两类厄米特对偶包含的BCH码及其应用

李 锦[1],高 楠[1],黄 山[2]
(1. 合肥工业大学数学学院,安徽合肥 230601; 2. 安徽警官职业学院,安徽合肥 230031)

摘 要: Bose-Chaudhuri-Hocquenghem(BCH)码是一类重要的经典纠错码,可以纠正多个错误且具有高效的编码和译码方法,满足一定结构关系的BCH码可以构造量子纠错码.本文研究了有限域上两类BCH码,基于分圆陪集的结构性质,给出了这两类BCH码满足厄米特对偶包含的条件,通过确定每个分圆陪集所含元素个数,计算出了这两类厄米特对偶包含的BCH码的维数,并利用厄米特构造法,由这两类厄米特对偶包含的BCH码得到了一些参数较好的量子纠错码.

关键词: 有限域; 循环码; BCH码; 量子纠错码; 厄米特对偶包含码; 分圆陪集
中图分类号: O157.4 **文献标识码:** A **文章编号:** 0372-2112(2022)11-2773-05
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210951

Two Classes of Hermitian Dual-Containing BCH Codes and Their Applications

LI Jin[1], GAO Nan[1], HUANG Shan[2]
(1. *School of Mathematics, Hefei University of Technology, Hefei, Anhui* 230601, *China*;
2. *Anhui Vocational College of Police Officers, Hefei, Anhui* 230031, *China*)

Abstract: Bose-Chaudhuri-Hocquenghem(BCH) codes are an important class of classical error-correcting codes, which can correct multiple errors and have efficient coding and decoding methods. BCH codes with certain conditions can be used to construct quantum error-correcting codes. In this paper, we study two classes of BCH codes over finite fields. Based on the structural properties of cyclotomic cosets, we give the conditions for these two classes of BCH codes to be Hermitian dual-containing codes. Then we determine the number of elements contained in each cyclotomic coset, and calculate the dimensions of these two classes of Hermitian dual-containing BCH codes. Furthermore, some quantum error-correcting codes with good parameters are obtained from two classes of Hermitian dual-containing BCH codes by Hermitian construction.

Key words: finite fields; cyclic codes; BCH codes; quantum error-correcting codes; Hermitian dual-containing codes; cyclotomic cosets

1 引言

经典纠错码是传统通信的重要保障,同样地,量子纠错码是实现量子通信必要条件之一. 1997年,Calderbank, Rains, Shor, Sloane[1] 给出了量子纠错码理论的数学形式,建立了量子纠错码和经典纠错码之间的联系. 2001年,Ashikhmin等人[2]给出了由有限域$F_{p^{2m}}$上厄米特自正交码构造p^m元量子纠错码的一般方法,即厄米特构造法. 2007年,Aly等人[3,4]由满足厄米特对偶包含条件的本原和非本原狭义的BCH码构造了量子纠错码. 2009年,Guardia等人[5]利用非狭义的BCH码构造了量子纠错码,其参数相较于狭义的BCH码构造的量子纠错码更好.

2018年,Zhang等人[6]研究了码长为$r\frac{q^{2m}-1}{q^2-1}$的BCH码,由此构造了一类参数较好的量子纠错码,其中$r\mid(q^2-1)$. Kai等人[7]研究了码长为$\frac{q^{2m}-1}{2}$的负循环BCH码并由此构造了一些新的量子纠错码. 2019年,Wang等人[8]用码长为$2(q^4-1)$的BCH码构造了量子纠

收稿日期:2021-07-20;修回日期:2021-11-12;责任编辑:覃怀银
基金项目:国家自然科学基金(No.62002093);中央高校基本科研业务费专项资金(No.PA2019GDZC0097)

错码. 2020年,Li等人[9]利用码长为$\frac{q^{2m}-1}{\alpha}$的BCH码构造量子纠错码,其中$\alpha\geq 2$. 最近,Zhang等人[10]研究长为$r(q^2-1)$的BCH码并由此构造了的量子纠错码,其中$\mathrm{ord}_n(q^2)=4$. 此外,还有许多学者利用各种码长的BCH码构造了很多参数优良的量子纠错码[11~16].

