Two Classes of \((r, t)\)-Locally Repairable Codes

Anyu Wang  
State Key Laboratory of Information Security  
Institute of Information Engineering  
Chinese Academy of Sciences, Beijing, China  
Email: wanganyu@iie.ac.cn

Zhifang Zhang  
Key Laboratory of Mathematics Mechanization, NCMIS  
Academy of Mathematics and Systems Science  
Chinese Academy of Sciences, Beijing, China  
Email: zfz@amss.ac.cn

Abstract—Recently, the \((r, t)\)-locally repairable code has attracted a lot of attention due to its potential application in distributed storage systems for hot data. A locally repairable code with locality \(r\) and availability \(t\), which is termed an \((r, t)\)-LRC, is a code satisfying the property that the value at each coordinate can be recovered from \(t\) disjoint repair sets, each set consists of at most \(r\) other coordinates. In this paper, we investigate two constructions of \((r, t)\)-LRCs. The first one is a cyclic code of which the parity check polynomial is closely related to the trace function over finite fields. This code can achieve high availability and large minimum distance. The second one is based on the incidence matrix of linear subspaces in \(F_q^m\). For some specific parameters, we prove that its information rate is always higher than \(\frac{r}{rt+1}\), which is conjectured to be near to the optimal information rate for \((r, t)\)-LRCs (A. Wang and Z. Zhang, ISIT 2015). By shortening this code in a specially designed way, we obtain \((r, t)\)-LRCs with slightly lower information rate but much more desirable locality \(r\).

I. INTRODUCTION

Modern distributed storage systems are usually delayed by node failures and network congestion, so providing efficient node repair procedure and smooth traffic in networks become the central problems. A potential solution is to use the locally repairable code with availability which was studied in [7, 8, 11]. Specifically, the \(i\)th coordinate of a linear code is said to have locality \(r\) and availability \(t\) if there exist \(t\) disjoint subsets, each containing at most \(r\) other coordinates that can together recover the value of the \(i\)th coordinate. A system employing an \([n, k]\) linear code with locality \(r\) \((r \ll k)\) can greatly reduce the disk I/O complexity for node repair, and with availability \(t\) can permit access of a code symbol from \(t\) ways in parallel which is particularly useful in hot data storage.

Besides locality and availability, codes with high information rate and large minimum distance are also preferred when taking account of storage efficiency and data reliability in distributed storage systems. For an \([n, k, d]\) linear code where each of its information coordinates has locality \(r\) and availability \(t\), an upper bound on the minimum distance, i.e.,

\[
d \leq n - k + 2 - \left\lfloor \frac{t(k-1)+1}{t(r-1)+1} \right\rfloor,
\]

was derived in [11], and the existence of codes attaining this upper bound when \(n \geq k(r+1)\) was also proved there. By further restricting each repair group contains only one parity symbol, a similar upper bound was developed along with some explicit code constructions attaining the bound [7]. Recently, Huang et al. [4] refined the bound (1) by taking the field size \(q\) into account. Instead of considering only information coordinates, here we focus on the linear code that has locality \(r\) and availability \(t\) for all its coordinates, termed \((r, t)\)-LRC for short. In [8], Tamo et al. proved the following bounds for \((r, t)\)-LRCs,

\[
\frac{k}{n} \leq \prod_{i=1}^{t} \frac{1}{1 + \frac{1}{it}}
\]

and

\[
d \leq n - \sum_{i=0}^{t} \left\lfloor \frac{k-1}{p_i^t} \right\rfloor.
\]

Unfortunately, no codes attaining any one of the two bounds for nontrivial values of \(t\) have been built so far.

The direct product code [8], [10] which is the direct product of \(t\) copies of the \([r+1, r]\) binary code, and the \([2^k-1, k, 2^k-1]\) simplex code [5] are two well known classes of \((r, t)\)-LRCs. The former has information rate \((\frac{r}{rt+1})^t\) and the latter has \(\frac{k}{n} = \frac{k}{2^{k-1}}\). Comparing with their large minimum distance, their information rate seems less satisfactory. In [9], the authors gave a method for constructing \((r, t)\)-LRCs with \(t = 2\) based on orthogonal partitions of finite sets and the method was further developed to construct \((r, t)\)-LRCs on algebraic curves [1]. But difficulties in constructing orthogonal partitions in general makes this method inflexible. For the specific case of \(t = 2\), Prakash et al. [6] constructed an \((r, t)\)-LRC with information rate \(\frac{rt}{rt+1}\) and they also proved this was the optimal information rate for \(t = 2\). In [2], the authors constructed cyclic \((r, t)\)-LRCs which were actually concatenations of \([7, 4, 3]\) Hamming code. Recently, a family of binary linear \((r, t)\)-LRC was constructed in [12] for general values of \(r\) and \(t\). Although its minimum distance is trivial, i.e. \(d = t + 1\), its information rate achieves \(\frac{rt}{rt+1}\) which is always higher than that of the direct product code.

