\) be a positive divisor of \(q - 1\). If \(\text{ord}_n(q) = \ell\), then \(\text{ord}_{rn}(q) = \frac{r}{\gcd(\ell, rn)}\), which is the size \(\ell_1\) of \(C_1^{(q, rn)}\), and the size \(\ell_i\) of each \(q\)-cyclotomic coset \(C_i^{(q, rn)}\) is a divisor of \(\text{ord}_{rn}(q)\).

**Proof** Since \(r\) is a divisor of \(q - 1, \gcd(q, r) = 1\). Consequently, \(\gcd(q, rn) = 1\). It is clear that \(\text{ord}_n(q)\) divides \(\text{ord}_{rn}(q)\). Suppose \(\text{ord}_{rn}(q) = s\ell\). Then \(s\) is the smallest positive integer such that \(q^{s \ell} \equiv 1 \pmod{rn}\). Clearly, \(q^{s \ell} \equiv 1 \pmod{rn}\) if and only if

\[
\left(\frac{q^{s \ell} - 1}{n}\right) = \left(\frac{q^{\ell} - 1}{n}\right) = s \equiv 0 \pmod{r}.
\]
Hence, \( s = \frac{r}{\gcd\left(\frac{q^r - 1}{q - 1}, r\right)} \), i.e., \( \text{ord}_{rn}(q) = \frac{r}{\gcd\left(\frac{q^r - 1}{q - 1}, r\right)} \ell \). The desired second conclusion is well known and its proof is thus omitted here. \(\square\)

### 2.2 Bounds of linear codes and Pless power moments

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

**Lemma 2** (Sphere Packing Bound [14]) Let \( C \) be an \([n, k, d]\) code over \( \text{GF}(q) \), then

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

where \([\cdot]\) is the floor function.

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

**Lemma 3** [11] Let \( C \) be an \([n, k, d]\) code over \( \text{GF}(q) \), where \( d \) is an even integer. Then

\[
\sum_{i=0}^{[d^2-2]/4} \binom{n-1}{i} (q-1)^i \leq q^{n-1-k}.
\]

An \([n, k, d]\) code over \( \text{GF}(q) \) is said to be distance-optimal if there is no \([n, k, d']\) code over \( \text{GF}(q) \) with \( d' > d \). An \([n, k, d]\) code over \( \text{GF}(q) \) is said to be dimension-optimal if there is no \([n', k, d]\) code over \( \text{GF}(q) \) with \( k' > k \). An \([n, k, d]\) code over \( \text{GF}(q) \) is said to be length-optimal if there is no \([n', k, d]\) code over \( \text{GF}(q) \) with \( n' < n \). A linear code is said to be optimal if it is distance-optimal, or dimension-optimal or length-optimal.

For an \([n, k, d]\) code \( C \) over \( \text{GF}(q) \) with weight distribution \((1, A_1, \ldots, A_n)\), we denote by \((1, A_1^{\perp}, \ldots, A_n^{\perp})\) the weight distribution of its dual code. The first four Pless power moments on the two weight distributions are given as follows:

\[
\sum_{i=0}^{n} A_i = q^k,
\]

\[
\sum_{i=0}^{n} iA_i = q^{k-1}[q(q-1)n - A_1^{\perp}],
\]

\[
\sum_{i=0}^{n} i^2 A_i = q^{k-2}\left\{q(q-1)2n^2 + (q-1)n - [2(q-1)n - q + 2]A_1^{\perp} + 2A_2^{\perp}\right\},
\]

\[
\sum_{i=0}^{n} i^3 A_i = q^{k-3}\left\{(q-1)n\left\{(q-1)^2n^2 + 3(q-1)n - q + 2\right\}ight. - \left. [3(q-1)^2n^2 - 3(q-3)(q-1)n + q^2 - 6q + 6]A_1^{\perp} + 6\left\{(q-1)n - q + 2\right\}A_2^{\perp} - 6A_3^{\perp}\right\}.
\]

### 2.3 Two equivalences of linear codes

We recall the following two equivalences of linear codes, which will be needed in the sequel.
A permutation matrix $P$ is a square matrix having exactly one 1 in each row and column and 0s elsewhere. Two linear codes $C_1$ and $C_2 \subseteq \text{GF}(q)^n$ are said to be permutation-equivalent if there is a permutation of coordinates which sends $C_1$ to $C_2$, i.e., there is a permutation matrix $P$ such that $C_2 = C_1P$, where $C_1P = \{ y : y = xP, \forall x \in C_1 \}$. Two permutation-equivalent codes have the same parameters and weight distribution.

A monomial matrix $M$ over $\text{GF}(q)$ is a square matrix having exactly one nonzero element of $\text{GF}(q)$ in each row and column and column. Two linear codes $C_1$ and $C_2 \subseteq \text{GF}(q)^n$ are said to be monomially-equivalent if there is a monomial matrix $M$ such that $C_2 = C_1M$. Two monomially-equivalent codes have the same parameters and weight distribution.

3 An irreducible constacyclic code and its associated codes

Throughout this section, let $p$ be a prime and $q = p^s$ for a positive integer $s$. Let $n$ be a positive integer with $\text{gcd}(n, q) = 1$ and $\ell = \text{ord}_n(q)$. Let $r$ be a positive divisor of $q - 1$ and $\kappa = \frac{r}{\text{gcd}(q^{\frac{r}{\ell}} - 1, n)}$. Then by Lemma 1, $\text{ord}_n(q) = \kappa \ell$. Let $\alpha$ be a primitive element of $\text{GF}(q^{\kappa \ell})$ and set $\beta = \alpha^{(q^{\kappa \ell} - 1)/rn}$ and $\lambda = \alpha^{(q^{\kappa \ell} - 1)/r}$. Then $\lambda \in \text{GF}(q)^*$ with $\text{ord}(\lambda) = r$ and $\beta \in \text{GF}(q^{\kappa \ell})$ is a primitive $rn$-th root of unity such that $\beta^n = \lambda$, where $\text{ord}(\lambda)$ denotes the order of $\lambda$ in $\text{GF}(q)^*$. It should be noted that the $\lambda$ defined above ranges over all the elements of order $r$ in $\text{GF}(q)$ when $\alpha$ ranges over all the primitive elements of $\text{GF}(q^{\kappa \ell})$.

Let $C$ be the irreducible $\lambda$-constacyclic code of length $n$ over $\text{GF}(q)$ with check polynomial $M_\beta(x)$, which is the minimal polynomial over $\text{GF}(q)$ of $\beta$. Let $\theta = \beta^{-1}$, then $\theta$ is a primitive $rn$-th root of unity. According to [10, 25] and [28, Theorem 1], we have

$$C = \left\{ c(a) = \left( \text{Tr}_{q^{\kappa \ell}/q}(a\theta^i) \right)_{i=0}^{n-1} : a \in \text{GF}(q^{\kappa \ell}) \right\},$$

(1)

where $\text{Tr}_{q^{\kappa \ell}/q}$ is the trace function from $\text{GF}(q^{\kappa \ell})$ onto $\text{GF}(q)$. The dual code $C^\perp$ is the $\lambda^{-1}$-constacyclic code of length $n$ over $\text{GF}(q)$ with generator polynomial $M_\beta^{-1}(x)$.

Note that $\frac{\ell}{\kappa}$ divides $\frac{q^{\ell} - 1}{n}$. We have

$$\left( \beta^x \right)^{q^{\ell} - 1} = \alpha^{q^{\kappa \ell} - 1} \left[ \frac{q^{\ell} - 1}{rn} \right] = 1.$$

Consequently, $\theta^x \in \text{GF}(q^{\ell})$. Associated with the irreducible $\lambda$-constacyclic code $C$ in Eq. (1) are the following two codes over $\text{GF}(q)$:

$$\text{Exp}_1(C) = \left\{ e_1(a) = \left( \text{Tr}_{q^{\ell}/q}(a\theta^i) \right)_{i=0}^{rn-1} : a \in \text{GF}(q^{\ell}) \right\},$$

(2)

and

$$\text{Exp}_2(C) = \left\{ e_2(a) = \left( \text{Tr}_{q^{\ell}/q}(a\theta^i) \right)_{i=0}^{\frac{n}{\kappa} - 1} : a \in \text{GF}(q^{\ell}) \right\}.$$

In the special case $\kappa = 1$, $C$ and $\text{Exp}_2(C)$ are identical.

The following two conclusions follow from the trace representation of constacyclic codes (see [25], [28, Theorem 1]):

1. $\text{Exp}_1(C)$ is the irreducible cyclic code of length $\frac{rn}{\kappa} = \text{gcd}(q^{\ell} - 1, rn)$ over $\text{GF}(q)$ with check polynomial $M_{\beta^x}(x)$, which is the minimal polynomial over $\text{GF}(q)$ of $\beta^x$.
2. \( \text{Exp}_2(C) \) is the irreducible \( \lambda \)-constacyclic code of length \( \frac{n}{\kappa} = \gcd \left( \frac{q^\ell - 1}{\ell}, n \right) \) over \( \GF(q) \) with check polynomial \( M_{\beta^k}(\lambda) \).

The code \( C \) and the two codes \( \text{Exp}_1(C) \) and \( \text{Exp}_2(C) \) have the following relationships.

**Theorem 1** Let notation be the same as before.

1. The cyclic code \( \text{Exp}_1(C) = \{ (c \parallel \lambda^{-1}c \parallel \cdots \parallel \lambda^{-(r-1)}c) : c \in \text{Exp}_2(C) \} \), where \( \parallel \) denotes the concatenation of vectors.

2. The code \( C \) is permutation-equivalent to \( \text{Exp}_2(C) \oplus \cdots \oplus \text{Exp}_2(C) \), where \( C_1 \oplus C_2 \) denotes the outer direct sum of \( C_1 \) and \( C_2 \), i.e., \( C_1 \oplus C_2 = \{ (c_1 || c_2) : c_1 \in C_1, c_2 \in C_2 \} \).

