Pure Mathematics 理论数学, 2018, 8(6), 644-649
Published Online November 2018 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2018.86086

A Class of New Quantum MDS Codes from Constacyclic Codes

Na Huang*, Xiling Tang
School of Mathematics, South China University of Technology, Guangzhou Guangdong
Email: xilintang2016@sina.com

Received: Oct. 19th, 2018; accepted: Oct. 31st, 2018; published: Nov. 13th, 2018

Abstract

Quantum MDS codes are an important family of quantum codes. In this paper, we obtain a new class of quantum MDS code of the length $n=\frac{q^2+1}{a}$ by means of Hermitian construction and constacyclic codes. The result is generalized of the theorem 7 in [13].

Keywords

Quantum MDS Codes, Hermitian Construction, Constacyclic Codes

基于Constacyclic码构造的一类新的量子MDS码

黄 娜*，唐西林
华南理工大学数学学院，广东 广州
Email: xilintang2016@sina.com

收稿日期：2018年10月19日；录用日期：2018年10月31日；发布日期：2018年11月13日

摘 要

量子MDS码是一类重要的量子码。在这篇文章中，我们通过厄米特结构和常循环码构造一类长度为$n=\frac{q^2+1}{a}$新的量子MDS码。这个结果是文献[13]中定理7的延伸。

*第一作者。

文章引用: 黄娜, 唐西林. 基于 Constacyclic 码构造的一类新的量子 MDS 码[J]. 理论数学, 2018, 8(6): 644-649.
DOI: 10.12677/pm.2018.86086

关键词

量子MDS码，Hermitian结构，Constacyclic码

1. 引言

量子纠错码在量子应用和量子通信中发挥着重要的作用。自从 Calderbank 等人(见[1])建立了量子码和经典码之间的联系以来，量子纠错码领域已经取得了很大的进步。近年来，通过欧几里得或厄米特自正交的经典纠错码构造了大量的量子码(见[2] [3] [4])。

一个 q 元量子码具有 3 个参数：码长，码字数和最小距离。一个具有码长为 n，码字数为 K 的 q 元量子码 Q 是 q^n 维 Hillbert 空间 $\left(C^q\right)^{\otimes n}$ 的一个 K 维子空间，令 $k=\log_q K$，则码长为 n，最小距离为 d 的量子码被记为 $[\![n,k,d]\!]_q$。参数为 $[\![n,k,d]\!]_q$ 的 q 元量子码可以检查 $d-1$ 位错误。纠正 $\left\lfloor \frac{d-1}{2} \right\rfloor$ 位错误。因此，在量子码理论中，一个主要的任务就是构造具有较大极小距离的量子码。带参数为 $[\![n,k,d]\!]_q$ 的 q 元量子码都满足量子 Singleton 界(见[5])：$k \le n-2d+2$。当达到量子 Singleton 界，即 $k=n-2d+2$ 的量子码称为 q 元量子极大距离可分离码(简称量子 MDS 码)。

量子 MDS 码是量子码中最重要的一类，它在理论和应用上都有着非常重要的意义。近年来，很多 q 元量子 MDS 码通过使用不同的方法被构造，其中一个重要的方法是 Hermitian 正交码方法，即利用一个定义在有限域 F_{q^2} 上关于 Hermitian 内积自正交的线性 MDS 码来构造一个 q 元量子 MDS 码。近年来常用的一些 MDS 线性码有：Reed Solomon 码、循环码、negacyclic 码、constacyclic 码等等，说明它是 Hermitian 自正交码就能去构造相应的 q 元量子 MDS 码(见[1] [6]-[16])。

当 q 为奇素数的方幂时，构造具有较大最小距离且码长 $q+1 \le n \le q^2-1$ 的量子 MDS 码是困难的。一些码长为 $n=\frac{q^2-1}{a}$ 已经被构造出来了，这些 q 元量子 MDS 码大都是利用 Hermitian 自正交码方法由线性 MDS 码得到。文献[13]构造了码长为 $n=\frac{q^2+1}{5}\left(q=10m\pm 3\right)$，且具有较大距离的量子 MDS 码。

