On the Maximal Code Length of Optimal Linear LRC Codes with Availability

Stanislav Kruglik, Kamilla Nazirkhanova and Alexey Frolov
Skolkovo Institute of Science and Technology, Moscow, Russia
Moscow Institute of Physics and Technology, Moscow, Russia
kruglik@phystech.edu, kamilla.nazirkhanova@phystech.edu, al.frolov@skoltech.ru

***Abstract*— A code over finite alphabet is said to be locally recoverable (LRC) if each code symbol is function of small number of other symbols forming the recovering set [1], [2], [3], [4], [5]. These codes were first proposed in [1] and immediate become popular due to obvious applications in distributed and cloud storage systems. Natural generalization of LRC codes is LRC codes with availability in which each code symbol has more than one disjoint recovering set. A LRC codes with availability is said to be optimal if its minimum distance achieves the Singleton- like bound developed by Kruglik et. al in this paper we study the maximum code length of q-ary optimal LRC with availability and then derive some structural properties.**

Keywords—locality, information theory, distributed storage, network coding, index coding

I. Introduction

Data coding with locality is a rapidly developing area in coding theory that was initially motivated by applications in distributed storage but since has expanded to applications in databases, with links to other parts of information theory (e.g., index coding and network coding) as well as to computer science in general. Temporary and permanent server failures in storage systems require new coding schemes that support efficient and fast data recovery without overloading system re- sources such as the number of reads, repair bandwidth, latency and others. Coding solutions relied on Reed-Solomon (RS) codes have been implemented in the file systems of Facebook and Google. These codes have been also standardized as a part of the well-known RAID 6 data protection technology. At the same time, RS does not meet the requirements for these applications due to big amount of inter-server communications during the procedure of one symbol recovery. This problem give rise to area of active research called codes with locality. Let us define it more formally. A locally recoverable code (LRC) is a code over finite alphabet such that each symbol is a function of small number of other symbols that form a recovering set [1], [2], [3], [4], [5], [6], [7], [8]. LRC codes are well-investigated in the literature. The bounds on the rate and minimum code distance are given in [1], [3] for the case of large alphabet size. The alphabet-dependent shortening bound (see [9] for the method explanation) is proposed in [10]. Optimal code constructions are given in [11] based on rank- metric codes (for large alphabet size, which is an exponential function of the code length) and in [12] based on Reed- Solomon codes (for small alphabet, which is a linear function of the code length).

The natural generalization of an LRC code is an LRC code with availability (or multiple disjoint recovering sets). Availability allows us to handle multiple simultaneous requests to erased symbols in parallel. This property is very important for hot data that is simultaneously requested by a large number of users. Bounds on parameters of such codes and constructions are given in [4], [6], [13], [14], [15]. In what follows we are interested in all-symbol locality and availability.

LRC codes with availability that attain bound on the min-mum distance proved in [6] are called optimal LRC codes with availability. This bound is in fact generalization of the classical Singleton bound for linear codes with locality and availability constraints.

In this paper we continue research started in [16] and extend it to the case of LRC codes with availability. Our contribution is as follows. New upper bound on code length of optimal LRC codes with availability are derived and structural properties of them are investigated.

II. Preliminaries

A. LRC codes

Let us denote by $\mathbb{F}_q$ a field with q elements. Let $[n] = \{1,2 \dots n\}$. The code $C \subset \mathbb{F}_q^n$ has locality r if every symbol of the codeword $c \in C$ can be recovered from a subset of r other symbols of c [1]. In other words, this means that, given $c \in C, i \in [n]$, there exists a subset of coordinates $R_i \subset [n] \backslash i, |R_i| \leq r$ such that the restriction of C to the coordinates in R_I enables one to find the value of c_i The subset R_i is called a recovering set for the symbol c_i.First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size.

B. LRC codes with availability

Assume that every symbol of the code C can be recovered from t disjoint subsets of symbols of size r. More formally, denote by C_I the restriction of the code C to a subset of coordinates $I \subset [n]$. Given $a \in \mathbb{F}_q$ define the set of codewords $C(i,a) = \{c \in C : c_i = a\}, i \in [n]$.

