利用射影Cap构造极大纠缠的纠缠辅助量子纠错码

李瑞虎， 付 强， 郭罗斌
(空军工程大学理学院，陕西西安，710051)

摘要 依据经典四元线性码理论和纠缠辅助量子纠错码理论，由四元线性码的生成矩阵给出四元线性码稳定极大纠缠的纠缠辅助量子码的几何特征。在给定几何特征基础上，由射影空间的Cap理论，设法用组合数学方法和搜索算法构造出给定几何特征的Cap，确定Cap码的参数。利用所得到的参数优良的Cap码，结合纠缠理论，构造出一些参数优良的极大纠缠的纠缠辅助量子码。其中，所构造的极大纠缠的纠缠辅助量子码有许多是最优码，还有一些纠缠辅助量子码改进了前人所得到的纠缠辅助量子码的参数，这些纠缠辅助量子纠错码是无法用已有方法得到的。这也证明了结合组合与搜索的方法来构造极大纠缠的纠缠辅助量子纠错码是有效的。

关键词 EAQECC；极大纠缠；射影空间；Cap；最优码
DOI 10.3969/j.issn.1009-3516.2014.05.018
中图分类号 O157.4 **文献标志码** A **文章编号** 1009-3516(2014)05-0080-04

Construction of Entanglement-assisted Quantum Codes with Maximal Entanglement from Projective Caps

LI Rui-hu, FU Qiang, GUO Luo-bin
(Science College, Air Force Engineering University, Xi′an 710051, China)

Abstract: According to the entanglement-assisted quantum error-correcting code (EAQECC) theory, a geometry character of a quaternary linear code stabilized a maximal entanglement EAQECC is presented. On the basis of this character and the theory of Cap in projective space, methods for constructing such Caps by combinational mathematics and search algorithm are designed, and good codes from such Caps are determined. Many maximal entanglement EAQECCs are constructed from these obtained Cap codes. Almost all the maximal entanglement EAQECCs constructed here are optimal or near optimal EAQECCs, and some of them are the improved parameters of EAQECCs previously known; and some of them are new ones, but are very difficult to be obtained by using the known methods.

Key words: EAQECC; maximal entanglement; projective space; Cap; optimal code

自从Shor和Steane于1995～1996年创立量子纠错码理论以来[1-2]，量子纠错码得到快速发展。量子纠错码的稳定子理论使得人们可以用满足对偶包含关系(或自正交)的经典码构造量子码，所得到的量子码叫做标准量子纠错码[3]。当经典码不满足对偶包含关系时，则不能用于构造标准量子码，这就

收稿日期：2014-02-27
基金项目：国家自然科学基金资助项目(11471011；11071255)
作者简介：李瑞虎(1966－)，男，安徽亳州人，教授，博士生导师，主要从事代数编码及密码研究.E-mail：liruihu@aliyun.com

引用格式：*李瑞虎，付 强，郭罗斌. 利用射影Cap构造极大纠缠的纠缠辅助量子纠错码[J]. 空军工程大学学报：自然科学版，2014，15(5)：80-83. LI Ruihu, FU Qiang, GUO Luobin.Construction of entanglement-assisted quantum codes with maximal entanglement from projective caps [J]. Journal of air force engineering university：natural science edition，2014，15(5)：80-83.*

限制了经典纠错码在量子编码领域的应用。2006 年 Brun 等人利用通信双方共享的纠缠比特对作为辅助资源,创立纠缠辅助量子纠错码(简记为 EAQECC)理论[4-6],相应的纠缠辅助稳定子称为 EA-稳定子;在此理论框架之下,标准量子码是纠缠辅助量子码的特例——纠缠比特数为零的 EAQECC。EAQECC 可由任意经典线性码构造出来,这极大地方便了人们将经典码转化为量子码。近年来的研究表明,纠缠能够改进量子码的码率和纠错能力,极大纠缠 EAQECC 能够达到量子信道容量[7]。

Cap 是射影几何的重要研究对象,与编码以及组合数学有密切联系,射影空间的 1 个 Cap 可以确定 2 个经典码[8]。近年来,人们发现可以用射影空间的特殊 Cap 构造性能优越的标准量子码[8]。受文献[6~8]的启发,本文研究能够用于构造极大纠缠 EAQECC 的射影 Cap 的特征,设法构造出相应的射影 Cap 和极大纠缠 EAQECC。

