一类特殊码长的非对称量子 BCH 码

马月娜[1],冯晓毅[2],刘 杨[1],郭冠敏[1]
(1. 空军工程大学基础部,陕西西安,710051; 2. 西北工业大学电子信息学院,陕西西安,710072)

摘 要: 非对称量子纠错码是针对量子通信中不同类型量子错误发生的概率而设计的有效编码方案. 纠错性能良好的量子码在量子通信的真实性和可靠性方面起着决定性的作用. 本文首先通过研究分圆陪集的性质确定出非本原狭义 BCH 码满足 Hermitian 对偶包含的条件;其次,利用推广的 CSS 构造法构造出一系列特殊码长的非对称量子 BCH 码;最后,给出了 m 分别为 3 和 5 的两类非对称量子 BCH 码维数,它们的 z-距离远大于已有文献中的结论,因而提高了非对称量子信道中对相位错误的纠错能力.

关键词: 非对称量子 BCH 码; 非本原 BCH 码; Hermitian 对偶包含条件; CSS 构造法
中图分类号: TN914.4 **文献标识码:** A **文章编号:** 0372-2112 (2019)11-2311-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.11.011

A Class of Special Code Length Asymmetric Quantum BCH Codes

MA Yue-na[1], FENG Xiao-yi[2], LIU Yang[1], GUO Guan-min[1]
(1. *Department of Basic Sciences, Air Force Engineering University, Xi'an, Shaanxi* 710051, *China*;
2. *School of Electronics and Information, Northwestern Polytechnical University, Xi'an, Shaanxi* 710072, *China*)

Abstract: Asymmetric quantum codes are an efficient coding scheme against different kinds of quantum errors in quantum communication, which occurs with different probability. The good quantum codes play a decisive role in ensuring the authenticity and reliability of quantum communication. In this paper, we first present Hermitian dual-containing conditions of the imprimitive narrow-sense BCH codes by a detailed analysis of cyclotomic cosets. Secondly, a series of asymmetric quantum BCH codes with special code length are constructed via the generalized CSS construction. Finally, dimensions of two types of asymmetric quantum BCH codes are determined for m as 3 and 5 respectively, whose z distances are much greater than the results in the literature. Hence, the error-correcting ability to the phase errors can be further improved.

Key words: asymmetric quantum code; imprimitive BCH code; Hermitian dual containing condition; CSS construction

1 引言

量子纠错过程是克服信道噪声在信息的编码和传输中所产生的不良影响重要方法. 由于传输信道的不同可能导致比特错误 σ_x、相位错误 σ_z 以及二者的混合错误 σ_y 这三种量子错误发生的可能性也不尽相同,而且相位错误发生的概率远大于比特错误. 基于量子错误发生的这一非对称特征,人们提出了一种新的量子码——非对称量子码. q-元非对称量子$[[n,k,d_z/d_x]]_q$码可以控制$\lfloor\frac{d_x-1}{2}\rfloor$个比特错误和$\lfloor\frac{d_z-1}{2}\rfloor$个相位错误. 与此同时,可以检测出 d_x-1 个比特错误和 d_z-1 个相位错误,因此 z-距离和 x-距离的大小决定了码的检错和纠错能力[1~3]. 1996 年,Steane[3] 在经典纠错码理论的基础上提出了量子信道的非对称性以及非对称量子纠错的概念;2007 年,Ioffe 和 Mezard[4] 明确了非对称量子信道的具体纠错方案;2009 年,Aly 和 Sarvepalli 等[5~8]将标准量子码的 CSS 构造法推广到非对称量子码,并构造出很多参数优良的非对称量子码;2011 年,CSS 构造法再次被加以推广并得到 CSS-like 构造法,利用该方法和嵌套的自正交线性码可构造出一系列新的非对称量子码[9]. 此后,人们便利用满足自正交或对偶

收稿日期:2019-04-15;修回日期:2019-07-18;责任编辑:马兰英
基金项目:国家自然科学基金面上项目(No. 11471011);国家自然科学基金青年项目(No. 11801564)

包含条件的经典码构造具有较好参数非对称量子码,见文献[10~14].近年来,研究人员集中围绕常循环码来研究非对称量子纠错码的构造[15~19].文献[20]利用本原 Euclidean 对偶包含 BCH 码来构造非对称量子码,并给出任意 $q\geq5$ 的码的参数.对于非本原的情形,文献[21,22]给出了利用 BCH 码构造的小码长非对称量子码的结论.本文将利用非本原 Hermitian 对偶包含 BCH 码来构造码长较大的非对称量子 BCH 码.

