Pure Mathematics 理论数学, 2019, 9(5), 653-663
Published Online July 2019 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2019.95087

Hans汉斯

Constructions of Six Classes of Entanglement-Assisted Quantum MDS Codes

Linxue Zhang*, **Xilin Tang**

School of Mathematics, South China University of Technology, Guangzhou Guangdong
Email: zhanglinxue2019@163.com

Received: Jul. 4th, 2019; accepted: Jul. 23rd, 2019; published: Jul. 30th, 2019

Abstract

Entanglement-assisted quantum error-correcting codes make use of preexisting entanglement between the sender and receiver to improve information rate. In this paper, we obtain six classes of entanglement-assisted quantum MDS codes by means of characterizing the relationship between the number of entangled states and the size of defining set of constacyclic codes.

Keywords

Entanglement-Assisted Quantum Codes, Constacyclic Codes, MDS Codes, Defining Sets

六类纠缠辅助量子MDS码的构造

张琳雪*，**唐西林**

华南理工大学数学学院，广东 广州
Email: zhanglinxue2019@163.com

收稿日期：2019年7月4日；录用日期：2019年7月23日；发布日期：2019年7月30日

摘　要

纠缠辅助量子码利用发送器和接收器之间预先存在的纠缠来提高信息速率。本文通过刻画常循环码纠缠态的数量与定义集大小的关系，构造了六类纠缠辅助量子MDS码。

关键词

纠缠辅助量子码，常循环码，MDS码，定义集

*第一作者。

文章引用: 张琳雪, 唐西林. 六类纠缠辅助量子 MDS 码的构造[J]. 理论数学, 2019, 9(5): 653-663.
DOI: 10.12677/pm.2019.95087

1. 引言

在量子信息和量子计算中，非常重要的任务就是构造好的量子纠错码。近年来，诸多研究者通过经典纠错码来构造量子纠错码(见[1] [2] [3])。一个参数为$[[n,k,d]]_q$ q元量子码Q是Hilbert空间$(C^q)^{\otimes n}$的一个q^k维子空间。参数为$[[n,k,d]]_q$量子码C满足量子Singleton界：$k \le n-2d+2$，如果$k=n-2d+2$，则称量子码C为量子极大距离可分离码(量子MDS码) (见[4])。

在量子纠错码中，纠缠辅助量子纠错码(简写为EAQEC码)扮演重要的角色。在[5]中，给出对EAQEC码纠缠辅助Singleton界，并把达到这个界的码称为纠缠辅助量子MDS码(简写为EAQMDS码)。在[6]中，在经典MDS码的基础上，通过加入一个或者更多的纠缠态，构造五类新的EAQMDS码。在[7]中，提出分解定义集的概念，并用这个方法分解BCH循环码的定义集，得到了一些好的EAQEC码。近年来，负循环码经常被用来构造EAQMDS码。在[8] [9]中，通过分解负循环码的定义集，得到新的EAQMDS码。在[10] [11]中由基于负循环码扩充到基于常循环码来构造新的EAQMDS码。本文通过分解常循环码的定义集构造了六类新的EAQMDS码。本文采用不同于[10] [11]的方法来计算纠缠态的数量c，在同样的长度n下定义集具有更一般的形式，从而可构造更多的EAQMDS码。

由于EAQMDS码的性能优劣是通过速率$\frac{k-c}{n}$来评价的，已知$\frac{k-c}{n}=\frac{n-(\delta+1)-c}{n}=1-\frac{\delta+c+1}{n}$，$c$随着$\delta$增大而增大，就其性能而言$\delta$越小越好。而EAQMDS码的纠错能力与最小距离$d$有关，$d$越大纠错能力越强，正如在[12]中给出最小距离大于$\frac{q}{2}+1$时，码具有较好的纠错能力。d随着δ增大而增大，因此在实际问题中δ尽可能大时保证c尽量小，我们有必要弄清楚c与δ的关系，本文将讨论这一问题。

2. 预备知识

2.1. 常循环码

令q为一个奇素数的方幂，设F_{q^2}为具有q^2个元素的有限域，给任意两个向量$X=(x_1,x_2,\cdots,x_n)$和$Y=(y_1,y_2,\cdots,y_n)\in F_{q^2}^n$，定义Hermitian内积为$\langle X,Y\rangle_H=\sum_{i=1}^{n}x_iy_i^q$。如果$\langle X,Y\rangle_H=0$，则称这两个向量Hermitian正交。$F_{q^2}^n$为$F_{q^2}$上的$n$维向量空间，一个参数为$[n,k,d]_{q^2}$的线性码$C$是指$F_{q^2}^n$空间中最小距离为$d$的$k$维子空间。定义线性码的Hermitian对偶码为$C^{\perp H}=\left\{X\in F_{q^2}^n \middle| \langle X,Y\rangle_H=0,\forall Y\in C\right\}$，如果$C\subseteq C^{\perp H}$，则$C$称为Hermitian自正交码。

设$(n,q)=1$。对于$\eta\in F_{q^2}^*$，如果$(c_0,c_1,\cdots,c_{n-1})\in C$，有$(\eta c_{n-1},c_0,\cdots,c_{n-2})\in C$，称线性码$C$为$\eta$-常循环码。一个码字$c=(c_0,c_1,\cdots,c_{n-1})$也可以用一个多项式$c(x)=c_0+c_1+\cdots+c_{n-1}x^{n-1}$表示。因此每个$\eta$-常循环码都是商环$F_{q^2}[x]/\langle x^n-\eta\rangle$的一个主理想，即$C=\langle g(x)\rangle$，其中$g(x)\mid x^n-\eta$，且$g(x)$是首1多项式。假设$\omega\in F_{q^2}^*$是$rn$次本原单位根且$\omega^n=\eta$，令$\zeta=\omega^r$，则$\zeta$是一个$n$次本原单位根。那么就有

$$x^n-\eta=x^n-\omega^n=\prod_{j=0}^{n-1}\left(x-\omega^{1+jr}\right).$$

令 $\Omega=\{1+jr \mid 0\le j\le n-1\}$。对于 $\forall j\in\Omega$，设 C 是 η-常循环码，且 $C=\langle g(x)\rangle$，称 $Z=\{j\in\Omega \mid g(\omega^j)=0\}$ 为 C 的定义集，因而 $Z^{\perp H}=\{j\in\Omega \mid -qj(\bmod rn)\notin Z\}$ 为 $C^{\perp H}$ 的定义集。称 $C_j=\{jq^{2i}(\bmod rn) \mid i\in Z\}$ 为 j 模 rn 的 q^2-分圆陪集。

