码长为 $3(q^2-1)$ 的对偶包含 BCH 码及量子码的构造

马月娜[1,2]，梁放驰[2]，郭罗斌[2]，李中华[2]
(1.西北工业大学电子信息学院，西安，710072 2.空军工程大学理学院，西安，710051)

摘要　利用分圆陪集刻划 q^2-元 BCH 码包含其 Hermitian 对偶码的条件，分别在 $q=3l+1$ 和 $q=3l+2$ 情况下，改进了码长 $n=3(q^2-1)$ 的非本原 Hermitian 对偶包含 BCH 码的最大设计距离的下界，确定出当 $2\leqslant\delta\leqslant\delta_{new}$ 时，对偶包含 BCH 码的参数，并构造出量子 BCH 码，结论证明：利用该方法构造出的量子 BCH 码的参数优于已有文献。

关键词　分圆陪集；BCH 码；Hermitian 对偶包含码；量子 BCH 码
DOI　10.3969/j.issn.1009-3516.2015.02.018
中图分类号　O157.4　　**文献标志码**　A　　**文章编号**　1009-3516(2015)02-0082-04

Dual Containing BCH Codes of Length $n=3(q^2-1)$ and Construction of Quantum Codes

MA Yue-na[1,2], LIANG Fang-chi[2], GUO Luo-bin[2], LI Zhong-hua[2]
(1.School of Electronics and Information, Northwest Polytechnical University, Xi′an 710072, China;
2.Science College, Air Force Engineering University, Xi′an 710051, China)

Abstract: Let $q=3l+1$ and $q=3l+2$ be prime powers. The maximal designed distances of imprimitive Hermitian dual containing q^2-ary narrow-sense (NS) and non-narrow-sense (NNS) BCH codes of length $n=3(q^2-1)$ are determined, and a series of NS and NNS BCH codes are constructed and their parameters are computed. Consequently, two families of q-ary quantum BCH codes are derived from these BCH codes. Some of these quantum BCH codes constructed from NNS BCH codes have better parameters than those quantum BCH codes available in the literature.

Key words: cyclotomic coset; BCH code; hermitian dual containing code; quantum BCH code

量子纠错码是量子计算机和量子通信系统得以实现的重要保证。人们广泛研究的量子纠错码可以由满足对偶包含关系(或自正交)的经典码构造[1-4]。La Guardia 等在文献[5～6]中，发现了性能优越的非狭义 BCH 码满足对偶包含条件，并用非狭义对偶包含 BCH 码构造出一些参数很好的量子 BCH 码，这些量子 BCH 码的参数优于前人用狭义对偶包含 BCH 码构造的参数。

收稿日期：2013-12-13
基金项目：国家自然科学基金资助项目(11471011)
作者简介：马月娜(1977－)，女，陕西西安人，博士生，主要从事代数编码及密码研究.E-mail: mayuena2013@163.com

引用格式：*马月娜，梁放驰，郭罗斌，等. 码长为 $3(q^2-1)$ 的对偶包含 BCH 码及量子码的构造[J]. 空军工程大学学报：自然科学版，2015，16(2)：82-85. MA Yuena LIANG Fangchi, GUO Luobin, et al. Dual Containing BCH Codes of Length $n=3(q^2-1)$ and Construction of Quantum Codes[J]. Journal of Air Force Engineering University: Natural Science Edition, 2015, 16(2): 82-85.*

1　预备知识

分圆陪集和循环码之间有着密切的联系,本节给出分圆陪集和 BCH 码的一些基本概念和相关结论,见文献[6～10]

定义 1.1　设 q 为素数的幂,$n>1$ 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 $(q^2)^k x\equiv x(\mathrm{mod}\ n)$ 的最小正整数[9]。

定义 1.2　n,q,C_x 按**定义 1.1** 所述。若 $n-qx\in C_x$,称 C_x 为斜对称的;否则称其为斜非对称的。斜非对称的模 n 的 q^2-分圆陪集 C_x 和 $C_{-qx}=C_{n-qx}$ 成对出现,叫做模 n 的 q^2-斜非对称偶(简称斜非对称偶),记为 (C_x,C_{-qx})。

