# BCH 码的定义集分解及应用

李瑞虎，　许　根，　吕良东
(空军工程大学理学院，陕西西安，710051)

**摘要**　以分圆陪集理论和方法为基础，由二元码的 Euclid 正交性理论和四元码的 Hermite 正交性理论，分别引入二元 BCH 码和四元 BCH 码的定义集分解概念；再利用 BCH 码的定义集分解导出二元 BCH 码和四元 BCH 码的对偶码的正交分解。在此基础上，研究并解决了本原二元和四元 BCH 码的定义集分解；依据 BCH 码的定义集分解结论，构造出一些参数优良的纠缠辅助量子纠错码。定义集分解方法简化了由 BCH 码构造纠缠辅助量子纠错码的理论推导，改进了已有文献中确定最优纠缠比特数的算法，提供了一种计算最优纠缠比特数的新思路，为研究由循环码构造纠缠辅助量子纠错码问题提供了可借鉴的新理论和新方法。

**关键词**　分圆陪集；BCH 码；定义集；纠缠辅助；量子纠错码
**DOI**　10.3969/j.issn.1009-3516.2013.02.019
**中图分类号**　O157.4　　**文献标识码**　A　　**文章编号**　1009-3516(2013)02-0086-04

## Decomposition of Defining Sets of BCH Codes and Its Applications

LI Rui-hu，XU Gen，LU Liang-dong
(Science College，Air Force Engineering University，Xi′an 710051，China)

**Abstract**：Based on basic theory of cyclotomic coset，the concepts of decomposition of defining sets for binary and quaternary BCH codes are introduced respectively this decomposition of defining sets builds up a bridge among the Euclidean orthogonal decomposition of binary BCH codes and Hermitian orthogonal decomposition of quaternary BCH codes. Then the orthogonal decomposition of the dual codes of binary and quaternary BCH codes is also presented. Furtherly，the decomposition of the defining sets of primitive binary and quaternary BCH codes with given designed distances is well studied and solved. Applying the results，some entanglement-assisted quantum codes with good parameters are constructed. The method proposed in this paper devised a new scheme in determining the optimal number of entangled bits，which can simplify the theoretical derivation in constructing entanglement-assisted quantum error correcting codes from classical BCH codes，and also be useful for studying general constructions of entanglement-assisted quantum error correcting codes from cyclic codes.

**Key words**：cyclotomic coset；BCH codes；defining set；entanglement-assisted；quantum error correcting codes

根据量子纠错码的稳定子理论，只有满足对偶包含关系(或自正交)的经典码才能用于构造标准量子纠错码[1-2]，这就限制了经典码在量子编码领域的应用。为突破这一困境，文献[3]利用量子纠缠理论

**收稿日期**：2012-12-03
**基金项目**：国家自然科学基金资助项目(11071255)
**作者简介**：李瑞虎(1966－)，男，安徽亳州人，教授，博士，主要从事代数编码及密码学研究.
E-mail：liruihu2008@yahoo.com.cn

创立纠缠辅助量子纠错码(简称 EAQECC)的理论框架体系,人们可以用任意的经典线性码构造 EAQECC,而不必要求经典码满足对偶包含条件,从而极大地促进了量子编码理论的发展。文献[3]同时给出了利用 CSS 方法构造 EAQECC 时所需最优纠缠比特数的公式,文献[4]中对此公式做了不同情况下的拓展,但是最优纠缠比特数的具体计算问题并没有解决,这使得 EAQECC 构造性研究进展缓慢,不能适应量子编码理论和应用发展的需要。

BCH 码是被人们广泛研究的一类循环码,在经典和量子信息等领域具有重要的理论和实际应用价值[5-10]。用经典 BCH 码构造标准量子码,首先应确定 BCH 码满足的对偶包含条件。文献[6～9]得到本原 BCH 码包含其 Euclid(或 Hermite)对偶码的充要条件——极大设计距离 $\delta_{\max}$ 条件。当 BCH 码的设计距离超过 $\delta_{\max}$ 时,必须使用纠缠辅助比特才能由 BCH 码构造量子码。本文以分圆陪集理论和文献[3]为基础,引入 BCH 码的定义集分解概念,确定本原 BCH 码的定义集分解并构造 EAQECC。

