

# 域 $F_2$ 上的三次剩余码

朱士信<sup>1</sup>, 陈安顺<sup>2</sup>

(1. 合肥工业大学数学系, 安徽合肥 230009; 2. 滁州学院, 安徽滁州 239012)

**摘要:** 对于某个奇素数  $p$ , 我们给出了判断 2 是  $\text{mod } p$  的三次剩余的一个引理, 由此引理, 我们定义了有限域  $F_2$  上的 6 种三次剩余码; 研究了 6 种三次剩余码之间的关系, 得出了三次剩余码的码长、重量特征和极小汉明距离范围; 最后给出了三次剩余码的对偶码的生成多项式, 以及在选择适当的  $p$  次本原单位根的情况下, 给出了它的生成幂等多项式.

**关键词:** 三次剩余码; 生成幂等多项式; 对偶码

**中图分类号:** TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2008) 12-2312-03

## Cubic Residue Codes over the Field $F_2$

ZHU Shi-xin<sup>1</sup>, CHEN An-shun<sup>2</sup>

(1. Department of Mathematics, Hefei University of Technology, Hefei, Anhui 230009, China;

2. Chuzhou University, Chuzhou, Anhui 239012, China)

**Abstract:** For any odd prime  $p$ , we give a lemma which is determined when 2 is a cubic residue modulo  $p$ . Using it, we define the notion of six cubic residue codes over  $F_2$ . We discuss the relations between six codes, and study the length of cubic-residue codes, character of weight and the bound of the minimum Hamming distance. We finally give the generator polynomials of dual codes, and the generating idempotents of cubic residue code when choose the appropriate primitive  $p$  root of unity.

**Key words:** cubic residue codes; generating idempotenes; dual codes

### 1 引言

域  $F_2$  上的二次剩余码是一类非常古老的码, 人们对它的研究已经有三十多年了, 它是一类好码, 并在实际中得到了广泛应用. 在文献[1]第 16 章中, 定义了域  $F_2$  上的二次剩余码, 研究了它的性质, 讨论了四种二次剩余码之间的关系, 给出了四种码的生成幂等多项式. 文献[4~9]也是对二次剩余码的相应研究. 我们知道: 域  $F_2$  上的二次剩余码的码长为奇素数  $p$  且  $p$  满足  $p \equiv \pm 1 \pmod{8}$ . 本文由文献[2]中的结论出发, 先给出了域  $F_2$  上的三次剩余码定义, 在此基础上探讨了六种三次剩余码之间的关系, 研究了它的相关性质, 最后给出了一个三次剩余码的生成幂等多项式.

### 2 域 $F_2$ 上的三次剩余码

**引理 1** 设存在整数  $A, B$ , 且  $A$  不被 3 整除,  $p$  为一素数, 若  $p$  满足  $p = A^2 + 27B^2$ , 则关于  $x$  的方程  $x^3 \equiv 2 \pmod{p}$  有解.

证明可以参照文献[2]中 Proposition 9.6.2 的证明.

显然, 在引理 1 中, 由于  $A$  不被 3 整除, 则必有  $3 \mid (p - 1)$ , 对于引理 1 中的素数  $p$  而言: 2 是  $\text{mod } p$  的三次剩

余.

本文规定: 文中所提及的素数  $p$  皆满足引理 1 中的条件. 如  $p$  可以等于 31, 43 等等. 下面介绍  $F_2$  上三次剩余码的定义.

设  $\rho$  为有限域  $F_p$  的本原元, 令  $R_0$  为所有  $\text{mod } p$  的三次剩余组成的集, 即  $R_0 = \{\rho^{3k} \in F_p \mid k \in Z\}$ , 又令  $R_1 = \{\rho^{3k+1} \in F_p \mid k \in Z\}$ ,  $R_2 = \{\rho^{3k+2} \in F_p \mid k \in Z\}$  (其中  $Z$  表示整数集).

