基于分圆陪集的量子 BCH 码的构造

邢莉娟，李卓
（西安电子科技大学综合业务网国家重点实验室，陕西 西安 710071）

摘 要：量子纠错码是克服量子消相干的主要手段，是实现量子计算机的关键技术。量子 BCH 码可以利用满足特定关系的经典码构造。首先推导了选择分圆陪集的一般性方法，给出了计算每一个分圆陪集包含元素个数的充要条件。然后给出了有限域 F_q 上利用 CSS 构造和 Steane 构造来构造量子 BCH 码的方法。最后将该方法扩展到有限域 F_q^2 上，给出了利用 Hermitian 构造来构造量子 BCH 码的方法。与已有的结果相比，所提方法具有更好的码参数和更高的最小距离下界，可以得到大量新的量子 BCH 码。此外，所提方法还可以得到一类任意域上的量子最大距离可分码。

关键词：量子 BCH 码；分圆陪集；Steane 构造；Hermitian 构造
中图分类号：TN929.12
文献标识码：A
DOI: 10.11959/j.issn.1000−436x.2021194

Construction of quantum BCH code based on cyclotomic coset

XING Lijuan, LI Zhuo
State Key Laboratory of Integrated Service Networks, Xidian University, Xi’an 710071, China

Abstract: Quantum-error-correcting code can overcome quantum decoherence efficiently, which is the key technology to realize quantum computers. A series of quantum BCH code was proposed based on classical codes. First, a general way of well-chosen cyclotomic coset was introduced. A sufficient condition was given to calculate the number of elements in cyclotomic coset. Then, a series of quantum BCH (Bose-Chaudhuri-Hocquenghem) code over finite field F_q was constructed by CSS (Calderbank-Shor-Steane) construction and Steane construction. The results were extended to finite field F_q^2 with Hermitian construction. Compared with the results in literature, the range of introduced cyclotomic coset is more wide, and the new quantum BCH code has higher dimensions and better lower bounds on minimum distances. Furthermore, a family of quantum maximum distance separable (quantum MDS) code over any finite fields is constructed.

Keywords: quantum BCH code, cyclotomic coset, Steane construction, Hermitian construction

1 引言

在实际环境中，量子计算机的量子态不是孤立的，它会与外部环境发生相互作用，破坏量子态间的相干性，从而导致量子消相干现象。环境中的噪声将纯纠缠态变成混合态，导致传输的量子信息出错。因此，若要量子计算机或长距离量子通信成为现实，必须克服消相干现象带来的影响。量子纠错码（QECC, quantum error correcting code）是解决量子消相干的主要方式之一。

量子纠错码可以由某些满足特定性质的经典线性码来构造。经典 BCH（Bose-Chaudhuri- Hocquenghem）码由于具有良好的代数结构，是经典编码理论中的一个重要子类。因此，用经典 BCH 码

收稿日期：2021−06−23；**修回日期**：2021−09−23
通信作者：李卓，lizhuo@xidian.edu.cn
基金项目：国家自然科学基金资助项目（No.61372072）；111 工程基金资助项目（No.B08038）
Foundation Items: The National Natural Science Foundation of China (No.61372072), The 111 Project (No.B08038)

来构造量子 BCH 码也引起了人们极大的关注。通过大量研究，目前已提出了很多构造给定参数量子纠错码的方案[1-5]。但是，现有方案中的量子码均具有一定约束性。例如，分圆陪集的选择必须满足一定前提[1]；有限域的阶必须是奇素数的幂[3]或者满足特定的表达式[5]。因此，需要对已有量子 BCH 码进行进一步扩展和补充[6-8]。

2　基础与定义

令 F_q 表示 q 阶有限域，其中 q 为素数的幂。码字 $C=[n,k,d]_q$ 表示基于 F_q 上的线性码，其中 n 为码长，k 为维数，d 为最小汉明距离。在本文中，若 n 与 q 互素，则令 $q^m\equiv 1 \bmod n$ 成立的最小正整数 m 为 q 模 n 的乘法阶，用 $m=\mathrm{ord}_n(q)$ 表示。

定义 1　有限域 F_q 上存在向量 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in F_q^n$ 和 $\boldsymbol{y}=(y_0,y_1,\cdots,y_{n-1})\in F_q^n$，其 Euclidean 内积可表示为 $\langle \boldsymbol{x},\boldsymbol{y}\rangle_{\mathrm{E}}=x_0y_0+x_1y_1+\cdots+x_{n-1}y_{n-1}$。

定义 2　有限域 F_{q^2} 上存在向量 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in F_{q^2}^n$ 和 $\boldsymbol{y}=(y_0,y_1,\cdots,y_{n-1})\in F_{q^2}^n$，其 Hermitian 内积可表示为 $\langle \boldsymbol{x},\boldsymbol{y}\rangle_{\mathrm{H}}=x_0y_0^q+x_1y_1^q+\cdots+x_{n-1}y_{n-1}^q$。