## 1　预备知识

为简化叙述,做如下约定:本文中 $q$ 为素数的幂,$\mathbf{F}_q$ 为 $q$ 元域;设 $n>1$ 为正整数且 $\gcd(n,q)=1$,所有的数为整数。用区间$[0,n-1]$表示$\{0,1,2,\cdots,n-1\}$,其子集$\{e,e+1,\cdots,f\}$记为区间$[e,f]$。若 $x\in[0,n-1]$,$C_x$ 记 $x$ 所在的模 $n$ 的 $q$－分圆陪集[5,9]。码 $\mathbf{C}$ 的 Euclid 对偶和 Hermite 对偶分别表示为 $\mathbf{C}^{\perp}$ 和 $\mathbf{C}^{\perp_h}$[5]。

若 $\mathbf{F}_q$ 上码长为 $n$ 的循环码 $\mathbf{C}$ 的定义集 $T=\bigcup_{i=0}^{\delta-2}C_{b+i}$,则称 $\mathbf{C}$ 为设计距离为 $\delta$ 的 BCH 码;当 $n=q^t-1$ 且 $b=1$ 时,称 $\mathbf{C}$ 为本原狭义 BCH 码[5]。文献[6～9]用定义集、分圆陪集等方法刻划对偶包含循环码(特别是 BCH 码)的特征,主要原理与结论如下**引理** 1.1－1.3。

**定义** 1.1[8-9] 1)若 $n-x\in C_x$,则称分圆陪集 $C_x$ 是对称的;否则称其为非对称的。非对称的分圆陪集 $C_x$ 和 $C_{-x}=C_{n-x}$ 成对出现,叫做非对称偶,简记为$(C_x,C_{-x})$。

2)设 $q=r^2$,若 $n-rx\in C_x$,则称分圆陪集 $C_x$ 是斜对称的;否则称其为斜非对称的。斜非对称的分圆陪集 $C_x$ 和 $C_{-rx}=C_{n-rx}$ 成对出现,叫做斜非对称偶,简记为$(C_x,C_{-rx})$。

**引理** 1.1[7]　设 $\mathbf{F}_q$(或 $\mathbf{F}_{q^2}$)上码长为 $n$ 的循环码 $\mathbf{C}$ 的定义集为 $T$。

1)若 $\mathbf{C}$ 为 $q$－元码,则 $\mathbf{C}^{\perp}\subseteq\mathbf{C}$ 当且仅当 $T\cap T^{-1}=\varnothing$,其中 $T^{-1}=\{n-x\mid x\in T\}$。

2)若 $\mathbf{C}$ 为 $q^2$－元码,则 $\mathbf{C}^{\perp_h}\subseteq\mathbf{C}$ 当且仅当 $T\cap T^{-q}=\varnothing$,其中 $T^{-q}=\{n-qx\mid x\in T\}$。

**引理** 1.2[8-9]　设 $\mathbf{F}_q$(或 $\mathbf{F}_{q^2}$)上码长为 $n$ 的循环码 $\mathbf{C}$ 的定义集为 $T=\bigcup_{i\in I}C_i$。则有:

1)若 $\mathbf{C}$ 为 $q$－元码,则 $\mathbf{C}^{\perp}\subseteq\mathbf{C}$ 当且仅当 $T$ 中每个 $C_i$ 为非对称的,且 $C_i$ 与 $C_j$ 不构成非对称偶,$0\leqslant i,j\leqslant\delta-2$。

2)若 $\mathbf{C}$ 为 $q^2$－元码,则 $\mathbf{C}^{\perp_h}\subseteq\mathbf{C}$ 当且仅当 $T$ 中每个 $C_i$ 为斜非对称的,且 $C_i$ 与 $C_j$ 不构成斜非对称偶,$0\leqslant i,j\leqslant\delta-2$。