本文首先给出码长为 $n=\frac{q^{2m}-1}{q^2-1}$ 的非本原嵌套 BCH 码满足 Hermitian 对偶包含的条件,其次利用推广的 CSS 构造法和非本原狭义 BCH 码确定出非对称量子 BCH 码的参数,并使其 z-距离远大于文献[12]给出的非本原狭义 BCH 码的最大设计距离 $\delta_{\max}$,其中当 $m=2t+1$ 时 $\delta_{\max}=\lfloor\frac{q^m-1}{q^2-1}\rfloor$,当 $m=2t$ 时 $\delta_{\max}=\lfloor\frac{q^{m+1}-q^2+1}{q^2-1}\rfloor$.

2 预备知识

利用分圆陪集研究 BCH 码的对偶包含条件,本节首先介绍分圆陪集、BCH 码的有关概念,并介绍判定两个 BCH 码满足对偶包含条件的方法.更多关于分圆陪集和 BCH 码的知识,见文献[14,16,20].

定义 1 设 q 为素数幂,$n>1$ 为正整数且 $\gcd(n,q)=1$.若 x 为正整数且满足 $x<n$,x 模 n 的 q^2 分圆陪集为 $C_x=\{x,xq^2,x(q^2)^2,\cdots,x(q^2)^{k-1}\}(\mathrm{mod}n)$,其中 k 是使得 $(q^2)^kx\equiv x(\mathrm{mod}n)$ 成立的最小正整数.

定义 2 设 ξ 为有限域 F_{q^2} 扩域上的 n 次本原单位根,若 $T=\bigcup_{i=0}^{\delta-2}C_{b+i}=T_{[b,b+\delta-2]}$,以 T 为定义集合的循环码 C 叫做 F_{q^2} 上的设计距离为 δ 的 BCH 码.设 $n=\frac{q^{2m}-1}{a}$,如果 $a\neq1$,C 叫做 q^2-元非本原 BCH 码,否则叫做本原 BCH 码;如果 $b=1$,C 叫做狭义 BCH 码,否则叫做非狭义 BCH 码.

引理 1 若 $\gcd(n,q)=1$,F_{q^2} 上的循环码 C 的定义集合为 T,则 $C^{\perp h}\subseteq C$ 当且仅当 $T\cap T^{-q}=\Phi$,其中 $T^{-q}=\{-qt(\mathrm{mod}n)\mid t\in T\}$.

引理 2 设 q^2-元 BCH 码 B_1 和 B_2 的定义集合分别为 T_1 和 T_2,$B_1^{\perp h}\subseteq B_2$ 当且仅当 $T_2\subseteq T_1^{\perp h}$.

文献[9]将标准的 CSS 构造法推广到满足 Hermitian 内积、迹 Hermitian 内积和迹 Euclidean 内积条件下的非对称量子码的构造中,给出了 CSS-like(CSS-type)构造法,下述定理给出了利用 Hermitian 对偶包含 BCH 码构造非对称量子码的方法.

定理 1 若 F_{q^2} 上参数为 $[n,k_i,d_i]$ 的线性码 $C_i(i=1,2)$ 满足 $C_1^{\perp h}\subseteq C_2$,则存在参数为 $[[n,k_1+k_2-n,d_z/d_x]]_{q^2}$ 的非对称量子码,其中 $d_x=wt(C_1\backslash C_2^{\perp h})$,$d_z=wt(C_2\backslash C_1^{\perp h})$.