定义 3　基于有限域 F_q 上的线性码 C，其 Euclidean 对偶码 $C^{\perp \mathrm{E}}$ 可表示为 $C^{\perp \mathrm{E}}=\{\boldsymbol{x}\in F_q^n \mid \langle \boldsymbol{x},\boldsymbol{y}\rangle_{\mathrm{E}}=0 \text{对} \forall \boldsymbol{y}\in C \text{都成立}\}$。如果 $C^{\perp \mathrm{E}}\subseteq C\subsetneq F_q^n$，则线性码 C 是 Euclidean 对偶包含的。

定义 4　基于有限域 F_{q^2} 上的线性码 C，其 Hermitian 对偶码 $C^{\perp \mathrm{E}}$ 可表示为 $C^{\perp \mathrm{H}}=\{\boldsymbol{x}\in F_{q^2}^n \mid \langle \boldsymbol{x},\boldsymbol{y}\rangle_{\mathrm{H}}=0 \text{对} \forall \boldsymbol{y}\in C \text{都成立}\}$。如果 $C^{\perp \mathrm{H}}\subseteq C\subsetneq F_{q^2}^n$，则线性码 C 是 Hermitian 对偶包含的。

定义 5　对于任意整数 i，有限域 F_q 上包含 i 的模 n 分圆陪集定义为 $C[i]=\left\{iq^z \bmod n \mid z\in \mathbb{Z}^+\right\}$。

性质 1[9]　有限域 F_q 中的分圆陪集满足以下性质。

1) 分圆陪集的元素个数一定是 q 模 n 的乘法阶的因子，即 $|C[i]|\,|\,\mathrm{ord}_n(q)$，其中 $|C[1]|=\mathrm{ord}_n(q)$。

2) 对于任意的分圆陪集，当且仅当 $i\neq jq^z \bmod n$ 时，$C[i]\neq C[j]$。

循环码因为其严谨的代数结构和循环特性，被认为是一类重要的线性码。

定义 6　有限域 F_q 上的码长为 n，设计距离为 δ 的 q 元 BCH 码 C 是一个循环码，其生成多项式可表示为 $g(x)=\mathrm{lcm}\{M^{(b)}(x),M^{(b+1)}(x),\cdots,M^{(b+\delta-2)}(x)\}$，其中，$M^{(i)}(x)$ 表示索引为 i 的最小多项式。码 C 的定义集合为

$$Z=\bigcup_{i=b}^{b+\delta-2} C[i]$$

当 $n=q^m-1$ 时，BCH 码是本原的；当 $b=1$ 时，BCH 码是狭义的。

量子稳定子码可以通过经典线性码来构造。目前，量子码主要的构造方法有 CSS（Calderbank-Shor-Steane）构造、Steane 构造和 Hermitian 构造。

定理 1[10-11]　设有限域上的经典线性码 $C_1=[n,k_1,d_1]_q\subseteq F_q^n$、$C_2=[n,k_2,d_2]_q\subseteq F_q^n$ 和 $C=\left[n,k,d\right]_{q^2}\subseteq F_{q^2}^n$。

1) CSS 构造。当 $C_1\subseteq C_2$ 时，存在参数为 $[[n,k_2-k_1,D]]_q$ 的量子稳定子码，其中 $D=\min wt\{(C_2\setminus C_1)\cup(C_1^{\perp \mathrm{E}}\setminus C_2^{\perp \mathrm{E}})\}$。

2) Steane 构造。当 $C_1^{\perp \mathrm{E}}\subseteq C_1=\left[n,k_1,d_1\right]_q$ 时，C_1 可以扩展至 $C_1'=[n,k_1',d_1']_q$，其中 $k_1'-k_1\geqslant 2$，存在参数为 $[[n,k_1+k_1'-n,D\geqslant \min\{d_1,\left\lceil \frac{q+1}{q}d_1'\right\rceil\}]]_q$ 的量子稳定子码。

3) Hermitian 构造。当 $C^{\perp \mathrm{H}}\subseteq C$ 时，存在参数为 $[[n,2k-n,D\geqslant d]]_q$ 的量子稳定子码。

根据上述定理，如果能找到满足对偶包含关系的经典线性码，就可以构造对应参数的量子码。引理 1 给出了循环码满足对偶包含的条件。

引理 1[10]　若 n 与 q 互素，即满足 $\gcd(n,q)=1$，存在以下结论。

1) 对于 F_q 上码长为 n 的循环码 C，如果 C 的定义集合为 Z，那么 $C^{\perp \mathrm{E}}\subseteq C$ 的充要条件是 $Z\cap Z^{-1}=\varnothing$，其中 $Z^{-1}=\{-z \bmod n \mid z\in Z\}$。

2) 对于 F_{q^2} 上码长为 n 的循环码 D，如果 D 的定义集合为 Z，那么 $D^{\perp \mathrm{H}}\subseteq D$ 的充要条件是 $Z\cap Z^{-q}=\varnothing$，其中 $Z^{-q}=\{-qz \bmod n \mid z\in Z\}$。

因此，构造量子稳定子码的关键是寻找满足上述条件的分圆陪集。这些特定的分圆陪集不仅保证经典循环码是对偶包含的，还便于计算该码的维数和最小距离。下面来寻找满足上述条件的分圆陪集。