本文主要从参考文献[13]中，码长为 $n=\frac{q^2+1}{5}\left(q=10m\pm 3\right)$ 的 q 元量子 MDS 码出发，构造了码长为 $n=\frac{q^2+1}{a}\left(q=2am\pm\sqrt{2a-1}\right)$，且具有较大距离的量子 MDS 码。

2. 预备知识

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，$F_{q^2}^n$ 为 F_{q^2} 的 n 维向量空间，一个具有参数为 $[n,k,d]_{q^2}$ 的线性码 C 是指有限域 F_{q^2} 上 n 维向量空间中最小距离为 d 的 k 维子空间，其中最小距离 d 为不同码字之间的 Hemming 距离的最小值，线性码 C 满足 Singleton 界：$k \le n-2d+2$。如果 C 达到 Singleton 界，即 $k=n-2d+2$，则称此线性码 C 为极大距离可分码，简称 MDS 码。

给任意两个向量 $X=\left(x_1,x_2,\cdots,x_n\right), Y=\left(y_1,y_2,\cdots,y_n\right)\in F_{q^2}^n$，定义 Hermitian 内积 $\langle X,Y\rangle=\sum_{i=1}^{n}x_i y_i^q$。如

果 $\langle X,Y\rangle=0$，则称这两个向量 Hermitian 正交。定义 $C^{\perp H}=\left\{X\in F_{q^2}^n \middle| \langle X,Y\rangle=0,\forall Y\in C\right\}$ 为线性码的对偶码，如果 $C\subseteq C^{\perp H}$，则 C 称为一个 Hermitian 自正交码。

2.1. 量子 MDS 码

如何构造 q 元量子 MDS 码最近成为研究热点，比较常用的构造 q 元量子 MDS 码方法是 Hermitian 方法，见如下定理。

定理 2.1：(见[1])如果存在一个有限域 F_{q^2} 上参数为 $[n,k,d]_{q^2}$ 的 MDS 码 C，而且 $C\subseteq C^{\perp H}$，则可以构造出一个 q 元量子 MDS 码 $[\![n,2k-n,\geq d]\!]_q$。

通过这个定理，可由 Reed Solomon 码、循环码、negacyclic 码、constacyclic 码这些经典的 MDS 码构造出很多的 q 元量子 MDS 码，此外选择具有较大最小距离 d 的 Hermitian 自正交 MDS 码，便可得到较大最小距离的 q 元量子 MDS 码。

2.2. Constacyclic 码

设 $(n,q)=1$。对于 $\eta\in F_{q^2}^*$，一个长度为 n 的 q^2 元类线性码 C 称为 η-constacyclic 码当且仅当它在 η-constacyclic 移位下是不变的：

$$(c_0,c_1,\cdots,c_{n-1})\to(\eta c_{n-1},c_0,\cdots,c_{n-2}).$$

一个码字 $c=(c_0,c_1,\cdots,c_{n-1})$ 可以用一个多项式 $c(x)=c_0+c_1+\cdots+c_{n-1}x^{n-1}$ 表示。很容易验证一个在长度的 η-constacyclic 码是商环 $F_{q^2}[x]/\langle x^n-\eta\rangle$ 的理想，并且 $xc(x)$ 对应 $c(x)$ 的 η-constacyclic 移位。而且，如果 $F_{q^2}[x]/\langle x^n-\eta\rangle$ 是主理想，那么 $C=\langle g(x)\rangle$，其中 $g(x)$ 是 $x^n-\eta$ 的首 1 因式。如果 $\eta=1$，那么 η-constacyclic 码就为 negacyclic 码。如果 $\eta\in F_{q^2}$ 是一个 r 次本原根，那么一定会存在 rn 次本原根 ω，即 $\omega^n=\eta$。那么，我们就有 $x^n-\eta=\prod_{i=0}^{n-1}(x-\omega^{1+ir})$。类似于循环码，对于 constacyclic 码，我们也有下面的 BCH 界。

定理 2.2：(见[17])设 C 是一个在 F_{q^2} 上，长度为 n 的 η-constacyclic 码，其中 η 是一个 r 次本原根。令 ω 是 F_{q^2} 扩域上的一个 rn 次本原根，即 $\omega^n=\eta$。假设 C 的生成多项式 $g(x)$ 的根包含集合 $\left\{\omega^{1+ri}\middle| i_1\leq i\leq i_1+d-2\right\}$。那么 C 的极小距离至少为 d。