Definition 1: A code C is said to have *t* disjoint recovering sets if for every $i \in [n]$ there are t pairwise disjoint subsets $R_i^1, \dots, R_i^t \subset [n] \backslash i$such that for all $j = 1, \dots t$ and every pair of symbols $a, a' \in \mathbb{F}_q, a \neq a'$

$$C(i,a)_{\mathcal{R}_i^j} \cap C(i,a')_{\mathcal{R}_i^j} = \emptyset.$$

In what follows we refer to these codes as (r,t)-LRC codes. We briefly list the existing results below. The first bound for the code distance d of (r, t)-LRC codes was given in [17], [18] (in [17] only for linear case)

The reported study was funded by RFBR according to the research projects no. 16-01-00716, 18-07-01427, 18-37-00459.

978-1-7281-0432-4/18/$31.00 ©2018 IEEE
DOI 10.1109/EnT-MIPT.2018.00018

$$d \le n - k + 2 - \left\lceil \frac{t(k-1)+1}{t(r-1)+1} \right\rceil.$$

The latest improvement of this bound for linear case which is the focus of this work was obtained in [6]

$$d \le \min_{1+(r-1)s<k} d^*(n-1-sr, k-1-(r-1)s),$$

where $d^*(q, n, d)$ is an upper bound on the distance of any linear code.

If we substitute the Singleton bound for $d^*(q, n, d)$ function we obtain

$$d \le n - (k-1) - \lceil \frac{k-2}{r-1} \rceil. \qquad (1)$$

The bound on the rate of (r,t)-LRC codes was given in [13]

$$\frac{k}{n} \le R^*(r,t) = \prod_{i=1}^{t} \frac{1}{1+\frac{1}{ir}}$$

III. Maximal code length of optimal LRCs with availability

For a q-ary [n,k,d] maximum distance separable (MDS) code that attain Singleton bound it is known that its' code length do not exceed $q + k$-1 but it is an open problem in what set of parameters equality holds or not in general case. In this field of study there is only famous MDS conjecture presented below.

MDS Conjecture For a nontrivial q-ary [n,k,d] MDS code, if q is even and $k = 3$ or $k = q$-1, the code length does not exceed $q + 2$ and $q + 1$ otherwise.

An linear [n,k,d] LRC code with locality r is called optimal if its' obtain Singleton like bound developed in [1]

$$d \le n - k - \lceil \frac{k}{r} \rceil + 2,$$

that can be reduced to classical Singleton bound $d \le n$-$k + 1$ in case of $r = k$. In [16] it was proven that for the length of optimal linear LRC the following bound holds

$$n = \begin{cases} q + k + \lceil \frac{k}{r} \rceil - 2 & \text{if } r \ge 2 \text{and } r|k \\ q + k + \lceil \frac{k}{r} \rceil - 2 & \text{if } r \ge 2 \text{ and } k \ge 2 \ mod \ r \\ 2q + k + \lceil \frac{k}{r} \rceil - 2 & \text{if } r \ge 2 \text{ and } k = 1 \ mod \ r \\ 2q + k + \lceil \frac{k}{r} \rceil - 2 & \text{if } r = 1. \end{cases}$$

Note that this bound is tight over small finite field for some cases.

IV. Bounds on the code length of optimal LRCs with availability

The proof of the bound for code length of optimal linear LRC codes with availability is based on shortening techniques used for proof of upper bound of minimum distance of such codes [6]. For simplicity of readers we present here its' main ides. Let us denote by $\mathrm{Cl}(I)$ the set of all coordinates such that for every $c \in C$ the values $c_i, i \in Cl(I)$ can be found from the values of c_I. We will call the subset $Cl(I) \supset I$ the closure of I in [n]. Assume we are given an [n,k,d] linear (r,t)-LRC code C over F_q. Within the proof we construct a set of coordinates I, |I|=1+(r-1)s with such a property

$$|\mathrm{Cl}(I)| \ge 1 + rs.$$

Let us denote the code dual to C by $C^{\perp}$. By $C^{\perp}_{r+1}$we denote the set of codewords of dual code with the weigt (here and in what follows by weight we mean the Hamming weight, i.e. a number of non-zero elements in a vector) less or equal to r+1 (local checks), i.e.

$$C^{\perp}_{r+1} = \left\{ h \in C^{\perp} : wt(h) \le r+1 \right\}.$$

In what follows we work only with the set of all local checks $C^{\perp}_{r+1}$.

