有限域上非本原 BCH 码的对偶包含判定

肖芳英[1],陈汉武[1],刘志昊[1],李志强[1,2],刘文杰[1,3]
(1.东南大学计算机科学与工程学院,江苏南京 210096;2.扬州大学信息工程学院计算机科学与技术系,
江苏扬州 225009;3.南京信息工程大学计算机科学与软件学院,江苏南京 210044)

摘 要: 循环陪集在经典和量子纠错编码理论中具有非常重要的作用.根据 CSS 编码定理知,利用经典 BCH 码构造量子 BCH 码时需要判断经典 BCH 码是否包含其对偶码.本文给出了循环陪集的若干重要性质,根据这些性质得到了判断有限域上非本原 BCH 码是否包含其对偶码的准则.本文给出的判断准则时间复杂度为多项式的,并且该判断准则对本原 BCH 码也适用.

关键词: 量子纠错码; BCH 码; 对偶码; 循环陪集
中图分类号: TP387 **文献标识码:** A **文章编号:** 0372-2112 (2010) 08-1858-04

Dual-Containing Determination Method for Non-Primitive BCH Codes over Finite Field

XIAO Fang-ying[1], CHEN Han-wu[1], LIU Zhi-hao[1], LI Zhi-qiang[1,2], LIU Wen-jie[1,3]
(1. *School of Computer Science and Engineering, Southeast University, Nanjing, Jiangsu* 210096, *China*;
2. *College of Information Engineering, Yangzhou University, Yangzhou, Jiangsu* 225009, *China*;
3. *School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, Jiangsu* 210044, *China*)

Abstract: Cyclotomic cosets play very important roles in classical and quantum error correction theory. In order to constructing quantum BCH (Bose Chaudhuri Hocquenghem) codes with CSS constructing method from classical BCH codes, it needs to determine whether a BCH code contains its dual. It proposed several properties of cyclotomic cosets. And according to these properties, an algorithm with polynomial time complexity was presented to determine whether a non-primitive BCH code over finite field contains its dual code, which can also be applied to nonnarrow sense primitive BCH codes.

Key words: quantum error correcting codes; BCH codes; dual codes; cyclotomic cosets

1 引言

循环陪集[1]在经典纠错编码理论中具有非常重要的作用,特别是与经典循环码、BCH 码、Goppa 码和 Alternant 码的构造过程密切相关.文献[2]和[3]对循环陪集的结构作了较为详细的讨论,并将其应用于确定 BCH 码和 Goppa 码的信息位数[2]以及它们的最小距离[3].文献[4]利用循环陪集来确定 Goppa 码和 Alternant 码的最小距离下限[5].循环陪集在量子编码理论中也起着重要的作用.根据引理 1[6]可知,如何判断一个码是否包含其对偶码在量子编码理论中尤为重要.

引理 1 如果存在参数为$[n,k,d]$的二元线性码 C,并且 $C^{\perp}\subseteq C$,这里 $C^{\perp}$是经典纠错码中 C 对于通常内积$(u,v)=\sum_{i=1}^{n}u_iv_i$ 的对偶码,则存在参数为$[\![n,2k-n,d]\!]$的纯量子码.

文献[7]中首次提出借助引理 1 的方法运用经典 BCH 码构造二元量子 BCH 码.它通过分析 BCH 码的循环陪集与其对偶码的循环陪集之间的关系,给出了一种判断二元经典 BCH 码是否包含其对偶码的方法,即设 C 是有限域 $GF(2)$上码长为 n 的 BCH 码,其定义集为 I_C,如果$\forall\, i\in I_C$,有$(n-i)\notin I_C$,则 C 一定包含其对偶码(即 $C^{\perp}\subseteq C$).文献[8]扩展了引理 1 中的量子码构造方法,得到如下引理.

引理 2 设二元线性码 $C=[n,k,d]$包含其对偶码(即 $C^{\perp}\subseteq C$),则 C 可以扩展为二元线性码 $C'=[n,k'>k+1,d']$,并且由线性码 C 和 C'可以构造参数为$[\![n,k+k'-n,\min(d_1,\lceil 3d'/2\rceil)]\!]$的量子码.

