Bounds on the Rate of Linear Locally Repairable Codes over Small Alphabets

Abhishek Agarwal and Arya Mazumdar *

Abstract

Locally repairable codes (LRC) have recently been a subject of intense research due to theoretical appeal and their application in distributed storage systems. In an LRC, any coordinate of a codeword can be recovered by accessing only few other coordinates. For LRCs over small alphabet (such as binary), the optimal rate-distance trade-off is unknown. In this paper we provide the tightest known upper bound on the rate of linear LRCs of a given relative distance, an improvement over any previous result, in particular [1].

1 Introduction

Let $C(n, d) \subseteq \{0, 1\}^n$ denote a binary linear code of length $n$ with minimum distance $d_{\text{min}} = d$ and $C^\perp$ denote the dual of the linear code $C$. A code $C(n, d)$ can recover any codeword after the erasure of at most $(d - 1)$ coordinate symbol. But, it requires knowledge of all other $n - d + 1$ coordinates of the codeword for recovery. For certain scenarios such as distributed storage systems, in addition to minimum distance, codes with a small locality are desired. In such systems, to repair a single symbol of a codeword of $C$, we want to utilize information about few other codeword symbols. Locally Repairable Codes (LRC) [5], with locality parameter $r$, allow the repair of any one symbol of a codeword by knowing at most $r$ other codeword symbols. Let $S$ be the subset of coordinates (of size at most $r$) required to repair a symbol at coordinate $i$ in the LRC. Then the set $R(i) := S \cup \{i\}$ is called the repair group of coordinate $i$. We denote the linear LRC of length $n$, minimum distance $d$ and locality $r$ as $C(n, d, r)$.

The dimension of $C(n, d)$ is defined as $k(C) = \log_2 |C|$, and the rate as $R(C) = \frac{k}{n}$. For a code $C(n, d, r)$, its dimension is known to be upper bounded by,

$$k(C) \leq m - \left\lfloor \frac{m}{r + 1} \right\rfloor$$

where $m = n - d + 1$ [5]. This bound is known to be achievable when the code is over alphabet size at least $n$ [9], but it is far from being tight for smaller, in particular binary, alphabets [1]. For binary code $C(n, d, r)$,
an upper bound on the dimension of LRC was presented in [1]:

$$k \leq \min_{t \in \mathbb{Z}_+} \left[ tr + k_{opt}(n - t(r + 1), d) \right],$$

(2)

where $k_{opt}(n, d)$ is the optimum dimension of an error-correcting code of length $n$ and distance $d$.

This bound can be translated into an asymptotic bound on rate and relative distance, assuming $k/n \to R$ and $d/n \to \delta$ as $n \to \infty$:

$$R \leq \min_{0 \leq x \leq \frac{r}{r+1}} \left[ x + (1 - x(1 + 1/r)) R_{opt} \left( \frac{\delta}{1 - x(1 + 1/r)} \right) \right],$$

(3)

where, $R_{opt}(\delta) \equiv \lim_{n \to \infty} \frac{k_{opt}(n, \delta n)}{n}$. The best known upper bound on the rate of a locally repairable code is found when $R_{opt}(\delta)$ is bounded by $R_{MRRW}(\delta)$ given below:

$$R_{MRRW}(\delta) = \min_{0 < \alpha \leq 1 - 4\delta} \left[ 1 + \frac{h(\alpha^2)}{\alpha^2 + 4\delta \alpha + 4\delta} \right],$$

(4)

with $h(x) = h(1/2 - 1/2\sqrt{1-x})$ and $h(x) \equiv -x \log_2 x - (1-x) \log_2(1-x)$ is the binary entropy function.

A Gilbert-Varshamov type achievability bound was also presented in [2]. These best known upper and lower bounds are well-separated. Despite intense research on LRCs, and in particular on rate-bounds (cf. [6]), no result asymptotically better than (3) is known. In this paper, we provide improved upper bounds on the rate of linear LRCs that are tighter than (3), for a range of rate-relative distance trade-off.