定义 1.3　设 F_{q^2} 为 q^2 元域,ξ 为 F_{q^2} 扩域上的 n 次本原单位根,若 $T=C_b\cup C_{b+1}\cup\cdots\cup C_{b+\delta-2}=T_{[b,b+\delta-2]}$,以 T 为定义集合的、码长为 n 的循环码 C 叫做 F_{q^2} 上的设计距离为 δ 的 BCH 码。当 $n=q^{2m}-1$ 时 C 叫做 q^2-元本原 BCH 码,否则叫做非本原 BCH 码;如果 $b=1$,C 叫做狭义 BCH 码,否则叫做非狭义 BCH 码。

q^2- 元本原 BCH 码包含其 Hermitian 对偶码的充要条件,也就是最大设计距离条件,因此可以通过对分圆陪集特征的刻划,从而简化了对偶包含充要条件的描述,见如下引理:

引理 1.1　若 $\gcd(q,n)=1$,F_{q^2} 上 BCH 码 C 的定义集合为 T,则 $C^{\perp_h}\subseteq C$ 当且仅当 T 中每个 C_i 为斜非对称的,且 C_i 和 C_j 不构成斜非对称偶,其中 $0\leqslant i,j\leqslant\delta-2$。

q^2-分圆陪集的斜对称性和斜非对称偶的判定由下述**定理 1.1** 完成,见文献[11～12]。

定理 1.1[11-12]　$\gcd(q,n)=1$,$\mathrm{ord}_n(q^2)=m$,$0\leqslant x,y,z\leqslant n-1$。

1) C_x 是斜对称分圆陪集当且仅当存在 $t\leqslant\left\lfloor\frac{m}{2}\right\rfloor$ 使得 $x\equiv-xq^{2t+1}(\mathrm{mod}x)$。

2) 若 $C_y\neq C_z$,(C_y,C_z) 形成斜非对称偶当且仅当存在 $t\leqslant\left\lfloor\frac{m}{2}\right\rfloor$ 使得 $y\equiv-zq^{2t+1}(\mathrm{mod}\ n)$ 或 $z\equiv-yq^{2t+1}(\mathrm{mod}\ n)$。

定理 1.2[6] 设 $\mathrm{ord}_n(q^2)=m$,$[m\quad\mathrm{even}]=m(\mathrm{mod}2)$,若 $2\leqslant\delta\leqslant\delta_{\max}$,则 $\mathrm{BCH}(n,q^2;\delta)^{\perp_h}\subseteq\mathrm{BCH}(n,q^2;\delta)$,其中 $\delta_{\max}=\left\lfloor\frac{n}{q^{2m-1}}(q^{m+[m\quad\mathrm{even}]}-1-(q^2-2)[m\quad\mathrm{even}])\right\rfloor$。

文献[3～10]给出了 q 元量子码的构造方法,利用 F_{q^2} 上满足 Hermitian 对偶包含(或自正交)条件的经典码,可构造出 q 元量子码。

定理 1.3[3,10]　若 C 为 F_{q^2} 上的 $[n,k]$ 线性码,并且 $C^{\perp_h}\subseteq C$,则在 F_{q^2} 上存在 $[[n,2k-n,d]]_q$ 量子码,其中 $d=\min\{wt(v);v\in C\backslash C^{\perp_h}\}$。

说明:为了叙述方便,将集合 $\{1,2,\cdots,n-1\}$ 记为区间 $[1,n-1]$,它的子集 $\{e,e+1,\cdots,f\}$ 记为 $[e,f]$。

2　Hermitian 对偶包含 BCH 码的构造

本节通过具体分析码长为 $n=3(q^2-1)$ 的非本原 BCH 码的定义集合,分别讨论当 $q=3l+1$ 和 $q=3l+2$ 时,Hermitian 对偶包含 BCH 码的最大设计距离的下界 δ_{new},从而构造出当 $2\leqslant\delta\leqslant\delta_{\mathrm{new}}$ 时,狭义与非狭义对偶包含 BCH 码的参数。

2.1　Hermitian 对偶包含 BCH 码的最大设计距离

2.1.1　狭义 BCH 码

设码长 $n=3(q^2-1)$,由**定理 1.2** 可知,非本原 Hermitian 对偶包含狭义 BCH 码的最大设计距离 $\delta_{\max}=\frac{3(q-1)}{(q^2-q+1)}$。

定理 2.1　设码长 $n=3(q^2-1)$,

1)当 $q=3l+1$ 时,Hermitian 对偶包含狭义 BCH 码的最大设计距离的下界 $\delta_{\mathrm{new}}=2q-1$,则 $2\leqslant\delta\leqslant\delta_{\mathrm{new}}$ 时狭义 BCH 码包含其 Hermitian 对偶码。

