新的非对称量子纠错码的构造

钱建发　　马文平
(西安电子科技大学 ISN 国家重点实验室　西安　710071)

摘　要：量子纠错码在量子通信和量子计算中起着非常重要的作用，之前的量子纠错码的构造大部分都集中在对称的量子信道，即量子比特翻转的错误概率与量子相位翻转的错误概率相等。该文在非对称量子信道上，即量子比特翻转的错误概率小于量子相位翻转的错误概率，利用经典的平方剩余码和 Reed-Muller 码构造一批非对称的量子纠错码。同已知的非对称量子纠错码的构造方法相比，该构造方法简单。并且，利用有限域的扩域到其子域的迹映射，构造得到了更多的非对称量子纠错码。

关键词：量子纠错码；非对称量子纠错码；平方剩余码；Reed-Muller 码；自正交码
中图分类号：TN911.22　　**文献标识码**：A　　**文章编号**：1009-5896(2009)12-2922-04

New Construction of Asymmetric Quantum Error-correcting Codes

Qian Jian-fa　　Ma Wen-ping
(*National Key Laboratory of ISN*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: Quantum error-correcting codes play an important role in not only quantum communication but also quantum computation. Previous work in constructing quantum error-correcting codes focuses on code constructions for symmetric quantum channels, i.e., qubit-flip and phase-shift errors have equal probabilities. This paper focuses on the asymmetric quantum channels, i.e., qubit-flip and phase-shift errors have different probabilities Some present families of asymmetric quantum codes are constructed with classical quadratic residue codes and Reed-Muller codes. Compared to previously known methods, the method is simple. Furthermore, using the Trace map, more asymmetric quantum error-correcting codes are obtained.

Key words: Quantum error-correcting codes; Asymmetric quantum error-correcting codes; Quadratic residue codes; Reed-Muller codes; Self-orthogonal codes

1　引言

1995–1996 年，Shor 和 Stean 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[1] 给出了第 1 个参数为 [[9,1,3]] 量子纠错码。Shor 的方法促进了量子纠错编码的产生与发展。通过借鉴经典纠错编码理论，人们提出了一系列量子纠错编码方案[2–10]，并且逐渐形成了量子纠错编码的理论体系。

2007 年，Loff 等人在文献[11]中指出，大部分已知的量子计算设备的松弛时间 T_1 比对应的降相位时间 T_2 大，它们的关系为 $1/T_1 = 1/(2T_2) + \Gamma_p$。通常松弛导致比特翻转和相位翻转的错误，而降相位仅仅导致相位翻转的错误。T_1 与 T_2 的这种非对称性使得比特翻转的错误概率小于相位翻转的错误概率，因此，量子纠错应考虑到这种非对称的量子信道。

在文献[11]中，Loff 等人利用 BCH 码和 LDPC 码的组合来构造非对称量子纠错码。在文献[12]中，Sarvepalli 等人使用 LDPC 码来构造非对称量子纠错码，而在文献[13]中，Aly 利用经典的 BCH 码和 RS 码来构造非对称量子纠错码。本文，利用经典的平方剩余码和 Reed-Muller 码来构造一批非对称量子纠错码。并且，利用有限域的扩域到其子域的迹映射，构造了更多的非对称量子纠错码。最后，具体给出一些参数性能较好的非对称量子纠错码。

2　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，记为 $d = wt(C)$。

2008-12-17 收到，2009-06-18 改回
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，新世纪优秀人才支持计划，国家 863 计划项目(2007AA01Z472)和 ISN 国家重点实验室开放基金资助课题

下面在有限域 F_q 上定义 Euclidean 内积。

设 $u=(u_1,\cdots,u_n)$， $v=(v_1,\cdots,v_n)\in R^n$，则 u 和 v 的 Euclidean 内积为

$$u\cdot v=\sum_{i=1}^{n}u_iv_i \tag{1}$$

线性码 C 的 Euclidean 对偶码定义为: $C^{\perp}=\{u\in F_q^n \mid u\cdot c=0,c\in C\}$。

在文献[11]中，非对称量子纠错码的构造基于相位翻转的错误概率小于量子比特翻转的错误概率的情况，而且非对称量子纠错码对不同类型的错误纠错的能力不同。基于这一事实，文献[11-13]中给出非对称量子纠错码的定义。