定义 $\Omega=\{1+ir|0\leq i\leq n-1\}$。对于 $\forall j\in\Omega$，C_j 为 j 模 rn 的 q^2-分圆陪集。设 C 是一个在 F_{q^2} 上，长度为 n 的 η-constacyclic 码，且 $C=\langle g(x)\rangle$，那么集合 $Z=\left\{j\in\Omega\middle| g(\omega^j)=0\right\}$ 称为集合 C 的定义集合。易知，$C=\bigcup_{j\in\Omega}C_j$ 和 $\dim(C)=n-|Z|$。此外，我们也定义 $C^{\perp H}$ 的定义集合 $Z^{\perp H}=\left\{j\in\Omega\middle| -qj(\bmod rn)\notin Z\right\}$。

因此我们有以下的引理去判断一个 η-constacyclic 码 C 是否包含 $C^{\perp H}$。

引理 2.3：(见[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-constacyclic 码，并且其定义集合为 $Z\subseteq\Omega$，那么 $C^{\perp H}\subseteq C$ 当且仅当 $Z\cap(-qZ)=\varnothing$，其中 $-qZ=\{-qz(\bmod rn)|z\in Z\}$。

3. 主要结果

为了定理的证明，我们需要以下的引理。

引理 3.1：令 $n=\dfrac{q^2+1}{a},s=\dfrac{q^2+1}{2}$ 和 $r=q+1$。那么对于正整数 $i\in\Omega=\{1+ri|0\leq i\leq n-1\}$，那么 C_j 为 j 模 $r(q+1)$ 的 q^2-分圆陪集有：

(1) $C_s=\{s\}$ 和 $C_{s+n(q+1)/2}=\{s+n(q+1)/2\}$。

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

证明：(1) 如果 $j=\dfrac{q-1}{2}$，那么 $1+(q+1)j=s$。这就说明 $s\in\Omega$。又因为 $sq^2\equiv s\bmod(q+1)n$，所以 $C_s=\{s\}$。另外，

$$[s+n(q+1)/2]q^2=sq^2+n(q+1)(q^2-1)/2+n(q+1)/2\equiv s+n(q+1)/2(\bmod(q+1)n).$$

因此，$C_{s+n(q+1)/2}=\{s+n(q+1)/2\}$。

(2) 这个证明类似于[13]中引理 3.12 的证明。

引理 3.2

(1) 令 q 是一个素数方幂且 $q=2am+t$，其中 a 是奇整数，$t=\sqrt{2a-1}$。如果 C 是一个在 F_{q^2} 上，长度为 $n=\dfrac{q^2+1}{a}$ 的 η-constacyclic 码，并且其定义集合为 $Z=\bigcup_{j=0}^{\delta}C_{s-(q+1)j}$，其中 $ord(\eta)=r$ 和 $0\le\delta\le mt$，那么 $C^{\perp H}\subseteq C$。

(2) 令 q 是一个素数方幂且 $q=2am-t$，其中 a 是奇整数，$t=\sqrt{2a-1}$。如果 C 是一个在 F_{q^2} 上，长度为 $n=\dfrac{q^2+1}{a}$ 的 η-constacyclic 码，并且其定义集合为 $Z=\bigcup_{j=0}^{\delta}C_{s-(q+1)j}$，其中 $ord(\eta)=r$ 和 $0\le\delta\le mt-2$，那么 $C^{\perp H}\subseteq C$。

证明：我们只证明第一部分，第二部分的证明是类似的。我们假设 $q=2am+t$ 和 $0\le\delta\le mt$，根据引理 2.3，我们只需要证明 $Z\cap(-qZ)=\varnothing$。利用反证法，假设存在 $0\le i\le j\le\delta$，使得 $C_{s-(q+1)i}=-qC_{s-(q+1)j}$。那么只有以下两种情况。