本文研究了有限域F_{q^2}上码长为$n=\lambda(q+1)(q^2+1)$($\lambda\,|\,(q-1)$或$\lambda\,|\,(q^4+1)$)和$n=\lambda(q-1)(q^2+1)$($\lambda\,|\,(q+1)$或$\lambda\,|\,(q^4+1)$)的两类BCH码,其中q是奇素数幂;给出了这两类BCH码是厄米特对偶包含码的条件,并由这两类厄米特对偶包含的BCH码构造了一些量子纠错码;与文献[4,7,10]中量子纠错码比较,本文构造的量子纠错码的参数更好一些.

2 预备知识

设F_{q^2}是包含q^2个元素的有限域,其中q是素数幂. 对任意正整数n,用$F_{q^2}^n$表示有限域F_{q^2}上n维向量空间. $F_{q^2}^n$的任意一个k维线性子空间C称作码长为n,维数为k的q^2元线性码,C中的向量称为码字. 若对线性码C中任意码字$(c_1,c_2,\cdots,c_n)$都有$(c_n,c_1,\cdots,c_{n-1})\in C$,则称$C$是循环码. 若$C$中任意码字$(c_1,c_2,\cdots,c_n)$等同于它的多项式表示$c_1+c_2x+\cdots+c_nx^{n-1}$,则$C$是长为$n$的$q^2$元循环码等价于$C$是主理想环$R_n=F_{q^2}[x]/(x^n-1)$的理想. 因此,存在$g(x)\in F_{q^2}[x]$满足$g(x)\,|\,(x^n-1)$,使得循环码$C=\langle\, g(x)\,\rangle$,$C$的维数为$k=n-\deg(g(x))$.

设m是q^2模n的乘法阶,记$m=\mathrm{ord}_n(q^2)$,ξ为在$F_{q^{2m}}$上的n次本原单位根,则$x^n-1=\prod_{i=0}^{n-1}(x-\xi^i)$. 记$\Omega=\{0,1,\cdots,n-1\}$,对$\forall i\in\Omega$,$q^2$模$n$含$i$的分圆陪集$C_i=\{i,iq^2,i(q^2)^2,\cdots,i(q^2)^{l-1}\}$,其中$l$是使$i(q^2)^l\equiv i \bmod n$成立的最小正整数.

设$C=\langle\, g(x)\,\rangle$是有限域$F_{q^2}$上长为$n$的循环码,称$Z=\{i\,|\,g(\xi^i)=0\}$是码$C$的定义集. 易知,$Z$是一些$q^2$模$n$的分圆陪集的并. 若循环码$C$的定义集为$Z=\bigcup_{i=b}^{b+\delta-2}C_i$,则称$C$是设计距离为$\delta$的BCH码. 特别地,当$b=1$时为狭义的BCH码,否则,为非狭义的BCH码.

引理1[17] (BCH界)设C是有限域F_{q^2}上设计距离为δ的BCH码,则C的最小距离$d\geq\delta$.

有限域F_{q^2}上长为n的线性码C的厄米特对偶码为$C^{\perp_H}=\{x\in F_{q^2}^n:\langle\, x,y\,\rangle_H=0,\forall y\in C\}$,其中,$\langle\, x,y\,\rangle_H=\sum_{i=1}^{n}x_iy_i^q$. 下面我们给出有限域$F_{q^2}$上循环码是厄米特对偶包含码的一个充要条件.

引理2[4] 设C是在F_{q^2}上的循环码且定义集为Z,$C^{\perp_H}\subseteq C$当且仅当$Z\cap Z^{-q}=\varnothing$,其中$Z^{-q}=\{-qz(\mathrm{mod}\,n)\,|\,z\in Z\}$.

通过下面引理中给出的厄米特构造法,利用厄米特对偶包含码可以构造量子纠错码.

引理3[4] 假设C是一个$[n,k,d]_{q^2}$的线性码且$C^{\perp_H}\subseteq C$,则存在一个$[[n,2k-n,\geq d]]_q$的量子纠错码.

3 两类厄米特对偶包含的BCH码的构造

设q是奇素数幂,$r=\lambda(q^2+1)/2$,下面分码长为$n=\lambda(q+1)(q^2+1)$和$n=\lambda(q-1)(q^2+1)$两种情况进行讨论.

