DOI:10.3969/j.issn.1003-5060.2023.01.022

一类量子负循环码的构造

刘陶然，　开晓山
(合肥工业大学 数学学院,安徽 合肥　230601)

摘　要:文章研究了有限域 F_{q^2} 上长为 $(q^4-1)/8$ 的负循环 Bose-Chaudhuri-Hocquenghem(BCH)码，其中 q 为奇素数幂且 $q\equiv 1 \pmod 4$;给出了厄米特对偶包含负循环 BCH 码的最大设计距离,并确定了它们的维数;利用厄米特构造法,得到了新的参数良好的量子码。

关键词:负循环码;厄米特对偶包含码;分圆陪集;量子码
中图分类号:O157.4　　**文献标志码**:A　　**文章编号**:1003-5060(2023)01-0141-04

Construction of a class of quantum negacyclic codes

LIU Taoran,　KAI Xiaoshan
(School of Mathematics, Hefei University of Technology, Hefei 230601, China)

Abstract: This paper studies negacyclic Bose-Chaudhuri-Hocquenghem (BCH) codes over the finite field F_{q^2} of length $(q^4-1)/8$, where q is an odd prime power and $q\equiv 1 \pmod 4$; the maximum designed distance of Hermitian dual-containing negacyclic BCH codes is given and the dimension of these codes is determined; a new class of quantum codes with good parameters is constructed using the Hermitian construction.

Key words: negacyclic codes; Hermitian dual-containing codes; cyclotomic coset; quantum codes

20 世纪 90 年代,量子码被证明是克服量子信道干扰最有效的编码方案,能实现量子比特在带有噪音的量子信道上可靠传输。量子码的理论研究的一个核心问题是构造极小距离尽可能大的量子纠错码,构造高纠错性能的量子码是近年来编码理论研究的一个热点。文献[1-4]将复杂的量子纠缠态转化为量子位上出现的几种错误类型,建立了量子纠错码与经典纠错码之间的联系。此后,编码学者们通过有限域上的各种经典码来构造量子码。

Bose-Chaudhuri-Hocquenghem (BCH)码是一类重要的循环码,其主要特点是具有高效的编码与译码算法,且其纠错能力可以通过设计距离来控制,得到了广泛的应用。文献[5]利用 BCH 码构造量子码,并给出了 BCH 码是厄米特对偶包含码的充分条件。文献[6]给出有限域 F_{q^2} 上长为 $(q^{2m}-1)/(q-1)$ 的 BCH 码是厄米特对偶包含码的一个充要条件,并且通过厄米特构造法得到了一系列量子码。常循环码是循环码的推广,它既继承了循环码的良好性能,又具有若干新特性。文献[7]给出了常循环 BCH 码的定义,并在此基础上获得了参数较好的量子码。文献[8]利用常循环码构造了具有较好参数的二元量子码。负循环码是常循环码的 1 个子类,学者们利用负循环码得到了参数较好的量子码。文献[9]研究了 2 类负循环对偶包含码,构造了量子码,相比于循环码,负循环获得的量子码具有更好的参数。此后,学者们对一些特定码长的量子常循环码展开研究。文献[10]构造了码长为 $(q^{2m}-1)/(q-1)$ 的量子负循环码;文献[11]通过厄米特构造法,

收稿日期:2021-11-03;**修回日期**:2021-12-24
基金项目:国家自然科学基金资助项目(61972126;62002093)
作者简介:刘陶然(1990—),男,内蒙古呼和浩特人,合肥工业大学硕士生;
开晓山(1975—),男,安徽合肥人,博士,合肥工业大学教授,博士生导师.

