新纠缠辅助量子MDS码的构造

汪 盼,王立启*,朱士信
(合肥工业大学数学学院,安徽合肥 230000)

摘 要: 纠缠辅助量子纠错码是经典量子纠错码的推广,通过在接收者和发送者双方预先共享纠缠态的方式实现量子通信. 由于预先共享纠缠态会造成额外的费用,如何构造具有较小预先共享纠缠态的纠缠辅助量子纠错码是一个有趣的问题. 本文给出了有限域F_{q^2}上一类负循环码是厄米特对偶包含码的充分条件,通过研究其分圆陪集的结构性质,确定了不同数目的预先共享纠缠态的存在条件,并结合纠缠辅助量子纠错码的构造方法,构造了一些新的具有较小预先共享纠缠态的纠缠辅助量子Maximum-Distance-Separable(MDS)码.

关键词: 分圆陪集;负循环码;纠缠辅助量子纠错码;MDS码
基金项目: 国家自然科学基金(No.12271137,No.U21A20428,No.12171134)
中图分类号: O157.4;TN911.22 **文献标识码:** A **文章编号:** 0372-2112(2024)01-0288-10
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220819

Construction of New Entanglement-Assisted Quantum MDS Codes

WANG Pan, WANG Li-qi*, ZHU Shi-xin
(*School of Mathematics*, *Hefei University of Technology*, *Hefei*, *Anhui* 230000, *China*)

Abstract: Entanglement-assisted quantum error-correcting codes are the generalization of classical quantum error-correcting codes, which realize quantum communication by using pre-shared entangled states between the receiver and the sender. It is an interesting problem to construct entanglement-assisted quantum error-correcting codes with small pre-shared entangled states because of the extra cost of pre-shared entangled states. In this paper, a sufficient condition for a class of negacyclic codes over finite fields to be Hermitian dual-containing codes is given. Then based on the structural properties of cyclotomic cosets, the existence conditions of different number of pre-shared entangled states are determined, and some new entanglement-assisted quantum maximum-distance-separable (MDS) codes with small pre-shared entangled states are obtained by using the construction method of entanglement-assisted quantum error-correcting codes.

Key words: cyclotomic coset; negacyclic codes; entanglement-assisted quantum error-correcting codes; maximum-distance-separable (MDS) codes
Foundation Item(s): National Natural Science Foundation of China (No.12271137, No.U21A20428, No.12171134)

1 引言

量子纠错码已被证明是克服量子信道噪声最有效的编码方案之一. 量子纠错码理论研究的一个重要问题是高性能量子纠错码的构造. 量子纠错码的现有构造均要求经典纠错码满足对偶包含条件[1],然而高效的现代码,如LDPC码(Low-Density Parity-Check codes)、Turbo码,其对偶包含判定难度较大,从而限制了量子纠错码的发展. 2006年,Brun等人[2]提出了通过在接收端和发送端预先共享纠缠态的码——纠缠辅助量子纠错码. 该类码一方面与同长度的经典量子纠错码相比,具有更大的最小距离;另一方面,可以由任意的经典码来构造. 同时,他们还建立了纠缠辅助量子纠错码的Singleton界. 基于纠缠辅助量子纠错码的优点,学者们开始关注纠缠辅助量子纠错码的构造. 文献[3,4]利用

收稿日期:2022-07-14;修回日期:2022-10-24;责任编辑:朱梅玉
*通讯作者:王立启

经典线性码构造了很多参数较优的纠缠辅助量子纠错码.

虽然纠缠辅助量子纠错码可以由任意经典码构造得到,但预先共享纠缠态数目的确定仍然是困难的.李瑞虎等人[5]设计了一种新的确定预先共享纠缠态数目的方案,并获得了几类好的纠缠辅助量子纠错码.Guenda等人[6]得到了从经典码构造纠缠辅助量子纠错码所需的最大纠缠态数目与经典码的Hull之间的关系,并构造了一些具有灵活参数的纠缠辅助量子纠错码.进一步地,文献[7~10]通过计算广义RS码和Goppa码的Hull维数,构造了许多纠缠辅助量子MDS码.

常循环码具有严谨的代数结构并且编译码电路简单,容易实现.因此,它被应用于纠缠辅助量子纠错码的构造,并成为构造纠缠辅助量子纠错码的一类重要码源.2014年,Lü等人[11]利用循环码定义集的分解来确定预先共享纠缠态的数目c,将c的确定转化为确定BCH码的定义集的一个子集所含元素个数,同时也构造了一些具有较大最小距离的纠缠辅助量子纠错码.随后,Lu等人[12]和Chen等人[13]分别将循环码定义集的分解推广到常循环码上,并构造了一些新的纠缠辅助量子MDS码.此后,基于此方法,许多长度整除$q^2\pm1$的纠缠辅助量子MDS码通过常循环码构造出来[14~21].

本文将利用有限域F_{q^2}上码长为$n=(q^2-1)/a$的负循环码来构造纠缠辅助量子纠错码.其中,$q=am\pm l$,$a=(l^2-1)/3$为偶数,m为正整数.首先通过选取合适的定义集,分别给出了负循环码是厄米特对偶包含码的充分条件;进一步地,得到了不同预先共享纠缠比特数的存在条件;最后,构造了一些新的纠缠辅助量子MDS码.

2　预备知识

设q是奇素数的方幂,F_{q^2}是含有q^2个元素的有限域.设n为正整数,$F_{q^2}^n$的任意一个k维线性子空间$\mathcal{C}$称作码长为n且维数为k的q^2-元线性码,记作$[n,k]$,并将$\mathcal{C}$中的向量称之为码字.设$\boldsymbol{x},\boldsymbol{y}\in F_{q^2}^n$,向量$\boldsymbol{x}$的汉明重量记作$\mathrm{wt}(\boldsymbol{x})$,定义为其非零分量的个数;向量$\boldsymbol{x}$和$\boldsymbol{y}$的汉明距离记作$\mathrm{dist}(\boldsymbol{x},\boldsymbol{y})$,定义为$\boldsymbol{x}-\boldsymbol{y}$的汉明重量,即$\mathrm{dist}(\boldsymbol{x},\boldsymbol{y})=\mathrm{wt}(\boldsymbol{x}-\boldsymbol{y})$.一个$q^2$-元$[n,k]$线性码$\mathcal{C}$的最小汉明距离定义为:$\min\{\mathrm{dist}(\boldsymbol{x},\boldsymbol{y})|\boldsymbol{x},\boldsymbol{y}\in\mathcal{C},\boldsymbol{x}\neq\boldsymbol{y}\}=\min\{\mathrm{wt}(\boldsymbol{x})|\boldsymbol{x}\in\mathcal{C},\boldsymbol{x}\neq0\}$.

码长为n、维数为k和最小汉明距离为d的q^2-元线性码,记作$[n,k,d]$.给定两个向量$\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$,$\boldsymbol{y}=(y_0,y_1,\cdots,y_{n-1})\in F_{q^2}^n$,定义其厄米特内积为

$$(\boldsymbol{x},\boldsymbol{y})_h=x_0{}^q y_0+x_1{}^q y_1+\cdots+x_{n-1}{}^q y_{n-1}.$$

若$(\boldsymbol{x},\boldsymbol{y})_h=0$,则称$\boldsymbol{x},\boldsymbol{y}$是正交的.码长为$n$的$q^2$-元线性码$\mathcal{C}$的厄米特对偶码为

$$\mathcal{C}^{\perp_h}=\{\boldsymbol{x}\in F_{q^2}^n|(\boldsymbol{x},\boldsymbol{y})_h=0,\forall\boldsymbol{y}\in\mathcal{C}\}.$$

当$\mathcal{C}^{\perp_h}\subseteq\mathcal{C}$时,码$\mathcal{C}$称为厄米特对偶包含码;当$\mathcal{C}^{\perp_h}=\mathcal{C}$时,$\mathcal{C}$称为厄米特自对偶码.

