

量子纠错码的一个统一构造方法

钱建发^{1,2} 马文平¹

(西安电子科技大学 ISN 国家重点实验室 西安 710071)¹ (安徽理工大学理学院 淮南 232001)²

摘要 在量子通信和量子计算中,量子纠错码起着至关重要的作用。人们已经利用 Hamming 码、BCH 码、Reed-Solomon 码等各种循环码、常循环码、准循环码来构造量子纠错码。利用准缠绕码将这些构造方法统一起来,给出了准缠绕码包含其对偶码的充分必要条件及准缠绕码的一个新构造方法,并且利用准缠绕码构造了新的量子纠错码。

关键词 量子纠错码,准缠绕码,循环码,常循环码,准循环码

中图分类号 TN918 **文献标识码** A

Unified Approach to Construct Quantum Error-correcting Code

QIAN Jian-fa^{1,2} MA Wen-ping¹

(National Key Laboratory of ISN, Xidian University, Xi'an 710071, China)¹

(College of Science, Anhui University of Science and Technology, Huainan 232001, China)²

Abstract Quantum error-correcting codes play an important role in not only quantum communication but also quantum computation. All kinds of cyclic codes, for example, Hamming codes, BCH codes and Reed-Solomon codes et al., constacyclic codes and quasi-cyclic codes have been used to construct quantum error-correcting codes. An unified approach to construct quantum error-correcting codes was presented by using quasi-twisted codes. A sufficient and necessary condition for quasi-twisted contained its dual codes, and a new method for constructing quasi-twisted codes was given. Moreover, new quantum quasi-twisted codes were obtained by using quasi-twisted codes.

Keywords Quantum error-correcting codes, Quasi-twisted codes, Cyclic codes, Constacyclic codes, Quasi-cyclic codes

量子通信和量子计算理论的提出,为将来信息技术的深入发展开辟了一个全新的领域。为了实现量子信息的可靠传输与处理,必须保证量子状态经过一定的时空距离后保持不变或能够正确恢复。然而,量子系统不可避免地会受到外界环境的干扰,这必然导致量子状态发生错误,因此要实现可靠的量子通信和计算,量子纠错编码是必不可缺的。

1995—1996 年,Shor^[1] 和 Stean^[2] 将量子错误的复杂机制简化为逐位纠错的物理模型,将每个量子位的错误归结为有限个 Pauli 算子。基于此,Shor 给出了第一个量子纠错码^[1,3,9]。1998 年 Calderbank 等人^[3] 利用有限交换群的特征理论给出构造量子码的系统数学方法,通过构造 F_2 和 F_4 上具有某种特性的经典纠错码来构造量子纠错码(稳定子码)。

此后,人们使用各种经典纠错码来构造量子纠错码^[4-7]。在文献[8]中, Beth 等人利用 Hamming 码来构造量子纠错码;文献[9]中, Aly 等人利用 BCH 码来构造量子纠错码;文献[10]中, Grassl 等人利用 Reed-Solomon 码来构造量子纠错码;文献[11]中, Lin 利用循环码和常循环码来构造量子纠错码,文献[12]利用准循环码构造了一批量子纠错码。

本文利用准缠绕码来构造量子纠错码,给出了准缠绕码包含其对偶码的充分必要条件及准缠绕码的一个新的构造方

法。研究结果表明,我们的方法是上述量子纠错码构造方法的统一,各种量子循环码(量子 Hamming 码、量子 BCH 码、量子 Reed-Solomon 码)、量子常循环码、量子准循环码都是量子准缠绕码的特例。

1 基本概念

假设 p 是一个素数, m 是一个正整数,令 $q = p^m$, F_q 记为元素为 q 的有限域。

经典的 q 元线性码 C 是 F_q 上的 n 维向量空间 F_q^n 的一个 k 维子空间,记为 $[n, k, d]$,其中 d 是码 C 的非零码字 c 的最小 Hamming 重量。

下面在有限域 F_q 上定义 Euclidean 内积。

设 $u = (u_0, u_1, \dots, u_{n-1}), v = (v_0, \dots, v_{n-1}) \in F_q^n$, 则 u 和 v 的 Euclidean 内积为

$$u \cdot v = \sum_{i=0}^{n-1} u_i v_i$$

线性码 C 的 Euclidean 对偶码定义为: $C^\perp = \{u \in F_q^n \mid u \cdot c = 0, c \in C\}$ 。显然, C^\perp 是线性码 $[n, n-k]$ 。如果 $C \subseteq C^\perp$, 则称 C 是自正交码。