情况1 码长为$n=\lambda(q+1)(q^2+1)$的BCH码

引理4 设$Z=\bigcup_{i=0}^{\delta-2}C_{r+i}$,当$2\leq\delta\leq\frac{q^2+1}{2}+1$时,$Z\cap Z^{-q}=\varnothing$.

证明 假设$Z\cap Z^{-q}\neq\varnothing$,则存在$f$和$h$,使得$(r+h)q^{2l}\equiv -q(r+f)\bmod n$,其中$0\leq f,h\leq\delta-2$,且$0\leq l\leq 3$. 设$f=h=0$,则$rq^{2l}\equiv -qr \bmod n\Rightarrow r(q^{2l-1}+1)\equiv 0 \bmod n\Rightarrow 2(q+1)\,|\,q^{2l-1}+1$,矛盾.

(1) 当$l=0$时,$(r+h)\equiv -q(r+f)\bmod n\Leftrightarrow r(q+1)+qf+h\equiv 0\bmod n\Leftrightarrow\lambda(q+1)(q^2+1)/2+qf+h\equiv 0\bmod\lambda(q+1)(q^2+1)\Rightarrow 2qf+2h\equiv 0\bmod\lambda(q+1)(q^2+1)$.

由于$0<2\leq 2qf+2h\leq 2(q+1)f\leq 2(q+1)\cdot((q^2+1)/2-1)<n$,矛盾.

(2) 当$l=1$时,$(r+h)q^2\equiv -q(r+f)\bmod n\Leftrightarrow r(q+1)+qh+f\equiv 0\bmod n$. 类似$l=0$可推出矛盾.

(3) 当$l=2$时,易知$\lambda q^4\equiv\lambda \bmod n$,$rq^2\equiv r \bmod n$. $(r+h)q^4\equiv -q(r+f)\bmod n\Leftrightarrow r(q^3+1)+q^3h+f\equiv 0\bmod n\Leftrightarrow r(q+1)+q^3h+f\equiv 0\bmod n\Rightarrow 2q^3h+2f\equiv 0\bmod\lambda(q+1)(q^2+1)\Rightarrow 2\lambda q^4h+2\lambda fq\equiv 0\bmod\lambda(q+1)(q^2+1)\Rightarrow 2\lambda h+2\lambda fq\equiv 0\bmod\lambda(q+1)(q^2+1)\Rightarrow 2h+2fq\equiv 0\bmod(q+1)(q^2+1)$.

由于$0<2\leq 2qf+2h\leq 2(q+1)f\leq 2(q+1)\cdot((q^2+1)/2-1)<(q+1)(q^2+1)$,矛盾.

(4) 当$l=3$时,$(r+h)q^6\equiv -q(r+f)\bmod n\Leftrightarrow r(q^5+1)+hq^5+f\equiv 0\bmod n\Leftrightarrow r(q+1)+hq^5+f\equiv 0\bmod n\Rightarrow 2r(q+1)+2hq^5+2f\equiv 0\bmod n\Rightarrow 2hq^5+2f\equiv 0\bmod\lambda(q+1)(q^2+1)\Rightarrow 2\lambda hq^5+2\lambda f\equiv 0\bmod\lambda(q+1)(q^2+1)\Rightarrow 2\lambda hq+2\lambda f\equiv 0\bmod\lambda(q+1)(q^2+1)\Rightarrow 2hq+2f\equiv 0\bmod(q+1)(q^2+1)$.

由于$0<2\leq 2qh+2f\leq 2(q+1)f\leq 2(q+1)\cdot((q^2+1)/2-1)<(q+1)(q^2+1)$,矛盾.

引理5 设$\gcd(\lambda,\frac{q-1}{2})=k$,当$0\leq i\leq\frac{q^2+1}{2}-1$,则有

$$\left|C_{r+i}\right|=\begin{cases}1, & i=0;\\ 2, \dfrac{\lambda}{k}\left|2i\right. 且 i\neq 0;\\ 3, \text{其他}.\end{cases}$$

证明　由于$\mathrm{ord}_n(q^2)=4$,则$\left|C_{r+i}\right|\left|4,q^2\right.$模$n$分圆陪集只能含1个、2个或4个元素.