假设码$\mathcal{C}$是F_{q^2}上码长为n的线性码,若码$\mathcal{C}$中任意一个码字的负循环移位依然是码$\mathcal{C}$中的一个码字,即对任意$(c_0,c_1,\cdots,c_{n-1})\in\mathcal{C}$,有$(-c_{n-1},c_0,\cdots,c_{n-2})\in\mathcal{C}$,则称$\mathcal{C}$是$F_{q^2}$上的负循环码.通常,$\mathcal{C}$中任意码字$(c_0,c_1,\cdots,c_{n-1})$亦可用多项式表示为$c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}$.此时,易知$\mathcal{C}$是$F_{q^2}$上的负循环码当且仅当$\mathcal{C}$是商环$\mathcal{R}=F_{q^2}[x]/<x^n+1>$的理想.事实上,$F_{q^2}[x]/<x^n+1>$是主理想环,从而存在唯一的多项式$g(x)\in F_{q^2}[x]$,使$g(x)|(x^n+1)$且$\mathcal{C}=<g(x)>$,$g(x)$称为码$\mathcal{C}$的生成多项式,并且码$\mathcal{C}$的维数$\dim(\mathcal{C})=n-k$,其中,$k=\deg(g(x))$.

假设$\gcd(n,q)=1$,设$\beta\in F_{q^{2m}}$是$2n$次本原单位根,其中m是q^2模$2n$的乘法阶,即$\mathrm{ord}_n(q^2)=m$.令$\xi=\beta^2$,则ξ是n次本原单位根.因此,$x^n+1=\prod_{j=0}^{n-1}(x-\beta\xi^j)=\prod_{j=0}^{n-1}(x-\xi^{1+2j})$.

令$Z_{2n}=\{0,1,\cdots,2n-1\}$,$\Omega$是$Z_{2n}$中具有$1+2j$形式的元素构成的集合,称$T=\{s\in\Omega|g(\beta^s)=0\}$为负循环码$\mathcal{C}$的定义集.对任意$s\in Z_{2n}$,包含元素$s$的$q^2$-元分圆陪集为$C_s=\{s,sq^2,sq^4,\cdots,sq^{2(m_s-1)}\}$,其中,$m_s$为满足$sq^{2m_s}\equiv s\pmod{2n}$的最小正整数.

负循环码的最小汉明距离存在如下经典的BCH界.

定理1[22]　负循环码的BCH界　设$\mathcal{C}$是有限域F_{q^2}上码长为n的负循环码,$\gcd(n,q)=1$,$\beta\in F_{q^{2m}}$是$2n$次本原单位根.若$\mathcal{C}$的生成多项式$g(x)$的根为$\{\xi^{1+2j}|0\leqslant j\leqslant\delta-2\}$,则码$\mathcal{C}$的最小汉明距离大于或等于$\delta$.

设F_{q^2}上码长为n的负循环码$\mathcal{C}$的定义集为$T=\bigcup_{i=0}^{\delta-2}C_{1+2i}=\bigcup_{s\in\Omega}C_s$,亦称$\mathcal{C}$为设计距离为$\delta$的负循环BCH码.若$2n-qs\pmod{2n}\in C_s$,则称分圆陪集$C_s$是斜对称的;否则称其为斜非对称的.非对称的分圆陪集C_s与C_{2n-qs}成对出现,叫作斜非对称偶,简记为(C_s,C_{2n-qs}).下面给出负循环码$\mathcal{C}$是厄米特对偶包含码的经典判定定理.

引理1[23]　设$\mathcal{C}$是有限域F_{q^2}上码长为n,定义集为$T=\bigcup_{i=0}^{\delta-2}C_{1+2i}=\bigcup_{s\in\Omega}C_s$的负循环码,则$\mathcal{C}^{\perp_h}\subseteq\mathcal{C}$当且仅当以

下条件之一成立：

（1）$T\cap T^{-q}=\varnothing$，其中，$T^{-q}=\{2n-qs|s\in T\}$.

（2）T中每个C_i为斜非对称的，且C_i和C_j不构成斜非对称偶，其中，$0\leqslant i,j\leqslant\delta-2$.

为了构造码长$n\leqslant q^2-1$的纠缠辅助量子纠错码，我们首先介绍$\mathcal{C}$的定义集T的分解和相关结论.

定义 1[5] 设$\mathcal{C}$是有限域F_{q^2}上码长为n，定义集为T的负循环码，假设$T_{ss}=T\cap T^{-q}$且$T_{sas}=T\backslash T_{ss}$，其中，$T^{-q}=\{2n-qs|s\in T\}$，则$T=T_{ss}\cup T_{sas}$称为$T$的分解.

引理 2[5] 若码$\mathcal{C}$的定义集为T，T的分解如定义 1 所述. 那么：

（1）若$i,j\in T_{sas}$，则C_i为斜非对称的，且C_i和C_j不构成斜非对称偶.

（2）若$l\in T_{ss}$，则C_l是斜对称，或C_l为斜非对称的且存在$p\in T_{ss}$，使C_l和C_p构成斜非对称偶.

构造纠缠辅助量子纠错码的一个关键点是确定预先共享纠缠态的数目c，有了上述结论，可以轻易地确定其取值如下.

引理 3[12] 若码$\mathcal{C}$的定义集为T，T的分解如定义 1 所述. 则预先共享纠缠态的数目$c=|T_{ss}|$.

下面给出利用负循环码构造纠缠辅助量子纠错码的方法.

定理 2[12] 设码$\mathcal{C}$是参数为$[n,k,d]$且定义集为T的q^2-元负循环码，T的分解如定义 1 所述. 则存在参数为$\left[\left[n,n-2|T|+|T_{ss}|,d;\ |T_{ss}|\right]\right]$的$q$-元纠缠辅助量子纠错码.

此外，纠缠辅助量子纠错码的各参数之间满足如下关系.

定理 3[2,21] 纠缠辅助量子Singleton界 设码$\mathcal{Q}$是有限域F_{q^2}上参数为$\left[\left[n,k,d;\ c\right]\right]$的纠缠辅助量子纠错码，其中，$d\leqslant(n+2)/2$. 则必有$n+c-k\geqslant 2(d-1)$，其中，$0\leqslant c\leqslant n-1$.

特别地，若等式$n+c-k=2(d-1)$成立，则称码$\mathcal{Q}$为纠缠辅助量子MDS码.

3 新纠缠辅助量子MDS码的构造

本节将利用负循环码构造码长为$n=(q^2-1)/a$的q-元纠缠辅助量子MDS码. 下面分$q=am+l$，$q=am-l$两种情况进行讨论，其中$a=(l^2-1)/3$为偶数，m为正整数. 由于$iq^2\equiv i(an+1)\equiv i\pmod{2n}$，因此，含$i$的$q^2$-模$2n$的分圆陪集是$C_i=\{i\}$. 为叙述方便，用$[a,b]$表示所有大于或等于$a$且小于或等于$b$的整数.

3.1 码长为$n=(q^2-1)/a$且$q=am+l$的纠缠辅助量子MDS码的构造

由于$a=(l^2-1)/3$为偶数，因此，$l\equiv 1\pmod 6$或$l\equiv 5\pmod 6$. 下面分这两种情况进行讨论.

3.1.1 $l=6t+1$的情形下纠缠辅助量子MDS码的构造

引理 4 设$n=(q^2-1)/a$，其中，$a=(l^2-1)/3$，$q=am+l$，$l=6t+1$，且t,m为正整数. 设码$\mathcal{C}$是码长为n且定义集为$T=\bigcup_{j=0}^{\delta-2}C_{1+2j}$的$q^2$-元负循环码. 若$2\leqslant\delta\leqslant(3t+1)m+2$，则$\mathcal{C}^{\perp_h}\subseteq\mathcal{C}$.

证明： 由引理 1 知，$\mathcal{C}^{\perp_h}\subseteq\mathcal{C}$当且仅当$T$中每个$C_i$为斜非对称的，且$C_i$和$C_j$不构成斜非对称偶，其中，$0\leqslant i,j\leqslant\delta-2$. 即证对任意$x,y\in T$，有$C_x\neq -qC_y$. 令$I_0=\left[1,2(3t+1)m+1\right]$，假设存在奇整数$x,y\in I_0$，使$C_x=-qC_y$，即$x\equiv -qy\pmod{2n}$，由$q^2\equiv 1\pmod{2n}$知$C_y=-qC_x$，因此仅需考虑$x\leqslant y$的情形即可.