得到了2类码长为$(q+1)(q^2+1)/r$与$(q-1)\times(q^2+1)/b$的量子常循环码。

受上述工作启发,本文研究有限域F_{q^2}上长为$(q^4-1)/8$的厄米特对偶包含负循环码,其中$q\equiv 1 \pmod 4$,给出这类负循环码分圆陪集的特性,确定这类负循环厄米特对偶包含码的最大设计距离;并利用负循环码构造参数良好的量子码。

1 基础知识

设q为素数幂,F_{q^2}为含有q^2个元素的有限域。设$n\geqslant 2$是正整数且$\gcd(q,n)=1$,并且用$\mathrm{ord}_n(q^2)$表示q^2模n的乘法阶。F_{q^2}上长为n的线性码是$F_{q^2}^n$子空间。记$Z_n=\{0,1,2,\cdots,n-1\}$,对任意$i\in Z_n$,含i的模n的分圆陪集定义为$C_i=\{iq^{2z}(\mathrm{mod}\ n)\mid z\in\mathbf{Z},0\leqslant z<m=\mathrm{ord}_n(q^2)\}$。对任意$\alpha\in F_{q^2}$,$\alpha$的共轭记为$\bar{\alpha}=\alpha^q$。对任意2个向量$\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$,$\boldsymbol{y}=(y_1,y_2,y_3,\cdots,y_n)\in F_{q^2}^n$,它们的厄米特内积为$(x,y)_h=\sum_{i=1}^{n}\bar{x}_i y_i=\bar{x}_1 y_1+\bar{x}_2 y_2+\cdots+\bar{x}_n y_n$。$F_{q^2}$上长为$n$的线性码$C$的厄米特对偶码定义为$C^{\perp h}=\{\boldsymbol{x}\in F_{q^2}^n\mid (x,y)_h=0,\ \forall\, \boldsymbol{y}\in C\}$。

若$C^{\perp h}\subseteq C$,则称C为厄米特对偶包含码。若对任意码字$(c_0,c_1,\cdots,c_{n-1})\in C$,均有$(-c_{n-1},c_0,\cdots,c_{n-2})\in C$,则称$C$为$F_{q^2}$上长为$n$的负循环码。记$R_n=F_{q^2}[x]/\langle x^n+1\rangle$,$F_{q^2}$上长为$n$的负循环码$C$为$R_n$中的理想。$R_n$中的任意理想均为主理想,故$C$具有生成多项式$g(x)$,其中$g(x)$是$x^n+1$的因子。显然,$C$的维数为$k=n-\deg(g(x))$。设$\beta$为$F_{q^2}$扩域中的本原$2n$次单位根,则$x^n+1=\prod_{j=1}^{n}(x-\beta^{2j-1})$。记$\Omega_n=\{1,3,\cdots,2n-1\}$,对负循环码$C=\langle g(x)\rangle$,称$T=\{i\in\Omega_n\mid g(\beta^i)=0\}$为$C$的定义集。显然,$T$是某些$q^2$模$2n$的分圆陪集的并集。注意到$F_{q^2}$上长为$n$的负循环码的厄米特对偶码仍是负循环码。

引理1[9] 设C为F_{q^2}上长为n的负循环码,其定义集为T,则$C^{\perp h}\subseteq C$当且仅当$T\cap T^{-q}=\varnothing$,其中$T^{-q}=\{-qi(\mathrm{mod}\ 2n)\mid i\in T\}$。若$T_\rho=C_b\cup C_{b+2}\cup\cdots\cup C_{b+2(\rho-2)}$为负循环码$C$的定义集,其中$b$是奇数,则称$C$为设计距离为$\rho$的负循环BCH码。

引理2[12] F_{q^2}上长为n且设计距离为ρ的负循环BCH码的最小距离为$d\geqslant\rho$。

设V_n表示n个q维复向量空间C^q的张量积,V_n中每个非零子空间Q称为长为n的q元量子码。设Q的维数为K,称$k=\log_q K$为量子码Q的维数。长为n、维数为k、极小距离为d的q元量子码记为$[[n,k,d]]$。下面的引理3建立了经典纠错码和量子码之间的联系,给出了量子码的一个构造方法。

引理3(厄米特构造法)[4] 设C是F_{q^2}上参数为$[n,k,d]$的厄米特对偶包含码,则由C可以得到参数为$[[n,2k-n,d]]$的q元量子码。

2 量子负循环码构造

设q为奇素数幂且$q\equiv 1(\mathrm{mod}\ 4)$,下面考虑利用$F_{q^2}$上码长为$n=(q^4-1)/8$的负循环BCH码来构造$q$元量子码。首先给出$q^2$模$2n$的分圆陪集的一些性质。

