Cryptography and Communications
https://doi.org/10.1007/s12095-026-00882-2

RESEARCH

Cyclic (r, δ) locally recoverable codes from their constacyclic and negacyclic subcodes

Rabia Zengin[1] · **Mehmet Emin Köroğlu**[2]

Received: 17 March 2025 / Accepted: 19 March 2026
© The Author(s) 2026

Abstract
If a symbol in any coordinate of a codeword in a code $\mathcal{C}$ can be repaired by accessing at most r other coordinates, then the positive integer r is called locality of the code. Codes with locality are called locally recoverable codes. Locally recoverable codes are preferred in distributed storage systems, such as Microsoft Azure and Hadoop (used by Facebook), due to their ability to recover a failed node by accessing the minimum number of surviving nodes. A code with (r, δ)-locality is a locally recoverable code that allows recovering $\delta - 1$ erasures simultaneously by reaching at most r other coordinates. In this paper, we obtained constacyclic and negacyclic codes by determining the structure of cyclotomic cosets. Then, we constructed cyclic (r, δ)-LRCs by virtue of their constacyclic and negacyclic subcodes which we found.

Keywords Distributed storage systems · Locally recoverable codes · Cyclic codes · Cyclotomic cosets

Mathematics Subject Classification (2010) 11C08 · 11T06 · 11T71 · 94B05

1 Introduction

Today, large-scale data storage systems are utilized in various fields. In some cases, storage units may not be inherently reliable. Thus, it is crucial to recover the data stored in such units when failures occur. Repetition codes and erasure codes have been employed to address this issue. For instance, 3-repetition codes and Reed-Solomon codes are com-

Mehmet Emin Köroğlu contributed equally to this work.

✉ Mehmet Emin Köroğlu
mkoroglu@yildiz.edu.tr

Rabia Zengin
rabia.zengin@bilgi.edu.tr

[1] Department of Mathematics, Istanbul Bilgi University, Istanbul 34060, Eyüpsultan, Türkiye

[2] Department of Mathematics, Yildiz Technical University, Istanbul 34220, Esenler, Türkiye

Published online: 06 April 2026

monly used for data recovery. However, a key consideration is to minimize the repair cost to expedite the recovery process. While the repair cost of the 3-repetition code is 200 %, the repair cost of the $[14, 10]_2$ Reed-Solomon code used by Facebook is 40 % [1]. Although Reed-Solomon codes offer a lower repair cost, it remains higher than desired. Consequently, Locally Recoverable Codes (LRCs) have been introduced to further reduce the repair cost in storage systems. Due to their applications in distributed storage, LRCs have garnered significant research interest.

The concept of locality in an erasure code was introduced in [2]. A code in which each symbol can be recovered by accessing at most r other symbols is called an LRC, where r is referred to as the locality of the code. A smaller locality is preferable. Additionally, an upper bound on the minimum distance of an LRC, known as the Singleton-Type bound, was established in [2]. If a code's minimum distance attains this bound, it is termed an Singleton-Type optimal LRC (for short STO-LRC). Another bound on the dimension of an LRC, known as the Cadambe-Mazumdar bound, was derived in [3]. Although it is tighter than the Singleton-Type bound, it has practical limitations due to its complexity in computation. STO-LRCs have been constructed in several works, including [4–14].

Due to their efficient encoding and decoding performance, cyclic codes have been favored for constructing LRCs. The locality of some well-known cyclic codes was analyzed in [15]. Cyclic LRCs were derived using their zeros in [16, 17]. Furthermore, constructions of cyclic LRCs using cyclotomic cosets can be found in [18, 19]. In [20], perfect cyclic LRCs were studied. For a comprehensive collection of studies on cyclic LRCs, see [21–25].

Although single-symbol errors are most commonly encountered in storage systems, it is beneficial to be prepared for multiple errors. To address scenarios with multiple node failures, (r, δ)-LRCs were introduced in [26]. If a punctured subcode of a code $\mathcal{C}$ exists such that its support contains index i, its length does not exceed $r + \delta - 1$, and its minimum distance is at least δ, then the i-th symbol of any codeword in $\mathcal{C}$ is said to have (r, δ)-locality, where $\delta \geq 2$. These codes are referred to as (r, δ)-LRCs. In [27], (r, δ)-LRCs were constructed from constacyclic codes. Furthermore, Chen et al. presented optimal cyclic (r, δ) -LRCs with respect to the Singleton-Type bound for codes with (r, δ)-locality in [28].

Additional research on (r, δ)-LRCs has recently advanced with works such as [29–32]. Specifically, Zhang et al. proposed three classes of optimal cyclic (r, δ)-LRCs by utilizing the zeros of the codes [32]. In [29], optimal (r, δ)-LRCs are constructed over $\mathbb{F}_4$. Four classes of optimal pseudo-cyclic (r, δ)-LRCs are obtained in [30]. Furthermore, Galindo et al. constructed optimal (r, δ)-LRCs from monomial-Cartesian codes and their subfield-subcodes [31]. While those works provide powerful frameworks for specific lengths, our construction differs by utilizing the structural relationship between cyclic codes and their constacyclic/negacyclic subcodes. This allows for the construction of (r, δ)-LRCs where the parameters are determined by the order of λ, offering flexibility in the locality r without requiring the strict divisibility constraints often found in Cartesian-based constructions.

There are several papers on (r, δ)-LRCs that satisfy various constraints. For example, in [22], q-ary cyclic (r, δ)-LRCs of length n are constructed under the conditions $n \mid (q + 1)$ and $n \mid (q - 1)$. In [33], families of optimal cyclic codes over $\mathbb{F}_q$ with (r, δ)-locality are derived, subject to the constraints $(r + \delta - 1) \mid (q - 1)$ and $(r + \delta - 1) \mid (q + 1)$. In [34], optimal q-ary cyclic (r, δ)-LRCs of length $\frac{(\delta+1)(q+1)}{2}$ are found under the condition $(\delta + 1) \mid (q - 1)$. In contrast to these studies, we have constructed cyclic codes with (r, δ)

-locality where the subcodes are λ-constacyclic codes, subject to constraints on $o(\lambda)$ but without any restrictions on r and δ. By selecting the subcodes as constacyclic codes of length $q+1$ and negacyclic codes of length $\frac{q+1}{2}$, we have determined the parameters of the cyclic code. Notably, there are no restrictions on the parameter δ, which ensures that the erased code symbol can be recovered, even if one of the repair sets becomes inaccessible. As a result, we expect that these codes will be advantageous for practical implementations.

The remainder of this paper is organized as follows. Section 2 provides the necessary background on linear codes, cyclic codes, and LRCs. Section 3 explores cyclotomic cosets for constacyclic and negacyclic codes, determines the parameters of cyclic codes constructed from these classes, and establishes their locality parameters r and δ using defining sets. Section 4 compares the parameters of the resulting (r, δ)-LRCs with recent results in the literature, specifically those in [29] and [31]. Finally, Section 5 concludes the paper.

2 Preliminaries

In this section, we discuss some basic facts about linear codes, cyclic codes, and LRCs. For further details, readers may refer to [35] and [36]. Let n and k be positive integers, q a prime power, $\mathbb{F}_q$ the finite field of order q, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, and the symbol $[n]$ be the set of integers from 1 to n. A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is a subspace of the vector space $\mathbb{F}_q^n$. The minimum distance $d(\mathcal{C})$ of $\mathcal{C}$ is defined by

$$\min\{d(\mathrm{c}_1, \mathrm{c}_2) : \mathrm{c}_1, \mathrm{c}_2 \in \mathcal{C}, \mathrm{c}_1 \neq \mathrm{c}_2\},$$

where $d(\mathrm{c}_1, \mathrm{c}_2)$ is the number of mutually different coordinates in c_1 and c_2. The dimension $\dim(\mathcal{C})$ is the number of elements in its basis. If $\mathcal{C}$ has dimension k and minimum distance d, it is denoted by $[n, k, d]$, or $[n, k, d]_q$. The dual code of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined as

$$\mathcal{C}^\perp = \left\{\mathrm{u} \in \mathbb{F}_q^n : \mathbf{u} \cdot \mathbf{w} = 0, \forall \mathrm{w} \in \mathcal{C}\right\},$$

where $\mathbf{u} \cdot \mathbf{w} = u_1 w_1 + \cdots + u_n w_n$ for $\mathrm{u} = (u_1, \ldots, u_n)$ and $\mathrm{w} = (w_1, \ldots, w_n) \in \mathbb{F}_q^n$. The order of an element $0 \neq x \in \mathbb{F}_q$, denoted by $o(x)$, is the smallest positive integer u such that $x^u = 1$. The support of c, the set of coordinates where c is nonzero, is denoted by $\mathrm{supp}(\mathrm{c})$. If $\gcd(n, q) = 1$, then the cyclotomic coset of q modulo n containing t is given by

$$C_t = \{tq^j \pmod n : j \geq 0\}.$$

A q-ary linear code $\mathcal{C}$ of length n is called a λ -constacyclic code for $\lambda \in \mathbb{F}_q^*$ if $(\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$. If $\lambda = 1$, then $\mathcal{C}$ is cyclic; if $\lambda = -1$, then $\mathcal{C}$ is negacyclic.