**引理** 1.3[6-7]　设 $\mathbf{C}$ 为 $\mathbf{F}_q$(或 $\mathbf{F}_{q^2}$)上码长为 $n$、设计距离为 $\delta$ 的本原狭义 BCH 码,则:

1)若 $n=q^m-1$,$\mathbf{C}=\mathrm{BCH}(n,q;\delta)$,则 $\mathbf{C}^{\perp}\subseteq\mathbf{C}$ 当且仅当 $\delta\leqslant\delta_{\max}=q^{\lceil\frac{m}{2}\rceil}-1$。

2)若 $n=q^{2m}-1$,$\mathbf{C}=\mathrm{BCH}(n,q^2;\delta)$,则 $\mathbf{C}^{\perp_h}\subseteq\mathbf{C}$ 当且仅当 $\delta\leqslant\delta_{\max}=q^{m+[m\ even]}-1+(q^2-2)[m\ even]$。

当 $\delta>\delta_{\max}$,本原狭义 BCH 码的定义集 $T$ 不满足**引理** 1.1,为此引入以下定义。

**定义** 1.2　设 $\mathbf{F}_q$(或 $\mathbf{F}_{q^2}$)上码长为 $n$ 的循环码 $\mathbf{C}$ 的定义集为 $T$。

1)对 $\mathbf{F}_q$ 上循环码 $\mathbf{C}$,记 $T\cap T^{-1}=T_s$,$T\setminus T_s=T_{as}$。$T_s$ 和 $T_{as}$ 叫做 $\mathbf{C}$ 的定义集分解。

2)对 $\mathbf{F}_{q^2}$ 上循环码 $\mathbf{C}$,记 $T\cap T^{-q}=T_{ss}$,$T\setminus T_{ss}=T_{sas}$。$T_{ss}$ 和 $T_{sas}$ 叫做 $\mathbf{C}$ 的定义集分解。

依据定义集分解,用文献[5]的**定理** 4.4.2 和 4.4.11(或文献[8～9])易推出如下**引理** 1.4 和**引理** 1.5。

**引理** 1.4　设 $\mathbf{F}_q$(或 $\mathbf{F}_{q^2}$)上 BCH 码 $\mathbf{C}$ 的定义集为 $T$。$T$ 的分解如**定义** 1.2 所述。

1)设 $i,j\in T_{as}$,则 $C_i$ 为非对称的,且 $C_i$ 和 $C_j$ 不构成非对称偶。若 $l\in T_s$,则 $C_l$ 为对称的,或 $C_l$ 为非对称的且存在 $p\in T_s$,$C_l$ 和 $C_p$ 构成非对称偶。

2)设 $i,j\in T_{sas}$,则 $C_i$ 为斜非对称的,且 $C_i$ 和 $C_j$ 不构成斜非对称偶。若 $l\in T_{ss}$,则 $C_l$ 为斜对称的,或 $C_l$ 为斜非对称的且存在 $p\in T_{ss}$,$C_l$ 和 $C_p$ 构成斜非对称偶。

**引理** 1.5　设 $\mathbf{F}_q$(或 $\mathbf{F}_{q^2}$)上 BCH 码 $\mathbf{C}$ 的定义集为 $T$。$T$ 的分解如**定义** 1.2 所述。

1)若 $\mathbf{C}$ 为 $\mathbf{F}_q$ 上循环码,以 $T_{as}$ 和 $T_s$ 为定义集的循环码分别记为 $\mathbf{C}_1$ 和 $\mathbf{C}_2$。则 $\mathbf{C}_1^{\perp}\subseteq\mathbf{C}_1$,$\mathbf{C}_2\cap\mathbf{C}_2^{\perp}=\{0\}$,$\mathbf{C}_1^{\perp}\subset\mathbf{C}_2$,$\mathbf{C}_1\cap\mathbf{C}_2=\mathbf{C}$,$\mathbf{C}_1^{\perp}+\mathbf{C}_2^{\perp}=\mathbf{C}^{\perp}$。