A. Our Contribution

In this paper, we construct two classes of \((r, t)\)-LRCs. The first one is an \([n = q^m - 1, k = q^{m-1} - 1, p]\) \(p\)-ary cyclic code with locality \(r = m - 1\) and availability \(t = em\), where \(q = p^e\) is a prime power. We prove its minimum distance satisfies \(d \geq \max\{q + 1, t + 1\}\). Thus by choosing a large \(e\), this code can achieve high availability \(t\) and large minimum distance \(d\).
The second code is a linear code, of which the parity check matrix is closely related to the structure of linear spaces in $\mathbb{F}_q^m$. In some cases, we prove that its information rate is always higher than $\frac{r}{m}$. Note that $\frac{r}{m}$ was guessed to be near to the optimal information rate for $(r, t)$-LRCs in [12]. So this construction narrows the gap between the known information rate and the optimal information rate for $(r, t)$-LRCs. Lastly, we apply the shortening technique to this code, and then obtain a class of binary linear $(r, t)$-LRCs with $t = 3$, of which the information rate is slightly lower than the original codes but the locality $r$ is much more desirable.

B. Organization

Section II introduces some notations and the formal definition of $(r, t)$-LRC. Section III studies the cyclic $(r, t)$-LRC based on the trace function on finite fields. Section IV investigates the $(r, t)$-LRC which is related to the linear spaces in $\mathbb{F}_q^m$. Section V concludes the paper.

II. NOTATIONS AND DEFINITIONS

Let $C$ be an $[n, k, d]_q$ linear code with generator matrix $G = (g_1, \ldots, g_n)$, where $g_i \in \mathbb{F}_q^m$ for $1 \leq i \leq n$. For any positive integer $m$, denote $[m] = \{1, 2, \ldots, m\}$. For a codeword $c = (c_1, \ldots, c_n) \in C$, let $\text{Supp}(c)$ be the support of $c$ and $\text{wt}(c)$ be the weight of $c$, i.e., $\text{Supp}(c) = \{i \in [n] : c_i \neq 0\}$ and $\text{wt}(c) = |\text{Supp}(c)|$.

**Definition 1.** The $i$th coordinate, $1 \leq i \leq n$, of $C$ is said to have locality $r$ and availability $t$ if there exist $t$ disjoint subsets $R_1(i), \ldots, R_t(i) \subseteq [n] \setminus \{i\}$ such that for $1 \leq j \leq t$,

1. $|R_j(i)| \leq r$, and
2. $g_i$ is an $\mathbb{F}_q$-linear combination of $\{g_l\}_{l \in R_j(i)}$.

The $[n, k, d]_q$ linear code $C$ is called an $(r, t)$-LRC if each of its coordinate has locality $r$ and availability $t$. In this paper, we study the locality and availability property of an $(r, t)$-LRC by investigating its parity checks. The following concept is useful for characterizing the locality and availability property of an $(r, t)$-LRC.

**Definition 2.** For an $[n, k, d]_q$ linear code $C$, a set of parity checks $h_1, \ldots, h_m \in C^\perp$ are called orthogonal on the $i$th coordinate, where $i \in [n]$, if $\text{Supp}(h_{i_1}) \cap \text{Supp}(h_{i_2}) = \{i\}$ for all $1 \leq i_1 < i_2 \leq m$.

Based on this concept, the locality $r$ and availability $t$ for the $i$th coordinate of a linear code $C$ is equivalent to that there exist $t$ parity checks $h_1, \ldots, h_t \in C^\perp$, which are orthogonal on the $i$th coordinate and $\text{wt}(h_{i_l}) \leq r$ for $1 \leq l \leq t$.

III. CYCLIC $(r, t)$-LRC VIA TRACE FUNCTION

In this section, we construct a cyclic $(r, t)$-LRC by using the trace function over finite fields. An $[n, k]$ $q$-ary cyclic code $C = \langle g(x) \rangle$ is the ideal generated by $g(x)$ in the ring $\mathbb{F}_q[x]/(x^n - 1)$, where $g(x) \mid x^n - 1$ and $\text{deg}(g) = n - k$. We call $g(x)$ the generator polynomial, and $h(x) = \frac{x^n - 1}{g(x)}$ the parity check polynomial of $C$.

For a cyclic code $C$ with parity check polynomial $h(x)$, each $u(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \in \langle h(x) \rangle$ defines a parity check $(a_0, \ldots, a_{n-1}) \in C^\perp$. If we can find $u_1(x), \ldots, u_t(x) \in \langle h(x) \rangle$ that define parity checks of weight no more than $r + 1$, and are orthogonal on the $i$th coordinate, then the $i$th coordinate of $C$ has locality $r$ and availability $t$. Furthermore, since $C$ is cyclic, the locality $r$ and availability $t$ is actually guaranteed for all coordinates, and therefore $C$ is an $(r, t)$-LRC. So the main idea for constructing a cyclic $(r, t)$-LRC is to properly choose $h(x)$ to make it possible to find such $u_1(x), \ldots, u_t(x) \in \langle h(x) \rangle$. Most importantly, to get better code parameters, we should try to use the cyclic shift of a polynomial, that is, $u_2(x)$ might be a cyclic shift of $u_1(x)$.