先将I_0分成$3t+2$个部分：

$$I_{0,i}=[2im+1,2(i+1)m-1],$$
$$\{2(t+1)m+1\},$$
$$I_{0,j}=[2jm+3,2(j+1)m+1]$$

其中，$0\leqslant i\leqslant t$，$t+1\leqslant j\leqslant 3t$. 那么$x\leqslant y$可分成以下 5 类情况考虑. 由于

$$l=6t+1,a=(l^2-1)/3=12t^2+4t,q=(12t^2+4t)m+6t+1,$$
$$n=(12t^2+4t)m^2+2(6t+1)m+3,$$

因此：

Case1 若$x,y\in I_{0,i}$，其中$0\leqslant i\leqslant t$，则有

$$\begin{aligned}2in&<(2im+1)\left[(12t^2+4t)m+6t+2\right]\leqslant x+qy\\&\leqslant\left[2(i+1)m-1\right]\left[(12t^2+4t)m+6t+2\right]<2(i+1)n.\end{aligned}$$

Case2 若$x,y\in I_{0,j}$，其中$t+1\leqslant j\leqslant 3t$，则有

$$\begin{aligned}2jn&<(2jm+3)\left[(12t^2+4t)m+6t+2\right]\leqslant x+qy\\&\leqslant\left[2(j+1)m+1\right]\left[(12t^2+4t)m+6t+2\right]<2(j+1)n.\end{aligned}$$

Case3 若$x\in I_{0,k},y\in I_{0,i}$，其中，$0\leqslant k<i\leqslant t$，则有

$$\begin{aligned}0&<12(i+1)tm+2(i+1)m+6i+(12t^2+4t)m+6t+7\\&\leqslant 2n-qy(\mathrm{mod}\,2n)\\&\leqslant 2n-(12t^2+4t)m-1+12itm+2im+6i-6t<2n,\end{aligned}$$

且$2n-qy(\mathrm{mod}\,2n)>2(k+1)m-1\geqslant x$.

Case4 若$x\in I_{0,k},y\in I_{0,i}$，其中，$0\leqslant k<i,t+1\leqslant i\leqslant 3t$，则有

$$\begin{aligned}0&<12(i+1)tm+2(i+1)m-(12t^2+4t)m+6i+5-6t\\&\leqslant 2n-qy(\mathrm{mod}\,2n)\\&\leqslant 2n+2im+12itm-3(12t^2+4t)m-18t-3+6i<2n,\end{aligned}$$

且$2n-qy(\mathrm{mod}\,2n)>x$.

Case5 由于$-q\left[2(t+1)m+1\right]\equiv-\left[(12t^2+4t)m+1+\right.$

$6t\rceil\cdot\lceil 1+2(t+1)m\rceil\equiv 2(5t+1)m+5(\mathrm{mod}2n)$, 且 $10tm+2m+5\notin T=\bigcup_{j=0}^{\delta-2}C_{1+2j}$, 其中, $2\leqslant\delta\leqslant(3t+1)m+2$, 因此, 对任意 $x,y\in T$, 均有 $x\not\equiv -qy\pmod{2n}$, 与假设矛盾! 故 $\mathcal{C}^{\perp_h}\subseteq\mathcal{C}$.

引理5　设码 $\mathcal{C}$ 定义如上, 则存在以下结论:

(1) $C_{2(3t+1)m+3}$ 是斜对称的, 且 $(C_{2(t+1)m+1},C_{2(5t+1)m+5})$, $(C_{2(7t+2)m+7},C_{2(5t+2)m+5})$, $(C_{2(9t+2)m+9},C_{2(3t+2)m+3})$ 分别构成斜非对称偶.

$$(2)|T_{\mathrm{ss}}(\delta)|=\begin{cases}0, & 2\leqslant\delta\leqslant(3t+1)m+2\\ 1, & (3t+1)m+3\leqslant\delta\leqslant(5t+1)m+3\\ 3, & (5t+1)m+4\leqslant\delta\leqslant(7t+2)m+4\\ 5, & (7t+2)m+5\leqslant\delta\leqslant(9t+2)m+5\end{cases}.$$

证明:

①因为

$$\begin{aligned}&-q\lceil 2(3t+1)m+3\rceil\\ &\equiv-\lceil(12t^2+4t)m+6t+1\rceil\cdot\lceil 2(3t+1)m+3\rceil\\ &\equiv 2(3t+1)m+3\pmod{2n},\\ &-q\lceil 2(5t+1)m+5\rceil\\ &\equiv-\lceil(12t^2+4t)m+6t+1\rceil\cdot\lceil 2(5t+1)m+5\rceil\\ &\equiv 2(t+1)m+1\pmod{2n},\\ &-q\lceil 2(7t+2)m+7\rceil\\ &\equiv-\lceil(12t^2+4t)m+6t+1\rceil\cdot\lceil 2(7t+2)m+7\rceil\\ &\equiv 2(5t+2)m+5\pmod{2n},\\ &-q\lceil 2(9t+2)m+9\rceil\\ &\equiv-\lceil(12t^2+4t)m+6t+1\rceil\cdot\lceil 2(9t+2)m+9\rceil\\ &\equiv 2(3t+2)m+3\pmod{2n},\end{aligned}$$

所以, $C_{2(3t+1)m+3}$ 是斜对称的, 且 $(C_{2(t+1)m+1},C_{2(5t+1)m+5})$, $(C_{2(7t+2)m+7},C_{2(5t+2)m+5})$, $(C_{2(9t+2)m+9},C_{2(3t+2)m+3})$ 分别构成斜非对称偶.

②由引理4知, 当定义集为 $T=\bigcup_{j=0}^{\delta-2}C_{1+2j}$, 其中, $2\leqslant\delta\leqslant(3t+1)m+2$ 时, 有 $\mathcal{C}^{\perp_h}\subseteq\mathcal{C}$, 即 $|T_{\mathrm{ss}}(\delta)|=0$.

令

$$\begin{aligned}I_1&=\lceil 2(3t+1)m+5,2(5t+1)m+3\rceil,\\ I_2&=\lceil 2(5t+1)m+7,2(7t+2)m+5\rceil,\\ I_3&=\lceil 2(7t+2)m+9,2(9t+2)m+7\rceil,\end{aligned}$$

下证当 $(3t+1)m+3\leqslant\delta\leqslant(5t+1)m+3$ 时, $|T_{\mathrm{ss}}(\delta)|=1$. 令 $T_0=\bigcup_{j=0}^{(3t+1)m}C_{1+2j}$, $T=\bigcup_{(3t+1)m+1}^{\delta-2}C_{1+2j}\cup T_0$, 其中, $(3t+1)m+3\leqslant\delta\leqslant(5t+1)m+3$. 根据引理2, 即证对任意 $x,y\in T\backslash C_{2(3t+1)m+3}$, 均有 $C_x\neq -qC_y$. 即证对任意奇整数 $x,y\in I_0\cup I_1$, $x\not\equiv -qy\pmod{2n}$. 假设存在奇整数 $x\in I_0\cup I_1$, $y\in I_1$, 使 $x\equiv -qy\pmod{2n}$, 下面分情形推出矛盾.

先将 I_1 分成 $2t$ 个部分:

$$I_{1,i}=\lceil 2im+5,2(i+1)m+3\rceil,$$

其中, $3t+1\leqslant i\leqslant 5t$. 那么 $x\leqslant y$ 可分成以下两种情况考虑.

Case1　若 $x,y\in I_{1,i}$, 其中 $3t+1\leqslant i\leqslant 5t$, 则有

$$\begin{aligned}2in&<(2im+5)\lceil(12t^2+4t)m+6t+2\rceil\leqslant x+qy\\ &\leqslant\lceil 2(i+1)m+3\rceil\lceil(12t^2+4t)m+6t+2\rceil<2(i+1)n,\end{aligned}$$

与假设矛盾.

Case2　若 $x\in I_{1,j}\cup I_0$, $y\in I_{1,i}$, 其中, $3t+1\leqslant j<i\leqslant 5t$, 则有

$$\begin{aligned}0&<12(i+1)tm+2(i+1)m-3(12t^2+4t)m+6i+3-18t\\ &\leqslant 2n-qy(\mathrm{mod}\,2n)\\ &\leqslant 2n-30t-5(12t^2+4t)m-5+12itm+2im+6i<2n,\end{aligned}$$

且 $2n-qy(\mathrm{mod}\,2n)>x$, 与假设亦矛盾.

因此, 有 $T_{\mathrm{ss}}(\delta)=T\cap T^{-q}=C_{2(3t+1)m+3}$, 即 $|T_{\mathrm{ss}}(\delta)|=1$.

类似地, 可以证明当 $(5t+1)m+4\leqslant\delta\leqslant(7t+2)\cdot m+4$ 时, $|T_{\mathrm{ss}}(\delta)|=3$; 当 $(7t+2)m+5\leqslant\delta\leqslant(9t+2)m+5$ 时, $|T_{\mathrm{ss}}(\delta)|=5$. 证毕.

