设计距离为5的q元BCH码的无内周期码字个数

陈　燕[1]，　辛小龙[1]，　蔺　昕[2]

(1. 西北大学数学系，陕西西安 710049；2. 空军工程大学理学院，陕西西安 710051)

摘要：利用一些重要的数论函数以及循环陪集，研究了BCH码的周期分布，得到了设计距离为5的q元BCH码的无内周期的码字个数，推广了文献[1]的结果。

关键词：BCH码；循环陪集；循环等价类；周期分布

中图分类号：O157.4　　文献标识码：A　　文章编号：1009-3516(2006)03-0089-03

码的周期分布是一个新的参数,它对线性码的研究有重要价值。例如最近一些国外学者发现用无内周期码字可以构造出一类新的具有良好相关特性并且在序列密码中有用的密钥流序列。而正是基于这点对 q 元 BCH 码中无内周期码字的个数问题进行了研究。通过对循环陪集的深入探讨得到了设计距离为5的 q 元 BCH 码的无内周期的码字个数。

1　预备知识

定义1[2]　给定有限域 $GF(q^m)$。设 $sq^{m_s}=s(\mathrm{mod}q^m-1)$，记 $\{s,sq,sq^2,\cdots,sq^{m_s-1}\}=C_s$ 为 $GF(q^m)$ 上关于 s 的循环陪集。称 $\{C_s\}_{0\leqslant s\leqslant q^m-1}$ 为 $GF(q^m)$ 上的循环陪集结构,记为 A。

定义2[2]　记 $a_s=\min\{p|p\in C_s\}$，则称 $\{a_s|a_s\in A\}$ 为 A 的循环陪集首集,记为 a，α 为 $GF(q^m)$ 的本原元,$C_s\in A,s\in a$。进而,记 $M^{(s)}(x)=\prod_{i\in C_s}(x-\alpha^i)$。

定义3[3]　α 为 $GF(q^m)$ 的本原元,记 $M^{(s)}(x)=\prod_{i\in C_s}(x-\alpha^i)$,码长为 $n(n\leqslant q^m-1)$ 的 $GF(q^m)$ 上的 BCH 码,对某个 $\delta>0$，其生成多项式可定义为

$$g(x)=\mathrm{LCM}\{M^{(b)}(x),M^{(b+1)}(x),\cdots,M^{(b+\delta-2)}\}$$

其中 $b\geqslant 0$，称以 $g(x)$ 为多项式的码 C 为设计距离为 δ 的一个 q 元 BCH 码。若 $b=1,n=q^m-1$，称 C 为狭义本原 BCH 码。下面将讨论的就是这类 BCH 码。

定义4[4]　$\forall c=(c_0,c_1,\cdots,c_{n-1})\in C$，定义循环置换 $\rho^1c=(c_1,c_2,\cdots,c_{n-1},c_0)$。$\forall c\in C$,若 $\rho^m c=c$，则 m 称为 C 的一个周期，C 的最小周期记为 $t(c)$，若 $t(c)=n$,则称码无内周期。并且记 $A_r=|\{c\in C:r\text{ 为 }c\text{ 的一个周期}\}|$，$B_r=|\{c\in C:t(c)=r\}|$，$r=1,2,\cdots,n$。

引理1[5]　给定多项式 $u(x)\in F_q[x]$，则存在 $q^{k-\deg[u(x)]}$ 个次数不超过 $j-1$ 的多项式 $v(x)$ 使得 $u(x)|v(x)$。

引理2[6]　与信息多项式 $a(x)=\sum_{i=0}^{k-1}a_ix^i$ 相应的码字 c 具有周期 $r\Leftrightarrow h(x)|a(x)(x^r-1)$。设 $h_r(x)=\gcd[h(x),x^r-1]$，则由引理1和引理2可以得到下面的结论:

$$A_t=q^{k-\deg(\gcd[h(x),x^r-1])}=q^{\deg[h_r(x)]},\quad B_t=\sum_{r|t}\mu(t/r)q^{\deg[h_r(x)]}\tag{1}$$

收稿日期:2005-04-21
基金项目:陕西省自然科学基金资助项目(2004A110);陕西省教育厅专项科研基金项目(03JK058)
作者简介:陈　燕(1981-),女,陕西咸阳人,硕士生,主要从事编码理论研究;
辛小龙(1955-),男,陕西西安人,教授,博士生导师,主要从事编码及信息论研究.

