基于循环码的三元局部修复码构造

郑尤良，李瑞虎，吕京杰，张　茂
(空军工程大学基础部，西安，710051)

摘要　局部修复码(Locally Repairable Codes)是一种能为分布式存储系统提供信息修复能力的新型纠删码。针对目前三元域上局部修复码的研究尚不充分的情况，给出了利用循环码构造局部修复码的一般方法。首先从循环码的码长出发，计算出对应的3－分圆陪集，然后通过分圆陪集的组合确定各循环码的定义集从而确定码的距离和局部度，进而构造了码长$8\leqslant n\leqslant 50$范围内达到Cadambe-Mazumdar(C-M)界的三元局部修复码。特别是通过定义集设计对偶距离，并利用BCH界筛选分圆陪集，构造了3种具有小局部度的最优局部修复码。这些研究结果进一步完善了三元局部修复码的相关构造理论。

关键词　局部修复码；三元域；C-M界；循环码；定义集
DOI　10.3969/j.issn.1009-3516.2020.04.017
中图分类号　O157.4　　**文献标志码**　A　　**文章编号**　1009-3516(2020)04-0108-04

Constructions of Ternary Locally Repairable Codes Based on Cyclic Code

ZHENG Youliang, LI Ruihu, LYU Jingjie, ZHANG Mao
(Department of Basic Sciences, Air Force Engineering University, Xi'an 710051, China)

Abstract　Locally repairable codes are a kind of new erasure codes capable of providing information repair ability for distributed storage systems. Aimed at the problem that the researches on the locally repairable codes are still insufficient in ternary field at present, a general method of constructing locally repairable codes based on cyclic codes is presented. Firstly, proceeded from the code length of cyclic codes, the corresponding 3-cyclotomic cosets are calculated, and then the defining sets of each cyclic codes are determined through the combinations of cyclotomic cosets, thus determining the distance and locality of codes, and constructing the three kinds locally repairable codes reaching Cadambe-Mazumdar (C-M) bound with $8\leqslant n\leqslant 50$. Particularly, three kinds of optimal locally repairable codes with small locality are constructed by designing the dual distance through defining sets and by using BCH boundary to filter the circular coset. The relevant construction theory of ternary locally repairable codes is further being perfected by these research results.

Key words　locally repairable codes; ternary field; C-M bound; cyclic code; defining set

随着大数据时代的到来，世界上的数据量急剧　　增长，对存储系统的要求也逐步提高。分布式存储

收稿日期：2020-01-16
基金项目：国家自然科学基金(11901579)
作者简介：郑尤良(1996—)，男，江西九江人，硕士生，主要从事存储编码及其应用研究。E-mail:zxy951783247@163.com
通信作者：李瑞虎(1966—)，男，安徽亳州人，教授，博士生导师，主要从事量子信息与编码、代数编码与密码研究。E-mail:llzsy110@163.com

引用格式：郑尤良，李瑞虎，吕京杰，等．基于循环码的三元局部修复码构造[J]．空军工程大学学报(自然科学版)，2020，21(4)：108-111.
ZHENG Youliang, LI Ruihu, LYU Jingjie, et al. Constructions of Ternary Locally Repairable Codes Based on Cyclic Code[J]. Journal of Air Force Engineering University (Natural Science Edition), 2020, 21(4): 108-111.

系统由于采用了可扩展结构，提高了系统的可用性和存储效率，因此得到了广泛应用。为了提高分布式存储系统的容错能力，2012 年 Gopalan 提出了局部修复码的概念[1]。局部修复码是一类特殊的纠删码，其码字的任一信息位发生错误时都可通过访问其它不超过 r 个信息位进行恢复，r 被称为码的局部修复度(Locality)[2]。此后，Cadambe 和 Mazumdar 提出了一个考虑域 q 大小的局部修复码的参数上界，即 C-M 界[3]。设 $C=[n,k,d]_q$，若其局部修复度为 r，则：

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

式中：$k_{opt}^q(n,d)$ 是码长为 n，距离为 d，q 元码的最大维数。本文以达到 C-M 界的三元码为最优局部修复码。

定义 1[4] 码长为 n 的 q 元线性码 C 叫作循环码，是指若 $c=(c_0,c_1,\cdots,c_{n-1})\in C$，则 c 的循环移位 $(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$。