2)若 $\mathbf{C}$ 为 $\mathbf{F}_{q^2}$ 上循环码,以 $T_{sas}$ 和 $T_{ss}$ 为定义集的循环码分别记为 $\mathbf{C}_1$ 和 $\mathbf{C}_2$。则 $\mathbf{C}_1^{\perp_h}\subseteq\mathbf{C}_1$,$\mathbf{C}_2\cap\mathbf{C}_2^{\perp_h}=\{0\}$,$\mathbf{C}_1^{\perp_h}\subset\mathbf{C}_2$,$\mathbf{C}_1\cap\mathbf{C}_2=\mathbf{C}$,$\mathbf{C}_1^{\perp_h}+\mathbf{C}_2^{\perp_h}=\mathbf{C}^{\perp_h}$。

**定理 1** 设 $\mathbf{F}_q$(或 $\mathbf{F}_{q^2}$)上 BCH 码 $\mathbf{C}$ 的定义集为 $T$。$T$ 的分解如**定义 1.2** 所述。则以 $\mathbf{C}^{\perp}$(或 $\mathbf{C}^{\perp_h}$)为纠缠辅助稳定子时,所需最优纠缠比特数 $c=|T_s|$(或 $c=|T_{ss}|$)。

证明:现仅证明 $\mathbf{C}$ 为 $\mathbf{F}_4$ 上 BCH 码的情况,至于 $\mathbf{C}$ 为 $\mathbf{F}_2$ 上 BCH 码的情况同理可证。

设以 $T_{sas}$ 和 $T_{ss}$ 为定义集的循环码分别为 $\mathbf{C}_1$ 和 $\mathbf{C}_2$,$\mathbf{C}_1$ 和 $\mathbf{C}_2$ 的校验矩阵分别为 $\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2$。由**引理 1.5** 可知 $\boldsymbol{H}_1\boldsymbol{H}_1^{+}=\{0\}$,$\boldsymbol{H}_1\boldsymbol{H}_2^{+}=\{0\}$,$\boldsymbol{H}_2\boldsymbol{H}_2^{+}=\{0\}$为满秩矩阵且其秩为$|T_{ss}|$。构造矩阵 $\boldsymbol{H}$ 如下,则 $\boldsymbol{H}$ 为 $\mathbf{C}$ 的校验矩阵且满足:

$$\boldsymbol{H}=\begin{pmatrix}\boldsymbol{H}_1\\ \boldsymbol{H}_2\end{pmatrix}\text{且}\quad \boldsymbol{H}\boldsymbol{H}^{+}=\begin{pmatrix}\boldsymbol{H}_1\\ \boldsymbol{H}_2\end{pmatrix}(\boldsymbol{H}_1^{+}\ \boldsymbol{H}_2^{+})=\begin{pmatrix}\mathbf{0} & \mathbf{0}\\ \mathbf{0} & \boldsymbol{H}_2\boldsymbol{H}_2^{+}\end{pmatrix}$$

从而有 $\boldsymbol{H}\boldsymbol{H}^{+}$ 的秩为 $|T_{ss}|$。根据文献[4]的推论 2,所需最优纠缠比特数 $c=|T_{ss}|$。

**定理 1** 将计算最优纠缠比特数 $c$ 转化为计算 $|T_s|$或者 $|T_{ss}|$。由**引理 1.2** 可知,当 BCH 码的设计距离 $\delta\leqslant\delta_{\max}$时,$|T_s|$或者 $|T_{ss}|$皆为零,故仅需要研究 $\delta>\delta_{\max}$时 $T$ 的分解。

## 2 本原狭义 BCH 码的定义集分解

由于二元码和四元码的内积不同,相应 BCH 码的定义集分解具有本质区别;而且二元码和四元码的 $\delta_{\max}$规律不同。为此,用 $\delta_m$ 和 $\delta_0$ 分别表示二元与四元时的 $\delta_{\max}$。

### 2.1 二元本原 BCH 码的定义集分解

本小节具体分析 $m\geqslant 8$,$n=2^m-1$,$\delta>\delta_{\max}=\delta_m$ 时二元狭义 BCH 码的定义集分解。因 $C_i=C_{2i}$,$T=T_{[1,2i]}=T_{[1,2i-1]}$。所以本节只需假定 $\delta$ 为奇数。