3 分圆陪集的选择

Guardia 等[1]给出了有限域 F_q 上阶为 2、码长为 $n=r(q-1)$ 的量子 BCH 码的构造方法。在此基础上，本文讨论如何利用 CSS 构造、Steane 构造和 Hermitian 构造等方法研究其镜像结果。Aly 等[12]的构造方法仅针对本原量子 BCH 码，而本文的研究对象是更一般的量子 BCH 码。首先讨论分圆陪集中包含一个元素的充要条件。

引理 2 设 $m=\mathrm{ord}_n(q)=2$，$n=r(q+1)$。

1) 若 $\frac{q-1}{r}$ 为奇数，当且仅当 $i\in\{l(q+1)\,|\,0\leqslant l\leqslant r-1\}$ 时，q 元分圆陪集 $C[i]$ 包含有一个元素。

2) 若 $\frac{q-1}{r}$ 为偶数，当且仅当 $i\in\{l\frac{(q+1)}{2}\,|\,0\leqslant l\leqslant 2r-1\}$ 时，q 元分圆陪集 $C[i]$ 包含有一个元素。

证明 已知 $m=\mathrm{ord}_n(q)=2$，可得 $q^2\equiv 1 \bmod n$。由分圆陪集的性质可知，q 元分圆陪集 $C[i]$ 只包含一个或两个元素。由 $n\,|\,q^2-1$ 可知 $r\,|\,q-1$。

1) 若 $\frac{q-1}{r}$ 为奇数，当 $i\in\{l(q+1)\,|\,0\leqslant l\leqslant r-1\}$ 时，推出 $l(q+1)q=l(q^2+q)\equiv l(q+1)\bmod n$，可知 $C[i]$ 中仅包含一个元素。相反，如果 $C[i]$ 只包含一个元素，可推出 $iq\equiv i \bmod n,\ 0\leqslant i\leqslant n-1$。由同余定理可知，$n\,|\,i(q-1)$ 和 $(q+1)\,|\,i\frac{(q-1)}{r}$ 均成立。下面分 2 种情况讨论。

① 若 $q=2^e$，e 表示任意正整数，则 $\gcd(q-1,q+1)=1$ 和 $\gcd(\frac{q-1}{r},q+1)=1$ 均成立，由此可推出 $q+1\,|\,i$。

②若 $q=p^e$，e 表示任意正整数，p 表示任意奇素数，则 $\gcd(q-1,q+1)=2$ 成立。当 $\frac{q-1}{r}$ 为奇数时，$\gcd(\frac{q-1}{r},q+1)=1$ 成立，由此可推出 $q+1\,|\,i$。

综上，若 $\frac{q-1}{r}$ 为奇数，当且仅当 $i\in\{l(q+1)\,|\,0\leqslant l\leqslant r-1\}$ 时，$C[i]$ 包含有一个元素。

2) 若 $\frac{q-1}{r}$ 为偶数，那么 $q\neq 2^e$。设 $q=p^e$，e 表示任意正整数，p 表示任意奇素数。如果 $i\in\{l\frac{(q+1)}{2}\,|\,0\leqslant l\leqslant 2r-1\}$，可推出 $l\frac{(q+1)}{2}q=l\frac{(q^2+q)}{r}\equiv l\frac{(q+1)}{2}\bmod n$。因此 $C[i]$ 只包含一个元素。反之，如果 $C[i]$ 只包含一个元素，则 $(q+1)\,|\,i\frac{(q-1)}{r}$ 成立。因为 $\gcd(q+1,q-1)=2$，所以 $\gcd(\frac{q+1}{2},\frac{q-1}{2})=1$。若 r 是偶数，则 $\gcd(\frac{q+1}{2},\frac{q-1}{r})=1$，此时 $\frac{q+1}{2}\,|\,i\frac{(q-1)}{r}$，故 $\frac{q+1}{2}\,|\,i$；若 r 是奇数，则 $\gcd(\frac{q+1}{2},\frac{q-1}{2r})=1$，此时 $\frac{q+1}{2}\,|\,\frac{(q-1)}{2r}i$，所以 $\frac{q+1}{2}\,|\,i$。

综上，若 $\frac{q-1}{r}$ 为偶数，当且仅当 $i\in\{l\frac{(q+1)}{2}\,|\,0\leqslant l\leqslant 2r-1\}$ 时，$C[i]$ 包含有一个元素。证毕。

其次，来讨论这些分圆陪集之间的关系。

引理 3 分圆陪集 $C[0]$, $C[1]$, …, $C[2r-1]$, $C[2r]$ 互不相交。

证明 由 $m=\mathrm{ord}_n(q)=2$ 和 $n=r(q+1)$ 可知，$rq\equiv -r \bmod n$ 和 $r\,|\,q-1$ 成立。若只考虑非本原量子 BCH 码，则 $2r\leqslant q-1$ 和 $n\geqslant 3r$ 成立。所以，分圆陪集 $C[0]$ 和 $C[1]$, …, $C[2r-1]$, $C[2r]$ 均不相交。