The unique monic polynomial of least degree generating a nonzero ideal I of $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$ is called the generator polynomial of I. Let $\phi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/\langle x^n - \lambda\rangle$ be the homomorphism defined by

$$\phi((c_0, c_1, \ldots, c_{n-1})) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

Then, the generator polynomial of an ideal $\phi(\mathcal{C})$ is also called the generator polynomial of the λ-constacyclic code $\mathcal{C}$. The generator polynomial of $\mathcal{C}^{\perp}$ is called the parity-check polynomial of $\mathcal{C}$.

Let α be an element of an extension field of $\mathbb{F}_q$. Then, the defining set $D(\mathcal{C})$ of a cyclic code $\mathcal{C}$ with generator polynomial $g(x)$ is given by

$$D(\mathcal{C}) = \{i : g(\alpha^i) = 0\}.$$

A punctured code is obtained by deleting one or more coordinates from $\mathcal{C}$. If $\mathcal{L}$ is the set of deleted locations, the punctured code is denoted by $\mathcal{C}_{\mathcal{L}}$.

Proposition 1 *[37] (BCH Bound for Constacyclic Codes) Let $\mathcal{C} = \langle g(x) \rangle$ be a λ-constacyclic code, and let β be an sn-th primitive root of unity with $\beta^n = \lambda$. If the roots of g(x) are $\{\beta^{1+sj} : l \leq j \leq l + d - 2\}$, then $d(\mathcal{C}) \geq d$.*

Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_q$. The code has locality r if, for every $\mathrm{c} = (c_1, \ldots, c_n) \in \mathcal{C}$ and every $i \in [n]$, there exists a subset $R_i \subset [n] \setminus \{i\}$ such that $|R_i| \leq r$ and c_i is a function of the c_v's, where $v \in R_i$. The set R_i is called a repair set for the i-th coordinate.

A code of length n, dimension k, and locality r is denoted by (n, k, r) LRC. In [2], an upper bound on the minimum distance d of an (n, k, r) LRC is given as

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2. \tag{1}$$

This bound is called the Singleton-Type bound.

In [3], an upper bound on the dimension of a q-ary (n, k, r) LRC with distance d is given by

$$k \leq \min_{t \in \mathbb{Z}^+} \left\{ tr + k^q_{\mathrm{opt}}(n - t(r+1), d) \right\}, \tag{2}$$

where $k^q_{\mathrm{opt}}(n - t(r+1), d)$ denotes the largest possible dimension of a code over $\mathbb{F}_q$ with distance d and length $n - t(r+1)$. This bound is known as the Cadambe-Mazumdar bound.

Proposition 2 *Let $\mathcal{C}$ be an (n, k, r) LRC. Then*

$$\frac{k}{n} \leq \frac{r}{r+1}. \tag{3}$$

The formal definition of a code with (r, δ)-locality is as follows.

Definition 1 [26] Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a linear code. Then $\mathcal{C}$ has (r, δ)-locality if, for every $j \in [n]$, there exists a subset $\mathcal{L}_j \subset [n]$ satisfying $j \in \mathcal{L}_j$, $|\mathcal{L}_j| \leq r + \delta - 1$, and $d(\mathcal{C}_{\mathcal{L}_j}) \geq \delta$. The subset $\mathcal{L}_j$ is called the local repair group of the j-th coordinate.

The Singleton-Type bound given in (1) extends to (r, δ)-LRCs.

Theorem 3 *[26] Suppose that $\mathcal{C}$ is an LRC with distance d and (r, δ)-locality. Then an upper bound on d is*

$$d \leq n + 1 - k - (\delta - 1)\left(\left\lceil \frac{k}{r} \right\rceil - 1\right). \tag{4}$$

Definition 2 Let $S(\mathcal{C}) = n + 1 - k - (\delta - 1)\left(\left\lceil \frac{k}{r} \right\rceil - 1\right)$. An (r, δ)-LRC with parameters $[n, k, d]_q$ is called Singleton-Type optimal (STO) if $d = S(\mathcal{C})$ and almost Singleton-Type optimal (ASTO) if $d = S(\mathcal{C}) - 1$.

The Cadambe-Mazumdar bound given in (2) is generalized for (r, δ)-LRCs as follows.

Theorem 4 *[38, 39] Let $\mathcal{C}$ be an (n, k, r) LRC over $\mathbb{F}_q$ with distance d. Then*

$$k \leq \min_{\mu \in \mathbb{Z}^+} \left\{ r\mu + k^q_{opt}(n - \mu(r + \delta - 1), d) \right\}, \tag{5}$$

where $k^q_{opt}(n - \mu(r + \delta - 1), d)$ denotes the largest possible dimension of a code over $\mathbb{F}_q$ with distance d and length $n - \mu(r + \delta - 1)$.

This bound depends on the size of the alphabet used. As with the Cadambe-Mazumdar bound, determining $k^q_{\text{opt}}(n - t(r + \delta - 1), d)$ for a given distance d and length $n - t(r + \delta - 1)$ is generally nontrivial.

3 Cyclic (r, δ) locally recoverable codes from their constacyclic and negacyclic subcodes

In this section, we will obtain (r, δ)-LRCs by using their constacyclic and negacyclic subcodes. We have observed that a constacyclic code is a punctured subcode of a cyclic code that has the same generator polynomial, as shown in the following lemma.

Lemma 5 *Let n and q be two positive integers such that $\gcd(n, q) = 1$, $\lambda \in \mathbb{F}_q^*$, and $o(\lambda) = s$. If $g(x) \mid (x^n - \lambda)$ and $\deg(g(x)) = n - k$, then the [n, k] λ-constacyclic code $\bar{\mathcal{C}} = \langle g(x) \rangle$ is a punctured subcode of the $[sn, n(s - 1) + k]$ cyclic code $\mathcal{C} = \langle g(x) \rangle$.*

Proof Clearly, $\bar{\mathcal{C}} = \langle g(x) \rangle$ is an $[n, k]$ λ -constacyclic code. Since $(x^n - \lambda) \mid (x^{sn} - 1)$ and $g(x) \mid (x^n - \lambda)$, it follows that $g(x) \mid (x^{sn} - 1)$. Thus, $\mathcal{C} = \langle g(x) \rangle$ is an $[sn, n(s - 1) + k]$ cyclic code. Let $g(x) = a_0 + a_1 x + \cdots + a_{n-k} x^{n-k}$. Then the generator matrix of $\bar{\mathcal{C}}$ can be obtained as

$$\bar{G} = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-k} & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{n-k-1} & a_{n-k} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & a_0 & a_1 & a_2 & \dots & a_{n-k} \end{pmatrix}_{k\times n}$$
$$\sim \begin{pmatrix} I_{k\times k} & | & A_{k\times(n-k)} \end{pmatrix}_{k\times n}$$

by deleting $n(s-1)$ coordinates and proper rows from the standard form of the generator matrix of $\mathcal{C} = \langle g(x)\rangle$

$$\begin{pmatrix} I_{n(s-1)\times n(s-1)} & | & B_{n(s-1)\times n)} \\ 0_{k\times n(s-1)} & | & G_{k\times n} \end{pmatrix}_{w\times sn}$$

which is the reduced row echelon form of the generator matrix

$$G = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-k} & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{n-k-1} & a_{n-k} & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & a_0 & a_1 & a_2 & \dots & a_{n-k} & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & a_0 & a_1 & a_2 & \dots & a_{n-k} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & a_0 & a_1 & a_2 & \dots & a_{n-k} \end{pmatrix}_{w\times sn}$$

of $\mathcal{C}$, where $w = n(s-1)+k$. The generator matrix of $\bar{\mathcal{C}}$ is effectively obtained by shortening the cyclic code $\mathcal{C}$ on $n(s-1)$ coordinates and selecting appropriate rows from the standard form. While this is a form of puncturing the dual, in the context of the generator matrix, it is a shortening operation that produces the λ-constacyclic code of length n. □

A condition for a cyclic code whose punctured subcode is a constacyclic code with the same generator polynomial to have (r,δ)-locality is given as follows.

