Modern Physics 现代物理,2019, 9(2), 114-119
Published Online March 2019 in Hans. http://www.hanspub.org/journal/mp
https://doi.org/10.12677/mp.2019.92013

Hans汉斯

Constructing $\left[\left[\frac{q^2+1}{53}, \frac{q^2+1}{53}-2d+2, d\right]\right]_q$ Quantum MDS Code

Meifang Zhao[1], Pengfei Guo[2*]

[1]Mathematics Institute, South China University of Technology, Guangzhou Guangdong
[2]College of Computational Science, Zhongkai University of Agriculture and Engineering, Guangzhou Guangdong
Email: 1669574413@qq.com, *450799063@qq.com

Received: Mar. 5th, 2019; accepted: Mar. 20th, 2019; published: Mar. 28th, 2019

Abstract

Quantum MDS codes are an important class of quantum codes. In this paper, we construct new quantum MDS code $\left[\left[\frac{q^2+1}{53}, \frac{q^2+1}{53}-2d+2, d\right]\right]_q$, the integer d belongs to $[2, 18m+4]$ and is even if $q=106m+23$ and the integer d belongs to $[2, 18m+4]$ and is even if $q=106m+83$.

Keywords

Conjugate Orthogonal, Quantum MDS Codes, Constacyclic Codes

构造$\left[\left[\frac{q^2+1}{53}, \frac{q^2+1}{53}-2d+2, d\right]\right]_q$量子MDS码

赵梅芳[1]，郭鹏飞[2*]

[1]华南理工大学数学学院，广东 广州
[2]仲恺农业工程学院计算科学学院，广东 广州
Email: 1669574413@qq.com, *450799063@qq.com

收稿日期：2019年3月5日；录用日期：2019年3月20日；发布日期：2019年3月28日
*通讯作者。

文章引用: 赵梅芳, 郭鹏飞. 构造$\left[\left[\frac{q^2+1}{53}, \frac{q^2+1}{53}-2d+2, d\right]\right]_q$量子 MDS 码[J]. 现代物理, 2019, 9(2): 114-119.

DOI: 10.12677/mp.2019.92013

摘　要

量子MDS码是一类重要的量子码。本文利用常循环码和Hermitian构造理论构造一种新的量子MDS码 $\left[\left[\frac{q^2+1}{53},\frac{q^2+1}{53}-2d+2,d\right]\right]_q$，其中 $q=106m+23$ 时，整数 d 在区间 $[2,18m+4]$ 且为偶数；其中 $q=106m+83$ 时，整数 d 在区间 $[2,18m+4]$ 且为偶数。

关键词

共轭正交，量子MDS码，常循环码

1. 引言

量子纠错码在量子信息理论和量子计算机发展进程中有着重要地位。与经典编码理论一样，量子理论中的一个主要问题是构建具有最佳可能最小距离的量子编码。许多量子编码已经通过使用经典方法构建出来了具有 Euclidean 或 Hermitian 自正交性的纠错码[1]-[7]。

设 q 是一个素数的幂，码长为 n 和码字个数为 K 的 q 元量子码 Q 是指一个 q^n 维希尔伯特空间 $H=\left(C^q\right)^{\otimes n}=C^q\otimes\cdots\otimes C^q$ 的一个 $k=\log_q K$ 维子空间。用 $\left[\left[n,k,d\right]\right]_q$ 表示码长为 n 最小距离为 d 的 q 元量子码，则此码可以检查 $\le d-1$ 错也可以纠正 $\le\left\lfloor\frac{d-1}{2}\right\rfloor$ 位错[8]。特别地，对于量子码 $\left[\left[n,k,d\right]\right]_q$ 均须达到满足量子 Singleton 边界：$n\ge k+2d-2$。当量子码达到边界：$n=k+2d-2$，称为量子极大可分码(MDS码)。近些年构造良好性能的量子纠错码成为热门研究。同样利用 Hermitian Construction 理论，本文构造了一种新的 MDS 码。

2. 基本概念与预备知识

首先，介绍一些基本概念[8]。令 q 为一个奇素数的幂，F_{q^2} 记为有 q^2 个元素的有限域.