(1) 设$d_1=\gcd(q^2-1,n)$,即$d_1=2(q+1)k$. C_{r+i}只有一个元素当且仅当$(r+i)q^2\equiv(r+i)\bmod n\Leftrightarrow(r+i)\dfrac{(q^2-1)}{d_1}\equiv 0\bmod\dfrac{n}{d_1}\Leftrightarrow\dfrac{n}{d_1}\left|(r+i)\dfrac{(q^2-1)}{d_1}\right.\Leftrightarrow\dfrac{n}{d_1}\left|(r+i)\right.\Leftrightarrow\dfrac{\lambda(q+1)(q^2+1)}{2(q+1)k}\left|(r+i)\right.\Leftrightarrow\dfrac{\lambda(q^2+1)}{2k}\left|(r+i)\right.\Leftrightarrow\dfrac{\lambda(q^2+1)}{2k}\left|i\right.$.

当$0\le i\le\dfrac{q^2+1}{2}-1$时,$\left|C_{r+i}\right|=1\Leftrightarrow i=0$.

(2) 设$i\neq 0,d_2=\gcd(\dfrac{q^4-1}{2},n)$,即$d_2=(q+1)(q^2+1)k$. C_{r+i}有两个元素当且仅当$(r+i)q^4\equiv(r+i)\bmod n\Leftrightarrow(r+i)\dfrac{(q^4-1)}{d_2}\equiv 0\bmod\dfrac{n}{d_2}\Leftrightarrow\dfrac{n}{d_2}\left|(r+i)\dfrac{(q^4-1)}{d_2}\right.\Leftrightarrow\dfrac{n}{d_2}\left|2(r+i)\right.\dfrac{(q^4-1)}{2d_2}\Leftrightarrow\dfrac{n}{d_2}\left|2(r+i)\right.\Leftrightarrow\dfrac{\lambda(q+1)(q^2+1)}{(q+1)(q^2+1)k}\left|2(r+i)\right.\Leftrightarrow\dfrac{\lambda}{k}\left|2(r+i)\right.\Leftrightarrow\dfrac{\lambda}{k}\left|2i\right.$.

当$0<i\le\dfrac{q^2+1}{2}-1$时,$\left|C_{r+i}\right|=2\Leftrightarrow\dfrac{\lambda}{k}\left|2i\right.$且$i\neq 0$.

引理6　当$2\le\delta\le\dfrac{q^2+1}{2}+1$时,分圆陪集$C_r,C_{r+1},\cdots,C_{r+\delta-2}$互不相交.

证明　由引理5,$C_r=\{r\}$与其他分圆陪集不相交. 不妨设$f>h$,其中$1\le f,h\le\delta-2$. 下证C_{r+f}和C_{r+h}不相交.

(1) 如果$r+f\equiv r+h\bmod n$,则$n\left|f-h\right.$. 由于$0<f-h\le\delta-2-1\le(q^2+1)/2-1-1<n$,矛盾.

(2) 如果$r+f\equiv(r+h)q^2\bmod n$,则$r+f\equiv(r+h)q^2\bmod n\Leftrightarrow r(q^2-1)+q^2h-f\equiv 0\bmod\lambda(q+1)(q^2+1)\Leftrightarrow q^2h-f\equiv 0\bmod\lambda(q+1)(q^2+1)\Leftrightarrow h(q^2+1)-h-f\equiv 0\bmod\lambda(q+1)(q^2+1)\Rightarrow h+f\equiv 0\bmod(q^2+1)$.

由于$0<2\le h+f<2f\le 2((q^2+1)/2-1)<q^2+1$,矛盾.

(3) 如果$r+f\equiv(r+h)q^4\bmod n$,则$r+f\equiv(r+h)q^4\bmod n\Leftrightarrow q^4h-f\equiv 0\bmod\lambda(q+1)(q^2+1)\Leftrightarrow h(q^4-1)+h-f\equiv 0\bmod\lambda(q+1)(q^2+1)\Rightarrow f-h\equiv 0\bmod(q+1)(q^2+1)$.

由于$0<f-h<\delta-2-1\le(q^2+1)/2-1-1<(q+1)(q^2+1)$,矛盾.