2)当 $q=3l+2$ 时,Hermitian 对偶包含狭义 BCH 码的最大设计距离的下界 $\delta_{\mathrm{new}}=q-1$,则 $2\leqslant\delta\leqslant\delta_{\mathrm{new}}$ 时狭义 BCH 码包含其 Hermitian 对偶码。

证明　1)在 $q=3l+1$ 的情况下,要证明 $2\leqslant\delta\leqslant\delta_{\mathrm{new}}=2q-1$ 时狭义 BCH 码包含 Hermitian 对偶码,由**引理 1.1** 可知,即就是要证明 $\forall x,y,z\in[1,2q-2]$ 时,C_x 为斜非对称的且 (C_y,C_z) 不构成斜非对称偶。

I.首先,证明当 $x\in[1,2q-2]$ 时 C_x 为斜非对称的。根据**定理 1.1**,只需证明 $x(q^{2t+1}+1)\neq 0(\mathrm{mod}n)$,$m=0,1$。

当 $t=0$ 时,$1<x(q+1)\leqslant 2(q-1)(q+1)=2(q^2-1)<n$,所以 $x(q+1)\neq 0(\mathrm{mod}\ n)$。

当 $t=1$ 时,$1<x(q^3+1)\leqslant 2(q-1)(q^3+1)=3(q^2-1)(q^2-q+1)-(q-1)(q^3+1)$,

所以 $x(q^3+1)\neq 0(\mathrm{mod}\ n)$。因此,$x\in[1,2q-2]$ 时 C_x 为斜非对称的。

II.其次,假设 $x<y$,证明 $\forall x,y\in[1,\delta_{new}-1]=[1,2q-2]$ 时,(C_x,C_y) 不构成斜非对称偶。

当 $t=0$ 时,$1<x+yq<y(q+1)\leqslant 2(q^2-1)<n$,$1<y+xq<y(q+1)\leqslant 2(q^2-1)<n$,所以 $x+yq\neq 0(\mathrm{mod}\ n)$ 且 $y+xq\neq 0(\mathrm{mod}\ n)$ 。

当 $t=1$ 时,$1<x+yq^3<y(q^3+1)\leqslant 2(q-1)(q^3+1)=3(q^2-1)(q^2-q+1)-(q-1)(q^3+1)$,由于 $-(lq+1)n<-(q-1)(q^3+1)<-(l\cdot q)n$ 且不为零,所以 $x+yq^3\neq 0(\mathrm{mod}\ n)$

同理 $y+xq^3\neq 0(\mathrm{mod}n)$ 。因此,$\forall x,y\in[1,\delta_{new}-1]=[1,2q-2]$ 时,(C_x,C_y) 不构成斜非对称偶。

由以上 2.1 节可知,当 $q=3l+1$,最大设计距离的下界可达到 $\delta_{new}=2q-1$,并且设计距离 $2\leqslant\delta\leqslant\delta_{new}$ 的狭义 BCH 码包含其 Hermitian 对偶码。

同理定理 2.1 的结论 2)成立。

2.1.2 非狭义 BCH 码

与狭义 BCH 码的讨论相类似,我们给出非狭义 BCH 码的最大设计距离的下界 δ_{new} 。

定理 2.2 设码长 $n=3(q^2-1)$,有:

1)当 $q=3l+1$,$s=3q$,$u=2$,$v=2q-5$ 时,定义集合为 $T_{[s-u,s+v]}$ 、码长为 n 的非狭义对偶包含 BCH 码的最大设计距离的下界为 $\delta=\delta_{new}=2q-1$。

2)当 $q=3l+2$,$s'=q+1$,$u'=1$,$v'=q-4$ 时,定义集合为 $T_{[s-u',s+v']}$ 、码长为 n 的非狭义对偶包含 BCH 码的最大设计距离的下界为 $\delta=\delta_{new}=q-1$。

证明:1)当 $q=3l+1$ 时,设 $s=3q$,$u=2$,$v=2q-5$,根据引理 1.2 可知,$\forall i,j\in[-u,v]$,C_{s+i} 为非斜对称的,C_{s+i} 和 C_{s+j} 不构成非斜对称偶。于是可以很容易找到一个非狭义 BCH 码定义集合 $T=[s-u,s+v]$,使得非狭义 BCH 码的最大设计距离的下界达到 $\delta_{new}=2q-1$。