引理 2.1 [13] 设 $C=\langle g(x)\rangle$ 是一个在 F_{q^2} 上，长度为 n 的 η-常循环码，其中 η 是一个 r 次本原单位根。如果 $g(x)$ 的根为 $\{\omega^{1+rj} \mid j_1\le j\le j_1+d-2\}$，那么 C 的极小距离至少为 d。

引理 2.2 [14] 设 $\eta\in F_{q^2}^*$ 和 $ord(\eta)=r$，其中 $r|q+1$。C 是一个在 F_{q^2} 上，长度为 n 的 η-常循环码，其定义集为 $Z\subseteq\Omega$，那么 $C^{\perp H}\subseteq C$ 当且仅当 $Z\cap(-qZ)=\varnothing$，其中 $-qZ=\{-qz(\bmod rn) \mid z\in Z\}$。

2.2. 纠缠辅助量子码

引理 2.3 [15] 如果在有限域 F_q 上存在一个参数为 $[n,k,d]$ 的线性码 C，则有 Singleton 界：$k\le n-d+1$。当达到 Singleton 界，即 $k=n-d+1$，则称 C 为 MDS 码。

令 H 为 C 的 $(n-k)\times n$ 的校验矩阵，则 $C^{\perp H}$ 有 $n\times(n-k)$ 的生成矩阵 H^*，其中 H^* 为 H 的共轭转置矩阵。

引理 2.4 [16] 如果 C 为有限域 F_q 上参数为 $[n,k,d]$ 的线性码，H 为 C 的校验矩阵，则存在参数为 $[\![n,2k-n+c,d;c]\!]_q$ 的 EAQEC 码，其中 $c=rank(HH^*)$。

引理 2.5 [5] C 为有限域 F_q 上带参数为 $[[n,k,d;c]]_q$ 的 EAQEC 码，如果 $d\le(n+2)/2$，则 C 满足纠缠辅助 Singleton 界：$n+c-k\ge 2(d-1)$。如果对于 $d\le(n+2)/2$，C 满足 $n+c-k=2(d-1)$，则 C 称为 EAQMDS 码。

定义 2.6 [8] 设 $\eta\in F_{q^2}^*$ 和 $ord(\eta)=r$，其中 $r|q+1$。C 是一个在 F_{q^2} 上，长度为的 n 的 η-常循环码，其定义集为 Z。假设 $Z_1=Z\cap(-qZ), Z_2=Z\setminus Z_1$，其中 $-qZ=\{-qz(\bmod rn) \mid z\in Z\}$。则 $Z=Z_1\cup Z_2$ 称为 C 的定义集的分解。

引理 2.7 [8] C 是一个在 F_{q^2} 上，长度为的 n 的 η-常循环码，其定义集为 Z，且 $Z=Z_1\cup Z_2$ 为定义集 Z 的分解，则纠缠态的数量为 $c=|Z_1|=|Z\cap(-qZ)|$。

本文未指明的符号、概念参见[11]。

3. 主要结果

3.1. 构造长为 $n=\dfrac{q^2-1}{r}$ 的 EAQMDS 码

在本节中 q 为一个奇素数的方幂，$r|q+1$。注意到 $n=\dfrac{q^2-1}{r}$，则有 $rn=q^2-1, ord_{rn}(q^2)=1$，这意味着每个模 rn 的 q^2-分圆陪集只包含一个元素。

定理 3.1 若 C 是一个在 F_{q^2} 上，长度为 $n=\dfrac{q^2-1}{r}$ 的 η-常循环码，它的定义集为 $Z=\bigcup_{j=0}^{\delta}C_{1+rj}$，则能找到所有长度为 n 的 EAQMDS 码，它的参数为 $[\![n,n-2(\delta+1)+c(\delta),\delta+2;c(\delta)]\!]_q$。

证明 由于 $|Z|=\delta+1$ 则从引理 2.1 和引理 2.3 可知 C 是一个参数为 $[n,n-(\delta+1),\delta+2]_{q^2}$ MDS 码。根据引理 2.7

$$
\begin{aligned}
c=|Z\cap(-qZ)|&=\left|\{(j,k) \mid 1+rj\equiv -q(1+rk)(\bmod rn), 0\le j,k\le\delta\}\right| \\
&=\left|\left\{(j,k) \,\middle|\, j+qk\equiv -\frac{q+1}{r}(\bmod n), 0\le j,k\le\delta\right\}\right|.
\end{aligned}
$$

这表明 c 与 δ 的取值范围有关。由引理 2.4 存在参数为 $[\![n,n-2(\delta+1)+c(\delta),\delta+2;c(\delta)]\!]_q$ 的 EAQMDS 码。为了找到 c 关于 δ 的对应关系，讨论同余方程 $j+qk\equiv-\frac{q+1}{r}(\bmod n)$ 的解，注意到 $\Omega=\{1+jr\,|\,0\le j\le n-1\}$，因此可假定 $0\le j,k\le n-1$。这样

$j+qk\equiv-\frac{q+1}{r}(\bmod n)$ 有整数解 (j,k)

$\Leftrightarrow$ 对 $l\in Z$ 来说，$nl-\frac{q+1}{r}=j+qk$ 有整数解 (j,k)。

由 $0\le j,k\le n-1$，当 $r\ne1$ 时，可得 $1\le l\le q$。在取定 l 后把 $nl-\frac{q+1}{r}$ 表示成 $j+qk$ 这种形式，其中 (j,k) 的取法是多样的，例如：

$$j+qk=nl-\frac{q+1}{r}=\frac{l(q^2-1)}{r}-\frac{q+1}{r}=\left(\frac{l(q+1)}{r}-x\right)q+xq-\frac{(l+1)(q+1)}{r}.$$