3 Hermitian 对偶包含 BCH 码的构造

在以往的研究中,人们利用 q 元或 q^2 元域上两个嵌套 BCH 码构造非对称量子码,所涉及的 BCH 码大多是本原码,至于非本原的情形仅有少数结论.鉴于此,本节讨论基于非本原 BCH 码的非对称量子 BCH 码的构造,即当码长 $n=\frac{q^{2m}-1}{q^2-1}$(其中 q 为任意素数或素数幂,$m\in Z^+$)时,利用满足 Hermitian 对偶包含条件的两个非本原嵌套 BCH 码构造非对称量子码,使所得到的 $d_z>\delta_{\max}$.

3.1 BCH 码的对偶包含条件

利用定理 1 构造非对称量子 BCH 码,首先需要确定出两个满足对偶包含关系的嵌套 BCH 码的参数.如果码长为 n 的 BCH 码的定义集合为 $T=\bigcup_{i=1}^{\delta_{\max}-1}C_i$,令 $u=\min\{x\mid x\in T^{-q}\}$,$v=\max\{y\mid y\in T^{-q}\}$,与文献[14,20]的证明类似,定义集合中的元素与最大设计距离存在如下关系:

引理 3 设 F_{q^2} 上码长为 n 的狭义 BCH 码 B 的定义集合为 $T=\bigcup_{i=1}^{r}C_i$,其对偶码 $B^{\perp h}$ 的定义集合为 $T^{\perp h}=Z_n\backslash T^{-q}$,则 B 和 $B^{\perp h}$ 的最大设计距离分别为 $\delta(B)=r+1$ 和 $\delta(B^{\perp h})=\max\{u,n-v\}$.

证明 由条件可知 BCH 码 B 的定义集合为 $T=\bigcup_{i=1}^{r}C_i=T_{[1,r]}$,因此 B 的最大设计距离为 $r+1$,即 $\delta(B)=r+1$.又因为:

$$\begin{aligned}T^{\perp h}&=Z_n\backslash T^{-q}=\{0,1,2,\cdots,n-1\}-\{-qx\mid x\in T\}\\&=\{0,1,2,\cdots,n-1\}-\{u,u+s,\cdots,v-t,v\}\\&\supseteq\{0,1,2,\cdots,u-1,\cdots,v+1,\cdots,n-1\}\end{aligned}$$

由此可知 $T^{\perp h}$ 至少包含 u 或者 $n-v-1$ 个连续整数,因此 $\delta(B^{\perp h})=\max\{u,n-v\}$.

下面定理 2 给出 BCH 码满足 Hermitian 对偶包含的条件.

定理 2 设 $n=\frac{q^{2m}-1}{a}$(其中 q 为任意素数或素数幂、$m\in Z^+$).当 $1\leq j\leq\lfloor\frac{m-1}{2}\rfloor$,$k=m-j$ 时,

(1) 若 $\delta_1=\sum_{i=1}^{j}q^{2(j-i)+1}$,$\delta_1<\delta_2\leq\sum_{i=1}^{k}q^{2(k-i)}$,则存在狭义 BCH 码 B 满足 $B_1^{\perp h}(n,\delta_1)\subseteq B_2(n,\delta_2)$.

(2) 若 $\delta_1=\sum_{i=1}^{j}q^{2(j-i)}$,$\delta_1<\delta_2\leq\sum_{i=1}^{k}q^{2(k-i)+1}$,则存

在狭义 BCH 码 B 满足 $B_1^{\perp_h}(n,\delta_1)\subseteq B_2(n,\delta_2)$.

证明　以(1)为例,令 $m=2t+1(t\geq 1)$,$1\leq j\leq t$. 当 $1\leq j\leq\lfloor\frac{m-1}{2}\rfloor=t$ 时,$\delta_1=\sum_{i=1}^{j}q^{2(j-i)}$,因此狭义 BCH 码 $B_1(n,\delta_1)$ 的定义集合为 $T_1=\bigcup_{r=1}^{\delta_1-1}C_r=\bigcup_{r=1}^{\sum_{i=1}^{j}q^{2(j-i)}+1}C_r$.