下面在有限域 F_{q^2} 上定义 Hermitian 内积：

设 $x=(x_1,x_2,\cdots,x_n),y=(y_1,y_2,\cdots,y_n)\in F_{q^2}^n$，则 x 和 y 的 Hermitian 内积为 $(x,y)=\sum_{i=1}^n x_i\overline{y}_i$，其中 $\overline{y}_i=y_i^q$。如果 $(x,y)=0$，则称 x，y 正交。

经典的 q^2 元线性码 C 是 F_{q^2} 上的 n 维向量空间 F_{q^2} 的一个 k 维子空间，记为 $\left[\left[n,k,d\right]\right]_{q^2}$，其中 d 是码 C 的非零码字 c 的最小 Hamming 重量。

线性码 C 的 Hermitian 对偶码定义为：$C^{\perp_H}=\left\{x\in F_{q^2}\,\middle|\,(x,y)=0,\forall y\in C\right\}$。当 $C\subseteq C^{\perp_H}$ 时，C 叫做自正交码；当 $C=C^{\perp_H}$ 时，C 叫做自对偶码。

定义 1 [9]：F_{q^2} 上码长为 n 的线性码 C 称为常循环码是指对 $\eta\in F_{q^2}^*$，如果 $c=(c_0,c_1,\cdots,c_{n-1})\in C$，那么 $c'=(\eta c_{n-1},c_0,\cdots,c_{n-2})\in C$。

当 $\eta=1$ 时，C 为循环码；当 $\eta=-1$ 时，C 为负循环码。

如果把码字 $c=(c_0,c_1,\cdots,c_{n-1})\in C$ 写成多项式 $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ 并且看成商环 $R=F_{q^2}/(x^n-\eta)$ 中的元素，则 C 是 $\eta-$ 常循环码的充要条件为 $C=F_{q^2}/(x^n-\eta)$ 是商环 R 的一个理想。易知 C 是主理想，由 $x^n-\eta$ 的单项式因子生成，即 $C=(g(x))$， $g(x)|x^n-\eta$。 $g(x)$ 称为 $\eta-$ 常循环码的生成式并且 $\dim(c)=n-k$，其中 $k=\deg(g(x))$。

假设 $\gcd(n,q)=1$。 ω 是个 rn 次本原单位根属于 F_{q^2} 的某些扩域中使得 $\omega^n=\eta$。令 $\xi=\omega^r$，那么 ξ 是 n 次本原单位根，则 $x^n-\eta=\prod_{i=1}^{n-1}(x-\omega^{1+ir})$。

令 $\Omega=\{1+ir|0\le i\le n-1\}$ 对于 $\forall j\in\Omega$，集合 C_j 表示包含 j 模 rn 的 q^2- 分圆陪集，即 $C_j=\{j,jq^2,\cdots,jq^{2(k-1)}\}(\mathrm{mod}\,rn)$， k 是满足 $j\equiv jq^{2k}(\mathrm{mod}\,rn)$ 的最小正整数。 $T=\{j\in\Omega|g(\omega^j)=0\}$ 称为 $\eta-$ 常循环码 C 的定义集。可以看到定义集 T 是一些模 rn 的 q^2- 分圆陪集的并而且 $\dim(C)=n-|T|$。

如果 C 有定义集 T，易知 $C^{\perp_H}$ 的定义集 $T^{\perp_H}=\{s\in\Omega|-qs\,\mathrm{mod}\,rn\notin T\}$。

定理 2 [2] [5]：(Hermitian Construction)如果 C 是一个 $[[n,k,d]]_{q^2}$ 线性码使得 $C^{\perp_H}\subseteq C$，那么存在一个 $[[n,2k-n,\ge d]]_q$ 量子码。

设 C 的生成式为 $g(x)=\prod_{j\in T}(x-\omega^j)$，则 $C^{\perp_H}$ 的生成式为 $g^{\perp_H}(x)=\prod_{j\in\Omega\setminus T}(x-\omega^{-qj})$。那么 $C^{\perp_H}\subseteq C$ 当且仅当 $g(x)|g^{\perp_H}(x)$。因此，我们有如下引理：

引理 3：设 C 是码长为 n 的 q^2 元常循环码且定义集为 T。那么 $C^{\perp_H}\subseteq C$ 当且仅当 $T\cap T^{-q}=\varnothing$，其中 $T^{-q}=\{-qs\,\mathrm{mod}\,rn|s\in T\}$。

因为循环码与常循环吗有惊人的相似性，我们给出偏斜对称和偏斜非对称的对应关系如下：

如果 $rn-qs\,\mathrm{mod}\,rn\in C_s$，则分圆陪集 C_s 是斜对称的；否则是不对称。如果不对称，则不对称陪集 C_s 和 C_{rn-qs} 成对出现，我们用 (C_s,C_{rn-qs}) 表示这样的一对。

引理 4：设 r 是 $q+1$ 的正因子，$\eta\in F_{q^2}^*$，$ord(\eta)=r$。设 $\gcd(q,n)=1$，$ord_{rn}(q^2)=m$，$0\le x,y,z\le n-1$。