Theorem 6 *Let $\mathcal{C}$ be a cyclic code of length sn with defining set $D(\mathcal{C}) = \{1+sj : j \in \{i_1, i_2, \dots, i_{n-k}\}\}$, where $i_t = i_1 + t - 1$ for $t = 1, \dots, \delta-1$. If there exists $u \in \mathbb{Z}$ such that $sn \mid ((sj+1)(1-q) + s(u-1))$ for some $j \in \{i_1, i_2, \dots, i_{n-k}\}$, then the $[sn, n(s-1)+k]$ code $\mathcal{C}$ has (r,δ)-locality, where $r = n - \delta + 1$.*

Proof Assume that there exists $u \in \mathbb{Z}$ such that $sn \mid ((sj+1)(1-q) + s(u-1))$ for some $j \in \{i_1, i_2, \dots, i_{n-k}\}$. Then

$$\begin{aligned} sn \mid ((sj+1)(1-q) + s(u-1)) &\Rightarrow sn \mid (sj(1-q) - ((q-1) - s(u-1))) \\ &\Rightarrow 1 + s(j+u) - s \equiv (1+sj)q \pmod{sn} \end{aligned}$$

and therefore the cyclotomic cosets C_{1+sj} and $C_{1+s(j+u)}$ have consecutive elements. Here, the word "consecutive" is defined with respect to the arithmetic progression of step size s (i.e., $1+sj$ and $1+s(j+1)$), rather than consecutive integers in the standard sense. If

$g(x) = \prod_{j=i_1}^{i_{n-k}} (x - \gamma^{1+sj})$, where γ is an sn-th root of unity, the constacyclic code $\bar{\mathcal{C}} = \langle g(x) \rangle$ is a punctured subcode by Lemma 5. By the BCH bound and

$$D(\mathcal{C}) = \{1 + sj : j \in \{i_1, i_2, \ldots, i_{n-k}\}, i_t = i_1 + t - 1 \text{ for } t = 1, \ldots, \delta - 1\}$$

the distance of $\bar{\mathcal{C}}$ is at least δ, i.e., $d(\bar{\mathcal{C}}) \geq \delta$. Since the number of deleted coordinates is $n(s-1)$, it follows that $ns - n(s-1) = r + \delta - 1$ and so $r = n - \delta + 1$. Hence, $\mathcal{C}$ is an $[sn, n(s-1) + k]$ cyclic code with (r, δ)-locality. □

We list some parameters of STO and ASTO (r, δ)-LRCs of length *ns* obtained via Theorem 6 in Tables 1 and 2, respectively. Notice that all the obtained codes can detect errors and their locality *r* remains significantly smaller than the dimension of the code.

Example 1 Let $n = 3$, $q = 7$, and $\lambda = 6$. Then $s = o(\lambda) = 2$. Assume that γ is a primitive 9^{th} root of unity. Then $sn \mid ((sj+1)(1-q) - s(u+1))$ for $j = 0$ implies that $9 \mid (-6 - 3(u+1))$ and hence we can choose $u = 0$. Then the cyclotomic coset is $C_1 = \{1, 4, 7\}$. If $\mathcal{C}$ has the defining set $D(\mathcal{C}) = \{1, 4, 7\}$, then $\delta - 1 = 1$, and the generator polynomial of $\mathcal{C}$ is $g(x) = x^3 + 5$. Since $\deg(g(x)) = 3 = 9 - k$, it follows that $k = 6$. Also, the minimum distance of the negacyclic code $\bar{\mathcal{C}} = \langle g(x) \rangle$ is at least 2. Thus, $\mathcal{C}$ is a [9, 6] STO-LRC cyclic code with (2, 2)-locality.

3.1 Locality parameters of cyclic codes whose subcodes are constacyclic codes of length $q + 1$

In this subsection, we have investigated the locality parameters of cyclic codes whose subcodes are constacyclic codes. All q-cyclotomic cosets for λ-constacyclic codes of length $n = q + 1$ when $o(\lambda) \neq q - 1$ are obtained in the following proposition.

Proposition 7 *Let q be an odd prime power integer and λ be an element of $\mathbb{F}_q^*$ such that $s = o(\lambda) \mid (n-2)$, $s \neq n-2$, and $q^2 \equiv 1 \pmod{sn}$. If $n = q + 1$, then all q-cyclotomic cosets are:*

i) $C_1 = \{1, n-1\}$,
ii) $C_{\left(\frac{n}{2}\right)^i} = \left\{\left(\frac{n}{2}\right)^i\right\}$, *where* $i = 1, 2$,
iii) $C_{1+sj} = \{1 + sj, n + s(n-j) - 1\}$, *where* $3 \leq j \leq \frac{n}{2}$, *if* $n \leq 2s + 2$ *and* $s \neq 1$.

Furthermore, the number of all q-cyclotomic cosets is $\frac{n+2}{2}$.

Proof The number of elements in the q-cyclotomic cosets is at most 2 due to $q^2 \equiv 1 \pmod{sn}$. Clearly, $C_1 = \{1, n-1\}$. Let $i = 1$. Since $q^2 \equiv 1 \pmod{sn}$, it follows that

$$\frac{n}{2}q = \frac{q+1}{2}q \equiv \frac{n}{2} \pmod{sn}.$$

If $i = 2$, then

Table 1 Some parameters of STO (r, δ)-LRCs of length ns obtained via Theorem 6

p	n	s	λ	u	j	t	$D(\mathcal{C})$	$g(x)$	ns	$\dim(\mathcal{C})$	$d(\mathcal{C})$	r	δ
3	4	2	2	0	1	2	$\{1,3\}$	x^2+2x+2	8	6	2	3	2
5	3	2	4	0	0	2	$\{1,5\}$	x^2+4x+1	6	4	2	2	2
5	12	4	2	6	1	4	$\{1,5,25,29\}$	x^4+4x^2+2	48	44	2	11	2
7	3	3	2	0	0	3	$\{1,4,7\}$	x^3+5	9	6	2	2	2
7	4	2	6	0	2	2	$\{3,5\}$	x^2+3x+1	8	6	2	3	2
7	8	2	6	0	2	2	$\{3,5\}$	x^2+4x+6	16	14	2	7	2
7	12	6	3	8	5	6	$\{1,7,25,31,49,55\}$	x^6+5x^3+2	72	66	2	11	2
11	3	2	10	0	0	2	$\{1,5\}$	$x^2+10x+1$	6	4	2	2	2
11	4	2	10	0	3	2	$\{5,7\}$	$x^2+3x+10$	8	6	2	3	2
11	6	2	10	0	0	2	$\{1,11\}$	x^2+5x+1	12	10	2	5	2
11	12	2	10	0	9	2	$\{17,19\}$	$x^2+5x+10$	24	22	2	11	2
13	3	3	3	2	0	3	$\{1,4,7\}$	x^3+10	9	6	2	2	2
13	6	4	8	4	5	2	$\{1,9,13,21\}$	x^4+6x^2+10	24	20	2	5	2
13	7	2	12	0	0	2	$\{1,13\}$	x^2+8x+1	14	12	2	6	2
13	8	3	3	5	0	2	$\{1,13,16\}$	$x^3+4x^2+11x+5$	24	21	2	7	2
13	9	4	8	1	2	3	$\{1,9,13,25\}$	$x^4+5x^3+11x+3$	36	32	2	8	2
17	3	2	16	0	0	2	$\{1,5\}$	$x^2+16x+1$	6	4	2	2	2
17	6	4	13	3	4	2	$\{1,5,13,17\}$	x^4+4x^2+16	24	20	2	5	2
17	8	4	13	5	0	2	$\{1,5,17,21\}$	x^4+9x^2+15	32	28	2	7	2
17	9	4	13	6	4	2	$\{1,5,13,17\}$	$x^4+16x^3+2x^2+x+1$	36	32	2	8	2
17	9	2	16	0	0	2	$\{1,17\}$	$x^2+13x+1$	18	16	2	8	2
17	12	4	13	9	1	2	$\{5,25,37,41\}$	$x^4+4x^3+8x^2+15x+13$	48	44	2	11	2
17	15	4	13	9	4	4	$\{1,17,49,53\}$	$x^4+3x^3+2x^2+7x+1$	60	56	2	14	2
19	4	2	18	0	1	2	$\{1,3\}$	$x^2+13x+18$	8	6	2	3	2
19	5	2	18	0	0	2	$\{1,9\}$	$x^2+14x+1$	10	8	2	4	2

Table 1 (continued)

p	n	s	λ	u	j	t	$D(\mathcal{C})$	$g(x)$	ns	$\dim(\mathcal{C})$	$d(\mathcal{C})$	r	δ
19	9	6	8	4	0	3	$\{1, 7, 19, 25, , 17, 19\}$ $37, 43\}$	$x^6 + 3x^3 + 9$	54	48	2	8	2
19	10	2	18	0	5	2	$\{9, 11\}$	$x^2 + 8x + 1$	20	18	2	9	2
19	12	3	7	7	6	2	$\{1, 4, 19\}$	$x^3 + 15x^2X + 5x + 10$	36	33	2	11	2
19	15	3	7	4	4	2	$\{13, 22, 25\}$	$x^3 + 8x^2 + 18x + 12$	45	42	2	14	2

