本原 BCH 码的维数与周期分布*

李 超

(国防科技大学系统工程与数学系 长沙 410073)

摘 要 本文给出了求分圆陪集首集中元素个数新的计算公式，确定了长度为 k 的分圆陪集的个数。给出了 q 元域上狭义本原 BCH 码的维数的计算公式，确定了狭义本原 BCH 码的周期分布。

关键词 BCH 码，分圆陪集，维数，周期分布

分类号 O157.4

On the Dimension and the Period Distribution of Primitive BCH Codes

Li Chao

(Department of Systems Engineering and Mathematics, NUDT, Changsha, 410073)

Abstract This paper presents the new formula for computing the number of the leader-set of cyclotomic cosets. The explicit number of the cyclotomic cosets of length k is fixed. The method for computing the dimension of narrow-sense primitive BCH codes is offered. Finally, we decide the period distribution of this kind of codes.

Key words BCH codes, cyclotomic cosets, dimension, period distribution

BCH 码是纠正多个随机错误的循环码，它的纠错能力强，特别是在短和中等码长的条件下，其性能接近于理论值。另一方面，BCH 码构造方便，编码简单，因此它在编码理论中起着十分重要作用。由于 BCH 码的纠错能力与它的最小距离 d_{BCH} 密切相关，自1959年 BCH 码提出至今[1]，人们对 BCH 码的最小距离进行了深入研究，给出了它的四个限[6]：BCH 限，HT 限，ROOS 限和 LW 限。其中 BCH 限是指 BCH 码的最小距离 d_{BCH} 不小于其设计距离 δ。BCH 码的设计距离越大，则 BCH 码的纠错能力越强，但在实际过程中，BCH 码的设计距离是有限制的，就狭义本原 BCH 码而言，其设计距离 δ 一定为某个分圆陪集的首[3]，而 q 元域上最大分圆陪集首是 $(q-1)\ q^{m-1}-1$[2]。对于设计距离为 δ 的狭义本原 BCH 码，文[3]给出了该码的维数的表示定理，给出了求此 BCH 码维数的一般迭代公式，但该公式复杂、烦琐，迭代过程中许多参数是未知的。本文在讨论分圆陪集特点的基础上，给出了求分圆陪集首集中元素个数新的计算公式，确定了长度为 k 的分圆陪集的个数，进而给出了计算狭义本原 BCH 码维数的算法，确定了狭义本原 BCH 码的周期分布。

1 分圆陪集的概念及性质

定义**1** 设正整数 $s\leq q^m-2$，m_s 是使得 $s\ q^{m_s}\equiv s \bmod q^m-1$ 成立的最小正整数，则称集合 $\{s, sq, sq^2, \cdots, sq^{m_s-1}\}$ 为以 q^m-1 为模关于 s 的分圆陪集，记为 C_s。而 m_s 称为分圆陪集 C_s 的长度。令 $a_s=\min\limits_{p\in C_s} p$，则称 a_s 为分圆陪集 C_s 中首元，简称分圆陪集首。而称 $A_m=\{a_s\ s\in C_s,\ s\leq q^m-2\}$ 为以 q^m-1 为模的分

* 东南大学移动通信国家重点实验室开放基金和国防科技大学青年基金资助
1997年9月6日收稿
第一作者：李超，男，1966年生，副教授

圆陪集首集。

定义**2** 给定任一有限域$GF(q)$及其扩域$GF(q^m)$，其中q为素数或素数的幂，m为某个正整数，C为$GF(q)$上一个n长循环码，如果C的生成多项式$g(x)$的根集合R中含有以下$\delta-1$个连续根：$R\supseteq\{\alpha^{m_0},\ \alpha^{m_0+1},\ \cdots,\ \alpha^{m_0+\delta-2},\}$，但$\alpha^{m_0+\delta-1}\notin R$，这里$\alpha$为$GF(q^m)$中$n$阶元素，则称$C$为$GF(q)$上设计距离为$\delta$的BCH码。如果$m_0=1$，$n=q^m-1$，则称这类BGH码为狭义本原BCH码。