接下来，证明其他分圆陪集 $C[1]\sim C[2r]$ 也互不相交。采用反证法，假设 $C[f]=C[r+h]$，其中 $1\leqslant f\leqslant r$，$1\leqslant h\leqslant r$。由 $1\leqslant f\leqslant r<r+h\leqslant 2r<n$ 可知 $f\neq r+h$。如果 $f\equiv(r+h)q \bmod n$，那么 $f\equiv hq-r \bmod n$ 成立。因为 $1\leqslant h\leqslant r$，所以 $r<q-r<hq-r\leqslant rq-r<n$。因为 $1\leqslant f\leqslant r$，可知 $f\equiv hq-r \bmod n$ 与 $1\leqslant f\leqslant r<hq-r<n$ 相矛盾，所以 $C[f]=C[r+h]$ 不成立。综上，分圆陪集 $C[0]$, $C[1]$, …, $C[2r-1]$, $C[2r]$ 均互不相交。证毕。

4 有限域 F_q 上的量子 BCH 码

由引理 2 可知，当 $\frac{q-1}{r}$ 取不同值时，分圆陪集包含一个元素的充要条件不同，其生成的 BCH 码的维数也不同。下面，构造 F_q 上码长为 $n=r(q+1)$ 的量子 BCH 码。

定理 2 若码长 $n=r(q+1)$，其中 $q\geqslant 3$，

$m=\mathrm{ord}_n(q)=2$。当$0\leqslant c\leqslant r-1$，$0\leqslant t\leqslant r$时，有以下结论。

1) 若$\frac{q-1}{r}$为奇数，存在参数为$[[n,n-2(c+t)-3,d\geqslant\min\{t+2,c+2\}]]_q$的量子BCH码。

2) 若$\frac{q-1}{r}$为偶数，①存在参数为$[[n,n-2(c+t)-3,d\geqslant\min\{t+2,c+2\}]]_q$的量子BCH码，其中$1\leqslant r<\frac{q+1-2t}{2}$；②存在参数为$[[n,n-2(c+t)-2,d\geqslant\min\{t+2,c+2\}]]_q$的量子BCH码，其中$\frac{q+1-2t}{2}\leqslant r\leqslant\frac{q-1}{2}$。

证明　首先由引理3可知，分圆陪集$C[0],C[1],\cdots,C[c],C[r],\cdots,C[r+t]$互不相交，其中$0\leqslant c\leqslant r-1$，$0\leqslant t\leqslant r$。

码C_1的生成多项式为$g_1(x)=\prod_i M^{(i)}(x)$，码$C_2$的生成多项式为$g_2(x)=\prod_j M^{(j)}(x)$，其中$i\in\{0,1,\cdots,c\}$，$j\notin\{r,r+1,\cdots,r+t\}$且$j$遍历整个分圆陪集。根据$C_1$和$C_2$的构造过程可知$C_2\subsetneq C_1$。因为由$h_2(x)=(x^n-1)/g_2(x)$生成的$C_2'$的定义集合$Z_2'$中包含$t+1$个连续整数，所以$C_2'$的最小距离满足$d'\geqslant t+2$。码$C_2^{\perp\mathrm{E}}$等价于$C_2'$，即$C_2^{\perp\mathrm{E}}$的最小距离满足$d_2^{\perp\mathrm{E}}\geqslant t+2$。

1) 若$\frac{q-1}{r}$为奇数，$0\leqslant c<r+t\leqslant 2r\leqslant q-1$成立。根据引理2，除了$C[0]=\{0\}$外，其他分圆陪集都包含2个元素。$C_1$的维数为$k_1=n-(2c+1)$，$C_2$的维数为$k_2=2(t+1)$。因为$C_1$的定义集合$Z_1$中包含$c+1$个连续整数，所以$C_1$的最小距离满足$d_1\geqslant c+2$。利用CSS构造方法，可以得到参数为$[[n,n-2(c+t)-3,\ d\geqslant\min\{t+2,c+2\}]]_q$的量子码。

2) 若$\frac{q-1}{r}$为偶数，$2r\leqslant q-1$成立。由引理2可知，$C[0]$包含一个元素，$C[1],\cdots,C[c],C[r]$中均包含2个元素。当$1\leqslant r<\frac{q+1-2t}{2}$时，由$1\leqslant j_0\leqslant t$可知，分圆陪集$C[r+j_0]$包含2个元素。当$\frac{q+1-2t}{2}\leqslant r\leqslant\frac{q-1}{2}$时，由$1\leqslant j_1\leqslant t$推出$r+j_1=\frac{q+1}{2}$，可知分圆陪集$C[r+j_1]$包含一个元素。其余的证明过程请参照步骤1)，利用CSS构造方法，可以得到对应参数的量子码。证毕。

例如，若令$q=13$，$m=2$，根据定理2可以构造不同参数的量子码，结果如表1所示。

表1　q=13, m=2 时 CSS 构造的量子码参数

n	r	c	t	新的量子码
56	4	3	3	$[[56,41,d\geqslant 5]]_{13}$
42	3	2	2	$[[42,31,d\geqslant 4]]_{13}$
84	6	5	5	$[[84,62,d\geqslant 7]]_{13}$

图1对定理2中分圆陪集的选择做了总结：$C[0],C[1],\cdots,C[c]$的并集代表码C_1的定义集合；$C[r],C[r+1],\cdots,C[r+t]$的并集代表码$C_2'$的定义集合；$C[0],C[1],\cdots,C[r-1]$和$C[a_1],\cdots,C[a_n]$的并集代表码$C_2$的定义集合；$C[a_1],\cdots,C[a_n]$用来补全剩余的分圆陪集。

