DOI:10.3969/j.issn.1003-5060.2023.02.022

新的最优非对称量子纠错码的构造

孙麒麟，　王立启
(合肥工业大学 数学学院,安徽 合肥　230601)

摘　要:非对称量子纠错码是量子纠错码中一类重要的码。因为量子比特翻转的错误概率小于量子相位翻转的错误概率,所以量子纠错需要考虑到非对称的量子信道。文章利用有限域上的经典常循环码,通过非对称量子纠错码的 CSS 构造法构造了 2 类非对称量子纠错码。所构造的非对称量子纠错码是新的,同时达到了非对称量子纠错码的 Singleton 界,因而也是最优的。

关键词:非对称量子纠错码;常循环码;CSS 构造;Singleton 界
中图分类号:O157.4　　**文献标志码**:A　　**文章编号**:1003-5060(2023)02-0285-04

On the construction of new optimal asymmetric quantum error-correcting codes

SUN Qilin,　WANG Liqi
(School of Mathematics, Hefei University of Technology, Hefei 230601, China)

Abstract: Asymmetric quantum error-correcting codes form an important class of quantum codes. Since the error probability of bit-flip is less than the error probability of phase reversal, quantum error correction should take into account the asymmetric quantum channel. In this paper, based on typical constacyclic codes over finite field, two classes of asymmetric quantum error-correcting codes are obtained according to the CSS construction. These asymmetric quantum error-correcting codes are new in the sense that their parameters are not covered by the codes available in the literature and they are also optimal due to the fact that they achieve the Singleton bound of asymmetric quantum error-correcting codes.

Key words: asymmetric quantum error-correcting code; constacyclic code; CSS construction; Singleton bound

0　引　　言

文献[1]给出了利用经典纠错码构造非对称量子纠错码的 CSS 构造法,并指出研究非对称量子纠错码的重要性,但没给出非对称的本质;文献[2]通过物理实验证明,量子比特翻转错误比量子相位翻转错误发生的概率大很多,由此引发了人们对非对称信道中的量子纠错码研究。学者们通过各种方法设计构造高性能的非对称量子纠错码,特别是 LDPC 码和 BCH 码被广泛应用于非对称量子纠错码的构造[3-5];文献[6]利用代数几何码构造非对称量子纠错码,并得到了一些参数较好的非对称量子纠错码;文献[7]在 F_4 上迹厄米特内积意义下,给出了加性码构造非对称量子纠错码的通用方法。此后,各种类型的新的非对称量子纠错码被构造出来[8-10]。文献[11]利用经典的负循环码构造了 2 类最优的非对称量子纠错码;文献[12]和文献[13]分别利用经典的常循环码构造了 6 类和 2 类最优的非对称量子纠错码;文献[14]利用经典的常循环码构造了 2 类长为

收稿日期:2022-01-19
基金项目:国家自然科学基金资助项目(12271137)
作者简介:孙麒麟(1995—),男,安徽合肥人,合肥工业大学硕士生;
王立启(1986—),男,安徽六安人,博士,合肥工业大学副教授,硕士生导师.

$(q^2+1)/5$ 的最优非对称量子纠错码;文献[15]利用准循环码构造了一些最优的非对称量子纠错码;文献[16]利用经典的常循环码构造了几类长为 $n=(q^2+1)/a$ 的新的量子 MDS 码。

受上述工作启发,本文通过 F_{q^2} 上的常循环码构造了 2 类长为 $n=(q^2+1)/a$ 的新的最优非对称量子纠错码,其中 q 为奇素数的方幂,$a=(m^2+1)/2$,$m\geqslant 3$ 为奇数。

1 基础知识

设 F_{q^2} 是含有 q^2 个元素的有限域,其中 q 是素数的方幂。给定任意向量

$$\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1}),$$

$$\boldsymbol{y}=(y_0,y_1,\cdots,y_{n-1})\in F_{q^2}^{n},$$

其厄米特内积定义为:

$$\langle \boldsymbol{x},\boldsymbol{y}\rangle = x_0y_0^q+x_1y_1^q+\cdots+x_{n-1}y_{n-1}^q\in F_{q^2}。$$