引理4 设$n=(q^4-1)/8$,$s=(q^2+1)/2$,$r=(q^2-1)/8$,则

(1) $C_i=C_j$当且仅当$iq^2\equiv j(\mathrm{mod}\ 2n)$或$jq^2\equiv i(\mathrm{mod}\ 2n)$。

(2) $C_i=\{i\}$当且仅当$i=ks$($k=1,3,\cdots,4r-1$)。

证明 (1) 由$\mathrm{ord}_{2n}(q^2)=2$易知,$|C_i|$至多为2。当$i\neq j$时,$C_i=C_j$等价于$iq^2\equiv j(\mathrm{mod}\ 2n)$。又因为$iq^2\cdot q^2=i(q^4-1+1)\equiv i(\mathrm{mod}\ 2n)$,所以$iq^2\equiv j(\mathrm{mod}\ 2n)$等价于$iq^4\equiv i\equiv jq^2(\mathrm{mod}\ 2n)$。

(2) 对于$i\in T$,$C_i=\{i\}$当且仅当$iq^2\equiv i(\mathrm{mod}\ 2n)\Leftrightarrow i(q^2-1)\equiv 0(\mathrm{mod}\ 2n)$。因此$s$整除$2i$。注意到$s$是奇数,故$s$整除$i$。设$i=ks$,由$i\in T$可得:$1\leqslant k\leqslant 4r-1$且$k$为奇数。由此得出结论。

下面讨论F_{q^2}上长为$n=(q^4-1)/8$的厄米特对偶包含负循环码存在的充要条件,给出它们最大的设计距离。

定理1 设C为F_{q^2}上长为$n=(q^4-1)/8$的负循环码。记$\delta_M=(q-1)s/4$。若C的定义集为$T=\bigcup_{i=1}^{\delta}C_{2i-1}$,则$C^{\perp h}\subseteq C$当且仅当$1\leqslant\delta\leqslant\delta_M$。

证明 先证充分性。采用反证法,假设$C^{\perp h}\not\subseteq C$,由引理1知$T\cap T^{-q}\neq\varnothing$。因此,存在2个整数$h$、$k$,$1\leqslant h,k<\delta_M$,使得:

$$2k-1\equiv-(2h-1)q^{2j+1}(\mathrm{mod}\ 2n)\quad(1)$$

其中,$j=0,1$。当$j=0$时,(1)式等价于$(2k-1)+(2h-1)q\equiv 0(\mathrm{mod}\ 2n)$。

注意到:

$$q+1\leqslant(2k-1)+(2h-1)q\leqslant\left[\frac{(q-1)s}{2}-1\right]\times(q+1)=\frac{q^4-1}{4}-(q+1)<2n,$$

由此得出矛盾。

当 $j=1$ 时，(1)式即为：

$$2k-1\equiv-(2h-1)q^3(\mathrm{mod}\ 2n)。$$

因为 $q^4\equiv1(\mathrm{mod}\ 2n)$，所以该式等价于 $(2k-1)q\equiv-(2h-1)(\mathrm{mod}\ 2n)$，类似于情况 $j=0$，可以得出矛盾。因此 $C^{\perp h}\subseteq C$。

再证必要性。假设 $\delta>\delta_M$，因为 $-q(2\delta_M+1)\equiv(q^3-q^2-3q-1)/4(\mathrm{mod}2n)$，所以 $(q^3-q^2-3q-1)/4\in-qC_{2\delta_M-1}$。但是 $\delta_M>(q^3-q^2-3q+3)/8$，因此有 $T\cap T^{-q}\neq\varnothing$。由引理 1 知，$C^{\perp h}\not\subseteq C$。因此 $1\leqslant\delta\leqslant\delta_M$。