令 $b_{l,x}=\max(j,k)=\max\left(xq-\frac{(l+1)(q+1)}{r},\frac{l(q+1)}{r}-x\right)$，得到所有的 $b_{l,x}$，只要给定 r，就可以把 $b_{l,x}$ 从小到大排列。依次记为 $b_1,b_2,b_3,\cdots$。若 b_i 对应的 $b_{l,x}$ 有 c_i 个，则当 $0\le\delta\le b_1-1$ 时，$c(\delta)=0$；当 $b_1\le\delta\le b_2-1$ 时，$c(\delta)=c_1$；$\cdots$；当 $b_i\le\delta\le b_{i+1}-1$ 时，$c(\delta)=c_1+c_2+\cdots+c_i$。接下来计算所有的 $b_{l,x}$。

当 $l=t(1\le t\le q)$ 时，有 $t\frac{q^2-1}{r}-\frac{q+1}{r}=\left(\frac{t(q+1)}{r}-x\right)q+xq-\frac{(t+1)(q+1)}{r}$，因为 $0\le j,k\le n-1$，则

$$0\le\frac{t(q+1)}{r}-x\le n-1,\quad 0\le xq-\frac{(t+1)(q+1)}{r}\le n-1$$

即当 $t>1$ 时

$$\left\lceil\frac{(t+1)(q+1)}{rq}\right\rceil\le x\le\left\lfloor\frac{q^2-1-r+(t+1)(q+1)}{rq}\right\rfloor.$$

当 $xq-\frac{(t+1)(q+1)}{r}\ge\frac{t(q+1)}{r}-x$ 即 $x\ge\left\lceil\frac{2t+1}{r}\right\rceil$ 时，$b_{t,x}=xq-\frac{(t+1)(q+1)}{r}$，否则 $b_{t,x}=\frac{t(q+1)}{r}-x$。得到所有的 $b_{t,x}$ 如下：

$$b_{t,\left\lceil\frac{(t+1)(q+1)}{rq}\right\rceil}=\frac{t(q+1)}{r}-\left\lceil\frac{(t+1)(q+1)}{rq}\right\rceil,\cdots,b_{t,\left\lceil\frac{2t+1}{r}\right\rceil-1}=\frac{t(q+1)}{r}-\left(\left\lceil\frac{2t+1}{r}\right\rceil-1\right)$$

$$b_{t,\left\lceil\frac{2t+1}{r}\right\rceil}=\left\lceil\frac{2t+1}{r}\right\rceil q-\frac{(t+1)(q+1)}{r},\cdots,b_{t,\left\lfloor\frac{q^2-1-r+(t+1)(q+1)}{rq}\right\rfloor}=\left\lfloor\frac{q^2-1-r+(t+1)(q+1)}{rq}\right\rfloor q-\frac{(t+1)(q+1)}{r}.$$

取 $l=1$，得到所有的 $b_{1,x}$：

$$b_{1,\left\lceil\frac{3}{r}\right\rceil}=\left\lceil\frac{3}{r}\right\rceil q-\frac{2(q+1)}{r},b_{1,\left\lceil\frac{3}{r}\right\rceil+1}=\left(\left\lceil\frac{3}{r}\right\rceil+1\right)q-\frac{2(q+1)}{r},\cdots,b_{1,\frac{q+1}{r}}=\frac{q+1}{r}q-\frac{2(q+1)}{r}.$$

取 $l=2$，得到所有的 $b_{2,x}$：

$$b_{2,\left\lceil\frac{3(q+1)}{r}\right\rceil}=\frac{2(q+1)}{r}-\left\lceil\frac{3(q+1)}{r}\right\rceil,\cdots,b_{2,\left\lceil\frac{5}{r}\right\rceil-1}=\frac{2(q+1)}{r}-\left(\left\lceil\frac{5}{r}\right\rceil-1\right)$$

$$b_{2,\left\lceil \frac{5}{r} \right\rceil} = \left(\left\lceil \frac{5}{r} \right\rceil \right) q - \frac{3(q+1)}{r}, \cdots, b_{2,\left\lfloor \frac{q^2-1-r+3(q+1)}{rq} \right\rfloor} = \left\lfloor \frac{q^2-1-r+3(q+1)}{rq} \right\rfloor q - \frac{3(q+1)}{r}.$$

$\vdots$

取 $l = q$，得到所有的 $b_{q,x}$：

$$b_{q,\frac{q+1}{r}+1} = \frac{q(q+1)}{r} - \left(\frac{q+1}{r} + 1 \right) = n-1, \cdots, b_{q,\frac{2(q+1)}{r}-1} = \frac{q(q+1)}{r} - \left(\frac{2(q+1)}{r} - 1 \right).$$

注意当 $r=1$ 时，同理可计算所有的 $b_{l,x}$。综上若 C 的定义集为 $Z = \bigcup_{j=0}^{\delta} C_{1+rj}$，当 $b_i \le \delta \le b_{i+1} - 1$ 时，则存在参数为 $[\![n, n-2(\delta+1)+c_1+\cdots+c_i, \delta+2; c_1+\cdots+c_i]\!]_q$ 的 EAQMDS 码。

推论 3.2 1) 若 C 是一个在 F_{q^2} 上，长度为 $n = q^2 - 1$ 的 η-常循环码，它的定义集为 $Z = \bigcup_{j=0}^{\delta} C_{1+j}$，则存在参数为 $[\![n, n-2(\delta+1)+c(\delta), \delta+2; c(\delta)]\!]_q$ EAQMDS 码。当 $0 \le \delta \le q-3$ 时，$c(\delta)=0$，得 $C^{\perp H} \subseteq C$；当 $q-2 \le \delta \le 2q-4$ 时，$c(\delta)=1$；当 $\delta = 2q-3$ 时，$c(\delta)=2$；当 $2q-2 \le \delta \le 3q-5$ 时，$c(\delta)=4$；当 $\delta = 3q-4$ 时，$c(\delta)=5$；当 $\delta = 3q-3$ 时，$c(\delta)=7$；当 $3q-2 \le \delta \le 4q-6$ 时，$c(\delta)=9$。