引理 1[5] 令循环码 $C=[n,k,d]$，D 为 C 的对偶码。若 D 的最小距离为 $d^\perp$，则 C 的局部修复度 $r=d^\perp-1$。

循环码由于其所具有的特殊结构，能够更好地设计和分析码的局部度，因此近年来关于循环码的局部度问题研究日益增多。Zeh 等人在 2015 年利用循环码生成了部分局部度 $r=2$ 的码[6]。Kim 等人通过分析二、三元域上的循环码，得到了一些距离大于 4 的局部修复码[7]。文献[8～9]中考虑通过常循环码来构造局部修复码。饶驿等给出了二元域上循环码构造具有 2、3 局部度的码的构造方法[10]。夏易冲与陈斌讨论了局部度为 1、$k-1$ 时码的特征[11]。杨瑞磊分析了一些有关三元本原长度码长的循环码的局部度[12]。本文主要利用循环码构造了码长 $8\leqslant n\leqslant 50$ 范围内达到 C-M 界的三元局部修复码，并着重讨论其中具有小局部度的码。这些码的研究对局部修复码在分布式存储系统上的应用具有重要的促进意义。

1　预备知识

令 $F_3=\{0,1,2\}$，F_3 上的码长为 n，维数为 k，最小距离为 d 的线性码 C 记作 $[n,k,d]$，若码的局部度为 r，则记为 $[n,k,d;r]$。

设 Z_n 表示模 n 整数环，本文研究的循环码的码长满足 $\gcd(n,3)=1$。令循环码 $C=[n,k,d]$，当码字写成多项式形式时，取 $g(x)$ 为 x^n-1 在 $F_q[x]$ 中的首一因式，则 C 为环 $R_n=F_q[x]/(x^n-1)$ 中由 $g(x)$ 生成的理想，并称 $g(x)$ 为 C 的生成多项式，$x^n-1/g(x)$ 为 C 的校验多项式[4]。

定义 2[4] 若 x 为整数且满足 $0\leqslant x\leqslant n$，x 模 n 的 3－分圆陪集 C_x 定义为：

$$C_x=\{x,3x,3^2x,\cdots,3^{l-1}x\}(\mathrm{mod}\ n) \quad (2)$$

式中：l 是满足 $xq^l\equiv x(\mathrm{mod}\ n)$ 的最小正整数，集合 C_x 中的最小元素称为代表元。

令 α 为 F_3 的某个扩域中的 n 次本原单位根，C_i $(1\leqslant i\leqslant s)$为模 n 的 3－分圆陪集。x^n-1 可分解为 $p_1(x)p_2(x)\cdots p_s(x)$，且 $p_i(x)=\prod_{j\in C_i}(x-a^j)$。$g(x)$ 由部分 $p_1(x),p_2(x),\cdots,p_s(x)$ 的乘积构成，其零点的幂指数构成的集合对应于不同分圆陪集的并集，称为 C 的定义集 T。设 D 为 C 的对偶码，若 C 的定义集为 T_C，则 D 的定义集 $T_D=Z_n/{T_C}^{-1}$[13-14]。

引理 2[13] (BCH 界)令循环码 $C=[n,k,d]$，若 C 的定义集 T 中存在 δ 长度的连续元素，则码的距离 $d\geqslant\delta+1$。

2　三元循环最优局部修复码的构造

为构造达到界的最优局部修复码，首先需计算出相应码长的 3－分圆陪集，通过分圆陪集的组合可以确定码的定义集从而确定循环码，最后通过分析该码及其对偶码，即可得到参数为 $[n,k,d;d^\perp-1]$ 以及 $[n,n-k,d^\perp;d-1]$ 的局部修复码。

相对而言，局部度越小，码的修复效率越高[15]，因此构造小局部度的码更有实用价值。根据引理 1，为构造局部度为 r 的码，对偶距离 $d^\perp=r+1$，再参考 BCH 界，确定对偶码的定义集 T_D 中连续整数的个数范围，即可有针对性地构造局部修复码。本文重点构造了局部度为 1、2、3 的 3 类小局部度的码，各对偶码定义集中的连续整数个数应不大于局部度 r。