定义 1　q 元非对称量子纠错码 Q, 记为 $[[n,k,d_z/d_x]]$，是 F_q 上 q^k 维的 Hilbert 空间 C^{q^n} 的一个子空间，它能同时纠正 $\lfloor (d_x-1)/2\rfloor$ 个量子比特翻转的错误和 $\lfloor (d_z-1)/2\rfloor$ 个量子相位翻转的错误，而且，能同时发现 (d_x-1) 个量子比特翻转的错误和 (d_z-1) 个量子相位翻转的错误。

注 1　该定义中 d_z/d_x 为一个比较因子，因此，如果 $d_z>d_x$，那么相位翻转对量子系统的影响比量子比特翻转的影响要大。

在文献[11-13]中，提出了可用经典的纠错码来构造非对称量子纠错码，其构造方法由下面定理给出。

定理 1　设 $C_1=[n,k_1,d_1]$, $C_2=[n,k_2,d_2]$ 为 F_q 上长度为 n，维数分别为 k_1,k_2，最小距离分别为 d_1,d_2 的线性码，如果 $C_1^{\perp}\subseteq C_2, C_2^{\perp}\subseteq C_1$，且

$$\left.\begin{aligned} d_x&=\min\{wt(C_1\setminus C_2^{\perp}),wt(C_2\setminus C_1^{\perp})\}\\ d_z&=\max\{wt(C_1\setminus C_2^{\perp}),wt(C_2\setminus C_1^{\perp})\}\end{aligned}\right\} \tag{2}$$

那么存在参数为 $[[n,k_1+k_2-n,d_z/d_x]]$ 的非对称量子纠错码。

3　平方剩余码构造非对称量子码

本节，利用平方剩余码来构造一批非对称的量子纠错码。首先，简单介绍平方剩余码的定义，具体介绍可参考文献[14-16]。

定义 2　对正整数 n，存在一个整数 r，使得式(3)成立

$$r^2\equiv i(\mathrm{mod}\,n) \tag{3}$$

则称 i 是模 n 的平方剩余，否则称 i 为模 n 的非平方剩余。

例 1　2 是模 7 的平方剩余，而 3 是模 7 的非平方剩余。

令 Q 表示模 n 的平方剩余集合，N 表示模 n 的非平方剩余集合，若 α 是 F_q 的扩域的一个本原域元素，则由文献[15]知，当 i 是偶数时，$\alpha^i\in Q$，而 i 为奇数时，$\alpha^i\in N$，且 $\alpha^0=1\in Q$，因而 Q 是 α^i 生成的一个循环群。

由有限域理论可知，F_q 的扩域中的所有非零元素都是方程 $x^{p^m}-1=0$ 的根。因此若在 F_q 的扩域中的某一子域内有一个 p 阶根 α，则 $\alpha^0=1$，α，$\cdots$，α^{p-1} 都是方程 $x^{p^m}-1=0$ 的根，所以

$$x^{p^m}-1=(x-1)(x-\alpha)\cdots(x-\alpha^{p-1})=(x-1)q(x)n(x) \tag{4}$$

其中

$$\left.\begin{aligned} q(x)&=\prod\nolimits_{i\in Q}(x-\alpha^i)\\ n(x)&=\prod\nolimits_{j\in N}(x-\alpha^j)\end{aligned}\right\} \tag{5}$$

是系数 F_q 为上的多项式。

定义 3　用下列多项式 $q(x)$，$(x-1)q(x)$，$n(x)$，$(x-1)n(x)$，生成的循环码，称为 F_q 上的平方剩余码，分别用 C_Q，C_Q'，C_N，C_N'，表示。

引理 1[15]　C_Q，C_N 是参数为 $[n,k,d]$ 的线性码，其中 $d^2>n$；C_Q'，C_N' 是参数为 $[n,k',d']$ 的线性码，其中 $d'>d$。

引理 2[15]　当 n 为素数，$n\equiv 1(\mathrm{mod}\,4)$，且 q 是模 n 的平方剩余，则有 $C_Q^{\perp}=C_N'\subset C_N$, $C_N^{\perp}=C_Q'\subset C_Q$。

定理 2　设 C_Q, C_N 为 F_q 上的平方剩余码，$n\equiv 1(\mathrm{mod}\,4)$，且 q 是模 n 的平方剩余，则存在参数为 $[[n,2k-n,d_z/d_x]]$ 的非对称量子纠错码。