定理4　设码 $\mathcal{C}$ 定义如上, 则存在以下参数的 q-元纠缠辅助量子MDS码:

(1) $\left[\left[(q^2-1)/a,(q^2-1)/a-2d+3,d;1\right]\right]$, 其中, $(3t+1)m+3\leqslant d\leqslant(5t+1)m+3$;

(2) $\left[\left[(q^2-1)/a,(q^2-1)/a-2d+5,d;3\right]\right]$, 其中, $(5t+1)m+4\leqslant d\leqslant(7t+2)m+4$;

(3) $\left[\left[(q^2-1)/a,(q^2-1)/a-2d+7,d;5\right]\right]$, 其中, $(7t+2)m+5\leqslant d\leqslant(9t+2)m+5$.

证明:　设 q 是奇素数的方幂, 且 $q=am+l$, $a=(l^2-1)/3$. 下面考虑 F_{q^2} 上码长为 $n=(q^2-1)/a$ 且定义集为 $T=\bigcup_{j=0}^{\delta-2}C_{1+2j}$ 的负循环码 $\mathcal{C}$, 其中, $2\leqslant\delta\leqslant(9t+2)m+5$.

由引理3和引理5知, 当 $(3t+1)m+3\leqslant\delta\leqslant(5t+1)m+3$ 时, 有 $c=|T_{ss}(\delta)|=1$; 当 $(5t+1)m+4\leqslant\delta\leqslant(7t+2)m+4$ 时, 有 $c=|T_{ss}(\delta)|=3$; 当 $5+(7t+2)m\leqslant\delta\leqslant(9t+2)m+5$ 时, 有 $c=|T_{ss}(\delta)|=5$.

由于每一个 q^2-元分圆陪集 $C_x=\{x\}$ 且 x 为奇数, 因此 T 包含 $\delta-1$ 个连续整数 $\{1,3,5,\cdots,2\delta-3\}$. 由定理1可得, $\mathcal{C}$ 的最小汉明距离大于或等于 δ. 因此 $\mathcal{C}$ 是参数为 $[n,n-\delta+1,\geqslant\delta]$ 的 q^2-元负循环码. 再根据定理2和定理3, 即可得出 q-元纠缠辅助量子MDS码的参数. 证毕.

例1　在表1中, 根据定理4的结论列出了一些新的码长 $n=(q^2-1)/a$ 的纠缠辅助量子MDS码, 其中, $a=$

$(l^2-1)/3$, $q=am+l$, $l=6t+1$, 且 t,m 为正整数.

表 1 码长为 $n=(q^2-1)/a$ 的 EAQMDS 码

l	m	q	$[[n,k,d;c]]_q$	d
7	1	23	$[[33,36-2d,d;1]]_{23}$	$7\leqslant d\leqslant 9$
			$[[33,38-2d,d;3]]_{23}$	$10\leqslant d\leqslant 13$
			$[[33,40-2d,d;5]]_{23}$	$14\leqslant d\leqslant 16$
	4	71	$[[315,318-2d,d;1]]_{71}$	$19\leqslant d\leqslant 27$
			$[[315,320-2d,d;3]]_{71}$	$28\leqslant d\leqslant 40$
			$[[315,322-2d,d;5]]_{71}$	$41\leqslant d\leqslant 49$
	6	103	$[[663,666-2d,d;1]]_{103}$	$27\leqslant d\leqslant 39$
			$[[663,668-2d,d;3]]_{103}$	$40\leqslant d\leqslant 58$
			$[[663,670-2d,d;5]]_{103}$	$59\leqslant d\leqslant 71$
13	3	181	$[[585,588-2d,d;1]]_{181}$	$24\leqslant d\leqslant 36$
			$[[585,590-2d,d;3]]_{181}$	$37\leqslant d\leqslant 52$
			$[[585,592-2d,d;5]]_{181}$	$53\leqslant d\leqslant 65$
	5	293	$[[1533,1536-2d,d;1]]_{293}$	$38\leqslant d\leqslant 58$
			$[[1533,1538-2d,d;3]]_{293}$	$59\leqslant d\leqslant 84$
			$[[1533,1540-2d,d;5]]_{293}$	$85\leqslant d\leqslant 105$
	6	349	$[[2175,2178-2d,d;1]]_{349}$	$45\leqslant d\leqslant 69$
			$[[2175,2180-2d,d;3]]_{349}$	$70\leqslant d\leqslant 100$
			$[[2175,2182-2d,d;5]]_{349}$	$101\leqslant d\leqslant 125$

3.1.2 $l=6t+5$ 的情形下纠缠辅助量子 MDS 码的构造

与 $l=6t+1$ 类似, 本节将讨论 $l=6t+5$ 情形下纠缠辅助量子 MDS 码的构造.

引理 6 设 $n=(q^2-1)/a$, 其中, $a=(l^2-1)/3$, $q=am+l$, $l=6t+5$, 且 t,m 为正整数. 若码 $\mathcal{C}$ 是码长为 n 且定义集为 $T=\bigcup_{j=0}^{\delta-2}C_{b+2j}$ 的 q^2-元负循环码, 其中, $b=2(t+1)m+3$. 当 $2\leqslant\delta\leqslant(2t+2)m+1$ 时, 有 $\mathcal{C}^{\perp_h}\subseteq\mathcal{C}$.

证明: 由引理 1, $\mathcal{C}^{\perp_h}\subseteq\mathcal{C}$ 当且仅当 T 中每个 C_i 为斜非对称的, 且 C_i 和 C_j 不构成斜非对称偶, 其中, $0\leqslant i,j\leqslant\delta-2$. 即证对任意 $x,y\in T$, 有 $C_x\neq -qC_y$. 令 $I_0=[2(t+1)m+3,2(3t+3)m+1]$, 假设存在奇整数 $x,y\in I_0$, 使 $x\equiv -qy \pmod{2n}$, 下面推出矛盾.

先将 I_0 分成 $2t+2$ 个部分:

$$I_{0,i}=\left[2im+3,2(i+1)m+1\right],$$

其中, $t+1\leqslant i\leqslant 3t+2$. 那么 $x\leqslant y$ 可分成以下两种情况考虑. 由于 $l=6t+5$, $a=(l^2-1)/3=12t^2+20t+8$, $q=(12t^2+20t+8)m+6t+5$, $n=(12t^2+20t+8)m^2+2(6t+5)m+3$.

因此:

Case1 若 $x,y\in I_{0,i}$, 其中, $t+1\leqslant i\leqslant 3t+2$, 则有

$$\begin{aligned}2in&<(2im+3)\left[(12t^2+20t+8)m+6t+6\right]\leqslant x+qy\\&\leqslant\left[2(i+1)m+1\right]\left[(12t^2+20t+8)m+6t+6\right]<2(i+1)n,\end{aligned}$$

与假设矛盾.

Case2 若 $x\in I_{0,j}$, $y\in I_{0,i}$, 其中, $t+1\leqslant j<i\leqslant 2+3t$, 则有

$$\begin{aligned}0&<2(i+1)(6t+5)m+6i-(12t^2+20t+8)m+1-6t\\&\leqslant 2n-qy \pmod{2n}\\&\leqslant 2n+6i-18t+2i(6t+5)m-3(12t^2+20t+8)m-15<2n,\end{aligned}$$

且 $2n-qy \pmod{2n}>x$, 与假设亦矛盾.

因此, 对任意 $x,y\in T$, 均有 $x\not\equiv -qy \pmod{2n}$.

故 $\mathcal{C}^{\perp_h}\subseteq\mathcal{C}$.

引理 7

设码 $\mathcal{C}$ 定义如上, 则存在以下结论:

(1) 当 $1\leqslant i\leqslant 3$ 时, $C_{(2i+1)[2(t+1)m+1]}$ 是斜对称的, $(C_{2(7t+6)m+7},C_{2(t+2)m+1})$ 构成斜非对称偶.

(2) $|T_{ss}(\delta)|=\begin{cases}0, & 2\leqslant\delta\leqslant(2t+2)m+1\\ 1, & (2t+2)m+2\leqslant\delta\leqslant(4t+4)m+2\\ 2, & (4t+4)m+3\leqslant\delta\leqslant(6t+5)m+3\\ 4, & (6t+5)m+4\leqslant\delta\leqslant(6t+6)m+3\end{cases}$.