下面计算定理 1 中厄米特对偶包含负循环 BCH 码的维数。为此，需要计算定义集 $T=\bigcup_{i=1}^{\delta}C_{2i-1}$ 中满足条件的互异的分圆陪集个数，该数可通过计算满足条件 $1\leqslant i<j\leqslant\delta\leqslant\delta_M$ 的分圆陪集 C_{2i-1} 的数目得到，其中 $C_{2i-1}=\{2i-1,2j-1\}$。用 $T(\delta)$ 表示定义集 T 中满足条件 $1\leqslant i<j\leqslant\delta\leqslant\delta_M$ 的元素个数。对任意 $i\in\{1,3,\cdots,2\delta_M+1\}$，由带余除法知，存在整数 u、v，使得 $i=2ur+v$，其中 $0\leqslant u\leqslant q-1$，$0\leqslant v\leqslant2r-1$。因为 i 是奇数，所以 v 也是奇数。因此 $i=2kr+\alpha$，其中：$k\in\{0,1,\cdots,q-1\}$；$\alpha\in\{1,3,\cdots,2r-1\}$。

引理 5　设 $s=(q^2+1)/2$，$r=(q^2-1)/8$。对任意 $i\in\{1,3,\cdots,2n-1\}$，C_i 可以表示为 $\{ks-2r\alpha,\ ks+2r\alpha\}$，其中，$k$、$\alpha$ 满足下列情况之一：

(1) $k\in\{1,3,\cdots,2r-1\}$，$\alpha\in\{0,1,\cdots,2k\}$。

(2) $k\in\{2r+1,\ 2r+3,\cdots,4r-1\}$，$\alpha\in\{0,1,\cdots,2r-1\}$。

证明　对任意 $i\in\{1,3,\cdots,2n-1\}$，由带余除法知，存在整数 u、v，使得 $i=2ur+v$，其中：$u\in\{0,1,\cdots,q^2\}$；$v\in\{1,3,\cdots,2r-1\}$。于是有：

$$iq^2\equiv2urq^2+vq^2\equiv-2ur+vq^2(\mathrm{mod}\ 2n)。$$

下面分 2 种情况讨论：

(1) 当 $0\leqslant u\leqslant4v$ 时，有

$$0<v\leqslant-2ur+vq^2\leqslant vq^2<2n。$$

注意到：

$$i=2ur+v=vs+(u-2v)2r,$$
$$-2ur+vq^2=vs-(u-2v)2r,$$

令 $k=v$，$\alpha=u-2v$，则

$$C_i=\{ks-2r\alpha,ks+2r\alpha\},$$

其中：$k\in\{1,3,\cdots,2r-1\}$；$\alpha\in\{0,1,\cdots,2k\}$。

(2) 当 $4v+1\leqslant u\leqslant q^2$ 时，有

$$-2n<-2ur+vq^2\leqslant-2r(4v+1)+vq^2=v-2r<0。$$

注意到 $i=(v+2r)s+(u-2v-4r-1)2r$，$-2ur+vq^2=(v+2r)s-(u-2v-4r-1)2r$，令 $k=v+2r$，$\alpha=u-2v-4r-1$，则

$$C_i=\{ks-2r\alpha,ks+2r\alpha\},$$

其中：$k\in\{2r+1,\cdots,4r-1\}$；$\alpha\in\{2k-8r,\cdots,8r-2k\}$。

由 C_i 中元素的对称性可得 $\alpha\in\{0,1,\cdots,8r-2k\}$。

引理 6　对任意 $i\in\{1,3,\cdots,2n-1\}$，设 $C_i=\{ks-2\alpha r,ks+2\alpha r\}$。记 $\lambda=\lfloor(2\delta-1+q^2)/2q^2\rfloor$，则 $0<ks-2\alpha r$，$ks+2\alpha r\leqslant2\delta-1$ 当且仅当 k、α 满足下列条件之一：

(1) k 为奇数且 $1\leqslant k\leqslant2\lambda-1$，$0\leqslant\alpha\leqslant2k$。

(2) k 为奇数且 $2\lambda+1\leqslant k\leqslant4\lambda-3$，$0\leqslant\alpha\leqslant\lfloor(2\delta-1-ks)/2r\rfloor$。

证明　(1) 当 k 为奇数且 $1\leqslant k\leqslant2\lambda-1$，$0\leqslant\alpha\leqslant2k$ 时，$k\leqslant\lfloor(2\delta-1)/q^2\rfloor$，故 $0<ks-2\alpha r\leqslant ks\leqslant ks+2\alpha r\leqslant kq^2\leqslant2\delta-1$。