1) C_s 是对称陪集当且仅当存在 $t\le\left\lfloor\frac{m}{2}\right\rfloor$ 使得 $x\equiv xq^{2t+1}(\mathrm{mod}\,rn)$。

2) 如果 $C_y\ne C_z$，(C_y,C_z) 形成一对不对称陪集当且仅当存在 $t\le\left\lfloor\frac{m}{2}\right\rfloor$ 使得 $y\equiv yq^{2t+1}(\mathrm{mod}\,rn)$ 或者 $z\equiv zq^{2t+1}(\mathrm{mod}\,rn)$。

由这个引理可以得出下面引理：

引理 5：设 r 是 $q+1$ 的正因子，$\eta\in F_{q^2}^*$，$ord(\eta)=r$。设 C 是码长为 n 的 q^2 元常循环码且定义集为 T，那么 $C^{\perp_H}\subseteq C$ 等价条件为：

1) $T\cap T^{-q}=\varnothing$，其中 $T^{-q}=\{-qs\,\mathrm{mod}\,rn|s\in T\}$。

2) 如果 $i,j,k\in T$，那么 C_i 不是偏斜非对称的和 (C_j,C_k) 不是成对非对称陪集。

定理 6：($\eta-$ 常循环码 BCH 界[4])设 C 是 F_{q^2} 码长为 n 的 $\eta-$ 常循环码，生成式 $g(x)$ 的根包括 $\{\omega^{1+ir}|i_1\le i\le i_1+d-2\}$，那么 C 的最小距离 $\ge d$。

3. 量子 MDS 码构造

引理 7 [2]：给定 $r=q+1$，设 $n=\frac{q^2+1}{53}$ 和 $s=\frac{q^2+1}{2}$，对于 $\forall j\in\Omega=\{1+(q+1)i|0\le i\le n-1\}$，有

1) $C_s=\{s\}$ 和 $C_{s+\frac{(q+1)n}{2}}=\left\{s+\frac{(q+1)n}{2}\right\}$；

2) $C_{s-(q+1)j}=\{s-(q+1)j,s+(q+1)j\}$，$1\le j\le\frac{n}{2}-1$。

定理 8：设 q 为一个奇素数的幂，$n=\frac{q^2+1}{53}$ 和 $s=\frac{q^2+1}{2}$，且 C 是码长为 n 的 q^2 元 $\eta-$ 常循环码及定义集 $T=\bigcup_{j=0}^{\delta}C_{s+(q+1)j}$。由 $m\ge 0$ 是正整数，则

1) 如果 $q=106m+23$，$0\le\delta\le 9m+1$，则 $C^{\perp_H}\subseteq C$。

2) 如果 $q=106m+83$，$0\le\delta\le 9m+6$，则 $C^{\perp_H}\subseteq C$。

证明：方法一：假设 $C^{\perp_H}\not\subset C$ 也就是说 $T\bigcap T^{-q}\neq\varnothing$。因此存在两个正整数 $0\le k,l\le 9m+1$ 使得

$$s-(q+1)k\equiv -q^{\varepsilon}(s-(q+1)l)(\mathrm{mod}\,rn),\varepsilon=1,3$$

1) 如果 $\varepsilon=1$，那么

$$s-(q+1)k\equiv -q(s-(q+1)l)(\mathrm{mod}(q+1)n)$$

$$s\equiv k+ql(\mathrm{mod}\,rn)$$

$$q^2+1=106lq+106k(\mathrm{mod}\,2(q+1))$$

因为 $0\le k,l\le 9m+1$，那么 $0\le 106k,106l\le 106(9m+1)=9q-101$，$0\le 106k+106lq\le 106(9m+1)9q^2$。