1　预备知识

本节介绍本文需要的基本概念,确定能够稳定极大 EAQECC 的经典四元码的几何特征,为构造极大纠缠 EAQECC 做好准备。

设 $F_4=\{0,1,\omega,\bar{\omega}\}$ 为四元域,$\bar{\omega}^2=\omega$,任意 $x\in F_4$ 的共轭元 $\bar{x}=x^2$。为了方便,用 2 和 3 表示 ω 和 $\bar{\omega}$。用 ${}^nF_4$ 表示 F_4 上 n 维向量空间。F_4^n 的 k 维子空间 C 叫 F_4 上 k 维线性码,记为 $C=[n,k]_4$。若 $x,y\in F_4$,则 x,y 的 Hermite 内积定义为:

$$(x,y)_h=x_1\bar{y}_1+x_2\bar{y}_2+\ldots+x_n\bar{y}_n=\sum_{i=1}^{i=n}x_i\bar{y}_i$$

码 C 的对偶码 $C^{\perp_h}=\{x\mid(x,y)_h=0,\forall y\in C\}$。

记 F_4 上 $k-1$ 维射影空间为 $PG(k-1,4)$,每个 k 维非零列向量叫做射影点,2 个平行的 k 维非零列向量对应同一个射影点。

定义 1.1[8-9] $PG(k-1,4)$ 的 n 个点的点集 K 叫一个 n-Cap,指 K 中任意 3 个点都线性无关。由 n-Cap K 的点排列起来构成的 $k\times n$ 矩阵记为 $\boldsymbol{G}(K)$,$\boldsymbol{G}(K)$ 生成的码 $C(K)$ 叫做 Cap 码,以 $\boldsymbol{G}(K)$ 为校验矩阵的码 $C^{\perp_h}(K)=[n,n-k,4]_4$ 码。

2013 年 Brun, Lai 与 Wilde 研究了最优 EAQECC 及最优极大纠缠 EAQECC 的距离问题。一个 EAQECC $[[n,k,d;c]]$ 叫做最优是指给定 n,k,c 时 d 取得最大值;如果 $k+c=n$,则 $[[n,k,d;c]]$ 的 EAQECC 叫做极大纠缠 EAQECC。

Brun 等人[7] 首先研究特殊最优极大纠缠 EAQECC 问题,证明以下结论:n 为奇数时,存在 $[[n,1,n;n-1]]$ 最优最大纠缠 EAQECC,其对偶码为 $[[n,n-1,2;1]]$ 最大纠缠 EAQECC;n 为偶数时,不存在 $[[n,1,n;n-1]]$ 极大纠缠 EAQECC,最优极大纠缠 EAQECC 为 $[[n,1,n;n-1]]$,其对偶码为 $[[n,n-1,1;1]]$ 极大纠缠 EAQECC。他们确定了 $n\leqslant 15$ 时最优极大纠缠 EAQECC 的距离和可能的界。

引理 1[10]:若 $C=[n,k,d]_4$ 的校验矩阵为 $\boldsymbol{H}$,$\boldsymbol{H}^+$ 是 $\boldsymbol{H}$ 的共轭转置,则由 $C^{\perp_h}$ 稳定的 EAQECC 为 $[[n,2m+c-n,d;c]]$。

为了用 Cap 构造极大纠缠 EAQECC,首先确定四元码稳定极大纠缠 EAQECC 的几何特征。

定理 1　若 $C=[n,k,d]_4$ 的生成矩阵为 $\boldsymbol{G}$,$\boldsymbol{G}^+$ 是 $\boldsymbol{G}$ 的共轭转置,则以 C 稳定最大纠缠 EAQECC 的充要条件 $\boldsymbol{G}\boldsymbol{G}^+$ 是四元满秩矩阵。

证明:1)设 $\boldsymbol{G}\boldsymbol{G}^+$ 是四元满秩矩阵,则由 C 稳定的 EAQECC 的参数为 $[[n,2(n-m)-n+m,d^\perp;m]]=[[n,n-m,d^\perp;m]]$,为极大纠缠 EAQECC,该 EAQECC 的对偶码 $[[n,m,d;n-m]]$ 即为 $C^{\perp_h}$ 稳定的 EAQECC,$[[n,m,d;n-m]]$ 也是极大纠缠的,故充分性成立。