(2) 当 k 为奇数且 $2\lambda+1\leqslant k\leqslant4\lambda-3$，$0\leqslant\alpha\leqslant\lfloor(2\delta-1-ks)/2r\rfloor$ 时，$4\lambda-3<(4\delta-2)/(q^2-1)<(4\delta-2)/(q^2+1)\leqslant(4\delta-2)/q^2+1\leqslant4\lambda-1$。

因此 $4\lambda-3\leqslant\lfloor(2\delta-1)/s\rfloor\leqslant4\lambda-1$。又因为 $k\geqslant2\lambda+1=2\lfloor(2\delta-1)/2q^2+1/2\rfloor+1\geqslant\lfloor(2\delta-1)/q^2\rfloor+1$，所以有 $0<(q^2+1)(\lfloor(2\delta-1)/q^2\rfloor+1)-(2\delta-1)\leqslant2ks-(2\delta-1)<ks-2\alpha r\leqslant ks\leqslant ks+2\alpha r\leqslant ks+2\lfloor(2\delta-1-ks)/2r\rfloor r\leqslant2\delta-1$。

而当 $\alpha>\lfloor(2\delta-1-ks)/2r\rfloor$ 时，$ks+2\alpha r>2\delta-1$，不满足条件。当 $k>4\lambda-3$ 时，$k>\lfloor(2\delta-1)/s\rfloor$，$ks>2\delta-1$，同样也不满足条件。

通过引理 6，可以计算定义集 T 中满足条件 $1\leqslant i<j\leqslant\delta\leqslant\delta_M$ 的元素数目 $T(\delta)$ 的值。

引理 7　设 $s=\dfrac{q^2+1}{2}$，$r=\dfrac{q^2-1}{8}$，$T=\bigcup_{i=1}^{\delta}C_{2i-1}$，其中 $1\leqslant\delta\leqslant\delta_M$，则当 $\lambda=0$ 时，$T(\delta)=0$；当 $\lambda\geqslant1$ 时，

$$T(\delta)=-8\lambda^2+18\lambda-5+(\lambda-1)\times(\lfloor(\delta-2\lambda+1)/r\rfloor+\lfloor(\delta-\lambda-1)/r\rfloor)\quad(2)$$

证明　当 $\lambda\geqslant1$ 时，在引理 6 的情况(1)中，组成 T 的分圆陪集中单元素集有 λ 个，故满足情况(1)条件的元素数目为 $3+(4\lambda-1)/2\cdot\lambda\cdot2-$

$\lambda=4\lambda^2+\lambda$。

情况(2)中组成 T 的分圆陪集中单元素集有 $(\lambda-1)$ 个。注意到：

$\lfloor(2\delta-1-ks)/2r\rfloor=\lfloor(2\delta-1-k)/2r-2k\rfloor$，

满足情况(2)的元素数目为：

$$(1-\lambda)+\left(\left\lfloor\frac{\delta-\lambda-1}{r}-4\lambda-2\right\rfloor+1\right)(\lambda-1)+\left(\left\lfloor\frac{\delta-2\lambda+1}{r}-8\lambda+6\right\rfloor+1\right)(\lambda-1)=(\lambda-1)\left(\frac{\delta-\lambda-1}{r}\left\lfloor\frac{\delta-2\lambda+1}{r}\right\rfloor\right)+(\lambda-1)(5-12\lambda)。$$

两者相加即得等式(2)。当 $\lambda=0$ 时，不存在满足引理6的分圆陪集的单元素集，此时 $T(\delta)=0$。综上，得到结论。

现在可以确定定理1中负循环BCH码的维数，进而利用厄米特构造法得到量子码。

定理2 设 C 为 F_{q^2} 上长为 $n=(q^4-1)/8$ 的负循环码，定义集为 $T=\bigcup_{i=1}^{\delta}C_{2i-1}$，其中 $1\leqslant\delta\leqslant\delta_M$，则 C 是参数为 $[n,n-2\delta+T(\delta),\geqslant\delta+1]$ 的厄米特对偶包含码。因此存在参数为 $[[n,n-4\delta+2T(\delta),\geqslant\delta+1]]$ 的 q 元量子码，其中 $T(\delta)$ 由(2)式给出。