(4) 如果$r+f\equiv(r+h)q^6\bmod n$,则$r+f\equiv(r+h)q^6\bmod n\Leftrightarrow q^6h-f\equiv 0\bmod\lambda(q+1)(q^2+1)\Rightarrow\lambda hq^2-\lambda f\equiv 0\bmod\lambda(q+1)(q^2+1)\Rightarrow hq^2-f\equiv 0\bmod(q+1)(q^2+1)\Rightarrow f+h\equiv 0\bmod(q^2+1)$.

由于$0<2\le h+f<2f\le 2((q^2+1)/2-1)<q^2+1$,矛盾.

定理1　当$2\le\delta\le\dfrac{q^2+1}{2}+1$时,可得以下三类量子纠错码:

(1) 如果$\lambda=4$,$\gcd(\lambda,\dfrac{q-1}{2})=1$,则存在参数为$[[\mathrm{n},\mathrm{n}-8\delta+4\lfloor(\delta-2)/2\rfloor+14,\ge\delta]]_q$的量子纠错码.

(2) 如果$\lambda\,|\,(q^4+1)$,则存在参数为$[[n,n-8\delta+14,\ge\delta]]_q$的量子纠错码.

(3) 如果$\lambda\,|\,(q-1)$,则存在参数为$[[n,n-4\delta+6,\ge\delta]]_q$的量子纠错码.

证明　设有限域F_{q^2}上长为n的循环码C的定义集为$Z=\bigcup_{i=0}^{\delta-2}C_{r+i}$. 当$2\le\delta\le(q^2+1)/2+1$时,即$0\le i\le(q^2+1)/2-1$.

(1) 如果$\lambda=4$,$\gcd(\lambda,\dfrac{q-1}{2})=1$,由引理5,可得$|Z|=1+2\lfloor(\delta-2)/2\rfloor+4(\delta-1-1-\lfloor(\delta-2)/2\rfloor)=4\delta-2\lfloor(\delta-2)/2\rfloor-7$.

因此,码C是参数为$[n,n-4\delta+2\lfloor(\delta-2)/2\rfloor+7,\ge\delta]_{q^2}$的BCH码. 由引理3,存在参数为$[[n,n-8\delta+4\lfloor(\delta-2)/2\rfloor+14,\ge\delta]]_q$的量子纠错码.

(2) 如果$\lambda\,|\,q^4+1$,由引理5,$|Z|=1+4(\delta-2)=4\delta-7$. 因此,码$C$是参数为$[n,n-4\delta+7,\ge\delta]_{q^2}$的BCH码,由引理3,存在参数为$[[n,n-8\delta+14,\ge\delta]]_q$的量子纠错码.

(3) 如果$\lambda\,|\,q-1$,由引理5,$|Z|=1+2(\delta-2)=2\delta-3$. 因此,码$C$是参数为$[n,n-2\delta+3,\ge\delta]_{q^2}$的BCH码,由引理3,存在参数为$[[n,n-4\delta+6,\ge\delta]]_q$的量子纠错码.

情况2　码长为$n=\lambda(q-1)(q^2+1)$的BCH码

设$T=\{(\lambda,q):\lambda\,|\,(q+1)$或$\lambda\,|\,(q^4+1),q\ge 5\}$,$T_1=\{(\lambda,q):\lambda=4,q\equiv 1\bmod 4\}$. 类似码长为$n=\lambda(q+1)(q^2+1)$的情况,可证明如下结论:

引理7　设$Z=\bigcup_{i=0}^{\delta-2}C_{r+i}$,当$(\lambda,q)\in T_1,2\le\delta\le\dfrac{q^2+1}{2}+1$,或$(\lambda,q)\in T\backslash T_1,2\le\delta\le q+1$时,$Z\cap Z^{-q}=\varnothing$.

引理8　设$\gcd(\lambda,\dfrac{q+1}{2})=k$,当$0\le i\le\dfrac{q^2+1}{2}-1$时,则

$$\left|C_{r+i}\right|=\begin{cases}1, & i=0;\\ 2, & \dfrac{\lambda}{k}\Big|2i\text{且}i\neq 0;\\ 3, & \text{其他}.\end{cases}$$

引理9 当$(\lambda,q)\in T_1, 2\le i\le \dfrac{q^2+1}{2}+1$,或$(\lambda,q)\in T\backslash T_1$, $2\le\delta\le q+1$时,分圆陪集$C_r, C_{r+1},\cdots, C_{r+\delta-2}$互不相交.

