

短码长四元最优局部修复码的构造

李瑞虎* 展秀珍 付强 张茂 郑尤良

(空军工程大学基础部 西安 710051)

摘要: 在分布式存储系统中, 当节点发生故障时局部修复码(LRC)可以通过访问少量其他节点来恢复数据, 然而LRC的局部度不尽相同, 该文构造了短码长且局部度较小的四元LRC。当码长不超过20, 最小距离大于2时, 若四元距离最优线性码的生成阵维数不超过校验阵维数, 可利用其生成阵给出LRC, 否则利用其校验阵给出LRC。对已构造的LRC的生成阵或校验阵, 利用删除、并置等方法得到新矩阵, 从而构造出190个码长 $n \leq 20$, 最小距离 $d \geq 2$ 的LRC。除12个LRC外, 其他LRC是局部度最优的。

关键词: 最优码; 局部修复码; 生成阵; 校验阵

中图分类号: TN918.3; O157.4

文献标识码: A

文章编号: 1009-5896(2021)12-3749-09

DOI: 10.11999/JEIT200740

Constructions of Quaternary Optimal Locally Repairable Code with Short Length

LI Ruihu ZHAN Xiuzhen FU Qiang ZHANG Mao ZHENG Youliang

(Fundamentals Department, Air Force Engineering University, Xi'an 710051, China)

Abstract: In distributed storage system, when a node fails, Locally Repairable Code (LRC) can access other nodes to recover data. However, the locality of LRC is not the same. Quaternary LRC with short code length and small locality is constructed. When code length is not more than 20 and minimum distance is greater than 2, if the dimension of generator matrix of a quaternary distance optimal linear code does not exceed the dimension of parity-check matrix, an LRC can be constructed from generator matrix, otherwise parity-check matrix can be used to construct an LRC. From generator matrices or parity-check matrices of LRCs constructed, other LRC are given by operations of deleting and juxtaposition. There are 190 LRC with code length $n \leq 20$ and minimum distance $d \geq 2$ to be constructed. Except for 12 LRC, other LRC are all locality optimal.

Key words: Optimal code; Locally Repairable Code (LRC); Generator matrix; Parity-check matrix

1 引言

在分布式存储系统中, 三重备份能够保证数据的可靠性, 并且它是最简单的方法^[1]。然而三重备份的存储效率低、存储代价过大, 于是人们提出了存储负荷更低的纠删码方案^[2,3]。传统纠删码能满足高效存储的需求, 但是修复效率低, 因此编码学者提出了局部修复码^[3]。2012年, Gopalan等人^[4]提

出LRC的概念以及Singleton-Like (S-L)界, 但是S-L界在小域^[4,5]上是不紧的。为了更加精确地描述 q 元局部修复码4个参数之间的关系, Cadambe和Mazumdar^[6]提出考虑域的大小的界, 即Cadambe-Mazumdar (C-M)界。

在工程应用中, 小域上LRC的编、解码复杂度较低, 更具有使用价值^[7]。二元域上LRC取得一定进展, 人们研究了达到S-L界^[8,9]以及C-M界^[10,11]的局部度最优LRC。文献^[12,13]研究了三元距离较小或者维数较低的局部度最优LRC。在四元域上, 人们得到一些局部度最优LRC: 文献^[14]构造了2类距离为3的四元LRC; 文献^[15]构造了距离为4的四元LRC; 这3类LRC是局部度最优和拟最优的^[14,15]。Barg等人^[16]利用代数曲线和代数曲面构造了码长为18、维数为11、距离为3、局部度为2的四元LRC。文献^[17]通过缩短 q 元汉明码与 $(q^2 + 1)$ -cap构造了

收稿日期: 2020-08-24; 改回日期: 2021-04-12; 网络出版: 2021-06-04

*通信作者: 李瑞虎 liruihu@aliyun.com

基金项目: 国家自然科学基金(11801564, 11901579), 陕西省自然科学基金(2021JM-216, 2021JQ-335), 空军工程大学基础部研究生创新基金

Foundation Items: The National Science Foundation of China (11801564, 11901579), Shaanxi Natural Science Foundation (2021JM-216, 2021JQ-335), The Graduate Scientific Research Foundation of Fundamentals Department of Air Force Engineering University

距离为3和4的LRC,从而可得到16个距离为3和12个距离为4的局部度最优四元LRC。Jin等人^[18]利用有限域上的自同构群构造一般域上LRC,可得到码长不超过5的四元LRC。由以上结果可知,当码长不超过20时,文献^[14,15,16]构造了特定距离的局部度最优或拟最优四元LRC,但只有1个码是距离最优码;文献^[17]的2个四元LRC以及文献^[18]的1个四元LRC都不是距离最优码。

由文献^[19]可知,当域的大小为2的幂次时,码的运行速度快,并且文献^[20]给出了RS码校验关系的等价转换方式,避免了复杂的符号转化。依据文献^[21-23],码长不超过20的距离最优四元码的参数完全确定。由文献^[23]可知,对于给定的码长和维数,距离最优四元码往往有很多,但是它们的局部度也有差别,人们往往更关注局部度尽可能小的LRC。基于此本文研究四元LRC,由已有文献结果可知,目前四元LRC的研究并不充分,其结果较为零散,因此本文将研究码长不超过20的四元码,设法构造距离最优且局部度尽可能小的四元LRC,并利用S-L界或C-M界判断其局部度的最优性。

2 预备知识

令 $F_4 = \{0, 1, \omega, \omega^2\}$ 为四元域,记 $\omega = 2$, $\omega^2 = 3$, $F_4 = \{0, 1, 2, 3\}$ 。 F_4^n 为 F_4 上的 n 维向量空间,若一个非零向量的第1个非零分量是1,则称此向量为首一向量。称 F_4^n 的 k 维子空间 C 为四元线性码 $[n, k]_4$,并记为 $C = [n, k]_4$, n 称为 C 的码长, C 中的向量称为码字。