文献[8]还根据循环陪集的性质,给出了判断二元本原 BCH 码是否包含其对偶码的改进方法.如果有限

收稿日期:2008-01-23;修回日期:2009-12-03
基金项目:国家自然科学基金(No.60873101);江苏省自然科学基金(No.BK2008209);东南大学优秀博士论文基金(No.YBJJ0820)

域 $GF(2)$上某本原 BCH 码 C 的设计距离 $\delta \leqslant 2^{\lceil m/2 \rceil}-1$,则 $C^{\perp} \subseteq C$,但是该结论对二元非本原 BCH 码不成立.文中还给出了一个 $C^{\perp} \not\subset C$ 的充分条件,如果存在 $i \in C_s \subseteq I_C$ 且 $n-i \in C_s$,一定有 m 和 $m_s = |C_s|$ 是偶数且 $C^{\perp} \not\subset C$.该结论仅对 m 是偶数且 m_s 是偶数的情况下,如果 $C_s \subseteq I_C$ 且 $n-s \in C_s$,则可以判断 $C^{\perp} \not\subset C$.但是,当 m 是偶数而 m_s 为奇数或 m 是奇数时,或当 $i \in C_s$ 和 $n-i \in C_s$ 只有一个成立时,利用该结论无法判断 C 是否包含其对偶码.文献[9]中给出了一种判断有限域 $GF(p)$上本原 BCH 码是否包含其对偶码的准则,即如果本原 BCH 码 C 的设计距离

$$\delta \leqslant \begin{cases} q^{\lceil m/2 \rceil}-1, & m \text{ is even} \\ q^{\lceil m/2 \rceil}-q+1, & m \text{ is odd} \end{cases}$$

则一定有 $C^{\perp} \subseteq C$.同样地,该结论对非本原 BCH 码也不成立.文献[7~9]中给出的方法都是针对狭义本原 BCH 码(即 $b=1$).到目前为止,没有检索到讨论有限域 $GF(p)$上狭义非本原 BCH 码以及广义本原或非本原 BCH 码($b>1$)是否包含其对偶码的文献.

量子纠错码基于量子力学基本原理和量子信息论,量子状态所处的 Hilbert 空间可能是高维的(非二维),所以研究有限域 $GF(p)$上的狭义(或广义)本原(或非本原)量子 BCH 码是非常有意义的.本文给出了循环陪集的若干重要性质,根据这些性质提出了一种在多项式的时间内可以判断出有限域 $GF(p)$上非本原或本原 BCH 码是否包含其对偶码的方法,该方法对狭义和广义 BCH 码均适用.

2　循环陪集的基本性质

定义 1　设 p 是素数,n 是正整数且 $\gcd(n,p)=1$(即 n 与 p 互素),m 是满足 $n \mid (p^m-1)$的最小正整数,$s \in GF(p^m)$且 $0 \leqslant s < n$,称集合 $C_s = \{s, ps, p^2 s, \cdots, p^{m_s-1}s\} \pmod n$为有限域 $GF(p^m)$上关于 s 的 mod$n$ 的循环陪集,其中 m_s 是满足 $p^{m_s}s \equiv s \pmod n$的最小正整数.$s$ 是 C_s 中的最小元素,称为循环陪集代表元.

定义 2　令 $H = \{s \mid s = \min C_s$(即 s 是 C_s 中的最小元素),C_s 是有限域 $GF(p^m)$上关于 $s(0 \leqslant s < p^m-1)$的 mod$n$ 的循环陪集$\}$,称 H 为 mod$n$ 的循环陪集首集.

例如　$p=5, \bmod 24 = 5^2-1$

$C_0=\{0\}$　$C_1=\{1,5\}$　$C_2=\{2,10\}$

$C_3=\{3,15\}$　$C_4=\{4,20\}$　$C_6=\{6\}$

$C_7=\{7,11\}$　$C_8=\{8,16\}$　$C_9=\{9,21\}$

$C_{12}=\{12\}$　$C_{13}=\{13,17\}$　$C_{14}=\{14,22\}$

$C_{18}=\{18\}$　$C_{19}=\{19,23\}$

由以上示例易得循环陪集的如下性质:

设 p 是素数,m 是满足 $n \mid (p^m-1)$的最小正整数.

(1)定义集 $I_C = \{0,1,2,\cdots,n-1\} = \bigcup_s C_s$[1]

循环陪集具有如下类似陪集的性质:

(2)有限域 $GF(p^m)$上任意两个关于 s 和 r 的 mod$n$ 的循环陪集 $C_s, C_r (s \neq r)$,满足:

(a) $\forall\, a \in I_C, \exists\, s \in H$ 使得 $a \in C_s$;

(b) $C_s = C_r \Leftrightarrow \exists\, t>0, r = sp^t \bmod n$;

(c) $s, r \in H$,则 $C_s \cap C_r = \varnothing$.