由定义2可知，如果循环码C的生成多项式为$g(x)$，则C是设计距离为δ的狭义本原BCH码$\Leftrightarrow g(\alpha)=g(\alpha^2)=\cdots=g(\alpha^{\delta-1})=0$，但$g(\alpha^{\delta})\neq 0$，这里$\alpha$是$GF(q^m)$中本原元。对任意$s$（$1\leq s\leq q^m-2$），令$M^{(s)}(x)=\prod_{i\in C_s}(x-\alpha^i)$，则有：

引理**1** $M^{(s)}(x)$是$\alpha^s\in GF(q^m)$在$GF(q)$上极小多项式，并且$\deg M^{(s)}(x)=m_s$，$p(m^{(s)}(x))=\dfrac{q^m}{(s,\ q^m-1)}$，这里$p(\ )$表示多项式的周期。

定义**3** 设α为有限域$GF(q)$上n次本原单位根，$(n,\ q)=1$，称$\Phi_n(x)=\prod_{\substack{s=1\\(s,n)=1}}^{n}(x-\alpha^s)$为$GF(q)$上$n$次分圆多项式。

引理**2**[7] (1) $GF(q)$上n次分圆多项式$\Phi_n(x)$是$GF(q)[x]$中$\varphi(n)$次多项式，这里$\varphi(n)$为欧拉函数；(2) $x^n-1=\prod_{d\mid n}\Phi_d(x)$

引理**3**[7] 如果$(n,\ q)=1$，则n次分圆多项式$\Phi_n(x)$在$GF(q)[x]$中可以分解成$\dfrac{\varphi(n)}{d}$个首项系数为1的d次不可约多项式乘积，这里d是满足$q^d\equiv 1 \bmod n$成立的最小正整数。

由上述三个引理我们可得：

定理**1** (1) 分圆陪集首集A_m中元素的个数为：$A_m=\sum_{d\mid q^m-1}\dfrac{\varphi(d)}{m_d}-1$，这里$m_d$是满足$q^{m_d}\equiv 1 \bmod d$成立的最小正整数。

(2) 任意分圆陪集中所含元素的个数必为m的正因子。

(3) 记y_k表示长度为k的分圆倍集的个数，则$y_k=\begin{cases}0 & \text{如果 } k\nmid m\\ \sum\limits_{\substack{d\mid q^m-1\\ d\neq 1\\ m_d=k}}\dfrac{\varphi(d)}{m_d} & \text{如果 } k\mid m\end{cases}$

证明 (1) 由于α为$GF(q^m)$中本原元，则$GF(q^m)=\{0,\ 1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^{q^m-2}\}$。又$n=q^m-1$，故$x^n-1=x^{q^m-1}-1=(x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{q^m-2})=(x-1)\prod_{s\in A_m}M^{(s)}(x)$。由此可知，$A_m$中元素个数恰好为$x^n-1$在$GF(q)[x]$中不可约因式的个数减1（注意到$A_m$中不同元素对应的极小多项式不同）。

另一方面：$x^n-1=x^{q^m-1}-1=\prod_{d\mid q^m-1}\Phi_d(x)=\Phi_{d_1}(x)\Phi_{d_2}(x)\cdots\Phi_{d_t}(x)=\left(\prod_{j_1=1}^{\varphi(d_1)/m_{d_1}}\Phi_{j_1}(x)\right)\left(\prod_{j_2=1}^{\varphi(d_2)/m_{d_2}}\Phi_{j_2}(x)\right)\cdots\left(\prod_{j_t=1}^{\varphi(d_t)/m_{d_t}}\Phi_{j_t}(x)\right)$，（式中$d_1,\ d_2,\ \cdots,\ d_t$为$q^m-1$为全部相异正因子）。对每个$i$（$1\leq i\leq t$），$\Phi_{j_i}(x)$　$(1\leq j_i\leq\varphi(d_i)/m_{d_i})$是$GF(q)$上$m_{d_i}$次不可约多项式，它们的周期均为$d_i$，而$m_{d_i}$是满足$q^{m_{d_i}}\equiv 1\ mod\ d_i$成立的最小正整数（以后我们称$\Phi_1(x)$，$\Phi_2(x)$，$\cdots$，$\Phi_{\varphi(d_i)/m_{d_i}}(x)$为属于$d_i$的不可约多项式）。由此可知$x^n-1$中不可约因式的个数为$\sum_{d\mid q^m-1}\dfrac{\varphi(d)}{m_d}$，于是$A_m=\sum_{d\mid q^m-1}\dfrac{\varphi(d)}{m_d}-1$.