3. The dual code \( C^\perp \) is permutation-equivalent to \( \text{Exp}_2(C)^\perp \oplus \cdots \oplus \text{Exp}_2(C)^\perp \).

**Proof** 1. Note that \( \theta^n = \lambda^{-1} \). For each \( c_1(a) \in \text{Exp}_1(C) \), by definition we have

\[
\begin{align*}
\text{Exp}_1(C) &= \{ (c \parallel \lambda^{-1}c \parallel \cdots \parallel \lambda^{-(r-1)}c) : c \in \text{Exp}_2(C) \}, \\
\text{Exp}_1(C) &= \{ (c \parallel \lambda^{-1}c \parallel \cdots \parallel \lambda^{-(r-1)}c) : c \in \text{Exp}_2(C) \}.
\end{align*}
\]

It follows that

\[
\text{Exp}_1(C) = \{ (c \parallel \lambda^{-1}c \parallel \cdots \parallel \lambda^{-(r-1)}c) : c \in \text{Exp}_2(C) \}.
\]

2. When \( \kappa = 1 \), \( C = \text{Exp}_2(C) \), the desired conclusion follows. When \( \kappa > 1 \),

\[
\text{Exp}_1(C) = \{ (c \parallel \lambda^{-1}c \parallel \cdots \parallel \lambda^{-(r-1)}c) : c \in \text{Exp}_2(C) \}.
\]

3. The third desired result follows directly from result 2.

By Theorem 1, we have the following results.

**Theorem 2** Let notation be the same as before. The following assertions are equivalent.
1. \( \text{Exp}_2(C) \) is a \[ \left( \gcd \left( \frac{q^d - 1}{r}, n \right), \ell, d \right) \] code over \( GF(q) \) with weight enumerator \( W(z) \).
2. \( \text{Exp}_1(C) \) is a \( \left[ \gcd(q^\ell - 1, rn), \ell, rd \right] \) code over \( GF(q) \) with weight enumerator \( W(z^r) \).
3. \( C \) is an \([n, \kappa \ell, d] \) code over \( GF(q) \) with weight enumerator \( W(z)^\kappa \).

Let \( C \) be a \( \lambda \)-constacyclic irreducible code \( C \) of length \( n \) over \( GF(q) \), where \( \gcd(n, q) = 1 \) and \( \ell = \text{ord}_n(q) \). Theorems 1 and 2 show that the weight enumerators of \( C \) and its associated irreducible cyclic code \( \text{Exp}_1(C) \) can be derived from each other. However, the weight enumerator of irreducible cyclic codes is known only in a few cases [9]. Similarly, the weight enumerator of irreducible constacyclic codes is known only in a few cases [25].

**Theorem 3** Let notation be the same as before. Then \( C^{\perp} \) is an \([n, n - \kappa \ell, d^{\perp}] \) code over \( GF(q) \) with weight enumerator \( W(z)^{\kappa} \) if and only if \( \text{Exp}_2(C)^{\perp} \) is a

\[
\left[ \gcd \left( \frac{q^d - 1}{r}, n \right), \gcd \left( \frac{q^d - 1}{r}, n \right) - \ell, d^{\perp} \right],
\]

code \( GF(q) \) with weight enumerator \( W(z) \).

The following example demonstrates the results of Theorems 2 and 3.

**Example 1** Let \( q = 4, n = 15 \) and \( r = 3 \). Then \( \ell := \text{ord}_n(q) = 2, \kappa = r = 3, \) and \( \text{ord}_n(q) = 6 \). Let \( \alpha \) be a primitive element of \( GF(4^6) \) with \( \alpha^{12} + \alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha + 1 = 0 \). Then \( \beta = \alpha^{(4^6 - 1)/3 \times 15} \) and \( \lambda = \alpha^{(4^6 - 1)/3} \) is a primitive element of \( GF(4) \). Then we have the following.

- \( \text{Exp}_2(C) \) is a \([5, 2, 4] \) code over \( GF(4) \) with weight enumerator \( W(z) = 1 + 15z^4 \), and \( \text{Exp}_2(C)^{\perp} \) is a \([5, 3, 3] \) code over \( GF(4) \) with weight enumerator \( W^{\perp}(z) = 1 + 30z^3 + 15z^4 + 18z^5 \).
- \( C \) is a \([15, 6, 4] \) code over \( GF(4) \) with weight enumerator \( W(z)^3 \), and \( C^{\perp} \) is a \([15, 9, 3] \) code over \( GF(4) \) with weight enumerator \( (W^{\perp}(z))^3 \).
- \( \text{Exp}_1(C) \) is a \([15, 2, 12] \) code over \( GF(4) \) with weight enumerator \( W(z^3) = 1 + 15z^{12} \).

The following theorem gives an estimate of the dual distance of the irreducible constacyclic code in Eq. (1).

**Theorem 4** Let \( C \) be the irreducible \( \lambda \)-constacyclic code in Eq. (1). Then \( C^{\perp} \) is a \( \lambda^{-1} \)-constacyclic code over \( GF(q) \) with parameters \( \left[ n, n - \frac{r}{\gcd \left( \frac{q^d - 1}{r}, n \right)} \ell, d^{\perp} \geq 2 \right] \), where \( r = \text{ord}(\lambda) \) and \( \ell = \text{ord}_n(q) \). Furthermore, if \( \ell \geq 2 \), then the following hold:

1. \( d^{\perp} = 2 \) if and only if \( \gcd \left( \frac{q^d - 1}{r}, n \right) > 1 \).
2. If \( n \mid \left( q^d - 1 \right) \), \( n > 2 \left( q^{\ell/2} - 1 \right) \), and \( \gcd \left( \frac{q^d - 1}{r}, n \right) = 1 \), then \( 3 \leq d^{\perp} \leq 4 \).
3. If \( n \mid \left( q^{d - 1} - 1 \right) \), \( n > q^{d - 1} - 1 + 2 \), and \( \gcd \left( \frac{q^d - 1}{r}, n \right) = 1 \), then \( C^{\perp} \) is an \([n, n - \ell, 3] \) code over \( GF(q) \), which is both distance-optimal and dimension-optimal.

**Proof** Note that \( C \) is an \([n, \kappa \ell] \) \( \lambda \)-constacyclic code. It is well known that \( C^{\perp} \) is an \([n, n - \kappa \ell] \) \( \lambda^{-1} \)-constacyclic code. It is clear that \( d^{\perp} \geq 2 \). Obviously, \( d^{\perp} = 2 \) if and only if there is an integer \( 1 \leq i \leq n - 1 \) such that \( \theta^i \in GF(q)^* \), i.e., \((q - 1)i \equiv 0 \pmod{rn} \) has a solution \( 1 \leq i \leq n - 1 \), which is equivalent to \( \gcd \left( \frac{q^d - 1}{r}, n \right) > 1 \).

Assume now that \( n \mid \left( q^d - 1 \right) \) and \( \gcd \left( \frac{q^d - 1}{r}, n \right) = 1 \). Then \( \kappa = 1 \) and \( C^{\perp} \) is an \([n, n - \ell, d^{\perp}] \) code over \( GF(q) \) with \( d^{\perp} \geq 3 \). If \( n > 2 \left( q^{\ell/2} - 1 \right) \), by the Sphere Packing bound, the minimum
distance of an \([n, n - \ell]\) code over GF\((q)\) is at most 4. Hence, \(d^\perp \leq 4\). If \(n > \frac{q^{\ell-1}-1}{q-1} + 2\), there is no \([n, n - \ell, 4]\) code over GF\((q)\) by the bound in Lemma 3, which means that \(C^\perp\) is distance-optimal, and there is no \([n, n - \ell + 1, 3]\) code over GF\((q)\) by the Sphere Packing bound, which means that \(C^\perp\) is dimension-optimal. \(\square\)

The following is a corollary of Theorem 4.

**Corollary 1** Let \(n = \frac{q^m-1}{(q-1)e}\), where \(m\) is a positive integer, \(e\) is a positive divisor of \(\frac{q^m-1}{q-1}\) and \(e \leq q - 1\). Let \(\gcd\left(\frac{q^m-1}{q-1}, n\right) = 1\) and let \(C\) be the irreducible \(\lambda\)-constacyclic code in Eq. (1). Then \(C^\perp\) is an \([n, n - m, 3]\) code over GF\((q)\) and is both distance-optimal and dimension-optimal.

The following example demonstrates the dual code \(C^\perp\) in Corollary 1.

**Example 2** Let \(m = 4\), \(q = 5\), and \(r = 4\). Then we have the following examples of the code \(C^\perp\) in Corollary 1.

1. When \(e = 1\) and \(\alpha\) is the primitive element of GF\((5^4)\) with \(\alpha^4 + 4\alpha^2 + 4\alpha + 2 = 0\), we have \(n = 156\) and \(\lambda = 2\). The dual code of the irreducible 2-constacyclic code \(C\) over GF\((5)\) in Corollary 1 has parameters \([156, 152, 3]\).
2. When \(e = 2\) and \(\alpha\) is the primitive element of GF\((5^4)\) with \(\alpha^4 + 4\alpha^2 + 4\alpha + 2 = 0\), we have \(n = 78\) and \(\lambda = 2\). The dual code of the irreducible 2-constacyclic code \(C\) over GF\((5)\) in Corollary 1 has parameters \([78, 74, 3]\).
3. When \(e = 3\) and \(\alpha\) is the primitive element of GF\((5^4)\) with \(\alpha^3 + 4\alpha^2 + 4\alpha + 2 = 0\), we have \(n = 52\) and \(\lambda = 2\). The dual code of the irreducible 2-constacyclic code \(C\) over GF\((5)\) in Corollary 1 has parameters \([52, 48, 3]\).
4. When \(e = 4\) and \(\alpha\) is the primitive element of GF\((5^4)\) with \(\alpha^4 + 4\alpha^2 + 4\alpha + 2 = 0\), we have \(n = 39\) and \(\lambda = 2\). The dual code of the irreducible 2-constacyclic code \(C\) over GF\((5)\) in Corollary 1 has parameters \([39, 35, 3]\).