2) 若 C 是一个在 F_{q^2} 上，长度为 $n = \frac{q^2-1}{2}$ 的 η-常循环码，它的定义集为 $Z = \bigcup_{j=0}^{\delta} C_{1+2j}$，则存在参数为 $[\![n, n-2(\delta+1)+c(\delta), \delta+2; c(\delta)]\!]_q$ EAQMDS 码。当 $0 \le \delta \le q-2$ 时，$c(\delta)=0$，得 $C^{\perp H} \subseteq C$；当 $q-1 \le \delta \le \frac{3q-5}{2}$ 时，$c(\delta)=2$；当 $\frac{3q-3}{2} \le \delta \le 2q-3$ 时，$c(\delta)=4$；当 $\delta = 2q-2$ 时，$c(\delta)=6$；当 $2q-1 \le \delta \le \frac{5q-7}{2}$ 时，$c(\delta)=8$。

证明 我们只证明 1)，2)的证明是类似的。在定理 3.1 中，取定 $r=1$，所有的 $b_{l,x}$ 取值如下：

当 $l=1$ 时，$q-2, 2q-2, 3q-2, 4q-2, 5q-2, \cdots, (q-1)q-2.$

当 $l=2$ 时，$2q-2, 2q-3, 3q-3, 4q-3, 5q-3, \cdots, (q-1)q-3.$

当 $l=3$ 时，$3q-2, 3q-3, 3q-4, 4q-4, 5q-4, \cdots, (q-1)q-4.$

当 $l=4$ 时，$4q-2, 4q-3, 4q-4, 4q-5, 5q-5, \cdots, (q-1)q-5.$

$\vdots$

当 $l=t$ 时，$tq-2, tq-3, tq-4, tq-5, \cdots, tq-t, tq-(t+1), (t+1)q-(t+1), \cdots, (q-1)q-(t+1).$

$\vdots$

当 $l=q+1$ 时，$(q+1)q-(q-2) = n-1.$

现在把 $b_{l,x}$ 从小到大排列出来，这里只排列出前面部分，有

$$b_1 = q-2, c_1 = 1; b_2 = 2q-3, c_2 = 1; b_3 = 2q-2, c_3 = 2;$$
$$b_4 = 3q-4, c_4 = 1; b_5 = 3q-3, c_5 = 2; b_6 = 3q-2, c_6 = 2.$$

根据定理 3.1 即可得出结论。

推论 3.3 1) 若 C 是一个在 F_{q^2} 上，长度为 $n = \frac{q^2-1}{r}$ 的 η-常循环码，其中 $r \mid q+1$ 且 $r \ge 3$，r 是一个奇数。令 $r = 2m+1, \lambda = \frac{q+1}{r}$。$C$ 的定义集为 $Z = \bigcup_{j=0}^{\delta} C_{1+rj}$，则存在参数为 $[\![n, n-2(\delta+1)+c(\delta), \delta+2; c(\delta)]\!]_q$ 的 EAQMDS 码。当 $0 \le \delta \le m\lambda - 2$ 时，$c(\delta)=0$，得 $C^{\perp H} \subseteq C$；当 $m\lambda - 1 \le \delta \le (m+1)\lambda - 2$ 时，$c(\delta)=1$；当 $(m+1)\lambda - 1 \le \delta \le (m+2)\lambda - 2$ 时，$c(\delta)=3$；当 $(m+2)\lambda - 1 \le \delta \le (m+3)\lambda - 2$ 时，$c(\delta)=5$；…；当

$(m+t)\lambda-1\le\delta\le(m+t+1)\lambda-2$ 时，$c(\delta)=2t+1$；⋯；当 $(2m-1)\lambda-1\le\delta\le q-2$ 时，$c(\delta)=2m-1$；当 $\delta=q-1$ 时，$c(\delta)=2m+1$。

2) 若 C 是一个在 F_{q^2} 上，长度为 $n=\dfrac{q^2-1}{r}$ 的 η-常循环码，其中 $r\mid q+1$ 且 $r\ge4$，r 是一个偶数。令 $r=2m$ 和 $\lambda=\dfrac{q+1}{r}$。C 的定义集为 $Z=\bigcup_{j=0}^{\delta}C_{1+rj}$，则存在参数为 $[\![n,n-2(\delta+1)+c(\delta),\delta+2;c(\delta)]\!]_q$ 的 EAQMDS 码。当 $0\le\delta\le m\lambda-2$ 时，$c(\delta)=0$，得 $C^{\perp H}\subseteq C$；当 $m\lambda-1\le\delta\le(m+1)\lambda-2$ 时，$c(\delta)=2$；当 $(m+1)\lambda-1\le\delta\le(m+2)\lambda-2$ 时，$c(\delta)=4$；当 $(m+2)\lambda-1\le\delta\le(m+3)\lambda-2$ 时，$c(\delta)=6$；⋯；当 $(m+t)\lambda-1\le\delta\le(m+t+1)\lambda-2$ 时，$c(\delta)=2(t+1)$；⋯；当 $(2m-2)\lambda-1\le\delta\le q-2$ 时，$c(\delta)=2m-2$；当 $\delta=q-1$ 时，$c(\delta)=2m$。

证明 我们只证明 1)，同理可证明 2)。当 $\delta\le q-1$ 时，有 $0\le j,k\le q-1$，得到 $nl=j+qk$ 的表示唯一，此时相当于对 nl 做带余除法。这里设定 $\delta\le q-1$，由 $0\le j,k\le n-1$ 和 $r=2m+1$ 可得 $1\le l\le 2m+1$。