定理 1　对于三元循环码 $C=[n,k,d]$，若码长 n 为偶数且满足 $\gcd(n,3)=1$，则当 $n\geqslant 8$ 时存在以下 2 种局部度 $r=1$ 的最优局部修复码：

$$\left[n,\frac{n}{2},2;1\right];$$

$$\left[n,\frac{n}{2}-1,4;1\right]$$

证明：根据分圆陪集的定义，易知当码长 n 为偶数且满足 $\gcd(n,3)=1$ 时，分圆陪集可区分为数个奇数元素集合与数个偶数元素集合。由于 n 为偶数，根据 $\frac{n}{2}\times 3-n=\frac{n}{2}$，可以得出 $\frac{n}{2}$ 所在集合为

单元素分圆陪集。下面对 2 种码的存在性进行证明：

1)设 $m=\frac{n}{2}(m\geqslant 4)$，当对偶码定义集取奇数或者偶数元素全集时，$x^n-1=x^{2m}-1=(x^m-1)\cdot(x^m+1)$，$(x^m+1)$ 及 (x^m-1) 分别对应定义集为奇数以及偶数元素全集的生成多项式，易知 $d=2$ 且 $d^{\perp}=2$，即可构造参数为 $[n,\frac{n}{2},2;1]$ 的局部修复码；

2)根据 $\frac{n}{2}$ 的奇偶性分别进行讨论。当 $\frac{n}{2}$ 为奇数时，设 $\frac{n}{2}=2m+1(m\geqslant 2)$，此时对偶码定义集取除 $\frac{n}{2}$ 以外的奇数元素，$x^n-1=x^{4m+2}-1=\frac{(x^{2m+1}+1)}{x+1}(x^{2m+1}-1)(x+1)$，易知 $\frac{(x^{2m+1}+1)}{x+1}=x^{2m}-x^{2m-1}+x^{2m-2}-\cdots+x^2-x+1$ 为循环码的校验多项式，$(x^{2m+1}-1)(x+1)=x^{2m+2}+x^{2m+1}-x-1$ 为循环码的生成多项式，可得 $d^{\perp}=2$ 且 $d=4$，即可构造参数为 $[4m+2,2m,4;1](m\geqslant 2)$ 的局部修复码；当 $\frac{n}{2}$ 为偶数时，设 $\frac{n}{2}=2m(m\geqslant 2)$，此时对偶码定义集取除 $\frac{n}{2}$ 以外的偶数元素，同理可得 $d^{\perp}=2$ 且 $d=4$，即可构造参数为 $[4m,2m-1,4;1](m\geqslant 2)$ 的局部修复码。综上，可构造参数为 $[n,\frac{n}{2}-1,4;1](n\geqslant 8)$ 的码。将 2 种码的参数分别代入 C-M 界公式中，经计算取 $t=k-1$ 时达到码界，为最优局部修复码。证毕。

3 三元循环最优局部修复码

本节主要构造了码长 $8\leqslant n\leqslant 50$ 范围内局部度 $r\leqslant 3$ 的最优局部修复码，并通过对偶码定义集给出了具体的构造方法，同时也给出了其余达到 C-M 界的局部修复码。以下各表中带 * 号的码为前人用其他方法构造的局部修复码，由于循环码相较一般码在应用中更具优势，所以仍在此给出。参数为[16,3,10;1]、[8,3,5;2]、[13,4,7;2]、[26,4,17;2]、[13,6,6;3]、[40,6,24;3]的码已于文献[12]中得到。

3.1 $r=1$ 的最优局部修复码

当对偶码定义集中无连续整数时，可以构造对偶距离 $d^{\perp}=2$ 的码，在码长 $8\leqslant n\leqslant 50$ 范围内共得到 39 个最优局部修复码，其中满足定理 1 的码长有 15 种，见表 1。