证明　前两个性质由定义 1 和定义 2 可以立即得出.下面证明第 3 个性质.不妨设 $s<r$,则 $s \notin C_r$.设 $|C_i| = m_i\ (i=s,r)$, $a \in C_s \cap C_r$,则存在 u、v,使 $a = sp^u \cdot (\bmod n)$和 $a = rp^v (\bmod n)$.不妨设 $u<v$,则 $s = rp^{v-u} \cdot (\bmod n)$,由此可知 $s \in C_r$,推出矛盾,故 $C_s \cap C_r = \varnothing$.

(3)设 $s>0$ 且 $s \in H$, C_s 是有限域 $GF(p^m)$上关于 s 的 mod$n$ 的循环陪集,则对任意的正整数 k 都有 $s \neq kp$.

证明　设 $s = kp, p \geqslant 2, k < s$,则由循环陪集的定义知,$s$ 一定属于 k 所在的循环陪集 C_t(即 $s \in C_t$),且 $t \leqslant k < s$,又由性质 2 知 $C_t \cap C_s = \varnothing$,故 $s \neq kp$.

(4)设 $C_s (s \in H)$是有限域 $GF(p^m)$上关于 s 的 mod$n$ 的循环陪集,则 $|C_s| \,\|\, m$.进一步,如果 $\gcd(n,s)=1$,则 $|C_s| = m$.令 $a = \max(C_s)$,则 $|C_s| = |C_{n-a}|$;特别地,如果 $n=2s$,则 $|C_s| = 1$.

证明　由文献[1]知:对任意的 $0<s<n$,都有 $|C_s| \,\|\, m$.因为 $sp^m \equiv s (\bmod n)$,设 $m_s \leqslant m$,且 $sp^{m_s} = s \cdot (\bmod n)$,即 $n \mid s(p^{m_s}-1)$,又由 $\gcd(n,s)=1$ 可知 $n \mid (p^{m_s}-1)$,故 $m_s = m$.设 $a = \max(C_s)$,则存在 $k \leqslant m_s$,使得 $a = sp^k (\bmod n)$.如果 $(n-a) \in C_s$,显然有 $|C_s| = |C_{n-a}|$.否则 $\forall\, b \in C_{n-a}$,存在 $i \leqslant m_{n-a}$,使 $b = (n-a)p^i = np^i - sp^{k+i} = -sp^{k+i} = n - sp^{k+i} (\bmod n)$,故 $C_{n-a} = \{n-r \mid r \in C_s\}$,所以 $|C_s| = |C_{n-a}|$.如果 $n=2s$,则 $C_s = \{s\}$,故 $|C_s| = 1$.

由性质(4)易得如下两个性质:

(5)设 $C_s (s \in H, s \neq 0)$是有限域 $GF(p^m)$上关于 s 的 mod$n$ 的循环陪集,令 $t = \max(C_s)$,对 $\forall\, a \in C_s$,则 $\exists\, b \in C_{n-t}$使得 $a+b \equiv 0 (\bmod n)$.特别地,如果 $s \mid n$ 且存在正整数 r,使得 $n/s - 1 = p^r \bmod n$,则 $\forall\, a \in C_s, \exists\, b \in C_s$,满足 $a+b \equiv 0 (\bmod n)$;如果 $n=2s$,则 $s+s \equiv 0 (\bmod n)$,即 $C_s = \{s\}$.

该性质简化了循环陪集的求解过程,使得只需求所有循环陪集的一半左右的循环陪集.

(6)有限域 $GF(p^m)$上关于 $s(0 \leqslant s < n)$的 mod$n$ 的循环陪集 C_s 至少有 $\lceil (n-1)/m \rceil + 1$ 个(即 $|H| \geqslant \lceil (n-1)/m \rceil + 1$);如果 m 是素数,则 C_s 的个数恰好为 $(n-1)/m+1$(即 $|H| = \lceil (n-1)/m \rceil + 1$).

文献[4]中给出了循环陪集首集中元素个数的精

确表达式：$|H|=\frac{1}{m}\sum_{d|m}q^{m/d}\cdot\varphi(d)-2$，其中 $\varphi(d)$ 是欧拉函数，表示小于 d 且与 d 互素的正整数个数.

将文献[8]中关于有限域 $GF(2)$ 上非本原 BCH 码的结论推广到有限域 $GF(p)$ 上可得如下性质：

(7)设有限域 $GF(p^m)$ 上关于 s 的 mod$n$ 的循环陪集为 $C_s(s\in H, s\neq 0)$，如果 $\forall\ a\in C_s$ 有 $n-a\in C_s$，则 m 和 $m_s=|C_s|$ 都为偶数.