To construct the required set of coordinates |I|, |I|=1+(r-1)s, we apply Algorithm 1 with input parameters $C^{\perp}_{r+1}$ and s. Let us explain algorithm in more detail. At each step the algorithm adds a new local check (from the set $C^{\perp}_{r+1}$) to the set X untill s linearly independent local checks are added. By J we denote the set of covered positions. The algorythm chooses a local check with the largest intersection with J (line 8). Two cases are possible:

1. there exists a local check, which intersects with J.
2. there is no new local checks, which intersects with J

In the first case we need to check linear dependency (to proper calculate the number of check symbols) and add the local check to X. The second case is more interesting. This condition means, that the elements of X form an (r, t)-LRC code of smaller length. Indeed the absence of new local checks, which intersects with at least one element of X means that each position is covered either t times or not covered at all. We store the number of recovery sets, that from an (r, t)- LRC code of smaller length in the variable j and the number of check symbols of this code in the variable s_1.

From the description of shortening techniwue and form of bound on minimum distance of LRC code with

Algorithm 1 Construction of the set I

Input:
$\mathcal{C}_{r+1}^{\perp}$, s
Output:
X, I, s_1, j
$H \leftarrow \mathcal{C}_{r+1}^{\perp}$
choose any $h \in H$
$J \leftarrow supp(h)$, $X \leftarrow \{h\}$, $H \leftarrow H \backslash h$
$l \leftarrow 1$ ▷ Number of added local checks
$i \leftarrow 1$ ▷ Number of added linearly independent local checks
$j \leftarrow 0$
while $i \leq s$ **do**
  find the element $\mathbf{h} \in H$ with the largest $|J \cap supp(h)|$
  if $|J \cap supp(h)| = 0$ **then**
    $j \leftarrow l$
    $s_1 \leftarrow i$
    $i \leftarrow i + 1$
  else
    if $h \notin span\{X\}$ **then**
      $i \leftarrow i + 1$
    end if
    $J \leftarrow J \cup supp(h)$, $X \leftarrow X \cup \{h\}$, $H \leftarrow H \backslash h$
  end if
  $l \leftarrow l + 1$
end while
find I from X ▷ Note, that $J = \mathrm{Cl}(I)$
if $|I| < 1 + (r-1)s$ **then**
  add any $1 + (r-1)s - |I|$ other coordinates
end if

availability it's clear that after all shortening iterations equal to $s = \lceil \frac{k-2}{r-1} \rceil - 1$ parity check matrix of remaining code correspond to code with length $n'=n-1-sr$, dimension $k'=n-1-(r-1)s$ and code distance $d'=d$. In case of optimal LRC with availability this code are MDS code. In that follows we need to introduce some definitions.

Definition 2: Singleton defect of q-ary [n,k,d] code C is

$$s(C) := n-k-d+1$$

A linear code C is MDS in case of $s(C)=0$ and near MDS code in case of $s(C)=1$

Also we need the following lemma from [19]

Lemma 1: A q-ary [n,k,d] linear code C with dimension k>1 and Singleton defect $s(\mathrm{C}) = s$ has minimum distance $d \leq q(s+1)$

Theorem 1: Let $k > r > 1$ and $d > 2$. For a q-ary optimal linear [n,k,d] (r, t)-LRC code attaining the Singleton-like bound (1), the code length is upper bounded by $n \leq q + k + \left\lceil \frac{k-2}{r-1} \right\rceil - 2$

Proof: According to shortening technique described above after $s = \left\lceil \frac{k-2}{r-1} \right\rceil - 1$ shortening iterations in case of optimal (r,t)-LRC code we receive [n-1-sr,k-1-(r-1)s,d] MDS code. Then we distinguish two cases

Case 1 $(r-1) | (k-2)$

In this case $k' = k - 1 - (r-1)\left(\frac{k-2}{r-1} - 1\right) = r$. Due to it if $r \geq 2$ then according to Lemma 1 $d = d' \leq q$

Case 2 $(r-1) \nmid (k-2)$

In this case $k - 2 = b(r-1) + l$, where $b > 0$ and $l = \{1, 2, \ldots r-2\}$. In this case $k' = k-1-(r-1)(s-1+1) = l+1$ due to it $k' \geq 2$ and according to Lemma 1 $d = d' \leq q$

Since $d = n-k-\left\lceil \frac{k-2}{r-1} \right\rceil + 2$ the upper bound on the minimum distance can be translated to an upper bound on the code length and the theorem holds

■

From description of shortening the following corollary trivially follows:

Corollary 1: Let $k > r > 1$ and $d > 2$. For a q-ary optimal linear [n,k,d] (r, t)-LRC code C attaining the Singleton-like bound (1) the following bound true:

$$d(\mathrm{C}^{\perp}) \leq r + 1$$

V. Conclusion

In this paper we studied the maximal code length of q-ary linear optimal LRC code with availability achieving the Singleton-like bound and give some upper bounds on the code length. As a side result we bounded distance of dual code of linear optimal LRC with availability. Application of proposed techniques for determining weight hierarchy of linear optimal LRC with availability is an interesting direction for further research.