若 $\langle \boldsymbol{x},\boldsymbol{y}\rangle=0$,则称向量 $\boldsymbol{x},\boldsymbol{y}$ 关于厄米特内积正交。F_{q^2} 上参数为$[n,k]$的线性码 C 是 $F_{q^2}^{n}$ 的 k-维子空间。对于长为 n 的 q^2-元线性码 C,其厄米特对偶码定义如下:

$$C^{\perp_H}=\{\boldsymbol{x}\in F_{q^2}^{n}\mid \langle \boldsymbol{x},\boldsymbol{y}\rangle=0,\ \forall\, \boldsymbol{y}\in C\}。$$

若 F_{q^2} 上长为 n 的线性码 C 满足 $C\subseteq C^{\perp_H}$,则称 C 为厄米特自正交码。

若 F_{q^2} 上长为 n 的线性码 C 在 $F_{q^2}^{n}$ 上的 η-常循环码移位 $(c_0,c_1,\cdots,c_{n-1})\to(\eta\, c_{n-1},c_0,\cdots,c_{n-2})$ 下是不变的,则称 C 为 F_{q^2} 上的 η-常循环码,其中 η 是 F_{q^2} 中的非零元。每一个码字 $c=(c_0,c_1,\cdots,c_{n-1})$ 都等价于它的多项式 $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$,故在商环 $F_{q^2}[x]/\langle x^n-\eta\rangle$ 中,$xc(x)$ 对应于 $c(x)$ 的 η-常循环移位。众所周知,F_{q^2} 上长为 n 的线性码 C 是 η-常循环码当且仅当 C 是商环 $F_{q^2}[x]/\langle x^n-\eta\rangle$ 的理想。此外,易知 $F_{q^2}[x]/\langle x^n-\eta\rangle$ 是主理想环,它的理想是由 $x^n-\eta$ 的首一因子生成的,即 $C=\langle f(x)\rangle$,其中 $f(x)\mid(x^n-\eta)$。多项式 $f(x)$ 称为码 C 的生成多项式。码 C 的维数为 $n-k$,其中 $k=\deg(f(x))$。

引理 1(Singleton 界)[17] 设 C 是 F_{q^2} 上的 $[n,k,d]$ 线性码,则 $k\leqslant n-d+1$;特别地,若等号成立,则称其为 MDS 码。

容易验证,F_{q^2} 上 η-常循环码的厄米特对偶码 $C^{\perp_H}$ 是 η^{-q}-常循环码。设 ω 是 F_{q^2} 中的本原元。假定 $\gcd(n,q)=1$,取 $\eta=\omega^{q-1}$,从而有 $\eta\eta^q=1$,因此,F_{q^2} 上 η-常循环码的厄米特对偶码 $C^{\perp_H}$ 是 η-常循环码。η-常循环码存在确定其距离的 BCH 界。

引理 2(常循环码的 BCH 界)[18] 假设 $\gcd(q,n)=1$,设 $C=\langle g(x)\rangle$ 是 F_{q^2} 上长为 n 且 $g(x)$ 的根为 $\{\delta^{1+ir}\mid 0\leqslant i\leqslant d-2\}$ 的 η-常循环码,其中 δ 是 rn 次本原单位根,则 C 的极小距离至少为 d。

记 $\Omega=\{1+ir\mid 0\leqslant i\leqslant n-1\}$,对于任意的 $j\in\Omega$,令 C_j 是包含 j 的模 rn 的分圆陪集,则 $m_i(x)=\Pi_{h\in C_j}(x-\delta^h)$ 是 $x^n-\eta$ 在 F_{q^2} 上的首一不可约因子。每一个 C_j 对应 $x^n-\eta$ 在 F_{q^2} 上的一个不可约因子。设 C 是 F_{q^2} 上由多项式 $g(x)$ 生成的长为 n 的 η-常循环码,则集合 $Z=\{j\in\Omega\mid g(\delta^j)=0\}$ 称为 C 的定义集。显然 C 的定义集是模 rn 的 q^2-分圆陪集的并集,且 $\dim(C)=n-|Z|$。