证明 由性质 5 知，$i\in C_s$ 且 $n-i\in C_s$ 当且仅当 $n-s\in C_s$，即存在 $k\leqslant m_s$，使得 $n-s=sp^k(\mathrm{mod}n)$，同余方程两边同时乘以 p^k 得到 $sp^{2k}=-sp^k=s(\mathrm{mod}n)$，即 $2k=m_s$，所以 m_s 为偶数，又 $m_s|m$，所以 m 也为偶数.

注意，该性质的逆命题不成立，即如果 m 和 $m_s=|C_s|$ 都为偶数，则 $\forall\ a\in C_s$ 不一定有 $n-a\in C_s$. 例如 $p=5, n=24=5^2-1, C_2=\{2,10\}, m_2=m=2$，但是 $24-2=22\notin C_2$.

(8)当 p 为偶素数时，$\forall\ C_s(s\neq 0)$，s 是奇数，如果 $n\neq 2s$，则 $\max(C_s)$ 是偶数，其中 $\max(C_s)$ 是 C_s 中的最大元素.

证明 由性质 3 知：对任意的 C_s 有 $s\neq kp$，故 s 是奇数，如果 $n\neq 2s$，则存在 $t(0<t<m_s)$ 使得 $\max(C_s)=s2^t$，故 $\max(C_s)$ 是偶数.

3 判断 BCH 码是否包含其对偶码

设 p 是素数，n 是正整数且 $\gcd(n,p)=1$，$Z_n^*=\{a|\gcd(a,n)=1, 1\leqslant a\leqslant n-1\}$，$p$ 在 Z_n^* 中的阶为 m，即 $p^m\mathrm{mod}n=1$. 设 $\alpha\in GF(p^m)$，且是 $GF(p^m)^*$（$GF(p^m)^*=GF(p^m)-\{0\}$）中的一个 n 阶元素（即 $\alpha^n=1$）. 如果 $n=p^m-1$，则 α 为有限域 $GF(p^m)$ 的本原元. 设 $M^{(i)}(x)$ 是 $\alpha^i\in GF(p^m)$ 在 $GF(p)$ 上的极小多项式，如果 $i\in C_s$，则 $M^{(i)}(x)=\prod_{j\in C_s}(x-\alpha^j)$[1]，其中 C_s 是有限域 $GF(p^m)$ 上关于 $s(0<s<n)$ 的 mod$n$ 的循环陪集. 设 b 是正整数（$b\geqslant 1$）且 $lcm\{M^{(b)}(x), M^{(b+1)}(x), \cdots, M^{(b+\delta-2)}(x)\}$ 是多项式 $M^{(b)}(x), M^{(b+1)}(x), \cdots, M^{(b+\delta-2)}(x)$ 的最小公倍式，则 $g(x)=lcm\{M^{(b)}(x), M^{(b+1)}(x), \cdots, M^{(b+\delta-2)}(x)\}$ 是有限域 $GF(p)$ 上码长为 n，设计距离为 $\delta(\delta>0)$ 的 p 元 *BCH* 码 C（记为 $B_p(n,\delta,\alpha,b)$）的生成多项式[1]. 如果 $n=p^m-1$，则该 BCH 码称为本原 BCH 码，否则称为非本原 BCH 码[1]；如果 $b=1$，则该 BCH 码称为狭义 BCH 码，否则称为广义 BCH 码[1]. 令 $I_C=C_{b_0}\cup C_{b_1}\cup\cdots\cup C_{b_{\delta-2}}$，其中 C_{b_i} 是有限域 $GF(p^m)$ 上关于 b_i 的 mod$n$ 的循环陪集且 $b+i\in C_{b_i}$，称 I_C 为 BCH 码 C 的定义集. 令该 BCH 码的循环陪集首集 $H_\delta=\{b_0, b_1, \cdots, b_{\delta-2}\}$，由于可能存在 $j>i(i,j\in\{0,1,2,\cdots,\delta-2\})$ 使得 $b+j\in C_{b_i}$（即 $C_{b_i}=C_{b_j}$），所以 $|H_\delta|\leqslant\delta-1$. 由文献[7]知，$C$ 的对偶码 $C^\perp$ 的定义集 $I_{C^\perp}=\bigcup_{i\in\bar{I}_C}C_{n-i}$，其中 $\bar{I}_C=\{0,1,2,\cdots,n-1\}\setminus I_C$.