如果 $\delta_1<\delta_2\leq\min\{n-qx_i\mid x_i\in T_1\}=\sum_{i=1}^{k}q^{2(k-i)}$,其中 $k=m-j$,则 $B_2(n,\delta_2)$ 的定义集合为:

$$T_2=\bigcup_{r=1}^{\delta_2-1}C_t=\bigcup_{r=1}^{\sum_{i=1}^{k}q^{2(k-i)}}C_r.$$

令 $T_1^{-q}=\{n-qx_i\mid x_i\in T_1\}$,由于 $B_1^{\perp_h}(n,\delta_1)$ 的定义集合.

$$T_1^{\perp_h}=Z_n\backslash T_1^{-q}=\{0,1,2,\cdots,n-1\}-\{n-qx_i\mid x_i\in T_1\}$$

如果 $T_2=C_1\cup C_2\cup\cdots\cup C_{\delta_2-1}$,由引理 3 可知,$\forall j\in T_2$,有 $j\notin T_1^{-q}$,即就是 $j\in Z_n\backslash T_1^{-q}$,因此可以推出 $T_2\subseteq T_1^{\perp_h}$,于是根据引理 2 可知,$B_1^{\perp_h}(n,\delta_1)\subseteq B_2(n,\delta_2)$.

同理可证(2)成立.

3.2　计算两类 BCH 码的参数

定理 2 提供了满足 Hermitian 对偶包含条件的两个嵌套 BCH 码的最大设计距离,众所周知,非对称量子码的构造问题中,一个很大的障碍就是维数的计算,因此本小节将提供 $m=3$ 和 $m=5$ 的两类特殊码长的 BCH 码的维数,并计算出码的参数.

定理 3　设 $m=3,n=\frac{q^{2m}-1}{q^2-1}=q^4+q^2+1$,存在参数为 $[n,n-3q,q+1]_{q^2}$,$[n,n-3q^2,q^2+1]_{q^2}$ 的非本原狭义 BCH 码 B_1 和 B_2,满足 $B_1^{\perp_h}\subseteq B_2$.

定理 4　设 $m=5,n=\frac{q^{2m}-1}{q^2-1}=\sum_{l=0}^{4}q^{2l}$.

(1) 存在参数分别为 $[n,n-5q,\delta_1]_{q^2}$,$[n,n-5(\delta_2-2(\sum_{i=0}^{2}q^{2i})),\delta_2]_{q^2}$ 的非本原狭义 BCH 码 B_1 和 B_2,满足 $B_1^{\perp_h}\subseteq B_2$,其中 $\delta_1=q+1,\delta_2=\sum_{i=0}^{2}q^{2i}$.

(2) 存在参数分别为 $[n,n-5q^2,\delta_1]_{q^2}$,$[n,n-5(\delta_2-\sum_{i=1}^{3}q^i),\delta_2]_{q^2}$ 的非本原狭义 BCH 码 B_1 和 B_2,满足 $B_1^{\perp_h}\subseteq B_2$,其中 $\delta_1=q^2+2,\delta_2=\sum_{i=0}^{2}q^{2i+1}$.

(3) 存在参数分别为 $[n,n-5q^3,\delta_1]_{q^2}$,$[n,n-5(\delta_2-q^2-2),\delta_2]_{q^2}$ 的非本原狭义 BCH 码 B_1 和 B_2,满足 $B_1^{\perp_h}\subseteq B_2$,其中 $\delta_1=q^3+q+1,\delta_2=\sum_{i=0}^{2}q^{2i}$.

4　非对称量子 BCH 码的构造

CSS 构造法将满足自正交或对偶包含关系的经典码与量子码联系在一起,本小节利用推广的 CSS 构造法和上述 BCH 码构造出非对称量子 BCH 码. 令设计距离为 δ 的 BCH 码的定义集合记为 $T(\delta)=\bigcup_{i=1}^{\delta-1}C_i$,$T(\delta)$ 的阶记为 $|T(\delta)|$.

定理 5　设 $n=\frac{q^{2m}-1}{q^2-1}$. 当 $1\leq j\leq\lfloor\frac{m-1}{2}\rfloor$,$k=m-j$ 时,

(1) 若 $\delta_1=\sum_{i=1}^{j}q^{2(j-i)+1}$,$\delta_1<\delta_2\leq\sum_{i=1}^{k}q^{2(k-i)}$,存在参数为 $[[n,n-|T(\delta_1)|-|T(\delta_2)|,d_z\geq\delta_2/d_x\geq\delta_2]]_{q^2}$ 的非对称量子 BCH 码.