若 $\mathbf{x} = (x_1, x_2, \dots, x_n)$, $\mathbf{y} = (y_1, y_2, \dots, y_n) \in F_4^n$, $\mathbf{x}$ 的汉明重量为 $\text{wt}(\mathbf{x}) = \#\{i | 1 \leq i \leq n, x_i \neq 0\}$, $\mathbf{x}$ 与 $\mathbf{y}$ 的汉明距离为 $d(\mathbf{x}, \mathbf{y}) = \text{wt}(\mathbf{x} - \mathbf{y})$ 。若 C 中非零码字的最小汉明重量为 d ,则记 $C = [n, k, d]_4$,若不存在 $[n, k, d+1]_4$ 码,则称 $C = [n, k, d]_4$ 为距离最优码。对于 $\mathbf{x}, \mathbf{y} \in F_4^n$, $\mathbf{x}$ 与 $\mathbf{y}$ 的内积为 $(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n x_i \cdot y_i$ 。称 $C^\perp = \{\mathbf{x} \in F_4^n | (\mathbf{x}, \mathbf{c}) = 0, \forall \mathbf{c} \in C\}$ 为 C 的对偶码,显然 $C^\perp$ 的维数为 $n - k$ 。由 C 的一组基构成的 $k \times n$ 矩阵 $\mathbf{G}_{k,n}$ 称为 C 的生成阵, $C^\perp$ 的生成阵 $\mathbf{H}_{n-k,n} = (\mathbf{h}_1^T, \mathbf{h}_2^T, \dots, \mathbf{h}_{n-k}^T)^T$ 称为 C 的校验阵。 $C = [n, k, d]_q$ 是码长为 n 、维数为 k 、最小距离为 d 的 q 元线性码,若码字 $\mathbf{c} = (c_1, c_2, \dots, c_n) \in C$ 的第 i 个码元 $c_i (1 \leq i \leq n)$ 都能通过除第 i 位以外的其他至多 r 位恢复,则称 C 的局部度为 r ,并记 $C = [n, k, d; r]_q$ 。线性码的局部度可以由生成阵和校验阵确定,具体如下:

引理1^[4] 设线性码 $C = [n, k, d]_q$ 的生成阵为 $\mathbf{G}_{k,n} = (\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_n)$, $\mathbf{g}_i$ 是 k 维列向量,当 $i \in [n]$ 时,若存在大小不超过 r 的子集 $A_i \subseteq [n] \setminus \{i\}$ 使得 $\mathbf{g}_i$ 被至

多 r 个 $\mathbf{g}_j (j \in A_i)$ 线性表出,则 C 的局部度为 r 。

引理2^[9] $\mathbf{H} = (\mathbf{H}_1^T, \mathbf{H}_{n-k-l}^T)^T$ 为线性码 $[n, k, d]_q$ 的校验阵, $\mathbf{H}_l$ 中的列均为非零列向量, $\mathbf{H}_l$ 的行称为 $\mathbf{H}$ 的局部度行。若 $\mathbf{H}_l$ 的行向量的汉明重量不超过 $r+1$,则 C 的局部度为 r 。

下面介绍常用的S-L界和C-M界。

引理3^[4,6] 若 $C = [n, k, d; r]_q$ 存在,式(1)和式(2)成立时,分别称为S-L界^[4]与C-M界^[6]

$$d \leq n - k + 2 - \lfloor k/r \rfloor \quad (1)$$

等式成立时,称码达到S-L界。特别地,当 $k = r$ 时,S-L界退化为经典的Singleton界。

$$k \leq \min_{t \in \mathbb{Z}^+} \{tr + k_{\text{opt}}^q(n - t(r+1), d)\} \quad (2)$$

其中, $k_{\text{opt}}^q(n, d)$ 是码长为 n 、最小距离为 d 的 q 元码的最大维数。等式成立时称 C 达到C-M界。

若 $C = [n, k, d; r]_q$ 达到S-L界或C-M界,或者 $[n, k, d; r-1]_q$ 的局部修复码不存在,则称 C 是局部度最优的(r -最优的)。

约定: $[n, k, d]_4$ 简记为 $[n, k, d]$; $[n, k, d; r]_4$ 简记为 $[n, k, d; r]$ 。 $\mathbf{i}_n = (i, i, \dots, i) (i = 0, 1, 2, 3)$ 表示长度为 n 且分量为 i 的行向量, $\mathbf{i}_n^T = (i, i, \dots, i)^T$ 为 $\mathbf{i}_n = (i, i, \dots, i)$ 的转置。 $[n] = \{1, 2, \dots, n\}$,并约定 $n \leq 20$; $\mathbf{I}_n$ 为 n 阶单位阵。记 $\mathbf{G}_{k,m}$ 的 l 个并置为 $\mathbf{G}_{k,lm} = (\mathbf{G}_{k,m}, \mathbf{G}_{k,m}, \dots, \mathbf{G}_{k,m}) = (l\mathbf{G}_{k,m})$ 。

3 F_4 上短码长LRC的构造

码长 $n \leq 20$ 的距离最优码共210个,其中 $[n, n, 1]$ 码不具有局部修复功能,还余下190个距离最优码。对于 $n \geq 2$, $\mathbf{I}_n$ 生成 $[n, 1, n; 1]$ 码,其对偶码为 $[n, n-1, 2; n-1]$,此两码达到S-L界。故以下仅需考虑 $[n, k, d]$ 和 $[n, n-k, d'] (k \geq 2)$ 形式的局部修复码构造,分7个小节展开讨论。

由文献^[22,23],分以下3步构造距离最优码的生成阵 $\mathbf{G}_{k,n}$:

步骤1 由文献^[22,23]得到距离最优码的生成阵,利用四元域中的乘法运算将生成阵中的列向量化为首一列向量;

步骤2 将首一列向量按照列汉明重量由小到大的顺序排列;

步骤3 对排序后的生成阵做列置换,依次删除生成阵 $\mathbf{G}_{k,n}$ 的最后 $j (1 \leq j < n-k)$ 个列向量得到子矩阵 $\mathbf{G}_{k,n-j}$,从而由已有LRC构造新LRC。

3.1 参数为 $[n, 2, d]$ 和 $[n, n-2, d']$ 的LRC

构造 $\mathbf{G}_{2,5} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \end{pmatrix} = (\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_5)$, $\mathbf{G}_{2,i} = (\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_i)$ 以及 $\mathbf{G}_{2,2i} = (\mathbf{G}_{2,i} | \mathbf{G}_{2,i})$, $2 \leq i \leq 5$ 。

由 $G_{2,i}(3 \leq i \leq 5)$ 可得 $[3, 2, 2; 2]$, $[4, 2, 3; 2]$ 和 $[5, 2, 4; 2]$ 码; 由 $G_{2,2i}(3 \leq i \leq 5)$ 可得 $[6, 2, 4; 1]$, $[8, 2, 6; 1]$ 和 $[10, 2, 8; 1]$ 码。令 $G_{2,5+j} = (G_{2,5} | G_{2,j})(j = 2, 4)$, 可得 $[7, 2, 5; 2]$ 和 $[9, 2, 7; 2]$ 码。若 $n = 5l$ 且 $l \geq 2$, 则 $G_{2,5l} = (lG_{2,5})$ 生成 $[5l, 2, 4l; 1]$ 码。若 $n = 5l + i \geq 11$, $1 \leq i \leq 4$ 且 $l \geq 2$, 则 $G_{2,5l+i} = (G_{2,5(l-1)} | G_{2,5+i})$ 生成 $[5l + i, 2, 4l + i - 1; 1]$ 码。当 $2m \geq 6$ 时, 构造校验阵

$$H_{2,2m} = \begin{pmatrix} \mathbf{1}_m & \mathbf{0}_m \\ \mathbf{0}_m & \mathbf{1}_m \end{pmatrix}, H_{2,2m+1} = \begin{pmatrix} \mathbf{1}_m & \mathbf{0}_{m+1} \\ \mathbf{0}_m & \mathbf{1}_{m+1} \end{pmatrix} \quad (3)$$