Our algebraic combinatorics methods are inspired by a recent work [7], that provides an improved estimate of rate of a code with sparse parity-check matrix. A combination of techniques from [1] and [7] leads to improvement over the bounds in [1] for linear LRCs with arbitrary repair groups of size at most $r$. We further improve over these bounds for disjoint repair groups. Our bounds apply for the asymptotic case and give an improvement over the best known bounds on linear LRC for small alphabets. For clarity, we state our result for binary alphabet.

The paper is organized as follows. In Section 2.1, we provide the main theorems: bounds on the rate of linear LRCs in general, and for the special case of disjoint repair groups. The main techniques of coset counting is presented in Section 2.2. The proof of the main results are presented subsequently.

**Notations**

For integers $a, b$ the relation $a \mid b$ denotes that $a$ divides $b$. $[m, n] := \{m, m + 1, \ldots, n\}$ and $[n] := \{1, 2, \ldots, n\}$. $\cup_i A_i$ denotes the union of disjoint sets $A_i$. $H((p_1, p_2, \ldots, p_n)^T) := \sum_i -p_i \log p_i$ denotes the entropy for the distribution $\{p_i\}$, while $h(p) := -p \log p - (1-p) \log 1-p$ denotes the binary entropy. The logarithms $\log(.)$ are taken to be base 2 throughout the paper. For a vector $v \in \mathbb{F}_2^n$, let $v(i)$ denote the symbol at coordinate $i$ of $v$. Denote $s(v)$ as the set $\{i \in [n] \mid v(i) \neq 0\}$ and $\text{wt}(v) := |s(v)|$. Define $e_i, i \in [n]$ as a vector in $\mathbb{F}_2^n$ such that $s(v) = \{i\}$. 

2
2 Rate upper bounds for LRC

2.1 Main results

Our first result for general linear LRC rate is presented below.

**Theorem 1** (Linear LRC). The rate of a binary linear LRC $C(n, \delta n, r)$ can be at most,

$$R(C) \leq \min_{0 \leq x \leq \frac{r}{r+1}} x + (1 - x(1 + 1/r)) \cdot R_1\left(\frac{\delta}{1 - x(1 + 1/r)}, r\right),$$

where, $R_1(\delta, r) = h(\rho) - c(r + 1, \rho)$, and $c(w, \rho) := \frac{\log_2 e^{w \cdot w}}{2^w} + 1$.

This bound is an improvement on (3) with $R_{\text{opt}}$ replaced by $R_{\text{MRRW}}$ and $R_1$ respectively. For LRCs with disjoint repair groups we have an even tighter bound on the rate.

**Theorem 2** (Linear LRC with Disjoint Repair Groups). Let,

$$\beta_i(x) := \begin{cases} \left(\frac{r+1}{2r+1}\right)^t, & i < t \\ \left(\frac{r+1}{2r+1}\right)^{t-i}, & i = t \end{cases}$$

The asymptotic rate $R(C)$ for a binary linear LRC $C(n, \delta n, r)$ with disjoint repair groups satisfies,

$$R(C) \leq \rho \log(x) + \frac{\log(\sum_{i=0}^t \beta_i(x))}{r+1} \bigg|_{x=\mu}$$

where $\mu = 1$ when $\left[\frac{\sum \beta_i(x)}{\sum \beta_i(x)}\right]_{x=1} \leq (r+1)\rho$ and

$$\mu = \text{Roots}^+(r+1)\rho \sum_{i=0}^t \binom{r+1}{i} x^{t-i} - \sum_{i=0}^t \binom{r+1}{i} i x^{t-i}$$

otherwise and where $t := \left\lfloor \frac{r+1}{2} \right\rfloor$ and $\text{Roots}^+(f(x))$ denotes the unique positive root of $f(x) = 0$.

