用四元循环码构造的线性量子码

李瑞虎[1,2]
(1,西安交通大学 理学院，陕西 西安 710049;2. 空军工程大学 理学院数理系，陕西 西安 710051)

摘　要:用模奇数 n 的4－分圆陪集和生成多项式刻划四元循环码,得到一般四元循环码的对偶码为自正交码的充要性判别准则,将前人关于自正交四元单根循环码和四元BCH码的对偶码为自正交判别准则推广到任意四元循环码,包括四元单根循环码和重根循环码.利用单根循环码与重根循环码关系,确定出所有能由短码长的四元循环码构造的线性量子码。

关键词:循环码;自正交码;线性量子码
中图分类号: O157.4　　**文献标识码**:A　　**文章编号**:1009－3516(2006)01－0085－03

自从文献[1]给出构造量子纠错码的一般方法,揭示出量子纠错码与二元自正交码、自正交四元码之间的联系,人们开始研究用二元自正交码和自正交四元码构造量子纠错码。除文献[1]给出四元循环码自正交的一个判别准则外，Grassl等人在[2]还给出四元BCH码的对偶码为自正交的判别准则,并给出 $n\leqslant 61$ 时用四元BCH码构造的线性量子码;Stean在[3]给出二元本原BCH码的对偶码为自正交的判别准则;文献[4]研究了一类特殊码长的四元循环码构造的线性量子码;文献[5]研究了用四元域的扩域上循环码构造量子码;我们在文献[6]中研究了用二元循环码构造量子码。

本文中,我们用模奇数 n 的4－分圆陪集和生成多项式描述码长为 $N=2^{\alpha}n$ 的循环码，用统一的形式刻划四元循环码 $C=[N,K,d]$ 的对偶码为自正交码的充要条件，将文献[1]关于自正交四元单根循环码的判别准则和文献[2]关于四元BCH码的对偶码为自正交码的判别准则推广到任意四元循环码，包括四元单根循环码和重根循环码。综合利用文献[7]、文献[2]以及文献[8]的结论，我们确定出所有能由码长 $N=2^{\alpha}n,\alpha\leqslant 2$ 且 $n\leqslant 99$ 的四元循环码构造的线性量子码。

1　分圆陪集与四元循环码的描述

设 $(n,2)=1,s$ 满足 $0\leqslant s<n$，s 的模 n 的4－分圆陪集为 $C_s^{(4)}=\{s,4s,4^2s,\cdots,4^{k-1}s\}\pmod n$,其中 k 是使得 $4^k s\equiv s\pmod n$ 成立的最小正整数。若 $n-2s\in C_s^{(4)}$,称模 n 的4－分圆陪集 $C_s^{(4)}$ 为对称的;否则,称其为非对称的. 非对称的模 n 的4－分圆陪集 $C_{-2s}^{(4)}=C_{n-2s}^{(4)}$ 成对出现,叫做模 n 的4－分圆非对称偶(简称非对称偶),记为 $(C_s^{(4)},C_{-2s}^{(4)})$。我们用 $k(n)$ 表示模 n 的对称4－分圆陪集 $C_s^{(4)}$ 的个数,用 $\mu(n)$ 表示模 n 的非对称4－分圆陪集偶 $(C_s^{(4)},C_{-2s}^{(4)})$ 的个数。

设 β 为包含 F_4 的某一域中的本原 n 次单位根，则 β^s 在 F_4 上的极小多项式为 $ms(x)=\prod_{i\in C_s^{(4)}}(x-\beta^i)$。从而,$x^n-1=\prod_{t=1}^{k(n)}m_{i_t}(x)\prod_{l=1}^{\mu(n)}(m_{j_l}(x)m_{-j_l}(x))^{2\alpha}$,其中 $C_{i_t}^{(4)}(1\leqslant t\leqslant\kappa(n))$ 全为对称分圆陪集,$(C_{j_l}^{(4)},C_{-2j_l}^{(4)})(1\leqslant l\leqslant\mu(n))$ 全为非对称分圆陪集偶。令 $N=2^{\alpha}n$，则 $x^N-1=\prod_{t=1}^{\kappa(n)}m_{i_l}^{2^{\alpha}}(x)\prod_{l=1}^{\mu(n)}(m_{j_l}(x)m_{-2j_l}(x))^{2\alpha}$。

对任意多项式 $f(x)$，以 $f(x)$ 表示 $f(x)$ 的互反多项式的共轭多项式。若 $C_s^{(4)}$ 对称，则 $m_s(x)=m_s(x)$，

收稿日期:2006－05－23
基金项目:国家自然科学基金资助项目(60573040);中国博士后基金资助项目(20060391009)
作者简介:李瑞虎(1966－),男,安徽亳州市人,教授,博士(后),主要从事代数编码及密码研究.