下面给出非对称量子纠错码的定义和相关性质。

定义 1[2] 一个 q-元非对称量子纠错码 Q,记为 $[[n,k,d_z/d_x]]_q$,是希尔伯特空间 $\mathbf{H}$ 的一个 q^k 维子空间,其能纠正的量子比特翻转错误达到 $\lfloor (d_x-1)/2\rfloor$,能纠正的相位翻转错误达到 $\lfloor (d_x-1)/2\rfloor$。

定理 1(CSS 构造)[3-4] 设 C_i 是参数为 $[n,k_i,d_i]_{q^2}$ 的经典线性码,$i=1,2$。若 $C_1^{\perp_H}\subseteq C_2$,则存在一个参数为 $[[n,k_2+k_1-n,d_z/d_x]]_{q^2}$ 的非对称量子纠错码,其中:$d_z=wt(C_2\backslash C_1^{\perp_H})$;$d_x=wt(C_1\backslash C_2^{\perp_H})$。

对于一个参数为 $[[n,k_2,d_z/d_x]]_{q^2}$ 的 CSS 非对称量子纠错码,其参数 n、k、d_z 和 d_x 之间的关系有下面的结论。

定理 2[4] 若存在一个参数为 $[[n,k_2,d_z/d_x]]_{q^2}$ 的 CSS 非对称量子纠错码 Q,则 Q 满足非对称量子 Singleton 界,具体为:

$$k\leqslant n-d_z-d_x+2。$$

特别地,当 $k=n-d_z-d_x+2$ 时,称 Q 为最优码或非对称量子 MDS 码。

2 最优非对称量子纠错码的构造

本文将利用经典的常循环码构造 2 类长度为 $n=(q^2+1)/a$ 的最优非对称量子纠错码,其中 q 为奇素数的方幂,$a=(m^2+1)/2$,$m\geqslant 3$ 为奇数,易知此时 $a\mid(q+m)$ 或 $a\mid(q-m)$。以下分这 2 种情形进行讨论。

2.1 最优非对称量子纠错码的构造Ⅰ

本节讨论当 $a\mid(q+m)$ 时,最优非对称量子纠

错码的构造,先给出一个重要的引理。

引理 3[16]　设 q 是奇素数的方幂,$a|(q+m)$,$a=(m^2+1)/2$,$m\geqslant 3$ 为奇数,$n=(q^2+1)/a$,$k=(q^2+1)/2$。若 C 是 F_{q^2} 上长为 n 的 ω^{q-1} 常循环码,且其定义集为 $Z=\bigcup_{j=0}^{\delta} C_{k-(q+1)j}$,其中 $0\leqslant\delta\leqslant(mq-1)/2a-1$,则 $C^{\perp_H}\subseteq C$。

定理 3　设 q 是奇素数的方幂,$a|(q+m)$,$a=(m^2+1)/2$,$m\geqslant 3$ 为奇数,$n=(q^2+1)/a$,则存在参数为 $[[n,n-2(s+t+1),(2s+2)/(2t+2)]]_{q^2}$ 的非对称量子纠错码,其中 s、t 为正整数,且 $0\leqslant t\leqslant s\leqslant(mq-1)/2a-1$。

证明　设 $k=(q^2+1)/2$,C_2 是 F_{q^2} 上长为 $n=(q^2+1)/a$ 的 q^2-元 ω^{q-1}-常循环码,且其定义集为 $Z_2=\bigcup_{i=0}^{t} C_{k-(q+1)i}$,其中 $0\leqslant t\leqslant(mq-1)/2a-1$,则 C_2 的维数为 $n-(2t+1)$。注意到 Z_2 中包含 $2t+1$ 个连续整数

$$\{k-(q+1)t,\cdots,k-(q+1),k,k+(q+1),\cdots,k+(q+1)t\},$$

由引理 1 知,C_2 的极小距离至少为 $2t+2$。根据引理 2 可得,C_2 的极小距离为 $2t+2$。因此,C_2 是参数为 $[n,n-(2t+2),2t+2]_{q^2}$ 的 q^2-元 ω^{q-1}-常循环码。