以 $H_{2,2m}$ 和 $H_{2,2m+1}$ 为校验阵的码为 $[n, n-2, 2; \lceil (n-2)/2 \rceil](n = 2m, 2m+1 \geq 6)$ 。

以上构造的LRC都是距离最优码, 其中 $r=1$ 的LRC的局部度已达到最小; 码长 $3 \leq n \leq 10$ ($n \neq 7, 9$) 的 $[n, 2, d; r]$ 码和 $n \geq 6$ 的 $[n, n-2, 2; \lceil (n-2)/2 \rceil]$ 达到S-L界; $[7, 2, 5; 2]$ 和 $[9, 2, 7; 2]$ 达不到S-L界和C-M界, 但不难验证 $[7, 2, 5; 1]$ 和 $[9, 2, 7; 1]$ 不存在, 故这两个码仍是 r -最优的。

3.2 参数为 $[n, 3, d]$ 和 $[n, n-3, d']$ 的LRC

记 $G_{3,n} = (I_3 | B_{3,n-3})$, 构造如式(4)的4个矩阵:

$$\begin{aligned} B_{3,2} &= \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 3 & 2 \end{pmatrix}, B_{3,6} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 3 & 1 & 2 & 2 & 3 \\ 2 & 0 & 3 & 1 & 3 & 1 \end{pmatrix}, \\ B_{3,13} &= \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 2 & 3 & 1 & 1 & 1 & 2 & 2 & 3 & 3 \\ 1 & 2 & 1 & 2 & 0 & 0 & 1 & 2 & 3 & 1 & 3 & 2 & 3 \end{pmatrix}, \\ G_{3,21} &= \begin{pmatrix} 1 & 0 & 0 & | & 0 & 1 & 1 & | & 0 & 1 & 1 & | & 0 & 1 & 1 & | & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & | & 1 & 0 & 1 & | & 1 & 0 & 2 & | & 1 & 0 & 3 & | & 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \\ 0 & 0 & 1 & | & 1 & 1 & 0 & | & 2 & 2 & 0 & | & 3 & 3 & 0 & | & 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 \end{pmatrix} \\ &= (\alpha_1, \alpha_2, \dots, \alpha_{21}) \quad (4) \end{aligned}$$

以上 $G_{3,n}$ 分别生成 $[5, 3, 3; 3]$, $[9, 3, 6; 2]$, $[16, 3, 12; 2]$ 和 $[21, 3, 16; 2]$ 码。由 $G_{3,5}$ 的子矩阵可得 $[4, 3, 2; 3]$; $G_{3,5}$ 添加列向量 $(1, 3, 1)^T$ 得到 $G_{3,6}$, $G_{3,6}$ 生成 $[6, 3, 4; 3]$ 。类似地, 由 $G_{3,9}$ 的子矩阵可得 $[7, 3, 4; 2]$ 和 $[8, 3, 5; 2]$ 码; 由 $G_{3,16}$ 的子矩阵 $G_{3,n}$ ($n = 16 - j, 1 \leq j \leq 5$) 可得 $[16 - j, 3, 12 - j; 2]$ 码。当 $17 \leq n = 21 - j \leq 21$ 时, 由 $G_{3,21}$ 的子矩阵 $G_{3,n}$ 可得 $[21 - j, 3, 16 - j; 2]$ 。特别地, 当 $i = 5, 6$ 时, 构造 $G_{3,2i} = (G_{3,i} | G_{3,i})$, $G_{3,2i}$ 生成 $[10, 3, 6; 1]$ 和 $[12, 3, 8; 1]$ 码。记 $G_{3,n} = (\alpha_1, \alpha_2, \dots, \alpha_n)$, $7 \leq n \leq 21$ 。当 $13 \leq n = 21 - j \leq 21$ 时, 以 $G_{3,n}$ 为校验阵的码为 $[n, n-3, 3; 15-j]$ [19]。当 $7 \leq n = 12 - j \leq 12$ 时, 以 $G_{3,n}$ 为校验阵的码为 $[12 - j, 9 - j, 3; 6 - \lfloor 2j/3 \rfloor]$ 。

以上构造的LRC均为距离最优码, 其中 $4 \leq n \leq 10$ 的 $[n, 3, d; r]$ 以及 $[n, n-3, 3; 6 - \lfloor 2j/3 \rfloor]$

($7 \leq n = 12 - j \leq 12$) 和 $[n, n-3, 3; 15-j]$ ($13 \leq n = 21 - j \leq 21$) 码达到S-L界; $11 \leq n = 16 - j \leq 15$ 的 $[n, 3, 12 - j; 2]$, $[16, 3, 12; 2]$ 和 $[n, 3, 16 - j; 2]$ ($17 \leq n = 21 - j \leq 21$) 码为达到C-M界的LRC。

3.3 参数为 $[n, 4, d]$ 和 $[n, n-4, d']$ 的LRC

记 $G_{4,n} = (I_4 | B_{4,n-4})$, 构造如式(5)的5个矩阵, $G_{4,17}$ 由文献[17]给出

$$\begin{aligned} B_{4,2} &= \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}, B_{4,6} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 1 & 3 & 3 \\ 2 & 0 & 1 & 3 & 1 & 3 \\ 3 & 3 & 0 & 1 & 3 & 2 \end{pmatrix}, \\ B_{4,19} &= \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 3 & 1 & 1 & 1 & 3 & 3 & 3 & 0 & 1 & 1 & 2 \\ 0 & 3 & 0 & 3 & 0 & 2 & 1 & 3 & 1 & 2 & 2 & 1 & 2 & 2 & 3 & 3 & 0 & 1 & 1 \\ 3 & 0 & 2 & 0 & 0 & 3 & 1 & 0 & 1 & 2 & 3 & 3 & 1 & 1 & 3 & 2 & 3 & 2 & 2 \end{pmatrix}, \\ B_{4,13} &= \begin{pmatrix} 0 & 1 & 1 & 1 & | & 0 & 1 & 1 & 1 & | & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 3 & 1 & | & 1 & 0 & 2 & 2 & | & 1 & 2 & 1 & 3 & 3 \\ 3 & 2 & 0 & 2 & | & 2 & 3 & 0 & 1 & | & 3 & 2 & 1 & 1 & 3 \\ 1 & 1 & 3 & 0 & | & 2 & 3 & 1 & 0 & | & 2 & 2 & 3 & 2 & 1 \end{pmatrix}, \\ H_{4,21} &= \begin{pmatrix} 1 & 0 & 0 & | & 1 & 0 & 0 & | & 1 & 0 & 0 & | & 1 & 0 & 0 & | & 0 & 1 & 1 & | & 0 & 1 & 1 & | & 0 & 1 & 1 \\ 0 & 1 & 0 & | & 0 & 1 & 0 & | & 0 & 1 & 0 & | & 0 & 1 & 0 & | & 1 & 0 & 1 & | & 1 & 0 & 2 & | & 1 & 0 & 3 \\ 0 & 0 & 1 & | & 0 & 0 & 1 & | & 0 & 0 & 1 & | & 0 & 0 & 1 & | & 1 & 1 & 0 & | & 2 & 2 & 0 & | & 3 & 3 & 0 \\ 0 & 0 & 0 & | & 1 & 1 & 1 & | & 2 & 2 & 2 & | & 3 & 3 & 3 & | & 0 & 0 & 0 & | & 0 & 0 & 0 & | & 0 & 0 & 0 \end{pmatrix} \quad (5) \end{aligned}$$