根据定理1，如果能找到满足Euclidean自正交关系的经典线性码，采用Steane构造方法，也可以构造出相应码参数的量子码。引理4给出了满足Steane构造的充分条件。

$$\overbrace{\underbrace{C[0],C[1],\cdots,C[c]}_{C_2},C[c+1],\cdots,C[r-1]}^{C_1},\underbrace{C[r],C[r+1],\cdots,C[r+t]}_{C_2'},\underbrace{C[a_1],\cdots,C[a_n]}_{C_2}$$

图1　分圆陪集的选择

引理4　当$Z=\bigcup_{i=1}^{r-1}C[r+i]$时，$Z\cap Z^{-1}=\varnothing$。

证明　由$n=r(q+1)$和$q\geqslant 3$可知，$n\geqslant 4r$。假设$Z\cap Z^{-1}=\varnothing$，分2种情况讨论。

1)若$(r+f)\equiv-(r+h)\bmod n$成立，其中$1\leqslant f$，$h\leqslant r-1$，则$2r+f+h\equiv 0\bmod n$，与不等关系$2r+2\leqslant 2r+f+h\leqslant 4r-2<n$相矛盾。

2) 若$(r+f)q\equiv-(r+h)\bmod n$成立，其中$1\leqslant f$，$h\leqslant r-1$，因为$rq\equiv -r\bmod n$，则$fq+h\equiv 0\bmod n$，与不等关系$q+1\leqslant fq+h\leqslant(r-1)(q+1)<n$相矛盾。

综上，当$Z=\bigcup_{i=1}^{r-1}C[r+i]$时，$Z\cap Z^{-1}=\varnothing$。证毕。

根据引理4，本文用Steane构造来设计F_q上码长为$n=r(q+1)$的量子BCH码。

定理3　若码长$n=r(q+1)$，$q\geqslant 3$，$m=\mathrm{ord}_n(q)=2$。当$2\leqslant t\leqslant r-1$，$1\leqslant c\leqslant t-1$时，有以下结论。

1) 若 $\frac{q-1}{r}$ 为奇数，存在参数为 $[[n,n-2(c+t),d\geqslant\min\{t+1,\lceil\frac{q+1}{q}(c+1)\rceil\}]]_q$ 的量子 BCH 码。

2) 若 $\frac{q-1}{r}$ 为偶数，①存在参数为 $[[n,n-2(c+t),d\geqslant\min\{t+1,\left\lceil\frac{q+1}{q}(c+1)\right\rceil\}]]_q$ 量子 BCH 码，其中 $2<r<\frac{q+1-2t}{2}$；②存在参数为 $[[n,n-2(c+t)+1,d\geqslant\min\{t+1,\left\lceil\frac{q+1}{q}(c+1)\right\rceil\}]]_q$ 的量子 BCH 码，其中 $\frac{q+1-2t}{2}\leqslant r<\frac{q+1-2c}{2}$；③存在参数为 $[[n,n-2(c+t)+2,d\geqslant\min\{t+1,\left\lceil\frac{q+1}{q}(c+1)\right\rceil\}]]_q$ 的量子 BCH 码，其中 $\frac{q+1-2c}{2}\leqslant r\leqslant\frac{q-1}{2}$。

证明 设 BCH 码 C_1 的生成多项式为 $g_1(x)=\prod_{i=r+1}^{r+t}M^{(i)}(x)$，其中 $2\leqslant t\leqslant r-1$。若码 C_1 的定义集合为 $Z_1=\bigcup_{i=r+1}^{r+t}C[i]$。由引理 3 可知，$Z_1$ 中的分圆陪集均不相交。根据引理 1 和引理 4 可判定 C_1 满足 Euclidean 自正交关系。设 BCH 码 C_1' 的生成多项式为 $g_1'(x)=\prod_{j=r+1}^{r+c}M^{(j)}(x)$，其中 $1\leqslant c\leqslant t-1$。

1) 若 $\frac{q-1}{r}$ 为奇数，由引理 2 可知，$\deg g_1(x)=2t$。因此，$C_1=[n,k_1=n-2t,d_1\geqslant t+1]_q$。同样可知 $C_1'=[n,k_1'=n-2c,d_1'\geqslant c+1]_q$，其中 $k_1'-k_1=2(t-c)\geqslant 2$。由 C_1 和 C_1' 的构造方式可知，码 C_1' 是 C_1 的扩展。使用 Steane 构造方法，可以得到参数为 $[[n,n-2(c+t),\quad d\geqslant\min\{t+1,\left\lceil\frac{q+1}{q}(c+1)\right\rceil\}]]_q$ 的量子 BCH 码。

2) 若 $\frac{q-1}{r}$ 为偶数。由引理 2 可知，当 $2<r<\frac{q+1-2t}{2}$ 时，码 C_1 和 C_1' 的所有分圆陪集中均包含 2 个元素；当 $\frac{q+1-2t}{2}\leqslant r<\frac{q+1-2c}{2}$ 时，C_1 仅有一个分圆陪集包含一个元素，其余分圆陪集包含 2 个元素，而 C_1' 的所有分圆陪集均包含 2 个元素；当 $\frac{q+1-2c}{2}\leqslant r\leqslant\frac{q-1}{2}$ 时，C_1 和 C_1' 均仅有一个分圆陪集包含一个元素，其余分圆陪集包含 2 个元素。其余证明与步骤 1)相同，利用 Steane 构造方法，可以得到对应参数的量子 BCH 码。证毕。