(2) 若 $\delta_1=\sum_{i=1}^{j}q^{2(j-i)}$,$\delta_1<\delta_2\leq\sum_{i=1}^{k}q^{2(k-i)+1}$,存在参数为 $[[n,n-|T(\delta_1)|-|T(\delta_2)|,d_z\geq\delta_2/d_x\geq\delta_2]]_{q^2}$ 的非对称量子 BCH 码.

证明　以(1)为例,设 $n=\frac{q^{2m}-1}{q^2-1},m\in Z^+$.

码长为 u 的狭义 BCH 码 B_1,令 $T(\delta_1)$ 为 B_1 的定义集合,$|T(\delta_1)|$ 为集合 $T(\delta_1)$ 的阶. 当 $1\leq j\leq\lfloor\frac{m-1}{2}\rfloor$,$\delta_1=\sum_{i=1}^{j}q^{2(j-i)+1}$ 时,存在参数为 $[n,n-|T(\delta_1)|,\sum_{i=1}^{j}q^{2(j-i)+1}]$ 的狭义 BCH 码. 对于另一个狭义 BCH 码 B_2,由定理 2 可知,当 $\delta_1<\delta_2\leq\sum_{i=1}^{k}q^{2(k-i)}$ 时,有 $B_1^{\perp_h}(n,\delta_1)\subseteq B_2(n,\delta_2)$,根据定理 1 给出的 CSS 构造法和上述满足 Hermitian 对偶包含关系的 BCH 码 B_1 和 B_2,可构造出参数为 $[[n,n-|T(\delta_1)|-|T(\delta_2)|,d_z\geq\delta_2/d_x\geq\delta_2]]_{q^2}$ 的非对称量子码,因此(2)得证.

定理 5 给出了两类非对称量子 BCH 码的参数,需要说明的是,虽然定理中没有提供任意的 m 所对应量子 BCH 码的维数,但是对于 m 分别为 3 和 5 这两种情况,本节将给出量子 BCH 码维数. 根据定理 3 和定理 4,构造出两类特殊码长的非对称量子 BCH 码,构造结果见下列两个推论.

推论 1　设 $m=3,n=\frac{q^{2m}-1}{q^2-1}=q^4+q^2+1$,存在参数为 $[[n,n-3(\delta_1+\delta_2-1),d_z\geq\delta_2/d_x\geq\delta_1]]_{q^2}$ 的非对称量子 BCH 码,其中 $\delta_1=q+1,\delta_2=q^2+1$.

推论 2　设 $m=5,n=\frac{q^{2m}-1}{q^2-1}=\sum_{l=0}^{4}q^{2l}$.

(1) 当 $\delta_1=q+1,\delta_2=\sum_{i=0}^{2}q^{2i}$ 时,存在参数为 $[[n,n-5(\delta_2-2(\sum_{i=0}^{2}q^{2i})+q),d_z\geq\delta_2/d_x\geq\delta_1]]_{q^2}$

的非对称量子 BCH 码.

(2) 当 $\delta_1 = q^2 + 2, \delta_2 = \sum_{i=0}^{2} q^{2i+1}$ 时,存在参数为 $[[n, n-5(\delta_2 - \sum_{i=1}^{3} q^i + q^2), d_z \geq \delta_2/d_x \geq \delta_1]]_{q^2}$ 的非对称量子 BCH 码.

(3) 当 $\delta_1 = q^3 + q + 1, \delta_2 = \sum_{i=0}^{2} q^{2i}$ 时,存在参数为 $[[n, n-5(\delta_2 + q^3 - q^2 - 2), d_z \geq \delta_2/d_x \geq \delta_1]]_{q^2}$ 的非对称量子 BCH 码.