Table 2 Some parameters of ASTO (r, δ)-LRCs of length ns obtained via Theorem 6

p	n	s	λ	u	j	t	$D(\mathcal{C})$	$g(x)$	ns	$\dim(\mathcal{C})$	$d(\mathcal{C})$	r	δ
3	4	2	2	2	0	2	$\{1,3,5,7\}$	x^4+1	8	4	2	2	3
3	10	2	2	0	9	4	$\{11,13,17,19\}$	x^4+2x^3+x+1	20	16	2	8	3
3	13	2	2	10	4	3	$\{1,3,9\}$	x^3+2x+1	26	23	2	12	2
5	3	2	4	2	2	2	$\{1,3,5\}$	x^3+1	6	3	2	2	2
5	4	2	4	3	0	2	$\{1,3,5,7\}$	x^4+1	8	4	2	2	3
5	12	2	4	11	11	2	$\{9,19,21,23\}$	x^4+2x^3+4x+1	24	20	2	10	3
5	13	2	4	11	2	4	$\{1,5,21,25\}$	$x^4+3x^3+x^2+3x+1$	26	22	2	11	3
7	4	2	6	2	3	2	$\{1,3,5,7\}$	x^4+1	8	4	2	2	3
7	10	2	6	0	6	4	$\{11,13,17,19\}$	$x^4+4x^3+4x^2+3x+1$	20	16	2	8	3
11	3	2	10	2	2	2	$\{1,3,5\}$	x^3+1	6	3	2	2	2
11	4	2	10	2	0	2	$\{1,3,5,7\}$	x^4+1	8	4	2	2	3
11	9	5	4	0	6	6	$\{1,11,16,26,31,41\}$	x^6+5x^3+3	45	39	2	8	2
11	15	2	10	1	4	2	$\{1,9,11\}$	x^3+10x^2+4x+4	30	27	2	14	2
13	14	3	3	7	6	2	$\{16,19,37,40\}$	x^4+2x^2+9	42	38	2	13	2
13	14	2	12	5	1	2	$\{1,3,11,13\}$	$x^4+2x^3+3x^2+11x+1$	28	24	2	12	3
13	15	4	8	7	14	4	$\{9,21,25,33,57\}$	$x^5+12x^4+8x^3+x^2+5x+7$	60	55	2	14	2
17	3	2	16	2	2	2	$\{1,3,5\}$	x^3+1	6	3	2	2	2
17	12	2	16	5	11	2	$\{7,9,23\}$	$x^3+10x^2+12x+9$	24	21	2	11	2
19	4	2	18	2	0	2	$\{1,3,5,7\}$	x^4+1	8	4	2	2	3
19	10	3	7	5	6	2	$\{1,4,16,19\}$	x^4+17x^2+7	30	26	2	9	2
19	10	2	18	4	8	2	$\{3,5,15,17\}$	$x^4+6x^3+2x^2+6x+1$	20	16	2	8	3
19	15	3	7	10	1	2	$\{4,16,31,34\}$	$x^4+7x^3+2x^2+6x+5$	45	41	2	14	2
19	15	2	18	4	13	2	$\{3,5,27\}$	$x^3+6x^2+3x+11$	30	27	2	14	2

$$\left(\frac{n}{2}\right)^2 q = \frac{(q+1)^2}{4} q \equiv \frac{n}{2} \pmod{sn}.$$

Also, $\frac{n^2}{4} \equiv \frac{n}{2} \pmod{sn}$. This implies that $\left(\frac{n}{2}\right)^2 q \equiv \frac{n}{2}^2 \pmod{sn}$. Therefore, $C_{\left(\frac{n}{2}\right)^i} = \left\{\left(\frac{n}{2}\right)^i\right\}$, where $i = 1, 2$. Now, let $3 \le j \le \frac{n}{2}$. Then

$$\begin{aligned}(1+sj)q = n - 1 + sj(n-1) &= n - 1 + s(n-j) + sn(j-1) \\ &\equiv n + s(n-j) - 1 \pmod{sn}.\end{aligned}$$

By the assumption $n \le 2s + 2$ and $s > 1$, it follows that $n \le 2s + 2 < 3s + 1$. Since $3 \le j$ and $n < 1 + 3s$, we get $s(n-j) \le s(n-3)$, and therefore

$$n - 1 + s(n-j) \le n - 1 + s(n-3) \le sn - (3s - n + 1) < sn.$$

Suppose $1 + sj = n + s(n-j) - 1$. Then

$$\begin{aligned}1 + sj = n + sn - sj - 1 \Rightarrow 2(1+sj) &= n(s+1) \\ \Rightarrow j = \frac{sn + n - 2}{2s} &= \frac{n}{2} + \frac{n-2}{2s} > \frac{n}{2}.\end{aligned}$$

This is a contradiction. Thus, $C_{1+sj} = \{1 + sj, n + s(n-j) - 1\}$, where $3 \le j \le \frac{n}{2}$. Hence, the number of q-cyclotomic cosets is

$$\bigcup_{j=3}^{\frac{n}{2}} |C_{1+sj}| + \bigcup_{i=1}^{2} |C_{\left(\frac{n}{2}\right)^i}| + |C_1| = \frac{n+2}{2}.$$

□

Example 2 Let $n = 8$, $q = 7$, and $\lambda = 2$. Then all 7-cyclotomic cosets are:

$$C_1 = \{1, 7\}, \mathrm{C}_4 = \{4\}, \mathrm{C}_{10} = \{10, 22\}, \mathrm{C}_{13} = \{13, 19\}, \mathrm{C}_{16} = \{16\}.$$

In the following proposition, we have examined whether the elements of a cyclotomic coset satisfying the conditions of Proposition 7 can be consecutive or not.

Proposition 8 *Let q be an odd prime power integer, $n = q + 1$, and λ be an element of $\mathbb{F}_q^*$ such that $s = o(\lambda) \mid (n-2)$, $s \ne n - 2$, and $q^2 \equiv 1 \pmod{sn}$. Then there are no consecutive elements in the cyclotomic coset C_{1+sj}.*

Proof Contrary to the assumption, suppose that the cyclotomic coset C_{1+sj} has consecutive elements. Due to $q^2 \equiv 1 \pmod{sn}$, the number of elements of C_{1+sj} is at most 2. By Proposition 7, $C_{1+sj} = \{1 + sj, n + s(n-j) - 1\}$, where $3 \le j \le \frac{n}{2}$. Since the elements are consecutive,

$$\begin{aligned} 1 + sj + s &= n + s(n-j) - 1 \\ &\Rightarrow 2sj = n + s(n-1) - 2 \\ &\Rightarrow j = \frac{n + s(n-1) - 2}{2s} = \frac{n-2}{2s} + \frac{n-1}{2}. \end{aligned}$$

The assumption $s \mid (n-2)$ implies that $\frac{n-2}{2s} \in \mathbb{Z}$. Also, $n-1$ is an odd integer since $n = q+1$ and q is odd. Thus, $j \notin \mathbb{Z}$, which is a contradiction. If C_1 has consecutive elements, then $1 + s = n - 1$, i.e., $s = n - 2$. This contradicts $s \neq n-2$. Hence, there are no cyclotomic cosets whose elements are consecutive. □

In the following theorem, we have obtained (r, δ)-LRCs by obtaining conditions to have a union of cyclotomic cosets whose elements are consecutive.

Theorem 9 *Let q be an odd prime power integer, $n = q + 1$, and λ be an element of $\mathbb{F}_q^*$ such that $s = o(\lambda) \mid (n-2)$, $s \neq n-2$, and $q^2 \equiv 1 \pmod{sn}$. If $j = \frac{n-2}{2s} - 1$, $j = \frac{n^2-4}{4s} + 1$, $j = \frac{n+2}{2s} + n - 1$, or $j = \frac{n(4-n)}{4} - s(n+1)$ for some $j \in \{i_1, i_2, \ldots, i_{n-k}\}$, then the $[sn, n(s-1)+k]$ code $\mathcal{C}$ has (r, δ)-locality, where $r = n - \delta + 1$.*

Proof If $i = 1$, then the cyclotomic coset $C_{\left(\frac{n}{2}\right)^i} = \left\{\frac{n}{2}\right\}$. Let $j = \frac{n-2}{2s} + 1$. Then $n + 2s = 2 + 2sj$, i.e., $\frac{n}{2} + s = 1 + sj$. If $j = \frac{n+2}{2s} + n - 1$, then $-2sj = -n - 2 + 2s(1-n)$, and therefore $n + 2s = 2n + 2s(n-j) + 2$. It follows that $\frac{n}{2} + s = n + s(n-j) + 1$. So, $C_{\frac{n}{2}} \cup C_{1+sj}$ has at least 2 consecutive elements if $j = \frac{n-2}{2s} - 1$ or $j = \frac{n+2}{2s} + n - 1$. Similarly, if $j = \frac{n^2-4}{4s} + 1$, then $n^2 + 4s = 4 + 4sj$, and therefore $\frac{n^2}{4} + s = 1 + sj$. If $j = \frac{n(4-n)}{4} - s(n+1)$, then $-4j = 4s(n+1) + n(n-4)$, and therefore $n^2 + 4s = 4n + 4s(n-j) - 4$, i.e., $\frac{n^2}{4} + s = n + s(n-j) - 1$. Thus, the set $C_{\left(\frac{n}{2}\right)^i} \cup C_{1+sj}$ has at least 2 consecutive elements when $i = 2$. Clearly, $\delta \geq 2$ in each case. □

In Table 3, we list some parameters of STO (r, δ)-LRCs of length $s(q+1)$ obtained via Theorem 9. Notice that all the obtained codes can detect errors, and their locality r remains reasonably smaller than the dimension of the code.