A. CODE CONSTRUCTION

Let $q = p^e$ be a prime power, and let $f(x) = x + x^{q^1} + \ldots + x^{q^{m-1}}$ be the trace function from $\mathbb{F}_q$ to $\mathbb{F}_q$. Define $C$ to be a cyclic code over $\mathbb{F}_p$ with length $n = q^m - 1$ and parity check polynomial $h(x) = f(x)/x$. Then its generator polynomial is $g(x) = (x^n - 1)/h(x) = f(x)^{q-1} - 1$, and the dimension of $C$ is $k = \text{deg}(h) = q^m - 1$. So $C$ is an $[n = q^m - 1, k = q^{m-1} - 1]_p$ $p$-ary cyclic code.

**Theorem 3.** The $[n = q^m - 1, k = q^{m-1} - 1]_p$ $p$-ary cyclic code $C$ is an $(r, t)$-LRC, where $r = m - 1$ and $t = em$.

**Proof:** Consider the following $e$ codewords in $\langle h(x) \rangle$,

$$h(x) = x^p + x^{pq} + \ldots + x^{p^{m-1}}$$

By cyclic shifting each of these $e$ polynomials, we can get $m$ polynomials all containing the term $x^e$. Therefore $em$ polynomials containing $x^e$ can be obtained by cyclic shifting these $e$ polynomials, i.e.,

$$\{h(x)^i x^{-p^i q^i + 1}\}_{0 \leq i < e, 0 \leq j < m},$$

where the power of each term is taken to mod $n$.

For any pair of these $em$ polynomials, we claim that $x^e$ is their only common term. Consider two polynomials

$$h(x)^{i_1} x^{-p^{i_1} q^{i_1} + 1} = \sum_{i_2=0}^{m-1} x^{p^{i_1} q^{i_1} - p^{i_2} q^{i_2} + 1},$$

$$h(x)^{i_2} x^{-p^{i_2} q^{i_2} + 1} = \sum_{i_2=0}^{m-1} x^{p^{i_2} q^{i_2} - p^{i_2} q^{i_2} + 1},$$

where $0 \leq i_1, i_2 < e$, $0 \leq i_1, i_2 < m$ and $(i_1, j_1) \neq (i_2, j_2)$. Suppose $x^{p^{i_1} q^{i_1} - p^{i_2} q^{i_2} + 1} = x^{p^{i_2} q^{i_2} - p^{i_2} q^{i_2} + 1}$ is a common term of them. Then $p^{i_1} (q^{i_1} - q^{i_2}) = p^{i_2} (q^{i_2} - q^{i_2}) \mod n$, i.e., $n \mid (p^{i_1} q^{i_1} - q^{i_1}) - p^{i_2} q^{i_2} - q^{i_2})$. Notice that $-p^{i_1} (q^{i_1 - 1} - 1) \leq p^{i_1} (q^{i_1} - q^{i_1}) \leq p^{i_1} (q^{i_1 - 1} - 1)$ and $-p^{i_2} (q^{i_2 - 1} - 1) \leq p^{i_2} (q^{i_2} - q^{i_2}) \leq p^{i_2} (q^{i_2 - 1} - 1)$ and $-p^{i_1} (q^{i_1 - 1} - 1) \leq p^{i_1} (q^{i_1} - q^{i_1}) \leq p^{i_1} (q^{i_1 - 1} - 1)$ and $-p^{i_2} (q^{i_2 - 1} - 1) \leq p^{i_2} (q^{i_2} - q^{i_2}) \leq p^{i_2} (q^{i_2 - 1} - 1)$.
\[ p^{ij}(q^{j_1} - q^{j_2}) \leq p^{e-1}(q^{m-1} - 1), \]
then we have
\[
\left| p^{i_1}(q^{j_1}) - p^{i_2}(q^{j_2}) \right| \\
\leq 2p^{e-1}(q^{m-1} - 1) \\
\leq p^{e}(q^{m-1} - 1) = q(q^{m-1} - 1) \\
< q^m - 1 = n.
\]

It follows that \( p^{i_1}(q^{j_1}) - p^{i_2}(q^{j_2}) = 0 \), i.e., \( p^{i_1}(q^{j_1}) = p^{i_2}(q^{j_2}) \). By the uniqueness of \( q \)-ary expansion of integers, we have \( l_1 = j_1, l_2 = j_2 \) or \( i_1 = i_2, l_1 = j_2, j_1 = j_2 \). The first case implies that the common term is \( x' \), and the second case contradicts the assumption \( (i_1, j_1) \neq (i_2, j_2) \). Therefore the claim holds.