$G_{4,6}$ 和 $G_{4,10}$ 分别生成 $[6, 4, 2; 2]$ 和 $[10, 4, 6; 3]$ 码。删除 $G_{4,10}$ 的后 i ($1 \leq i \leq 3$) 列, 可得 $[9, 4, 5; 3]$, $[8, 4, 4; 3]$ 和 $[7, 4, 3; 3]$ 码。 $G_{4,23}$ 生成 $[23, 4, 16; 2]$ 码, 删除 $G_{4,23}$ 的后 i ($1 \leq i \leq 4$) 列可得 $[22, 4, 15; 2]$, $[21, 4, 14; 2]$, $[20, 4, 13; 2]$ 和 $[19, 4, 12; 2]$ 码。 $G_{4,17}$ 添加 $G_{4,17}$ 中的1列可得 $[18, 4, 12; 3]$, 由文献[17]删除校验阵 $G_{4,17}$ 的列可得到 $[n, n-4, 4; r_n]$, $9 \leq n = 17 - j \leq 17$, 其中 $n = 9, 10, \dots, 16, 17$ 时局部度分别为 $r_n = 4, 5, 6, 6, 7, 8, 9, 10, 11$ 。记 $G_{4,17} = (\beta_1, \beta_2, \dots, \beta_{17})$, 令 $G_{4,n} = (\beta_1, \beta_2, \dots, \beta_n)$, ($11 \leq n = 17 - j \leq 17$), $G_{4,n}$ 生成 $[n, 4, 12 - j; 3]$ 码。以 $H_{4,21}$ 为校验阵的码为 $[21, 17, 3; 9]$ 。当 $1 \leq i \leq 3$ 时, 删除 $H_{4,21}$ 的后 i 列得到 $[20, 16, 3; 9]$, $[19, 15, 3; 8]$ 和 $[18, 14, 3; 7]$ 码。以上构造的LRC都是距离最优码, 其中 $6 \leq n \leq 10$ 的 $[n, 4, d; r]$ 码和 $9 \leq n \leq 17$ 的 $[n, n-4, 4; r]$ 码达到S-L界; 达到C-M界的LRC为 $11 \leq n \leq 23$ ($n \neq 19$) 的 $[n, 4, d; r]$ 以及 $18 \leq n \leq 21$ 的 $[n, n-4, 3; r]$; 而 $[19, 4, 12; 2]$ LRC达不到S-L界和C-M界。

3.4 参数为 $[n, 5, d]$ 和 $[n, n-5, d']$ 的LRC

记 $G_{5,n} = (I_5 | B_{5,n-5})$, 构造以下7个矩阵, $X_i = (\gamma_1, \gamma_2, \dots, \gamma_i)$ ($4 \leq i \leq 6$):

由 $G_{5,n}$ 分别可得 $[7, 5, 2; 3]$, $[11, 5, 6; 4]$, $[14, 5, 8; 3]$, $[17, 5, 10; 3]$ 和 $[24, 5, 16; 2]$ 码。由 $G_{5,11}$ 的

子矩阵可得 $[10, 5, 5; 4]$, $[9, 5, 4; 4]$, $[8, 5, 3; 4]$ 码; 由 $\mathbf{G}_{5,14}$ 的子矩阵可得 $[13, 5, 7; 3]$, $[12, 5, 6; 4]$ 码; 由 $\mathbf{G}_{5,17}$ 的子矩阵可得 $[16, 5, 9; 3]$, $[15, 5, 8; 3]$ 码。当 $1 \leq i \leq 6$ 时, 依次删除 $\mathbf{G}_{5,24}$ 的后 i 列分别可得 $[23, 5, 15; 3]$, $[22, 5, 14; 3]$, $[21, 5, 13; 2]$, $[20, 5, 12; 3]$, $[19, 5, 11; 3]$, $[18, 5, 10; 2]$ 码。以 $\mathbf{H}_{5,3i}(i = 4, 5, 6)$ 为校验阵的码为 $[12, 7, 4; 3]$, $[15, 10, 4; 4]$ 和 $[18, 13, 4; 5]$ 。删除 $\mathbf{H}_{5,3i}(i = 5, 6)$ 的最后1列可分别为 $[14, 9, 4; 4]$ 与 $[17, 12, 4; 5]$; 删除 $\mathbf{H}_{5,15}$ 的第10和15列得到 $[13, 8, 4; 4]$

码, 删除 $\mathbf{H}_{5,18}$ 的第12和18列可得 $[16, 11, 4; 5]$ 码。 $\mathbf{H}_{5,18}$ 依次添加列向量 $(1, 1, 1, 2, 3)^T$ 和 $(1, 2, 3, 1, 1)^T$ 得到 $\mathbf{H}_{5,19}$ 与 $\mathbf{H}_{5,20}$, 以 $\mathbf{H}_{5,19}$ 为校验阵的码为 $[19, 14, 4; 6]$, 以 $\mathbf{H}_{5,20}$ 为校验阵的码为 $[20, 15, 4; 7]$ 。以上构造的LRC都是距离最优码, 其中 $7 \leq n \leq 11$ 的 $[n, 5, d; r]$ 和 $12 \leq n \leq 20(n \neq 13)$ 的 $[n, n-5, 4; r]$ 码达到S-L界; $12 \leq n \leq 24(n \neq 19, 20)$ 的 $[n, 5, d; r]$ 码以及 $[13, 8, 4; 4]$ 码达到C-M界; 而 $[19, 5, 11; 3]$ 和 $[20, 5, 12; 3]$ 码达不到S-L界和C-M界。