Remark 1 If $j = \frac{n+2}{2s} + n - 1$ and $j = \frac{n-2}{2s} - 1$ or $j = \frac{n(4-n)}{4} - s(n+1)$ and $j = \frac{n(4-n)}{4} - s(n+1)$ in Theorem 9, then $\delta = 3$.

Example 3 Let $n = 6$, $q = 5$ and $\lambda = 4$. Then $s = 2$ and all 5 -cyclotomic cosets are

$$C_1 = \{1, 5\}, \quad C_3 = \{3\}, \quad C_7 = \{7, 11\}, \quad C_9 = \{9\}.$$

For $n = 6$ and $j = \frac{n^2-4}{4s} + 1 = 5$, the corresponding cyclotomic cosets are $C_{1+sj} = C_{11}$ and $C_{(\frac{n}{2})^2} = C_9$. Then $C_{11} \cup C_9 = \{7, 9, 11\}$ and therefore $\delta - 1 = 3$ and $6 - k = 3$, i.e., $k = 3$. So, $r = n - \delta + 1 = 3$. Hence, $\mathcal{C}$ is a [12, 9] code with (3, 4)-locality.

Table 3 Some parameters of STO (r, δ)-LRCs of length $s(q+1)$ obtained via Theorem 9

p	n	s	λ	j	t	$D(\mathcal{C})$	$g(x)$	ns	$\dim(\mathcal{C})$	$d(\mathcal{C})$	r	δ
7	8	2	6	0	2	$\{1,4,7,12\}$	x^4+x^3+x+6	16	12	4	7	2
11	12	2	10	14	2	$\{5,6,7,18\}$	$x^4+6x^3+6x+10$	24	20	4	11	2
13	14	4	8	0	2	$\{1,7,13,35\}$	$x^4+5x^3+12x+1$	56	52	2	13	2
19	20	2	18	38	2	$\{10,23,30,37\}$	$x^4+12x^3+12x+18$	40	36	4	19	2

Remark 2 It can be obtained cyclic codes with better locality by virtue of the structure of constacyclic codes. Namely, although the cyclic codes in Examples 1 and 3 have the same length and dimension, the code in Example 3 has better locality due to the choices of the cyclotomic cosets as in Proposition 7.

The structure of all q-cyclotomic cosets for λ-constacyclic codes of length $n = q + 1$ when $o(\lambda) = q - 1$ are found as follows.

Proposition 10 *Let q be an odd prime power integer and λ be an element of $\mathbb{F}_q^*$ such that $o(\lambda) = s$ and $q^2 \equiv 1 (mod sn)$. If $n = q + 1$ and $s = n - 2$, then all q-cyclotomic cosets are*

i) $C_1 = \{1, n - 1\}$,
ii) $C_{1+sj} = \{1 + sj, n + s(n - j) - 1\}$, *where* $2 \leq j \leq \frac{n}{2}$.

Moreover, the number of all q-cyclotomic cosets is $\frac{n}{2}$.

Proof The proof is similar to proof of Proposition 7. When $s = q - 1$, there is no cyclotomic coset that has only one element. Otherwise, there would exist some j such that $(1 + sj)q \equiv 1 + sj (\mathrm{mod}\ sn)$. Due to $s = q - 1$,

$$sn \mid (1 + sj)(q - 1) \Rightarrow n \mid (1 + sj)$$

However, if $n \mid (1 + sj)$ then there exists some $x \in \mathbb{Z}$ such that $1 + sj = nx$. Then

$$x = \frac{1 + sj}{n} = \frac{1}{n} + \frac{sj}{n}$$

which is a contradiction. Therefore, there is no such a j. The number of q-cyclotomic cosets is

$$\bigcup_{j=2}^{\frac{n}{2}} |C_{1+sj}| + |C_1| = \frac{n}{2}.$$

□

Example 4 Let $n = 8$, $q = 7$ and $\lambda = 3$. Then $s = 6$ and all 7-cyclotomic cosets are

$$C_1 = \{1, 7\}, \quad C_{13} = \{13, 43\}, \quad C_{19} = \{19, 37\}, \quad C_{25} = \{25, 31\}.$$

Theorem 11 *Let $n = q + 1$, $s = n - 2$ and $\mathcal{C}$ be a cyclic code of length sn with defining set $\{1 + sj : j \in \{i_1, i_2, \ldots, i_{n-k}\}\}$, where $i_t = i_1 + t - 1$ for $1 \leq t \leq \delta - 1$. If $j = 2$, $j = \frac{n}{2}$ or there exists $u \in \mathbb{Z}$ such that $u = n - j + 2$ for some $j \in \{i_1, i_2, \ldots, i_{n-k}\}$, then the $[sn, n(s - 1) + k]$ code $\mathcal{C}$ has (r, δ)-locality, where $r = n - \delta + 1$.*

Proof Let $n = q + 1$. By Proposition 10, all q-cyclotomic cosets are

i) $C_1 = \{1, n-1\}$,
ii) $C_{1+sj} = \{1 + sj, n + s(n-j) - 1\}$, where $2 \le j \le \frac{n}{2}$.

Note that the cyclotomic coset C_1 has 2 consecutive elements owing to $s = n - 2$, i.e., $1 + s = n - 1$. Suppose $j = 2$. Then

$$\begin{aligned} j = 2 \Rightarrow j &= \frac{n-2+s}{s} \\ &\Rightarrow n - 1 + s = 1 + sj \end{aligned}$$

and therefore the elements $n - 1 \in C_1$ and $1 + sj \in C_{1+sj}$ are consecutive. So, $C_1 \cup C_{1+sj}$ has at least 3 consecutive elements, i.e, $\delta \ge 3$. Let $j = \frac{n}{2}$. Due to $s = n - 2$,

$$\begin{aligned} j = \frac{n}{2} \Rightarrow j &= \frac{n-2-s+sn}{2s} \\ &\Rightarrow 2sj = n + sn - 1 - s - 1 \\ &\Rightarrow 1 + sj + s = n + s(n-j) - 1. \end{aligned}$$

Thus, the cyclotomic coset C_{1+sj} has 2 consecutive elements and the number of elements of $C_1 \cup C_{1+sj}$ is at least 4, i.e., $\delta \ge 4$. Assume that there exists $u \in \mathbb{Z}$ such that $u = n - j + 2$ for some $j \in [i_1, i_{n-k}]$,

$$\begin{aligned} u = n - j + 2 \Rightarrow u &= \frac{n-2+s(n-j)+s}{s} \\ &\Rightarrow n + s(n-j) - 1 + s = 1 + su. \end{aligned}$$

Then the elements $n + s(n-j) - 1 \in C_{1+sj}$ and $1 + su \in C_{1+su}$ are consecutive. Therefore, $C_1 \cup C_{1+sj} \cup C_{1+su}$ has at least 4 consecutive elements, i.e., $\delta \ge 4$. Hence, the cyclic code $\mathcal{C}$ of length sn with defining set $\{1 + sj : j \in \{i_1, i_2, \ldots, i_{n-k}\}\}$, where $i_t = i_1 + t - 1$ for $1 \le t \le \delta - 1$ has (r, δ)-locality, where $r = n - \delta + 1$ by Theorem 6. □

In Table 4, we list some parameters of ASTO (r, δ)-LRCs of length $s(q+1)$ obtained via Theorem 11.

Example 5 Let $n = 6$, $q = 5$ and $\lambda = 2$. Then $s = 4$ and all 5-cyclotomic cosets are

$$C_1 = \{1, 5\}, \quad C_9 = \{9, 21\}, \quad C_{13} = \{13, 17\}.$$

Then $\{1, 5, 9\} \in C_1 \cup C_9$ and therefore $\delta - 1 = 3$. So, $r = n - \delta + 1 = 3$. Hence, the code with defining set $C_1 \cup C_9$ is a [24, 20] cyclic code with (3, 4)-locality.

We summarized the locality parameters of the cyclic codes of length $n = q + 1$ obtained in the following table.

