* 1

斜对称 q^2 – 分圆陪集及其应用研究

李瑞虎，　左　飞，　刘　杨
(空军工程大学理学院,陕西　西安　710051)

摘要　引入斜对称 q^2 – 分圆陪集及斜非对称偶的概念,深入考察了 $n = q^{2m} - 1$ 时斜对称分圆陪集及斜非对称偶的性质及确定方法。以此为基础研究了 Hermite 对偶包含 BCH 码的极大设计距离。解决了前人留下的一个疑难问题,并改进了前人的一个判别上界,所得到的界是紧的。再利用所得到的满足 Hermite 对偶包含条件的非狭义 BCH 码构造出一些具有很好参数的量子纠错码,这些量子码超过已有文献中由狭义 BCH 码构造的量子纠错码。

关键词　q^2 – 分圆陪集; 斜非对称偶; BCH 码; 量子码
DOI　10. 3969/j. issn. 1009 – 3516. 2011. 01. 019
中图分类号　O157. 4　　**文献标识码**　A　　**文章编号**　1009 – 3516(2011)01 – 0087 – 03

量子纠错码是量子计算和量子通信的保障,构造具有良好参数的量子纠错码则是其中的最重要研究内容。文献[1 – 3]先后建立了二元加性量子纠错码以及 q – 元加性量子纠错码与自正交经典线性码的联系。基于这些工作,人们开始研究用特殊自正交经典线性码构造二元和非二元(q – 元)量子纠错码[3 – 7]。而利用经典线性码构造量子纠错码首先要解决经典线性码的自正交性(或对偶包含判定条件)问题, 文献[4 – 5]先后讨论了本原与非本原 BCH 码的对偶包含判定条件,以及用对偶包含 BCH 码构造量子纠错码的参数。2009 年 Guardia[6] 发现性能优越的非狭义 BCH 码满足对偶包含条件,并用非狭义 BCH 码构造出更好的量子码。

本文将文献[7]中的 2 – 分圆陪集的对称性与非对称偶概念推广至 q^2 – 分圆陪集,我们用分圆陪集理论再深入研究 q^2 – 元 BCH 码包含其 Hermite 对偶码的条件,解决文献[4 – 5]留下的一个疑难问题,并改进 $n = q^{2m} - 1$ 且 m 为偶数时,一般 BCH 码满足对偶包含的极大设计距离的上界。为此,介绍本文需要的相关概念和结论。

1　q^2 – 分圆陪集与 BCH 码

设 q 为素数的幂, $n > 1$ 为正整数且 $\gcd(n, q) = 1$。若 x 为整数且满足 $0 \leqslant x < n$, x 模 n 的 q^2 – 分圆陪集 C_x 为:

$$C_x = \{x, xq^2, x(q^2)^2, \cdots, x(q^2)^{k-1}\} \pmod n \tag{1}$$

式中 k 是使得 $(q^2)^k s \equiv x \pmod n$ 的最小正整数。若 $(n - qx) \pmod n \in C_x$, 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})。

约定: 为下文叙述方便,我们将集合 $\{1, 2, \cdots, n-1\}$ 叫做区间 $[1, n-1]$,它的子集 $\{e, e+1, e+2, \cdots, f\}$ 叫做区间 $[e, f]$。将 $T = C_b \cup C_{b+1} \cup \cdots \cup C_{b+\delta-1}$ 记为 $T = T_{[b, b+\delta-1]}$。

定义　若 q^2 – 元域 F_{q^2} 上码长为 n 的循环码 C 的定义集合为 $T = T_{[b, b+\delta-1]}$, C 叫做 F_{q^2} 上的设计距离为 δ

*　**收稿日期**:2010 – 12 – 30
基金项目:国家自然科学基金资助项目(11071255);陕西省自然科学基础研究计划资助项目(SJ08A02)
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:liruihui2008@ yahoo. com. cn

的 BCH 码,$[b,b+\delta-1]$叫做 C 的定义区间。当 $n=q^{2m}-1$ 时 C 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。

关于 F_{q^2}上循环码 C 包含其 Hermite 对偶,文献[4-5]得到如下判断方法:

引理 1 若 $\gcd(n,q)=1$,F_{q^2}上循环码 C 的定义集合 T,则 C 包含其 Hermite 对偶的充要条件是 $T\cap T^{-q}=\varnothing$, 其中 $T^{-q}=\{-qx \mid x\in T\}$。

具体到 F_{q^2}上的 BCH 码 C, 引理 1 可具体用 q^2 - 分圆陪集描述如下:

引理 2 若 $\gcd(n,q)=1$, F_{q^2}上的 BCH 码 C 的定义集合 $T=C_b\cup C_{b+1}\cup\cdots\cup C_{b+\delta-1}=T_{[b,b+\delta-1]}$, 则 C 包含其 Hermite 对偶的充要条件是每个 C_{b+i}为斜非对称的,且 C_{b+i}与 C_{b+j}不构成斜非对称偶, $0\leqslant i,j\leqslant\delta-1$。

文献[4-5]得到 q^2 - 元狭义 BCH 码包含其 Hermite 对偶码的一些必要或充分条件,同时给出一般 BCH 码满足对偶包含时极大设计距离的上限;但是它所给出的上限太弱,且还有 $n=q^4-1$ 这一情况未解决。文献[6]所给出满足对偶包含条件非狭义 BCH 码的设计距离比较小,还可以进一步改进。关于 F_{q^2}上 BCH 码 C 包含其 Hermite 对偶,文献[4-6]得到的结论可概括如下:

引理 3[4-5] 若 $n=q^{2m}-1$,q 为素数的幂且 $m\geqslant 3$ (m 为偶数或奇数),$\delta_{\max}=q^{m+1}-q^2+1$, 则设计距离 $\delta\leqslant\delta_{\max}$的狭义本原 BCH 码包含其 Hermite 对偶。而当 $m\geqslant 4$ 为偶数时, 则设计距离 $\delta\geqslant 2\delta_{\max}$的本原 BCH 码(狭义或非狭义)一定不包含其 Hermite 对偶。

引理 4[6] 若 $n=q^{2m}-1$,$q\geqslant 3$ 为素数的幂,则有如下结论成立:

1) 若 $m=2$, $\delta\leqslant q^2$, 则存在设计距离为 δ 的非狭义 BCH 码包含其 Hermite 对偶;

2) 若 $m\geqslant 4$, $\delta\leqslant 2q^2+2$, 则存在设计距离为 δ 的非狭义 BCH 码包含其 Hermite 对偶。

2 Hermite 对偶包含的 BCH 码的极大设计距离

本节讨论 m 为偶数时,如何改进**引理 3** 和**引理 4** 的结论,同时确定出 $n=q^4-1$ 时 BCH 码包含其 Hermite 对偶的极大设计距离。本文的主要结论是:

定理 1 若 $n=q^4-1$,q 为素数的幂,$\delta_{\text{new}}=q^3-q^2+q-1$, 则设计距离 $\delta\leqslant\delta_{\text{new}}$的狭义本原 BCH 码包含其 Hermite 对偶。并且任何设计距离 $\delta\geqslant\delta_{\text{new}}+1$ 的本原 BCH 码(狭义或非狭义)一定不包含其 Hermite 对偶。

定理 2 $n=q^{2m}-1$,q 为素数的幂,且 $m\geqslant 4$ 为偶数,$\delta_{\max}=q^{m+1}-q^2+1$,

1)存在设计距离为 $\delta=\delta_{\max}+1$ 的非狭义本原 BCH 码包含其 Hermite 对偶;

2)设计距离为 $\delta\geqslant\delta_{\max}+2$ 的本原 BCH 码(狭义或非狭义)一定不包含其 Hermite 对偶。

设 $s=q^{2(m-1)}+q^{2(m-2)}+\cdots+q^2+1$。因为$(q^2-1)s\equiv 0(\bmod n)$, 所以 $q^2s\equiv s(\bmod n)$,$C_{is}=\{is\}$。若 C_{xs}为斜对称的,则 $xs=-q(xs)$,所以$(q+1)xs\equiv 0(\bmod n)$,即$(q-1)\mid x$。所以,斜对称分圆陪集有 $C_{(q-1)s}$, $C_{2(q-1)s},\cdots,C_{q(q-1)s}$及 C_0。利用$(q-1)s,2(q-1)s,\cdots,q(q-1)s$,可将$[1,n-1]$分成如下$(q+1)$个区间。$[1,(q-1)s-1],[(q-1)s+1,2(q-1)s-1],\cdots,[q(q-1)s+1,(q^2-1)s-1]$。

我们证明**定理 1** 和**定理 2** 的思路是将$[1,n-1]$分成若干个小区间,小区间的元素个数为 $\delta_{\max}$或 $\delta_{\max}-1$,再考察小区间中某些特殊元素所在分圆陪集的斜对称性以及斜非对称偶如何确定。若以$[i,j]$为定义区间的 BCH 码包含其 Hermite 对偶,则$[i,j]$必在上述某个区间之内。为此仅需要考察以上$(q+1)$个区间内元素的分圆陪集及其非对称偶。下面以 $n=q^4-1$ 为例,说明对偶包含其 BCH 码的极大设计距离如何确定。