假设 C_1 是 F_{q^2} 上长为 $n=(q^2+1)/a$ 的 q^2-元 ω^{q-1}-常循环码,且定义集为 $Z_1=\bigcup_{i=0}^{s} C_{k-(q+1)i}$,其中 $0\leqslant t\leqslant s\leqslant(mq-1)/2a-1$。与 C_2 的讨论相似,C_1 具有参数 $[n,n-(2s+2),2s+2]_{q^2}$。由定理 1 可知,存在参数为 $[[n,n-2(s+t+1),(2s+2)/(2t+2)]]_{q^2}$ 的非对称量子纠错码。

定理 3 中的非对称量子纠错码满足 $d_z+d_x=2s+2t+4=n-k+2$。由定理 2 可知,参数为 $[[n,n-2(s+t+1),(2s+2)/(2t+2)]]_{q^2}$ 的非对称量子纠错码达到非对称量子纠错码的 Singleton 界。因此这些非对称量子码是最优的。

例 1　设 $m=5$,$q=31$,则 $n=74$。假设 ω^{30}-常循环码 C_1 的定义集为 $Z_1=C_{481}=\{481\}$,则 C_1 是参数为 $[74,73,2]_{961}$ 的 MDS 码。假设 ω^{30}-常循环 C_2 的定义集为:

$$Z_2=C_{481}\cup C_{449}\cup C_{417}\cup C_{385}\cup C_{353}\cup C_{321}\cup C_{289}\cup C_{257}=\{481,289,321,353,385,417,449,481,513,609,641,673,705\},$$

则 C_2 是参数为 $[74,59,16]_{961}$ 的 MDS 码。由定理 3 可知,存在参数为 $[[74,58,16/2]]_{961}$ 的最优非对称量子纠错码。通过赋予 C_1 和 C_2 不同的定义集,得到最优非对称量子纠错码,见表 1 所列。

表 1　长为 74 的 961 元最优非对称量子纠错码

$[[n,k,d_z/d_x]]_{q^2}$	$[[n,k,d_z/d_x]]_{q^2}$	$[[n,k,d_z/d_x]]_{q^2}$
$[[74,72,2/2]]_{961}$	$[[74,60,12/4]]_{961}$	$[[74,54,14/8]]_{961}$
$[[74,70,4/2]]_{961}$	$[[74,58,14/4]]_{961}$	$[[74,52,16/8]]_{961}$
$[[74,68,6/2]]_{961}$	$[[74,56,16/4]]_{961}$	$[[74,56,10/10]]_{961}$
$[[74,66,8/2]]_{961}$	$[[74,64,6/6]]_{961}$	$[[74,54,12/10]]_{961}$
$[[74,64,10/2]]_{961}$	$[[74,62,8/6]]_{961}$	$[[74,52,14/10]]_{961}$
$[[74,62,12/2]]_{961}$	$[[74,60,10/6]]_{961}$	$[[74,50,16/10]]_{961}$
$[[74,60,14/2]]_{961}$	$[[74,58,12/6]]_{961}$	$[[74,52,12/12]]_{961}$
$[[74,58,16/2]]_{961}$	$[[74,56,14/6]]_{961}$	$[[74,50,14/12]]_{961}$
$[[74,68,4/4]]_{961}$	$[[74,54,16/6]]_{961}$	$[[74,48,16/12]]_{961}$
$[[74,66,6/4]]_{961}$	$[[74,60,8/8]]_{961}$	$[[74,48,14/14]]_{961}$
$[[74,64,8/4]]_{961}$	$[[74,58,10/8]]_{961}$	$[[74,46,16/14]]_{961}$
$[[74,62,10/4]]_{961}$	$[[74,56,12/8]]_{961}$	$[[74,44,16/16]]_{961}$

2.2　最优非对称量子纠错码的构造Ⅱ

本节讨论当 $a|(q-m)$ 时,最优非对称量子纠错码的构造,先给出一个重要的引理。

引理 4[16]　设 q 是奇素数的方幂,$a|(q-m)$,$a=(m^2+1)/2$,$m\geqslant 3$ 为奇数,$n=(q^2+1)/a$,$k=(q^2+1)/2$。若 C 是 F_{q^2} 上长为 n 的 ω^{q-1}-常循环码,且其定义集为 $Z=\bigcup_{j=0}^{\delta} C_{k-(q+1)j}$,其中 $0\leqslant\delta\leqslant(mq+1)/2a-1$,则 $C^{\perp_H}\subseteq C$。