2)设 $\boldsymbol{G}\boldsymbol{G}^+$ 的秩为 r,则由 C 稳定的 EAQECC 的参数为 $[[n,2(n-m)-n+r,d^\perp;r]]=[[n,n-2m+r,d^\perp;r]]$,由 $C^{\perp_h}$ 稳定的 EAQECC $[[n,r,d;n-2m+r]]$。使这 2 个 EAQECC 为极大纠缠的必有 $n-2m+2r=n$,则 $m=r$,从而可以证明必要性。

2　基于射影 Cap 的极大纠缠的 EAQECC

2.1　基于 $PG(3,4)$ 中 Cap 的极大纠缠的 EAQECC 构造

由(13321033012331000000)循环生成的 4×17 矩阵 $\boldsymbol{G}_{4\times 17}$ 构成 17-Cap,这是 $PG(3,4)$ 中最大 Cap。该 Cap 生成的码为自正交码,可用于构造标准量子码,但是不能用来构造极大纠缠的 EAQECC。删截 $\boldsymbol{G}_{17}$ 可得到 13-Cap,12-Cap,11-Cap,10-Cap,…,7-Cap,这些 Cap 能用来构造极大纠缠的 EAQECC。这些 n-Cap 对应的码的距离 $d=n-5$。除 13-Cap,12-Cap, 11-Cap 的码为最优码外,其余 Cap 码为拟最优码。删截 $\boldsymbol{G}_{17}$ 的第 1,2,3,4 列得到 13-Cap,删截第 1,2,3,4,5 列得到 12-Cap,删截第 1,2,3,4,5,6 列得到 11-Cap。

利用随机搜索算法得到 10-Cap,其最优码为:

$$\boldsymbol{G}_{10}=\begin{pmatrix}0011011111\\0102021133\\1223113113\\0000111223\end{pmatrix}$$

删截 $\boldsymbol{G}_{10}$的第 1 列得到 9-Cap,删截第 1,4 列得到 8-Cap,删截第 1,4,7 列得到 7-Cap,删截第 1,2,3,4 列得到 6-Cap;这些 n -Cap 满足**定理** 1 且对应码的距离 $d=n-4$。

总结以上 n -Cap 的讨论,可得到如下极大纠缠的 EAQECC:

定理 2 若 6≤n≤13,则有$[[n,n-4,4;4]]$极大纠缠的 EAQECC,$[[n,4,n-4;n-4]]$ $(6\leqslant n\leqslant 10)$ 以及 $[[n,4,n-5;n-4]]$ $(11\leqslant n\leqslant 13)$ 极大纠缠的 EAQECC。

2.2 基于 $PG(4,4)$ 中 Cap 的极大纠缠的 EAQECC 构造

Bierbraue 和 Edel[8]证明了在 $PG(4,4)$里,最大的完备 Cap 是 41-Cap,存在 2 个不等价的 41-Cap,其中一个 Cap 的码是自正交码,另一个不是,却不满足**定理** 1 的条件。删截自正交 41-Cap,得到 Cap 码的参数都不好。不自正交的 41-Cap 矩阵 $\boldsymbol{G}_{41}$满足 $\boldsymbol{G}_{41}\boldsymbol{G}_{41}{}^{+}$的秩为 1,$\boldsymbol{G}_{41}$如下:

$$\begin{pmatrix}10000213010223333122103103230321021023032\\01000132101013221322010121332022301101303\\00100303223220123321330101023302112102012\\00010032111103331223101030223133210010212\\00001130331132032231021013303320332120102\end{pmatrix}$$

删截 $\boldsymbol{G}_{41}$得到满足**定理** 1 的 n -Cap $(14\leqslant n\leqslant 37)$,这里省略删截过程,仅列出相应 n -Cap 码$[n,5,d]$的码长和距离,见表 1,表中 d 为黑体的可以得到改进。

表 1 由 $\boldsymbol{G}_{41}$删截得到的 Cap 码参数(秩($\boldsymbol{GG}^{+}$)=5)