引理 1^[3] (CSS 构造) 如果存在自正交的线性码 $C = [n, k]$, 则存在量子纠错码 $[[n, n-2k, d]]$, 其中 $d = \min\{wt(c) \mid c \in$

到稿日期:2009-04-15 返修日期:2009-07-15 本文受 863 国家重点基金项目(2007AA01Z472), 国家自然科学基金(60773002, 60672119, 60873144), 教育部留学回国人员科研启动基金, ISN 开放课题, 安徽省自然科学基金(090412251)资助。

钱建发(1976—), 男, 讲师, 主要研究方向为编码理论、量子通信等, E-mail: qianjianfa@xidian.edu.cn; 马文平(1966—), 男, 教授, 主要研究方向为编码、密码等。

$C^1 \setminus C$ }, 这里 $w(c)$ 表示 F_q^n 中向量 c 的 Hamming 重量。

定义 1 F_q 上长度为 n 的线性码 C 称为循环码, 是指如果 $c = (c_0, c_1, \dots, c_{n-1}) \in C$, 那么 c 循环移位得到的 $c' = (c_{n-1}, c_0, \dots, c_{n-2}) \in C$ 。

如果把码字 $c = (c_0, c_1, \dots, c_{n-1})$ 写成多项式, 并且看成是商环 $R_1 = F_q[x]/(x^n - 1)$ 中的元素, 即 $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in F_q[x]$, 则 C 是循环码的充分必要条件为 C 是商环 R_1 的一个理想。

定义 2 F_q 上长度为 n 的线性码 C 称为常循环码, 是指对 $\alpha \in F_q - \{0\}$, 如果 $c = (c_0, c_1, \dots, c_{n-1}) \in C$, 那么 $c' = (\alpha c_{n-1}, c_0, \dots, c_{n-2}) \in C$ 。

显然, 当 $\alpha = 1$ 时, 即为循环码。

同样, 如果把码字 $c = (c_0, c_1, \dots, c_{n-1})$ 写成多项式, 并且看成是商环 $R_2 = F_q[x]/(x^n - \alpha)$ 中的元素, 即 $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in F_q[x]$, 则 C 是常循环码的充分必要条件为 C 是商环 R_2 的一个理想。

定义 3 F_q 上长度为 $n = ml$ 的线性码 C 称为 l -准循环码, 是指如果它的码字 $c = (c_{11}, c_{21}, \dots, c_{m1}, c_{12}, \dots, c_{m2}, \dots, c_{1l}, \dots, c_{ml}) \in C$, 那么 $c' = (c_{m1}, c_{11}, \dots, c_{m-1,1}, c_{m2}, c_{12}, \dots, c_{m,l}, \dots, c_{m-1,l}) \in C$ 。

显然, 当 $l = 1$ 时, 即为循环码。

定义 4 F_q 上长度为 $n = ml$ 的线性码 C 称为 l -准缠绕码, 是指对 $\alpha \in F_q - \{0\}$, 如果它的码字 $c = (c_{11}, c_{21}, \dots, c_{m1}, c_{12}, \dots, c_{m2}, \dots, c_{1l}, \dots, c_{ml}) \in C$, 那么 $c' = (\alpha c_{m1}, c_{11}, \dots, c_{m-1,1}, \dots, \alpha c_{m,l}, c_{1l}, \dots, c_{m-1,l}) \in C$ 。

显然, 当 $\alpha = 1$ 时, 即为准循环码; 当 $l = 1$ 时, 即为常循环码; 当 $\alpha = 1, l = 1$ 时, 即为循环码。

2 量子纠错码的构造

本节利用 l -准缠绕码来构造一批量子纠错码。首先, 给出准缠绕码包含其对偶码的充分必要条件。

类似于准循环码^[13], F_q 上长度为 $n = ml$ 的 l -准缠绕码可视为 $(F_q[x]/(x^n - \alpha))^l$ 的 $F_q[x]/(x^n - \alpha)$ 子模。

定理 1^[14] 设线性码 C 是 F_q 上长度为 $n = ml$ 的 l -准缠绕码, 那么 C 有下列形式的生成多项式, 即

$$g(x) = (f_1(x)g_1(x), f_2(x)g_2(x), \dots, f_l(x)g_l(x))$$

其中, 对 $1 \leq i \leq l, g_i(x) | (x^n - \alpha), (f_i(x), (x^n - \alpha)/g_i(x)) = 1$ 。