设  $n$  是使  $2^n \equiv 1 \pmod{p}$  成立的最小正整数 (即  $n$  是  $2 \pmod{p}$  的阶),  $\alpha \in F_2^n$  且  $\alpha$  是  $p$  次的本原单位根.

$$\text{令 } g_0(x) = \prod_{r_0 \in R_0} (x - \alpha^{r_0}), g_1(x) = \prod_{r_1 \in R_1} (x - \alpha^{r_1}),$$

$$g_2(x) = \prod_{r_2 \in R_2} (x - \alpha^{r_2}).$$

**命题 1** 若  $p$  满足引理 1 中的条件, 则  $g_0(x), g_1(x), g_2(x) \in F_2[x]$ .

证明: 由于  $p$  满足引理 1 的条件, 我们有  $2 \in R_0$ . 易知,  $2R_0 = R_0, 2R_1 = R_1, 2R_2 = R_2$ .

所以,  $R_0, R_1, R_2$  分别是  $F_2$  上  $\text{mod } p$  的不相连的分圆陪集之并. 即  $g_0(x), g_1(x), g_2(x)$  分别是  $F_2^n$  中某些元的极小多项式的乘积. 由文献[1]的 ch4 § 3 可知:  $g_0(x)$ ,

$g_1(x), g_2(x) \in F_2[x]$ .

定义 1 环  $F_2[x]/(x^p - 1)$  中分别由多项式  $g_0(x), (x-1)g_0(x), g_1(x), (x-1)g_1(x), g_2(x), (x-1)g_2(x)$  生成的循环码(或理想)称为三次剩余码, 分别记为  $C_0, \bar{C}_0, C_1, \bar{C}_1, C_2, \bar{C}_2$ .

显然由此定义和命题 1 可知循环码  $C_0, \bar{C}_0, C_1, \bar{C}_1, C_2, \bar{C}_2$  是  $F_2$  上的码.

定义 2 设  $0 < j < p$ , 记  $j^{-1}$  为  $j$  在  $F_p$  中的逆元(关于乘法), 定义映射

$$\pi_j: i \rightarrow \bar{i}, i = 0, 1, \dots, p-1$$

将此定义延伸到环  $F_2[x]/(x^p - 1)$  上, 有:

$$\pi_j: F_2[x]/(x^p - 1) \rightarrow F_2[x]/(x^p - 1)$$

$$f(x) = a_0 + \sum_{i=1}^{p-1} a_i x^i \rightarrow \pi_j(f(x)) = a_0 + \sum_{i=1}^{p-1} a_i x^{\bar{i}}$$

显然,  $\pi_j(f(x)) = a_0 + \sum_{i=1}^{p-1} a_i x^{\bar{i}} = f(x^{j^{-1}})$ .

因此, 由上可得到:

命题 2  $\alpha$  是  $g_k(x), (k = 0, 1, 2)$  的根当且仅当  $\bar{\alpha}$  是  $g_k(x^{j^{-1}})$  的根, 且  $\deg g_k(x) = \deg g_k(x^{j^{-1}})$ .

定理 1 设  $0 < j < p$ , 将  $\pi_j$  对码  $C_0, \bar{C}_0, C_1, \bar{C}_1, C_2, \bar{C}_2$  进行变换, 若  $j \in R_0$ , 则它们在  $\pi_j$  的作用下保持不变; 若  $j \in R_1$ , 则它们分别变换为:  $C_1, \bar{C}_1, C_2, \bar{C}_2, C_0, \bar{C}_0$ ; 若  $j \in R_2$ , 则它们分别变换为:  $C_2, \bar{C}_2, C_0, \bar{C}_0, C_1, \bar{C}_1$ .