$$\begin{aligned} \mathbf{B}_{5,2} &= \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}, \mathbf{B}_{5,6} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 3 & 2 & 2 & 3 \\ 3 & 2 & 1 & 3 & 1 & 3 \\ 1 & 3 & 3 & 0 & 1 & 2 \\ 3 & 1 & 0 & 1 & 3 & 3 \end{pmatrix}, \mathbf{B}_{5,9} = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 & 3 & 1 & 2 \\ 1 & 1 & 3 & 1 & 2 & 2 & 2 & 3 & 3 \\ 1 & 0 & 3 & 1 & 1 & 0 & 3 & 2 & 2 \\ 3 & 2 & 3 & 0 & 0 & 3 & 2 & 3 & 1 \end{pmatrix}, \mathbf{B}_{5,12} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 3 & 1 & 2 & 1 & 1 & 2 & 2 \\ 1 & 2 & 3 & 2 & 3 & 1 & 0 & 3 & 3 & 1 & 3 & 2 \\ 2 & 0 & 2 & 1 & 2 & 2 & 3 & 1 & 1 & 3 & 3 & 2 \\ 2 & 1 & 0 & 2 & 0 & 0 & 2 & 2 & 3 & 1 & 3 & 3 \end{pmatrix}, \\ \mathbf{B}_{5,19} &= \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 2 & 3 & 1 & 1 & 2 & 3 & 2 & 0 & 3 & 2 & 0 & 3 \\ 0 & 1 & 0 & 3 & 0 & 1 & 2 & 2 & 1 & 3 & 3 & 2 & 1 & 3 & 1 & 2 & 0 & 1 & 3 \\ 0 & 1 & 2 & 0 & 1 & 2 & 3 & 0 & 3 & 1 & 2 & 2 & 3 & 1 & 0 & 2 & 3 & 1 & 2 \\ 0 & 1 & 3 & 2 & 1 & 3 & 0 & 3 & 0 & 3 & 1 & 3 & 3 & 1 & 1 & 1 & 2 & 0 & 3 \end{pmatrix}, \mathbf{H}_{3,6} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 3 & 1 & 2 & 1 & 3 \\ 1 & 1 & 2 & 2 & 3 & 3 \end{pmatrix} = \begin{pmatrix} 1, 1, 1, 1, \dots, 1 \\ \gamma_1, \gamma_2, \dots, \gamma_6 \end{pmatrix}, \\ \mathbf{H}_{5,3-i} &= \begin{pmatrix} \mathbf{1}_i & \mathbf{0}_i & \mathbf{0}_i \\ \mathbf{0}_i & \mathbf{1}_i & \mathbf{0}_i \\ \mathbf{0}_i & \mathbf{0}_i & \mathbf{1}_i \\ \mathbf{X}_i & \mathbf{X}_i & \mathbf{X}_i \end{pmatrix} \end{aligned} \quad (6)$$

3.5 参数为 $[n, 6, d]$ 和 $[n, n-6, d']$ 的LRC

记 $\mathbf{G}_{6,n} = (\mathbf{I}_6 | \mathbf{B}_{6,n-6})$, 构造以下7个矩阵, 横线以上的行为校验阵的局部度行。

由 $\mathbf{G}_{6,12}$ 和 $\mathbf{G}_{6,12}$ 的子矩阵可得 $[12, 6, 6; 5]$ 和 $[11, 6, 5; 5]$ 码; 由 $\mathbf{G}_{6,15}$ 和 $\mathbf{G}_{6,15}$ 的子矩阵可得 $[15, 6, 8; 4]$, $[14, 6, 7; 4]$ 和 $[13, 6, 6; 4]$ 码; 由 $\mathbf{G}_{6,18}$ 和 $\mathbf{G}_{6,18}$ 的子矩阵可得 $[18, 6, 10; 4]$, $[17, 6, 9; 4]$, $[16, 6, 8; 4]$ 码; 由 $\mathbf{G}_{6,20}$ 和 $\mathbf{G}_{6,20}$ 的子矩阵可得 $[20, 6, 11; 3]$ 和 $[19, 6, 10; 3]$ 码。以 $\mathbf{H}_{6,14}$ 为校验阵的码为 $[14, 8, 5; 5]$, 删除 $\mathbf{H}_{6,14}$ 的最后1列得到 $[13, 7, 5; 4]$ 码; 以 $\mathbf{H}_{6,17}$ 为校验阵的码为 $[17, 11, 5; 7]$, 依次删除 $\mathbf{H}_{6,17}$ 的后2列得到 $[16, 10, 5; 6]$ 和 $[15, 9, 5; 5]$ 码; 由 $\mathbf{H}_{6,21}$ 可得 $[21, 15, 5; 11]$, 删除 $\mathbf{H}_{6,21}$ 的后3列得到 $[20, 14, 5; 10]$, $[19, 13, 5; 9]$, $[18, 12, 5; 8]$ 码。以上构造的LRC均为距离最优码, 其中 $[11, 6, 5; 5]$ 和 $[12, 6, 6; 5]$ 码达到S-L界; $13 \leq n \leq$

18的 $[n, 6, d; 4]$ 及 $13 \leq n \leq 21$ 的 $[n, n-6, 5; r]$ 码达到C-M界; 而 $[19, 6, 10; 3]$ 和 $[20, 6, 11; 3]$ 码达不到S-L界和C-M界。

3.6 参数为 $[n, 7, d]$ 和 $[n, n-7, d']$ 的LRC

记 $\mathbf{G}_{7,n} = (\mathbf{I}_7 | \mathbf{B}_{7,n-7})$, 构造4个矩阵(见下页)。矩阵 $\mathbf{G}_{7,n}$ 分别生成 $[16, 7, 8; 5]$, $[18, 7, 9; 5]$ 和 $[20, 7, 10; 5]$ 码; 删除这3者的最后1列分别得到 $\mathbf{G}_{7,n-1}(n = 16, 18, 20)$ 及其生成的 $[15, 7, 7; 5]$, $[17, 7, 8; 5]$ 和 $[19, 7, 9; 5]$ 码。以 $\mathbf{H}_{7,20}$ 为校验阵得到 $[20, 13, 6; 7]$ 码, 依次删除 $\mathbf{H}_{7,20}$ 的后 $i(1 \leq i \leq 6)$ 列得到 $[19, 12, 6; 7]$, $[18, 11, 6; 6]$, $[17, 10, 6; 6]$, $[16, 9, 6; 5]$, $[15, 8, 6; 5]$, $[14, 7, 6; 4]$ 码。以上构造的LRC都是距离最优码, 其中 $15 \leq n \leq 18$ 的 $[n, 7, d; r]$ 和 $14 \leq n \leq 20$ 的 $[n, n-7, 6; r]$ 码达到C-M界; 而 $[19, 7, 9; 5]$ 和 $[20, 7, 10; 5]$ 码达不到S-L界和C-M界。