**情况 1** $n=2^{2t}-1$ 的二元 BCH 码的定义集分解

设 $m=2t$,则 $t\geqslant 4$,$\delta_m=2^t-1$,此时分圆陪集 $C_{\delta_m}$是对称的;故当 $k\geqslant 2$,$C_{k\delta_m}$ 均为对称的。下面考察区间 $I=[1,3\delta_m-2]$,并且记 $a=3\times 2^{t-1}-1$,$b=2\delta_m-1$,$a'=2^{t-1}-1$,$b'=2\delta_m+1=2^{t+1}-1$,$a''=2\delta_m-3$,$b''=2\delta_m+2^{t-1}+1$。仿照文献[8],易验证$(C_a,C_b)$,$(C_{a'},C_{b'})$和$(C_{a''},C_{b''})$均为非对称偶。且对 $x$,$y\in I\backslash\{\delta_m,2\delta_m,a,b,a',b',a'',b''\}$,可证明 $C_x$ 是非对称的,$C_x$ 和 $C_y$ 不构成非对称偶。故 $T_s$ 随 $\delta$ 变化而变化的规律 $R_1$ 如下:

1)当 $\delta_m+1\leqslant\delta\leqslant 2\delta_m-1$ 时,则 $T_s=C_{\delta_m}$;

2)当 $\delta=2\delta_m+1$ 时,则 $T_s=C_{\delta_m}\cup C_a\cup C_b$;

3)当 $2\delta_m+3\leqslant\delta\leqslant 5\cdot 2^{t-1}-1$,则 $T_s=C_{\delta_m}\cup C_a\cup C_b\cup C_{a'}\cup C_{b'}$;

4)当 $5\cdot 2^{t-1}+1\leqslant\delta\leqslant 3\delta_m$ 时:

$T_s=C_{\delta_m}\cup C_a\cup C_b\cup C_{a'}\cup C_{b'}\cup C_{a''}\cup C_{b''}$。

注 1:当 $\delta\geqslant 3\delta_m$ 时,$|T_s|\geqslant 8m$ 已比较大,此时讨论 $T_s$ 及 EAQECC 没有多大意义[3]。

**情况 2** $n=2^{2t+1}-1$ 的二元 BCH 码的定义集分解

设 $m=2t+1$,则 $t\geqslant 4$,$\delta_m=2^{t+1}-1$。考察区间 $I=[1,b''=q^{t+2}-9]$,并记 $a=2^t-1$,$b=\delta_m$,$a'=\delta_m-2=q^{t+1}-3$,$b'=\delta_m+q^t=q^{t+1}+q^t-1$,$a''=q^{t+1}+q^t+q^{t-1}-1$,$b''=q^{t+2}-7$。不难验证$(C_a,C_b)$,$(C_{a'},C_{b'})$以及$(C_{a''},C_{b''})$为非对称偶;且对 $x,y\in I\backslash\{a,b,a',b',a'',b''\}$,可以证明 $C_x$ 是非对称的,$C_x$ 和 $C_y$ 不构成非对称偶。故 $T_s$ 随 $\delta$ 变化而变化的规律 $R_2$ 如下:

1)当 $\delta_m+2\leqslant\delta\leqslant b'-2$ 时,$T_s=C_a\cup C_b$;

2)当 $3q^t+1\leqslant\delta\leqslant q^{t+2}-7$ 时,$T_s=C_a\cup C_b\cup C_{a'}\cup C_{b'}$;

### 2.2 四元本原 BCH 码的定义集分解

本小节分析 $m\geqslant 3$,$n=4^m-1$,$\delta>\delta_{\max}=\delta_0$ 时四元狭义 BCH 码的定义集分解。

**情况 3** $n=4^{2t}-1$ 的四元 BCH 码的定义集分解

设 $m\geqslant 2t$,则 $t\geqslant 2$,$\delta_0=2^{m+1}-3$。根据文献[9],若 $x,a,b\in[1,2^{m+2}-8]$,则 $C_x$ 是斜非对称的,且 $C_a$ 与 $C_b$ 构成斜非对称偶的$(a,b)$仅有如下几种情况:

$(a_1,b_1)=(3\times 2^{m-1}-1,\delta_0)$;$(a_2,b_2)=(2\times 2^{m-1}-1,\delta_0+1)$;

$(a_3,b_3)=(2^{m-1}-1,\delta_0+2)$;$(a_4,b_4)=(\delta_0-2,\delta_0+2^{m-1}+2)$;

$(a_5,b_5)=(\delta_0-3,\delta_0+2\times 2^{m-1}+2)$;$(a_6,b_6)=(\delta_0-4,\delta_0+3\times 2^{m-1}+2)$。

故 $T_{ss}$随 $\delta$ 变化而变化的规律 $R_3$ 如下:

1)当 $\delta=\delta_0+i(1\leqslant i\leqslant 2)$时:

$T_{ss}=\bigcup_{j=1}^{j=i}(C_{a_j}\cup C_{b_j})$;

2)当 $\delta_0+3\leqslant\delta\leqslant 2^{m+1}+2^{m-1}-1$ 时:

$T_{ss}=\bigcup_{j=1}^{j=3}(C_{a_j}\cup C_{b_j})$;

3)当 $2^{m+1}+2^{m-1}\leqslant\delta\leqslant 2^{m+1}+2^m-1$ 时:

$T_{ss}=\bigcup_{j=1}^{j=4}(C_{a_j}\cup C_{b_j})$;

4)当 $2^{m+1}+2^m\leqslant\delta\leqslant 2^{m+1}+3\times 2^{m-1}-1$ 时:

$T_{ss}=\bigcup_{j=1}^{j=5}(C_{a_j}\cup C_{b_j})$;

5)当 $2^{m+1}+3\times 2^{m-1}\leqslant\delta\leqslant 2^{m+2}-7$ 时:

$T_{ss}=\bigcup_{j=1}^{j=6}(C_{a_j}\cup C_{b_j})$。

**情况 4** $n=4^m-1=4^{2t+1}-1$ 的四元 BCH 码的

定义集分解

设 $m=2t+1$,则 $t\geqslant 1$,$\delta_0=2^m-1$,因 $C_{\delta_0}$ 是斜对称的;对任意正整数 $k\geqslant 2$,$C_{k\delta_0}$ 均为斜对称的。根据[9],若 $x,a,b\in[1,\ 2^{m+2}-15]$,$x,a,b\neq\delta_0,\ 2\delta_0,\ 3\delta_0$,则 $C_x$ 是斜非对称的,且 $C_a$ 与 $C_b$ 构成斜非对称偶的$(a,b)$仅有如下几种情况:

$(a,b)=(\delta_0-1,\ 2\delta_0+1)$;$(a',b')=(2\delta_0-1,\ 3\delta_0+1)$;$(a'',b'')=(\delta_0-2,\ 3\delta_0+2)$。

故 $T_{ss}$ 随 $\delta$ 变化而变化的规律 $R_4$ 如下:

1)当 $\delta_0+1\leqslant\delta\leqslant 2\delta_0$ 时,$T_{ss}=C_{\delta_0}$;

2)当 $\delta=2\delta_0+1$ 时,$T_{ss}=C_{\delta_0}\cup C_{2\delta_0}$;

3)当 $2\delta_0+2\leqslant\delta\leqslant 3\delta_0$ 时:

$T_{ss}=C_{\delta_0}\cup C_{2\delta_0}\cup C_a\cup C_b$;

4)当 $\delta=3\delta_0+1$ 时:

$T_{ss}=C_{\delta_0}\cup C_{2\delta_0}\cup C_a\cup C_b\cup C_{3\delta_0}$;

5)当 $\delta=3\delta_0+2$ 时:

$T_{ss}=C_{\delta_0}\cup C_{2\delta_0}\cup C_a\cup C_b\cup C_{3\delta_0}\cup C_{a'}\cup C_{b'}$。