证明 由定理1知，C 是厄米特对偶包含码。由引理7知，$\dim(C)=n-(2\delta-T(\delta))=n-2\delta+T(\delta)$。再由引理2知，$d(C)\geqslant\delta+1$。因此，$C$ 是参数为 $[n,n-2\delta+T(\delta),\geqslant\delta+1]$ 的厄米特对偶包含码。根据引理3，由 C 可以得到参数为 $[[n,n-4\delta+2T(\delta),\geqslant\delta+1]]$ 的 q 元量子码。

例1 当 $q=5$ 时，根据定理2，可以得到参数如下的五元量子码：

$[[78,78-4\delta,\geqslant\delta+1]]$，$1\leqslant\delta\leqslant6$；

$[[78,78-4\delta+2,\geqslant\delta+1]]$，$7\leqslant\delta\leqslant8$；

$[[78,78-4\delta+6,\geqslant\delta+1]]$，$10\leqslant\delta\leqslant11$。

当 $7\leqslant\delta\leqslant12$ 时，文献[13]中量子码的参数为 $[[78,78-4\delta,\geqslant\delta+1]]$。显然，定理2得到的量子码均优于码表中所给的量子码；同时也得到一个新的五元量子码 $[[78,36,\geqslant14]]$。

3 结 论

本文研究了 F_{q^2} 上的长为 $n=(q^4-1)/8$ 的负循环码，其中 $q\equiv1(\mathrm{mod}\ 4)$，通过研究分圆陪集的性质，得到设计距离 δ 的负循环码为厄米特对偶包含码的一个充要条件；进一步确定了厄米特对偶包含负循环码的确切维数，并由此构造了参数良好的量子码。一个值得探讨的问题是利用其他类型的常循环码构造参数优良的量子码。

[参 考 文 献]

[1] SHOR P W. Scheme for reducing decoherence in quantum computer memory[J]. Physical Review A, 1995, 52(4): 2493-2496.

[2] STEANE A M. Error correcting codes in quantum theory [J]. Physical Review Letters, 1996, 77(5): 793-797.

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

[4] ASHIKHMIN A, KNILL A E. Nonbinary quantum stabilizer codes[J]. IEEE Transactions on Information Theory, 2001, 47: 3065-3072.

[5] ALY S A, KLAPPENECKER A, SARVEPALLI P K. On quantum and classical BCH codes[J]. IEEE Transactions on Information Theory, 2007, 53(3): 1183-1188.

[6] MA Z, LU X, FENG K Q, et al. On non-binary quantum BCH codes[C]//Proceedings of The Third International Conference on Theory and Applications of Models of Computation. Berlin: Springer, 2006: 675-683.

[7] LA GUARDIA G G. Constructions of new families of nonbinary quantum codes [J]. Physical Review A, 2009, 80(4): 042331.

[8] LIN X Y. Quantum cyclic and constacyclic codes[J]. IEEE Transactions on Information Theory, 2004, 50(3): 547-549.

[9] KAI X S, ZHU S X, TANG Y S. Quantum negacyclic codes [J]. Physical Review A, 2013, 88(1): 012326.

[10] ZHU S X, SUN Z H, LI P. A class of negacyclic BCH codes and its application to quantum codes[J]. Designs Codes and Cryptography, 2018, 86(10): 2139-2165.

[11] LI R H, WANG J L, LIU Y. et al. New quantum constacyclic codes [J]. Quantum Information Processing, 2019, 18: 127.

[12] KRISHNA A, SARWATE D V. Pseudocyclic maximum-distance-separable codes[J]. IEEE Transactions on Information Theory, 1990, 36(4): 880-884.

[13] EDEL Y. Some good quantum twisted codes[EB/OL]. (2020-10-09) [2021-10-28]. https://www.mathi.uni-heidelberg.de/~yves/Matritzen/QTBCH/QTBCHIndex.html.

(责任编辑 朱晓临)