类似定理 3 的讨论,可得如下结论。

定理 4　设 q 是奇素数的方幂,$a|(q-m)$,$a=(m^2+1)/2$,其中 $m\geqslant 3$ 为奇数。设 $n=(q^2+1)/a$,则存在参数为 $[[n,n-2(s+t+1),(2s+2)/(2t+2)]]_{q^2}$ 的非对称量子纠错码,其中 s,t 为正整数,且 $0\leqslant t\leqslant s\leqslant(mq+1)/2a-1$。

定理 4 中的非对称量子纠错码满足

$$d_z+d_x=2s+2t+4=n-k+2。$$

由定理 2 可知,参数为 $[[n,n-2(s+t+1),(2s+2)/(2t+2)]]_{q^2}$ 的非对称量子纠错码达到非对称量子纠错码的 Singleton 界,因此这些非对称量子纠错码是最优的。

例 2　设 $m=7$,$q=57$,则 $n=74$。假设 ω^{56}-常循环码 C_1 的定义集为 $Z_1=C_{1\,625}=\{1\,625\}$,则 C_1 是参数为 $[130,129,2]_{3\,429}$ 的 MDS 码。假设 ω^{56}-常循环码 C_2 的定义集为:

$$Z_2=C_{1\,625}\cup C_{1\,567}\cup C_{1\,509}\cup C_{1\,451}\cup C_{1\,393}\cup C_{1\,335}\cup C_{1\,227}\cup C_{1\,219}=\{1\,219,1\,227,1\,335,1\,393,1\,451,1\,509,1\,567,1\,625,1\,683,1\,741,1\,799,1\,857,1\,915,1\,973,2\,031\},$$

则 C_2 是参数为 $[130,115,16]_{3\,429}$ 的 MDS 码。由

定理 4 知,存在参数为$[[130,114,16/2]]_{3\,429}$的最优非对称量子码。通过赋予 C_1 和 C_2 不同的定义集,得到最优非对称量子纠错码,见表 2 所列。

表 2 长为 130 的 3 249 元最优非对称量子纠错码

$[[n,k,d_z/d_x]]_{q^2}$	$[[n,k,d_z/d_x]]_{q^2}$	$[[n,k,d_z/d_x]]_{q^2}$
$[[130,128,2/2]]_{3\,429}$	$[[130,116,12/4]]_{3\,429}$	$[[130,110,14/8]]_{3\,429}$
$[[130,126,4/2]]_{3\,429}$	$[[130,114,14/4]]_{3\,429}$	$[[130,108,16/8]]_{3\,429}$
$[[130,124,6/2]]_{3\,429}$	$[[130,112,16/4]]_{3\,429}$	$[[130,112,10/10]]_{3\,429}$
$[[130,122,8/2]]_{3\,429}$	$[[130,120,6/6]]_{3\,429}$	$[[130,110,12/10]]_{3\,429}$
$[[130,120,10/2]]_{3\,429}$	$[[130,118,8/6]]_{3\,429}$	$[[130,108,14/10]]_{3\,429}$
$[[130,118,12/2]]_{3\,429}$	$[[130,118,10/6]]_{3\,429}$	$[[130,106,16/10]]_{3\,429}$
$[[130,116,14/2]]_{3\,429}$	$[[130,114,12/6]]_{3\,429}$	$[[130,108,12/12]]_{3\,429}$
$[[130,114,16/2]]_{3\,429}$	$[[130,112,14/6]]_{3\,429}$	$[[130,106,14/12]]_{3\,429}$
$[[130,124,4/4]]_{3\,429}$	$[[130,110,16/6]]_{3\,429}$	$[[130,104,16/12]]_{3\,429}$
$[[130,124,6/4]]_{3\,429}$	$[[130,116,8/8]]_{3\,429}$	$[[130,104,14/14]]_{3\,429}$
$[[130,120,8/4]]_{3\,429}$	$[[130,114,10/8]]_{3\,429}$	$[[130,102,16/14]]_{3\,429}$
$[[130,118,10/4]]_{3\,429}$	$[[130,112,12/8]]_{3\,429}$	$[[130,100,16/16]]_{3\,429}$