Li 等[13]利用 Hermitian 构造方法，构造出一类基于 F_{q^2} 上码参数为 $[[n,n-4,3]]_q$ 的量子最大距离可分码（QMDSC，quantum maximum distance separable code）。在文献[13]的基础上，如果选择合适的分圆陪集，使用 Steane 构造方法可以得到任意有限域上参数为 $[[n,n-4,3]]_q$ 的量子 MDS 码。

推论 1 若码长 $n=r(q+1)$，$m=\mathrm{ord}_n(q)=2$。当 $q\geqslant 5$，$r>3$ 时，存在参数为 $[[n,n-4,3]]_q$ 的量子 MDS 码。

证明 若 $\frac{q-1}{r}$ 为奇数，令 $C_1=\left\langle M^{(q+1)}(x)M^{(q+2)}(x)\right\rangle$ 和 $C_1'=\left\langle M^{(q+1)}(x)\right\rangle$。选择分圆陪集 $C[q+1]=\{q+1\}$，$C[q+2]=\{q+2,2q+1\}$。与定理 3 的证明类似，$C_1=[n,k_1=n-3,d_1\geqslant 3]_q$ 是 Euclidean 对偶包含的，$C_1'=[n,k_1'=n-1,d_1'\geqslant 2]_q$。由 $k_1'-k_1=2$ 可知，码 C_1' 是 C_1 的扩展。使用 Steane 构造方法，可得到 $[[n,n-4,d\geqslant 3]]_q$ 的量子 MDS 码。

若 $\frac{q-1}{r}$ 为偶数，令 $C_1=\left\langle M^{(\frac{q+1}{2})}(x)M^{(\frac{q+3}{2})}(x)\right\rangle$ 和 $C_1'=\left\langle M^{(\frac{q+1}{2})}(x)\right\rangle$。选择分圆陪集 $C[\frac{q+1}{2}]=\{\frac{q+1}{2}\}$，$C[\frac{q+3}{2}]=\{\frac{q+3}{2},\frac{3q+1}{2}\}$。同样使用 Steane 构造方法，可得到 $[[n,n-4,d\geqslant 3]]_q$ 的量子 MDS 码。证毕。

例如，选取参数 q=13、m=2 和 n=56，可知 $r=4$，$\frac{q-1}{r}=3$。令 $C_1'=\left\langle M^{(14)}(x)\right\rangle$，$C_1=\left\langle M^{(14)}(x)M^{(15)}(x)\right\rangle$。由于 C_1 的定义集合为 $Z_1=C[14]\cup C[15]$，满足 $Z_1\cap Z_1^{-1}=\varnothing$ 的条件，因此 C_1 是 Euclidean 对偶包含的。可知 $C_1=[56,53,d\geqslant 3]_{13}$，$C_1'=[56,55,d\geqslant 2]_{13}$。使用 Steane 构造方法，得到了参数为 $[[56,52,3]]_{13}$ 的量子 MDS 码。

5 有限域 F_{q^2} 上的量子 BCH 码

本节讨论基于 F_{q^2} 上，码长为 $n=r(q^2+1)$、

$m=\mathrm{ord}_n(q^2)=2$ 的量子 BCH 码的构造问题。在 F_{q^2} 中，由 $n\mid q^4-1$ 可知 $r\mid q^2-1$ 成立。

引理 5　若码长 $n=r(q^2+1)$，$m=\mathrm{ord}_n(q^2)=2$。

1) 若 $\frac{q^2-1}{r}$ 为奇数，当且仅当 $i\in\{l(q^2+1)\mid 0\leqslant l\leqslant r-1\}$ 时，$C[i]$ 含有一个元素。

2) 若 $\frac{q^2-1}{r}$ 为偶数，当且仅当 $i\in\{l\frac{(q^2+1)}{2}\mid 0\leqslant l\leqslant r-1\}$ 时，$C[i]$ 含有一个元素。

引理 6　q^2 元分圆陪集 $C[r]$, $C[r+1]$, $\cdots$, $C[r+t]$ 互不相交。

引理 5 和引理 6 的证明过程请参考引理 2 和引理 3。

根据定理 1，如果能找到满足 Hermitian 自正交关系的经典线性码，采用 Hermitian 构造方法，可以构造出基于有限域 F_{q^2} 上的相应码参数的量子码。引理 7 给出了满足 Hermitian 构造的充分条件。

引理 7　当 $Z=\bigcup_{i=0}^{r}C[r+i]$ 时，$Z\cap Z^{-q}=\varnothing$。

证明　采用反证法，假设 $Z\cap Z^{-q}\neq\varnothing$。下面，分 2 种情况讨论。

1) 若 $r+f\equiv -q(r+h)\bmod n$ 成立，其中 $0\leqslant f$，$h\leqslant r$，可推出 $r(q+1)+f+qh\equiv 0\bmod n$。这与 $r(q+1)\leqslant r(q+1)+f+qh\leqslant 2r(q+1)<n$ 相矛盾，因此，$r+f\equiv -q(r+h)\bmod n$ 不成立。