(2) 设C_s为任意分圆陪集，其中最小元为a_s，则$a_s\in A_m$。由于α^s与α^{a_s}对应的极小多项式相同，故$M^{(s)}(x)=M^{(a_s)}(x)$，其周期为$\dfrac{q^m-1}{(s,\ q^m-1)}\triangleq t_s$，故$M^{(s)}(x)$是属于$t_s$的不可约多项式，从而$m_s=\deg M^{(s)}(x)=m_{t_s}$，这里$m_{t_s}$是满足$q^{m_{t_s}}\equiv 1 \bmod t_s$成立的最小正整数。又$t_s\mid q^m-1$，则$q^m\equiv 1 \bmod t_s$，从

而 $q^{(m,m_{t_s})}\equiv 1 \bmod t_s$, 由 m_{t_s}的最小性, $(m, m_{t_s}) = m_{t_s}$, 于是 $m_{t_s} \mid m$, 即 $m_s \mid m$.

(3) 对任意 k $(1\leq k\leq m)$, 如果 $k \nmid m$, 由 (2) 可知 $y_k = 0$, 如果 $k \mid m$, 则 y_k 即为 $(x^n - 1) / (x - 1)$ 中次数为 k 的不可约因式的个数 $\sum\limits_{\substack{d \mid q^m-1\\ d\neq 1\\ m_d = k}} \dfrac{\varphi(d)}{m_d}$.

例**1** 当 $q = 5$, $m = 2$时, $q^m - 1 = 24$的全部正因子为 $d_1 = 1$, $d_2 = 2$, $d_3 = 3$, $d_4 = 4$, $d_5 = 6$, $d_6 = 8$, $d_7 = 12$, $d_8 = 24$. 相应的 m_d 为: $m_{d_1} = m_{d_2} = m_{d_4} = 1$, $m_{d_3} = m_{d_5} = m_{d_6} = m_{d_7} = m_{d_8} = 2$, 于是以 $q^m - 1$为模的分圆陪集着 A_m 中元素个数 $= \sum\limits_{d\mid 24} \dfrac{\varphi(d)}{m_d} - 1 = 13$. 其中长度为1的分圆陪集个数为3, 长度为2的分圆陪集个数为10。

文 [4] 将模 $q^m - 1$的分圆陪集对应到模 q 的纯轮换的状态图中圈, 由此得出模 $q^m - 1$的分圆陪集首中元素个数为 $A_m = \dfrac{1}{m}\sum\limits_{d\mid m} q^{\frac{m}{d}}\varphi(d) - 2$. 于是我们有:

推论**1** $\dfrac{1}{m}\sum\limits_{d\mid m} q^{\frac{m}{d}}\varphi(d) - 1 = \sum\limits_{d\mid q^{m_d}-1} \dfrac{\varphi(d)}{m_d}$, 其中 m_d 是满足 $q^{m_d}\equiv 1 \bmod d$ 成立的最小正整数。

推论**2** 当 m 为素数时, 长度为1的分圆陪集的个数是 $\sum\limits_{\substack{d\mid q-1\\ d\neq 1}}\varphi(d)$, 而长度为 m 的分圆陪集的个数是 $\dfrac{1}{m}\sum\limits_{\substack{d\mid q^m-1\\ d\nmid q-1}}\varphi(d)$.

由推论2可知文 [3] 中引理3是错误的, 从而文 [3] 中定理2也是错误的, 事实上例1是文 [3] 中引理3的一个反例。

2 狭义本原 BCH 码的维数

设 C 为 $GF(q)$ 上设计距离为 δ 的狭义本原 BCH 码, 生成多项式为 $g(x)$, 校验多项式为 $h(x) = (x^n - 1) / g(x)$, 我们称校验多项式的次数 k 为码 C 的维数。

引理**4**[3] (1) 狭义本原 BCH 码的设计距离 δ 是某个分圆陪集首。(2) 任意一个分圆陪集首必是某个狭义本原 BCH 码的设计距离。

定理**2** 设 $A(m, \delta) = \{i \mid i\in A_m 1 \leq i\leq \delta - 1\}$, 则 q 元域上设计距离为 δ 的狭义本原 BCH 码 C 的维数 $\dim C = q^m - 1 - \sum\limits_{i\in A(m,\delta)} m_{t_i}$, 其中 $t_i = \dfrac{q^m - 1}{(i, q^m - 1)}$, 而 m_{t_i}是满足 $q^{m_{t_i}}\equiv 1 \bmod t_i$ 成立的最小正整数。