2)当 $q=3l+2$ 时,设 $s'=q+1$,$u'=1$,$v'=q-4$,根据引理 1.2 可知,$\forall i,j\in[-u',v']$,C_{s+i} 为非斜对称的,C_{s+i} 和 C_{s+j} 不构成非斜对偶。于是可以很容易找到一个非狭义 BCH 码定义集合 $T=[s'-u',s'+v']$,使得最大设计距离的下界达到 $\delta_{new}=q-1$。

总结上述讨论,**定理 2.2** 得证。

2.2 Hermitian 对偶包含 BCH 码的构造

这节中我们通过对定义集合的讨论,计算码长为 $n=3(q^2-1)$,$2\leqslant\delta\leqslant\delta_{new}$ 的狭义和非狭义对偶包含 BCH 码的维数,从而构造出满足 Hermitian 对偶包含条件的 BCH 码。给出当 $2\leqslant\delta\leqslant\delta_{new}$ 时狭义和非狭义对偶包含 BCH 码的维数,从而构造 BCH 码。构造结果由**定理 2.3** 给出。

定理 2.3 设 $n=3(q^2-1)$,$q=3l+1,3l+2$,$\delta_{new}=2q-1$,则:

1)当 $2\leqslant\delta\leqslant\delta_{new}$ 时,存在参数为 $[n,n-(\left\lfloor\frac{\delta-1}{3}\right\rfloor+3(\delta-\lceil\frac{\delta}{3}\rceil)),d\geqslant\delta]$ 的 Hermitian 对偶包含狭义 BCH 码。

2)当 $2\leqslant\delta\leqslant\delta_{new}$ 时,存在参数为 $[n,n-(\left\lfloor\frac{\delta-1}{3}\right\rfloor+3(\delta-\lceil\frac{\delta+2}{3}\rceil)),d\geqslant\delta]$ 的 Hermitian 对偶包含非狭义 BCH 码。

证明:1)当 $q=3l+1$,$\delta=\delta_{new}$ 时,存在一个定义集合为 $T_{[1,\delta_{new}-1]}$ 。当 $2\leqslant\delta\leqslant\delta_{new}$ 时,令 $f\leqslant\delta-1$,于是 $T_{[1,\delta-1]}$ 定义一个以 δ 为设计距离的 Hermitian 对偶包含狭义 BCH 码,所以存在参数为 $[n,n-(\left\lfloor\frac{\delta-1}{3}\right\rfloor+3(\delta-\lceil\frac{\delta}{3}\rceil)),d\geqslant\delta]$ 的 Hermitian 对偶包含狭义 BCH 码。

2)由**定理 2.2** 结论 1)可知,此时存在一个定义集合为 $T_{[s-u,s+v]}$,如果集合 $[e,f]\subset[s-u,s+v]$,则存在一个定义集合为 $T_{[e,f]}$ 的 Hermitian 对偶包含非狭义 BCH 码。当 $2\leqslant\delta\leqslant\delta_{new}$ 时,令 $f=s$,$e=s-\delta+2$,则定义集合为 $T_{[s-\delta+2,s]}$ 的对偶包含非狭义 BCH 码的设计距离为 δ 。所以存在参数为 $[n,n-(\left\lfloor\frac{\delta-1}{3}\right\rfloor+3(\delta-\lceil\frac{\delta+2}{3}\rceil)),d\geqslant\delta]$ 的 Hermitian 对偶包含非狭义 BCH 码。

根据**定理 2.1** 结论 2)和**定理 2.2** 结论 2),当 $q=3l+2$ 时,**定理 2.3** 的结论依然成立。利用这些对偶包含 BCH 码可进一步构造出量子 BCH 码。

3 量子 BCH 码的构造

本节将利用上节中当 q 取不同值时得到的 2 类 Hermitian 对偶包含狭义和非狭义 BCH 码,以及**定理 1.3** 提供的量子码的 Hermitian 构造法,进一步构造出量子 BCH 码。分别由狭义和非狭义 BCH 码构造出的量子 BCH 码具有不同的参数,具体由如下定理给出。

定理 3.1 设 $n=3(q^2-1)$,$q=3l+1$,$\delta_{new}=2q-1$,有

1)当 $2\leqslant\delta\leqslant\delta_{new}$,$\theta_\delta=\left\lfloor\frac{\delta-1}{3}\right\rfloor+3(\delta-\lceil\frac{\delta}{3}\rceil)$ 时,存在参数为 $[[n,n-2\theta_\delta,\delta]]_q$ 的量子 BCH 码。