2 $\delta=5$ 的 q 元 BCH 码无内周期的码字个数

约定 q 为奇素数。由式(1)可知,要确定无内周期的码字个数关键在于求 $h_r(x)$ 的次数。当 $\delta=5$ 时,码 C 含有 $\alpha,\alpha^2,\alpha^3,\alpha^4$ 4 个连续根。BCH 码 C 的生成多项 $g(x)=\mathrm{LCM}\{M^{(1)}(x),M^{(2)}(x),M^{(3)}(x),M^{(4)}(x)\}$。记

$$P=C_1=\{1,q,q^2,\cdots,q^{m_1-1}\} \qquad L=C_2=\{2,2q,2q^2,\cdots,2q^{m_2-1}\}$$

$$Q=C_3=\{3,3q,3q^3,\cdots,3q^{m_3-1}\} \qquad R=C_4=\{4,4q,4q^2,\cdots,4q^{m_4-1}\}$$

定理 1 当 $q>4,m>1$ 时,集合 C_i 中元素个数为 m_i,并且 $m_i=m(i=1,2,3,4)$。

证明: $\because q>4,m>1,\therefore 4q^{m-1}=[q-(q-4)]q^{m-1}=q^m-(q-4)q^{m-1}<q^m-1$,而$4q^m=4(\mathrm{mod}q^m-1)$,若集合 R 中的元素不循环重复,则说明 $m_4=m$。事实上,如果存在集合 R 里的两个元素使得 $4q^l=4q^k(\mathrm{mod}q^m-1)(l>k)$,则有 $q^{l-k}=1(\mathrm{mod}q^m-1)$,即 $m|l-k$。由于 $0\leqslant l-k<m$,故 $l-k=0$,即 $l=k$。同理 $m_1=m_2=m_3=m$。

定理 2 给定一整数 r,α^j 为 x^r-1 的一个根当且仅当$\frac{n}{(n,r)}|j$。

证明: 由 α 的阶为 n,得 α^j 的阶为$\frac{n}{(n,r)}$, α^j 为 x^r-1 的一个根$\Leftrightarrow \frac{n}{(n,r)}|r$,即$\frac{n}{(n,r)}|j$。

定理 3 设 $q>4,m>1$,令 $n=q^m-1$, $\Delta(n)=\sum_{r|n}\mu(r)q^{n/r}$。若 C 为一 q 元 BCH 码且具有设计距离 5,则

$$B_n=\begin{cases}\Delta(n)+2q^{\frac{n}{3}-m}(q^m-1)q^{\frac{n}{2}-2m}(q^{2m}-1)-q^{4m}(q^{4m}-1), & \text{若 3 整除 } n\\ \Delta(n)+q^{\frac{n}{2}-2m}(q^{2m}-1)-q^{n-4m}(q^{4m}-1), & \text{若 3 整除 } n\end{cases}$$

证明: 令 $X=\{0,1,\cdots,n\}$ $N=X-P-L-Q-R$,则 $h(x)=\prod_{i\in N}(x-\alpha^i)$。

记 $X_r=\left\{j\in X|\frac{n}{(n,r)}|j\right\},N_r=X_r\cap N,P_r=X_r\cap P,L_r=X_r\cap L,Q_r=X_r\cap Q,R_r=X_r\cap R$。这样求 $h_r(x)$ 次数的问题就进而转化为求集合 N_r 中元素个数问题。因为 q 为奇素数,所以一定有 2 是 n 的一个因子,所以下面只考虑 4 种情况来讨论这个问题:

1)$4|n,3|n$; 当 $r=\frac{n}{4}$ 时,$\frac{n}{(n,\frac{n}{4})}|j\Rightarrow j=4k$,也就是说集合 $X_{\frac{n}{4}}\supseteq R$,但是与集合 P,L,Q 却不相交. 所以