Table 4 Some parameters ASTO (r, δ)-LRCs of length $s(q+1)$ obtained via Theorem 11

p	n	s	λ	u	j	t	$D(\mathcal{C})$	$g(x)$	ns	$\dim(\mathcal{C})$	$d(\mathcal{C})$	r	δ
19	20	2	18	20	2	2	$\{1,5,15,19\}$	$x^4+18x^3+6x^2+x+1$	40	36	2	18	3

3.2 Locality parameters of cyclic codes whose subcodes are negacyclic codes of length $\frac{q+1}{2}$

In this subsection, we have proposed the locality parameters of cyclic codes whose punctured subcodes are negacyclic codes. We will get all q-cyclotomic cosets for negacyclic codes when $q \equiv 1(\mathrm{mod}\ 4)$ in the following proposition.

Proposition 12 *Let q be an odd integer such that $q \equiv 1(mod 4)$, $n = \frac{q+1}{2}$ and $J = \{\frac{q-i}{2} | i \in \mathbb{Z} isodd, n+2 \leq i \leq 2n-1\}$. Then the cyclotomic cosets are*

i) $C_{1+2j} = \{\frac{q+1}{2}\}$ *if* $j = \frac{q-1}{4}$,
ii) $C_{1+2j} = \{1+2j, q-2j\}$ *if* $j \in J$.

Further, the number of the cyclotomic cosets is $\frac{n+1}{2}$.

Proof Due to $n = \frac{q+1}{2}$, we have $q^2 - 1 = (q-1)(q+1) \equiv 0(\mathrm{mod}\ 2n)$. Then $q^2 \equiv 1(\mathrm{mod}\ 2n)$ and therefore $(1+2j)q^2 \equiv 1 + 2j(\mathrm{mod}\ 2n)$. So $|C_{1+2j}| \leq 2$. Let $j \in J$. Also,

$$(1+2j)q = (1+2j)(2n-1) = 2n - 1 + 4nj - 2j \equiv -2j - 1(\mathrm{mod}\ 2n). \tag{6}$$

On the other hand,

$$q - 2j = q + 1 - 2j - 1 = 2n - (2j+1) \equiv -2j - 1(\mathrm{mod}\ 2n). \tag{7}$$

By the (6) and (7), we get $q - 2j \equiv (1+2j)q(\mathrm{mod}\ 2n)$. Since $q - 2j = 2n - 1 - 2j = 2n - (1+2j) < 2n$, we obtain $C_{1+2j} = \{1+2j, q-2j\}$ for $j \in J$. To show $1 + 2j \neq q - 2j$, on the contrary, assume $1 + 2j = q - 2j$. Then $4j = q - 1$, i.e., $j = \frac{q-1}{4}$. If $j = \frac{q-1}{4} \in J$, then there exists some i such that $\frac{q-1}{4} = \frac{q-i}{2}$. It follows that $i = \frac{q+1}{2}$. This contradicts with $n + 2 \leq i \leq 2n - 1$. Thus $j \notin J$ and $1 + 2j \neq q - 2j$. Let $j = \frac{q-1}{4}$.Then$1 + 2j = \frac{q+1}{2}$and$(1+2j)q \equiv \frac{q+1}{2}(\mathrm{mod}\ 2n)$dueto$q^2 \equiv 1(\mathrm{mod}\ 2n)$.Clearly, $\frac{q+1}{2} < n$. Therefore, $C_{\frac{q+1}{2}} = \{\frac{q+1}{2}\}$. Note that n is an odd integer. Otherwise, there exists an integer m such that $n = 2m$ and therefore $q + 1 = 4m$. This implies that $q \equiv -1(\mathrm{mod}\ 4)$ which is a contradiction because $q \equiv 1(\mathrm{mod}\ 4)$ and so n is odd. Furthermore, we have $\frac{n-1}{2}$ choices from the range of i. For $j = \frac{q-1}{4}$, there is a q-cyclotomic coset as well. Hence, the number of q-cyclotomic cosets is

$$\bigcup_{j \in J} |C_{1+2j}| + \bigcup_{j = \frac{q-1}{4}} |C_{1+2j}| = \frac{n+1}{2}.$$

□

Corollary 1 *There is no cyclotomic coset whose elements are consecutive when $n = \frac{q+1}{4}$ and $q \equiv 1(mod 4)$.*

Table 5 Cyclic codes with (r, δ)-locality when $n = q + 1$

j	δ	r
$j = \frac{n-2}{2s} - 1$	2	$n(s-1)-1$
$j = \frac{n^2-4}{4s} + 1$	2	$n(s-1)-1$
$j = \frac{n+2}{2s} + n - 1$	2	$n(s-1)-1$
$j = \frac{n(4-n)}{4} - s(n+1)$	2	$n(s-1)-1$
2	3	$n(s-1)-2$
$\frac{n}{2}$	4	$n(s-1)-3$
$n-u+2$	4	$n(s-1)-3$

Proof On the contrary to the assumption, suppose that the cyclotomic coset $C_{1+2j} = \{1 + 2j, q - 2j\}$ has consecutive elements. Thus, $1 + 2j + 2 = q - 2j$, i.e., $j = \frac{q-3}{4}$. However, this contradicts with $q \equiv 1 (\mathrm{mod}\ 4)$. □

Example 6 Let $q = 5$. Then $n = 3$ and the q-cyclotomic cosets are

$$C_1 = \{1, 5\}, \mathrm{C}_3 = \{3\}.$$

Example 7 Let $q = 17$. Then $n = 9$ and the q-cyclotomic cosets are

$$C_1 = \{1, 17\}, \mathrm{C}_3 = \{3, 15\}, \mathrm{C}_5 = \{5, 13\}, \mathrm{C}_7 = \{7, 11\}, \mathrm{C}_9 = \{9\}.$$

Theorem 13 *Let $n = \frac{q+1}{2}$, $q \equiv 1 (mod 4)$ and $\mathcal{C}$ be a cyclic code of length 2n with defining set $\{1 + 2j : j \in \{i_1, i_2, \ldots, i_{n-k}\}\}$, where $i_t = i_1 + t - 1$ for $1 \leq t \leq \delta - 1$. If $j = \frac{q-5}{4}$ or $u = j + 1$ for an integer u and for some $j \in \{i_1, i_2, \ldots, i_{n-k}\}$, then the $[2n, n + k]$ code $\mathcal{C}$ has (r, δ)-locality, where $r = n - \delta + 1$.*

Proof Let $n = \frac{q+1}{2}$ and $u = j + 1$. Then $1 + sj + s = 1 + su$ and therefore the set $C_{1+sj} \cup C_{1+su}$ has 2 consecutive elements. If $j = \frac{q-5}{4}$, then $j = \frac{2q-4-q-1}{4}$ and therefore $q - 2j = 2 + \frac{q+1}{2}$. Also, $j = \frac{q-5}{4}$ implies that $4j + 6 = q + 1$, i.e., $1 + 2j + 2 = \frac{q+1}{2}$. Thus, the set $C_{1+2j} \cup C_{\frac{q+1}{2}}$ has 3 consecutive elements which is maximum. Hence, $\mathcal{C}$ is an $[2n, n + k]$ code with (r, δ)-locality, where $r = n - \delta + 1$. □

In Table 6, we list some parameters of STO (r, δ)-LRCs of length $n = \frac{q+1}{2}$ obtained via Theorem 13.

Example 8 Let $q = 13$. Then $n = 7$, $\lambda = 12$ and the q-cyclotomic cosets are

$$C_1 = \{1, 13\}, \mathrm{C}_3 = \{3, 11\}, \mathrm{C}_5 = \{5, 9\}, \mathrm{C}_7 = \{7\}.$$

So, the code with defining set $C_5 \cup C_7$ is a [26, 11] cyclic code with (4, 4)-locality.

Table 6 Some parameters of STO (r, δ)-LRCs of length $n = \frac{q+1}{2}$ obtained via Theorem 13

p	n	s	λ	u	j	t	$D(\mathcal{C})$	$g(x)$	ns	$\dim(\mathcal{C})$	$d(\mathcal{C})$	r	δ
17	9	4	13	4	3	2	$\{1,5,13,17\}$	$x^4+16x^3+2x^2+x+1$	36	32	2	8	2
29	15	4	12	7	6	2	$\{1,5,25,29\}$	$x^4+8x^3+19x^2+21x+1$	60	56	2	14	2

We will obtain the cyclotomic cosets for negacyclic codes when $q \equiv 3 (\mathrm{mod}\ 4)$ in the following proposition.