All the codes \(C^\perp\) in this example are both dimension-optimal and distance-optimal.

We now introduce another irreducible cyclic code associated to the irreducible constacyclic code \(C\) in Eq. (1). Note that \(\beta^r\) is an \(n\)-th primitive root of unity in GF\((q^{\kappa \ell})\), where \(\ell = \operatorname{ord}_n(q)\) and

\[
\kappa = \frac{r}{\gcd\left(\frac{q^\ell-1}{q-1}, r\right)}.
\]

Let \(\text{Exp}_3(C)\) be the irreducible cyclic code of length \(n\) over GF\((q)\) with check polynomial \(M_{\beta^r}(x)\). It is easily seen that

\[
M_{\beta^r}(x) = \prod_{i=0}^{\ell-1} (x - \beta^r q^i).
\]

Consequently, \(\text{Exp}_3(C)\) is an \([n, \ell]\) cyclic code over GF\((q)\), while \(C\) is an \([n, \kappa \ell]\) irreducible constacyclic code over GF\((q)\). The four codes \(C\), \(\text{Exp}_1(C)\), \(\text{Exp}_2(C)\) and \(\text{Exp}_3(C)\) are related by definition. In a special case, we have the following.

**Theorem 5** If \(\gcd(r, n) = 1\), then \(C\) and \(\text{Exp}_3(C)\) have length \(n\) and dimension \(\ell\) and are permutation-equivalent.
Proof Let \( \gcd(r, n) = 1 \). Then we have \( \kappa = 1 \). By Theorem 2, \( C \) has length \( n \) and dimension \( \ell \). Let \( \theta = \beta^{-1} \). By definition, the trace representation of \( \text{Exp}_3(C) \) is given by

\[
\text{Exp}_3(C) = \left\{ c_3(a) = \left( \text{Tr}_{q^{\ell}/q} \left( a\theta^i \right) \right)_{i=0}^{n-1} : a \in \text{GF}(q^\ell) \right\}.
\]

Since \( \gcd(r, n) = 1 \), \( \kappa = 1 \) and the trace representation of \( C \) in Eq. (1) becomes

\[
C = \left\{ c(a) = \left( \text{Tr}_{q^{\ell}/q} \left( a\theta^i \right) \right)_{i=0}^{n-1} : a \in \text{GF}(q^\ell) \right\}.
\]

It is easily seen that the coordinate permutation \( i \mapsto ir \mod n \) sends \( C \) to \( \text{Exp}_3(C) \). Therefore, \( C \) and \( \text{Exp}_3(C) \) are permutation-equivalent. \( \square \)

When \( \gcd(r, n) = 1 \), the relations among the weight enumerators and parameters of the four codes \( C, \text{Exp}_1(C), \text{Exp}_2(C) \) and \( \text{Exp}_3(C) \) are clearly known by combining Theorems 2 and 5. It is very interesting to note that the irreducible \( \lambda \)-constacyclic code \( C \) in Eq. (1) is permutation-equivalent to the irreducible cyclic code \( \text{Exp}_3(C) \) under the special condition \( \gcd(r, n) = 1 \). This is a special result only for this special code \( C \) in Eq. (1) under this special condition. Theorem 5 will be used to study two families of irreducible constacyclic codes in Sects. 5 and 6. In fact, all the known results about the irreducible cyclic code \( \text{Exp}_3(C) \) surveyed in [9] can be translated into similar results about the irreducible \( \lambda \)-constacyclic code \( C \) under the condition that \( \gcd(r, n) = 1 \) and \( r = \text{ord}(\lambda) \).

We remark that the three codes \( \text{Exp}_1(C), \text{Exp}_2(C) \) and \( \text{Exp}_3(C) \) are associated only to the irreducible \( \lambda \)-constacyclic code \( C \) in Eq. (1), although similar codes may be associated to a general \( \lambda \)-constacyclic code. This irreducible \( \lambda \)-constacyclic code \( C \) in Eq. (1) is very special in the following senses:

- Its dimension is known to be \( \kappa \ell \), while the dimension of other irreducible \( \lambda \)-constacyclic codes is known to be a divisor of \( \kappa \ell \) only.
- Its trace representation is very simple and cannot be reduced to a trace representation over a proper subfield of \( \text{GF}(q^{\kappa \ell}) \).

It should be informed that this paper studies only this special irreducible \( \lambda \)-constacyclic code \( C \) in Eq. (1) and its associated codes.

Let \( C^{(t)} \) denote the \( \lambda \)-constacyclic code of length \( n \) over \( \text{GF}(q) \) with check polynomial \( M_{\beta^t}(x) \). It is easily seen from the trace representations of \( C \) and \( C^{(t)} \) that the two codes are permutation-equivalent if \( \gcd(t, n) = 1 \) and \( t \equiv 1 \mod r \) [25]. Almost all the results about \( C \) presented in this paper are also valid for all the \( \lambda \)-constacyclic codes \( C^{(t)} \) with \( \gcd(t, n) = 1 \) and \( t \equiv 1 \mod r \).

4 Parameters of the code \( C \) in (1) in the case \( \gcd\left(\frac{q-1}{r}, n\right) = 1 \)

In this section, we consider only the case that \( \gcd\left(\frac{q-1}{r}, n\right) = 1 \). Recall that \( \ell = \text{ord}_n(q) \) and \( \gcd(q, n) = 1 \). In this case, we have

\[
\kappa = \frac{r}{\gcd\left(\frac{q-1}{n}, r\right)} = \frac{q-1}{\gcd\left(\frac{q-1}{n}, q-1\right)}.
\]

It follows that \( C \) is an \( \left[ n, \frac{(q-1)\ell}{\gcd\left(\frac{q-1}{n}, q-1\right)} \right] \) code over \( \text{GF}(q) \) in this case. Theorem 2 shows that determining the parameters of the irreducible constacyclic code \( C \) is equivalent to determining
the parameters of the irreducible cyclic code Exp1 (C). Recall that the irreducible cyclic code Exp1 (C) has length gcd\( (q^e - 1, r) = r \cdot \text{gcd} \left( \frac{q^e - 1}{q - 1}, n \right) \) and check polynomial \( M_{p^e} (x) \). Let

\[
e = \text{gcd} \left( \frac{q^e - 1}{q - 1}, \frac{q^e - 1}{\text{gcd}(q^e - 1, rn)} \right) = \frac{(q^e - 1) \text{gcd}(q - 1, rn)}{(q - 1) \text{gcd}(q^e - 1, (q - 1)n)} \tag{3}
\]

The following lemma follows directly from the results in [9]. We will use it later to prove a main result of this paper.

**Lemma 4** Let notation be as before, and let \( r \) be a positive divisor of \( q - 1 \).

1. If \( n = r \left( \frac{q^m - 1}{q - 1} \right) \) for some integer \( m \geq 2 \), then \( e = 1 \) and Exp1 (C) is an \([n, m, r q^{m-1}]\) one-weight cyclic code.
2. If \( n = r \left( \frac{q^m - 1}{2(q - 1)} \right) \) for some even integer \( m \geq 2 \) and \( \text{gcd}(r, 2) = 1 \), then \( e = 2 \) and Exp1 (C) is an \([n, m, r(q^{m-1} - \frac{m-2}{2})]\) two-weight cyclic code with weight enumerator

\[
1 + \left( \frac{q^m - 1}{2} \right) z^{r(q^{m-1} - \frac{m-2}{2})} + \left( \frac{q^m - 1}{2} \right) z^{r(q^{m-1} - \frac{m-2}{2})}.
\]

3. If \( n = r \left( \frac{q^m - 1}{3(q - 1)} \right) \) for some odd integer \( m \geq 3 \), \( sm \equiv 0 \) (mod 3), \( \text{gcd}(r, 3) = 1 \) and \( p \equiv 1 \) (mod 3), then \( e = 3 \) and Exp1 (C) is an \([n, m]3\) three-weight cyclic code with weight enumerator

\[
1 + \left( \frac{q^m - 1}{3} \right) z^{r(q^{m-1} - \frac{m-3}{3})} + \left( \frac{q^m - 1}{3} \right) z^{r(q^{m-1} - \frac{m-3}{3})} + \left( \frac{q^m - 1}{3} \right) z^{r(q^{m-1} - \frac{m-3}{3})},
\]

where \( c_1 \) and \( d_1 \) are given by \( 4q^m/3 = c_1^2 + 27d_1^2 \), \( c_1 \equiv 1 \) (mod 3) and \( \text{gcd}(c_1, p) = 1 \).

4. If \( n = r \left( \frac{q^m - 1}{4(q - 1)} \right) \) for some even integer \( m \geq 4 \) with \( sm \equiv 0 \) (mod 4), \( \text{gcd}(r, 2) = 1 \), and \( p \equiv 1 \) (mod 4), then \( e = 4 \) and Exp1 (C) is an \([n, m]\) cyclic code with weight enumerator

\[
1 + \left( \frac{q^m - 1}{4} \right) z^{r(q^{m-1} - \frac{m-2}{4} + 4d_1 q \frac{m-4}{4})} + \left( \frac{q^m - 1}{4} \right) z^{r(q^{m-1} - \frac{m-2}{4} - 2c_1 q \frac{m-4}{4})} + \left( \frac{q^m - 1}{4} \right) z^{r(q^{m-1} - \frac{m-2}{4} + 4d_1 q \frac{m-4}{4})},
\]

where \( c_1 \) and \( d_1 \) are given by \( q^m/4 = c_1^2 + 4d_1^2 \), \( c_1 \equiv 1 \) (mod 4) and \( \text{gcd}(c_1, p) = 1 \).