**定理** 2　本原狭义二元 BCH 码的定义集分解由规律 $R_1$ 和 $R_2$ 确定,本原狭义四元 BCH 码的定义集分解由规律 $R_3$ 和 $R_4$ 确定。

## 3　应用

利用第 2 节的结果,当码长不太大时,可用给定设计距离的 BCH 码构造出距离 $d\geqslant\delta_{\max}+1$ 的 EAQECCs,这些 EAQECCs 是新的或超过已有文献中由 BCH 码构造的量子码。这里仅列出 $n=4^3-1$,由四元 BCH 码构造的纠缠辅助量子纠错码;类似的,可给出二元 BCH 码构造 EAQECCs。表 1 中的 EAQECC 是新的且优于已有文献中得到的同样码长的 EAQECC。以[[63,30,9;3]]为例,其明显优于文献[10]构造的[[63,21,9;6]],后者消耗 6 个纠缠比特对,才得到维数 21 的码;而前者只消耗 3 个纠缠比特对,却得到维数 30 的码。

**表** 1　$n=4^3-1$ **的** EAQECCs $[[n,k,d;c]]$

Tab. 1 EAQECCs $[[n,k,d;c]]$ for $n=4^3-1$

| BCH 码的设计距离 $\delta$ | $\lvert T_{ss}\rvert$ | $[[n,k,d;c]]$ |
|---|---|---|
| $\delta=8$ | 3 | [[63,30,9;3]] |
| $\delta=10$ | 3 | [[63,24,10;3]] |
| $\delta=11$ | 3 | [[63,18,11;3]] |
| $\delta=12$ | 3 | [[63,12,13;3]] |
| $\delta=14$ | 3 | [[63,16,14;3]] |
| $\delta=15$ | 6 | [[63,3,15;6]] |

## 4　结语

本文以分圆陪集理论和纠缠辅助理论为基础,引入 BCH 码的定义集分解概念,建立二元(四元)BCH 码的对偶码的正交分解与 BCH 码的定义集分解之间的联系,解决(除几个例外情况)了本原二元(四元)BCH 码的定义集分解,构造出一些参数优良的纠缠辅助量子纠错码。这些结果为进一步研究给定设计距离 $\delta$ 的 BCH 码的维数以及构造出距离 $d\geqslant\delta\geqslant\delta_{\max}+1$ 的一般码长的纠缠辅助量子纠错码奠定了基础。

**参考文献**(References):


[1] Gottesman D. Class of quantum error-correcting codes saturating the quantum hamming bound[J]. Phys rev A,1996,54: 1862-1868.

[2] Calderbank A R, Rains E M, Shor P W,et al. Quantum error correction via codes over GF(4)[J]. IEEE trans inform theory, 1998, 44: 1369-1387.

[3] Brun T, Devetak I, Hsieh M H. Correcting quantum errors with entanglement[J]. Science, 2006, 314: 436-439.

[4] Wilde M M, Brun T A. Optimal entanglement formulas for entanglement-assisted quantum coding[J]. Phys rev A, 2008,77: 064302.

[5] Huffman W C,Pless V. Fundamentals of error-correcting codes[M]. Cambridge: Cambridge university press, 2003.

[6] Steane A. Enlargement of calderbank-shor-steane codes[J]. IEEE trans inform theory, 1999,45:2492-2495.

[7] Aly S A, Klappenecker A, Sarvepalli P K. On quantum and classical BCH codes[J]. IEEE trans inform theory, 2007, 53(3): 1183-1188.

[8] Yang Liu, Youqian Feng, Ruihu Li. A Class of Imprimitive BCH codes and new quantum codes[J]. American journal of engineering and technology research, 2011, 11(12): 1792-1796.

[9] R Li, F Zuo, Y Liu,et al. Hermitian dual containing BCH codes and construction of new quantum codes [J]. Quantum inf and comp, 2013, 13(1):21-35.

[10] Hsieh M H, Devetak I, Brun T A. General entanglement-assisted quantum error-correcting codes[J]. Phys rev A, 2007, 76: 062313.


(编辑:徐敏)