当 $l\le 2m-1$ 时，有 $l\dfrac{q^2-1}{r}-\dfrac{q+1}{r}=\left(\dfrac{l(q+1)}{r}-1\right)q+q-\dfrac{(l+1)(q+1)}{r}$；

当 $l=2m$ 时，有 $2m\dfrac{q^2-1}{r}-\dfrac{q+1}{r}=\left(\dfrac{2m(q+1)}{r}-2\right)q+q-1$；

当 $l=2m+1$ 时，有 $(2m+1)\dfrac{q^2-1}{r}-\dfrac{q+1}{r}=(q-1)q+q-\dfrac{q+1}{r}-1.$

因为 $r=2m+1$，所以

当 $l=m$ 时，有

$$q-\frac{(m+1)(q+1)}{r}=\frac{m(q+1)}{r}-1,\quad b_{m,1}=m\frac{q+1}{r}-1;$$

当 $1\le l<m$ 时，有

$$q-\frac{(l+1)(q+1)}{r}>\frac{l(q+1)}{r}-1,\quad b_{l,1}=q-\frac{(l+1)(q+1)}{r};$$

当 $m<l\le 2m+1$ 时，有

$$q-\frac{(l+1)(q+1)}{r}<\frac{l(q+1)}{r}-1,\quad b_{l,1}=\frac{l(q+1)}{r}-1.$$

又因为

$$\frac{(m+t)(q+1)}{r}-1=q-\frac{(m-t+1)(q+1)}{r}$$

故有

$$b_{m,1}=m\frac{q+1}{r}-1,b_{m-1,1}=b_{m+1,1}=\frac{(m+t)(q+1)}{r}-1,\cdots,b_{m-t,1}=b_{m+t,1}=\frac{(m+t)(q+1)}{r}-1$$
$$,\cdots,b_{1,1}=b_{2m-1,1}=\frac{(2m-1)(q+1)}{r}-1,b_{2m,1}=q-1,b_{2m+1,1}=q-1.$$

将它们从小到大排列出来：

$$b_1=m\lambda-1,c_1=1;b_2=(m+1)\lambda-1,c_2=2;b_3=(m+2)\lambda-1,c_3=2;\cdots;$$
$$b_{t+1}=(m+t)\lambda-1,c_{t+1}=2;\cdots;b_m=(2m-1)\lambda-1,c_m=2;b_{m+1}=q-1,c_{m+1}=2.$$

根据定理 3.1 即可得出结论。

3.2. 构造长为 $n=\frac{q^2+1}{10}$，其中 $q\equiv 7(\bmod 10)$ 与长为 $n=\frac{q^2+1}{34}$，其中 $q\equiv 21(\bmod 34)$ 的 EAQMDS 码

在本节中 q 为一个奇素数的方幂，$r|q+1$。注意到 $n=\frac{q^2+1}{10}$ 或者 $n=\frac{q^2+1}{34}$，则有 $ord_{rn}(q^2)=2$。令 $s=\frac{q^2+1}{2}$ 则模 rn 的 q^2-分圆陪集分别是 $C_s=\{s\},C_{s-rj}=\{s-rj,s+rj\}$，其中 $1\le j\le\frac{n-1}{2}$。

引理 3.4 令 $s=\frac{q^2+1}{2}$，当 $n|s$ 时，有

(j,k) 是 $s-rj\equiv -q(s-rk)(\bmod rn)$ 的解 $\Leftrightarrow$ (k,j) 是 $s-rj\equiv -q(s+rk)(\bmod rn)$ 的解。

证明 要证 (j,k) 是 $s-rj\equiv -q(s-rk)(\bmod rn)$ 的解 $\Leftrightarrow$ (k,j) 是 $s-rj\equiv -q(s+rk)(\bmod rn)$ 的解，即证 (j,k) 是 $j+qk\equiv 0(\bmod n)$ 的解 $\Leftrightarrow$ (k,j) 是 $j-qk\equiv 0(\bmod n)$ 的解。

先证必要性，由 (j,k) 是 $j+qk\equiv 0(\bmod n)$ 的解，有

$$-q(j+qk)=-qj-q^2k=-qj+k-(q^2+1)k=k-qj\equiv 0(\bmod n)$$

即

$$k-qj\equiv 0(\bmod n)$$

得 (k,j) 是 $j-qk\equiv 0(\bmod n)$ 的解。同理可证充分性。

引理 3.5 $s=\frac{q^2+1}{2}$，当 $n|s$ 时，则 (j,k) 是 $s-r\left(\frac{n-1}{2}-j\right)\equiv -q\left(s-r\left(\frac{n-1}{2}-k\right)\right)(\bmod rn)$ 的解 $\Leftrightarrow$ (k,j) 是 $s-r\left(\frac{n-1}{2}-j\right)\equiv -q\left(s+r\left(\frac{n-1}{2}-k\right)\right)(\bmod rn)$ 的解。

证明 只需证 (j,k) 是 $j+qk-\frac{q+1}{2}\equiv 0(\bmod n)$ 的解 $\Leftrightarrow$ (k,j) 是 $j-qk+\frac{q-1}{2}\equiv 0(\bmod n)$ 的解。

先证必要性，由 (j,k) 是 $j+qk-\frac{q+1}{2}\equiv 0(\bmod n)$ 的解，有

$$-q\left(j+qk-\frac{q+1}{2}\right)=-qj-q^2k+\frac{q^2+q}{2}=-qj+k-(q^2+1)k+\frac{q^2+1+q-1}{2}=k-qj+\frac{q-1}{2}\equiv 0(\bmod n)$$

即

$$k-qj+\frac{q-1}{2}\equiv 0(\bmod n)$$

得 (k,j) 是 $j-qk+\frac{q-1}{2}\equiv 0(\bmod n)$ 的解。同理可证充分性。

定理 3.6 q 为一个奇素数的方幂，且 $q\equiv 7(\bmod 10),q>7$，若 C 是一个在 F_{q^2} 上，长度为 $n=\frac{q^2+1}{10}$ 的 η-常循环码，它的定义集为 $Z=\bigcup_{j=0}^{\delta}C_{s-rj}$，则存在参数为 $[\![n,n-2(2\delta+1)+c(\delta),2\delta+2;c(\delta)]\!]_q$ 的 EAQMDS 码。