In fig. 1 we compare the result of theorem 2 with the existing asymptotic bounds. The bounds converge together as $\delta$ and $r$ increase. But we can see from fig. 2 that our bound improves over the bound in (3) (cf. [1]) for $\delta \geq 0.38$ for $r = 2$ and this range improves as $r$ increases.

2.2 The method of counting cosets

The first MRRW bound provides the tightest (except for the second MRRW bound) upper bound on the rate of a code $C(n, \delta)$:

$$R(C) \leq h(\rho),$$

where $\rho := \frac{1}{2} - \sqrt{\delta(1 - \delta)}$. The bound is derived in [8] using linear constraints on the weight (distance) distribution of the code $C$. Another way to derive the first MRRW bound for linear codes is to analyze the distance between the codewords in the *coset leader graph* of $C$ [4]. These graphs are defined as follows [4].
Figure 1: Comparison of the asymptotic upper-bound on rate (vs relative minimum distance) in eq. (6) with the existing bounds in [1, 5, 8].

Figure 2: Difference between the bound in (3) (cf. [1]) and our bound eq. (6).
Definition 1. The coset leader graph $\mathcal{T}(C) = (\mathcal{V}, \mathcal{E})$ of a binary linear code $C$ is a graph with vertex set, $\mathcal{V} = \{x + C^\perp \mid x \in \mathbb{F}_2^n\}$ as the cosets of $C^\perp$. Two vertices in $\mathcal{T}(C)$ are connected iff the corresponding cosets are Hamming distance 1 apart i.e, $\{x + C^\perp, y + C^\perp\} \in \mathcal{E} \implies x = y + e_i + v$, for some $v \in C^\perp$ and $i \in [n]$.

It is known [3] that the eigenvalues $\lambda_1 \geq \lambda_2 \geq ...$ of the adjacency matrix of $\mathcal{T}(C)$ satisfy,

$$\lambda_i = n - 2d_i$$

where $d_1 \leq d_2 \leq ...$ are the weights of the codewords in $C$. Since $d_1 = 0$ for any linear code, we have $\delta = \frac{1}{2}(1 - \lambda_2/n)$, i.e., the minimum distance of the code corresponds to the second eigenvalue of the coset leader graph.

Note that, the shortest path length between the cosets $C^\perp$ and $x + C^\perp$ is equal to the weight of the coset leader of $x + C^\perp$. Denote the distance between two vertices in the graph $\mathcal{T}(C)$ as the length of the shortest path between them. Let $B_T(v, r)$ denote the vertices in $\mathcal{T}(C)$ inside a ball of radius $r$ and centered at vertex $v$. Since, the graph $\mathcal{T}(C)$ is vertex transitive, the volume in the $B_T(v, r)$ does not depend on $v$ and is written as $|B_T(r)|$. Thus, $B_T(r)$ also denotes the number of coset leaders of $C^\perp$ of weight not greater than $r$. From [7, Theorem 1.1], we know that the asymptotic rate, $R(C)$ of code $C$ with relative minimum distance $\delta$, can be upper-bounded using the coset leader graph $\mathcal{T}(C)$ as,

$$|C| \leq 2^{o(n)}|B_T \rho n|,$$  \hspace{1cm} (9)

where, recall, $\rho := \frac{1}{2} - \sqrt{\delta(1 - \delta)}$. Thus, the asymptotic MRRW bound on $R(C)$ in eq. (8) can be derived using a very general bound,

$$B_T \rho n \leq \sum_{i \leq \rho n} \binom{n}{i}.$$  \hspace{1cm} (10)

Note that the binary linear LRC $C(n, \delta n, r)$ also satisfies eq. (9). To improve the rate upper-bound eq. (8) for these codes, we can use their locality property to improve the counting upper-bound on $B_T \rho n$, eq. (10).

### 2.3 Upper bound for linear LRCs: proof of theorem 1

Consider a binary linear code $C$ with parity check matrix of constant row weights $w$. Then, for this code $C$ the following bound holds [7, Thm 1.2],

$$|B_T \rho n| \leq 2^{-c(w, \rho)n}|B(\rho n)|$$  \hspace{1cm} (11)

$B(t)$ denotes a ball of radius $t$ in $\mathbb{F}_2^n$. We describe a sketch of the proof of this bound from [7] below. Our proof of theorem 1 will then follow.