Note that each \( c_0 + c_1x + \ldots + c_{n-1}x^{n-1} \in (h(x)) \) defines a parity check \( (c_{n-1}, \ldots, c_0) \in C^t \). Then these \( em \) polynomials in \( (h(x)) \) define \( em \) parity checks of \( C \) such that: 1) the weight of each parity check is \( m; 2) \) they are orthogonal on the \( (n-1) \)th coordinate of \( C \). Therefore \( C \) is an \( (r, t) \)-LRC with \( r = m-1 \) and \( t = em \).

According to Theorem 3, the cyclic code \( C \) can achieve high availability \( t \) by choosing a large \( e \). Next, we determine the minimum distance of \( C \). Since \( C \) is an \( (r, t) \)-LRC, then any \( t+1 \) erasures are recoverable for \( C \). So its minimum distance satisfies \( d \geq t+1 \). Furthermore, by applying the BCH bound to \( C \), we can obtain a better estimate of the minimum distance.

**Theorem 4.** The minimum distance of \( C \) satisfies \( d \geq \max\{q+1, t+1\} \).

**Proof:** It suffices to show \( d \geq q+1 \). Note that in all \( n \)th roots of unit, there are \( n - \deg(g) = q^{n-1} - 1 \) nonzeros of \( g(x) \). Then by the pigeonhole principle, \( g(x) \) has at least \( \left\lfloor \frac{n-q^{n-1}}{q^{n-1} - 1} \right\rfloor = q \) consecutive zeros, i.e., there exists an integer \( i \) such that \( \alpha^i, \alpha^{i+1}, \ldots, \alpha^{i+q-1} \) are zeros of \( g(x) \), where \( \alpha \) is a primitive \( n \)th root of unit. Then the lemma follows directly from the BCH bound.

When \( q = 2 \) (i.e., \( p = 2, e = 1 \)), \( C \) is an \( [n = 2^{m-1}, k = 2^{m-1} - 1, d = t+1] \) binary \( (r, t) \)-LRC with \( r = m-1 \) and \( t = m \). Since \( g(x) = f(x)-1 = x + x^2 + \cdots + x^{2m-2} - 1 \) for \( q = 2 \), the minimum distance of \( C \) satisfies \( d \leq \text{wt}(g) = m+1 = t+1 \), then we have \( d = t+1 \) according to Theorem 4. Although \( d = t+1 \) is the lowest minimum distance for an \( (r, t) \)-LRC, we can see \( C \) performs better than the direct product code and the binary \( (r, t) \)-LRC in [12] with respect to the information rate \( \frac{d}{n} \) and relative distance \( \frac{d}{r} \). Table 1 gives a comparison of these three codes under the same \( r, t \).

**Remark.** For given \( r \) and \( t \), the minimum distance of the direct product code (i.e., \( d = 2^t \)) is larger than that of \( C \) with \( q = 2 \) (i.e., \( d = t+1 \)). However, owing to the code length of \( C \) is much smaller, we can see from Table 1 that \( C \) greatly outperforms the direct product code with respect to the relative distance.

When \( q > em = t \), we can conclude from Theorem 4 that \( d \) is strictly larger than \( t+1 \). Moreover, the real minimum distance of \( C \) could be further larger than the lower bound in Theorem 4. For example, when \( q = 4, m = 3 \), it can be verified \( C \) is an \( [n = 63, k = 15, d = 10] \) binary \((r, t)\)-LRC with \( r = 2 \) and \( t = 6 \), while Theorem 4 implies that \( d \geq \max\{q+1, t+1\} = 7 \).

**IV. \((r, t)\)-LRC Related to Subspaces in \( F_q \)**

Let \( A = \{A \subseteq F_q^m : \dim A = s-1\} \), \( B = \{B \subseteq F_q^m : \dim B = s\} \), where \( 1 < s < m \) and \( q = p^e \) is a prime power. Define a matrix \( H = (h_{A,B}) \in \mathbb{F}_p^{[A \times |B|]} \) such that
\[
h_{A,B} = \begin{cases} 
1, & \text{if } A \subseteq B \\
0, & \text{if } A \nsubseteq B
\end{cases}
\]

Then \( H \) defines a \( p \)-ary linear code \( C \). By the basic facts of Gaussian binomial coefficients (see [5]), the code length is
\[
n = |B| = \binom{m}{s}_q = \frac{(q^m-q)(q^{m-q}) \cdots (q^{m-s+1})}{(q^s-1)(q^{s-1}) \cdots (q^{s-s+1})},
\]
the weight of each row of \( H \) is \( \binom{m-s+1}{m-s}_q = \frac{q^{m-s+1}-1}{q-1} \), and the weight of each column of \( H \) is \( \binom{s}{s}_q = \frac{q^s-1}{q-1} \). The locality and availability property of \( C \) is stated in the following theorem.