表 1 $r=1$ 的最优局部修复码

序号	码长	对偶码定义集 T	*LRCs*
1	8	1	[8,2,6;1]*
2	8	1,5	[8,4,2;1]
3	8	0,2	[8,3,4;1]
4	10	1,5	[10,5,2;1]
5	10	1	[10,4,4;1]
6	14	1	[14,6,4;1]
7	14	0,2	[14,7,2;1]
8	16	0,2	[16,3,10;1]*
9	16	2,4	[16,4,8;1]
10	16	1,5	[16,8,2;1]
11	16	0,2,4,10	[16,7,4;1]
12	20	1	[20,4,12;1]*
13	20	2,4,10	[20,9,4;1]
14	20	1,5,11	[20,10,2;1]
15	22	1,11	[22,6,10;1]
16	22	0,2,4	[22,11,2;1]
17	22	1,7	[22,10,4;1]
18	26	1	[26,3,18;1]*
19	26	0,2,4,8,14	[26,13,2;1]
20	26	1,5,7,17	[26,12,4;1]
21	28	2,4,14	[28,13,4;1]
22	28	1,5,7	[28,14,2;1]
23	32	4	[32,2,24;1]
24	32	1,5	[32,16,2;1]
25	32	2,4,8,10,16,20	[32,15,4;1]
26	34	1	[34,16,4;1]
27	34	0,2	[34,17,2;1]
28	38	1	[38,18,4;1]
29	38	0,2	[38,19,2;1]
30	40	5	[40,2,30;1]
31	40	1,5,7,11,13,25	[40,20,2;1]
32	40	0,2,4,8,10,22	[40,19,4;1]
33	44	1,7,11	[44,22,2;1]
34	44	2,4,8,14,22	[40,21,4;1]
35	46	0,23	[46,12,23;1]
36	46	1,5	[46,22,4;1]
37	46	0,2,10	[46,23,2;1]
38	50	1,5	[50,24,4;1]
39	50	0,2,10	[50,25,2;1]

3.2 $r=2$ 的最优局部修复码

当对偶码定义集中的连续整数个数不大于 2 时，可以构造对偶距离 $d^{\perp}=3$ 的码，进而构造了 5 个 $r=2$ 的最优局部修复码，见表 2。

表 2 $r=2$ 的最优局部修复码

序号	码长	对偶码定义集 T	*LRCs*
1	8	0,1	[8,3,5;2]*
2	13	0,1	[13,4,7;2]*
3	13	1,3	[13,3,9;2]*
4	26	0,1	[26,4,17;2]*
5	40	0,1,25	[40,7,18;2]

3.3 $r=3$ 的最优局部修复码

当对偶码定义集中的连续整数个数不大于 3

时，可以构造对偶距离 $d^{\perp}=4$ 的码，进而构造了 15 个 $r=3$ 的最优局部修复码，见表 3。

表 3　$r=3$ 的最优局部修复码

序号	码长	对偶码定义集 T	*LRCs*
1	8	1,2	[8,4,4;3]*
2	8	1,2,5	[8,6,2;3]
3	10	0,1	[10,5,4;3]
4	13	1,7	[13,6,6;3]
5	20	0,1	[20,5,11;3]
6	20	1,4	[20,8,8;3]
7	20	0,10,11	[20,6,10;3]*
8	22	2,11	[22,6,12;3]*
9	26	1,2	[26,6,15;3]*
10	28	1,4,5,7	[28,20,2;3]
11	28	4,5,7	[28,14,8;3]
12	28	1,2,5,14	[28,19,4;3]
13	32	1,4,5,8,16,20	[32,23,2;3]
14	32	0,1,4,5,8,16,20	[32,24,2;3]
15	40	2,25	[40,6,24;3]*