5. Let \( m \geq 2 \) be an even integer and \( e > 2 \) be a divisor of \( \frac{q^m - 1}{q - 1} \) such that \( \text{gcd}(e, r) = 1 \).

Let \( n = r \left( \frac{q^m - 1}{(q - 1)e} \right) \). If \( p^j \equiv -1 \) (mod \( e \)) for a positive integer \( j \). Assume that \( j \) is the smallest positive integer such that \( p^j \equiv -1 \) (mod \( e \)). Define \( \gamma = \frac{sm}{2j} \).

(a) If \( \gamma \) and \( p \) and \( p^j + 1 \) are all odd, then Exp1 (C) is an \([n, m]2\) two-weight cyclic code with weight enumerator

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

provided that \( e < q^m/2 + 1 \).

\[\text{Springer}\]
(b) In all other cases, then $\text{Exp}_1(C)$ is an $[n, m]$ two-weight cyclic code with weight enumerator
\begin{align*}
1 + \left( \frac{q^m - 1}{e} \right) z^{\left( q^m - 1 \right) r} + \left( q^m - 1 \right) z^{\left( q^m - 1 \right) r + 1},
\end{align*}

provided that $q^{m/2} + (-1)^t (e - 1) > 0$.

One of the main results of this paper is documented in the following theorem.

**Theorem 6** Let $n = u\left( \frac{q^m - 1}{q-1} \right)$, where $m \geq 2$, $e$ is a positive divisor of $\frac{q^m - 1}{q-1}$ and $e \leq \frac{q^{m/2} + 1}{2}$, $u$ is a positive divisor of $q - 1$ and $\text{gcd}(e, u) = 1$. Let $C$ be the irreducible $\lambda$-constacyclic code in Eq. (1).

1. If $e = 1$ and $\text{gcd}\left( \frac{q^m - 1}{q-1}, n \right) = 1$, then $C$ is an $[n, um, q^{m-1}]$ code over $\text{GF}(q)$ with weight enumerator
\begin{align*}
\left[ 1 + (q^m - 1) z^{q^{m-1}} \right].
\end{align*}

The dual code $C^\perp$ has parameters $[n, n - um, 3]$.

2. If $m$ is even, $e = 2 < q$ and $\text{gcd}\left( \frac{q^m - 1}{q-1}, n \right) = 1$, then $C$ is an $[n, um, \frac{q^m - 1}{2} \cdot \frac{m^2}{2}]$ code over $\text{GF}(q)$ with weight enumerator
\begin{align*}
\left[ 1 + \left( \frac{q^m - 1}{2} \right) z^{\frac{q^m - 1}{2} \cdot \frac{m^2}{2}} + \left( \frac{q^m - 1}{2} \right) z^{\frac{q^m - 1}{2} \cdot \frac{m^2}{2}} \right].
\end{align*}

The dual code $C^\perp$ has parameters $[n, n - um, 3]$.

3. If $e = 3 < q$, $m \geq 3$ is odd, $sm \equiv 0 \pmod{3}$, $p \equiv 1 \pmod{3}$ and $\text{gcd}\left( \frac{q^m - 1}{q-1}, n \right) = 1$, then $C$ is an $[n, um]$ code over $\text{GF}(q)$ with weight enumerator
\begin{align*}
\left[ 1 + \left( \frac{q^m - 1}{3} \right) z^{\frac{q^m - 1}{3} \cdot \frac{m^2}{3}} + z^{\frac{q^m - 1}{3} \cdot \frac{m^2}{3}} + z^{\frac{q^m - 1}{3} \cdot \frac{m^2}{3}} \right],
\end{align*}

where $c_1$ and $d_1$ are given by $4q^{m/3} = c_1^2 + 27d_1^2$, $c_1 \equiv 1 \pmod{3}$ and $\text{gcd}(c_1, p) = 1$. The dual code $C^\perp$ has parameters $[n, n - um, 3]$.

4. If $e = 4 < q$, $m \geq 4$ is even, $sm \equiv 0 \pmod{4}$, $p \equiv 1 \pmod{4}$ and $\text{gcd}\left( \frac{q^m - 1}{q-1}, n \right) = 1$, then $C$ is an $[n, um]$ code over $\text{GF}(q)$ with weight enumerator
\begin{align*}
\left[ 1 + \left( \frac{q^m - 1}{4} \right) z^{\frac{q^m - 1}{4} \cdot \frac{m^2}{4}} + \left( \frac{q^m - 1}{4} \right) z^{\frac{q^m - 1}{4} \cdot \frac{m^2}{4}} + \left( \frac{q^m - 1}{4} \right) z^{\frac{q^m - 1}{4} \cdot \frac{m^2}{4}} + \left( \frac{q^m - 1}{4} \right) z^{\frac{q^m - 1}{4} \cdot \frac{m^2}{4}} \right],
\end{align*}

where $c_1$ and $d_1$ are given by $q^{m/2} = c_1^2 + 4d_1^2$, $c_1 \equiv 1 \pmod{4}$ and $\text{gcd}(c_1, p) = 1$. The dual code $C^\perp$ has parameters $[n, n - um, 3]$.

5. Let $\text{gcd}\left( \frac{q^m - 1}{q-1}, n \right) = 1$, $e > 2$ and $p^j \equiv -1 \pmod{e}$ for a positive integer $j$. Assume that $j$ is the smallest positive integer such that $p^j \equiv -1 \pmod{e}$. Define $\gamma = \frac{sm}{2j}$.
(a) If $\gamma$ is odd, then $C$ is an \([n, um, \frac{q^{m-1}-(e-1)q^{m-2}}{e}]\) code over GF(q) with weight enumerator
\[
1 + \left(\frac{q^m - 1}{e}\right) z^{\frac{q^{m-1}-(e-1)q^{m-2}}{e}} + \left(\frac{q^m - 1}{e}\right) z^{\frac{q^{m-1}+q^{m-2}}{e}}.
\]

(b) If $\gamma$ is even, then $C$ is an \([n, um, \frac{q^{m-1}-q^{m-2}}{e}]\) code over GF(q) with weight enumerator
\[
1 + \left(\frac{q^m - 1}{e}\right) z^{\frac{q^{m-1}+q^{m-2}}{e}} + \left(\frac{q^m - 1}{e}\right) z^{\frac{q^{m-1}-q^{m-2}}{e}}.
\]

The dual code $C^\perp$ has parameters $[n, n - um, d^\perp]$, where
\[
d^\perp = \begin{cases} 
4 & \text{if } m = 4 \text{ and } e = q + 1, \\
3 & \text{otherwise}.
\end{cases}
\]

**Proof** In each case, we assume that $\gcd\left(\frac{q-1}{T}, n\right) = 1$. Hence, in each case we have $\kappa = u$, and
\[
\frac{q^m - 1}{\gcd(q^m - 1, (q - 1)n)} = e.
\]

By Theorem 2, $C$ has weight enumerator $W(z)^\perp$ if and only if $\text{Exp}_1(C)$ has weight enumerator $W(z'^*)$. Then the desired weight enumerator of $C$ in each case follows from the weight enumerator of the code $\text{Exp}_1(C)$ given in Lemma 4.

We now settle the parameters of the dual code $C^\perp$. The dimension of $C^\perp$ follows from that of $C$. It remains to treat the minimum distance of $C^\perp$. Note that $\text{Exp}_2(C)$ is an irreducible $\lambda$-constacyclic code of length $\frac{q^m - 1}{(q-1)e}$ over GF(q). If $e \leq q - 1$, from Theorem 4, $\text{Exp}_2(C)$ is a $[\frac{q^m - 1}{(q-1)e}, \frac{q^m - 1}{(q-1)e} - m, 3]$ code over GF(q). By Theorem 3, $C^\perp$ is an $[n, n - um, 3]$ code over GF(q).

If $e > 2$ and $p^j \equiv -1 \pmod{e}$ for a positive integer $j$. From Lemma 4, the code $\text{Exp}_2(C)$ has weight enumerator
\[
1 + \left(\frac{q^m - 1}{e}\right) z^{\frac{q^{m-1}-(e-1)q^{m-2}}{e}} + \left(\frac{q^m - 1}{e}\right) z^{\frac{q^{m-1}+q^{m-2}}{e}}.
\]

If $m = 2$, then $\text{Exp}_2(C)^\perp$ is a $[\frac{q+1}{e}, \frac{q+1}{e} - 2, 3]$ MDS code over GF(q). If $m \geq 4$, from the Pless power moments, we have
\[
6A_3^\perp = \frac{(q^m - 1)[q^m - (-1)^\gamma(e^2 - 3e + 2)q^{m/2} - (q - 2)e^2 - 3e + 1]}{e^5}.
\]

It follows that $A_3^\perp = 0$ if and only if
\[
\Delta := q^m - (-1)^\gamma(e^2 - 3e + 2)q^{m/2} - (q - 2)e^2 - 3e + 1 = 0.
\]

- When $\gamma$ is odd, $q^m \equiv -1 \pmod{e}$. It is easy to check that
  \[
  \Delta = e \left[ (q^{m/2} - q + 2)e - 3q^{m/2} - 3 \right] + q^m + 2q^{m/2} + 1 > 0.
  \]

  Hence, $\text{Exp}_2(C)^\perp$ is a $[\frac{q^{m-1}}{(q-1)e}, \frac{q^{m-1}}{(q-1)e} - m, 3]$ code over GF(q).
When $\gamma$ is even, $q^\frac{m}{\gamma} \equiv 1 \pmod{e}$. It is easy to check that
\[
\Delta = (q^\frac{m}{\gamma} - 1)\left(q^\frac{m}{\gamma} - 1 - e^2 + 3e\right) - (q - 1)e^2 = 0,
\]
if and only if
\[
\left(q^\frac{m}{\gamma} - 1\right)\left(q^\frac{m}{\gamma} - 1\right) - e + 3 = q - 1.
\]
This equation holds if and only if $m = 4$ and $e = q + 1$. Therefore, $\text{Exp}_2(C)$ is a
\[
\left[q^m - 1, \frac{q^m - 1}{(q - 1)e} - m, d\right],
\]
code over $\mathbb{F}(q)$, where
\[
\begin{cases}
4 & \text{if } m = 4 \text{ and } e = q + 1, \\
3 & \text{otherwise}.
\end{cases}
\]
According to Theorem 3, $d^\perp$ is equal to the minimum distance of $\text{Exp}_2(C)^\perp$. The desired result follows.}

The results in the special case $u = 1$ in Theorem 6 may be proved with some results in [25]. If this is possible, it may take some work to do so. When $u > 1$, the results in Theorem 6 may not be derived from [25].