情况 1： $s-(q+1)i\equiv-q(s-(q+1)j)(\bmod(q+1)n)$。

那么我们有

$$i+qj-\frac{q^2+1}{2}\equiv0\left(\bmod\frac{q^2+1}{a}\right).$$

因为 $\dfrac{q^2+1}{2}=\dfrac{q^2+1}{2a}\cdot a=\dfrac{q^2+1}{2a}+\dfrac{q^2+1}{a}\cdot\dfrac{a-1}{2}$，所以

$$i+qj-\frac{q^2+1}{2a}\equiv0\left(\bmod\frac{q^2+1}{a}\right).$$

令 $q=2am+t$，则

$$i+(2am+t)j-(2am^2+2mt+1)\equiv0(\bmod 4am^2+4mt+2).$$

等式左边

$$-(2am^2+2mt+1)\le i+(2am+t)j-(2am^2+2mt+1)<\frac{t-1}{2}(4am^2+4mt+2),$$

令 $i+(2am+t)j-(2am^2+2mt+1)=x(4am^2+4mt+2)$，从而 $0\le x\le\dfrac{t-3}{2}$。因此我们有

$$i=2a(2x+1)m^2+2(2x+1)mt+2x+1-j(2am+t).$$

如果 $j \le (2x+1)m$，那么 $i \ge 2mtx+2mt+2x+1 > mt$，与已知矛盾。

如果 $j \ge (2x+1)m+1$，那么 $i \le (2xt+t-2a)m+(2x+1-t) < 0$，也与已知矛盾。

情况 2： $s-(q+1)i \equiv -q\left(s+(q+1)j\right)\left(\bmod (q+1)n\right)$。

那么我们有

$$-i+qj+\frac{q^2+1}{2} \equiv 0\left(\bmod \frac{q^2+1}{a}\right).$$

因为 $\frac{q^2+1}{2}=\frac{q^2+1}{2a}\cdot a=\frac{q^2+1}{2a}+\frac{q^2+1}{a}\cdot\frac{a-1}{2}$，所以

$$-i+qj+\frac{q^2+1}{2a} \equiv 0\left(\bmod \frac{q^2+1}{a}\right).$$

令 $q=2am+t$，则

$$-i+(2am+t)j+\left(2am^2+2mt+1\right) \equiv 0\left(\bmod 4am^2+4mt+2\right).$$

等式左边

$$2am^2+mt+1 \le -i+(2am+t)j+\left(2am^2+2mt+1\right) < \frac{t+1}{2}\left(4am^2+4mt+2\right),$$

令 $-i+(2am+t)j+\left(2am^2+2mt+1\right)=x\left(4am^2+4mt+2\right)$，从而 $1 \le x \le \frac{t-1}{2}$。因此我们有

$$i=2a(1-2x)m^2+2(1-2x)mt+1-2x+j(2am+t).$$

如果 $j \le (2x-1)m$，那么 $i \le mt-2mtx+1-2x < 0$，与已知矛盾。

如果 $j \ge (2x-1)m+1$，那么 $i \ge (t-2tx+2a)m+1-2x+t > mt$，也与已知矛盾。

所以假设不成立，故 $Z \cap (-qZ)=\varnothing$。即原命题得证。

定理 3.3：

(1) 令 q 是一个素数方幂且 $q=2am+t$，其中 a 是奇整数，$t=\sqrt{2a-1}$。那么存在一个参数为 $\left[\left[\frac{q^2+1}{a},\frac{q^2+1}{a}-2d+2,d\right]\right]$ 的 q 元的量子 MDS 码，其中 $2 \le d \le 2mt+2$ 且 d 为偶数。

(2) 令 q 是一个素数方幂且 $q=2am-t$，其中 a 是奇整数，$t=\sqrt{2a-1}$。那么存在一个参数为 $\left[\left[\frac{q^2+1}{a},\frac{q^2+1}{a}-2d+2,d\right]\right]$ 的 q 元的量子 MDS 码，其中 $2 \le d \le 2mt-2$ 且 d 为偶数。

证明 由引理 3.1 可知，除了 C_s 和 $C_{s+n(q+1)/2}$，其余的 q^2-分圆陪集都含有两个元素，再根据引理 3.2，定理 2.3，定理 2.2 和定理 2.1 易证得该定理。