5 参数分析

本节对定理 5 中一部分非对称量子 BCH 码 z - 距离的最大下界与文献[12]中的 $\delta_{\max}$ 进行比较,给出当 $q=3,4,5$, m 分别取 4,5,6 时 d_x 和 $\delta_{\max}$ 的值,说明我们得到的 z - 距离远大于 $\delta_{\max}$;其次以 $q=4, m=3$ 为例,给出了利用两个嵌套 BCH 码构造出的非对称量子 BCH 码的参数;最后列出推论 1 以及推论 2 中,由维数计算方法得到的一部分码的参数,并且比较了 $q \geq 7$ 的三类在 Hermitian 对偶包含条件和 Euclidean 对偶包含条件下的一些非对称量子 BCH 码的参数. 本节将非对称量子 BCH 码的参数记为 $[[n, k, d_z/d_x]]_{q^2}$.

表 1 d_z 的最大下界与 $\delta_{\max}$ 的比较

q	m	d_z	$\delta_{\max}$
3	4	91	30
	5	820	91
	6	7381	273
4	4	273	68
	5	4369	273
	6	69905	1092
5	4	651	130
	5	16276	651
	6	406901	3255

表 1 给出了 m 分别为 4,5,6 时,我们构造出的非对称量子 BCH 码的 z-距离的最大下界和文献[12]中相应码长的 $\delta_{\max}$ 进行比较,可以看出我们的 z-距离远大于 $\delta_{\max}$.

表 2 给出了当 $q=4, m=3$ 时,由非本原狭义嵌套 BCH 码对构造的非对称量子 BCH 码,可以看出表中的 z-距离和 x-距离的比值大于 1,从而说明我们构造的非对称量子 BCH 码对相位错误具有更好的纠错能力.

表 3 给出了推论 1 和推论 2 中,由维数计算公式得到的非对称量子 BCH 码的参数. 需要说明的是,这里仅以 $q=3,4,5$ 为例进行说明,实际上推论 1 和推论 2 中提供的维数与距离之间的计算公式适用于 q 取任意素数或素数幂.

表 4 比较了 Hermitian 对偶包含条件和 Euclidean 对偶包含条件这两种情形下构造出的非对称量子 BCH 码的参数,分别记 Hermitian 情形下的量子 BCH 码为 $Q=[n, k, d_z/d_x]_{q^2}$, Euclidean 情形下的量子 BCH 码为 $Q'=[n, k', d_z'/d_x']_q$. 从码的参数可以看出,在同一域中,当码长相同时,非对称量子 BCH 码 Q 的纠错能力优于 Q'. 例如,当码长为 2451 时,非对称量子 BCH 码 $Q=[[2451, 1533, d_z \geq 350/d_x \geq 7]]_{49}$, $Q'=[[2451, 2289, d_z \geq 50/d_x \geq 7]]_{49}$. 尽管这两个码控制比特错误的能力同为 3,但是 Q' 最多可控制 24 个相位错误,而 Q 控制相位错误的能力可达到 174,由此可见 Q 对相位错误 σ_z 的纠错能力远大于 Q'.

表 2 由 $n=\frac{4^6-1}{15}$ 的 BCH 码构造的非对称量子 BCH 码的参数

$[[n, k, d_z/d_x]]_{q2}$	d_z/d_x
$[[273, 213, d_z \geq 17/d_x \geq 4]]_{16}$	4.25
$[[273, 216, d_z \geq 16/d_x \geq 4]]_{16}$	4
$[[273, 219, d_z \geq 15/d_x \geq 4]]_{16}$	3.75
$[[273, 222, d_z \geq 14/d_x \geq 4]]_{16}$	3.5
$[[273, 225, d_z \geq 13/d_x \geq 4]]_{16}$	3.25
$[[273, 228, d_z \geq 12/d_x \geq 4]]_{16}$	3
$[[273, 231, d_z \geq 11/d_x \geq 4]]_{16}$	2.75
$[[273, 234, d_z \geq 10/d_x \geq 4]]_{16}$	2.5
$[[273, 237, d_z \geq 9/d_x \geq 4]]_{16}$	2.25
$[[273, 240, d_z \geq 8/d_x \geq 4]]_{16}$	2
$[[273, 243, d_z \geq 7/d_x \geq 4]]_{16}$	1.75
$[[273, 246, d_z \geq 6/d_x \geq 4]]_{16}$	1.5
$[[273, 249, d_z \geq 5/d_x \geq 4]]_{16}$	1.25