根据循环陪集的相关性质，本文提出了一种有效的方法判断有限域 $GF(p)$ 上 BCH 码是否包含其对偶码，对本原（或非本原）BCH 码（$b\geqslant 1$）也都成立.

将关于有限域 $GF(2)$ 上本原（或非本原）狭义 BCH 码是否包含其对偶码的结论推广到有限域 $GF(p)$ 上本原（或非本原）BCH 码[7]（$b\geqslant 1$）上可得如下引理：

引理 3 设 C 是有限域 $GF(p)$ 上码长为 n 的本原（或非本原）BCH 码（$b\geqslant 1$），其定义集为 I_C，如果 $\forall\ i\in I_C$，有 $(n-i)\notin I_C$，则 $C^\perp\subseteq C$.

证明 设有限域 $GF(p)$ 上码长为 n，设计距离为 $\delta(\delta>0)$ 的 BCH 码 $C=B_p(n,\delta,\alpha,b)$（$b\geqslant 1$）的生成多项式为 $g(x)=lcm\{M^{(b+i)}(x)\}(i\in\{0,1,2,\cdots,\delta-2\})$，则 C 的定义集为 $I_C=\bigcup_{i=0}^{\delta-2}C_{b_i}$，其对偶码 $C^\perp$ 的定义集 $I_{C^\perp}=\bigcup_{i\in\bar{I}_C}C_{n-i}$，其中 $\bar{I}_C=\{0,1,2,\cdots,n-1\}\setminus I_C$；如果 $\forall\ i\in I_C$，满足 $(n-i)\notin I_C$，则 $(n-i)\in\bar{I}_C$，从而 $C_i\in I_{C^\perp}$，由此可得 $I_C\subseteq I_{C^\perp}$，所以 $C^\perp$ 的生成多项式 $q(x)=lcm\{g(x), M^{(r)}(x), \cdots\}$，其中 $r\in I_{C^\perp}\setminus I_C$. 由此可知 $g(x)|q(x)$，所以 $\langle q(x)\rangle\subseteq\langle g(x)\rangle$，其中 $\langle q(x)\rangle$、$\langle g(x)\rangle$ 分别表示 $q(x)$、$g(x)$ 生成的 BCH 码，即 $C^\perp\subseteq C$.

由循环陪集性质 4、性质 5、性质 7 以及上述引理 3 可得如下定理：

定理 1 设 $C=B_p(n,\delta,\alpha,b)$ 是有限域 $GF(p)$ 上码长为 n，设计距离为 $\delta(\delta>0)$ 的 BCH 码，其定义集为 I_C，对应的循环陪集首集为 H_δ，则：

(a)设 $\forall\ s\neq 0$ 且 $s\in H_\delta$，即 $C_s\subseteq I_C$，令 $a=\max C_s$（$\max C_s$ 是 C_s 中的最大元素），如果 $n-a\notin H_\delta$，则 $C^\perp\subseteq C$；

(b)如果 $n=2s$ 且 $s\in H_\delta$，则 $C^\perp\not\subset C$；

(c)当 m 是偶数时，如果 $C_s\subseteq I_C$ 满足 m_s 是偶数且 $n-s\in C_s$，则 $C^\perp\not\subset C$.

证明 (a)由性质 5 知，$\forall\ C_s\subseteq I_C(s\neq 0)$，令 $a=\max C_s$，则 $\forall\ t\in C_s$，$\exists\ r\in C_{n-a}$，使得 $t+r=n$ 即：$r=n-t$. 故如果 $\forall\ t\in C_s\subseteq I_C$，有 $n-a\notin H_\delta$，则 $C_{n-a}\cap I_C=\varnothing$，所以 $n-t\notin I_C$，由引理 2 知 $C^\perp\subseteq C$.

(b)如果 $n=2s$，则 $n-s=s\in C_s\subseteq I_C$，故 $C^\perp\not\subset C$.

(c)由性质 7 知，如果 m 是偶数，在判断有限域 $GF(p)$ 上某 BCH 码是否包含其对偶码时，可以先判断 $C_s\subseteq I_C$ 且 m_s 是偶数的循环陪集 C_s. 如果存在 $C_s\subseteq I_C$，满足 $m_s=|C_s|$ 是偶数且 $n-s\in C_s$，则一定有 $C^\perp\not\subset C$. 否则，还需要利用(a)对剩余的循环陪集进行判断.