令 $106k=qt+h(0\le h<q)$，则 $t=0,1,2,3,4,5,6,7,8$。

我们可知 $(106l+t)q+h=q^2+1$，$3q^2+3$，$5q^2+5$，$7q^2+7$。

① 若 $(106l+t)q+h=q^2+1\Rightarrow h=1$，那么

$$(106l+t)=q\Rightarrow t=23(\mathrm{mod}106)\Rightarrow t=23\text{ 矛盾。}$$

② 若 $(106l+t)q+h=3q^2+3\Rightarrow h=3$，那么

$$(106l+t)=3q\Rightarrow t=69(\mathrm{mod}106)\Rightarrow t=69\text{ 矛盾。}$$

③ 若 $(106l+t)q+h=5q^2+5\Rightarrow h=5$，那么

$$(106l+t)=5q\Rightarrow t=105(\mathrm{mod}106)\Rightarrow t=9\text{ 矛盾。}$$

④ 若 $(106l+t)q+h=7q^2+7\Rightarrow h=7$，那么

$$(106l+t)=7q\Rightarrow t=161(\mathrm{mod}106)\Rightarrow t=55\text{ 矛盾。}$$

1) 如果 $\varepsilon=3$，那么

$$s-(q+1)k\equiv -q^3(s-(q+1)l)(\mathrm{mod}(q+1)n)$$

$$106lq\equiv 106k(\mathrm{mod}\,q^2+1)$$

$$106lq\equiv qt+h(\mathrm{mod}\,q^2+1)$$

那么 $106lq=qt+h+p(q^2+1)$，其中 $0\le p\le 8$。

① 如果 $p=0$ 那么 $106lq=106k$。不可能成立。

② 如果 $p\neq 0$ 那么 $106lq=qt+h+p(q^2+1)\Rightarrow h+p=(106l-t-pq)q\Rightarrow h\equiv -p(\mathrm{mod}\,q)\Rightarrow h=q-p$。

接下来，我们有 $1=106l-t-pq$，则

$$1\equiv 106l-t-p(106m+23)(\mathrm{mod}106)$$

$$1\equiv -t-23p(\mathrm{mod}106)$$

不可能成立。由(1)(2)可知假设不成立，所以 $T\cap T^{-q}=\varnothing$。

方法二：通过引理 5，想证明 $C^{\perp_H}\subseteq C$ 则需要证明 $T=\bigcup_{j=0}^{\delta}C_{s+(q+1)j}$ 中不存在偏斜对称分圆陪集以及任何两个偏斜非对称分圆陪集成对出现。

令 $q=106m+23$，则 $n=\dfrac{q^2+1}{53}=212m^2+92m+10$，$s=\dfrac{q^2+1}{2}=5618m^2+2438m+265$。

令 $x,y\in Z=\left\{s+(q+1)j\middle|0\le j\le 9m+1\right\}$。我们需要证明 $x+yq\neq 0(\bmod rn)$ 成立。

令 $Z=\bigcup_{i=1}^{5}I_i$，$I_1=\left[s,s+(q+1)m\right]$，$I_2=\left[s+(q+1)(m+1),s+(q+1)3m\right]$，

$I_3=\left[s+(q+1)(3m+1),s+(q+1)(5m+1)\right]$，$I_4=\left[s+(q+1)(3m+2),s+(q+1)(7m+1)\right]$，

$$I_5=\left[s+(q+1)(7m+2),s+(q+1)(9m+1)\right]。$$

① $x\in I_1$ 时 $26rn<26rn+\dfrac{(q^2+1)(q+1)}{106}=s(q+1)\le x(q+1)\le\left[s+(q+1)m\right](q+1)<27rn$。

② $x\in I_2$ 时 $27rn<\left[s+(q+1)(m+1)\right](q+1)\le x(q+1)\le\left[s+(q+1)3m\right](q+1)<28rn$。

③ $x\in I_3$ 时 $28rn<\left[s+(q+1)(3m+1)\right](q+1)\le x(q+1)\le\left[s+(q+1)(5m+1)\right](q+1)<29rn$。

④ $x\in I_4$ 时 $29rn<\left[s+(q+1)(5m+2)\right](q+1)\le x(q+1)\le\left[s+(q+1)(7m+1)\right](q+1)<30rn$。

⑤ $x\in I_5$ 时 $30rn<\left[s+(q+1)(7m+2)\right](q+1)\le x(q+1)\le\left[s+(q+1)(9m+1)\right](q+1)<31rn$。