Tab.1 Cap code parameter of $\boldsymbol{G}_{41}$ ($(\boldsymbol{GG}^{+})=5$)

n	d	n	d	n	d
14	7	22	13	30	19
15	**7**	23	14	31	19
16	**8**	24	14	32	20
17	9	25	15	33	21
18	**9**	26	**15**	34	22
19	**10**	27	**16**	35	23
20	**11**	28	17	36	23
21	12	29	18	37	24

利用搜索算法,本文得到如下满足**定理** 1 的 n-Cap$(n=20,26,27)$。

$$\boldsymbol{G}_{20}=\begin{pmatrix}10021302231010101111\\00013210121101112100\\01030322211310123002\\00003211031012020323\\00113031302202002211\end{pmatrix}$$

$$\boldsymbol{G}_{26}=\begin{pmatrix}10000213010223310011111110\\01000132101013201111033111\\00100303223220122102330113\\00010032111103323030121103\\00001130331132010312021212\end{pmatrix}$$

$$\boldsymbol{G}_{27}=\begin{pmatrix}10000102233111011101010021 3\\01001010132120132211101013 2\\00102232201322001013230030 3\\00011111033133221322213003 2\\00003311320002221213011113 0\end{pmatrix}$$

这 3 个 Cap 码的参数分别为$[20,5,12]$,$[26,5,16]$,$[27,5,17]$。删截 $\boldsymbol{G}_{26}$可得到满足**定理** 1 的 n -Cap $(n=15,16,18,19)$,其中删截 $\boldsymbol{G}_{26}$的第 17,21-26 列得到 19-Cap,删截 $\boldsymbol{G}_{26}$第 17,20-26 列得到 18-Cap,删截 $\boldsymbol{G}_{26}$第 11,13-15,17,18,21,22,24,25 列可得到 16-Cap,删截 $\boldsymbol{G}_{26}$第 13-15,17,19～22,24～26 列得到 15-Cap。这些 n-Cap 码的参数分别为$[19,5,11]$,$[18,5,10]$,$[16,5,9]$,$[15,5,8]$。

总结以上关于 $PG(4,4)$中 n-Cap 的讨论,可得到如下极大纠缠的 EAQECC。

定理 3 1)若 $14\leqslant n\leqslant 37$,则有$[[n,n-5,4;5]]$极大纠缠的 EAQECC。

2)存在如下参数的极大纠缠的 EAQECCs $[[n,5,n-7;n-5]]$ $(14\leqslant n\leqslant 16)$,$[[n,5,n-8;n-5]]$ $(17\leqslant n\leqslant 19)$,$[[n,5,n-9;n-5]]$ $(20\leqslant n\leqslant 23)$,$[[n,5,n-10;n-5]]$ $(24\leqslant n\leqslant 27)$,$[[n,5,n-11;n-5]]$ $(28\leqslant n\leqslant 30)$,$[[n,5,n-12;n-5]]$ $(31\leqslant n\leqslant 35)$以及 $[[n,5,n-13;n-5]]$ $(36\leqslant n\leqslant 37)$极大纠缠的 EAQECCs。

利用纠缠辅助量子 Hamming 界和文献[7],可判断以上极大纠缠的 EAQECC 的最优性。

推论:1)若 $6\leqslant n\leqslant 13$,则极大纠缠的 EAQECC $[[n,n-4,4;4]]$为最优码;若 $14\leqslant n\leqslant 37$,则其构造的极大纠缠 EAQECC $[[n,n-5,4;5]]$为最优码。

2)若 $6\leqslant n\leqslant 10$,则极大纠缠的 EAQECC$[[n,4,n-4;n-4]]$为最优码;若 $11\leqslant n\leqslant 13$,则极大纠缠的 EAQECC $[[n,4,n-5;n-4]]$为最优码。

3)设 $n=15,16,18,19,20,26,27$,则**定理** 3(2)给出的极大纠缠的 EAQECC $[[n,5,d;n-5]]$为最优码。若 $14\leqslant n\leqslant 37$ 且 $n\leqslant 15,16,18,19,20,24,26,27$,则**定理** 3(2)给出的极大纠缠的 EAQECC