Consider a random binary vector $v$ such that $v(i) \sim Bernoulli(\rho)$ are iid for $i \in [n]$. Then the probability $p(\rho)$ that the vector $v$ is a coset leader of $C^\perp$ satisfies [7, Lemma 2.1],

$$p(\rho) \geq \Omega \left( \frac{1}{\sqrt{n}} \frac{|B_T \rho n|}{|B(\rho n)|} \right).$$  \hspace{1cm} (12)

We now upper bound the probability $p(\rho)$ by determining a necessary condition for each coset leader. Next, we use eq. (12) and the upper bound on $p(\rho)$ to find an upper bound on $B_T \rho n$. 


Let the parity check matrix for the code $C$ be $H = [v_1 v_2 \ldots v_m]^T$ such that $\text{wt}(v_i) = w, \forall i$. Then we divide the coordinates $[n]$ into partitions $\{I_j\}_{j \in [w]}$ using a recursive algorithm. Assume that $I_l, l > j$ have already been constructed. Then $I_j$ is constructed as in algorithm 1. Note that each partition $I_j$ is such that $I_j = \bigcup_{i=1}^{j} U_{ji}$ for $U_{ji} : |U_{ji}| = j$. Let the $v_{ji} \in \{v_i\}_i$ be the vector containing the support of the $U_{ji}$. Then, it is easy to see that $s(v_{ji}) \setminus U_{ji} \subseteq \bigcup_{i=1}^{j+1} I_i$.

**Algorithm 1:** Recursive algorithm for partitioning the coordinates in the code $C$

**Data:** $\{v_i\}_{i \in [m]}$, $\{I_l\}_{l = j+1}^w$

**Result:** $I_j \emptyset$, $T = \{v_i : i \in [m]\}$

1. while $\exists v_i \in T$ do
   2. if $|s(v_i) \setminus \bigcup_{i=j} I_i| = j$ then
      3. $I_j = I_j \cup \{s(v_i) \setminus \bigcup_{i=j} I_i\}$
   4. end
   5. $T = T \setminus \{v_i\}$

**Lemma 3.** There exists a partition $I_k$ such that,

$$|I_k| \geq \max \left\{ A \sum_{j > k} |I_j|, B \right\}$$

where $A = \frac{2}{\rho^2}$ and $B = \frac{n}{2w}$. The proof of lemma 3 follows from the requirement that there must exist at least one $k \in [n]$ such that $|I_k| \geq n/w$. Let the coordinate $k$ be such that lemma 3 is satisfied i.e. $|I_k| \geq \max \left\{ A \sum_{j > k} |I_j|, B \right\}$. Then, we claim that the support for every coset leader $x$ can contain at most $\frac{\rho^k}{2}t$ of the $k$-tuples $\{U_{ki}\}_{i=1}^t$. This can be immediately seen, since

$$y = x + \sum_{i \in S} v_{ki}$$

has weight less than $x$ for the set $S := \{i \mid U_{ki} \subseteq s(x)\}$ such that $|S| \geq \frac{\rho^k}{2}$. Thus, using this necessary condition for the coset leader $x$ we can upper bound $p(\rho)$ in eq. (12) as follows,

$$p(\rho) \leq \Pr \left( \text{Binomial}(\rho, t) \leq \frac{\rho^k}{2}t \right) \leq \exp \left( -\frac{\rho^k t}{8} \right) \leq \left( \frac{a}{2-c(w, \rho)n} \right)^t \leq 2^{-c(w, \rho)n},$$
where inequality (a) above follows since for $k$ satisfying lemma 3 we have,

$$\rho^k \cdot t \leq \frac{\rho^w}{w} B = \frac{\rho^w}{w} \cdot \frac{1}{2w^w} \cdot n.$$  

Here, we note that the upper-bound eq. (11) requires only the assumption that the parity check matrix $H$ of $C$ contains constant weight row vectors $v_i$ whose support covers the coordinates $[n]$. Note that for an LRC, every coordinate must have a repair group of size at most $r + 1$. Hence in the parity check matrix, there must be rows of weight $r + 1$ that covers all the coordinates by their support. Thus, we have the following upper bound for an LRC $C(n, \delta n, r)$.