3 结 论

本文利用有限域上 F_{q^2} 上的经典常循环码构造了 2 类长为 $n=(q^2+1)/a$ 的最优非对称量子纠错码,其中 q 为奇素数的方幂,$a=(m^2+1)/2$,$m\geqslant 3$ 为奇数。具体如下。

(1) 当 $a\mid(q+m)$时,存在参数为$[[n,n-2(s+t+1),(2s+2)/(2t+2)]]_{q^2}$的最优非对称量子纠错码,其中 $0\leqslant t\leqslant s\leqslant(mq-1)/2a-1$,$s$、$t$ 均为正整数。

(2) 当 $a\mid(q-m)$时,存在参数为$[[n,n-2(s+t+1),(2s+2)/(2t+2)]]_{q^2}$的最优非对称量子纠错码,其中 $0\leqslant t\leqslant s\leqslant(mq+1)/2a-1$,$s$、$t$ 均为正整数。

[参 考 文 献]

[1] STEANE A M. Simple quantum error correcting codes[J]. Physical Review A,1997,54(6):4741-4751.

[2] IOFFE L,MEZARD M. Asymmetric quantum error-correcting codes[J]. Physical Review A,2007,75(3):1-4.

[3] SARVEPALLI P K, KLAPPENECKER A, RÖTTELER M. Asymmetric quantum LDPC codes[C]//Proceedings International Symposium Information Theory. [S. l. :s. n.], 2008:6-11.

[4] ALY S A. Asymmetric quantum BCH codes[C]//Proceedings IEEE International Conference on Computer Engineering and Systems. [S. l. :s. n.],2008:157-162.

[5] LA GUARDIA G G. New families of asymmetric quantum BCH codes[J]. Quantum Information and Computation, 2011,11(3/4):239-252.

[6] WANG L,FENG K Q,LING S,et al. Asymmetric quantum codes:characterization and constructions[J]. IEEE Transactions on Information Theory,2010,56(6):2938-2945.

[7] EZERMAN M F, LING S, SOLÉ P. Additive asymmetric quantum codes[J]. IEEE Transactions on Information Theory,2011,57(8):5536-5550.

[8] LA GUARDIA G G. Asymmetric quantum Reed-Solomon and generalized Reed-Solomon codes[J]. Quantum Information Processing,2012,11:591-604.

[9] LA GUARDIA G G. Asymmetric quantum codes:new codes from odd[J]. Quantum Information Processing, 2013, 12: 2771-2790.

[10] LA GUARDIA G G. On the construction of asymmetric quantum codes[J]. International Journal of Theoretical Physics,2014,53(7):2312-2322.

[11] CHEN J Z,LI J P,LIN J. New optimal asymmetric quantum codes derived from negacyclic codes[J]. International Journal of Theoretical Physics,2014,53(1):72-79.

[12] WANG L Q,ZHU S X. On the construction of optimal asymmetric quantum codes[J]. International Journal of Quantum Information,2014,12(3):1-11.

[13] ZHANG G H,CHEN B C,LI L C. New optimal asymmetric quantum codes from constacyclic codes[J]. Modern Physics Letter B,2014,28(15):1-9.

[14] CHEN X J,ZHU S X,KAI X S. Two new classes of new optimal asymmetric quantum codes[J]. International Journal of Theoretical Physics,2018,57(6):1829-1838.

[15] LV J J,LI R H,YAO Y. Quasi-cyclic constructions of asymmetric quantum error-correcting codes[J]. Cryptography and Communications,2021,13(5):1-20.

[16] GUO G M,LI R H,GUO L B. On the construction of quantum MDS codes[J]. International Journal of Theoretical Physics,2018,57:3525-3539.

[17] MACWILLIAMS F J,SLOANE N J A. The theory of error-correcting codes[M]. Amsterdam:North Holland Publishing Co. ,1977:317-331.

[18] KAI X S,ZHU S X,LI P. Constacyclic codes and some new quantum MDS codes[J]. IEEE Transactions on Information Theory,2014,60(4):2080-2085.

(责任编辑 朱晓临)