Let $\lambda$ be a generator of $\mathbb{F}(q)^*$ with $\alpha^8 + 4\alpha^3 + 6\alpha^2 + 2\alpha + 3 = 0$. Then the corresponding $\lambda = 3$, which is a primitive element of $\mathbb{F}(7)$. Let $C$ be the corresponding irreducible $\lambda$-constacyclic code in Eq. (1):
\[
\begin{align*}
L := \text{gcd} & \left(\frac{q^\lambda - 1}{q - 1}, \frac{q^\lambda - 1}{nr}\right) \\
\end{align*}
\]
(4)
The parameter $e$ defined in Eq. (3) may be different from the $L$ defined above. In [25], Gaussian periods of order $L$ are used to express the weight distribution of the code $C$ in Eq. (1). This way of determining the weight distribution of $C$ is infeasible in most cases, as $L$ could be very large and Gaussian periods of order $L$ are not evaluated for most orders $L$. Below is such example.

**Example 3** Let $q = 7$, $m = 4$, $r = 6$ and $n = 800$. Then $\text{ord}_{16}(q) = 8$. Let $\alpha$ be a primitive element of $\mathbb{F}(7^8)$ with $\alpha^8 + 4\alpha^3 + 6\alpha^2 + 2\alpha + 3 = 0$. Then the corresponding $\lambda = 3$, which is a primitive element of $\mathbb{F}(7)$. Let $C$ be the corresponding irreducible $\lambda$-constacyclic code in Eq. (1). Then $C$ has parameters $[800, 8, 343]$ and weight enumerator $1 + 4800z^{343} + 5, 760, 000z^{686} = (1 + 2400z^{343})^2$. For this code, the parameter $e$ defined in Eq. (3) is 1 and the corresponding $u = 2$ in terms of the notation of Theorem 6. Hence, the parameters and the weight enumerator of this code $C$ follow from the conclusions of the first case in Theorem 6. However, the parameter $L$ in Eq. (4) is equal to 1201, and the parameters and the weight enumerator of this code $C$ cannot be deduced from the results in [25], as Gaussian periods of order 1201 over $\mathbb{F}(7^8)$ are not evaluated. Note that 1201 is a prime.

Below we present a number of examples for illustrating the cases in Theorem 6.

**Example 4** Let $m = 2$, $q = 2^4$, $r = q - 1 = 15$, $e = 1$, $u = 3$. Then $n = u\left(\frac{q^m - 1}{(q - 1)e}\right) = 51$. Let $\alpha$ be a generator of $\mathbb{F}(16^5)*$ with $\alpha^{24} + \alpha^{16} + \alpha^{15} + \alpha^{14} + \alpha^{13} + \alpha^{10} + \alpha^9 + \alpha^7 + \alpha^5 + \alpha^3 + 1 = 0$. Then the $\lambda$-constacyclic code $C$ in Eq. (1) has parameters $[51, 6, 16]$ and weight enumerator
\[16, 581, 375z^{48} + 195, 075z^{32} + 765z^{16} + 1.\]
$C^\perp$ has parameters [51, 45, 3]. These results are consistent with the conclusions in the first case in Theorem 6.

**Example 5** Let $m = 2, q = 7, r = q - 1 = 6, e = 2, u = 3$. Then $n = u\left(\frac{q^{m-1}}{(q-1)r}\right) = 12$. Let $\alpha$ be a generator of $\text{GF}(7^6)^*$ with $\alpha^6 + \alpha^4 + 5\alpha^3 + 4\alpha^2 + 6\alpha + 3 = 0$. Then the $\lambda$-constacyclic code $C$ in Eq. (1) has parameters [12, 6, 3] and weight enumerator $(24z^4 + 24z^3 + 1)^3$. $C^\perp$ has parameters [12, 6, 3]. These results are consistent with the conclusions in the second case in Theorem 6.

**Example 6** Let $m = 3, q = 7, r = q - 1 = 6, e = 3, u = 2$. Then $n = u\left(\frac{q^{m-1}}{(q-1)r}\right) = 38$. Let $\alpha$ be a generator of $\text{GF}(7^6)^*$ with $\alpha^6 + \alpha^4 + 5\alpha^3 + 4\alpha^2 + 6\alpha + 3 = 0$. Then the $\lambda$-constacyclic code $C$ in Eq. (1) has parameters [38, 6, 15] and weight enumerator $(114z^{18} + 114z^{16} + 114z^{15} + 1)^2$. $C^\perp$ has parameters [38, 32, 3]. These results are consistent with the conclusions in the third case in Theorem 6.

**Example 7** Let $m = 4, q = 13, r = q - 1 = 12, e = 4, u = 1$. Then $n = u\left(\frac{q^{m-1}}{(q-1)r}\right) = 595$. Let $\alpha$ be a generator of $\text{GF}(13^4)^*$ with $\alpha^4 + 3\alpha^2 + 12\alpha + 2 = 0$. Then the $\lambda$-constacyclic code $C$ in Eq. (1) has parameters [595, 4, 540] and weight enumerator $7140z^{555} + 7140z^{552} + 7140z^{550} + 7140z^{540} + 1$. $C^\perp$ has parameters [595, 591, 3]. These results are consistent with the conclusions in the fourth case in Theorem 6.

**Example 8** Let $m = 2, q = p = 11, r = q - 1 = 10, e = 4, u = 3$. Then $n = u\left(\frac{q^{m-1}}{(q-1)r}\right) = 9$. Let $\alpha$ be a generator of $\text{GF}(11^6)^*$ with $\alpha^6 + 3\alpha^4 + 4\alpha^3 + 6\alpha^2 + 7\alpha + 2 = 0$. Then the $\lambda$-constacyclic code $C$ in Eq. (1) has parameters [9, 6, 2] and weight enumerator $(90z^3 + 30z^2 + 1)^3$. $C^\perp$ has parameters [9, 3, 3]. These results are consistent with the conclusions in Case 5.a in Theorem 6.

**Example 9** Let $m = 4, q = p = 11, r = q - 1 = 10, e = 3, u = 2$. Then $n = u\left(\frac{q^{m-1}}{(q-1)r}\right) = 976$. Let $\alpha$ be a generator of $\text{GF}(11^8)^*$ with $\alpha^8 + 7\alpha^4 + 7\alpha^3 + \alpha^2 + 7\alpha + 2 = 0$. Then the $\lambda$-constacyclic code $C$ in Eq. (1) has parameters [976, 8, 440] and weight enumerator $(4880z^{451} + 9760z^{440} + 1)^2$. $C^\perp$ has parameters [976, 968, 3]. These results are consistent with the conclusions in Case 5.b in Theorem 6.

The following is a list of corollaries of Theorem 6.

**Corollary 2** Let $m \geq 2$ and $q$ be a prime power. Let $r$ be a positive divisor of $q - 1$ such that $\gcd\left(\frac{q-1}{r}, m\right) = 1$. Let $n = \frac{q^m - 1}{q - 1}$. Then the irreducible $\lambda$-constacyclic code over $\text{GF}(q)$ with $\text{ord}(\lambda) = r$ in Eq. (1) is monomially-equivalent to the Simplex code Simplex$(q, m)$ and its dual is monomially-equivalent to the Hamming code Hamming$(q, m)$.

**Proof** It is easily seen that

$$\gcd\left(\frac{q-1}{r}, n\right) = \gcd\left(\frac{q-1}{r}, m\right) = 1.$$ 

Let $u = 1$ and $e = 1$ in Theorem 6. We then deduce from the first case in Theorem 6 that $C$ has the same parameters as the Simplex code and $C^\perp$ has the same parameters as the Hamming code. It is well known that every linear code sharing the parameters of the Hamming code must be monomially-equivalent to the Hamming code [14].

When $r = q - 1$, Corollary 2 was proven in [11, 13]. With Corollary 2, we proved that there are more classes of constacyclic codes which are monomially-equivalent to the Hamming code.
Corollary 3 Let \( n = 2\left(\frac{q^m - 1}{q - 1}\right) \), where \( m \geq 2 \) and \( q \) is an odd prime power. Let \( r \) be a positive divisor of \( q - 1 \) such that \( \gcd\left(\frac{q^m - 1}{q - 1}, 2m\right) = 1 \). Let \( C \) be the irreducible \( \lambda \)-constacyclic code in Eq. (1). Then \( C \) is an \([n, 2m, q^m - 1]\) two-weight code with weight enumerator

\[
1 + 2(q^m - 1)z^{q^m - 1} + (q^m - 1)^2 z^{2q^m - 1}.
\]

Its dual code has parameters \([n, n - 2m, 3]\).