2) 当 $2 \leqslant \delta \leqslant \delta_{new}$, $\theta_\delta' = \left\lfloor \frac{\delta-1}{3} \right\rfloor + 3(\delta - \left\lceil \frac{\delta+2}{3} \right\rceil)$ 时,存在参数为 $[[n, n-2\theta_\delta', \delta]]_q$ 的量子 BCH 码。

定理 3.2　设 $n=3(q^2-1)$, $q=3l+2$, $\delta_{new}=q-1$,有

1)当 $2 \leqslant \delta \leqslant \delta_{new}$, $\theta_\delta = \left\lfloor \frac{\delta-1}{3} \right\rfloor + 3(\delta - \left\lceil \frac{\delta}{3} \right\rceil)$ 时,存在参数为 $[[n, n-2\theta_\delta, \delta]]_q$ 的量子 BCH 码。

2)当 $2 \leqslant \delta \leqslant \delta_{new}$, $\theta_\delta' = \left\lceil \frac{\delta-1}{3} \right\rceil + 3(\delta - \left\lceil \frac{\delta+2}{3} \right\rceil)$ 时,存在参数 $[[n, n-2\theta_\delta', \delta]]_q$ 的量子 BCH 码。

由**定理 2.3**　以及 Hermitian 构造法,很容易得到上述**定理 3.1** 和**定理 3.2** 的结论,于是这 2 个定理的证明过程不再叙述。

4　结语

本文首先给出了码长为 $n=3(q^2-1)$ 的 q^2-元非本原 Hermitian 对偶包含狭义 BCH 码最大设计距离的下界 δ_{new},证明了非狭义 BCH 码的最大设计距离的下界也可达到 δ_{new};其次,计算出两类 Hermitian 对偶包含 BCH 码的维数;最后,构造出量子 BCH 码。并且由非狭义 BCH 码构造出的量子 BCH 码的参数优于文献[13]中由狭义 BCH 码构造出的量子 BCH 的参数,而且当 $\delta_{max}+1 \leqslant \delta \leqslant \delta_{new}$ 时,不论是由狭义 BCH 码构造的量子码,还是由非狭义 BCH 码构造的量子码,其参数都是新的。

参考文献(References):

[1] Shor P W. Scheme for Reducing Decoherence in Quantum Computer Memory [J]. Phy Rev A, 1995, 52:2493-2496.

[2] Steane A M. Error Correcting Codes in Quantum Theory [J]. Phys rev ltt, 1996, 77:793-797.

[3] Calderbank A R, Rains E M, Shor P W, et al. Quantum Error-Correction Via Codes over GF(4) [J]. IEEE Trans Inf Theory, 1998, 44:1369-1387.

[4] Gottesman D. Stabilizer Codes and Quantum Error Correction [D]. California: California Inestitute of Technology. quant-ph/9707027, 1997.

[5] La G G. Guardia. Constructions of New Families of Nonbinary Quantum Codes [J]. Phy Rev A, 2009, 80:042331(1-11).

[6] Aly S A, Klappenecker A, Sarvepalli P K. On Quantum and Classical BCH Codes [J]. IEEE Trans Inf Theory, ISIT, 2007:1114-1118.

[7] Huffman W C, Pless V. Fundamentals of Error-Correcting Codes Fundamentals of Error - Correcting Codes[M]. Cambridge: Cambridge University Press, 2003.

[8] Macwilliams F J, Sloane N J A. The Theory of Error-Correcting Codes [M]. Amsterdam Netherlands: North-Holland, 1997.

[9] 李瑞虎,左飞,刘杨.斜对称 q^2 - 分圆陪集及应用 [J]. 空军工程大学学报:自然科学版, 2011, 12, 87-89.
LI Ruihu, ZUO Fei, LIU Yang.

[10] Ketkar A, Klappenecker A, Kumar S, et al. Saverpalli. Nonbinary Stabilizer Codes Over Finite Fields [J]. IEEE Trans Inf Theory, 2006, 52:4892-4914.

[11] Li RH, Zuo F, Liu Y. Hermitian Dual Containing BCH Codes and Construction of New Quantum Codes [J]. Quantum Inf Comp, 2013, 13:0021-0036.

[12] Liu Y, Ma Y N, Feng Y Q. New Quantum Codes Constructed From A Class of Imprimitive BCH Codes [J]. Int J Quantum Inf, 2013, 11:1350006.

[13] Ling S, Luo J, Xing C. Generalization of Steane's Enlargement Construction of Quantum Codes and Applications [J]. IEEE Trans Inf Theory, 2010, 56:4080-4084.

(编辑:徐敏)