引理 2^[3] 设 $g(x)$ 是 F_q 上长度为 n 的线性常循环码 C 的生成多项式, 则 C 包含其对偶码的充分必要条件为

$$x^n - \alpha \equiv 0 \pmod{g(x)g^*(x)}$$

其中 $g^*(x) = x^{n-k}g(1/x)$, 即 $g^*(x)$ 是 $g(x)$ 的互反多项式。

定理 2 设线性码 C 是 F_q 上长度为 $n = ml$ 的 l -准缠绕码, 其生成多项式为

$$g(x) = (f_1(x)g_1(x), f_2(x)g_2(x), \dots, f_l(x)g_l(x))$$

其中, 对 $1 \leq i \leq l, g_i(x) | (x^n - \alpha), (f_i(x), (x^n - \alpha)/g_i(x)) = 1$, 那么 C 包含它的对偶码的充分必要条件为

$$x^n - \alpha \equiv 0 \pmod{g_1(x)g_1^*(x), \dots, x^n - \alpha \equiv 0 \pmod{g_l(x)g_l^*(x)}}$$

其中, $g_i^*(x)$ 是 $g_i(x)$ 的互反多项式。

证明: 令 $1 \leq i \leq l$, 对某一个固定的 i , 定义下面第 i 个在 C 上的映射 θ_i 如下:

$$\theta_i(c_{11}, c_{21}, \dots, c_{m1}, c_{12}, \dots, c_{m2}, \dots, c_{1l}, \dots, c_{ml}) = (c_{1i}, c_{2i}, \dots, c_{mi})$$

令 $\theta_i(C) = C_i$, 显然 $C_i \subseteq F_q[x]/(x^n - \alpha)$ 。由于 C 是 $(F_q[x]/(x^n - \alpha))^l$ 的 $F_q[x]/(x^n - \alpha)$ 子模, 则对任意 $c(x) = (c_1(x), c_2(x), \dots, c_l(x)) \in C$ 和 $a(x) \in F_q[x]/(x^n - \alpha)$, 有 $a(x)c(x) \in C$ 。因此, 对任意的 $c_i(x) \in C_i$, 有 $a(x)c_i(x) \in C_i$ 。所以 C_i 是 $F_q[x]/(x^n - \alpha)$ 的一个理想, 即 C_i 是 F_q 上长度为 m 的循环码。由纠错码理论及引理 2 可知, 该结论成立。证毕。

下面定义量子准缠绕码。

定义 5 如果量子纠错码是由准缠绕码通过 CSS 构造得到, 则称该量子纠错码为量子准缠绕码。

定理 3 设 $C = [n, k, d]$ 是 F_q 上长度为 $n = ml$ 的 l -准缠绕码, 其生成多项式为

$$g(x) = (f_1(x)g_1(x), f_2(x)g_2(x), \dots, f_l(x)g_l(x))$$

其中, 对 $1 \leq i \leq l, g_i(x) | (x^n - \alpha), (f_i(x), (x^n - \alpha)/g_i(x)) = 1$, 如果 $x^n - \alpha \equiv 0 \pmod{g_1(x)g_1^*(x)}, \dots, x^n - \alpha \equiv 0 \pmod{g_l(x)g_l^*(x)}$, 那么存在参数为 $[[n, 2k - n, d]]$ 的量子准缠绕码。

证明: 由引理 1 及定理 2 可知, 该结论成立。

注 1: 由上述可知, 量子循环码、量子常循环码、量子准循环码都是量子准缠绕码的特例。

例 1 Glynn 等人在文献[15]中, 通过 Tabu 搜索, 找到了一些参数较好的四元自正交准缠绕码。为节省篇幅, 选择自正交准缠绕码[12, 4, 8], [16, 4, 12], 通过 CSS 构造, 可得到量子准缠绕码[[12, 4, 4]], [[16, 8, 3]]。

3 准缠绕码的构造

本节利用常循环码来构造准缠绕码, 并且利用常循环码的对偶包含关系得到准缠绕码对偶包含关系。

定义 6 映射 $Tr: F_q \rightarrow F_p, Tr(\alpha) = \alpha + \alpha^p + \dots + \alpha^{p^{m-1}}$ 称为有限域 F_q 到其子域 F_p 的迹映射。注意到对于每个 $\alpha \in F_q$, 有 $\alpha^q = \alpha$ 。