**Theorem 5.** The linear code \( C \) defined by \( H \) is an \( (r, t) \)-LRC with \( r = \frac{q^{m-s+1}-1}{q-1} - 1 \) and \( t = \frac{q^s-1}{q-1} \).

**Proof:** Denote the rows of \( H \) by \( \{c_A\}_{A \in \mathcal{A}} \). Then for any \( A_1 \neq A_2 \subseteq A \), we have
\[
|\text{Supp}(c_{A_1}) \cap \text{Supp}(c_{A_2})| = |\{B \in B : A_1 \subseteq B\} \cap \{B \in B : A_2 \subseteq B\}| = |\{B \in B : A_1 \cup A_2 \subseteq B\}| = \begin{cases} 
1, & \text{if } \dim(A_1 + A_2) = s \\
0, & \text{if } \dim(A_1 + A_2) > s.
\end{cases}
\]
Thus for each $B \in \mathcal{B}$, the $\frac{q^m-1}{q-1}$ rows $\{c_A\}_{A \subseteq B}$ are orthogonal on the coordinate $B$, where the weight of each row is $\frac{q^{m+1}-1}{q-1}$. Therefore $C$ is an $(r,t)$-LRC with $r = \frac{q^{m+1}-1}{q-1} - 1$ and $t = \frac{q^m-1}{q-1}$.

**Example 1.** Let $m = 3$ and $s = 2$, then $n = \frac{q^3-1}{q-1}$ and $C$ is an $(r,t)$-LRC with $r = q, t = q + 1$. It was proved in [3] that $\text{rank}_p(H) = 1 + (\frac{p+1}{2})^c$, and therefore the dimension of $C$ is $k = n - \text{rank}_p(H) = q^3 - q + (\frac{q+1}{2})^c$. In fact, it can be verified $C$ is equivalent to the difference set code (see, e.g., [5], [13]) for $m = 3$ and $s = 2$.

To determine the dimension of $C$, we have to compute the $p$-rank of the parity check matrix $H$, which is still an open problem in the general case. However, for the special case $s = 2, q = 2$, we can derive a simple expression for $\text{rank}_p(H)$.

**A. A Special Case: $s = 2, q = 2$**

This subsection focuses on the special case $s = 2, q = 2$. In this case, $C$ is a binary linear code. The linear spaces corresponding to the rows of $H$ are $A = \{A \subseteq F_q^2 : \dim A = 1\}$, in which each linear space $A$ contains only one nonzero vector $u(A)$; and the spaces corresponding to the columns of $H$ are $B = \{B \subseteq F_q^2 : \dim B = 2\}$, in which each linear space $B$ contains three nonzero vectors $v_1^{(B)}, v_2^{(B)}, v_3^{(B)}$ such that $v_1^{(B)} + v_2^{(B)} + v_3^{(B)} = 0$.

**Lemma 6.** When $s = 2, q = 2$, we have $\text{rank}_2(H) = 2^m - 1 - m$.

**Proof:** The proof is given in Appendix A.

Finally we determine the minimum distance of $C$. Let $a, b, c \in F_q^2 \setminus \{0\}$ be three nonzero vectors that are linearly independent over $F_2$. Consider the 4 columns of the parity check matrix $H$ which correspond to the 4 linear spaces $\{0, a, b, a+b\}, \{0, a, c, a+c\}, \{0, b, c, b+c\}, \{0, a+b, a+c, b+c\}$ respectively. It is clear the sum of these 4 columns are zero, and therefore $C$ has minimum distance $d \leq 4$. On the other hand, we have $d = t + 1 = 4$, so the minimum distance of $C$ is $d = 4$. From Lemma 6, we can see the dimension of $C$ is $k = n - \text{rank}_2(H) = n - (2^m - 1 - m)$.

Then by setting $s = 2, q = 2$ in Theorem 5, we derive the following theorem.

**Theorem 7.** When $s = 2, q = 2$, $C$ is an $[n = \frac{1}{2}(2^m - 1)(2^m - 2), k = n - 2^m(1 - m), d = 4]$ binary $(r,t)$-LRC with $r = 2^m(1 - 2), t = 3$.

In [12], the authors gave a class of binary $(r,t)$-LRCs, whose information rate $\frac{r}{r+t}$ is always higher than that of the direct product code. In fact, $\frac{r}{r+t}$ was guessed to be near to the optimal information rate for $(r,t)$-LRCs with $r \geq t$ therein. Note that when $m = 4$, the code $C$ in Theorem 7 is an $[35, 24, 4]$ binary $(r,t)$-LRC with $r = 6, t = 3$, whose information rate $\frac{r}{r+t} = \frac{24}{35}$ is larger than $\frac{2}{3}$. In fact, it can be proved that the information rate of $C$ is always larger than $\frac{r}{r+t}$ for $m \geq 4$ (see Appendix B). Thus Theorem 7 narrows the gap between the known information rate of $(r,t)$-LRC with $r \geq t$ and the optimal value.