References

[1] P. Goplan, C. Huang, H. Simitci, and S. Yekhanin, "On the locality of codeword symbols," IEEE Trans. Inf. Theory, vol. 58, no. 11, pp. 6925–6934, Nov. 2011.
[2] P. Goplan, C. Huang, B. Jenkins, and S. Yekhanin, "Explicit maximally recoverable codes with locality," IEEE Trans. Inf. Theory, vol. 60, no. 9, pp. 5245 –5256, Sep. 2014.
[3] D. S. Papailiopoulos and A. G. Dimakis, "Locally repairable codes," IEEE Trans. Inf. Theory, vol. 60, no. 10, pp. 5843–5855, Oct 2014.
[4] A. S. Rawat, O. O. Koyluoglu, N. Silberstein, and S. Vishwanath, "Optimal locally repairable and secure codes for distributed storage systems," IEEE Trans. Inf. Theory, vol. 60, no. 1, pp. 212–236, Jan 2014.
[5] S. Yekhanin, "Locally decodable codes," Found. Trends Theoretical Comput. Sci., vol. 6, no. 3, pp. 139 –255, 2012.
[6] S. Kruglik and A. Frolov, "Bounds and constructions of codes with all-symbol locality and availability," in 2017 IEEE International Symposium on Information Theory (ISIT), June 2017, pp. 1023–1027.
[7] S. Kruglik, K. Nazirkhanova, and A. Frolov, "On distance properties of (r; t; x)-lrc codes," in 2018 IEEE International Symposium on Infor-mation Theory (ISIT), June 2018, pp. 1336–1339.
[8] S. Kruglik, M. Didina, V. Potapova, and A. Frolov, "On one generaliza-tion of lrc codes with availability," in 2017 IEEE Information Theory Workshop (ITW), November 2017, pp. 1–5.
[9] Y. Ben-Haim and S. Litsyn, "Upper bounds on the rate of ldpc codes as a function of minimum distance," IEEE Trans. Inf. Theory, vol. 52, no. 5, pp. 2092 –2100, May 2006.
[10] V. R. Cadambe and A. Mazumdar, "Bounds on the size of locally recoverable codes," IEEE Trans. Inf. Theory, vol. 61, no. 11, pp. 5787 –5794, Nov. 2015.
[11] N. Silberstein, A. S. Rawat, O. Koyluogly, and S. Vishwanath, "Optimal locally repairable codes via rank metric codes," in

Proceedings IEEE International Symposium on Information Theory (ISIT), 2013, pp. 1819– 1823.
[12] I. Tamo and A. Barg, "A family of optimal locally recoverable codes," IEEE Trans. Inf. Theory, vol. 60, no. 8, pp. 4661 –4676, Aug. 2014.
[13] I. Tamo, A. Barg, and A. Frolov, "Bounds on the parameters of locally recoverable codes," IEEE Trans. Inf. Theory, vol. 62, no. 6, pp. 3070 –3083, Jun. 2016.
[14] N. Prakash, V. Lalitha, and P. V. Kumar, "Codes with locality for two erasures," in Proceedings IEEE International Symposium on Information Theory (ISIT), 2014, pp. 1962–1966.
[15] P. Huang, E. Yaakobi, H. Uchikawa, and P. H. Siegel, "Linear locally repairable codes with availability," in Proceedings IEEE International Symposium on Information Theory (ISIT), Jun. 2015, pp. 1871–1875.
[16] J. Hao, K. Shum, S. Xia, and Y. Yang, "On the maximal code length of optimal linear locally repairable codes," in 2018 IEEE International Symposium on Information Theory (ISIT), June 2018, pp. 1326–1330.
[17] A. Wang and Z. Zhang, "Repair locality with multiple erasure tolerance," IEEE Trans. Inf. Theory, vol. 60, no. 11, pp. 6979–6987, Nov 2014.
[18] A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, "Locality and availability in distributed storage," in Proceedings IEEE International Symposium on Information Theory (ISIT), June 2014, pp. 681–685.
[19] A. Faldum and W. Willems, "Codes of small defect," Design, Codes and Cryptography, no. 10, pp. 341 –350, 1997.