$$\mathbf{B}_{6,6} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 1 & 2 \\ 1 & 0 & 2 & 3 & 3 & 1 \\ 2 & 3 & 3 & 0 & 2 & 1 \\ 2 & 3 & 0 & 2 & 1 & 3 \\ 3 & 2 & 3 & 2 & 1 & 1 \end{pmatrix}, \mathbf{B}_{6,9} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 3 & 0 & 1 & 1 & 2 & 3 & 3 \\ 3 & 1 & 1 & 2 & 0 & 0 & 1 & 2 & 2 \\ 3 & 1 & 0 & 2 & 1 & 3 & 0 & 1 & 3 \\ 3 & 0 & 0 & 3 & 3 & 1 & 1 & 1 & 2 \\ 0 & 0 & 1 & 2 & 3 & 1 & 2 & 2 & 1 \end{pmatrix}, \mathbf{B}_{6,12} = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 3 & 1 & 2 \\ 1 & 2 & 0 & 0 & 1 & 0 & 1 & 1 & 3 & 3 & 3 & 3 \\ 1 & 1 & 3 & 0 & 0 & 1 & 2 & 1 & 1 & 0 & 1 & 3 \\ 1 & 0 & 3 & 2 & 0 & 0 & 2 & 2 & 2 & 3 & 3 & 1 \\ 1 & 3 & 2 & 2 & 3 & 3 & 1 & 2 & 0 & 3 & 2 & 3 \end{pmatrix},$$

$$\begin{aligned}
B_{6,14} &= \begin{pmatrix} 00011011111111 \\ 01100101231233 \\ 12122332123311 \\ 20303230331111 \\ 01030312031312 \\ 10332312302323 \end{pmatrix}, H_{6,14} = \begin{pmatrix} 11000000303032 \\ 10002020000311 \\ 10303000310001 \\ 01320000200302 \\ 00112003000012 \\ 00103100001202 \end{pmatrix}, \\
H_{6,17} &= \begin{pmatrix} 10000013020120013 \\ 01320000202003011 \\ 00122310000200031 \\ 10002020100003123 \\ \hline 01303000300130303 \\ 00103100220012020 \end{pmatrix}, H_{6,21} = \begin{pmatrix} 100001013020120320121 \\ 010000101302011032212 \\ 001223310000200110221 \\ \hline 000100033221201133102 \\ 000010130211213202200 \\ 000001331303303113111 \end{pmatrix}; \\
B_{7,9} &= \begin{pmatrix} 011111011 \\ 101123101 \\ 210110232 \\ 223100111 \\ 120103322 \\ 301011132 \\ 031023312 \end{pmatrix}, B_{7,11} = \begin{pmatrix} 11001011111 \\ 03012131112 \\ 00111113323 \\ 03130212311 \\ 10131100112 \\ 12313213133 \\ 21203322313 \end{pmatrix}, B_{7,13} = \begin{pmatrix} 0101101111111 \\ 1012010301331 \\ 1200113200212 \\ 3021121332013 \\ 0300012323211 \\ 3330200012123 \\ 0032332031103 \end{pmatrix}, \\
H_{7,20} &= \begin{pmatrix} 10020103000001101001 \\ 01100000023010102030 \\ 00123320000000020110 \\ 00000002333200010201 \\ \hline 12003010300132000000 \\ 01013200310300203200 \\ 00013311032220001000 \end{pmatrix} \quad (7)
\end{aligned}$$

3.7 参数为 $[n, k \geq 8, d]$ 和 $[n, n-k, d']$ 的LRC

构造以下7个矩阵, 如式(9), 以 $H_{8,17}$ 为生成阵的码为 $[17, 8, 8; 6]$, 其前16列生成 $[16, 8, 7; 6]$ 码; 以 $H_{8,17}$ 为校验阵的码为 $[17, 9, 7; 7]$ 。由校验阵 $H_{8,21}$ 可得 $[21, 13, 6; 8]$ 码, 删除 $H_{8,21}$ 的后 $s(1 \leq s \leq 3)$ 列可得到 $[20, 12, 6; 7]$, $[19, 11, 6; 7]$ 和 $[18, 10, 6; 6]$ 码。由 $H_{9,18}$ 可得 $[18, 9, 8; 7]$ 码, 删除 $H_{9,18}$ 的最后1列可得 $[17, 8, 8; 6]$ 码。由校验阵 $H_{9,21}$ 可得 $[21, 12, 7; 8]$ 码, 删除 $H_{9,21}$ 的后 $i(1 \leq i \leq 2)$ 列可得 $[21-i, 12-i, 7; 8-i]$ 码。以 $H_{10,20}$ 为校验阵的码为 $[20, 10, 8; 7]$ 码, 删除

$H_{10,20}$ 的后 $i(1 \leq i \leq 2)$ 列可得 $[20-i, 10-i, 8; 7-i]$ 码。由校验阵 $H_{11,22}$ 可得 $[22, 11, 8; 7]$ 码, 删除 $H_{11,22}$ 的后 $s(1 \leq s \leq 3)$ 列可得 $[21, 10, 8; 6]$, $[20, 9, 8; 5]$ 和 $[19, 8, 8; 5]$ 码。以上构造的LRC均为距离最优码, 其中 $[n, n-8, 7; r](n=16, 17)$, $19 \leq n \leq 21$ 的 $[n, n-9, 7; r]$, $[n, n-9, 8; r](n=17, 18)$, $18 \leq n \leq 20$ 的 $[n, n-10, 8; r]$ 以及 $20 \leq n \leq 23$ 的 $[n, n-12, 9; r]$ 达到C-M界; 而 $[n, n-8, 6; r](18 \leq n \leq 20)$, $[19, 8, 8; 5]$ 和 $[20, 9, 8; 5]$ 达不到S-L界和C-M界。

$$\begin{aligned}
H_{8,17} &= \begin{pmatrix} 10000000121232003 \\ 01000030332220003 \\ 00010002220030331 \\ 12000201230010002 \\ 12100030110000012 \\ 01003002130010033 \\ \hline 00131012000120030 \\ 00001210000232103 \end{pmatrix}, H_{8,21} = \begin{pmatrix} 103320000010302000011 \\ 012002032001000300011 \\ 000010111110000001302 \\ 000000000000111111101 \\ \hline 120201300200010030001 \\ 103320000010302000012 \\ 010101301000201002110 \\ 001002110200101032030 \end{pmatrix},
\end{aligned}$$

$$\begin{aligned}
 H_{9,18} &= \begin{pmatrix} 100001000013231002 \\ 013000003100100321 \\ 000100001022331001 \\ 000010000132211003 \\ 000001103000111032 \\ 000000133101310003 \\ \hline 001003300110031003 \\ 001100003101300110 \\ 000010110200012310 \end{pmatrix}, H_{9,21} = \begin{pmatrix} 100000000122010220022 \\ 010130000003002010333 \\ 001023100300000031031 \\ 000100122000302300012 \\ \hline 000010110000003103313 \\ 000001001302010303012 \\ 000000100130201030213 \\ 000000012201202020022 \\ 000000001220122202200 \end{pmatrix}, \\
 H_{10,20} &= \begin{pmatrix} 10000003000013100331 \\ 01000020210100002021 \\ 00100311300300000031 \\ 00010031310030000013 \\ 00001003131003000013 \\ \hline 00000100200010220211 \\ 00000011200212002100 \\ 00000001011331003003 \\ 13030010010130000030 \\ 01303300000010300101 \end{pmatrix}, H_{11,22} = \begin{pmatrix} 1000302030001000020011 \\ 0010003100010000003313 \\ 0120002100100200000031 \\ 0100023030000001003021 \\ 1002003000003010002033 \\ \hline 1020310000300000200032 \\ 0001202000230003302000 \\ 0000101000303023100020 \\ 0000000303103000131010 \\ 0000001031100200001201 \\ \hline 1000000000230331010001 \end{pmatrix} \quad (8)
 \end{aligned}$$