于是 $Tr(\alpha)^p = \alpha^p + \alpha^{p^2} + \dots + \alpha^{p^{m-1}} + \alpha = Tr(\alpha)$, 即 $Tr(\alpha) \in F_p$, 所以 Tr 是 F_q 到 F_p 的映射。

由文献[16]可知, 迹映射有以下性质。

性质 1 对所有 $\alpha, \beta \in F_q$, 有

$$(1) Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta);$$

$$(2) Tr(\lambda\alpha) = \lambda Tr(\alpha), \text{ 其中 } \lambda \in F_p.$$

定义 7 设 $B = \{\alpha_1, \alpha_2, \dots, \alpha_m\}$ 是 F_q 在 F_p 上的一组基, 如果

$$Tr(\alpha_i\alpha_j) = \begin{cases} 1, & i=j \\ 0, & \text{其它} \end{cases}$$

则称 $B = \{\alpha_1, \alpha_2, \dots, \alpha_m\}$ 是 F_q 在 F_p 上的自对偶基。

由文献[17]知, 如果 p 是偶数, 或者 p 和 m 都是奇数, 则 F_q 在 F_p 上的自对偶基是存在的。

下面, 令 $B = \{\alpha_1, \alpha_2, \dots, \alpha_m\}$ 是 F_q 在 F_p 上的自对偶基。对 $c = (c_1, c_2, \dots, c_n) \in C$, 定义映射 $\varphi: F_q^n \rightarrow F_p^m$ 为

$$\varphi(c) = (c_{11}, c_{21}, \dots, c_{m1}, c_{12}, \dots, c_{m2}, \dots, c_{1m}, \dots, c_{mm})$$

这里 $c_i = \sum_{j=1}^m c_{ij}\alpha_j$, 其中 $c_{ij} \in F_p$ 。

令 $\varphi(C)$ 是码 C 在 φ 下的像, 下面利用常循环码来构造准缠绕码, 即有下面的定理。

定理 4 如果 C 是 F_q 上长度为 n 的常循环码, 其中 $\alpha \in F_p - \{0\}$, 那么 $\varphi(C)$ 是 F_p 上长度为 mn 的 m -准缠绕码。

证明: 设 $c = (c_1, c_2, \dots, c_n) \in C$, 其中 $c_i = \sum_{j=1}^m c_{ij} \alpha_j$, 那么 $\varphi(\alpha c_n, c_1, \dots, c_{n-1}) = (\alpha c_{n1}, c_{11}, \dots, c_{n-1,1}, \dots, \alpha c_m, c_{1m}, \dots, c_{n-1,m})$ 。由于 C 是常循环码, 由准缠绕码的定义可知, $\varphi(C)$ 是 F_p 上长度为 mn 的 m -准缠绕码。

引理 3^[12] 如果 C 是 F_q 上长度为 n 的自正交码, 则 $\varphi(C)$ 是 F_p 上长度为 mn 的自正交码。

由引理 3 和定理 4, 可得到下面定理:

定理 5 如果 C 是 F_q 上包含它的对偶码的常循环码, 那么 $\varphi(C)$ 是 F_p 包含它的对偶码的准缠绕码。

由引理 1 及定理 5, 可得到一大批新的量子准缠绕码, 即有下面定理:

定理 6 如果 $C = [n, k, d]$ 是 F_q 上长度为 n 的包含它的对偶码的常循环码, 那么存在参数为 $[[mn, m(2k-n), d']]$ 的量子准缠绕码, 其中 $d' \geq d$ 。

结束语 本文利用准缠绕码来构造量子纠错码, 通过对准缠绕码的结构分析, 将量子循环码、量子常循环码、量子准循环码的构造方法统一起来。如何在实际的物理背景下对这些量子纠错码加以应用, 将是未来量子纠错码研究的一个重点。

参 考 文 献

[1] Shor P W. Scheme for reducing decoherence in quantum memory [J]. Phys. Rev. A, 1995, 52(4): 2493-2496
 [2] Steane A M. Simple quantum error correcting codes[J]. Phys. Rev. Lett., 1996, 77: 793-797
 [3] Calderbank A R, et al. Quantum error correction via codes over GF(4) [J]. IEEE Trans. Inf. Theory, 1998, 44(4): 1369-1387
 [4] Li R, Li X. Binary construction of quantum codes of minimum distance three and four[J]. IEEE Trans. Inf. Theory, 2004, 50