证明: 三种情况只证第三种, 其它的证明方法与之相似.

$$A = \begin{pmatrix} -a_0 & a_0 - a_1 & a_1 - a_2 & \dots & a_{m-1} - a_m & a_m & 0 & \dots & 0 \\ 0 & -a_0 & a_0 - a_1 & a_1 - a_2 & \dots & a_{m-1} - a_m & a_m & 0 & \dots & 0 \\ \dots & \dots \\ 0 & \dots & \dots & 0 & -a_0 & a_0 - a_1 & \dots & a_{m-1} - a_m & a_m \end{pmatrix}$$

对于  $A$  中任意两行而言, 易知它们的重量之和为偶数, 再对这两行对应列分三种情况 00, 01, 11 讨论, 可知两行和的重量也为偶数, 定理即证.

(4) 设  $a(x)$  是  $C_0$  中重量为  $d$  的码字, 因为  $d$  是奇数, 所以  $(x-1)$  不能整除  $a(x)$ . 再由定理 1, 若  $j_1 \in R_1, j_2 \in R_2$  则  $\pi_{j_1}(a(x)) \in C_1, \pi_{j_2}(a(x)) \in C_2$ . 显然, 由  $\pi_{j_1}(a(x))$  和  $\pi_{j_2}(a(x))$  分别是  $C_1$  和  $C_2$  中的码字, 可以得到  $a(x) \pi_{j_1}(a(x)) \pi_{j_2}(a(x))$  必然在  $C_0 \cap C_1 \cap C_2$  中且是  $g_0(x)g_1(x)g_2(x) = \prod_{j=0}^{p-1} x^j$  的倍数. 因此  $a(x) \pi_{j_1}(a(x)) \pi_{j_2}(a(x))$  汉明重量为  $p$ , 因为  $a(x) \pi_{j_1}(a(x)) \pi_{j_2}(a(x))$  的非零系数个数最大为  $d^3$ , 所以  $d^3 \geq p$ .

下面我们来研究  $F_2$  上三次剩余码的对偶码. 由文献[1]的第七章可以得到以下引理:

引理 2 设  $g(x)h(x) = x^p - 1$ , 若  $C$  是由  $g(x)$  生

若  $j \in R_2$  设  $\forall r_k \in R_k, (k = 0, 1, 2)$ , 则  $\alpha$  是  $g_k(x)$  的根. 由于  $jr_0 \in R_2, jr_1 \in R_0, jr_2 \in R_1$ , 所以  $\alpha^0, \alpha^1, \alpha^2$  分别是  $g_2(x), g_0(x), g_1(x)$  的根. 即  $\pi_j(g_0(x)) = g_2(x), \pi_j(g_1(x)) = g_0(x), \pi_j(g_2(x)) = g_1(x)$ .

故定理得证.

至此我们可以对三次剩余码给出总结.

定理 2 (1) 码  $C_0, C_1, C_2$  相互等价,  $\bar{C}_0, \bar{C}_1, \bar{C}_2$  也相互等价.

(2) 码  $C_0, C_1, C_2$  都是长为  $p$ 、维数为  $\frac{1}{3}(2p+1)$ ; 而

$\bar{C}_0, \bar{C}_1, \bar{C}_2$  都是长为  $p$ 、维数为  $\frac{1}{3}(2p-2)$  的码.

(3)  $\bar{C}_k, (k = 0, 1, 2)$  是  $C_k$  的子码, 且  $\bar{C}_k$  中的码字重量全为偶数.

(4) 若  $C_k (k = 0, 1, 2)$  的汉明距离为奇数  $d$ , 则  $d \geq \sqrt[p]{p}$ .

证明: (1)(2) 显然. 下证(3)和(4), 只证  $k = 0$  的情况, 其它情况与之相似.  $\bar{C}_0$  是  $C_0$  的子码由定义 1 即知.

由定义 1,  $\bar{C}_0$  由多项式  $(x-1)g_0(x)$  生成, 令  $g_0(x) = a_0 + a_1x + \dots + a_mx^m$ , 其中  $m = \frac{1}{3}(p-1), a_i \in F_2, i = 0, 1, \dots, m$ .

所以  $(x-1)g_0(x) = -a_0 + (a_0 - a_1)x + (a_1 - a_2)x^2 + \dots + (a_{m-1} - a_m)x^m + a_mx^{m+1}$  由上式知  $(x-1)g_0(x)$  对应  $\bar{C}_0$  中的码字重量为偶数.