**Lemma 4.** The asymptotic rate $R(C)$ for a binary linear LRC $C(n, \delta n, r)$ satisfies,

$$R(C) \leq h(\rho) - c(r + 1, \rho)$$

where and $c(w, \rho) := \log_2 e \left( \frac{\rho^w}{2} \right)^{w+1}$.

The upper bound in lemma 4 gives an upper-bound worse than the bound in (3). But we can construct a better bound by using the bound in lemma 4 inside the shortening bound in (3). A mild change in the argument of [1] first leads to the following bound.

**Theorem 5.** The rate for an LRC code $C(n, \delta n, r)$ satisfies,

$$R(C) \leq \min_{0 \leq x \leq r/(r+1)} x + (1 - x(1 + 1/r)) \cdot R_{\text{opt}} \left( \frac{\delta}{1 - x(1 + 1/r)}, r \right)$$

where $R_{\text{opt}}(\delta, r)$ is the optimal asymptotic rate of $C(n, \delta n, r)$.

In [1], the MRRW bound for $R_{\text{opt}}(x, r)$ was used. If we use the bound in lemma 4 for $R_{\text{opt}}(.)$ we have,

$$R(C) \leq \min_{0 \leq x \leq r/(r+1)} x + (1 - x(1 + 1/r)) \cdot R_1 \left( \frac{\delta}{1 - x(1 + 1/r)}, r \right)$$

where $R_1(.)$ is as defined in lemma 4.

This completes the proof of theorem 1.

### 2.4 Upper bound on LRC for disjoint repair groups: proof of theorem 2

In this section we consider the special case of LRC codes with disjoint repair groups. For this case too, the bound in lemma 4 applies. But we can improve that bound significantly in this situation. Consider a binary linear LRC $C(n, \delta n, r)$ with disjoint repair groups $R_j, j \in \left[ \frac{n}{r+1} \right]$. For clarity, in this section we assume
\((r + 1) \mid n\). The parity check-matrix of \(C\) must be of the form,

\[
H = \begin{pmatrix}
v_1 \\
v_2 \\
\vdots \\
v_{n'} \\
H'
\end{pmatrix}
\]

where \(n' = \frac{n}{r+1}\), \(s(v_i) \cap s(v_j) = \emptyset\) and \(R_i := s(v_i)\) are such that \(|R_i| = r + 1\) (even if the repair groups are of smaller size, we can add redundant coordinates in them to equal \(r + 1\)). Then, \(v \in B_T \rho n\) satisfies the following constraint,

\[
wt(v) \leq \min_{S \subseteq [n']} wt\left(v + \sum_{i \in S} v_i\right) \quad \text{(14a)}
\]

\[
wt(v) \leq \rho n \quad \text{(14b)}
\]

\[
|B_T \rho n \cap (x + \text{span}\{\{v_i\}_i\})| \leq 1 \forall x \in F_{2^n} \quad \text{(14c)}
\]

We use eq. (14) to find a better upper bound on \(R(C)\).

**Proof of theorem 2.** We find all vectors satisfying eq. (14) to upper bound \(|B_T \rho n|\) and to subsequently get an upper bound on \(R(C) = \log |B_T \rho n|/n\). Using eqs. (14a) and (14b) we must have,

\[
B_T \rho n \subseteq \left\{x \in F_{2^n} \bigg| wt(x) \leq \rho n, \ |s(x) \cap R_i| \leq \left\lfloor \frac{r + 1}{2} \right\rfloor \forall R_i\right\} \quad \text{(15)}
\]

The number of words in \(S\) is given by

\[
\sum_{k \leq \rho n} [x^k]\left(1 + \sum_{i=0}^{t} \binom{r+1}{i} x^i\right)^n \quad \text{(16)}
\]

where \(t = \left\lfloor \frac{r+1}{2} \right\rfloor\) and \([x^k]g(x)\) denotes the coefficient of \(x^k\) in \(g(x)\).