若$(C_s^{(4)}, C_{-2s}^{(4)})$为非对称分圆陪集偶,则$m_s(s)^+ = \gamma m_{-2s}(x)$,其中$\gamma \in F_4^*$。

若C是码长为N的四元循环码,则C具有生成多项式$f(x)$,$f(x)$是x^N-1的因子,从而$C^\perp$具有生成多项式:$g(x) = (\frac{x^N-1}{f(x)})^+$,总结以上讨论,可得到如下的定理1。

定理1 设C是码长为$N = 2^\alpha N$的循环码,如果$C = (\prod_{t=1}^{k(n)} m_{i_t}^{a_t}(x) \prod_{l=1}^{\mu(n)} (m_{j_l}^{b_l}(x) m_{-2j_l}^{c_l}(t)))$,则$C^\perp \subset C$当且仅当$a_t \leqslant 2^{\alpha-1}$且$b_l + c_l \leqslant 2^\alpha$。

证明:令$f(x) = \prod_{t=1}^{k(n)} m_{i_t}^{a_t}(x) \prod_{l=1}^{\mu(n)} (m_{j_l}^{b_l}(x) m_{-2j_l}^{c_l}(x)$,则$C^\perp$具有生成多项式$g(x) = (\frac{x^N-1}{f(x)}) = \prod_{t=1}^{k(n)} m_{i_t}^{2^\alpha-a_t}(x) \prod_{l=1}^{\mu(n)} (m_{j_t}^{2^\alpha-c_t}(x) m_{-2j_t}^{2^\alpha-b_t}(x))$,$C \subseteq C^\perp$当且仅当$g(x) \mid f(x)$,比较$f(x)$与$g(x)$的不可约因子的次数,即可知定理成立。

2 由短码长的四元循环码构造的线性量子码

四元单根循环码的理论远不如二元单根循环码的理论成熟,所取得的研究成果也比二元单根循环码的成果少,对任意N难以确定循环码的距离,故我们仅考虑码长较小的四元循环码。$N \leqslant 50$时,文献[7]给出一些具有较好参数的四元循环码(包括单根循环码和重根循环码). 利用文献[8]关于重根循环码和单根循环码关系的结论以及循环码的界,不难确定当$N = 2^\alpha n$且$N \leqslant 99$时,对偶码为自正交码的四元循环码的参数,从而能确定出相应的由四元循环码构造的线性量子码的参数。

为节省篇幅,在表1中列出循环码的参数和生成多项式以及相应线性量子码. 表中第一列列出整数n;第二列中的$[N,k,d] = i_1^{\alpha_1}, i_2^{\alpha_2}, \cdots, i_k^{\alpha_k}$表示一个码$C = [N,k,d] = (m_{i_1}^{a_1}(x), \cdots, m_{i_k}^{a_k}(x))$,$C$满足$C^\perp \subset C$;第三列列出由$C$得到的参数为$[[N,K,d]] = [[N,2k-N,d]]$的线性量子码。如果用四元循环码构造的线性量子码与前人用其它方法构造的量子码的参数相同,在表中不再列出. 请注意:我们用的记法$[N,k,d] = i_1^{\alpha_1}, i_2^{\alpha_2}, \cdots, i_k^{\alpha_k}$与文献[7]中码的记法形式一样,但代表的含义明显不同。