将$[1,n-1]$分成$(q+1)$个区间$[1,(q-1)s-1]$, …, $[q(q-1)s+1,(q^2-1)s-1]$, 每个包含的元素个数为$(q-1)s-1=q^{m+1}-q^2+q-2$,从而不存在 $\delta\geqslant q^3-q^2+q$ 的 BCH 码包含其 Hermite 对偶。由文献[5]的定理 18 可知,$T=C_1\cup C_2\cup\cdots\cup C_{q^3-q^2}$满足条件 $T\cap T^{-q}=\varnothing$。容易证明 $T_{[1,(q-1)s-1]}=C_1\cup C_2\cup\cdots\cup C_{q^3-q^2+q-2}=T$, 因此设计距离 $\delta\leqslant\delta_{\text{new}}$的狭义本原 BCH 码包含其 Hermite 对偶。

3 应用

利用**定理 1** 和**定理 2** 的结果,可用非狭义对偶包含其 BCH 码构造出距离 $3\leqslant d\leqslant\delta_{\max}+1$ 的量子码,这些量子码超过已有文献中由狭义 BCH 码构造的量子纠错码。距离 $3\leqslant d\leqslant 2q^2+2$ 的量子码与文献[6]一样,这

里仅列出 $n=q^4-1, q=4$ 时,$2q^2+3\leqslant d\leqslant\delta_{new}=q^3-q^2+q-1$ 的量子码。

表 1　$n=q^4-1, q=4$ 时,非狭义 BCH 码构造的量子码与狭义 BCH 码构造的量子码比较

Tab. 1　Comparisons of quantum codes constructed from non – narrow – sense and narrow sense BCH codes, for $n=q^4-1, q=4$

非狭义 BCH 码	新量子码	狭义 BCH 码	已知量子码
$\lvert T_{[17,34+i]}\rvert=32+2i$	$[[n,n-2(32+2i),19+i]]_4$	$\lvert T_{[1,18+i]}\rvert=33+2i$	$[[n,n-2(33+2i),19+i]]_4$
$\lvert T_{[17,48]}\rvert=\cdots=\lvert T_{[17,50]}\rvert=60$	$[[n,n-2\times60,35]]_4$	$\lvert T_{[1,32]}\rvert=\lvert T_{[1,33]}\rvert=61$	$[[n,n-2\times61,34]]_4$
$\lvert T_{[17,51]}\rvert=61$	$[[n,n-2\times61,36]]_4$	$\lvert T_{[1,34]}\rvert=62$	$[[n,n-2\times62,35]]_4$

4　结论

通过引入斜对称 q^2 – 分圆陪集及斜非对称偶的概念,研究斜对称分圆陪集及斜非对称偶的性质及确定方法。我们确定出 Hermite 对偶包含本原 BCH 码的极大设计距离。解决了前人留下的一个疑难问题,并改进了前人的一个判别上界。利用本文的理论和方法,可进一步研究 Hermite 对偶包含非本原 BCH 码的极大设计距离,构造出新的量子纠错码。

参考文献:

[1] 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.

[2] Ashikhmin A, Knill E. Non – binary quantum stabilizer codes[J]. IEEE trans inf theory, 2001, 47 (7):3065 – 3072.

[3] Ketkar A, Klappenecker A, Kumar S, et al. Nonbinary stabilizer codes over finite fields[J]. IEEE trans inf theory, 2006, 52:4892 – 4914.

[4] Aly S A, Klappenecker A, Sarvepalli P K. Primitive quantum BCH codes over finite fields[C]//Proc int symp inform theory. [S. l.]:ISIT, 2006:1105 – 1108.

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

[6] La Guardia G G. Constructions of new families of nonbinary quantum codes[J]. Phys rev A, 2009, 80(4):042331.

[7] Sloane N J A, Thompson J GCyclic self – dual codes[J]. IEEE trans inform theory, 1983, 29:364 – 366.

(编辑:徐楠楠)

A Study of Skew Symmetric q^2 – cyclotomic Coset and Its Application

LI Rui – hu , ZUO Fei , LIU Yang

(Institute of Science, Air Force Engineering University, Xi′an 710051, China)

Abstract: On the basis of concepts of skew symmetric – cyclotomic coset and skew asymmetric coset pair, and their properties deeply studied, and methods determined, a maximal design distance of BCH codes with length contained in its Hermitian dual is studied. Thus, such an unsolved problem for maximal design distance of BCH codes with length is solved, upper bound of maximal design distance of BCH codes previously known is improved, and a new upper bound picked up is sharp. By utilizing these Hermitian dual containing non – narrow – sense BCH codes, many new quantum codes with good parameters are constructed, these new quantum codes are better than that constructed from narrow – sense BCH codes in the literature.

Key Words: q^2 – cyclotomic coset; skew asymmetric coset pairs; BCH codes; quantum codes