当 $0\le\delta\le\frac{3q-1}{10}-1$ 时，$c(\delta)=1$；当 $\frac{3q-1}{10}\le\delta\le\frac{4q+2}{10}-1$ 时，$c(\delta)=5$；

当 $\frac{4q+2}{10}\le\delta\le\frac{5q+5}{10}-1$ 时，$c(\delta)=9$；当 $\frac{5q+5}{10}\le\delta\le\frac{6q-2}{10}-1$ 时，$c(\delta)=13$；

当$\frac{6q-2}{10}\le\delta\le\frac{7q+1}{10}-1$时，$c(\delta)=17$；当$\frac{7q+1}{10}\le\delta\le\frac{8q-6}{10}-1$时，$c(\delta)=21$；

当$\frac{8q-6}{10}\le\delta\le\frac{8q+4}{10}-1$时，$c(\delta)=25$；当$\frac{8q+4}{10}\le\delta\le\frac{9q-3}{10}$时，$c(\delta)=29$；

当$\frac{9q-3}{10}\le\delta\le\frac{9q+7}{10}-1$时，$c(\delta)=33$。

证明 由于$|Z|=2\delta+1$则从引理2.1和引理2.3得C是一个带参数为$[n,n-(2\delta+1),2\delta+2]_{q^2}$ MDS码。由引理2.4得存在参数为$[\![n,n-2(2\delta+1)+c(\delta),2\delta+2;c(\delta)]\!]_q$的EAQMDS码。当$\delta\le q-1$时，有$0\le j,k\le q-1$，得到$nl=j+qk$的表示唯一，此时相当于对$nl$做带余除法。设定$\delta\le q-1$，由于$s\equiv -qs(\bmod rn)$，根据引理2.7

$$\begin{aligned}c&=|Z\cap(-qZ)|\\&=\left|\{(j,k)|s\pm rj\equiv -q(s\pm rk)(\bmod rn),1\le j,k\le q-1\}\right|+1\\&=2\left|\{(j,k)|j+qk\equiv 0(\bmod n),1\le j,k\le q-1\}\right|\\&\quad+2\left|\{(j,k)|j-qk\equiv 0(\bmod n),1\le j,k\le q-1\}\right|+1.\end{aligned}$$

又因为

$j+qk\equiv 0(\bmod n)$有整数解(j,k)，其中$1\le j,k\le q-1$,

$\Leftrightarrow$对$1\le l\le 9,l\in Z$来说，$nl=j+qk$有整数解(j,k)，其中$1\le j,k\le q-1$。

$j-qk\equiv 0(\bmod n)$有整数解(j,k)，其中$1\le j,k\le q-1$,

$\Leftrightarrow$对$-9\le l\le -1,l\in Z$来说，$nl=j-qk$有整数解(j,k)，其中$1\le j,k\le q-1$。

取定l后把nl表示成$j+qk$这种形式，令$b_{l,1}=\max(j,k)$。

当$l=1$时，有$\frac{q^2+1}{10}=\left(\frac{q-7}{10}\right)q+\frac{7q+1}{10}$，$b_{1,1}=\frac{7q+1}{10}$；

当$l=2$时，有$2\frac{q^2+1}{10}=\left(\frac{2(q-7)}{10}+1\right)q+\frac{4q+2}{10}$，$b_{2,1}=\frac{4q+2}{10}$；

当$l=3$时，有$3\frac{q^2+1}{10}=\left(\frac{3(q-7)}{10}+2\right)q+\frac{q+3}{10}$，$b_{3,1}=\frac{3q-1}{10}$；

当$l=4$时，有$4\frac{q^2+1}{10}=\left(\frac{4(q-7)}{10}+2\right)q+\frac{8q+4}{10}$，$b_{4,1}=\frac{8q+4}{10}$；

当$l=5$时，有$5\frac{q^2+1}{10}=\left(\frac{5(q-7)}{10}+3\right)q+\frac{5q+5}{10}$，$b_{5,1}=\frac{5q+5}{10}$；

当$l=6$时，有$6\frac{q^2+1}{10}=\left(\frac{6(q-7)}{10}+4\right)q+\frac{2q+6}{10}$，$b_{6,1}=\frac{6q-2}{10}$；

当$l=7$时，有$7\frac{q^2+1}{10}=\left(\frac{7(q-7)}{10}+4\right)q+\frac{9q+7}{10}$，$b_{7,1}=\frac{9q+7}{10}$；

当$l=8$时，有$8\frac{q^2+1}{10}=\left(\frac{8(q-7)}{10}+5\right)q+\frac{6q+8}{10}$，$b_{8,1}=\frac{8q-6}{10}$；

当$l=9$时，有$9\frac{q^2+1}{10}=\left(\frac{9(q-7)}{10}+6\right)q+\frac{3q+9}{10}$，$b_{9,1}=\frac{9q-3}{10}$；

对 $1 \le l \le 9, l \in Z$，将 $b_{l,1} = \max(j,k)$ 从小到大排列，依次记为 $b_1, b_2, b_3, \cdots, b_9$。得

$$b_1 = \frac{3q-1}{10}，\quad b_2 = \frac{4q+2}{10}，\quad b_3 = \frac{5q+5}{10}，\quad b_4 = \frac{6q-2}{10}，\quad b_5 = \frac{7q+1}{10}，$$

$$b_6 = \frac{8q-6}{10}，\quad b_7 = \frac{8q+4}{10}，\quad b_8 = \frac{9q-3}{10}，\quad b_9 = \frac{9q+7}{10}.$$