Though the information rate of $C$ is always higher than $\frac{1}{r+t}$, its locality $r = 2^m(1 - 2)$ is a power of $m$, which increases very fast as $m$ increasing. In the next subsection, we apply the shortening technique to $C$, and obtain a class of $(r,t)$-LRCs with slightly lower information rate but much more desirable locality $r$.

**B. Shortening $C$ when $s = 2, q = 2$**

In this subsection, we still focus on the case $s = 2, q = 2$. First, we propose some properties of the parity check matrix $H$ which can help us to shorten $C$.

**Lemma 8.** When $m$ is even, the binary matrix $H$ has the following block form,

$$H = \begin{pmatrix} H_0 & H_1 & \ldots & H_l \end{pmatrix},$$

where $l = \frac{1}{2}(2^m - 4)$. $H_0$ is a binary matrix of size $\left(2^m - 1\right) \times \frac{1}{4}(2^m - 1)$, in which the weight of each row is 1 and the weight of each column is 3. For all $1 \leq i \leq l$, $H_i$ is a binary matrix of size $(2^m - 1) \times (2^m - 1)$, in which the weight of each row or each column is 3.

**Proof:** By fixing a basis of $F_q^{m}$ over $F_q$, we can assume that each row of $H$ corresponds to an element $u$ in $F_q^{m}$, and each column of $H$ corresponds to a 3-tuple $\{v_1, v_2, v_3\} \subseteq F_q^2$ such that $v_1 + v_2 + v_3 = 0$. Denote $V$ to be all such 3-tuples, i.e., $V = \{\{v_1, v_2, v_3\} \subseteq F_q^2 : v_1 + v_2 + v_3 = 0\}$. Define an equivalence relation ‘∼’ in $V$ by $\{v_1, v_2, v_3\} \sim \{v_1', v_2', v_3'\}$ if there exists a $\lambda \in F_q^\times$ such that $\lambda \cdot \{v_1, v_2, v_3\} = \{v_1', v_2', v_3'\}$, where $\lambda \cdot \{v_1, v_2, v_3\} = \{\lambda v_1, \lambda v_2, \lambda v_3\}$. Let $V'_0 \cup V_1 \cup \ldots \cup V_l$ be the equivalence class partition of $V$, where $V_0$ is the equivalence class containing the 3-tuple $\{1, \omega, \omega^2\}$ and $\omega$ is the primitive 3th root of unit. Note that $\omega$ is contained in $F_q^{m}$ because $m$ is even. Then this partition defines a block form of $H$, i.e.,

$$H = \begin{pmatrix} H_0 & H_1 & \ldots & H_l \end{pmatrix},$$

where $H_0$ is the submatrix corresponds to $V_i$ for all $0 \leq i \leq l$.

We next determine the size of each equivalence class. If for a 3-tuple $\{v_1, v_2, v_3\} \in V$, there exists a $\lambda \in F_q^{m}$ such that $\lambda \neq 1$ and $\lambda \cdot \{v_1, v_2, v_3\} = \{v_1, v_2, v_3\}$, then we have $\lambda v_1 = v_2, \lambda v_2 = v_3, \lambda v_3 = v_1$ or $\lambda v_1 = v_3, \lambda v_2 = v_1, \lambda v_3 = v_2$. In both case we have $\lambda^3 = 1$, and thus $\lambda = \omega$ or $\lambda = \omega^2$. It follows that $\{v_1, v_2, v_3\} \sim \{1, \omega, \omega^2\}$. Therefore for all $1 \leq i \leq l$, $V_i$ consists of the $(2^m - 1)$ distinct 3-tuples $\{\lambda \cdot \{v_1, v_2, v_3\} \lambda \in F_q^\times \}$, where $\lambda \cdot \{v_1, v_2, v_3\} \in V_i$, and each 3-tuple in $V_0$ occurs three times in $\{\lambda \cdot \{1, \omega, \omega^2\} \lambda \in F_q^\times \}$, i.e., $\{\lambda \cdot \{1, \omega, \omega^2\} = \{\lambda \cdot \{1, \omega, \omega^2\}\} \lambda \in F_q^\times \}$, and $\lambda \cdot \{1, \omega, \omega^2\} \in F_q^{m}$. Then for any $1 \leq i \leq l$, $H_i$ is a binary matrix of size $(2^m - 1) \times (2^m-1)$, and each row of $H_i$ has weight 3 because any element $u \in F_q^2$ is contained in three 3-tuples in $V_i$, i.e., $u v_1^{-1} \cdot \{v_1, v_2, v_3\}, u v_2^{-1} \cdot \{v_1, v_2, v_3\}, u v_3^{-1} \cdot \{v_1, v_2, v_3\}$, where $\{v_1, v_2, v_3\} \in V_i$. Similarly, $H_0$ is a binary matrix of size $(2^m - 1) \times \frac{1}{3}(2^m - 1)$, and each row of $H_0$ has
weight 1. Finally, we have \( l = \left( n - \frac{1}{3}(2^m - 1) \right) / (2^m - 1) = \frac{1}{6}(2^m - 2) - \frac{1}{3} = \frac{1}{6}(2^m - 4) \), which completes the proof of the lemma.