证明:

(1) 因为

$$\begin{aligned}&-q(2i+1)\left[2(t+1)m+1\right]\\&\equiv-\left[(12t^2+20t+8)m+6t+5\right]\cdot\left[2(t+1)m+1\right](2i+1)\\&\equiv(2i+1)\left[2(t+1)m+1\right](\mathrm{mod}\,2n),\\&-q\left[2(7t+6)m+7\right]\\&\equiv-\left[2(7t+6)m+7\right]\cdot\left[(12t^2+20t+8)m+6t+5\right]\\&\equiv 2(t+2)m+1 \pmod{2n},\end{aligned}$$

所以当 $1\leqslant i\leqslant 3$ 时, $C_{(2i+1)[2(t+1)m+1]}$ 是斜对称的, $(C_{2(7t+6)m+7},C_{2(t+2)m+1})$ 构成斜非对称偶.

(2) 由引理 6 知, 当码 $\mathcal{C}$ 的定义集为 $T=\bigcup_{j=0}^{\delta-2}C_{b+2j}$, 其中 $2\leqslant\delta\leqslant(2t+2)m+1$, $b=2(t+1)m+3$ 时, 有 $\mathcal{C}^{\perp_h}\subseteq\mathcal{C}$, 即 $|T_{ss}(\delta)|=0$.

令

$$\begin{aligned}I_1&=\left[2(3t+3)m+5,2(5t+5)m+3\right],\\I_2&=\left[2(5t+5)m+7,2(7t+6)m+5\right],\\I_3&=\left[2(7t+6)m+9,2(7t+7)m+5\right],\end{aligned}$$

下证当 $(2t+2)m+2\leqslant\delta\leqslant(4t+4)m+2$ 时, $|T_{ss}(\delta)|=1$. 令 $T_0=\bigcup_{j=0}^{(2t+2)m-1}C_{b+2j}$, $T=T_0\cup\bigcup_{(2t+2)m}^{\delta-2}C_{b+2j}$, 其中, $b=2(t+1)m+3$, $(2t+2)m+2\leqslant\delta\leqslant(4t+4)m+2$. 根据引理 2, 即证对任意 $x,y\in T\backslash C_{2(3t+3)m+3}$, 有 $C_x\neq -qC_y$. 即证对任意奇整数 $x,y\in I_0\cup I_1$, 有 $x\not\equiv -qy \pmod{2n}$. 假设存在奇整数

$x\in I_0\cup I_1, y\in I_1$,使 $x\equiv -qy \pmod{2n}$,下面分情况推出矛盾.

先将 I_1 分成 $2t+2$ 个部分:

$$I_{1,i}=\left[2im+5, 2(i+1)m+3\right],$$

其中,$3t+3\leqslant i\leqslant 5t+4$. 那么 $x\leqslant y$ 可分成以下两种情况考虑:

Case1　若 $x,y\in I_{1,i}$,其中,$3t+3\leqslant i\leqslant 5t+4$,则有

$$2in<(2im+5)\left[(12t^2+20t+8)m+6t+6\right]\leqslant x+qy$$
$$\leqslant\left[2(i+1)m+3\right]\left[(12t^2+20t+8)m+6t+6\right]<2(i+1)n,$$

与假设矛盾.

Case2　若 $x\in I_{1,j}\cup I_0, y\in I_{1,i}$,其中,$3t+3\leqslant j<i\leqslant 5t+4$,则有

$$0<2(i+1)(6t+5)m-18t-3(12t^2+20t+8)m+6(i+1)-15$$
$$\leqslant 2n-qy \pmod{2n}$$
$$\leqslant 2n-5(12t^2+20t+8)m-30t-25+2i(6t+5)m+6i<2n,$$

且 $2n-qy\pmod{2n}>x$. 与假设亦矛盾.

因此,$T_{ss}(\delta)=T\cap T^{-q}=C_{2(3t+3)m+3}$,即 $|T_{ss}(\delta)|=1$.

类似地,可以证明当 $(4t+4)m+3\leqslant\delta\leqslant 3+(6t+5)m$ 时,$|T_{ss}(\delta)|=2$;当 $(6t+5)m+4\leqslant\delta\leqslant 3+(6t+6)m$ 时,$|T_{ss}(\delta)|=4$. 证毕.

定理5　设码 $\mathcal{C}$ 定义如上,则存在以下参数的 q-元纠缠辅助量子MDS码:

(1) $\left[\left[(q^2-1)/a,\ (q^2-1)/a-2d+3, d;\ 1\right]\right]$,其中,$(2t+2)m+2\leqslant d\leqslant(4t+4)m+2$;

(2) $\left[\left[(q^2-1)/a,\ (q^2-1)/a-2d+4, d;\ 2\right]\right]$,其中,$(4t+4)m+3\leqslant d\leqslant(6t+5)m+3$;

(3) $\left[\left[(q^2-1)/a,\ (q^2-1)/a-2d+6, d;\ 4\right]\right]$,其中,$(6t+5)m+4\leqslant d\leqslant(6t+6)m+3$.

证明　设 q 是奇素数的方幂,且 $q=am+l$, $a=(l^2-1)/3$. 下面考虑 F_{q^2} 上码长为 $n=(q^2-1)/a$,定义集为 $T=\bigcup_{j=0}^{\delta-2}C_{b+2j}$ 的负循环码 $\mathcal{C}$,其中,$b=2(t+1)m+3$, $2\leqslant\delta\leqslant(6t+6)m$.

由引理3和引理7知,$(2t+2)m+2\leqslant\delta\leqslant(4t+4)m+2$ 时,有 $c=|T_{ss}(\delta)|=1$;当 $(4t+4)m+3\leqslant\delta\leqslant(6t+5)m+3$ 时,有 $c=|T_{ss}(\delta)|=2$;当 $(6t+5)m+4\leqslant\delta\leqslant(6t+6)m+3$ 时,有 $c=|T_{ss}(\delta)|=4$.

由于每一个 q^2-元分圆陪集 $C_x=\{x\}$ 且 x 为奇数,从而 T 包含 $\delta-1$ 个连续整数 $\{2(t+1)m+3, 2(t+1)m+5,\cdots, 2(t+1)m+2\delta-1\}$. 由定理1可得,$\mathcal{C}$ 的最小汉明距离大于或等于 δ. 因此,$\mathcal{C}$ 是参数为 $[n, n-\delta+1, \geqslant\delta]$ 的 q^2-元负循环码. 再根据定理2和定理3即可得出 q-元纠缠辅助量子MDS码的参数. 证毕.

例2　在表2中,我们根据定理5的结论列出了一些码长 $n=(q^2-1)/a$ 的纠缠辅助量子MDS码,其中,$a=(l^2-1)/3$, $q=am+l$, $l=6t+5$,且 t,m 为正整数.

表2　码长为 $n=(q^2-1)/a$ 的EAQMDS码

l	m	q	$[[n,k,d;c]]_q$	d
5	1	13	$[[21,24-2d,d;1]]_{13}$	$4\leqslant d\leqslant 6$
			$[[21,25-2d,d;2]]_{13}$	$7\leqslant d\leqslant 8$
			$[[21,27-2d,d;4]]_{13}$	$9\leqslant d\leqslant 9$
	3	29	$[[105,108-2d,d;1]]_{29}$	$8\leqslant d\leqslant 14$
			$[[105,109-2d,d;2]]_{29}$	$15\leqslant d\leqslant 18$
			$[[105,111-2d,d;4]]_{29}$	$19\leqslant d\leqslant 21$
	4	37	$[[171,174-2d,d;1]]_{37}$	$10\leqslant d\leqslant 18$
			$[[171,175-2d,d;2]]_{37}$	$19\leqslant d\leqslant 23$
			$[[171,177-2d,d;4]]_{37}$	$24\leqslant d\leqslant 27$
11	1	51	$[[165,168-2d,d;1]]_{51}$	$6\leqslant d\leqslant 10$
			$[[165,169-2d,d;2]]_{51}$	$11\leqslant d\leqslant 14$
			$[[165,171-2d,d;4]]_{51}$	$15\leqslant d\leqslant 15$
	2	91	$[[207,210-2d,d;1]]_{91}$	$10\leqslant d\leqslant 18$
			$[[207,211-2d,d;2]]_{91}$	$19\leqslant d\leqslant 25$
			$[[207,213-2d,d;4]]_{91}$	$26\leqslant d\leqslant 27$
	3	131	$[[429,432-2d,d;1]]_{131}$	$14\leqslant d\leqslant 26$
			$[[429,433-2d,d;2]]_{131}$	$27\leqslant d\leqslant 36$
			$[[429,435-2d,d;4]]_{131}$	$37\leqslant d\leqslant 39$

3.2　码长为 $n=(q^2-1)/a$ 且 $q=am-l$ 的纠缠辅助量子MDS码的构造

与第3.1节类似,本节将讨论 $q=am-l$ 的情形下纠缠辅助量子MDS码的构造. 同样,分 $l\equiv 1 \pmod 6$ 和 $l\equiv 5 \pmod 6$ 两种情形进行讨论,相关结论的证明方法与第3.1节类似,这里从略.