由引理 3.4 得 (j,k) 是 $j+qk \equiv 0(\bmod n)$ 的解 $\Leftrightarrow$ (k,j) 是 $j-qk \equiv 0(\bmod n)$ 的解。对 $-9 \le l \le -1, l \in Z$，$nl = j-qk$，令 $b_{l,1} = \max(j,k)$，将 $b_{l,1}$ 从小到大排列，顺序依然为 $b_1, b_2, b_3, \cdots, b_9$。令 $b_0 = 0$，综上，对 $0 \le i \le 8, i \in Z$，当 $b_i \le \delta \le b_{i+1}-1$ 时，$c(\delta) = 4i+1$。

定理 3.7 q 为一个奇素数的方幂，且 $q \equiv 7(\bmod 10), q > 7$，若 C 是一个在 F_{q^2} 上，长度为 $n = \frac{q^2+1}{10}$ 的 η-常循环码，它的定义集为 $Z = \bigcup_{j=0}^{\delta} C_{s-r\left(\frac{n-1}{2}-j\right)}$，则存在参数为 $[\![n, n-2(2\delta+1)+c(\delta), 2\delta+2; c(\delta)]\!]_q$ 的 EAQMDS 码。

当 $0 \le \delta \le \frac{2q+6}{10}-1$ 时，$c(\delta) = 0$；当 $\frac{2q+6}{10} \le \delta \le \frac{4q+2}{10}-1$ 时，$c(\delta) = 4$；

当 $\frac{4q+2}{10} \le \delta \le \frac{5q+5}{10}-1$ 时，$c(\delta) = 8$；当 $\frac{5q+5}{10} \le \delta \le \frac{6q+8}{10}-1$ 时，$c(\delta) = 16$；

当 $\frac{6q+8}{10} \le \delta \le \frac{7q+1}{10}-1$ 时，$c(\delta) = 20$；当 $\frac{7q+1}{10} \le \delta \le \frac{7q+11}{10}-1$ 时，$c(\delta) = 24$；

当 $\frac{7q+11}{10} \le \delta \le \frac{8q+4}{10}-1$ 时，$c(\delta) = 28$；当 $\frac{8q+4}{10} \le \delta \le \frac{9q-3}{10}-1$ 时，$c(\delta) = 32$；

当 $\frac{9q-3}{10} \le \delta \le \frac{9q+7}{10}-1$ 时，$c(\delta) = 36$。

证明 由于 $|Z| = 2\delta+1$ 则从引理 2.1 和引理 2.3 得 C 是参数为 $[n, n-(2\delta+1), 2\delta+2]_{q^2}$ 的 MDS 码。由引理 2.4 得存在参数为 $[\![n, n-2(2\delta+1)+c(\delta), 2\delta+2; c(\delta)]\!]_q$ 的 EAQMDS 码。当 $\delta \le q-1$ 时，有 $0 \le j,k \le q-1$，得到 $nl = j+qk$ 的表示是唯一的，此时相当于对 nl 做带余除法。我们设定 $\delta \le q-1$，由引理 2.7，有

$$\begin{aligned}
c &= |Z \cap (-qZ)| \\
&= \left|\left\{(j,k) \middle| s \pm r(\frac{n-1}{2}-j) \equiv -q(s \pm r\left(\frac{n-1}{2}-k\right)(\bmod rn), 0 \le j,k \le q-1\right\}\right| \\
&= 2\left|\left\{(j,k) \middle| j+qk-\frac{q+1}{2} \equiv 0(\bmod n), 0 \le j,k \le q-1\right\}\right| \\
&\quad + 2\left|\left\{(j,k) \middle| j-qk+\frac{q-1}{2} \equiv 0(\bmod n), 0 \le j,k \le q-1\right\}\right|.
\end{aligned}$$

而我们知道

$j+qk-\frac{q+1}{2} \equiv 0(\bmod n)$ 有整数解 (j,k)，其中 $0 \le j,k \le q-1$,

$\Leftrightarrow$ 对 $0 \le l \le 9, l \in Z$ 来说，$nl+\frac{q+1}{2} = j+qk$ 有整数解 (j,k)，其中 $0 \le j,k \le q-1$。

$j-qk+\frac{q-1}{2} \equiv 0(\bmod n)$ 有整数解 (j,k)，其中 $0 \le j,k \le q-1$,

$\Leftrightarrow$ 对 $-9 \le l \le 0, l \in Z$ 来说，$nl-\frac{q-1}{2} = j-qk$ 有整数解 (j,k)，其中 $0 \le j,k \le q-1$。

取定 l 后把 $nl+\frac{q+1}{2}$ 表示成 $j+qk$ 这种形式，令 $b_{l,1}=\max(j,k)$。对 $0\le l\le 9, l\in Z$，将 $b_{l,1}$ 从小到大排列，依次记为 $b_0,b_1,b_2,b_3,\cdots,b_9$。得

$$b_0=\frac{2q+6}{10},\quad b_1=\frac{4q+2}{10},\quad b_2=\frac{5q+5}{10},\quad b_3=\frac{5q+5}{10},\quad b_4=\frac{6q+8}{10},$$
$$b_5=\frac{7q+1}{10},\quad b_6=\frac{7q+11}{10},\quad b_7=\frac{8q+4}{10},\quad b_8=\frac{9q-3}{10},\quad b_9=\frac{9q+7}{10}。$$

由引理 3.5 得 $j+qk-\frac{q+1}{2}\equiv 0(\bmod n)$ 有解 $(j,k)\Leftrightarrow j-qk+\frac{q-1}{2}\equiv 0(\bmod n)$ 有解 (k,j)。对 $-9\le l\le -1, l\in Z$，$nl=j-qk$，令 $b_{l,1}=\max(j,k)$。将 $b_{l,1}$ 从小到大排列，顺序依然为 $b_0,b_1,b_2,b_3,\cdots,b_9$。综上即可得出结论。