表 3 新的非对称量子 BCH 码的参数

m	$[[n, k, d_z/d_x]]_{q2}$
3	$[[91, 55, d_z \geq 10/d_x \geq 3]]_9$
5	$[[7381, 6846, d_z \geq 91/d_x \geq 30]]_9$ $[[7381, 6166, d_z \geq 273/d_x \geq 10]]_9$ $[[7381, 4176, d_z \geq 820/d_x \geq 3]]_9$
3	$[[273, 213, d_z \geq 17/d_x \geq 4]]_{16}$
5	$[[69905, 68310, d_z \geq 273/d_x \geq 68]]_{16}$ $[[69905, 64785, d_z \geq 1092/d_x \geq 17]]_{16}$ $[[69905, 50770, d_z \geq 4369/d_x \geq 4]]_{16}$
3	$[[651, 561, d_z \geq 26/d_x \geq 5]]_{25}$
5	$[[406901, 403156, d_z \geq 651/d_x \geq 130]]_{25}$ $[[406901, 391226, d_z \geq 3255/d_x \geq 26]]_{25}$ $[[406901, 332006, d_z \geq 16276/d_x \geq 5]]_{25}$

表 4　两种对偶包含条件下的非对称量子 BCH 码参数比较

q	m	$n=\frac{q^{2m}-1}{q^2-1}$	$Q=[[n,k,d_z/d_x]]_{q^2}$	q	m	$n=\frac{q^m-1}{q-1}$	$Q'=[[n,k',d_z'/d_x']]_q$
7	3	2451	$[[n,1533,d_z\geq350/d_x\geq7]]_{49}$	49	3	2451	$[[n,2289,d_z\geq50/d_x\geq7]]_{49}$
	4	120100	$[[n,66124,d_z\geq17157/d_x\geq7]]_{49}$		4	120100	$[[n,110572,d_z\geq2451/d_x\geq7]]_{49}$
9	3	6643	$[[n,4651,d_z\geq738/d_x\geq9]]_{81}$	81	3	6643	$[[n,6376,d_z\geq82/d_x\geq9]]_{81}$
	4	538084	$[[n,338688,d_z\geq59787/d_x\geq9]]_{81}$		4	538084	$[[n,511936,d_z\geq6643/d_x\geq9]]_{81}$
11	3	14763	$[[n,11073,d_z\geq1342/d_x\geq11]]_{121}$	121	3	14763	$[[n,14370,d_z\geq122/d_x\geq11]]_{121}$

6　结论

本文利用 q^2 元域上满足对偶包含关系的非本原狭义 BCH 码构造码长为 $n=\frac{q^{2m}-1}{q^2-1}$ 非对称量子 $[[n,k,d_z/d_x]]_{q^2}$ 码. 首先,利分圆陪集刻划了两个嵌套的 BCH 码满足 Hermitian 对偶包含的条件;其次,根据推广的 CSS 构造法和这些嵌套 BCH 码计算出非对称量子 BCH 码参数,并给出了 m 分别为 3 和 5 的两类非对称量子 BCH 码的维数;最后,将所构造出的一部分结果和已有文献中的结论进行比较,通过对参数的分析可以看出,我们构造出的一部分非对称量子 BCH 码的 z-距离远大于 $\delta_{\max}$,从而对相位错误具有更好的纠错能力.

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] Calderbank A R, Rains E M, Shor P W, Sloane N J A. Quantum error-correction Via codes over GF(4)[J]. IEEE Transactions on Information Theory, 1998, 44(4): 1369 – 1387.

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

[4] Ioffe L, Mezard M M. Asymmetric quantum error-correcting codes[J]. Physical Review A,2007,75(3):032345(1 – 4).

[5] Aly S A. Asymmetric quantum BCH codes[A]. IEEE International Conference on Computer Engineering and Systems (ICCES'08)[C]. Cairo, Egypt: IEEE Computer Society,2008. 157 – 162.