3.2.1　$l=6t+1$ 的情形下纠缠辅助量子MDS码的构造

引理8　设 $n=(q^2-1)/a$,其中,$a=(l^2-1)/3$, $q=am-l, l=6t+1$,且 t,m 为正整数. 若码 $\mathcal{C}$ 是码长为 n,定义集为 $T=\bigcup_{j=0}^{\delta-2}C_{b+2j}$ 的 q^2-元负循环码,其中,$b=2tm+1$. 当 $2\leqslant\delta\leqslant 2tm-1$ 时,$\mathcal{C}^{\perp_h}\subseteq\mathcal{C}$.

引理9　设码 $\mathcal{C}$ 定义如上,则存在以下结论:

(1) 当 $1\leqslant i\leqslant 4$ 时,$C_{(2i+1)(2tm-1)}$ 是斜对称的,$(C_{2(9t+1)m-9}, C_{2(3t-1)m-3})$ 构成斜非对称偶.

(2) $$|T_{ss}(\delta)|=\begin{cases}0, & 2\leqslant\delta\leqslant 2tm-1\\ 1, & 2tm\leqslant\delta\leqslant 4tm-2\\ 2, & 4tm-1\leqslant\delta\leqslant 6tm-3\\ 3, & 6tm-2\leqslant\delta\leqslant 8tm-4\\ 4, & 8tm-3\leqslant\delta\leqslant(8t+1)m-4\end{cases}.$$

定理6　设码 $\mathcal{C}$ 定义如上,则存在以下参数的 q-元

纠缠辅助量子MDS码：

（1）$\left[\left[(q^2-1)/a,(q^2-1)/a-2d+3,d;1\right]\right]$，其中，$2tm\leqslant d\leqslant 4tm-2$；

（2）$\left[\left[(q^2-1)/a,(q^2-1)/a-2d+4,d;2\right]\right]$，其中，$4tm-1\leqslant d\leqslant 6tm-3$；

（3）$\left[\left[(q^2-1)/a,(q^2-1)/a-2d+5,d;3\right]\right]$，其中，$6tm-2\leqslant d\leqslant 8tm-4$；

（4）$\left[\left[(q^2-1)/a,(q^2-1)/a-2d+6,d;4\right]\right]$，其中，$8tm-3\leqslant d\leqslant(8t+1)m-4$.

例3 在表3中，根据定理6的结论列出了一些码长 $n=(q^2-1)/a$ 的纠缠辅助量子MDS码，其中 $a=(l^2-1)/3$，$q=am-l$，$l=6t+1$，且 t,m 为正整数.

表3 码长为 $n=(q^2-1)/a$ 的EAQMDS码

l	m	q	$[[n,k,d;c]]_q$	d
7	2	25	$[[39,42-2d,d;1]]_{25}$	$4\leqslant d\leqslant 6$
			$[[39,43-2d,d;2]]_{25}$	$7\leqslant d\leqslant 9$
			$[[39,44-2d,d;3]]_{25}$	$10\leqslant d\leqslant 12$
			$[[39,45-2d,d;4]]_{25}$	$13\leqslant d\leqslant 14$
	3	41	$[[105,108-2d,d;1]]_{41}$	$6\leqslant d\leqslant 10$
			$[[105,109-2d,d;2]]_{41}$	$11\leqslant d\leqslant 15$
			$[[105,110-2d,d;3]]_{41}$	$16\leqslant d\leqslant 20$
			$[[105,111-2d,d;4]]_{41}$	$21\leqslant d\leqslant 23$
	4	57	$[[203,206-2d,d;1]]_{57}$	$8\leqslant d\leqslant 14$
			$[[203,207-2d,d;2]]_{57}$	$15\leqslant d\leqslant 21$
			$[[203,208-2d,d;3]]_{57}$	$22\leqslant d\leqslant 28$
			$[[203,209-2d,d;4]]_{57}$	$29\leqslant d\leqslant 32$
13	1	43	$[[33,36-2d,d;1]]_{43}$	$4\leqslant d\leqslant 6$
			$[[33,37-2d,d;2]]_{43}$	$7\leqslant d\leqslant 9$
			$[[33,38-2d,d;3]]_{43}$	$10\leqslant d\leqslant 12$
			$[[33,39-2d,d;4]]_{43}$	$13\leqslant d\leqslant 13$
	4	211	$[[795,798-2d,d;1]]_{211}$	$16\leqslant d\leqslant 30$
			$[[795,799-2d,d;2]]_{211}$	$31\leqslant d\leqslant 45$
			$[[795,800-2d,d;3]]_{211}$	$46\leqslant d\leqslant 60$
			$[[795,801-2d,d;4]]_{211}$	$61\leqslant d\leqslant 64$

3.2.2 $l=6t+5$ 的情形下纠缠辅助量子MDS码的构造

引理10 设 $n=(q^2-1)/a$，其中，$a=(l^2-1)/3$，$q=am-l$，$l=6t+5$，且 t,m 为正整数. 若码 $\mathcal{C}$ 是码长为 n，定义集为 $T=\bigcup_{j=0}^{\delta-2}C_{b+2j}$ 的 q^2-元负循环码，其中，$b=2tm+1$. 当 $2\leqslant\delta\leqslant(2t+2)m-1$ 时，则 $\mathcal{C}^{\perp_h}\subseteq\mathcal{C}$.

引理11 设码 $\mathcal{C}$ 定义如上，则存在以下结论：

（1）当 $0\leqslant i\leqslant 1$ 时，$C_{(2i+1)[2(3t+2)m-3]}$ 是斜对称的；$(C_{2(7t+5)m-7},C_{2(5t+3)m-5})$，$(C_{2(9t+7)m-9},C_{2(3t+1)m-3})$ 分别构成斜非对称偶.

（2）$|T_{ss}(\delta)|=\begin{cases}0, & 2\leqslant\delta\leqslant(2t+2)m-1\\ 1, & (2t+2)m\leqslant\delta\leqslant(6t+5)m-3\\ 3, & (6t+5)m-2\leqslant\delta\leqslant(8t+6)m-4\\ 4, & (8t+6)m-3\leqslant\delta\leqslant(8t+7)m-4\end{cases}$.

定理7 设码 $\mathcal{C}$ 定义如上，则存在以下参数的 q-元纠缠辅助量子MDS码：

（1）$\left[\left[(q^2-1)/a,(q^2-1)/a-2d+3,d;1\right]\right]$，其中，$(2t+2)m\leqslant d\leqslant(6t+5)m-3$；

（2）$\left[\left[(q^2-1)/a,(q^2-1)/a-2d+5,d;3\right]\right]$，其中，$(6t+5)m-2\leqslant d\leqslant(8t+6)m-4$；

（3）$\left[\left[(q^2-1)/a,(q^2-1)/a-2d+6,d;4\right]\right]$，其中，$(8t+6)m-3\leqslant d\leqslant(8t+7)m-4$.

例4 在表4中，根据定理7的结论列出了一些码长 $n=(q^2-1)/a$ 的纠缠辅助量子MDS码，其中 $a=(l^2-1)/3$，$q=am-l$，$l=6t+5$，且 t,m 为正整数.