Proposition 14 *Let q be an odd integer such that $q \equiv 3 (mod 4)$, $n = \frac{q+1}{2}$ and $J = \{\frac{q-i}{2} | i \in \mathbb{Z} is odd, n+1 \leq i \leq 2n-1\}$. Then all q-cyclotomic cosets are $C_{1+2j} = \{1+2j, q-2j\}$ for $j \in J$. Moreover, the number of the cyclotomic cosets is $\frac{n}{2}$.*

Proof Similar to proof of Proposition 12, the q-cyclotomic cosets are $C_{1+2j} = \{1+2j, q-2j\}$ for $j \in J$. Moreover, we have $\frac{n}{2}$ choices from the range of i. Therefore, the number of q-cyclotomic cosets is

$$\bigcup_{j \in J} |C_{1+2j}| = \frac{n}{2}.$$

□

Example 9 Let $q = 11$. Then $n = 6$ and the q-cyclotomic cosets are

$$C_1 = \{1, 11\}, \quad C_3 = \{3, 9\}, \quad C_5 = \{5, 7\}.$$

Theorem 15 *Let $n = \frac{q+1}{2}$, $q \equiv 3 (mod 4)$ and $\mathcal{C}$ be a cyclic code of length $2n$ with defining set $\{1+2j : j \in \{i_1, i_2, \ldots, i_{n-k}\}\}$, where $i_t = i_1 + t - 1$ for $1 \leq t \leq \delta - 1$. If $j = \frac{q-3}{4}$ or there exists $u \in \mathbb{Z}$ such that $u = \frac{q-2j-1}{2}$ for some $j \in \{i_1, i_2, \ldots, i_{n-k}\}$, then the $[2n, n+k]$ code $\mathcal{C}$ has (r, δ)-locality, where $r = n - \delta + 1$.*

Proof Let $n = \frac{q+1}{2}$ and $j = \frac{q-3}{4}$. Then $1 + 2j + 2 = q - 2j$ and therefore the cyclotomic coset C_{1+sj} has 2 consecutive elements. If, for some j, there exists $u \in \mathbb{Z}$ such that $u = \frac{q-2j-1}{2}$ then the elements $q - 2j \in C_{1+2j}$ and $1 + 2u \in C_{1+2u}$ are consecutive. Then $\mathcal{C}$ is an $[2n, n+k]$ code $\mathcal{C}$ has (r, δ)-locality, where $r = n - \delta + 1$. □

Example 10 Let $q = 19$. Then $n = 10$, $\lambda = 18$ and the q-cyclotomic cosets are

$$C_1 = \{1, 19\}, C_3 = \{3, 17\}, C_5 = \{5, 15\}, C_7 = \{7, 13\}, C_9 = \{9, 11\}.$$

A code with defining the set $C_1 \cup C_3$ is a [20, 16] cyclic code with (8, 3)-locality.

In Table 7, we have summarized the locality parameters of the cyclic codes of length $\frac{q+1}{2}$ obtained.

Table 7 Cyclic codes with (r, δ)-locality when $n = \frac{q+1}{2}$

j	δ	r
$u-1$	2	$n-1$
$\frac{q-1}{4}$	$\frac{q+1}{4}$	1
$\frac{q-3}{4}$	$\frac{q-1}{4}$	3

Example 11 Let $q = 13$. Then $n = 7$, $\lambda = 12$, and the q-cyclotomic cosets are

$$C_1 = \{1, 13\}, \quad C_3 = \{3, 11\}, \quad C_5 = \{5, 9\}, \quad C_7 = \{7\}.$$

Thus, the code with the defining set $C_5 \cup C_7$ is a $[26, 11]$ cyclic code with $(4, 4)$-locality.

We now derive the cyclotomic cosets for negacyclic codes when $q \equiv 3 \pmod 4$ in the following proposition.

Proposition 16 *Let q be an odd integer such that $q \equiv 3 \pmod 4$, $n = \frac{q+1}{2}$, and let $J = \left\{ \frac{q-i}{2} \mid i \in \mathbb{Z}, and if i is odd, n+1 \leq i \leq 2n-1 \right\}$. Then all q-cyclotomic cosets are $C_{1+2j} = \{1 + 2j, q - 2j\}$ for $j \in J$. Moreover, the number of cyclotomic cosets is $\frac{n}{2}$.*

Proof Similar to the proof of Proposition 12, the q-cyclotomic cosets are $C_{1+2j} = \{1 + 2j, q - 2j\}$ for $j \in J$. Moreover, there are $\frac{n}{2}$ choices for j within the specified range of i. Therefore, the number of q-cyclotomic cosets is

$$\bigcup_{j \in J} |C_{1+2j}| = \frac{n}{2}.$$

□

Example 12 Let $q = 11$. Then $n = 6$, and the q-cyclotomic cosets are

$$C_1 = \{1, 11\}, \quad C_3 = \{3, 9\}, \quad C_5 = \{5, 7\}.$$

Theorem 17 *Let $n = \frac{q+1}{2}$, $q \equiv 3 \pmod 4$, and let $\mathcal{C}$ be a cyclic code of length $2n$ with defining set $\{1 + 2j : j \in \{i_1, i_2, \ldots, i_{n-k}\}\}$, where $i_t = i_1 + t - 1$ for $1 \leq t \leq \delta - 1$. If $j = \frac{q-3}{4}$ or if there exists $u \in \mathbb{Z}$ such that $u = \frac{q-2j-1}{2}$ for some $j \in \{i_1, i_2, \ldots, i_{n-k}\}$, then the $[2n, n + k]$ code $\mathcal{C}$ has (r, δ)-locality, where $r = n - \delta + 1$.*

Proof Let $n = \frac{q+1}{2}$ and $j = \frac{q-3}{4}$. Then $1 + 2j + 2 = q - 2j$, and therefore the cyclotomic coset C_{1+sj} contains 2 consecutive elements. If, for some j, there exists $u \in \mathbb{Z}$ such that $u = \frac{q-2j-1}{2}$, then the elements $q - 2j \in C_{1+2j}$ and $1 + 2u \in C_{1+2u}$ are consecutive. Thus, $\mathcal{C}$ is an $[2n, n + k]$ code, and it has (r, δ)-locality, where $r = n - \delta + 1$. □

Example 13 Let $q = 19$. Then $n = 10$, $\lambda = 18$, and the q-cyclotomic cosets are

$$C_1 = \{1, 19\}, C_3 = \{3, 17\}, C_5 = \{5, 15\}, C_7 = \{7, 13\}, C_9 = \{9, 11\}.$$

A code with the defining set $C_1 \cup C_3$ is a [20, 16] cyclic code with (8, 3)-locality.

In Table 8, we summarize the locality parameters of the cyclic codes of length $\frac{q+1}{2}$ obtained.

Table 8 Cyclic codes with (r, δ)-locality when $n = \frac{q+1}{2}$

j	δ	r
$u-1$	2	$n-1$
$\frac{q-5}{4}$	3	$n-2$
$\frac{q-3}{4}$	2	$n-1$
$\frac{q-2u-1}{2}$	2	$n-1$

4 Comparison of parameters and optimality

In this section, we compare the parameters of our (r, δ)-LRCs with those found in recent literature, specifically [29] and [31]. Our construction utilizes a total length $N = sn$ and dimension $K = n(s-1) + k$, where n is the length of the constituent subcode. The locality is fixed at $r = n - \delta + 1$.

A direct comparison with the quaternary LRCs presented in [29] is not feasible, as our cyclotomic coset structure assumes q to be an odd prime power. A general observation from our results is that our codes typically achieve an information rate $R > 0.5$. The construction in [29] primarily focuses on cyclic subcodes where the locality r is determined by the size of the cyclotomic cosets. While [29] provides optimal codes, the code rate R is often restricted by the field size q and the requirement $n \mid (q-1)$. In contrast, our approach allows for a flexible parameter s. As s increases, the rate $R = 1 - \frac{1}{s} + \frac{k}{sn}$ approaches 1, enabling the construction of high-rate LRCs over relatively small fields. Furthermore, our construction facilitates high availability δ by selecting subcodes with larger minimum distances d_0; this flexibility is more constrained in the direct cyclic constructions of [29].

A direct comparison with our results in Table 5 reveals that, in most cases, our codes exhibit a trade-off: while the minimum distance d and locality (r, δ) may be less optimal than some reference codes, our information rates consistently exceed 0.5 and outperform the rates reported in [31]. For example, as seen in the second row of Table 3 for $q = 7$, we obtain codes with the same minimum distance as those in [31] but with a superior information rate, albeit with less favorable locality parameters r and δ. Furthermore, for a code of length $N = 14$ and dimension $K = 6$, Galindo et al. [31] typically achieves $(r, \delta) = (3, 3)$. Our construction provides a distinct trade-off; for $\delta = 4$, we obtain a fixed locality $r = 14 - 4 + 1 = 11$. This yields higher availability ($\delta = 4$ vs. $\delta = 3$), meaning our code can survive a greater number of concurrent failures within a local recovery group. Moreover, while locality in [31] is often presented as an upper bound, in our work, r is an exact parameter determined by the subcode structure, ensuring more predictable repair performance.

5 Conclusion

In this paper, we have obtained the parameters of a cyclic code whose subcode is a constacyclic code with the same generator polynomial. In particular, we have determined the structure of cyclotomic cosets for constacyclic codes when $n = q + 1$ and negacyclic codes when $n = \frac{q+1}{2}$. By using these cyclotomic cosets, we derived the locality parameters of these codes. We then constructed cyclic codes with (r, δ)-locality based on these cyclic codes. The resulting codes possess significantly low locality compared to their dimension. As a

direction for future research one may extend our framework to more general lengths or to cases where the generator polynomials define multi-generator cyclic or quasi-cyclic codes.