For any integer \( i \in [l] \), consider the submatrix \( H_1^{(i)} = (H_0, H_1, \ldots, H_l) \) consisting of the first \( i + 1 \) blocks of \( H \). Let \( C_1^{(i)} \) be the binary code defined by parity check matrix \( H_1^{(i)} \). In fact, \( C_1^{(i)} \) consists of all codewords of \( C \) that have zero at the coordinates corresponding to \( H_{i+1}, H_{i+2}, \ldots, H_l \), with these zero coordinates deleted. Therefore \( C_1^{(i)} \) is short from \( C \).

**Theorem 9.** Suppose \( m \) is even. For any \( 1 \leq i \leq \frac{1}{6}(2^m - 4) \), the code \( C_1^{(i)} \) is an \( [n = (i + \frac{1}{3})(2^m - 1), k \geq n - (2^m - 1 - m), d \geq 4] \) binary linear \((r, t)\)-LRC, where \( r = 3i \) and \( t = 3 \).

**Proof:** Since \( H_1^{(i)} \) is a submatrix of \( H \), the supports of any two rows of \( H_1^{(i)} \) have at most one common coordinate. Thus for each coordinate of \( C_1^{(i)} \), we can find 3 rows of \( H_1^{(i)} \) which are orthogonal on this coordinate, where the weight of each row is \( 3i + 1 \). It follows that \( C_1^{(i)} \) is an \((r, t)\)-LRC with \( r = 3i \) and \( t = 3 \). On the other hand, we have \( \text{rank}_2(H_1^{(i)}) \leq \text{rank}_2(H) = 2^m - 1 - m \). Therefore the dimension of \( C_1^{(i)} \) satisfies \( k = n - \text{rank}_2(H_1^{(i)}) \geq n - (2^m - 1 - m) \). Finally, the minimum distance of \( C_1^{(i)} \) satisfies \( d \geq t + 1 = 4 \).

Since \( C_1^{(i)} \) is a short code, its information rate is lower than that of the original code \( C \), but their difference can be small according to Theorem 7 and Theorem 9. Moreover, the choice of locality \( r \) for \( C_1^{(i)} \) is more flexible than the original code \( C \), which makes the code \( C_1^{(i)} \) much more desirable.

For any \( i \in [l] \), consider the binary code \( C_2^{(i)} \) defined by the parity check matrix \( H_2^{(i)} = (H_1, \ldots, H_l) \). Then similar to the code \( C_1 \), we have the following theorem.

**Theorem 10.** Suppose \( m \) is even. For any \( 1 \leq i \leq \frac{1}{6}(2^m - 4) \), the code \( C_2^{(i)} \) is an \( [n = (i)(2^m - 1), k \geq n - (2^m - 1 - m), d \geq 4] \) binary linear \((r, t)\)-LRC, where \( r = 3i \) and \( t = 3 \).

**Example 2.** When \( m = 4 \), we have \( l = \frac{1}{6}(2^m - 4) = 2 \). Then we can obtain 2l = 4 codes from Theorem 9 and Theorem 10, which are listed in Table 2, where codes with information rate exceeding \( \frac{1}{r-t} \) are marked in bold.

<table>
<thead>
<tr>
<th>( i )</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n, k, d )</td>
<td>[20, 9, 4]</td>
<td>[15, 4, 4]</td>
</tr>
<tr>
<td>( r, t )</td>
<td>(3, 3)</td>
<td>(2, 3)</td>
</tr>
</tbody>
</table>

Table 2

When \( m \) is odd, by a deduction similar to the proof of Lemma 8, we can prove the following lemma.

**Lemma 11.** When \( m \) is odd, we have

\[ H = \begin{pmatrix} H_1 & H_2 & \ldots & H_l \end{pmatrix}, \]

where \( l = \frac{1}{6}(2^m - 2) \), and for all \( 1 \leq i \leq l \), \( H_i \) is a binary matrix of size \((2^m - 1) \times (2^m - 1)\), of which the weight of each row or each column is 3.

For any \( i \in [l] \), consider the code \( C_3^{(i)} \) which is defined by parity check matrix \( H_3^{(i)} = (H_1, \ldots, H_l) \). We have the following theorem.

**Theorem 12.** Suppose \( m \) is odd. For any \( 1 \leq i \leq \frac{1}{6}(2^m - 2) \), the code \( C_3^{(i)} \) is an \([n = i(2^m - 1), k \geq n - (2^m - 1 - m), d \geq 4] \) binary linear \((r, t)\)-LRC, where \( r = 3i - 1 \) and \( t = 3 \).