表4 码长为 $n=(q^2-1)/a$ 的EAQMDS码

l	m	q	$[[n,k,d;c]]_q$	d
5	2	11	$[[15,18-2d,d;1]]_{11}$	$4\leqslant d\leqslant 7$
			$[[15,20-2d,d;3]]_{11}$	$8\leqslant d\leqslant 8$
			$[[15,21-2d,d;4]]_{11}$	$9\leqslant d\leqslant 10$
	3	19	$[[45,48-2d,d;1]]_{19}$	$6\leqslant d\leqslant 12$
			$[[45,50-2d,d;3]]_{19}$	$13\leqslant d\leqslant 14$
			$[[45,51-2d,d;4]]_{19}$	$15\leqslant d\leqslant 17$
	4	27	$[[91,94-2d,d;1]]_{27}$	$8\leqslant d\leqslant 17$
			$[[91,96-2d,d;3]]_{27}$	$18\leqslant d\leqslant 20$
			$[[91,97-2d,d;4]]_{27}$	$21\leqslant d\leqslant 24$
11	1	29	$[[21,24-2d,d;1]]_{29}$	$4\leqslant d\leqslant 8$
			$[[21,26-2d,d;3]]_{29}$	$9\leqslant d\leqslant 10$
			$[[21,27-2d,d;4]]_{29}$	$11\leqslant d\leqslant 11$
	3	109	$[[297,300-2d,d;1]]_{109}$	$12\leqslant d\leqslant 30$
			$[[297,302-2d,d;3]]_{109}$	$31\leqslant d\leqslant 38$
			$[[297,303-2d,d;4]]_{109}$	$39\leqslant d\leqslant 41$

4 码的比较

本文利用负循环码构造了一些码长为 $n=(q^2-1)/a$（其中，$a=(l^2-1)/3$ 为偶数）的 q-元纠缠辅助量子MDS码. 事实上，码长为 $n=(q^2-1)/a$ 的纠缠辅助量子MDS码已被广泛研究（参见文献[2~4,12,15~20]）. 然而，文献[2,4,15~20]中的 a 要么整除 $q-1$，要么整除 $q+1$，而我们研究的 a 整除 $q-l$ 或 $q+l$，其中，$l>1$. 因此，我们的结果是新的.

文献[3]给出了长度整除 q^2-1 的纠缠辅助量子MDS码的构造，但其只研究了预先共享纠缠态为1的情形，本文中的预先共享纠缠态还可以为2,3,4,5. 文献[12]中分别

构造了码长为$n=(q^2-1)/12$的纠缠辅助量子MDS码,其中,$q=12t+5$,及码长为$n=(q^2-1)/30$的纠缠辅助量子MDS码,其中,$q=30t\pm11$. 虽然12和30既不整除$q-1$,也不整除$q+1$,但该类长度的码显然与本文得到的码不同.

特别地,将l赋值为$5,7,11,13,\cdots$,可以得到码长为$n=(q^2-1)/8$,$n=(q^2-1)/16$,$n=(q^2-1)/40$,$n=(q^2-1)/56$,$\cdots$的纠缠辅助量子MDS码. 因此,本文构造的纠缠辅助量子MDS码的码长更具有一般性,详情请见表5.

表5　码长整除q^2-1的纠缠辅助量子MDS码

n	q,t,m,c,e,b	$[[n,k,d;c]]_q$	d	参考文献
$n\mid(q^2-1)$	—	$[[n,n-2d+3,d;1]]$	$2\leqslant d\leqslant 2\left\lfloor\frac{n}{q+1}\right\rfloor$	文献[3]
$\frac{q^2-1}{2}$	q为奇数	$[[\frac{q^2-1}{2},\frac{q^2-1}{2}-2d+4,d;2]]$	$\frac{q+5}{2}\leqslant d\leqslant\frac{3q-1}{2}$	文献[3]
$\frac{q+1}{3}(q-1)$	—	$[[\frac{q^2-1}{3},\frac{q^2-1}{3}-2d+3,d;1]]$ $[[\frac{q^2-1}{3},\frac{q^2-1}{3}-2d+5,d;3]]$	$\frac{2q+2}{3}\leqslant d\leqslant q$ $q+1\leqslant d\leqslant\frac{4q-2}{3}$	文献[18]
$\frac{q^2-1}{4}$	$q\equiv3\pmod4$	$[[\frac{q^2-1}{4},\frac{q^2-1}{4}-2d+4,d;2]]$ $[[\frac{q^2-1}{a},\frac{q^2-1}{a}-2d+6,d;4]]$	$\frac{q-9}{4}\leqslant d\leqslant q$ $\frac{3q+7}{3}\leqslant d\leqslant\frac{5q+1}{3}$	文献[16]
$\frac{q+1}{t}(q-1)$	$t\in\{4,6\}$ $e\in\left[1,\frac{t}{2}\right]$	$[[\frac{q^2-1}{t},\frac{q^2-1}{t}-2d+2e+2,d;2e]]$	$\frac{(2e+t)(q+1)}{2t}\leqslant d\leqslant\frac{(2e+t+2)(q+1)-2t}{2t}$	文献[18]
$\frac{q+1}{t}(q-1)$	$t\in\{3,5,7\}$ $e\in\left[0,\left\lfloor\frac{t-1}{2}\right\rfloor\right]$	$[[\frac{q^2-1}{t},\frac{q^2-1}{t}-2d+2e+3,d;2e+1]]$	$\frac{(2e+1+t)(q+1)}{2t}\leqslant d\leqslant\frac{(2e+t+3)(q+1)-2t}{2t}$	文献[18]
$\frac{q^2-1}{2t}$	$2t\mid(q+1)$ $t\in\{3,5,7\}$	$[[\frac{q^2-1}{2t},\frac{q^2-1}{2t}-2d+3,d;1]]$	$\frac{q+2t+1}{2t}\leqslant d\leqslant\frac{qt+q-t+1}{2t}$	文献[19]
$\frac{q^2-1}{12}$	$q=12t+5$	$[[\frac{q^2-1}{12},\frac{q^2-1}{12}-2d+4,d;2]]$ $[[\frac{q^2-1}{12},\frac{q^2-1}{12}-2d+6,d;4]]$	$5t+3\leqslant d\leqslant7t+3$ $7t+4\leqslant d\leqslant8t+3$	文献[12]
$\frac{q^2-1}{30}$	$q=30t+11$ $e\in\{1,2\}$	$[[\frac{q^2-1}{30},\frac{q^2-1}{30}-2d+2e+2,d;2e]]$	$\frac{(6e+10)t+4e+4}{2}\leqslant d\leqslant\frac{(6e+16)t+4e+6}{2}$	文献[12]
$\frac{q^2-1}{30}$	$q=30t+19$	$[[\frac{q^2-1}{30},\frac{q^2-1}{30}-2d+4,d;2]]$ $[[\frac{q^2-1}{30},\frac{q^2-1}{30}-2d+6,d;4]]$ $[[\frac{q^2-1}{30},\frac{q^2-1}{30}-2d+8,d;6]]$	$8t+6\leqslant d\leqslant11t+7$ $11t+8\leqslant d\leqslant13t+8$ $13t+9\leqslant d\leqslant16t+10$	文献[12]
$t(q+1)$	$t\geqslant2,t\mid(q-1)$	$[[t(q+1),t(q+1)-2d+3,d;1]]$	$\frac{q-1+t}{t}\leqslant d\leqslant\frac{2q-2}{t}$	文献[20]
$t(q+1)$	$q\geqslant7,t$为奇数 $t\geqslant3,t\mid(q-1)$	$[[t(q+1),t(q+1)-2d+6,d;4]]$	$q+2+t\leqslant d\leqslant q+2t$	文献[13]
$2t(q+1)$	$q\geqslant1,t$为奇数 $q\equiv1\pmod4$ $t\geqslant3,t\mid(q-1)$	$[[2t(q+1),2t(q+1)-2d+6,d;4]]$	$q+2t+2\leqslant d\leqslant q+4t$	文献[13]
$2t(q-1)$	q,t为奇数 $e\in\{1,2\}$ $8\mid(q+1),t\mid(q+1)$	$[[2t(q-1),2t(q-1)-2d+2e+2,d;2e]]$	$\frac{qe-q+8t-e+3}{2}\leqslant d\leqslant\frac{q+4et+4t-1}{2}$	文献[19]
$\frac{q^2-1}{t}$	q,t为奇数 $t\geqslant3,t\mid(q+1)$	$[[\frac{q^2-1}{t},\frac{q^2-1}{t}-2d+t+2,d;t]]$	$\frac{tq-q+3t+1}{t}\leqslant d\leqslant\frac{tq+q-t+1}{t}$	文献[3]
$\frac{q^2-1}{2t}$	q为奇数 $2t\mid(q-1),e\in[1,t]$	$[[\frac{q^2-1}{2t},\frac{q^2-1}{2t}-2d+2e+2,d;2e]]$	$\frac{(t+e)(q-1)+4t}{2t}\leqslant d\leqslant\frac{(t+e+1)(q-1)+2t}{2t}$	文献[17]