(4): 1331-1336

[5] Chen H, Ling S, Xing C. Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound [J]. IEEE Trans. Inf. Theory, 1998, 47(4): 2055-2058
 [6] 马智, 冯克勤. 量子纠错码的 Gilbert-Varshamov 界和有限西几何[J]. 自然科学进展, 2002, 12: 1202-1204
 [7] 郑大钟, 赵千川. 量子计算和量子信息(2)[M]. 北京: 清华大学出版社, 2005
 [8] Beth T, Grassl M. The quantum Hamming and Hexacodes [J]. Fortschr. Phys., 1998, 46(5): 459-491
 [9] Aly S A, Klappenecker A, Sarvepalli P K. On quantum and classical BCH codes[J]. IEEE Trans. Inf. Theory, 2007, 53(3): 1183-1188
 [10] Grassl M, Geiselmann W, Beth T. Quantum Reed-Solomon codes [J]. AAECC, 1999, 13: 231-241
 [11] Lin X. Quantum cyclic and constacyclic codes[J]. IEEE Trans. Inf. Theory, 2004, 50(3): 547-549
 [12] Qian J F, Ma W P, Wang X M. Quantum error-correcting codes from quasi-cyclic Codes[J]. International Journal of Quantum Information, 2008, 6(6): 1150-1156
 [13] Siap I, et al. New ternary quasi-cyclic codes with better minimum distances[J]. IEEE Trans. Inf. Theory, 2000, 46(4): 1554-1557
 [14] Aydin N, et al. The structure of 1-generator quasi-twisted codes and new linear codes[J]. Des., Codes and Cryptogr., 2001, 24(6): 313-326
 [15] Glynn D, Gulliver T, Gupta M. On some quaternary self-orthogonal codes [EB/OL]. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.6.4341>
 [16] 王新梅, 肖国镇. 纠错码—原理和方法[M]. 西安: 电子科技大学出版社, 2001
 [17] Seroussi G, Lempel A. Factorization of symmetric matrices and trace-orthogonal bases in finite fields[J]. SIAM J. Comput., 1980, 9: 758-767

(上接第 63 页)

[3] National Security Agency. NSA tempest series [OL]. <http://cryptome.org/#NSA-TS>
 [4] Standaert F X, Malkin T G, Yung M. A unified framework for the analysis of side-channel key recovery attacks (Version 2.0) [C]//Proceedings of Eurocrypt 2009. LNCS 5479. Berlin/Heidelberg: Springer-Verlag, 2009: 443-461
 [5] Micali S, Reyzin L. Physically observable cryptography (extended abstract) [C]//Proceedings of the TCC 2004. LNCS 2951. Berlin/Heidelberg: Springer-Verlag, 2004: 278-296
 [6] Dent A W, Lee J M. The physically observable security of signature schemes [C]//N. P Smart, ed. Cryptography and Coding: 10th IMA International Conference. LNCS 3796. Berlin/Heidelberg: Springer-Verlag, 2005: 220-232
 [7] Chari S, Rao J, Rohatgi P. Template attacks [C]//Proceedings of Cryptographic Hardware and Embedded Systems-CHES 2002. LNCS 2535. Berlin/Heidelberg: Springer-Verlag, 2003: 13-28
 [8] Köpf B, Basin D. An information theoretic model for adaptive side-channel attacks [C]//Proceedings of the 14th ACM Conference on Computer and Communications Security-CCS 2007. USA: ACM, 2007: 286-296
 [9] Kocher P, Jaffe J, Jun B. Differential power analysis [C]//Ad-

vances in Cryptology: Proceedings of CRYPTO'99. LNCS 1666. Berlin/Heidelberg: Springer-Verlag, 1999: 388-397

[10] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model [C]//Cryptographic Hardware Embedded System-CHES 2004. LNCS 3156. Berlin/Heidelberg: Springer-Verlag, 2004: 16-29
 [11] Zhang Peng, Deng Gao-ming, ZHAO Qiang. An automatic experimental platform for differential electromagnetic analysis on cryptographic ICs [C]//Proceedings of the Second International Symposium on Test Automation & Instrumentation-ISTAI'2008. Beijing: World Publishing Corporation, 2008: 1078-1082
 [12] National Institute of Standards and Technology. FIPS 197: Advanced encryption standard [S]. 2001
 [13] Mangard S, Oswald E, Popp T. Power Analysis Attacks—Revealing the Secrets of Smart Cards [M]. USA: Springer, 2007: 86-98
 [14] Bellare M, Desai A, Jokipii E, et al. A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation [C]//Proceedings of the 38th Annual Symposium on Foundations of Computer Science. USA: IEEE Computer Society Press, 1997: 394-403