定理2 当λ,q,δ满足如下条件时,可得以下三类量子纠错码:

(1) 当$(\lambda,q)\in T_1, 2\le\delta\le(q^2+1)/2+1$时,存在参数为$[[n,n-8\delta+4\lfloor(\delta-2)/2\rfloor+14,\ge\delta]]_q$的量子纠错码.

(2) 当$\lambda\,|\,(q^4+1), 2\le\delta\le q+1$时,存在参数为$[[n,n-8\delta+14,\ge\delta]]_q$的量子纠错码.

(3) 当$\lambda\,|\,(q+1), 2\le\delta\le q+1$时,存在参数为$[[n,n-4\delta+6,\ge\delta]]_q$的量子纠错码.

4 比较

下面将本文构造的量子纠错码与文献[4,7,10]中的量子纠错码进行比较,如表1、表2所示. 在码长n和设计距离δ相同时,文献[4]构造了维数为$n-8\lceil(\delta-1)(1-1/q^2)\rceil$的量子纠错码,文献[7]构造了维数为$n-4\delta$的量子纠错码,本文构造了维数为$n-8\delta+4\lfloor(\delta-2)/2\rfloor+14$和$n-8\delta+14$的量子纠错码,易知本文的维数更大.

本文构造了参数为$[[n,n-4\delta+6,\ge\delta]]_q$的量子纠错码,其中$2\le\delta\le(q^2+1)/2+1$,文献[10]构造了相同参数的量子纠错码,其中$2\le\delta\le q+1$. 例如,当$q=5, r=13$, $\lambda=2$时,即$n=312$时,本文和文献[10]都构造了参数为$[[312,312-4\delta+6,\ge\delta]]_q$的量子纠错码,而文献[10]中的设计距离$2\le\delta\le 6$,本文中的设计距离$2\le\delta\le 14$. 显然,我们的设计距离的范围更大,可以得到更多的量子纠错码.

表1 本文与文献[4]构造的量子纠错码比较

n	q	λ	本文的量子纠错码	文献[4]的量子纠错码
$\lambda(q+1)(q^2+1)$	3	4	$[[160,150,\ge 3]]_3$	$[[160,144,\ge 3]]_3$
			$[[160,146,\ge 4]]_3$	$[[160,136,\ge 4]]_3$
			$[[160,138,\ge 5]]_3$	$[[160,128,\ge 5]]_3$
			$[[160,134,\ge 6]]_3$	$[[160,120,\ge 6]]_3$
		41	$[[1640,1630,\ge 3]]_3$	$[[1640,1624,\ge 3]]_3$
			$[[1640,1622,\ge 4]]_3$	$[[1640,1616,\ge 4]]_3$
			$[[1640,1614,\ge 5]]_3$	$[[1640,1608,\ge 5]]_3$
			$[[1640,1606,\ge 6]]_3$	$[[1640,1600,\ge 6]]_3$
$\lambda(q-1)(q^2+1)$	5	4	$[[416,406,\ge 3]]_5$	$[[416,400,\ge 3]]_5$
			$[[416,402,\ge 4]]_5$	$[[416,392,\ge 4]]_5$
			$[[416,394,\ge 5]]_5$	$[[416,384,\ge 5]]_5$
			$[[416,390,\ge 6]]_5$	$[[416,376,\ge 6]]_5$
	9	17	$[[11152,11126,\ge 5]]_9$	$[[11152,11120,\ge 5]]_9$
			$[[11152,11118,\ge 6]]_5$	$[[11152,11112,\ge 6]]_9$
			$[[11152,11110,\ge 7]]_9$	$[[11152,11104,\ge 7]]_9$
			$[[11152,11102,\ge 8]]_9$	$[[11152,11096,\ge 8]]_5$
			$[[11152,11094,\ge 9]]_9$	$[[11152,11088,\ge 9]]_9$
			$[[11152,11086,\ge 10]]_9$	$[[11152,11080,\ge 10]]_9$