**Proof** It is straightforward to see that

\[
\gcd\left(\frac{q - 1}{r}, n\right) = \gcd\left(\frac{q - 1}{r}, 2m\right) = 1.
\]

Let \( u = 2 \) and \( e = 1 \) in Theorem 6. Then the desired conclusions follow. \(\Box\)

Example 10 Let \( m = 3, q = 3 \) and \( r = 2 \). Let \( \alpha \) be a generator of \( \mathbb{GF}(3^6)^* \) with \( \alpha^6 + 2\alpha^4 + \alpha^2 + 2\alpha + 2 = 0 \). Then the irreducible negacyclic code \( C \) of length \( q^m - 1 \) over \( \mathbb{GF}(q) \) in Eq. (1) has parameters \([26, 6, 9]\) and weight enumerator \( 1 + 52z^9 + 676z^{18} \). The dual code \( C^⊥ \) has parameters \([26, 20, 3]\).

Corollary 4 Let \( n = 3\left(\frac{q^m - 1}{q - 1}\right) \), where \( m \geq 2 \) and \( q \equiv 1 \pmod{3} \) is a prime power. Let \( r \) be a positive divisor of \( q - 1 \) such that \( \gcd\left(\frac{q - 1}{r}, 3m\right) = 1 \). Let \( C \) be the irreducible \( \lambda \)-constacyclic code in Eq. (1). Then \( C \) is an \([n, 3m, q^m - 1]\) three-weight code with weight enumerator

\[
1 + 3(q^m - 1)z^{q^m - 1} + 3(q^m - 1)^2 z^{2q^m - 1} + (q^m - 1)^3 z^{3q^m - 1},
\]

and \( C^⊥ \) has parameters \([n, n - 3m, 3]\).

**Proof** Let \( q = rt + 1 \). Then

\[
\gcd\left(\frac{q - 1}{r}, n\right) = \gcd\left(\frac{q - 1}{r}, 3q^m - 1\right) = \gcd\left(t, 3(q^m - 1 + q^{m - 2} + \cdots + q + 1)\right) = \gcd\left(\frac{q - 1}{r}, 3m\right) = 1.
\]

Let \( u = 3 \) and \( e = 1 \) in Theorem 6. Then the desired conclusions follow. \(\Box\)

Example 11 Let \( m = 4, q = 4 \) and \( r = q - 1 \). Let \( \alpha \) be a generator of \( \mathbb{GF}(4^{12})^* \) with

\[
\alpha^{24} + \alpha^{16} + \alpha^{15} + \alpha^{14} + \alpha^{13} + \alpha^{10} + \alpha^9 + \alpha^7 + \alpha^5 + \alpha^3 + 1 = 0.
\]

Then the irreducible \( \lambda \)-constacyclic code \( C \) of length \( 3\left(\frac{q^m - 1}{q - 1}\right) \) over \( \mathbb{GF}(q) \) in Eq. (1) has parameters \([255, 12, 64]\) and weight enumerator \( 1 + 765z^{64} + 195075z^{128} + 16581375z^{192} \). The dual code \( C^⊥ \) has parameters \([255, 243, 3]\).

5 A family of irreducible cyclic codes over \( \mathbb{GF}(q) \) with parameters \([2n, (n - 1)/2, d \geq 2(\sqrt{n} + 1)]\)

Throughout this section, let \( q \) be an odd prime power and let \( n \) be an odd prime such that

\[
m := \text{ord}_{2n}(q) = (n - 1)/2.
\]

Note that \( \gcd(2, n) = 1 \). We have then \( \kappa = 1 \). Consequently, \( \text{ord}_n(q) = \text{ord}_{2n}(q) = (n - 1)/2 \).
Let $\alpha$ be a primitive element of $\text{GF}(q^m)$ and put $\beta = \alpha^{(q^m-1)/2n}$. Then $\beta^n = -1$. By definition and assumption, we have

$$C_1^{(q,2n)} = \{1, q, q^2, \ldots, q^{m-1}\} \mod 2n.$$  

Clearly, all the $(n - 1)/2$ elements in $C_1^{(q,2n)}$ are odd. Take any $h$ from

$$\{2i + 1 : 0 \leq i \leq n - 1\} \setminus (C_1^{(q,2n)} \cup \{n\}).$$

Then the cosets $C_h^{(q,2n)}$ and $C_1^{(q,2n)}$ are disjoint and

$$C_1^{(q,2n)} \cup C_h^{(q,2n)} = \{2i + 1 : 0 \leq i \leq n - 1\} \setminus \{n\}.$$  

Then for $i \in \{1, h\}$ the minimal polynomial

$$M_{\beta^i}(x) = \prod_{j \in C_1^{(q,2n)}} (x - \beta^j),$$

and $x^n + 1 = (x + 1)M_{\beta^1}(x)M_{\beta^h}(x)$.

Let $C(q, n, i; 2)$ denote the negacyclic code of length $n$ over $\text{GF}(q)$ with check polynomial $M_{\beta^i}(x)$. Then the dimension of $C(q, n, i; 2)$ equals $(n - 1)/2$ for $i \in \{1, h\}$. Consequently, its dual has dimension $(n + 1)/2$. We first prove the following theorem.

**Theorem 7** Let notation and assumptions be the same as before. Then the irreducible negacyclic code $C(q, n, 1; 2)$ has parameters $[n, (n - 1)/2, d]$ with $d \geq \sqrt{n} + 1$ and its dual $C(q, n, 1; 2)^\perp$ has parameters $[n, (n + 1)/2, d^\perp]$ with $d^\perp \geq \sqrt{n}$.

For the code $C(q, n, i; 2)$, the lower bound on the minimum distance developed in [25, Theorem 4.3] is negative and not useful. We have to prove the desired square-root bounds with a different approach. To this end, we need to do some preparations.

**Lemma 5** Let $q$ be an odd prime power and let $n$ be an odd prime such that $\text{ord}_{2n}(q) = (n - 1)/2$ and $n > q$. Then $q$ is a quadratic residue modulo $n$.

**Proof** It was shown at the beginning of this section that $\text{ord}_n(q) = \text{ord}_{2n}(q) = (n - 1)/2$. Let $\zeta$ be a primitive root of $n$. Since $n > q$, then there exists an integer $i$ with $1 \leq i < n - 1$ such that $q = \zeta^i \mod n$. It is well known that $\text{ord}_n(q) = (n - 1)/\gcd(i, n - 1)$. As a result, $\gcd(i, n - 1) = 2$ and $i$ must be even. The desired result then follows. \hfill $\Box$

**Lemma 6** $\text{Exp}_3(C(q, n, 1; 2))$ has parameters $[n, (n - 1)/2, d \geq \sqrt{n} + 1]$ and $\text{Exp}_3(C(q, n, 1; 2))^\perp$ has parameters $[n, (n + 1)/2, d^\perp \geq \sqrt{n}]$.

**Proof** Note that $\beta^2$ is an $n$-th primitive root of unity in $\text{GF}(q^m)$. Let $\text{QR}(n)$ and $\text{QN}(n)$ denote the set of quadratic residues and nonresidues modulo $n$, respectively. It follows from Lemma 5 that the canonical factorization of $x^n - 1$ over $\text{GF}(q)$ is given by

$$x^n - 1 = (x - 1) \left( \prod_{i \in \text{QR}(n)} (x - \beta^{2i}) \right) \left( \prod_{i \in \text{QN}(n)} (x - \beta^{2i}) \right). \quad (5)$$

Since $M_{\beta^2}(x)$ is an irreducible divisor of $x^n - 1$ and $\beta^2 \notin \text{GF}(q)$, we have

$$M_{\beta^2}(x) = \prod_{i \in \text{QR}(n)} (x - \beta^{2i}),$$
Table 1 The code $C(q, n, 1; 2)$ and its dual

| $q$ | $n$ | $d$ | Best distance | $d^\perp$ | Best distance |
|-----|-----|-----|---------------|--------|---------------|
| 3   | 11  | 6   | 6, optimal    | 5      | 5, optimal    |
| 3   | 23  | 9   | 9, optimal    | 8      | 8, optimal    |
| 3   | 37  | 11  | 12            | 10     | 10            |
| 3   | 47  | 15  | 15            | 14     | 14            |
| 3   | 59  | 18  | 18            | 17     | 17            |
| 3   | 71  | 18  | 18            | 17     | 17            |
| 5   | 11  | 6   | 6, optimal    | 5      | 5, optimal    |
| 5   | 19  | 8   | 8             | 7      | 7             |
| 5   | 29  | 12  | 12, optimal   | 11     | 11, optimal   |
| 5   | 41  | 14  | 14            | 13     | 13            |
| 7   | 31  | 13  | 13            | 12     | 12            |
| 7   | 47  | 17  | 17            | 16     | 16            |

or

$$M_{n^2}(x) = \prod_{i \in QN(n)} (x - \beta^{2i}).$$

Consider now the code $\text{Exp}_3(C(q, n, 1; 2))$, which is the third code associated to the irreducible negacyclic code $C(q, n, 1; 2)$ and has check polynomial $M_{n^2}(x)$. The check polynomial $M_{n^2}(x)$ above shows that $\text{Exp}_3(C(q, n, 1; 2))$ is a quadratic-residue code. The desired conclusions then follow from [14, Theorem 6.6.22]. □

Since $\gcd(2, n) = 1$, the desired conclusions of Theorem 7 then follow from Theorem 5 and Lemma 6. This completes the proof of Theorem 7. Theorem 5 tells us that $C(q, n, 1; 2)$ and $\text{Exp}_3(C(q, n, 1; 2))$ are permutation-equivalent. Hence, the negacyclic code $C(q, n, 1; 2)$ is a counterpart of the corresponding quadratic-residue code $\text{Exp}_3(C(q, n, 1; 2))$. Combining Theorems 2 and 7, we obtain the following main result of this section.