Acknowledgements The authors would like to thank the editors and the referees for their constructive comments, which have greatly contributed to improving the paper.

Author Contributions The topic of the paper was determined by Mehmet E. Koroglu, and the sections of the paper were written by Rabia Zengin. Each section was reviewed by Mehmet E. Koroglu, who made corrections and improvements. The software required to generate the tables was developed by Mehmet E. Koroglu, and the tables were created. The final review was conducted by both authors.

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK). First author is partially supported by the Scientific and Technological Research Council of Türkiye (TÜBİTAK) (Grant Number: BİDEB 2211-A).

Data Availability No datasets were generated or analysed during the current study.

Declarations

Conflicts of Interest All authors declare that they have no conflict of interest.

Competing interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Asteris, M., Papailiopoulos, D., Dimakis, A.G., Vadali, R., Chen, S., Borthakur, D.: XORing elephants: Novel erasure codes for big data. In: Proceedings of the VLDB Endowment **6**(5) (2013)
2. Gopalan, P., Huang, C., Simitci, H., Yekhanin, S.: On the locality of codeword symbols. IEEE Trans. Inf. Theory **58**(11), 6925–6934 (2012)
3. Cadambe, V.R., Mazumdar, A.: Bounds on the size of locally recoverable codes. IEEE Trans. Inf. Theory **61**(11), 5787–5794 (2015)
4. Tamo, I., Barg, A.: A family of optimal locally recoverable codes. IEEE Trans. Inf. Theory **60**(8), 4661–4676 (2014)
5. Micheli, G.: Constructions of locally recoverable codes which are optimal. IEEE Trans. Inf. Theory **66**(1), 167–175 (2019)
6. Tamo, I., Papailiopoulos, D.S., Dimakis, A.G.: Optimal locally repairable codes and connections to matroid theory. IEEE Trans. Inf. Theory **62**(12), 6661–6671 (2016)
7. Prakash, N., Kamath, G.M., Lalitha, V., Kumar, P.V.: Optimal linear codes with a local-error-correction property. In: 2012 IEEE International Symposium on Information Theory Proceedings, pp. 2776–2780 (2012). IEEE
8. Luo, Y., Xing, C., Yuan, C.: Optimal locally repairable codes of distance 3 and 4 via cyclic codes. IEEE Trans. Inf. Theory **65**(2), 1048–1053 (2018)
9. Guruswami, V., Xing, C., Yuan, C.: How long can optimal locally repairable codes be? IEEE Trans. Inf. Theory **65**(6), 3662–3670 (2019)
10. Hao, J., Xia, S.T., Chen, B.: On optimal ternary locally repairable codes. In: 2017 IEEE International Symposium on Information Theory (ISIT), pp. 171–175 (2017). IEEE

11. Li, X., Ma, L., Xing, C.: Optimal locally repairable codes via elliptic curves. IEEE Trans. Inf. Theory **65**(1), 108–117 (2018)
12. Chen, B., Fang, W., Xia, S.T., Hao, J., Fu, F.W.: Improved bounds and singleton-optimal constructions of locally repairable codes with minimum distance 5 and 6. IEEE Trans. Inf. Theory **67**(1), 217–231 (2020)
13. Jin, L.: Explicit construction of optimal locally recoverable codes of distance 5 and 6 via binary constant weight codes. IEEE Trans. Inf. Theory **65**(8), 4658–4663 (2019)
14. Liu, J., Mesnager, S., Tang, D.: Constructions of optimal locally recoverable codes via dickson polynomials. Des. Codes Crypt. **88**, 1759–1780 (2020)
15. Huang, P., Yaakobi, E., Uchikawa, H., Siegel, P.H.: Cyclic linear binary locally repairable codes. In: 2015 IEEE Information Theory Workshop (ITW), pp. 1–5 (2015). IEEE
16. Tamo, I., Barg, A., Goparaju, S., Calderbank, R.: Cyclic LRC codes and their subfield subcodes. In: 2015 IEEE International Symposium on Information Theory (ISIT), pp. 1262–1266 (2015). IEEE
17. Tamo, I., Barg, A., Goparaju, S., Calderbank, R.: Cyclic LRC codes, binary LRC codes, and upper bounds on the distance of cyclic codes. Int. J. Inf. Coding Theory **3**(4), 345–364 (2016)
18. Kim, C., No, J.S.: New constructions of binary and ternary locally repairable codes using cyclic codes. IEEE Commun. Lett. **22**(2), 228–231 (2017)
19. Tan, P., Zhou, Z., Yan, H., Parampalli, U.: Optimal cyclic locally repairable codes via cyclotomic polynomials. IEEE Commun. Lett. **23**(2), 202–205 (2018)
20. Fang, W., Chen, B., Xia, S.T., Fu, F.W.: Singleton-optimal LRCs and perfect LRCs via cyclic codes. In: 2021 IEEE International Symposium on Information Theory (ISIT), pp. 3261–3266 (2021). IEEE
21. Goparaju, S., Calderbank, R.: Binary cyclic codes that are locally repairable. In: 2014 IEEE International Symposium on Information Theory, pp. 676–680 (2014). IEEE
22. Chen, B., Xia, S.T., Hao, J., Fu, F.W.: Constructions of optimal cyclic (r, δ)-locally repairable codes. IEEE Trans. Inf. Theory **64**(4), 2499–2511 (2017)
23. Fang, W., Fu, F.W.: Optimal cyclic (r, δ)-locally repairable codes with unbounded length. Finite Fields Appl. **63**, 101650 (2020)
24. Luo, Y., Xing, C., Yuan, C.: Optimal locally repairable codes of distance 3 and 4 via cyclic codes. IEEE Trans. Inf. Theory **65**(2), 1048–1053 (2018)
25. Qiu, J., Zheng, D., Fu, F.W.: New constructions of optimal cyclic (r, δ)-locally repairable codes from their zeros. IEEE Trans. Inf. Theory **67**(3), 1596–1608 (2020)
26. Prakash, N., Kamath, G.M., Lalitha, V., Kumar, P.V.: Optimal linear codes with a local-error-correction property. In: 2012 IEEE International Symposium on Information Theory Proceedings, pp. 2776–2780 (2012). IEEE
27. Chen, B., Fang, W., Xia, S.T., Fu, F.W.: Constructions of optimal (r, δ)-locally repairable codes via constacyclic codes. IEEE Trans. Commun. **67**(8), 5253–5263 (2019)
28. Chen, B., Xia, S.-T., Hao, J., Fu, F.W.: Constructions of optimal cyclic (r, δ)-locally repairable codes. IEEE Trans. Inf. Theory **64**(4), 2499–2511 (2017)
29. Xu, L., Zhou, Z., Zhang, J., Mesnager, S.: Optimal quaternary (r, δ)-locally recoverable codes: Their structures and complete classification. Des. Codes Crypt. **91**(4), 1495–1526 (2023)
30. Chen, B., Xia, S.T., Hao, J., Fu, F.W.: On optimal pseudo-cyclic (r, δ)-locally repairable codes. In: 2018 IEEE International Symposium on Information Theory (ISIT), pp. 1191–1195 (2018). IEEE
31. Galindo, C., Hernando, F., Martín Cruz, H.: Optimal (r, δ)-LRCs from monomial-Cartesian codes and their subfield-subcodes. Designs, Codes and Cryptography, 1–38 (2024)
32. Zhang, Y., Zheng, D., Wang, X.: Three classes of new optimal cyclic (r, δ)-locally recoverable codes (2023). arXiv:2311.18432
33. Tian, F., Shixin, Z.: Optimal cyclic locally repairable codes with unbounded length from their zeros. Discret. Math. **345**(9), 112978 (2022)
34. Qiu, J., Fang, W., Fu, F.W.: Optimal and almost optimal cyclic (r, δ)-LRCs with large code lengths. In: 2022 IEEE International Symposium on Information Theory (ISIT), pp. 3126–3131 (2022). IEEE
35. Ling, S., Xing, C.: Coding Theory: A First Course. Cambridge University Press, New York (2004)
36. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, New York (2010)
37. Krishna, A., Sarwate, D.V.: Pseudocyclic maximum-distance-separable codes. IEEE Trans. Inf. Theory **36**(4), 880–884 (1990)
38. Grezet, M., Freij Hollanti, R., Westerbäck, T., Hollanti, C.: Alphabet-dependent bounds for linear locally repairable codes based on residual codes. IEEE Trans. Inf. Theory **65**(10), 6089–6100 (2019)
39. Rawat, A.S., Mazumdar, A., Vishwanath, S.: Cooperative local repair in distributed storage. EURASIP J. Adv. Signal Process. **2015**, 1–17 (2015)

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