因此在 T 中不存在任何偏斜对称分圆陪集。

① $x,y\in I_1$ 时，$26rn<x+yq<27rn$。

② $x,y\in I_2$ 时，$27rn<x+yq<28rn$。

③ $x,y\in I_3$ 时，$28rn<x+yq<29rn$。

④ $x,y\in I_4$ 时，$29rn<x+yq<30rn$。

⑤ $x,y\in I_5$ 时，$30rn<x+yq<31rn$。

⑥ $x\in I_1\cup I_2,y\in I_1$ 时，$26rn<x+yq<27rn$。

⑦ $x\in I_1\cup I_2\cup I_3,y\in I_1$ 时，$26rn<x+yq<27rn$。

⑧ $x\in I_1\cup I_2\cup I_3\cup I_4,y\in I_1$ 时，$26rn<x+yq<27rn$。

⑨ $x\in I_1\cup I_2\cup I_3\cup I_4\cup I_5,y\in I_1$ 时，$26rn<x+yq<27rn$。

⑩ $x\in I_2\cup I_3,y\in I_2$ 时，$27rn<x+yq<28rn$。

⑪ $x\in I_2\cup I_3\cup I_4,y\in I_2$ 时，$26rn<x+yq<27rn$。

⑫ $x\in I_2\cup I_3\cup I_4\cup I_5,y\in I_2$ 时，$26rn<x+yq<27rn$。

⑬ $x\in I_3\cup I_4,y\in I_3$ 时，$28rn<x+yq<29rn$。

⑭ $x\in I_3\cup I_4\cup I_5,y\in I_3$ 时，$28rn<x+yq<29rn$。

⑮ $x\in I_4\cup I_5,y\in I_4$ 时，$29rn<x+yq<30rn$。因此不存在偏斜非对称分圆陪集成对出现。

定理 9：如果 $q=106m+23$ 或 $q=106m+83$，则存在 $\left[\left[\dfrac{q^2+1}{53},\dfrac{q^2+1}{53}-2d+2,d\right]\right]_q$ 量子 MDS 码。当 $q=106m+23$ 时，$2\le d\le 18m+4$ 且为偶数；当 $q=106m+83$ 时，$2\le d\le 18m+14$ 且为偶数。

证明：$2\le d\le 18m+14$，当 $2\le d\le 18m+14$ 时，考虑 F_{q^2} 域上码长为 $n=\dfrac{q^2+1}{53}$ 上的 $\eta-$ 常循环码 C 并且它的定义集 $T=\bigcup_{j=0}^{\delta}C_{s+(q+1)j}$，$0\le\delta\le 9m+1$，通过引理 8，可知 $C^{\perp_H}\subseteq C$ 又由引理 7，可知 T 包含 $2\delta+1$ 个元素 $\left\{s-(q+1)\delta,\cdots,s,s+(q+1),\cdots,s+(q+1)\delta\right\}$。说明 C 的最小距离 $d_C\ge 2\delta+2$ 且为偶数。因此 C 的参

数为$\left[n, n-\left(2\delta+1\right), \geq 2\delta+2\right]_{q^2}$。由 Hermitian Construction 定理和量子 Singleton 界可知存在量子 MDS 码$\left[\left[n, n-4\delta-2, 2\delta+2\right]\right]_q$。因此$\left[\left[\frac{q^2+1}{53}, \frac{q^2+1}{53}-2d+2, d\right]\right]_q$，$2 \leq d \leq 18m+4$ 量子 MDS 码存在。

同理当$q=106m+83$时，$\left[\left[\frac{q^2+1}{53}, \frac{q^2+1}{53}-2d+2, d\right]\right]_q$，$2 \leq d \leq 18m+14$ 量子 MDS 码存在。

参考文献

[1] 钱建发, 马文平. 量子纠错码的一个统一构造方法[J]. 计算机科学, 2010, 37(3): 70-72.

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

[3] Kai, X.S. and Zhu, S.X. (2013) New Quantum MDS Codes from Negacyclic Codes. *IEEE Transactions on Information Theory*, **59**, 1193-1197. https://doi.org/10.1109/TIT.2012.2220519

[4] Taneja, D., Gupta, M., Narula, R. and Bhullar, J. (2017) Construction of New Quantum MDS Codes Derived from Constacyclic Codes. *International Journal of Quantum Information*,**15**, 1750008-1-175008-12. https://doi.org/10.1142/S0219749917500083

[5] Chen, B.C., Ling, S. and Zhang, G.H. (2015) Application of Constacyclic Codes to Quantum MDS Codes. *IEEE Transactions on Information Theory*, **61**, 1474-1484. https://doi.org/10.1109/TIT.2015.2388576

[6] Shi, X.,Yue, Q. and Zhu, X. (2017) Construction of Some New Quantum MDS Codes. *Finite Fields and Their Applications*, **46**, 347-362. https://doi.org/10.1016/j.ffa.2017.04.002

[7] Jin, L.,Ling, S., Luo, L. and Xing, C. (2010) Application of Classical Hermitian Self-Orthogonal MDS Codes to Quantum MDS Codes. *IEEE Transactions on Information Theory*, **56**, 4735-4740. https://doi.org/10.1109/TIT.2010.2054174

[8] 冯克勤, 陈豪. 量子纠错码[M]. 北京: 科学出版社, 2010.

[9] Yang, Y. and Cai, W. (2015) On Self-Dual Constacyclic Codes over Finite Fields. *Designs*, *Codes and Cryptography*, **74**, 355-364. https://doi.org/10.1007/s10623-013-9865-9