证明　由引理 2 可知，当 $n\equiv 1(\mathrm{mod}\,4)$，且 q 是模 n 的平方剩余，有 $C_Q^{\perp}=C_N'\subset C_N$, $C_N^{\perp}=C_Q'\subset C_Q$。不妨假设 $d_x=\min\{wt(C_N\setminus C_Q^{\perp}),wt(C_Q\setminus C_N^{\perp})\}$，$d_z=\max\{wt(C_N\setminus C_Q^{\perp}),wt(C_Q\setminus C_N^{\perp})\}$。因此，由定理 1 可知，存在参数为 $[[n,2k-n,d_z/d_x]]$ 的非对称量子纠错码。

4　迹映射构造

定义 4　映射

$$\left.\begin{aligned} &\mathrm{Tr}: F_q\to F_p\\ &\mathrm{Tr}(\alpha)=\alpha+\alpha^p+\cdots+\alpha^{p^{m-1}}\end{aligned}\right\} \tag{6}$$

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 $\mathrm{Tr}(\alpha)^p=\alpha^p+\alpha^{p^2}+\cdots+\alpha^{p^{m-1}}+\alpha=\mathrm{Tr}(\alpha)$，即 $\mathrm{Tr}(\alpha)\in F_p$，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) $\mathrm{Tr}(\alpha+\beta)=\mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta)$;

(2) $\mathrm{Tr}(\lambda\alpha)=\lambda\mathrm{Tr}(\alpha)$，其中 $\lambda\in F_p$。

定义 5　设 $B=\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$ 是 F_q 在 F_p 上的一组基，如果

$$\mathrm{Tr}(\alpha_i\alpha_j)=\begin{cases}1, & i=j\\ 0, & \text{其它}\end{cases} \tag{7}$$

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

$$\varphi(c)=(c_{11},c_{21},\cdots,c_{n1},c_{12},\cdots,c_{n2},\cdots,c_{1m},\cdots,c_{nm}) \tag{8}$$

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，则有下面的引理。

引理 3 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。

证明 设 $c=(c_1,c_2,\cdots,c_n)$，$d=(d_1,d_2,\cdots,d_n)\in F_q^n$ 为 C 的任意两个码字，其中 $c_i=\sum_{j=1}^m c_{ij}\alpha_j$，$d_i=\sum_{j=1}^m d_{ij}\alpha_j$，由于 C 是自正交码，则有

$$c\cdot d=\sum_{i=1}^n c_id_i=\sum_{i=1}^n\Big(\sum_{j=1}^m c_{ij}\alpha_j\Big)\Big(\sum_{k=1}^m d_{ij}\alpha_k\Big)=0 \tag{9}$$

对上式在 F_p 上取 Tr，有

$$\sum_{i=1}^n\sum_{j=1}^m\sum_{k=1}^m c_{ij}d_{ij}\mathrm{Tr}(\alpha_j\alpha_k)=0 \tag{10}$$

由于 $B=\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$ 是 F_q 在 F_p 上的自对偶基，则有

$$\sum_{i=1}^n\sum_{j=1}^m c_{ij}\cdot d_{ij}=\varphi(c)\cdot\varphi(d)=0 \tag{11}$$

因此，$\varphi(C)$ 是 F_p 上长度为 mn 的自正交码。

由引理 3，可得到下面定理。

定理 3 设 C_Q, C_N 为 F_q 上两个平方剩余码，且有 $C_Q^\perp\subseteq C_N$，$C_N^\perp\subseteq C_Q$，则有 $\varphi(C_Q^\perp)\subseteq\varphi(C_N)$，$\varphi(C_N^\perp)\subseteq\varphi(C_Q)$。

由定理 1 及定理 3，可得到一大批新的非对称量子纠错码，即有下面定理：

定理 4 设 C_Q, C_N 为 F_q 上的平方剩余码，且有 $C_Q^\perp\subseteq C_N$，$C_N^\perp\subseteq C_Q$，则存在参数为 $[[mn, m(2k-n), d_{z'}/d_{x'}]]$ 的非对称量子纠错码，其中

$$\left.\begin{aligned} d_{x'}>d_x&=\min\{wt(C_N\setminus C_Q^\perp),wt(C_Q\setminus C_N^\perp)\}\\ d_{z'}>d_z&=\max\{wt(C_N\setminus C_Q^\perp),wt(C_Q\setminus C_N^\perp)\}\end{aligned}\right\} \tag{12}$$