[6] Aly S A, Ashikhmin A. Nonbinary quantum cyclic and subsystem codes over asymmetrically-decohered quantum channels[A]. IEEE Information Theory Workshop 2010 (ITW 2010)[C]. Cairo, Egypt: IEEE Computer Society, 2010. 5503199(1 – 5).

[7] Aly S A. Quantum error control codes[D]. College Station, TX, : Department of Computer Science and Engineering, Texas A & M Univercity, 2008.

[8] Sarvepalli P K, Klappenecker A, Rotteler M. Asymmetric quantum codes: constructions, bounds and performance [J]. Proceedings of the Royal Society A-Mathematical Physical and Engineering Science, 2009, 465(2105): 1645 – 1672.

[9] Ezerman M F, Ling S, Pasechnik D V. CSS-Like constructions of asymmetric quantum codes[J]. IEEE Transactions on Information Theory, 2013, 59(10): 6732 – 6754.

[10] Wang L, Feng K Q, Ling S, Xing C. Asymmetric quantum codes: characterization and constructions[J]. IEEE Transactions on Information Theory, 2010, 56(6): 2938 – 2945.

[11] Ezerman M F, Ling S, Sole P. Additive asymmetric quantum codes[J]. IEEE Transactions on Information Theory, 2011, 57(8): 5536 – 5550.

[12] 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.

[13] La Guardia G G. On the construction of asymmetric quantum codes[J]. International Journal of Theoretical Physics, 2014, 53(7): 2312 – 2322.

[14] Li R H, Xu G, Guo L B. On two problems of asymmetric quantum codes[J]. International Journal of Modern Physics letter B, 2014, 28(6): 1450017 – 1450031.

[15] Chen J Z, Li J P, Huang Y Y. Some families of asymmetric quantum codes and quantum convolutional codes from constacyclic codes[J]. Linear Algebra and its Applications, 2015, 475: 186 – 199.

[16] Xu G, Li R H, Guo L B, Lu L D. New optimal asymmetric quantum codes constructed from constacyclic codes [J]. International Journal of Modern Physics B, 2017, 31(5): 1750030(1 – 14).

[17] Huang Y Y, Chen J Z, Feng C H. Some families of asymmetric quantum mds codes constructed from constacyclic codes[J]. International Journal of Theoretical Physics, 2018, 57(2): 453 – 464.

[18] Chen X J, Zhu S X, Kai X S. Two classes of new optimal

asymmetric quantum codes[J]. International Journal of Theoretical Physics,2018,57(6):1829 – 1838.
[19] Chen J Z,Chen Y Q,Huang Y Y,Feng C H. New optimal asymmetric quantum codes and quantum convolutional codes derived from constacyclic codes[J]. Quantum Information Processing,2019,18(2):725 – 742.
[20] Ma Y N,Feng X Y,Xu G. New asymmetric quantum codes over F_q[J]. Quantum Information Processing,2016,15(7):2759 – 2769.
[21] Chen J Z,Li J P,Huang Y Y. Asymmetric quantum codes and quantum convolutional codes derived from nonprimitive non-narrow-sense BCH codes[J]. IEICS Transaction on Fundamentals of Electronics Communications and Computer Sciences,2015,E98A(5):1130 – 1135.
[22] Li R H,Xu G,Fu Q. Asymmetric quantum codes of large z-distance constructed from a class of quaternary imprimitive BCH codes[A]. 5th International Conference on Instrumentation and Measurement,Computer,Communication,and Control (IMCCC 2015)[C]. Qinhuangdao,China,2015. 545 – 549.

作者简介

马月娜 女,1977 年生于陕西西安,空军工程大学副教授,硕士生导师. 主要研究方向为纠错码的性能与构造,纠错码在图像与视频处理中的应用.
E-mail:mayuena2013@163.com

冯晓毅 女,1969 年生于陕西蓝田,西北工业大学教授,博士生导师,电子信息学院副院长. 主要研究方向为图像处理,计算机视觉,情感识别,雷达成像,嵌入式系统设计与应用.
E-mail:fengxiao@nwpu.edu.cn