表1 利用满足条件$C^\perp \subset C$的四元循环码构造的线性量子码

n	$[N,k,d]$	$[[N,2k-N,d]]$
5	$[10,5,4] = 0.1^2$	$[[10,0,4]]$
15	$[30,25,3] = 0 \cdot 1^2$	$[[30,20,3]]$
15	$[30,20,5] = 0 \cdot 1^2 \cdot 5$	$[[30,18,4]]$
15	$[30,20,5] = 1^2 \cdot 2^2 \cdot 3$	$[[30,10,5]]$
15	$[30,20,5] = 1^2 \cdot 2^2 \cdot 3$	$[[30,8,6]]$
15	$[30,16,7] = 0 \cdot 1^2 \cdot 2^2 \cdot 3 \cdot 5$	$[[30,2,7]]$
15	$[30,15,8] = 0 \cdot 1^2 2^2 \cdot 3^2 \cdot 5 \cdot 10$	$[[30,0,8]]$
17	$[34,26,4] = 2^2$	$[[34,18,4]]$
17	$[34,22,7] = 2^2 \cdot 6$	$[[34,10,7]]$
17	$[34,21,8] = 0 \cdot 2^2 \cdot 6$	$[[34,8,8]]$
17	$[68,48,7] = 2^4 \cdot 6$	$[[68,28,7]]$
17	$[68,47,8] = 0 \cdot 2^2 \cdot 6$	$[[68,28,8]]$
35	$[35,27,5] = 6 \cdot 7$	$[[35,19,5]]$
35	$[70,63,4] = 5 \cdot 7^2$	$[[70,56,4]]$
35	$[70,63,4] = 5^2 \cdot 6 \cdot 7^2$	$[[70,38,7]]$
35	$[70,53,8] = 0 \cdot 5^2 \cdot 6 \cdot 7^2$	$[[70,36,8]]$
35	$[140,131,4] = 5 \cdot 7^3$	$[[140,122,4]]$
41	$[82,62,6] = 1^2$	$[[82,42,6]]$
41	$[82,62,6] = 0 \cdot 1^2$	$[[82,40,7]]$
41	$[82,52,11] = 1^2 \cdot 3$	$[[82,22,11]]$
41	$[82,50,12] = 0 \cdot 1^2 \cdot 3$	$[[82,20,12]]$
63	$[126,119,3] = 0 \cdot 1^2$	$[[126,112,3]]$
63	$[126,116,4] = 0 \cdot 1^2 \cdot 2$	$[[126,106,4]]$
63	$[126,111,5] = 1^2 \cdot 2^2 \cdot 3$	$[[126,96,5]]$
65	$[65,59,3] = 1$	$[[65,53,3]]$
65	$[65,57,4] = 9 \cdot 13$	$[[65,49,4]]$
65	$[65,53,5] = 1 \cdot 3$	$[[65,41,5]]$
85	$[85,83,2] = 34$	$[[85,81,2]]$
85	$[85,79,4] = 30 \cdot 34$	$[[85,73,4]]$
85	$[85,79,4] = 13 \cdot 14 \cdot 30 \cdot 34 \cdot 42$	$[[85,49,8]]$
85	$[85,79,4] = 2 \cdot 7 \cdot 18 \cdot 29 \cdot 30 \cdot 34$	$[[85,41,10]]$
85	$[85,57,11] = 3 \cdot 5 \cdot 6 \cdot 7 \cdot 15 \cdot 19 \cdot 21$	$[[85,29,11]]$
85	$[170,162,4] = 30 \cdot 34^2$	$[[170,154,4]]$
85	$[170,154,5] = 1^2 \cdot 2 \cdot 3$	$[[170,138,5]]$
85	$[170,154,6] = 0 \cdot 1^2 \cdot 2 \cdot 3$	$[[170,136,6]]$
85	$[170,146,7] = 3 \cdot 6 \cdot 7^2 \cdot 15 \cdot 19^2$	$[[170,122,7]]$
85	$[170,146,8] = 13 \cdot 14 \cdot 30^2 \cdot 34^2 \cdot 42$	$[[170,122,8]]$

3 结论

利用四元循环码能构造具有很好参数线性量子码,如本文得到的[10,0,4],[34,10,7][34,8,8]以及码长为 170 的量子码. 但是由于目前计算能力的限制,我们还不能确定出 n 更大时的线性量子码的参数;相信随着计算能力的增强,利用本文的理论还能构造出更多具有很好参数线性量子码.

参考文献:

[1] Calderbank A R, Rains E M, Shor P W, et al. Quantum Error Correction Via Codes Over GF(4)[J]. IEEE Trans. Inf. Theory, 1998, 44(4): 1369 - 1387.

[2] Grassel M, Beth T. Quantum BCH Codes, [ED/OL] heep://xxx. Lanl. gov. ArXiv: Quant - ph/9910060, 14 Oct. 1999.

[3] Steane A M. Enlargement of Calderbank - Shor - Steane Quantum codes[J]. IEEE Trans. Inf. Theory, 1999, 45(2): 2492 - 2495.

[4] Lin Xiaoyan. Quantum Cyclic Codes and Constacyclic Codes[J]. IEEE Trans. Inf. Theory, 2004, 50(3): 547 - 4549.

[5] Thangaraj A, McLaughlin S W. Quantum Codes From Cyclic Codes Over GF(4m)[J]. IEEE Trans. Inf. Theory, 2001, 47(3): 1176 - 1178.

[6] Li Ruihu, Li Xueliang. Quantum Codes Constructed From Binary Cyclic Codes[J]. Int. J. Quantum Informm, 2004, 2(2): 265 - 272.

[7] Kschischang F R, Pasupathy S. Some Ternary and Quaternary Codes and Associated Sphere Packings[J]. IEEE Trans. Inf. Theory, 1992, 38(2): 227 - 246.

(编辑:田新华)

Linear Quantum Codes Constructed from Quaternary Cyclic Codes

LI Rui - hu[1,2]

(1. College of Science, Xi'an Jiaotong University, Xi'an 710049, Shaanxi, China; 2. The Science Institute, Air Force Engineering University, Xi'an 710051, Shaanxi, China)

Abstract: A method of describing quaternary cyclic codes with 4 - cyclotomic cosets of modulo odd n and generator polynomials is presented. A necessary and sufficient condition under which a quaternary cyclic code containing its dual code is given, thus generalizing the related known results on self - orthogonal simple root cyclic codes and on BCH codes to al quaternary cyclic codes. Using the relation of simple root cyclic codes and repeat root cyclic codes, the linear quantum codes that can be constructed from quaternary cyclic codes of short lengths are determined.

Key words: cyclic codes; self - orthogonal codes; linear quantum codes