证明 由于狭义本原 BCH 码 C 的设计距离为 δ, 由引理4, $\delta\in A_m$. 若 $g(x)$ 为码 C 的生成多项式, 则 $g(\alpha) = g(\alpha^2) = \cdots = g(\alpha^{\delta-1}) = 0$, 但 $g(\alpha^{\delta}) \neq 0$, 于是 $M^{(i)}(x) \nmid g(x)$ $(1\leq i\leq \delta - 1)$, 但 $M^{(\delta)}(x) \mid g(x)$。又由于 $\delta\in A_m$, 故 $M^{(\delta)}(x)$ 与 $M^{(1)}(x)$, $M^{(2)}(x)$, $\cdots$, $M^{(s-1)}(x)$ 互异, 从而可取 $g(x) = l.c.m[m^{(1)}(x), M^{(2)}(x), \cdots, M^{(\delta-1)}(x)]$, 于是 $\dim C = \deg h(x) = n - \deg g(x) = q^m - 1 - \sum\limits_{i\in A(m,\delta)} \deg M^{(i)}(x)$。因为对每个 $i\in A(m, \delta)$, $M^{(i)}(x)$ 的周期为 $t_i = \dfrac{q^m - 1}{(i, q^m - 1)}$, 从而 $M^{(i)}(x)$ 必是属于 t_i 的某个不可约多项式, 故 $\deg M^{(i)}(x) = m_{t_i}$, 于是 $\dim C = q^m - 1 - \sum\limits_{i\in A(m,\delta)} m_{t_i}$

例**2** 当 $q = 5$, $m = 2$时, $A_m = \{1, 2, 3, 4, 6, 7, 8, 9, 12, 13, 14, 18, 19\}$, 则设计距离为 $\delta = 12$的狭义本原 BCH 码的维数为:

$$\dim C = q^m - 1 - \sum_{i\in A(m,\delta)} m_{t_i} = 25 - 1 - 7\times 2 - 1 = 9$$

推论**3** 当 m 为素数时, 设计距离为 δ 的狭义本原 BCH 码 C 的维数为:

$$\dim C = q^m - 1 - m \sum_{\substack{i\in A(m,\delta)\\ t_i \mid q-1}} 1 - \sum_{\substack{i\in A(m,\delta)\\ t_i \nmid q-1}} 1$$

推论**4** 当 m 为素数时, 如果 $\delta - 1 < q^{m-1} + q^{m-2} + \cdots + 1$, 则 $\dim C = q^m - 1 - m\sum\limits_{i\in A(m,\delta)} 1 = q^m - 1 - m\ A\ (m, \delta)$.

下面我们给出计算设计距离为 δ 的 q 元狭义本原 BCH 码的维数的算法:

Step1: 输入两个正整数 q 和 m, 其中 q 为素数或素数的幂;

Step2: 计算 q^m-1 的全部相异正因子 $d_1, d_2, \cdots, d_t$;

Step3: 对每个正因子 d_i $(1\leq i\leq t)$, 计算 m_{d_i}, m_{d_i} 是使得 $q^{m_{d_i}}\equiv 1 \bmod d_i$ 成立的最小正整数;

Step4: 对每个正整数 s $(1\leq s\leq \delta-1)$, 用欧氏算法计算 (s, q^m-1), 从而得到 $t_s=\dfrac{q^m-1}{(s, q^m-1)}$;

Step5: 置 $l=0$;

Step6: 对每个正整数 s $(1\leq s\leq \delta-1)$, 判定 s 是否为模 q^m-1 的分圆陪集首, 如果是, 则 $l=l+m_{t_s}$, 否则 $l=l$。

则 BCH 码的维数 $\dim C=q^m-1-l$.