$\bar{C}_0$  的生成矩阵可以看成是

成的长为  $p$  的循环码, 则  $C$  的对偶码  $C^\perp$  也是循环码, 且生成多项式为:  $g^\perp(x) = x^{\deg h(x)} h(x^{-1})$ .

定理 3 码  $C_0, \bar{C}_0, C_1, \bar{C}_1, C_2, \bar{C}_2$  的对偶码分别为:  $C_0^\perp = \langle (x-1)g_1(x)g_2(x) \rangle, C_0^\perp = \langle g_1(x)g_2(x) \rangle, \bar{C}_1^\perp = \langle (x-1)g_0(x)g_2(x) \rangle, \bar{C}_1^\perp = \langle g_0(x)g_2(x) \rangle, \bar{C}_2^\perp = \langle (x-1)g_0(x)g_1(x) \rangle, \bar{C}_2^\perp = \langle g_0(x)g_1(x) \rangle$ .

证明: 我们只证  $C_2, \bar{C}_2$  的对偶码生成多项式, 而  $C_0, \bar{C}_0, C_1, \bar{C}_1$  与之相仿.

由定义 1 可知: 码  $C_2$  的根为  $\alpha^s (s \in R_2)$ , 码  $\bar{C}_2$  的根为  $\alpha^t (t \in R_2 \cup \{0\})$ . 再由引理 2 有: 码  $C_2^\perp$  的根为  $\alpha^{-u} (u \in R_0 \cup R_1 \cup \{0\})$ , 码  $\bar{C}_2^\perp$  的根为  $\alpha^{-v} (v \in R_0 \cup R_1)$ . 又由于  $-1 \in R_0$  则  $-u \in R_0 \cup R_1 \cup \{0\}, -v \in R_0 \cup R_1$ , 即证码  $C_2^\perp, \bar{C}_2^\perp$  的生成多项式分别为:

$$(x-1)g_0(x)g_1(x), g_0(x)g_1(x).$$

最后来研究  $F_2$  上三次剩余码的生成幂等多项式.

由于  $C_0, C_1, C_2$  相互等价, 而  $\bar{C}_0$  又是由  $C_0$  中的重量为偶数的码字构成, 因此我们只对  $C_0$  的生成幂等多项式进行讨论.

$$\text{令 } e_0(x) = \sum_{r_0 \in R_0} x^{r_0}, e_1(x) = \sum_{r_1 \in R_1} x^{r_1}, e_2(x) = \sum_{r_2 \in R_2} x^{r_2}.$$

于是我们有:

**命题 3**  $e_0(x), e_1(x), e_2(x)$  都是环  $F_2[x]/(x^p -$

$1)$  的幂等多项式, 且  $e_0(x) + e_1(x) + e_2(x) + \sum_{i=0}^{p-1} x^i = 1$ .

**证明:** 根据上文对素数  $p$  的规定, 可知  $2 \in R_0$ , 且  $2R_0 = R_0, 2R_1 = R_1, 2R_2 = R_2$ , 则

$$(e_0(x))^2 = \left( \sum_{r_0 \in R_0} x^{2r_0} \right) = \sum_{r'_0 \in R_0} x^{r'_0} = e_0(x)$$

对于  $e_1(x), e_2(x)$  是幂等多项式的证明与  $e_0(x)$  的证明相仿. 而命题的后一个等式由  $e_0(x), e_1(x), e_2(x)$  的定义即可得到.

**定理 4** 选择适当的  $p$  次本原单位  $\alpha$ , 若  $e_0(\alpha) = 1, e_1(\alpha) = e_2(\alpha) = 0$ , 则  $C_0$  的生成幂等多项式为:  $1 + e_0(x)$ ; 若  $e_1(\alpha) = 1, e_0(\alpha) = e_2(\alpha) = 0$ , 则  $C_0$  的生成幂等多项式为:  $1 + e_1(x)$ ; 若  $e_2(\alpha) = 1, e_0(\alpha) = e_1(\alpha) = 0$ , 则  $C_0$  的生成幂等多项式为:  $1 + e_2(x)$ .