**Example 3.** When \( m = 5 \), we have \( l = \frac{1}{6}(2^m - 2) = 5 \). Then the \( l = 5 \) codes obtained from Theorem 12 are listed in Table 3, where codes with information rate exceeding \( \frac{1}{r-t} \) are marked in bold.

<table>
<thead>
<tr>
<th>( i )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n, k, d )</td>
<td>[31, 5]</td>
<td>[62, 36]</td>
<td>[93, 67]</td>
<td>[124, 98]</td>
<td>[155, 129]</td>
</tr>
<tr>
<td>( r, t )</td>
<td>(2, 3)</td>
<td>(5, 3)</td>
<td>(8, 3)</td>
<td>(11, 3)</td>
<td>(14, 3)</td>
</tr>
</tbody>
</table>

Table 3

V. CONCLUSION

We construct two classes of \((r, t)\)-LRCs. The first one is a cyclic code of which the parity check polynomial is closely related to the trace function over finite fields. The second one is based on the incidence matrix of the linear subspaces in \( \mathbb{F}_q^m \). Then a class binary linear \((r, t)\)-LRCs with \( t = 3 \) and desirable value of \( r \) is obtained by shortening the second code. We expect this shortening technique could be used to construct more linear \((r, t)\)-LRCs with good locality and availability property.

**REFERENCES**

APPENDIX A

PROOF OF LEMMA 6

Let $T$ be the binary matrix consisting of all nonzero columns of length $m$, i.e., $T = (u)_{u \in \mathbb{F}_2^m}$. Then $T$ is the parity check matrix of the $[2^m - 1, 2^m - 1 - m]$ binary Hamming code $\mathcal{H}_m$. We claim that the binary matrix $H^\top$ generates $\mathcal{H}_m$, and then the lemma follows directly. Note that each coordinate of $H^\top$ corresponds to a nonzero vector $u^{(A)}$, so we can assume the columns of $H^\top$ and $T$ are in the same order.

First, we show that the rows of $H^\top$ are codewords of $\mathcal{H}_m$. For any $B \in \mathcal{B}$, let $h_B$ be the row of $H^\top$ which corresponds to the linear space $B$. Then $h_B$ has 1's at three coordinates, i.e., the coordinates correspond to the linear space $H$ is a codeword of $\mathcal{H}_m$, and thus $h_B$ is a codeword of $\mathcal{H}_m$.

It remains to show that for any codeword $c \in \mathcal{H}_m$, $c$ is a linear combination of rows in $H^\top$. We prove it by inducting on the weight of $c$. When $wt(c) = 3$, suppose the three nonzero coordinates of $c$ are $u_1, u_2, u_3$, where $u_1, u_2, u_3 \in \mathbb{F}_2^m \setminus \{0\}$ and $u_1 + u_2 + u_3 = 0$. Denote $B$ to be the linear space spanned by $\{u_1, u_2, u_3\}$, then $\dim B = 2$, and thus $c$ is the row of $H^\top$ which corresponds to $B$. Therefore the statement holds for $wt(c) = 3$. Suppose for any $c \in \mathcal{H}_m$ such that $wt(c) \leq w$, $c$ is a linear combination of rows in $H^\top$, where $3 \leq w < n$.

Then for a codeword $c' \in \mathcal{H}_m$ such that $wt(c') = w + 1$, suppose $u'_1$ and $u'_2$ are two of its nonzero coordinates, where $u'_1, u'_2 \in \mathbb{F}_2^m \setminus \{0\}$. Let $B'$ be the linear space spanned by $u'_1$ and $u'_2$, then $\dim B' = 2$ and $h_{B'}$ is a row of $H^\top$. Note that $c' + h_{B'} \in \mathcal{H}_m$ and $wt(c' + h_{B'}) \leq wt(c') - 1 = w$, then by the inductive assumption, $c' + h_{B'}$ is a linear combination of rows in $H^\top$. It follows that $c'$ is also a linear combination of rows in $H^\top$.

APPENDIX B

COMPARISON OF THE INFORMATION RATE

By Theorem 7, $C$ is an $[n = \frac{1}{6}(2^m - 1)(2^m - 2), k = n - (2^m - 1 - m)]$ binary $(r, t)$-LRC with $r = 2^m - 1 - 2, t = 3$.

Then for $m \geq 4$, the information rate of $C$ satisfies

\[
\frac{k}{n} = 1 - \frac{2^m - 1 - m}{2^m - 1 - m} = 1 - \frac{6(2^m - 1 - m)}{(2^m - 1)(2^m - 2)} \geq 1 - \frac{6(2^m - 5)}{(2^m - 1)(2^m - 2)} = 1 - \frac{3}{2^m - 1 + 1} \frac{(2^m + 2)(2^m - 5)}{(2^m - 1)(2^m - 2)} > 1 - \frac{2^m - 1 + 1}{3} = 1 - \frac{t}{r + t} = \frac{r}{r + t}.
\]

Thus the information rate of $C$ is always larger than $\frac{r}{r + t}$ for $m \geq 4$. 