**Theorem 8** $\text{Exp}_1(C(q, n, 1; 2))$ is an irreducible cyclic code with parameters

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

**Example 12** The irreducible cyclic code $\text{Exp}_1(C(3, 11, 1; 2))$ has parameters $[22, 5, 12]$ and is distance-optimal.

One question is whether there are infinitely many primes $n$ such that $\text{ord}_{2n}(q) = (n - 1)/2$ for a fixed odd prime power $q$. This question may be open. But experimental data indicates that the answer to this question is positive. Table 1 contains a list of examples of the code $C(q, n, 1; 2)$, where only the parameters $q, n, d(C(q, n, 1; 2)), d(C(q, n, 1; 2)^\perp)$ are listed, and the first best distance and the second best distance denote the minimum distance of the best linear code of length $n$ and dimension $(n - 1)/2$ and the best linear code of length $n$ and dimension $(n + 1)/2$ over $\text{GF}(q)$, respectively, maintained at http://www.codetables.de/. The experimental data in Table 1 shows that the codes $C(q, n, 1; 2)$ and $C(q, n, 1; 2)^\perp$ are optimal or the best known in every case except one.
6 A family of irreducible cyclic codes over GF(q) with parameters 
[(q − 1)n, (n − 1)/2, d ≥ (q − 1)(√n + 1)]

Throughout this section, let \( q > 2 \) be a prime power and let \( n > q \) be an odd prime such that \( m := \text{ord}_{q^{-1}n}(q) = (n - 1)/2 \). Note that \( q < n \) and \( n \) is a prime. We have \( \gcd(q - 1, n) = 1 \) and \( \kappa = 1 \). Consequently, \( \text{ord}_n(q) = \text{ord}_{q^{-1}n}(q) = (n - 1)/2 \).

Let \( \alpha \) be a primitive element of GF\((q^m)\) and let \( \beta = \alpha^{q^m-1}/(q-1)n \). Put \( \lambda = \beta^n \). Then \( \lambda \) is a primitive element of GF\((q)\). Let \( h \) denote the multiplicative inverse of \( n \) modulo \( q - 1 \), where \( 1 \leq h \leq q - 2 \). Then we have \( C_{\lambda h}^{(q, (q^{-1}n))} = \{\lambda n\} \) and 
\[
C_{1}^{(q, (q^{-1}n))} = \{1, q, q^2, \ldots, q^{m-1}\} \pmod{(q - 1)n}.
\]

Take any \( t \) from \( \{(q - 1)i + 1 : 0 \leq i \leq n - 1\} \setminus (C_{1}^{(q, (q^{-1}n))} \cup C_{\lambda h}^{(q, (q^{-1}n))}) \). It can be verified that the cosets \( C_{1}^{(q, (q^{-1}n))}, C_{t}^{(q, (q^{-1}n))} \) and \( C_{\lambda h}^{(q, (q^{-1}n))} \) form a partition of the set \( \{(q - 1)i + 1 : 0 \leq i \leq n - 1\} \). Then for \( i \in \{1, t\} \) the minimal polynomial
\[
M_{\beta^i}(x) = \prod_{j \in C_{i}^{(q, (q^{-1}n))}} (x - \beta^j).
\]

Let \( C(q, n, i) \) denote the \( \lambda \)-constacyclic code of length \( n \) over GF\((q)\) with check polynomial \( M_{\beta^i}(x) \) for \( i \in \{1, t\} \). Then the dimension of \( C(q, n, i) \) equals \( (n - 1)/2 \) for \( i \in \{1, t\} \). Consequently, its dual has dimension \( (n + 1)/2 \). We now prove the following theorem.

**Theorem 9** Let notation and assumptions be the same as before. Then the irreducible constacyclic code \( C(q, n, 1) \) has parameters \([n, (n - 1)/2, d]\) with \( d \geq \sqrt{n} + 1 \) and \( C(q, n, 1)^\perp \) has parameters \([n, (n + 1)/2, d^\perp \geq \sqrt{n}]\).

To prove Theorem 9, we need to do some preparations below. We first prove the following lemma.

**Lemma 7** Let \( q \) be a prime power and let \( n > q \) be an odd prime such that \( \text{ord}_{q^{-1}n}(q) = (n - 1)/2 \). Then \( q \) is a quadratic residue modulo \( n \).

**Proof** It was shown at the very beginning of this section that \( \text{ord}_n(q) = \text{ord}_{q^{-1}n}(q) = (n - 1)/2 \). Let \( \zeta \) be a primitive root of \( n \). Since \( n > q \), then there exists an integer \( i \) with \( 1 \leq i < n - 1 \) such that \( q = \zeta^i \mod n \). It is well known that \( \text{ord}_n(q) = (n - 1)/\gcd(i, n - 1) \). As a result, \( \gcd(i, n - 1) = 2 \) and \( i \) must be even. The desired result then follows.

**Lemma 8** \( \text{Exp}_3(C(q, n, 1)) \) has parameters \([n, (n - 1)/2, d \geq \sqrt{n} + 1]\) and \( \text{Exp}_3(C(q, n, 1))^\perp \) has parameters \([n, (n + 1)/2, d^\perp \geq \sqrt{n}]\).

**Proof** Let \( \text{QR}(n) \) and \( \text{QN}(n) \) denote the set of quadratic residues and nonresidues modulo \( n \), respectively. Note that \( \beta^{q-1} \) is an \( n \)-th primitive root of unity in GF\((q^m)\). It follows from Lemma 7 that the canonical factorization of \( x^n - 1 \) over GF\((q)\) is given by
\[
x^n - 1 = (x - 1) \left( \prod_{i \in \text{QR}(n)} (x - \beta^{(q^{-1})i}) \right) \left( \prod_{i \in \text{QN}(n)} (x - \beta^{(q^{-1})i}) \right).
\]

Since \( M_{\beta^{q-1}}(x) \) is an irreducible divisor of \( x^n - 1 \) and \( \beta^{q-1} \notin \text{GF}(q) \), we have
\[
M_{\beta^{q-1}}(x) = \prod_{i \in \text{QR}(n)} (x - \beta^{(q^{-1})i}),
\]
Table 2 The code $C(q, n, 1)$ and its dual

| $q$ | $n$ | $d$ | Best distance | $d^\perp$ | Best distance |
|-----|-----|-----|---------------|----------|---------------|
| 4   | 7   | 4   | Optimal       | 3        | Optimal       |
| 4   | 11  | 6   | Optimal       | 5        | Optimal       |
| 4   | 13  | 6   | Optimal       | 5        | Optimal       |
| 4   | 19  | 8   | Optimal       | 7        | Optimal       |
| 4   | 23  | 8   | 9            | 7        | 8             |
| 4   | 29  | 12  | Optimal       | 11       | Optimal       |
| 4   | 37  | 12  | 12           | 11       | Optimal       |
| 4   | 47  | 12  | 14           | 11       | 13            |
| 4   | 59  | 15  | 17           | 14       | 16            |
| 4   | 61  | 18  | 18           | 17       | 17            |
| 5   | 11  | 6   | Optimal       | 5        | Optimal       |
| 5   | 19  | 8   | 8            | 7        | 7             |
| 5   | 29  | 12  | Optimal       | 11       | Optimal       |
| 5   | 41  | 14  | 14           | 13       | 13            |
| 7   | 31  | 13  | 13           | 12       | 12            |

Consider now the code $\text{Exp}_3(C(q, n, 1))$, which is the third code associated to the irreducible constacyclic code $C(q, n, 1)$ and has check polynomial $M_{q-1}(x)$. The check polynomial $M_{q-1}(x)$ above shows that $\text{Exp}_3(C(q, n, 1))$ is a quadratic-residue code. The desired conclusions then follow from [14, Theorem 6.6.22].

By assumption $n > q$ and $n$ is a prime. Hence, $\gcd(q-1, n) = 1$. The desired conclusions of Theorem 9 then follow from Theorem 5 and Lemma 8. Theorem 5 tells us that $C(q, n, 1)$ and $\text{Exp}_3(C(q, n, 1))$ are permutation-equivalent. Hence, the constacyclic code $C(q, n, 1)$ is a counterpart of the corresponding quadratic-residue code $\text{Exp}_3(C(q, n, 1))$. Combining Theorems 2 and 9, we get the following main result of this section.

**Theorem 10** The set $\text{Exp}_1(C(q, n, 1))$ is an irreducible cyclic code over $\text{GF}(q)$ with parameters $[(q-1)n, (n-1)/2, d \geq (q-1)(\sqrt{n}+1)]$.

**Example 13** The irreducible cyclic code $\text{Exp}_1(C(3, 11, 1))$ has parameters [22, 5, 12] and is distance-optimal.