推论 3.4 ([13]中定理 7)

(1) 令 q 是一个素数方幂且 $q=10m+3$，那么存在一个参数为 $\left[\left[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+2,d\right]\right]$ 的 q 元的量子 MDS 码，其中 $2 \le d \le 6m+2$ 且 d 为偶数。

(2) 令 q 是一个素数方幂且 $q=10m-3$，那么存在一个参数为 $\left[\left[\frac{q^2+1}{5},\frac{q^2+1}{5}-2d+2,d\right]\right]$ 的 q 元的量子 MDS 码，其中 $2 \le d \le 6m-2$ 且 d 为偶数。

基金项目

广州市对外科技合作项目：小弧形表面缺陷自动检测技术和系统(编号 201704030062)。

参考文献

[1] Calderbank, A.R., Rains, E.M., Shor, P.W. and Sloane, N.J.A. (1998) Quantum Error Correction via Codes over GF(4). *IEEE Transactions on Information Theory*, **44**, 1369-1387. https://doi.org/10.1109/18.681315

[2] Ashikhmin, A. and Knill, E. (2001) Nonbinary Quantum Stablizer Codes. *IEEE Transactions on Information Theory*, **47**, 3065-3072. https://doi.org/10.1109/18.959288

[3] Chen, H., Ling, S. and Xing, C. (2005) Quantum Codes from Concatenated Algebraic-Gemeotric Codes. *IEEE Transactions on Information Theory*, **51**, 2915-2920. https://doi.org/10.1109/TIT.2005.851760

[4] Aly, S.A., Klappenecker, A. and Sarvepalli, P.K. (2007) On Quantum and Classical BCH Codes. *IEEE Transactions on Information Theory*, **53**, 1183-1188. https://doi.org/10.1109/TIT.2006.890730

[5] Knill, E. and Laflamme, R. (1997) Theory of Quantum Error-Correcting Codes. *Physical Review A*, **55**, 900-911. https://doi.org/10.1103/PhysRevA.55.900

[6] Chen, B., Ling, S. and Zhang, G. (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

[7] Li, F. and Yue, Q. (2015) New Quantum MDS-Convolutional Codes Derived from Constacyclic Codes. *Modern Physics Letters B*, **29**, Article ID: 1550252. https://doi.org/10.1142/S0217984915502528

[8] Jin, L. and Xing, C. (2014) A Construction of New Quantum MDS Codes. *IEEE Transactions on Information Theory*, **60**, 2921-2925. https://doi.org/10.1109/TIT.2014.2299800

[9] Jin, L., Kan, H. and Wen, J. (2017) Quantum MDS Codes with Relatively Large Minimum Distance from Hermitian Self-Orthogonal Codes. *Designs Codes and Cryptography*, **84**, 463-471. https://doi.org/10.1007/s10623-016-0281-9

[10] Wang, L. and Zhu, S. (2015) New Quantum MDS Codes Derived from Constacyclic Codes. *Quantum Information Processing*, **14**, 881-889. https://doi.org/10.1007/s11128-014-0903-y

[11] Jin, L., Ling, S., Luo, J. and Xing, C. (2010) Application of Classic 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

[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] Zhang, T. and Ge, G. (2015) Some New Classes of Quantum MDS Codes from Constacyclic Codes. *IEEE Transactions on Information Theory*, **61**, 5224-5228. https://doi.org/10.1109/TIT.2015.2450235

[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] He, X., Xu, L. and Chen, H. (2016) New q-ary Quantum MDS Codes with Distance Bigger than $\frac{q}{2}$. *Quantum Information Processing*, **15**, 2745-2758. https://doi.org/10.1007/s11128-016-1311-2

[16] 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

[17] Yang, Y. and Cai, W. (2013) On Self-Dual Constacyclic Codes over Finite Fields. *Designs*, *Codes and Cryptography*, **74**, 355-364. https://doi.org/10.1007/s10623-013-9865-9

知网检索的两种方式：

1. 打开知网页面 http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD
   下拉列表框选择：[ISSN]，输入期刊 ISSN：2160-7583，即可查询
2. 打开知网首页 http://cnki.net/
   左侧“国际文献总库”进入，输入文章标题，即可查询