**证明:** 由命题 3 可知:  $e_0(\alpha) + e_1(\alpha) + e_2(\alpha) = 1$

当  $e_0(\alpha) = 1, e_1(\alpha) = e_2(\alpha) = 0$  时, 我们有:

对于  $\forall s \in R_0$  有,  $1 + e_0(\alpha^s) = 1 + e_0(\alpha) = 0$  而对于  $\forall t \in R_1 \cup R_2 \cup \{0\}$ , 有:

若  $t \in R_1, 1 + e_0(\alpha^t) = 1 + e_1(\alpha) = 1$ ; 若  $t \in R_2, 1 + e_0(\alpha^t) = 1 + e_2(\alpha) = 1$ ; 若  $t = 0, 1 + e_0(1) = 1 + \frac{1}{3}(p-1) = 1$  (因为  $\frac{1}{3}(p-1)$  一定是偶数). 即证定理第一部分. 其它证明如上相似. 定理证明结束.

### 3 一个例子

设  $p = 31$ , 我们知道 2 是 mod 31 的三次剩余. 因为 3 是域  $F_{31}$  的一个本原元,  $f(x) = x^5 + x^3 + x^2 + x + 1$  是  $F_2$  上的一个本原多项式, 5 是使  $2^5 \equiv 1 \pmod{31}$  成立的最小整数. 设  $\alpha \in F_{31} = F_2[x]/(f(x))$  是一个 31 次本原的单位根,  $R_0 = \{3^i \in F_{31} | i \in Z\} = \{1, 2, 4, 8, 15, 16, 23, 27, 29, 30\}$ , 由定义 1 设生成多项式为  $g_0(x) = \prod_{r_0 \in R_0} (x - \alpha^{r_0}) = x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$ , 则我们得到一个  $F_2$  上参数为  $[31, 21, d \geq 4]$  的三次剩余码.

**致谢** 感谢审稿人对本文提出修改意见.

### 参考文献:

- [1] MacWilliams F J, Sloane N J A. The Theory of Error Correcting Codes[M]. Amsterdam, the Netherlands: North-Holland, 1977.
- [2] Kenneth Ireland, Michael Rosen. A Classical Introduction to Modern Number Theory, Second Edition[M]. New York: Springer-Verlag, 2003.
- [3] Wan zhe xian. Quaternary Codes[M]. Singapore: World Scientific, 1997.
- [4] Reed S, Yin X. Algebraic decoding of the (32, 16, 8) quadratic residue code[J]. IEEE Trans Info Theory, 1990, 36(4): 876-880.
- [5] Reed I S, Truong T K. Algebraic decoding of the (41, 21, 9) quadratic residue code[J]. IEEE Trans Info Theory, 1992, 38(3): 974-986.
- [6] Higgs R J, Humphreys J F. Decoding the ternary (23, 12, 8) quadratic residue codes[J]. IEEE Trans Info Theory, 1995, 42(3): 129-134.
- [7] Alexis Bonnetcaze. Quaternary quadratic residue codes and unimodular lattices[J]. IEEE Trans Info Theory, 1995, 41(2): 366-377.
- [8] Robin Chapman. Higher power residue codes[J]. Finite Field and Their Applications, 1997, 3(4): 353-369.
- [9] Cunsheng Ding, Niederreiter H. Cyclotomic linear codes of order 3[J]. IEEE Trans Info Theory, 2007, 53(6): 2274-2277.

### 作者简介:



朱士信 男, 1962 年生于安徽省枞阳县. 教授, 博士, 研究方向为代数编码理论和序列密码理论.

E-mail: sxizhu@tom.com



陈安顺 男, 1978 年出生于安徽省怀宁县. 讲师, 硕士, 研究方向为代数编码理论.

E-mail: chenanshun2008@163.com