Similarly, one would ask if there are infinitely many primes $n$ such that $\text{ord}_{(q-1)n}(q) = (n-1)/2$ for a fixed prime power $q > 2$. This question may be open. But experimental data indicates that the answer to this question is positive. Table 2 contains a list of examples of the code $C(q, n, 1)$, where only the parameters $q, n, d(C(q, n, 1)), d(C(q, n, 1)^\perp)$ are listed, and the first best distance and the second best distance denote the minimum distance of the best linear code of length $n$ and dimension $(n-1)/2$ and the best linear code of length $n$ and dimension $(n+1)/2$ over $\text{GF}(q)$, respectively, maintained at http://www.codetables.de/. The experimental data in Table 2 shows that the codes $C(q, n, 1)$ and $C(q, n, 1)^\perp$ are optimal or the best known in every case except three cases.
7 The objective of studying the two families of constacyclic codes in Sects. 5 and 6

Recall that the constacyclic codes $C(q, n, 1; 2)$ studied in Sect. 5 and $C(q, n, 1)$ treated in Sect. 6 were proved to be permutation-equivalent to a quadratic-residue code under the condition $\text{ord}_{2n}(q) = (n - 1)/2$ and $\text{ord}_{(q-1)n}(q) = (n - 1)/2$, respectively. Then one would question the objective of studying the constacyclic codes $C(q, n, 1; 2)$ and $C(q, n, 1)$. The major objective of doing this is to obtain the parameters of the two irreducible cyclic codes $\text{Exp}_1(C(q, n, 1; 2))$ documented in Theorem 8 and $\text{Exp}_1(C(q, n, 1))$ documented in Theorem 10, where the constacyclic code $C(q, n, 1; 2)$ (or $C(q, n, 1)$) serves as a bridge between the irreducible cyclic codes $\text{Exp}_1(C(q, n, 1; 2))$ and $\text{Exp}_3(C(q, n, 1; 2))$ (or $\text{Exp}_1(C(q, n, 1))$ and $\text{Exp}_3(C(q, n, 1)))$ of length $2n$ and $n$ (or $(q - 1)n$ and $n$), respectively.

Recall that we associated to each irreducible $\lambda$-constacyclic code $C$ of length $n$ an irreducible cyclic code $\text{Exp}_1(C)$ of length $rn/\lambda$ and another irreducible cyclic code $\text{Exp}_3(C)$ of length $n$. By definition, the two cyclic codes $\text{Exp}_1(C)$ and $\text{Exp}_3(C)$ are related to some extent in general via the bridge code $C$, and are closely related in some special cases. One may be able to obtain results about $\text{Exp}_1(C)$ from those about $\text{Exp}_3(C)$ or the other way around in some special cases via the bridge constacyclic code $C$. Hence, studying the bridging constacyclic code $C$ is a key step in this approach. There are other ways to associate a cyclic code to a constacyclic codes $[3]$.

8 Summary and concluding remarks

The main contributions of this paper are the following:

1. The relations among the weight distributions of the irreducible constacyclic code $C$ and the related code $\text{Exp}_1(C)$ and the irreducible constacyclic code $\text{Exp}_2(C)$ were discovered (see Theorem 2), and the relations among the three codes were found (see Theorem 1).
2. For the irreducible constacyclic code $C$ in Eq. (1), another irreducible cyclic code $\text{Exp}_3(C)$ of the same length was associated. Relations between the two codes in a special case were established in Theorem 5, which serves as a bridge between irreducible constacyclic codes and irreducible cyclic codes.
3. The weight distributions of several families of irreducible constacyclic codes were settled. Several families of constacyclic codes with a few weights were produced. These results were documented in Theorem 6 and its corollaries. The dual codes of these irreducible constacyclic codes were also studied (see Theorem 6 and its corollaries). Several families of constacyclic codes with optimal parameters were presented.
4. A family of irreducible cyclic codes over $\text{GF}(q)$ with parameters $[2n, (n - 1)/2, d \geq 2(\sqrt{n} + 1)]$ was constructed in Sect. 5.
5. A family of irreducible cyclic codes over $\text{GF}(q)$ with parameters $[(q - 1)n, (n - 1)/2, d \geq (q - 1)(\sqrt{n} + 1)]$ was constructed in Sect. 6.

It was shown in [25, Theorem 3.6] that the weight distribution of the irreducible constacyclic code $C$ in Eq. (1) can be expressed in terms of the Gaussian periods of order $L$, where $L$ was defined in Eq. (4). However, Gaussian periods were evaluated only in a few cases. Consequently, the weight distribution of the irreducible constacyclic code $C$ in Eq. (1) was known only in a few cases [25]. As explained in Example 3, Theorem 6 complements the work in [25]. Hence, Corollaries 3 and 4 of Theorem 6 may not be easily derived from the results in [25]. This paper treated the code $C$ in Eq. (1) with length $n$ of several special
forms only, while reference [25] documented some general results of $C$ with general length $n$. Hence, the focuses of this paper and [25] are different. It may be extremely difficult to use the results in [25] to study the codes and their duals presented in Sects. 5 and 6, as Gaussian periods of such large orders are not evaluated. Another difference between this paper and [25] is that the dual code $C^\perp$ was studied in this paper, while the dual code of $C$ was not touched in [25].

The evaluation of Gaussian periods is related to several areas of number theory and is known to be a hard problem. Hence, it is very hard to determine the weight distributions of irreducible cyclic codes [9] and irreducible constacyclic codes [25]. The reader is cordially invited to make progress on this topic.

Acknowledgements The authors are very grateful to Prof. Anuradha Sharma for providing reference [25] and the reviewers as well as the editors for their comments and suggestions that improved the presentation of the paper. All the code examples in this paper were computed with the Magma software package.

Funding Z. Sun’s research was supported by the National Natural Science Foundation of China under Grant Number 62002093. X. Wang’s research was supported by the National Natural Science Foundation of China under Grant Number 12001175. C. Ding’s research was supported by the Hong Kong Research Grants Council, Proj. No. 16301522.

Data availability Not applicable.

Code Availability Not applicable.

Declarations

Conflict of interest The authors declare there are no conflict of interest.

References

1. Abdukhalikov K., Ho D.: Extended cyclic codes, maximal arcs and ovoids. Des. Codes Cryptogr. 89, 2283–2294 (2021).
2. Berlekamp E.R.: Negacyclic codes for the Lee metric. In: Proceedings of the Conference on Combinatorial Mathematics and Its Applications, pp. 298–316. University of North Carolina Press, Chapel Hill (1968).
3. Chen B., Fan Y., Lin L., Liu H.: Constacyclic codes over finite fields. Finite Fields Appl. 18(6), 1217–1231 (2012).
4. Chen B., Dinh H.Q., Fan Y., Ling S.: Polyadic constacyclic codes. IEEE Trans. Inf. Theory 61(9), 4895–4904 (2015).
5. Dahl C., Pedersen J.P.: Cyclic and pseudo-cyclic MDS codes of length $q + 1$. J. Comb. Theory Ser. A 59, 130–133 (1992).
6. 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).
7. Ding C., Heng Z.: The subfield codes of ovoid codes. IEEE Trans. Inf. Theory 65(8), 4715–4729 (2019).
8. Ding C., Tang C.: Designs from Linear Codes, 2nd edn World Scientific, Singapore (2022).
9. Ding C., Yang J.: Hamming weights in irreducible cyclic codes. Discr. Math. 313(4), 434–446 (2013).
10. Dong X., Yin S.: The trace representation of $\lambda$-constacyclic codes over $F_q$. J. Liaoning Normal Univ. (Nat. Sci. Ed.) 33, 129–131 (2010).
11. Fang W., Wen J., Fu F.: A $q$-polynomial approach to constacyclic codes. Finite Fields Appl. 47, 161–182 (2017).
12. 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(2), 284–285 (1983).
13. Heng Z., Ding C.: A construction of $q$-ary linear codes with irreducible cyclic codes. Des. Codes Cryptogr. 87, 1087–1108 (2019).
14. Huffman W.C., Pless V.: Fundamentals of Error Correcting Codes. Cambridge University Press, Cambridge (2003).
15. Kølve T.: Codes for Error Detection. World Scientific, Singapore (2007).
16. Krishna A., Sarwate D.V.: Pseudocyclic maximum-distance-separable codes. IEEE Trans. Inf. Theory 36(4), 880–884 (1990).
17. Li F., Yue Q.: The primitive idempotents and weight distributions of irreducible constacyclic codes. Des. Codes Cryptogr. 86, 771–784 (2018).
18. Li F., Yue Q., Liu F.: The weight distribution of constacyclic codes. Adv. Math. Commun. 11(3), 471–480 (2017).
19. Lidl R., Niederreiter H.: Finite Fields. Addison-Wesley, New York (1983).
20. Liu Y., Li R., Lv L., Ma Y.: A class of constacyclic BCH codes and new quantum codes. Quantum Inf. Process. 16, 66 (2017).
21. Mi J., Cao X.: Constructing MDS Galois self-dual constacyclic codes over finite fields. Discr. Math. 344(6), 112388 (2021).
22. Myerson G.: Period polynomials and Gauss sums for finite fields. Acta Arith. 39(3), 251–264 (1981).
23. Pedersen J.P., Dahl C.: Classification of pseudo-cyclic MDS codes. IEEE Trans. Inf. Theory 37(2), 365–370 (1991).
24. Peterson W.W., Weldon E.J. Jr.: Error-Correcting Codes, 2nd edn MIT Press, Cambridge (1972).
25. Sharma A., Rani S.: Trace description and Hamming weights of irreducible constacyclic codes. Adv. Math. Commun. 12(1), 123–141 (2018).
26. Shi Z., Fu F.: The primitive idempotents of irreducible constacyclic codes and LCD cyclic codes. Cryptogr. Commun. 12, 29–52 (2020).
27. Singh M.: Weight distributions of all irreducible $\mu$-constacyclic codes of length $\ell^n$. https://arxiv.org/abs/1806.10600v1.
28. Sun Z., Zhu S., Wang L.: A class of constacyclic BCH codes. Cryptogr. Commun. 12, 265–284 (2020).
29. Wang L., Sun Z., Zhu S.: Hermitian dual-containing narrow-sense constacyclic BCH codes and quantum codes. Quantum Inf. Process. 18, 323 (2019).
30. Wolfmann J.: Projective two-weight irreducible cyclic and constacyclic codes. Finite Fields Appl. 14(2), 351–360 (2008).
31. Zhu S., Sun Z., Li P.: A class of negacyclic BCH codes and its application to quantum codes. Des. Codes Cryptogr. 86, 2139–2165 (2018).

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.