$[[n,5,d;n-5]]$为拟最优码。

证明:1)由文献[7]的表 1 可知:当 $6\leqslant n\leqslant 13$ 时,极大纠缠的 EAQECC$[[n,n-4,4;4]]$为最优码;$14\leqslant n\leqslant 15$ 时,极大纠缠的 EAQECC$[[n,n-5,4;5]]$为最优码。易验证 $16\leqslant n\leqslant 37$ 时,有 $1+3n+9n(n-1)>2^{n+5-(n-5)}$ 成立,由纠缠辅助量子 Hamming 界可推出$[[n,n-5,5;5]]$极大纠缠的 EAQECC 不存在,所以当 $16\leqslant n\leqslant 37$ 时,极大纠缠的 EAQECC $[[n,n-5,4;5]]$为最优码。从而推论 1)得证。

2)由文献[7]的表 1 可知,推论 2)中所有极大纠缠的 EAQECC 的距离都达到最优码距离的上界,故为最优码。

3)$14\leqslant n\leqslant 37$ 且 $n\neq 24$,对**定理** 3 中 2)给出的极大纠缠的 EAQECC $[[n,5,d;n-5]]$,利用纠缠辅助量子 Hamming 界,可逐一验证$[[n,5,d+2;n-5]]$极大纠缠的 EAQECC 不存在,故相应的极大纠缠的 EAQECC $[[n,5,d;n-5]]$至少是拟最优码。然后再验证 $n=15,16,18,19,20,26,27$ 时,极大纠缠的$[[n,5,d+1;n-5]]$ EAQECC 也不存在,从而证得 $n=15,16,18,19,20,26,27$ 时的极大纠缠的 EAQECC 为最优码。

3　讨论和结论

本文利用射影空间 $PG(3,4)$和 $PG(4,4)$里的特殊 Cap,构造了一些码长为 $6\leqslant n\leqslant 37$ 的极大纠缠的 EAQECC*s*;除$[[24,5,14;19]]$外,其余极大纠缠的 EAQECC*s* 都是拟最优码或最优码。其中极大纠缠的 EAQECC$[[12,4,7;8]]$,$[[13,4,8;9]]$,$[[14,5,7;9]]$ 分别改进了文献[7]得到的$[[12,4,6;8]]$,$[[13,4,7;9]]$,$[[14,5,6;9]]$;码长 $16\leqslant n\leqslant 37$ 的极大纠缠的 EAQECC,则是新的 EAQECC,是用文献[5]中优化算法难以构造的。本文构造的极大纠缠的 EAQECC$[[n,4,d;n-4]]$的码长 $n\leq 13$,$[[n,5,d;n-5]]$的码长 $n\leqslant 37$,至于构造码长更大的$[[n,4,d;n-4]]$和$[[n,5,d;n-5]]$极大纠缠的 EAQECCs,还需要探索新的方法。

参考文献(References):

[1] Shor P W. Scheme for reducing decoherence in quantum computer memory[J]. Phys rev a, 1995, 52: 2493-2396.

[2] Steane A M. Error correcting codes in quantum theory[J]. Phys rev lett, 1996, 77: 793-797.

[3] 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: 1369-1387.

[4] Brun T, Devetak I, Hsieh M H. Correcting quantum errors with entanglement[J]. Science, 2006, 314: 436-439.

[5] Lai C Y, Brun T A. Entanglement increases the error-correcting ability of quantum error-correcting codes [J]. Phys rev a, 2013, 88: 012320.

[6] Lai C Y, Brun T A, Wilde M M. Duality in Entanglement-assisted quantum error correction[J]. IEEE trans inf theory, 2013, 49: 4020-4024.

[7] Lai C Y, Brun T A, Wilde M M. Dualities and identities for entanglement-assisted quantum codes [J]. Quantum information processing, 2014, 13, 957-999.

[8] Edel Y, Bierbrauer J. 41 is the largest size of a cap in *PG* (4,4) [J]. Des codes crypt, 1999, 59: 151-160.

[9] Tonchev V. Quantum codes from caps[J]. Discrete mathematics, 2008, 308: 368-6372.

[10] Wilde M M, Brun T A. Optimal entanglement formulas for entanglement-assisted quantum coding[J]. Phys rev a, 2008, 77: 064302.

(编辑:徐敏)