4 时间复杂度分析

利用引理 3 判断某 p 元 BCH 码 C 是否包含其对偶码时,需要将 I_C 中的所有元素两两比较,时间复杂度为 $O(|I_C|^2)$,其中 $|I_C|$ 表示 I_C 中元素个数.因为对 $\forall b_i \in H_\delta$ 有 $|C_{b_i}| \leqslant m$(等号成立,当且仅当 $\gcd(n, b_i) = 1$),所以 $|I_C| \leqslant m|H_\delta| = m(\delta - 1)$,即时间复杂度为 $O((m(\delta-1))^2)$.而利用定理 1 给出的方法判断时,只需要找出各 $C_s(b_0 \leqslant s \leqslant b_{\delta-2})$中的最大值 a,并判断 $n - a$ 是否属于 H_δ.如果对任意 $C_s \subseteq I_C$ 都有 $n - a \notin H_\delta$,则 $C^\perp \subseteq C$,否则 $C^\perp \not\subset C$. I_C 中共有 $H_\delta(|H_\delta| \leqslant \delta - 1)$个 C_s 且 $|C_s| \leqslant m$,查找每个 C_s 中的最大值最多需要比较 $m-1$ 次,找到最大值 a 之后再在 H_δ 中查找是否存在 $n - a$ 时,需要比较 $\delta - 2$ 次 (因为 H_δ 是有序的,所以当 δ 较大时可以利用折半查找法查找,最多需要 $\log\delta$ 次比较),所以总共最多需要 $(\delta-1)(\log\delta + m - 1)$次运算,时间复杂度为多项式的.

参考文献:

[1] F J MacWilliams, N J A Sloane. The Theory of Error-Correcting Codes[M]. Oxford, New York, Amsterdam: North-Holland publishing company, 1977. 103 – 105.

[2] 岳殿武.循环陪集结构及应用[J].系统科学与数学,1992,12(1):15 – 20.
Yue Dian-wu. The structure of cyclotomic cosets and its applications[J]. Journal of Systems Science and Complexity, 1992, 12(1):15 – 20. (in Chinese)

[3] Yue Dian-wu, Feng Guang-zeng. Minimum cyclotomic cosets representatives and their applications to bch codes and goppa codes[J]. IEEE Transactions on Information Theory, 2000, 46(7):2625 – 2628.

[4] 王建宇.循环陪集首集与 Goppa 码、Alternant 码最小距离下限[J].通信学报,1994,15(1):107 – 112.
Wang Jian-yu. The leed set of cyclotomic cosets and the lower bounds of minimum distance for goppa codes and alternant codes[J]. Journal on Communications, 1994, 15(1):107 – 112. (in Chinese)

[5] 冯贵良.Goppa 码的最小距离下限和维数上限的扩张[J].电子学报,1983,2(2):66 – 72.
Feng Gui-liang. Generalization of lower bound on the minimum distance and the upper bound on the number of parity check digits for Goppa codes[J]. Acta Electronica Sinica, 1983, 2(2):66 – 72. (in Chinese)

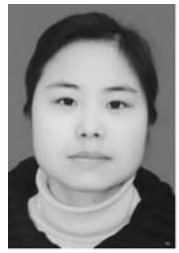
[6] 陈汉武.量子信息与量子计算简明教程[M].江苏南京:东南大学出版社,2006.138 – 139.

[7] M Grassl, Th Beth. Codes for the quantum erasure channel[J]. Physical Review A, 1997, 56(1):33 – 38.

[8] A M Steane. Enlargement of Calderbank-Shor-Steane quantum codes[J]. IEEE Transactions on Information Theory, 1999, 45(7):2492 – 2495.

[9] Salah A. Aly, Andreas Klappenecker, Pradeep Kiran Sarvepalli. Primitie quantum BCH codes over finite fields[A]. Proceedings of the IEEE ISIT International Symposium on Information Theory[C]. Washington: IEEE Press, 2006. 1114 – 1118.

作者简介:



肖芳英　女,1982 年生于江西高安,2005 年毕业于江西师范大学计算机信息工程学院.现为东南大学计算机科学与工程学院硕博连读生,从事可逆电路错误检测与定位以及量子纠错码方面的有关研究.
E-mail: xfy504@hotmail.com

陈汉武　男,1955 年生于江苏南京,教授、博士生导师.1981 年、2000 年分别在东南大学、日本国立山口大学获理学学士和理工学博士学位.主要从事经典信息论、量子信息与量子计算、数理解析等方面的研究工作.
E-mail: hw_chen@seu.edu.cn