$|R_{n/4}|=|X_{n/4}\cap R|=|R|=m$, $|L_{n/4}|=|Q_{n/4}|=|R_{n/4}|=0$。

当 $r=\frac{3n}{4}$或 $r=\frac{n}{4}$时得到$|R_{3n/4}|=|X_{3n/4}\cap R|=|R|=m$, $|L_{3n/4}|=|Q_{3n/4}|=|R_{3n/4}|=0$。

当 $r=\frac{3n}{4}$时,$|Q_{n/3}|=m,|P_{n/3}|=|L_{n/3}|=|R_{n/3}|=0$。$r=\frac{2n}{3}$与 $r=\frac{n}{3}$ 情况类似。

当 $r=\frac{n}{2}$时,$|R_{n/2}|=|L_{n/2}|=m,|P_{n/2}|=|Q_{n/2}|=0$。最后当 $r=n$,$|P_n|=|L_n|=|Q_n|=|R_n|=m$。

归结上述所讨论的情况,当 $r\neq\frac{n}{4}、\frac{3n}{4}、\frac{n}{3}、\frac{2n}{3}、\frac{n}{2}、n$ 时,X_r 与 P,L,Q,R 都不相交,这时 $N=X-P-L-Q-R=X$,而$|N_r|=|X_r\cap X|=(n,r)$, $|N_{n/4}|=|N_{3n/4}|=\frac{n}{4}-m,|N_{n/3}|=|N_{2n/3}|=\frac{n}{3}-m,|N_{n/2}|=\frac{n}{2}-m$ $|N_n|=n-4m$。

所以 当 $r\neq\frac{n}{4}、\frac{3n}{4}、\frac{n}{3}、\frac{2n}{3}、\frac{n}{2}、n$ 时:

$$A_r=q^{(n,r)};$$

$$A_{\frac{n}{4}}=A_{\frac{3n}{4}}=q^{\frac{n}{4}-m},A_{\frac{n}{3}}=A_{\frac{2n}{3}}=q^{\frac{n}{3}-m},A_{\frac{n}{2}}=q^{\frac{n}{2}-2m},A_n=q^{n-4m};$$

$$B_n=\sum_{r|n}\mu(r)A_{n/r}=\Delta(n)+2q^{\frac{n}{3}-m}(q^m-1)+q^{\frac{n}{2}-2m}(q^{2m}-1)-q^{n-4m}(q^{4m-1})。$$

2)$4|n$ 及 3 不整除 n。在这种情况下$\frac{n}{3}$ 和$\frac{2n}{3}$ 显然不是一整数,所以 $r=\frac{n}{3}$, $r=\frac{2n}{3}$,这两个条件我们不

予考虑,方法与1)相同,我们只给出写实结果。

当 $r\neq\frac{n}{4}$、$\frac{3n}{4}$、$\frac{n}{2}$、n 时,$A_r=q^{(n,r)}$;其余情况为:$A_{\frac{n}{4}}=A_{\frac{3n}{4}}=q^{\frac{n}{4}-m}$,$A_{\frac{n}{2}}=q^{\frac{n}{2}-2m}$,$A_n=q^{n-4m}$,$B_n=\Delta(n)+q^{\frac{n}{2}-2m}(q^{2m}-1)-q^{n-4m}(q^{4m-1})$。

3)3|n 及4不整除 n。当 $r\neq\frac{n}{3}$、$\frac{2n}{3}$、$\frac{n}{2}$、n 时,$A_r=q^{(n,r)}$;其余情况为:$A_{\frac{n}{3}}=A_{\frac{2n}{3}}=q^{\frac{n}{3}-m}$,$A_{\frac{n}{2}}=q^{\frac{n}{2}-2m}$,$A_n=q^{n-4m}$,$B_n=\Delta(n)+2q^{\frac{n}{3}-m}(q^m-1)+q^{\frac{n}{2}-2m}(q^{2m}-1)-q^{n-4m}(q^{4m-1})$。