2) 若 $(r+f)q^2\equiv -q(r+h)\bmod n$ 成立，其中 $0\leqslant f$，$h\leqslant r$，由 $\gcd(n,q)=1$ 可知，$(r+f)q\equiv -(r+h)\bmod n$。同样，$(r+f)q^2\equiv -q(r+h)\bmod n$ 也不成立。

综上，当 $Z=\bigcup_{i=0}^{r}C[r+i]$ 时，$Z\cap Z^{-q}=\varnothing$。证毕。

根据引理 7，本文用 Hermitian 构造方法来设计 F_{q^2} 上码长为 $n=r(q^2+1)$ 的量子 BCH 码。

定理 4　若码长 $n=r(q^2+1)$，$q\geqslant 3$，$m=\mathrm{ord}_n(q^2)=2$。当 $0\leqslant t\leqslant r$ 时，有以下结论。

1) 若 $\frac{q^2-1}{r}$ 为奇数，存在参数为 $[[n,n-4t-4,d\geqslant t+2]]_q$ 的量子 BCH 码。

2) 若 $\frac{q^2-1}{r}$ 为偶数，① 存在参数为 $[[n,n-4t-4,d\geqslant t+2]]_q$ 的量子 BCH 码，其中 $1\leqslant r<\frac{q^2+1-2t}{2}$；② 存在参数为 $[[n,n-4t-2,d\geqslant t+2]]_q$ 的量子 BCH 码，其中 $\frac{q^2+1-2t}{2}\leqslant r\leqslant\frac{q^2-1}{2}$。

证明　由引理 6 可知，分圆陪集 $C[r]$, $C[r+1],\cdots,C[r+t]$ 互不相交，其中 $0\leqslant t\leqslant r$。设 $C_1=\left\langle\prod_i M^{(i)}(x)\right\rangle$，$r\leqslant i\leqslant r+t$，由引理 7 可知，$C_1$ 满足 Hermitian 对偶包含。

1) 若 $\frac{q^2-1}{r}$ 为奇数，当 $r+t\leqslant 2r<q^2+1$ 时，分圆陪集 $C[r]\sim C[r+t]$ 均包含 2 个元素，$C_1=[n,n-2(t+1),\ d_1\geqslant t+2]_{q^2}$。使用 Hermitian 构造方法，可以构造出 $[[n,n-4t-4,d\geqslant t+2]]_q$ 的量子 BCH 码。

2) 若 $\frac{q^2-1}{r}$ 为偶数，当 $1\leqslant r<\frac{q^2+1-2t}{2}$ 时，分圆陪集 $C[r]\sim C[r+t]$ 均包含 2 个元素；当 $\frac{q^2+1-2t}{2}\leqslant r\leqslant\frac{q^2-1}{2}$ 时，仅有一个分圆陪集包含一个元素。剩余证明过程同步骤 1)。使用 Hermitian 构造方法，可以得到对应参数的量子 BCH 码。证毕。

最后，将本文通过 CSS 构造、Steane 构造和 Hermitian 构造得到的量子码与已有的结果进行比较。首先，比较基于有限域 F_q 上的构造结果。

1) CSS 构造结果分析

文献 [10] 构造参数为 $[[n=r(q+1),2(\delta_2-\delta_1),d\geqslant\delta_1]]_q$ 的量子码，其中最小距离下界满足 $2\leqslant\delta_1<\delta_2\leqslant\delta_{max}\leqslant r$。采用本文方法，当其他参数相同时，量子码的最小距离满足 $d\geqslant r+1$。与文献[10]相比，本文方法构造的量子码具有更高的最小距离下界。

2) Steane 构造结果分析

文献[10-11]中构造的量子码的最小距离下界满足 $d\geqslant\delta$，$2\leqslant\delta\leqslant r$。采用本文方法，在得到与文献[10-11]相同的最小距离下界的同时，码参数中的维数结果均好于文献[10-11]。具体比较结果如表 2 所示。更重要的是，通过选择合适的分圆陪集，本文方法还得到了任意有限域上最小距离为 3 的量子 MDS 码。

其次，比较基于有限域 F_{q^2} 上的构造结果。

表 2 Steane 构造方法得到的量子 BCH 码参数比较

构造的量子码	文献[10]	文献[11]
$[[40,32,d\geqslant 4]]_9$	$[[40,28,d\geqslant 4]]_9$	$[[40,30,d\geqslant 4]]_9$
$[[40,36,3]]_9$ (MDS)	—	—
$[[60,48,d\geqslant 5]]_{11}$	$[[60,44,d\geqslant 5]]_{11}$	$[[60,46,d\geqslant 5]]_{11}$
$[[60,56,3]]_{11}$ (MDS)	—	—
$[[84,68,d\geqslant 6]]_{13}$	$[[84,60,d\geqslant 6]]_{13}$	$[[84,62,d\geqslant 6]]_{13}$
$[[84,80,3]]_{13}$ (MDS)	—	—