上述算法不足之处在于预先知道模 q^m-1 的分圆陪集首集 A_m, 但分圆陪集的首集 A_m 可以按文[4]中方法得到, 该算法的实用之处在于它可以确定给定设计距离为 δ 的 BCH 码应具有的维数, 从而可以选取适当的校验多项式来生成所需的 BCH 码。

3 狭义本原 BCH 码的周期分布

定义4 设 C 为 $GF(q)$ 上 $[n, k]$ —循环码, $c=(c_0, c_1, \cdots, c_{n-1})\in C$, c 的循环置换定义为: $s(c)=(c_1, c_2, \cdots, c_{n-1}, c_0)$, 如果 $s^r(c)=c$. 则称 r 为码字 c 的周期, 使得 $s^r(c)=c$ 成立的最小正整数称为码字 c 的最小周期。

定义5 设 C 为 $GF(q)$ 上 $[n, k]$ —循环码, C 中最小周期为 t 的码字数目记为 A_t $(t=1, 2, \cdots, n)$, 而周期为 t 的码字数目记为 B_t $(t=1, 2, \cdots, n)$, 则称非负整数序列 $\{A_1, A_2, \cdots, A_n\}$ 和 $\{B_1, B_2, \cdots, B_n\}$ 分别为码 C 的最小周期分布与周期分布。

易知循环码的最小周期分布 $\{A_1, A_2, \cdots, A_n\}$ 与周期分布 $\{B_1, B_2, \cdots, B_n\}$ 之间具有如下关系: $B_t=\sum_{r\mid t} A_r$, $A_t=\sum_{r\mid t} u\left(\frac{t}{r}\right) B_r$, 其中 $u(\ )$ 为 Möbus 函数。

引理5[5] 如果 $h(x)$ 是 $GF(q)$ 上某个 $[n, k]$ 循环码 C 的校验多项式, 则码 C 的最小周期分布 $\{A_1, A_2, \cdots, A_n\}$ 和周期分布 $\{B_1, B_2, \cdots, B_n\}$ 为: $B_r=q^{\deg[(h(x), x^r-1)]}$ $(1\leq r\leq n)$, $A_r=\sum_{r\mid t} u\left(\frac{t}{r}\right) q^{\deg[(h(x), x^r-1)]}$ $(1\leq t\leq n)$

引理6 对 n 的每个正因子 d_i, 如果 $d_i \mid r$ 则 $(\Phi_{d_i}(x), x^r-1)=\Phi_{d_i}(x)$, 否则 $(\Phi_{d_i}(x), x^r-1)=1$.

证明 如果 $d_i \mid r$, 由于 $x^r-1=\prod_{d\mid r}\Phi_d(x)$, 于是 $\Phi_{d_i}(x) \mid x^r-1$, 从而 $(\Phi_{d_i}(x), x^r-1)=\Phi_{d_i}(x)$. 如果 $d_i \nmid r$, 则 $(\Phi_{d_i}(x), x^r-1)=1$, 否则若 $(\Phi_{d_i}(x), x^r-1)\neq 1$, 则存在 $GF(q)$ 上不可约多项式 $p(x)$, 使得 $p(x) \mid (\Phi_{d_i}(x), x^r-1)$, 由 $p(x) \mid \Phi_{d_i}(x)$, 可知 $p(x)$ 的周期为 d_i, 又 $p(x) \mid x^r-1$, 故 $x^r\equiv 1 \bmod p(x)$, 于是 $d_i \mid r$, 矛盾!

定理3 设 C 是 $GF(q)$ 上设计距离为 δ 的狭义本原 BCH 码, 其生成多项式 $g(x)=l.c.m(M^{(1)}(x), M^{(2)}(x), \cdots, M^{(\delta-1)}(x))=\prod_{i\in A(m, \delta)} M^{(i)}(x)$, 设 $d_1, d_2, \cdots, d_t$ 是 q^m-1 的全部相异正因子, 在 $g(x)$ 的不可约因式中周期为 d_i 的不可约因式的个数为 l_i $(1\leq i\leq t)$, 即 $l_i=\{j \mid j\in A(m, \delta), (q^m-1)/(j, q^m-1)=d_i\}$, 则

(1) BCH 码 C 的周期分布 $\{B_1, B_2, \cdots, B_n\}$ 为: $B_r=q^{k_r}$ $(1\leq r\leq n)$,

其中 $k_r=\sum_{\substack{d_i \mid r\\ i=1, 2, \cdots, t}} (\varphi(d_i)-l_i m_{d_i})$

(2) BCH 码 C 的对偶码的周期分布 $\{\bar{B}_1, \bar{B}_2, \cdots, \bar{B}_n\}$ 为: $\bar{B}_r=q^{\bar{k}_r}$ $(1\leq r\leq n)$,