定理 3.8 q 为一个奇素数的方幂，且 $q\equiv 21(\bmod 34), q>21$，若 C 是一个在 F_{q^2} 上，长度为 $n=\frac{q^2+1}{34}$ 的 η-常循环码，它的定义集为 $Z=\bigcup_{j=0}^{\delta}C_{s-rj}$，则存在参数为 $[[n,n-2(2\delta+1)+c(\delta),2\delta+2;c(\delta)]]_q$ 的 EAQMDS 码。有

$$b_0=0,\quad b_1=\frac{5q-3}{34},\quad b_2=\frac{8q+2}{34},\quad b_3=\frac{10q-6}{34},\quad b_4=\frac{11q+7}{34},$$
$$b_5=\frac{13q-1}{34},\quad b_6=\frac{14q+12}{34},\quad b_7=\frac{15q-9}{34},\quad b_8=\frac{16q+4}{34},\quad b_9=\frac{17q+17}{34},$$
$$b_{10}=\frac{18q-4}{34},\quad b_{11}=\frac{19q+9}{34},\quad b_{12}=\frac{20q-12}{34},\quad b_{13}=\frac{21q+1}{34},\quad b_{14}=\frac{22q-20}{34},$$
$$b_{15}=\frac{22q+14}{34},\quad b_{16}=\frac{23q-7}{34},\quad b_{17}=\frac{24q+6}{34},\quad b_{18}=\frac{25q-15}{34},\quad b_{19}=\frac{25q+19}{34},$$
$$b_{20}=\frac{26q-2}{34},\quad b_{21}=\frac{27q-23}{34},\quad b_{22}=\frac{27q+11}{34},\quad b_{23}=\frac{28q-10}{34},\quad b_{24}=\frac{28q+24}{34},$$
$$b_{25}=\frac{29q+3}{34},\quad b_{26}=\frac{30q-18}{34},\quad b_{27}=\frac{30q+16}{34},\quad b_{28}=\frac{31q-5}{34},\quad b_{29}=\frac{31q+29}{34},$$
$$b_{30}=\frac{32q-26}{34},\quad b_{31}=\frac{32q+8}{34},\quad b_{32}=\frac{33q-13}{34},\quad b_{33}=\frac{33q+21}{34},\quad b_{34}=q$$

对 $0\le i\le 33, i\in Z$，当 $b_i\le\delta\le b_{i+1}-1$ 时，$c(\delta)=4i+1$。

证明 证明过程与定理 3.6 类似，此处省略。

参考文献

[1] Lin, X.Y. (2004) Quantum Cyclic and Constacyclic Codes. *IEEE Transactions on Information Theory*, **50**, 547-549. https://doi.org/10.1109/TIT.2004.825502

[2] Chen, H. (2001) Some Good Quantum Error-Correcting Codes from Algebraic-Geometric Codes. *IEEE Transactions on Information Theory*, **47**, 2059-2061. https://doi.org/10.1109/18.930942

[3] Qian, J. and Zhang, L. (2013) New Optimal Subsystem Codes. *Discrete Mathematics*, **313**, 2451-2455. https://doi.org/10.1016/j.disc.2013.06.021

[4] Ketkar, A., Klappenecker, A., Kumar, S. and Sarvepalli, P.K. (2006) Nonbinary Stabilizer Codes over Finite Fields. *IEEE Transactions on Information Theory*, **52**, 4892-4914. https://doi.org/10.1109/TIT.2006.883612

[5] Brun, T., Devetak, I. and Hsieh, M.-H. (2006) Correcting Quantum Errors with Entanglement. *Science*, **52**, 436-439. https://doi.org/10.1126/science.1131563

[6] Fan, J., Chen, H. and Xu, J. (2016) Constructions of q-Ary Entanglement-Assisted Quantum MDS Codes with Minimum Distance Greater Than q + 1. *Quantum Information and Computation*, **16**, 423-434.

[7] Li, R., Zuo, F. and Liu, Y. (2011) A Study of Skew Asymmetric q2-Cyclotomic Coset and Its Application. *Journal of Air Force Engineering University* (*Natural Science Edition*), **12**, 87-89.

[8] Chen, J., Huang, Y., Feng, C. and Chen, R. (2017) Entanglement-Assisted Quantum MDS Codes Constructed from Negacyclic Codes. *Quantum Information Processing*, **16**, 303. https://doi.org/10.1007/s11128-017-1750-4

[9] Lu, L.D., Li, R.H., Guo, L.B., Ma, Y.N. and Liu, Y. (2018) Entanglement-Assisted Quantum MDS Codes from Negacyclic Codes. *Quantum Information Processing*, **17**, 69. https://doi.org/10.1007/s11128-018-1838-5

[10] Chen, X., Zhu, S. and Kai, X. (2018) Entanglement-Assisted Quantum MDS Codes Constructed from Constacyclic Codes. *Quantum Information Processing*, **17**, 273. https://doi.org/10.1007/s11128-018-2044-1

[11] Koroglu, M.E. (2018) New Entanglement-Assisted MDS Quantum Cods from Constacyclic Codes. *Quantum Information Processing*, **18**, 44. https://doi.org/10.1007/s11128-018-2155-8

[12] Zhang, T. and Ge, G. (2017) Quantum MDS Codes with Large Minimum Distance. *Designs*, *Codes and Cryptography*, **83**, 503-517. https://doi.org/10.1007/s10623-016-0245-0

[13] Aydin, N., Siap, I. and Ray-Chaudhuri, D.K. (2001) The Structure of 1-Generator Quasi-Twisted Codes and New Linear Codes. *Designs*, *Codes and Cryptography*, **24**, 313-326. https://doi.org/10.1023/A:1011283523000

[14] Kai, X., Zhu, S. and Li, P. (2014) Constacyclic Codes and Some New Quantum MDS Codes. *IEEE Transactions on Information Theory*, **60**, 2080-2086. https://doi.org/10.1109/TIT.2014.2308180

[15] MacWilliams, F.J. and Sloane, N.J.A. (1977) The Theory of Error-Correcting Codes. Elsevier, Amsterdam, North-Holland, 370-762.

[16] Lu, L. and Li, R. (2014) Entanglement-Assisted Quantum Codes Constructed from Primitive Quaternary BCH Codes. *International Journal of Quantum Information*, **12**, Article No. 1450015. https://doi.org/10.1142/S0219749914500154