四元距离最优LRC的构造结果：码长 $n \leq 20$ 的距离最优码共210个，除 $[n, n, 1]$ 码外的190个距离最优码具有局部修复功能，其中 $d = 2$ 的码共34个且达到S-L界。表1给出剩下的156个LRC $[n, k, d; r]$ ，达到S-L界的67个LRC用蓝色表示；达到C-M界的75个LRC用黑色表示；红色表示12个达不到S-L界和C-M界且非 r -最优的LRC； $[7, 2, 5; 2]$ 和 $[9, 2, 7; 2]$ 达不到S-L界和C-M界，但它们仍是 r -最优的。经查阅已有文献，这些构造结果包含了文献[15]

中参数为 $[7, 4, 3; 3]$ 的四元LRC，以及文献[17]中的16个 $d = 3$ 和12个 $d = 4$ 的四元LRC，具体参数为 $[17 - s, 13 - s, 4; 11 - s] (0 \leq s \leq 5)$ ， $[12 - j, 8 - j, 4; 6 - 3i - t] (j = 4i + t, 0 \leq t \leq 3, 0 \leq i \leq 1)$ 及 $[21 - s, 18 - s, 3; 15 - s] (1 \leq s \leq 9)$ 和 $[12 - j, 9 - j, 3; 6 - 2i - t] (1 \leq j = 3i + t \leq 4, 0 \leq t \leq 2, 0 \leq i \leq 2)$ 。此外，还包含文献[18]中参数为 $[2, 1, 2; 1]$ ， $[4, 1, 4; 1]$ ， $[4, 3, 2; 3]$ ， $[3, 2, 2; 2]$ ， $[5, 4, 2; 4]$ 的5个四元LRC。

$$H_{12,23} = \begin{pmatrix} 10320000200000200000213 \\ 00000000011013003000133 \\ 00000303300000300200112 \\ 00000120003000032000111 \\ 01000002000002000033221 \\ 01202300000020000000231 \\ 00000030200320000010112 \\ \hline 00130000000002010013110 \\ 00010033000003301001010 \\ 00003003000003001230210 \\ 00000000330213300010010 \\ 10001000200300001030220 \end{pmatrix},$$

$$H_{12,27} = \begin{pmatrix} 10000000000000010312031033323 \\ 01000000000000320300332022221 \\ 000000100000233002030112321 \\ 001203002002022000200003212 \\ 010100000300013130003003131 \\ 102003320300000020020003331 \\ 000130300001200000002222112 \\ 103202100020000302000003113 \\ \hline 000001000000302213132020130 \\ 000000001000200302122230233 \\ 000000000100321301323300130 \\ 000000000010002130132333013 \end{pmatrix} \quad (9)$$

4 结束语

本文研究了四元域上局部度较小的短码长LRC的构造,通过分析四元距离最优码的码长和维

数,首先利用其生成阵或校验阵构造少量参数优良的LRC,然后删除或并置已有矩阵得到新LRC的生成阵或校验阵,最后利用S-L界或C-M界判断

表1 $d \geq 3, n \leq 20$ 时四元LRC的结果

n/k	1	2	3	4	5	6	7	8	9
3	3(1)								
4	4(1)	3(2)							
5	5(1)	4(2)	3(3)						
6	6(1)	4(1)	4(3)						
7	7(1)	5(2)	4(2)	3(3)					
8	8(1)	6(1)	5(2)	4(3)	3(4)				
9	9(1)	7(2)	6(2)	5(3)	4(4)	3(4)			
10	10(1)	8(1)	6(1)	6(3)	5(4)	4(5)	3(5)		
11	11(1)	8(1)	7(2)	6(3)	6(4)	5(5)	4(6)	3(6)	
12	12(1)	9(1)	8(1)	7(3)	6(3)	6(5)	4(3)	4(6)	3(6)
13	13(1)	10(1)	9(2)	8(3)	7(3)	6(4)	5(4)	4(4)	4(7)
14	14(1)	11(1)	10(2)	9(3)	8(3)	7(4)	6(4)	5(5)	4(4)
15	15(1)	12(1)	11(2)	10(3)	8(3)	8(4)	7(5)	6(5)	5(5)
16	16(1)	12(1)	12(2)	11(3)	9(3)	8(4)	8(5)	7(6)	6(5)
17	17(1)	13(1)	12(2)	12(3)	10(3)	9(4)	8(5)	8(6)	7(7)
18	18(1)	14(1)	13(2)	12(3)	10(2)	10(4)	9(5)	8(5)	8(7)
19	19(1)	15(1)	14(2)	12(2)	11(3)	10(3)	9(5)	8(5)	8(6)
20	20(1)	16(1)	15(2)	13(2)	12(3)	11(3)	10(5)	9(4)	8(5)
n/k	10	11	12	13	14	15	16	17	
13	3(7)								
14	4(8)	3(8)							
15	4(4)	4(9)	3(9)						
16	5(6)	4(5)	4(10)	3(10)					
17	6(6)	5(7)	4(5)	4(11)	3(11)				
18	6(6)	6(6)	5(8)	4(5)	3(7)	3(12)			
19	7(6)	6(7)	6(7)	5(9)	4(6)	3(8)	3(13)		
20	8(7)	7(7)	6(7)	6(7)	5(10)	4(7)	3(9)	3(14)	

LRC的局部度最优性。与文献[15,17,18]比较,本文构造的四元LRC都是距离最优码且其结果更具有一般性,这对研究四元域上其他LRC的构造有很好的借鉴意义。在未来的工作中,将进一步研究四元域上码长和维数均较大时最优LRC的新构造。