其中 $\bar{k}_r=\sum_{\substack{d_i \mid r\\ i=1, 2, \cdots, t}} l_i m_{d_i}$

证明 (1) 由于 $x^n-1=x^{q^m-1}-1=\prod_{d\mid q^m-1}\varphi(x)=\varphi_{d_1}(x)\varphi_{d_2}(x)\cdots\varphi_{d_t}(x)$，如果 $g(x)=\prod_{i\in A(m,\delta)}M^{(i)}(x)$ 中周期为 d_i 的不可约因式的个数为 l_i $(i=1,2,\cdots,t)$，则因为 $h(x)=(x^{q^m-1}-1)/g(x)$，故 $h(x)$ 中属于 d_i 的不可约因式个数为 $(\frac{\varphi(d_i)}{m_{d_i}}-l_i)$，其中 m_{d_i} 是满足 $q^{m_{d_i}}\equiv 1 \bmod m_{d_i}$ 成立的最小正整数。而由引理6，$(\varphi_{d_i}(x),x^r-1)=\begin{cases}\varphi_{d_i}(x) & \text{若 } d_i \mid r\\ 1 & \text{若 } d_i \nmid r\end{cases}$，从而 $k_r=\deg(h(x),x^r-1)=\sum_{\substack{d_i\mid r\\ i=1,2,\cdots,t}}(\frac{\varphi(d_i)}{m_{d_i}}-l_i)$ $m_{d_i}=\sum_{\substack{d_i\mid r\\ i=1,2,\cdots,t}}(\varphi(d_i)-l_i m_{d_i})$

(2) 注意到 BCH 码的对偶码的校验多项式恰好为 $g(x)$，即可得出结论。

例**3** 当 $q=5$，$m=2$时，设 C 是 $GF(q)$ 上设计距离为 $\delta=12$的狭义本原 BCH 码，此时模 q^m-1 的分圆陪集首集 $A_m=\{1,2,3,4,6,7,8,9,12,13,14,18,19\}$，$A(m,\delta)=\{1,2,3,4,6,7,8,9\}$。故在 $g(x)=\prod_{i\in A(m,\delta)}M^{(i)}(x)$ 分解式中周期分别1，2，3，4，6，8，12，24的不可约因式个数依次是0，0，1，1，1，2，1，2，从而 $h(x)$ 的分解式中周期分别为1，2，3，4，6，8，12，24的不可约因式的个数依次是1，1，0，1，0，0，1，2，于是 $k_1=1$，$k_2=2$，$k_3=1$，$k_4=3$，$k_5=1$，$k_6=2$，$k_7=1$，$k_8=3$，$k_9=1$，$k_{10}=2$，$k_{11}=1$，$k_{12}=5$，$k_{13}=1$，$k_{14}=2$，$k_{15}=1$，$k_{16}=3$，$k_{17}=1$，$k_{18}=2$，$k_{19}=1$，$k_{20}=3$，$k_{21}=1$，$k_{22}=2$，$k_{23}=1$，$k_{24}=9$，于是5元域上设计距离为12的 [24，9] – BCH 码的周期分布为 $B_1=B_3=B_5=B_7=B_9=B_{11}=B_{13}=B_{15}=B_{17}=B_{19}=B_{21}=B_{23}=5$，$B_2=B_6=B_{10}=B_{14}=B_{18}=B_{22}=5^2$，$B_4=B_8=B_{16}=B_{20}=5^3$，$B_{12}=5^5$，$B_{24}=5^9$。

参考文献

1 Macwilliams F J, Sloane N J A. The Theory of Error– Correcting Codes, Amsterdam: North– Holland, Publishing Company, 1997: 201～267

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

3 岳殿武等. 关于 q 元 BCH 码的维数与最小距离. 电子科学学刊，1996，18 (3)：263～269

4 王建宇. 循环陪集首集与Goppa 码，Alternant 码最小距离下限. 通信学报，1994，15 (1)：107～112

5 符方伟等. 循环码周期分布新的计算公式. 通信学报，1996，17 (2)：1～6

6 王新梅等. 纠错码—原理与方法. 西安：西安电子科技大学出版社，1991

7 Lidl R，Niederreiter H. Finite Field，Addison– Wesley Publishing Company，Canada，1983