3.4　$r\geqslant 4$ 的最优局部修复码

除了 $r\leqslant 3$ 的码以外，还得到了以下 30 个最优局部修复码，见表 4。

表 4　$r=4$ 的最优局部修复码

序号	*LRCs*	序号	*LRCs*
1	[8,5,3;4]*	16	[28,24,2;6]
2	[11,6,5;5]*	17	[32,30,2;15]
3	[13,7,5;5]	18	[34,32,2;16]
4	[13,9,3;6]	19	[35,28,2;4]
5	[16,14,2;7]	20	[35,30,2;6]
6	[20,18,2;9]	21	[38,36,2;18]
7	[20,15,4;10]	22	[40,38,2;29]
8	[20,14,4;7]	23	[40,35,3;23]
9	[22,12,7;8]	24	[40,33,4;17]
10	[22,10,9;6]	25	[40,34,4;23]
11	[23,12,8;8]	26	[44,42,2;21]
12	[23,11,9;7]	27	[49,42,2;6]
13	[26,20,4;14]	28	[50,45,2;9]
14	[26,22,3;16]	29	[50,48,2;24]
15	[28,26,2;13]	30	[50,40,2;4]

本节所构造的几类码均达到了目前最为关注的 C-M 界，其中局部度 $r\leqslant 3$ 的码具有较高的修复效率，可进一步考虑其实用价值，局部度 $r\geqslant 4$ 的码则主要是对结果的完善。

4　结语

本文利用定义集合设计三元循环码的对偶距离，构造了码长在 $8\leqslant n\leqslant 50$ 范围内达到 C-M 界的最优局部修复码，尤其是构造了一批具有较大实用价值的小局部度的码。本文的方法与结论为深入研究三元局部修复码提供了依据，今后会进一步研究如何基于拟循环码来构造局部修复码。

参考文献

[1] GOPALAN P, HUANG C, SIMITCI H, et al. On the Locality of Codeword Symbols [J]. IEEE Transactions on Information Theory, 2012, 58 (11): 6925-6934.

[2] RAWAT A, PAPAILIOPOULOS D, DIMAKIS A, et al. Locality and Availability in Distributed Storage [C]//IEEE International Symposium on Information Theory. Piscataway, NY: IEEE, 2014: 681-685.

[3] CADAMBE V, MAZUMDAR A. An Upper Bound on the Size of Locally Recoverable Codes [C]// IEEE International Symposium on Network Coding. Piscataway, NY: IEEE, 2013:1-5.

[4] 冯克勤. 量子纠错码 [M]. 北京：科学出版社，2010.

[5] HUANG P, YAAKOBI E, UCHIKA H, et al. Binary Linear Locally Repairable Codes [J]. IEEE Transactions on Information Theory, 2016, 62 (11): 6268-6283.

[6] ZEH A, YAAKOBI E. Optimal Linear and Cyclic Locally Repairable Codes over Small Fields [C]// IEEE Information Theory Workshop. Piscataway, NY: IEEE, 2015:1-5.

[7] KIM C, SEON J. New Constructions of Binary and Ternary Locally Repairable Codes Using Cyclic Codes [J]. IEEE Communications Letters, 2015, 2 (22): 228-231.

[8] SUN Z, ZHU S, WANG L. Optimal Constacyclic Locally Repairable Codes [J]. IEEE Communications Letters, 2018, 23(2): 206-209.

[9] CHEN B, FANG W J, XIA S T, et al. Constructions of Optimal Locally Repairable Codes via Constacyclic Codes [J]. IEEE Transactions on Communications, 2019, 67(8): 5253-5263.

[10] 饶驿，李瑞虎，付强，等. 短码长二元循环码的局部修复度 [J]. 空军工程大学学报(自然科学版)，2017，18 (2): 106-110.

[11] XIA Y C, CHEN B. Complete Characterizations of Optimal Locally Repairable Codes with Locality 1 and $k-1$[J]. IEEE Access, 2019(7): 111271-111276.

[12] 杨瑞硒. 三元码的局部修复度研究 [D]. 西安：空军工程大学，2017.

[13] HUFFMAN W, PLESS V. Fundamentals of Error-Correcting Codes [M]. Cambridge: Cambridge University Press, 2003.

[14] HUFFMAN W, WELDON E. Error Correcting Codes [M]. Cambridge: MIT Press, 1996: 493-534.

[15] GOPRAJU S, CALDERBANK R. Binary Cyclic Codes that are Locally Repairable [C]// IEEE International Symposium on Information Theory. Piscataway, NY: IEEE, 2014: 676-680.

（编辑：陈斐）