5 Reed-Muller 码构造非对称量子码

Reed-Muller(RM)码是与 1954 年 Muller 首先提出其构造方法，同年 Reed 用大数逻辑译码方法解决了它的译码。RM 码最早是从线性空间的角度出发构造的，以后发现它与循环码，几何码和格等有密切关系，因此 RM 码是一类重要的线性码，具体关于 RM 码的描述见文献[15,16]。

对于一个 r 阶 RM 码 $\mathrm{RM}(r,m)$，设其参数为 $[n,k,d]$，由文献[15,16]可知，RM 码有下列性质。

性质 2 设 $\mathrm{RM}(r,m)$ 为 r 阶 RM 码，则有

(1)码的长度 $n=2^m$；

(2)码的维数 $k=1+C(m,1)+\cdots+C(m,r)$，其中 $C(m,l)=m!/l!(m-l)!$

(3)码的最小距离 $d=2^{m-r}$；

(4) $\mathrm{RM}(r,m)^\perp=\mathrm{RM}(m-r-1,m)$。

定理 5 设 $C_1=\mathrm{RM}(r_1,m)$，$C_2=\mathrm{RM}(r_2,m)$ 为 F_2 上两个的 RM 码，如果 $r_1<r_2$，那么 $wt(C_2\setminus C_1)=wt(C_2)$。

证明 由 RM 码定义及性质 2 知，当 $r_1<r_2$ 时，有 $C_1\subseteq C_2$。设 C_1 的最小距离为 $d_1=2^{m-r_1}$，C_2 的最小距离为 $d_2=2^{m-r_2}$，如果 $r_1<r_2$，则有 $d_2<d_1$。因此，$C_2\setminus C_1$ 有一个重量为 d_2 的码字。所以，$wt(C_2\setminus C_1)=wt(C_2)$。

下面，利用 RM 码来具体构造一批非对称量子纠错码。首先，记 $\mathrm{RM}(r,m)=[n,k,d]$ 的对偶码的参数为 $\mathrm{RM}(r,m)^\perp=[n,k^\perp,d^\perp]$。

定理 6 设 $C_1=[n,k_1,d_1]$，$C_2=[n,k_2,d_2]$ 为 F_2 上两个长度为 $n=2^m$ 的 RM 码，当 $k_1^\perp<k_2, k_2^\perp<k_1$ 时，则存在参数为 $[[n,k_1+k_2-n,d_z/d_x]]$ 的非对称量子纠错码，其中

$$\left.\begin{aligned} d_x&=\min\{wt(C_1\setminus C_2^\perp),wt(C_2\setminus C_1^\perp)\}\\ d_z&=\max\{wt(C_1\setminus C_2^\perp),wt(C_2\setminus C_1^\perp)\}\end{aligned}\right\} \tag{13}$$

证明 由性质 2 知，当 RM 码的维数满足 $k_1^\perp<k_2$ 时，有 $C_1^\perp\subseteq C_2$ 成立。同样，当 RM 码的维数满足 $k_2^\perp<k_1$ 时，有 $C_2^\perp\subseteq C_1$ 成立。不妨假设 $d_x=\min\{wt(C_N\setminus C_Q^\perp),wt(C_Q\setminus C_N^\perp)\}$，$d_z=\max\{wt(C_N\setminus C_Q^\perp),wt(C_Q\setminus C_N^\perp)\}$。因此，由定理 1 可知，存在参数为 $[[n,k_1+k_2-n,d_z/d_x]]$ 的非对称量子纠错码。

例 2 令 $m=5$，$n=128$，则有 7 个 RM 码，它们分别为：$[128,1,128]$，$[128,8,64]$，$[128,29,32]$，$[128,64,16]$，$[128,99,8]$，$[128,120,4]$，$[128,127,2]$。可分别选择这些码来构造非对称量子纠错码，如设 $C_1=[128,8,64]$，$C_2=[128,127,2]$，由 RM 码性质 2 知，$C_1^\perp=[128,120,4]$，$C_2^\perp=[128,1,128]$，且有 $C_1^\perp\subseteq C_2$，$C_2^\perp\subseteq C_1$。由定理 1 及定理 5 可知，存在参数为 $[[128,7,64/2]]$ 的非对称量子纠错码。表 1 具体给出非对称量子纠错码的参数。

注 2 同文献[11–13]中的非对称量子纠错码比较，本文的非对称量子纠错码的参数 d_z/d_x 值较大，说明相位翻转对量子系统的影响比量子比特翻转的影响要大。并且本文构造的非对称量子纠错码都是新的，在目前的文献中都未曾出现。