续表

n	q,t,m,c,e,b	$[[n,k,d;c]]_q$	d	参考文献
$b\frac{q^2-1}{2t}$	$q=2tm-1>3,\ 1\leqslant b\leqslant 2t$ $c\in[1,2t-1]$	$[[b\frac{q^2-1}{2t}, b\frac{q^2-1}{2t}-2d+c+2, d; c]]$	$cm+2\leqslant d\leqslant(t+\lfloor\frac{c}{2}\rfloor)m$	文献[4]
$b\frac{q^2-1}{2t+1}$	$q=(2t+1)m-1,\ 1\leqslant b\leqslant 2t$ $c\in[1,2t]$	$[[b\frac{q^2-1}{2t+1}, b\frac{q^2-1}{2t+1}-2d+c+2, d; c]]$	$cm+2\leqslant d\leqslant(t+1+\lfloor\frac{c}{2}\rfloor)m$	文献[4]
$\frac{q^2-1}{a}$	$q=am+l, a=\frac{l^2-1}{3}$ $l=6t+1$	$[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+3, d; 1]]$ $[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+5, d; 3]]$ $[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+7, d; 5]]$	$(3t+1)m+3\leqslant d\leqslant(5t+1)m+3$ $(5t+1)m+4\leqslant d\leqslant(7t+2)m+4$ $(7t+2)m+5\leqslant d\leqslant(9t+2)m+5$	本文
$\frac{q^2-1}{a}$	$q=am+l, a=\frac{l^2-1}{3}$ $l=6t+5$	$[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+3, d; 1]]$ $[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+4, d; 2]]$ $[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+6, d; 4]]$	$(2t+2)m+2\leqslant d\leqslant(4t+4)m+2$ $(4t+4)m+3\leqslant d\leqslant(6t+5)m+3$ $(6t+5)m+4\leqslant d\leqslant(6t+6)m+3$	本文
$\frac{q^2-1}{a}$	$q=am-l, a=\frac{l^2-1}{3}$ $l=6t+1$	$[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+3, d; 1]]$ $[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+4, d; 2]]$ $[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+5, d; 3]]$ $[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+6, d; 4]]$	$2tm\leqslant d\leqslant 4tm-2$ $4tm-1\leqslant d\leqslant 6tm-3$ $6tm-2\leqslant d\leqslant 8tm-4$ $8tm-3\leqslant d\leqslant(8t+1)m-4$	本文
$\frac{q^2-1}{a}$	$q=am-l, a=\frac{l^2-1}{3}$ $l=6t+5$	$[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+3, d; 1]]$ $[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+5, d; 3]]$ $[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+6, d; 4]]$	$(2t+2)m\leqslant d\leqslant(6t+5)m-3$ $(6t+5)m-2\leqslant d\leqslant(8t+6)m-4$ $(8t+6)m-3\leqslant d\leqslant(8t+7)m-4$	本文

5 结语

本文研究了有限域F_{q^2}上码长为$n=(q^2-1)/a$(其中,$a=(l^2-1)/3$为偶数)的负循环码,基于其分圆陪集的结构,给出了该类负循环码是厄米特对偶包含码的充分条件,同时确定了不同数目的预先共享纠缠态的存在条件,并利用纠缠辅助量子纠错码的构造方法,得到了最优的纠缠辅助量子MDS码. 本文的研究进一步丰富了码长整除q^2-1的纠缠辅助量子MDS码的理论. 此外,对于$a=(l^2-1)/3$为奇数的情形,本文的方法不再适用,我们将在另一篇文章中讨论.

参考文献

[1] CALDERBANK A R, RAINS E M, SHOR P M, et al. Quantum error correction via codes over GF(4)[J]. IEEE Transactions on Information Theory, 1998, 44(4): 1369-1387.

[2] BRUN T, DEVETAK I, HSIEH M H. Correcting quantum errors with entanglement[J]. Science, 2006, 314(5798): 436-439.

[3] FAN J H, CHEN H W, XU J A. Constructions of q-ary entanglement-assisted quantum MDS codes with minimum distance greater than q+1[J]. Quantum Information and Computation, 2016, 16(5&6): 423-434.

[4] LI L Q, ZHU S X, LIU L, et al. Entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes[J]. Quantum Information Processing, 2019, 18(5): 1-15.

[5] 李瑞虎, 许根, 吕良东. BCH码的定义集分解及应用[J]. 空军工程大学学报(自然科学版), 2013, 14(2): 86-89.
LI R H, XU G, LÜ L D. Decomposition of defining sets of BCH codes and its applications[J]. Journal of Air Force Engineering University (Natural Science Edition), 2013, 14 (2): 86-89. (in Chinese)

[6] GUENDA K, JITMAN S, GULLIVER T A. Constructions of good entanglement-assisted quantum error correcting codes[J]. Designs, Codes and Cryptography, 2018, 86(1): 121-136.

[7] LUO G J, CAO X W, CHEN X J. MDS codes with hulls of arbitrary dimensions and their quantum error correction[J].

IEEE Transactions on Information Theory, 2019, 65(5): 2944-2952.

[8] FANG W J, FU F W, LI L Q, et al. Euclidean and Hermitian hulls of MDS codes and their applications to EAQECCs[J]. IEEE Transactions on Information Theory, 2020, 66(6): 3527-3537.

[9] GAO Y Y, YUE Q, HUANG X M, et al. Hulls of generalized Reed-Solomon codes via Goppa codes and their applications to quantum codes[J]. IEEE Transactions on Information Theory, 2021, 67(10): 6619-6626.

[10] CAO M. MDS codes with Galois hulls of arbitrary dimensions and the related entanglement-assisted quantum error correction[J]. IEEE Transactions on Information Theory, 2021, 67(12): 7964-7984.

[11] LÜ L D, LI R H. Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes[J]. International Journal of Quantum Information, 2014, 12(3): 1450015.

[12] LU L D, LI R H, GUO L B, et al. Entanglement-assisted quantum MDS codes from negacyclic codes[J]. Quantum Information Processing, 2018, 17(3): 69.

[13] CHEN J Z, HUANG Y Y, FENG C H, et al. Entanglement-assisted quantum MDS codes constructed from negacyclic codes[J]. Quantum Information Processing, 2017, 16(12): 303.

[14] QIAN J F, ZHANG L N. Constructions of new entanglement-assisted quantum MDS and almost MDS codes[J]. Quantum Information Processing, 2019, 18(3): 1-12.

[15] KOROGLU M E. New entanglement-assisted MDS quantum codes from constacyclic codes[J]. Quantum Information Processing, 2019, 18(2): 1-28.

[16] SARı M, KOLOTOĞLU E. An application of constacyclic codes to entanglement-assisted quantum MDS codes [J]. Computational and Applied Mathematics, 2019, 38 (2): 75.

[17] LI R H, GUO G M, SONG H, et al. New constructions of entanglement-assisted quantum MDS codes from negacyclic codes[J]. International Journal of Quantum Information, 2019, 17(3): 1950022.

[18] LIU Y, LI R H, LV L D, et al. Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes[J]. Quantum Information Processing, 2018, 17(8): 210.

[19] LU L D, MA W P, GUO L B. Two families of entanglement-assisted quantum MDS codes from constacyclic codes[J]. International Journal of Theoretical Physics, 2020, 59: 1657-1667.

[20] WANG J L, LI R H, LV J J, et al. Entanglement-assisted quantum codes from cyclic codes and negacyclic codes [J]. Quantum Information Processing, 2020, 19: 138.

[21] WANG L Q, ZHU S X, SUN Z H. Entanglement-assisted quantum MDS codes from cyclic codes[J]. Quantum Information Processing, 2020, 19(2): 1-18.

[22] MACWILLIAMS F J, SLOANE N J A. The Theory of Error Correcting Codes[M]. Amsterdam: North-Holland Pub. Co., 1977.

[23] LI R H, ZOU F, LIU Y, et al. Hermitian dual containing BCH codes and construction of new quantum codes[J]. Quantum Information and Computation, 2013, 13(1&2): 21-35.

作者简介

汪　盼　女,1997年生,安徽安庆人. 合肥工业大学数学学院硕士研究生. 研究方向为代数编码.
E-mail: panwang_hfut@163.com

王立启　男,1986年生,安徽六安人. 合肥工业大学数学学院副教授、硕士生导师. 研究方向为代数编码.
E-mail: liqiwangg@163.com

朱士信　男,1962年生,安徽枞阳人. 合肥工业大学数学学院教授、博士生导师. 研究方向为代数编码、序列密码与信息安全研究.
E-mail: zhushixin@hfut.edu.cn