We can further reduce the bound in eq. (15) using eq. (14c). Since, \(v\) and \(v + v_i\) are of equal weight and are in the same coset we need to count only one of them in \(S\). Thus, for \(r + 1 = \text{even}\), we can improve the bound in eq. (16) as follows,

\[
|B_T \rho n| \leq \sum_{k \leq \rho n} [x^k]\left(1 + \sum_{i=0}^{t-1} \binom{r+1}{i} x^i + \frac{(r+1)}{2r \mod 2} x^t\right)^n \quad \text{where} \quad g(x) \quad \text{(17)}
\]

We now see that the upper bound in eq. (17) is dominated (asymptotically) by \(\max_k [x^k]g(x)\) i.e.

\[
\log \sum_{k \leq \rho n} [x^k]g(x) \quad \text{for} \quad n = \max_{k \leq \rho n} \frac{\log [x^k]g(x)}{n},
\]
as \( n \to \infty \). Thus we have,

\[
R(C) \leq \max_{k \leq \rho n} \frac{\log [x^k] g(x)}{n}
\]

\[
= \max_{\sum_i \alpha_i = \frac{t}{r+1}} \frac{1}{\sum_i \alpha_i \leq \rho} H((r + 1) \cdot \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_t \end{pmatrix})
\]

\[
+ \sum_{i=0}^{t-1} \alpha_i \log \left( \frac{r + 1}{i} \right) + \alpha_t \log \left( \frac{r + 1}{t} \right) \frac{2^n \text{mod} 2}{2^n \text{mod} 2}. \tag{18}
\]

Since, eq. (18) represents a concave optimization with linear constraints, we can find the optima in eq. (18) analytically. The optimum value is achieved at \( \alpha_i = \beta_i(x) \) for \( \beta_i(x) \) and \( \mu \) as defined in eqs. (5) and (7) and eq. (18) evaluates to eq. (6). \( \square \)

References

[1] V. Cadambe and A. Mazumdar. An upper bound on the size of locally recoverable codes. In Proc. IEEE Int. Symp. Network Coding, June 2013.

[2] V. Cadambe and A. Mazumdar. Bounds on the size of locally recoverable codes. Information Theory, IEEE Transactions on, 61(11):5787–5794, 2015.

[3] C. Delorme and P. Solé. Diameter, covering index, covering radius and eigenvalues. European Journal of Combinatorics, 12(2):95–108, 1991.

[4] J. Friedman and J.-P. Tillich. Generalized alon–boppana theorems and error-correcting codes. SIAM Journal on Discrete Mathematics, 19(3):700–718, 2005.

[5] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin. On the locality of codeword symbols. IEEE Trans. Inform. Theory, 58(11):6925–6934, Nov. 2012.

[6] S. Hu, I. Tamo, and A. Barg. Combinatorial and lp bounds for lrc codes. In Information Theory Proceedings (ISIT), 2016 IEEE International Symposium on. IEEE, 2016.

[7] E. Iceland and A. Samorodnitsky. On coset leader graphs of ldpc codes. Information Theory, IEEE Transactions on, 61(8):4158–4163, 2015.

[8] R. McEliece, E. Rodemich, H. Rumsey, and L. Welch. New upper bounds on the rate of a code via the delsarte-macwilliams inequalities. Information Theory, IEEE Transactions on, 23(2):157–166, 1977.

[9] I. Tamo and A. Barg. A family of optimal locally recoverable codes. IEEE Transactions on Information Theory, 60(8):4661–4676, 2014.