表 1 非对称量子纠错码

RM 码 C_1	RM 码 C_2	非对称量子码 C
[128, 8, 64]	[128, 127, 2]	[[128, 7, 64/2]]
[128, 29, 32]	[128, 120, 4]	[[128, 21, 32/4]]
[128, 29, 32]	[128, 127, 2]	[[128, 28, 32/2]]
[128, 99, 8]	[128, 64, 16]	[[128, 35, 16/8]]
[128, 120, 4]	[128, 127, 2]	[[128, 115, 4/2]]
[128, 99, 8]	[128, 120, 4]	[[128, 91, 8/4]]
[128, 99, 8]	[128, 127, 2]	[[128, 98, 8/2]]

6 结束语

本文在非对称的量子信道上，利用经典的平方剩余码和 Reed-Muller 码构造了一批非对称量子纠错码，并且，利用有限域的扩域到其子域的映射，构造得到了更多的非对称量子纠错码。最后，具体给出一些参数性能较好的非对称量子纠错码。由于非对称量子纠错码的概念在 2007 年才首次提出，目前，对非对称量子纠错码的研究还处在初步阶段。对编码理论学者来说，如何设计构造性能好的非对称量子纠错码是未来研究的一个重点，而对物理学家来说，如何在实际的物理背景下对这些量子码实现应用，将是量子纠错码是否实用的关键。

参 考 文 献

[1] Shor P W. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A*, 1995, 52(4): 2493–2496.

[2] Steane A M. Simple quantum error-correcting codes. *Phys. Rev. Lett*, 1996, 77(6): 793–797.

[3] Calderbank A R, *et al.*. Quantum error correction via codes over GF(4). *IEEE Transactions on Information Theory*, 1998, 44(4): 1369–1387.

[4] Feng K, Ling S, and Xing C. Asymptotic bounds on quantum codes from algebraic geometry codes. *IEEE Transactions on Information Theory*, 2006, 52(3): 986–991.

[5] Li R, Xu Z, and Li X. Standard forms of stabilizer and normalizer matrices for additive quantum codes. *IEEE Transactions on Information Theory*, 2008, 54(8): 1331–1336.

[6] Chen H, Ling S, and Xing C. Quantum codes from concatenated algebraic-geometric codes. *IEEE Transactions on Information Theory*, 2005, 51(8): 2915–2920.

[7] Guo Y, Chen Z, Huang D, and Zeng G. A novel deterministic quantum communication scheme using stabilizer quantum code. *Communications in Theoretical Physics*, 2008, 49(1): 93–99.

[8] Qian J F, Ma W P, and Wang X M. Quantum error-correcting codes from quasi-cyclic codes. *International Journal of Quantum Information*, 2008, 6(6): 1150–1156.

[9] Grassl M, Geiselmonn W, and Beth T. Quantm Reed-Solomon codes. *Applicable Algebra in Engineering, Communication and Computation*, 1999, 13(4): 231–241.

[10] 郑大钟, 赵千川. 量子计算和量子信息(2). 北京: 清华大学出版社, 2005: 12–145.

[11] Ioffe L and Mezard M. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 2007, 75(3): 86–90.

[12] Sarvepalli P K, *et al.*. Asymmetric quantum LDPC codes. Proceeding of the IEEE International Symposium on Information Theory, Toronto, Canada, 2008: 305–309.

[13] Aly A. Asymmetric and symmetric subsystem BCH codes and beyond. http://arxiv.org/abs/0803.0764 , 2008.

[14] Ketkar A, *et al.*. Nonbinary quantum stabiliter codes over finite fields. *IEEE Transactions on Information Theory*, 2006, 52(11): 4892–4914.

[15] MacWilliams F J and Sloane N J A. The Theory of Error Correcting Codes. Amsterdam. The Netherlands: North-Holland. 1977: 132–139.

[16] 王新梅, 肖国镇. 纠错码 —— 原理和方法. 西安: 西安电子科技大学出版社, 2001: 162–165.

[17] Seroussi G and Lempel A. Factorization of symmetric matrices and trace-orthogonal bases in finite fields. *SIAM Journal of Computation*, 1980, 9(6): 758–767.

钱建发： 男，1976 年生，博士生，研究方向为编码理论与量子通信.

马文平： 男，1966 年生，教授，博士生导师，研究方向为编码理论与密码学等.