3) Hermitian 构造结果分析

对于非本原量子 BCH 码，文献[1]构造了一类码参数为 $[[n=r'(q^2-1),\ n-4r+6,d\geqslant r']]_q$ 的量子码。本文方法构造的量子码参数至少与文献[1]相当，在某些码参数中，本文构造的量子码的最小距离下界高于文献[1]中的最小距离下界。具体结果如表 3 所示。

表 3 Hermitian 构造方法得到的非本原量子 BCH 码参数比较

构造的量子码	文献[1]
$[[40,20,d\geqslant 6]]_3$	$[[40,26,d\geqslant 5]]_3$
$[[312,262,d\geqslant 14]]_5$	$[[312,266,d\geqslant 13]]_5$
$[[1200,1104,d\geqslant 26]]_5$	$[[1200,1106,d\geqslant 25]]_7$

最后，文献[14]给出了一种 F_{q^2} 上码长为 $n=(q^4-1)/2$ 的量子码的构造方法，文献[2]对文献[14]的结果做了进一步优化，在某些特定域中其码参数更好。采用本文方法得到了与文献[2]相同的码参数，所以结果同样优于文献[14]。但是，文献[2]只能构造基于奇素数幂有限域上的量子码。本文方法既可以构造奇素数幂有限域上的量子码，也可以构造偶素数幂有限域上的量子码，进一步丰富了量子 BCH 码的种类。具体结果如表 4 所示。

表 4 Hermitian 构造方法得到的量子 BCH 码参数比较

构造的量子码	文献[2]	文献[14]
$[[40,34,d\geqslant 3]]_3$	$[[40,34,d\geqslant 3]]_3$	$[[41,33,d\geqslant 3]]_3$
$[[312,306,d\geqslant 3]]_5$	$[[312,306,d\geqslant 3]]_5$	$[[313,305,d\geqslant 3]]_5$
$[[312,298,d\geqslant 5]]_5$	$[[312,298,d\geqslant 5]]_5$	$[[313,297,d\geqslant 5]]_5$
$[[1200,1194,d\geqslant 3]]_7$	$[[1200,1194,d\geqslant 3]]_7$	$[[1201,1193,d\geqslant 3]]_7$
$[[1200,1186,d\geqslant 5]]_7$	$[[1200,1186,d\geqslant 5]]_7$	$[[1201,1185,d\geqslant 3]]_7$
$[[1200,1178,d\geqslant 7]]_7$	$[[1200,1178,d\geqslant 7]]_7$	$[[1201,1177,d\geqslant 3]]_7$

6 结束语

本文方法构造出的量子 BCH 码与现有的构造方法相比，具有更好的码参数和更高的最小距离下界；更重要的是，本文方法构造出了大量新的量子 BCH 码，进一步丰富了量子 BCH 码的种类。此外，作者还找到了一类任意域上的量子 MDS 码。这是非常有趣的现象，值得未来进行进一步的研究。

参考文献：

[1] LA GUARDIA G G. On the construction of nonbinary quantum BCH codes[J]. IEEE Transactions on Information Theory, 2014, 60(3): 1528-1535.

[2] QIAN J F, ZHANG L N. Improved constructions for nonbinary quantum BCH codes[J]. International Journal of Theoretical Physics, 2017, 56(4): 1355-1363.

[3] MA Z, LU X, FENG K Q, et al. On non-binary quantum BCH codes[C]//Lecture Notes in Computer Science. Berlin: Springer, 2006: 675-683.

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

[5] MA Y N, LIANG F C, GUO L B. Some Hermitian dual containing BCH codes and new quantum codes[J]. Applied Mathematics & Information Sciences, 2014, 8(3): 1231-1237.

[6] TANG N Q, LI Z, XING L J, et al. The gilbert-varshamov bound for stabilizer codes over Zm[J]. IEEE Access, 2018, 6: 45699-45706.

[7] LI Z, XING L J. Classification of q-ary perfect quantum codes[J]. IEEE Transactions on Information Theory, 2013, 59(1): 631-634.

[8] TANG N Q, LI Z, XING L J, et al. Quantum cyclic codes over $\mathbb{Z}_m$ [J]. International Journal of Theoretical Physics, 2019, 58(4): 1088-1107.

[9] HUFFMAN W C, PLESS V. Fundamentals of error-correcting codes[M]. Cambridge: Cambridge University Press, 2003.

[10] 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.

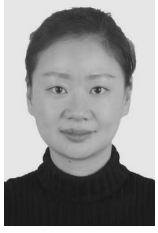
[11] LING S, LUO J Q, XING C P. Generalization of steane's enlargement construction of quantum codes and applications[J]. IEEE Transactions on Information Theory, 2010, 56(8): 4080-4084.

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

[13] LI R H, XU Z B. Construction of [[n, n–4, 3]]$_q$ quantum codes for odd prime power q[J]. Physical Review A, 2010, 82(5): 052316.

[14] KAI X S, ZHU S X, TANG Y S. Erratum: quantum negacyclic codes[J]. Physical Review A, 2013, 88(2): 029907.

[作者简介]



邢莉娟（1982− ），女，陕西西安人，博士，西安电子科技大学副教授，主要研究方向为量子信息论、量子通信、量子纠错码理论。

李卓（1980− ），男，陕西西安人，博士，西安电子科技大学教授，主要研究方向为量子计算、量子信息论、5G 中的编码调制技术。