4)3不整除 n 且4不整除 n。这种情况只需考虑 $r=\frac{n}{2}$ 和 $r=n$,得到的结果为

当 $r\neq\frac{n}{2}$、n 时,$A_r=q^{(n,r)}$;$A_{\frac{n}{2}}=q^{\frac{n}{2}-2m}$,$A_n=q^{n-4m}$,$B_n=\Delta(n)+q^{\frac{n}{2}-2m}(q^{2m}-1)-q^{n-4m}(q^{4m-1})$。

综合上述4种情况,则定理得证。

最后考虑 $q=3$,当 $\delta=5$,$q=3$ 时,码 C 含有 α、α^2、α^3、α^4 这4个连续根。由文献[7,8]可知在特征为3的域上 α^i 与 α^{3i} 的最小多项式相同,因此三元 BCH 码 C 的生成多项式为 $g(x)=LCM\{M^{(1)}(x),M^{(2)}(x),M^{(4)}(x)\}$,因而循环陪集就只有3个集合 $P=C_1=\{1,3,3^2,\cdots 3^{m-1}\}$,$L=C_2=\{2,2\cdot 3,2\cdot 3^2,\cdots,2\cdot 3^{m-1}\}$,$R=C_4=\{4,4\cdot 3,4\cdot 3^2,\cdots,4\cdot 3^{m-2},3^{m-1}+1\}$,仿以上证明得到:

当 $r\neq\frac{n}{4},\frac{n}{2},\frac{3n}{2},n$ 时,$A_r=3^{(n,r)}$;$A_{\frac{n}{4}}=3^{\frac{n}{4}-m}$,$A_{\frac{3n}{4}}=3^{\frac{n}{4}-m}$,$A_{\frac{n}{2}}=3^{\frac{n}{2}-2m}$,$A_n=3^{n-3m}$,$B_n=\sum_{r|n}\mu(r)A_{n/r}=\Delta(n)+3^{\frac{n}{2}-2m}(3^{2m-1})-3^{n-3m}(3^{3m}-1)$,证毕。

参考文献:

[1] Fu Fangwei ,Shen Shiyi. On the Nonperiodic Cyclic Equivalence Classes of Hanmming Codes and BCH Codes[J]. Journal of Statistical Planning and Inference , 2001, 94(2): 205 - 209.

[2] 岳殿武. 循环陪集结构及其应用[J]. 系统科学与数学, 1992, 12(1): 15 - 20.

[3] 岳殿武, 胡正明. 关于 q 元 BCH 码的维数和最小距离[J]. 电子科学学刊, 1996, 18(3): 263 - 269.

[4] 王建宇. 线性码的周期分布与广义周期分布[J]. 通信学报, 1994, 15(1): 8 - 14.

[5] 符方伟, 沈世益. 循环码的周期分布的新的计算公式[J]. 通信学报, 1996, 17(2): 1 - 6.

[6] 扬义先, 胡正明. 纠错码的周期分布[J]. 通信学报, 1992, 13(3): 50 - 54.

[7] 肖国镇, 卿斯汉. 编码理论[M]. 北京, 国防工业出版社, 1993.

[8] 马月娜,赵学军,冯有前. F_4 上2维和3维的最优自正交码[J]. 空军工程大学学报(自然科学版),2005,6(6):63 - 65.

(编辑:田新华)

The Number of Non -periodic Equivalence Classes of BCH Codes with Design 5

CHEN Yah1, XIN Xiao - long1 , LIN Xi2

(1. Department of Mathematics, Northwest University, Xi'an, Shaanxi 710069, China; 2. The Science Institute, Air Force Engineering University, Xi'an, Shaanxi 710051, China)

Abstract :The period distribution of q - ary BCH codes is studied by some important theory functions and cyclotomic coset, and the number of non - periodic equivalence classes of q - ary BCH codes with design 5 is given. The research results of Fu Fangwei and Shen Shiyi in literature [1] are generalized.

Key words:BCH codes; cyclotomic cosets; cyclic equivalence classes; period distribution