参 考 文 献

- [1] WEATHERSPOON H and KUBIATOWICZ J D. Erasure coding vs. replication: A quantitative comparison[C]. The 1st International Workshop on Peer-to-Peer Systems, Cambridge, UK, 2002: 328–337. doi: [10.1007/3-540-45748-8_31](https://doi.org/10.1007/3-540-45748-8_31).
- [2] HUANG Cheng, SIMITCI H, XU Yikang, *et al.* Erasure coding in windows azure storage[C]. 2012 USENIX Annual Technical Conference, Boston, USA, 2012: 15–26.
- [3] BALAJI S B, KRISHNAN M N, VAJHA M, *et al.* Erasure coding for distributed storage: An overview[J]. *Science China Information Sciences*, 2018, 61(10): 100301. doi: [10.1007/s11432-018-9482-6](https://doi.org/10.1007/s11432-018-9482-6).
- [4] GOPALAN P, HUANG Cheng, SIMITCI H, *et al.* On the locality of codeword symbols[J]. *IEEE Transactions on Information Theory*, 2012, 58(11): 6925–6934. doi: [10.1109/TIT.2012.2208937](https://doi.org/10.1109/TIT.2012.2208937).
- [5] PAPAILIOPOULOS D S and DIMAKIS A G. Locally repairable codes[C]. 2012 IEEE International Symposium on Information Theory, Cambridge, USA, 2012: 2771–2775. doi: [10.1109/ISIT.2012.6284027](https://doi.org/10.1109/ISIT.2012.6284027).
- [6] CADAMBE V and MAZUMDAR A. An upper bound on the size of locally recoverable codes[C]. 2013 International Symposium on Network Coding, Calgary, Canada, 2013: 1–5. doi: [10.1109/NetCod.2013.6570829](https://doi.org/10.1109/NetCod.2013.6570829).
- [7] GOPARAJU S and CALDERBANK R. Binary cyclic codes that are locally repairable[C]. 2014 International Symposium on Information Theory, Honolulu, USA, 2014: 676–680. doi: [10.1109/ISIT.2014.6874918](https://doi.org/10.1109/ISIT.2014.6874918).
- [8] HAO Jie, XIA Shutao, and CHEN Bin. Some results on optimal locally repairable codes[C]. 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona, Spain, 2016: 440–444. doi: [10.1109/ISIT.2016.7541337](https://doi.org/10.1109/ISIT.2016.7541337).
- [9] HAO Jie and XIA Shutao. Bounds and constructions of locally repairable codes: Parity-check matrix approach[EB/OL]. <https://arxiv.org/abs/1601.05595v1>, 2019.
- [10] FU Qiang, LI Ruihu, GUO Luobin, *et al.* Locality of optimal binary codes[J]. *Finite Fields and Their Applications*, 2017, 48: 371–394. doi: [10.1016/j.ffa.2017.08.013](https://doi.org/10.1016/j.ffa.2017.08.013).
- [11] 杨森, 李瑞虎, 付强, 等. 二元局部修复码的新构造[J]. 空军工程大学学报: 自然科学版, 2019, 20(6): 104–108.
YANG Sen, LI Ruihu, FU Qiang, *et al.* The new Constructions of binary locally repairable codes[J]. *Journal of Air Force Engineering University: Natural Science Edition*, 2019, 20(6): 104–108.
- [12] HAO Jie, XIA Shutao, and CHEN Bin. On optimal ternary locally repairable codes[C]. 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 2017: 171–175. doi: [10.1109/ISIT.2017.8006512](https://doi.org/10.1109/ISIT.2017.8006512).
- [13] YANG Ruipan, LI Ruihu, GUO Luobin, *et al.* Locality of some optimal ternary linear codes[J]. *Procedia Computer Science*, 2017, 107: 164–169. doi: [10.1016/j.procs.2017.03.073](https://doi.org/10.1016/j.procs.2017.03.073).
- [14] WESTERBACK T, ERNVALL T, and HOLLANTI C. Almost affine locally repairable codes and matroid theory[C]. 2014 IEEE Information Theory Workshop, Hobart, Australia, 2014: 621–625. doi: [10.1109/ITW.2014.6970906](https://doi.org/10.1109/ITW.2014.6970906).
- [15] ERNVALL T, WESTERBÄCK T, and HOLLANTI C. Constructions of optimal and almost optimal locally repairable codes[C]. The 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), Aalborg, Denmark, 2014: 1–5. doi: [10.1109/VITAE.2014.6934442](https://doi.org/10.1109/VITAE.2014.6934442).
- [16] BARG A, HAYMAKER K, HOWE E W, *et al.* Locally Recoverable Codes from Algebraic Curves and Surfaces[M]. HOWE E W, LAUTER K E, and WALKER J L. Algebraic Geometry for Coding Theory and Cryptography. Cham: Springer, 2016, 95–127. doi: [10.1007/978-3-319-63931-4_4](https://doi.org/10.1007/978-3-319-63931-4_4).
- [17] FU Qiang, LI Ruihu, GUO Luobin, *et al.* Singleton-type optimal LRCs with minimum distance 3 and 4 from projective code[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer*, 2021, E104-A(1): 319–323. doi: [10.1587/transfun.2019eal2158](https://doi.org/10.1587/transfun.2019eal2158).
- [18] JIN Lingfei, MA Liming, and XING Chaoping. Construction of optimal locally repairable codes via automorphism groups of rational function fields[J]. *IEEE Transactions on Information Theory*, 2020, 66(1): 210–221. doi: [10.1109/TIT.2019.2946637](https://doi.org/10.1109/TIT.2019.2946637).
- [19] PLANK J, GREENAN K, and MILLER E. Screaming fast Galois field arithmetic using Intel SIMD instructions[C]. The 11th USENIX Conference on File and Storage Technologies, San Jose, USA, 2013: 299–306.

- [20] 吴昭军, 张立民, 钟兆根, 等. 一种软判决下的RS码识别算法[J]. 电子与信息学报, 2020, 42(9): 2150–2157. doi: [10.11999/JEIT190690](https://doi.org/10.11999/JEIT190690).
- WU Zhaojun, ZHANG Limin, ZHONG Zhaogen, *et al.* Blind recognition of RS codes based on soft decision[J]. *Journal of Electronics & Information Technology*, 2020, 42(9): 2150–2157. doi: [10.11999/JEIT190690](https://doi.org/10.11999/JEIT190690).
- [21] FEULNER T. Classification and nonexistence results for linear codes with prescribed minimum distances[J]. *Designs, Codes and Cryptography*, 2014, 70(1): 127–138. doi: [10.1007/s10623-012-9700-8](https://doi.org/10.1007/s10623-012-9700-8).
- [22] GRASSL M. Bounds on the minimum distance of linear codes[EB/OL]. <http://www.codetables.de>, 2020.
- [23] BOUYUKLIEV I, GRASSL M, and VARBANOV Z. New bounds for and classification of some optimal codes over[J]. *Discrete Mathematics*, 2004, 281(1/3): 43–66. doi: [10.1016/j.disc.2003.11.003](https://doi.org/10.1016/j.disc.2003.11.003).
- 李瑞虎: 男, 1966年生, 教授, 博士生导师, 主要研究方向为群论、图论、编码和密码学.
- 展秀珍: 女, 1995年生, 硕士生, 研究方向为大数据存储编码.
- 付强: 男, 1989年生, 讲师, 博士, 研究方向为射影几何、经典编码与量子纠错码.
- 张茂: 男, 1996年生, 硕士, 研究方向为编码理论.
- 郑尤良: 男, 1996年生, 硕士, 研究方向为分布式存储编码和纠错码.
- 责任编辑: 马秀强