表2 本文与文献[7]构造的量子纠错码比较

n	q	λ	本文的量子纠错码	文献[7]的量子纠错码
$\lambda(q+1)(q^2+1)$	5	2	$[[312,290,\ge 7]]_5$	$[[312,288,\ge 7]]_5$
			$[[312,286,\ge 8]]_5$	$[[312,284,\ge 8]]_5$
			$\cdots$	$\cdots$
			$[[312,274,\ge 11]]_5$	$[[312,272,\ge 11]]_5$
			$[[312,270,\ge 12]]_5$	$[[312,268,\ge 12]]_5$
$\lambda(q-1)(q^2+1)$	7	4	$[[1200,1170,\ge 9]]_7$	$[[1200,1170,\ge 9]]_7$
			$[[1200,1166,\ge 10]]_7$	$[[1200,1164,\ge 10]]_7$
			$\cdots$	$\cdots$
			$[[1200,1114,\ge 23]]_7$	$[[1200,1112,\ge 23]]_7$
			$[[1200,1110,\ge 24]]_7$	$[[1200,1108,\ge 24]]_7$

5 总结

本文构造了有限域上F_{q^2}两类厄米特对偶包含的BCH码,并利用这两类BCH码构造了一些新的量子纠错码. 在码长和设计距离相同时,本文所构造的量子纠错码比已知量子纠错码具有更大的维数.

参考文献

[1] 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.

[2] ASHIKHMIN A, KNILL E. Nonbinary quantum stabilizer codes[J]. IEEE Transactions on Information Theory, 2001, 47(7): 3065-3072.

[3] ALY S A, KLAPPENECKER A, SARVEPALLI P K. Primitive quantum BCH codes over finite fields[C]//2006 IEEE International Symposium on Information Theory. Seattle: IEEE, 2006: 1114-1118.

[4] 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.
[5] GUARDIA G G L. Constructions of new families of nonbinary quantum codes[J]. Physical Review A, 2009, 80(4): 042331.
[6] ZHANG M, LI Z, XING L J, et al. Construction of some new quantum BCH codes[J]. IEEE Access, 2018, 6: 36122-36131.
[7] KAI X S, LI P, ZHU S X. Construction of quantum negacyclic BCH codes[J]. International Journal of Quantum Information, 2018, 16(7): 1850059.
[8] WANG J L, LI R H, Ma Y N, et al. New quantum BCH codes of length $n=2(q^4-1)$[J]. Procedia Computer Science, 2019, 154: 677-685.
[9] LI F W, SUN X M. The Hermitian dual containing nonprimitive BCH codes[J]. IEEE Communications Letters, 2020, 25(2): 379-382.
[10] ZHANG H, ZHU S X. New quantum BCH codes of length $n=r(q^2-1)$[J]. International Journal of Theoretical Physics, 2021, 60(1): 172-184.
[11] SUN Z H, ZHU S X, WANG L Q. A class of constacyclic BCH codes[J]. Cryptography and Communications, 2019, 12(2): 265-284.
[12] TANG N Q, LI Z, XING L J, et al. Some improved constructions for nonbinary quantum BCH codes[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2019, E102A(1): 303-306.
[13] GUO G M, LI R H, LIU Y, et al. A family of negacyclic BCH codes of length $n=(q^{2m}-1)/2$[J]. Cryptography and Communications, 2020, 12(2): 187-203.
[14] ZHAO X B, LI X P, WANG Q, et al. Hermitian dual-containing constacyclic BCH codes and related quantum codes of length $n=(q^{2m}-1)/(q+1)$[EB/OL]. [2020-07-27]. http://arxiv.org/abs/20 07.13309.
[15] WANG J, LI R H, LIU Y, et al. Some negacyclic BCH codes and quantum codes[J]. Quantum Information Processing, 2020, 19(2): 74.
[16] SONG H, LI R H, WANG J L, et al. Two families of BCH codes and new quantum codes[J]. Quantum Information Processing, 2018, 17(10): 270.
[17] MACWILLIAMS F J, SLOANE N J A. The Theory of Error -Correcting Codes[M]. The Netherlands: North-Holland Publishing Company, 1977.

作者简介

李　锦　女,1987年1月出生于陕西省彬州市,现为合肥工业大学数学学院副教授,研究方向为代数编码.
E-mail: lijin_0102@126.com

高　楠　女,1997年8月出生于安徽省蚌埠市,现为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: gaonan_2775@163.com

黄　山　女,1993年5月出生于安徽省桐城市,现为安徽警官职业学院教师,研究方向为代数编码.
E-mail: huangshan5197@163.com