Pure Mathematics 理论数学, 2018, 8(4), 383-397
Published Online July 2018 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2018.84052

Hans汉斯

Repeated-Root Constacyclic Codes of Length $klmp^n$ over a Finite Field

Jiamei Zhou, Xilin Tang

School of Mathematics, South China University of Technology, Guangzhou Guangdong
Email: xilintang2016@sina.com

Received: Jun. 23rd, 2018; accepted: Jul. 9th, 2018; published: Jul. 17th, 2018

Abstract

Constacyclic codes play an important role in coding theory for their abundant algebraic structures which lead to high efficiency in decoding procedure by simple shift registers. In this paper, for different odd primes k, l, m and p, we obtain generator polynomials of constacyclic codes of length $klmp^n$ over finite field F_q, where char $F_q = p$.

Keywords

Constacyclic Codes, Generator Polynomials, Cyclotomic Cosets

在有限域上构造长度为$klmp^n$的常循环码

周佳美，唐西林

华南理工大学数学学院，广东 广州
Email: xilintang2016@sina.com

收稿日期：2018年6月23日；录用日期：2018年7月9日；发布日期：2018年7月17日

摘　要

常循环码在编码理论中起着重要的作用，它可以通过简单的移位寄存器来提高编码过程的效率。在本篇文章中，对于不同的奇素数k，l，m和p，我们得到了在F_q上长度为$klmp^n$的常循环码的生成多项式，其中p为F_q的特征。

关键词

常循环码，生成多项式，分圆陪集

文章引用: 周佳美, 唐西林. 在有限域上构造长度为 $klmp^n$ 的常循环码[J]. 理论数学, 2018, 8(4): 383-397.
DOI: 10.12677/pm.2018.84052

1. 引言

常循环码构成了循环码的显著推广，因此在编码理论中形成了一类重要的线性码。而且，常循环码也有实际的应用程序，因为它们可以用移位寄存器进行编码。

令 F_q 是一个特征为 p 的有限域。在 F_q 上一个长度为 n 的循环码是商环 $F_q[x]/\langle x^n-1\rangle$ 的理想，其中 $g(x)$ 是首一多项式并且满足 $g(x)|(x^n-1)$。作为循环码的泛化，对于 F_q 中任意的非零元素 λ， F_q 上一个长度为 n 的 λ 常循环码为商环 $F_q[x]/\langle x^n-\lambda\rangle$ 的理想 $\langle g(x)\rangle$，其中 $g(x)$ 是首一多项式并且满足 $g(x)|(x^n-\lambda)$。

常循环码在[1] [2] [3]中已经得到了很多的基本结果，更进一步地，长度为 $2p^s$， $3p^s$， $6p^s$ 的常循环码在[4] [5] [6]中已经进行了很好的研究。[7]进一步得到了长度为 lp^s 的常循环码。在此基础上，长度为 $2l^m p^n$ 的常循环码的生成多项式的问题在[8]中得到了解决。[9]得到了更为一般化的长度为 $kl^a p^b$ 的常循环码。

在本文中，我们主要得到在 F_q 上长度为 $klmp^n$ 的重根常循环码，其中 k，l，m，p 为不同的奇素数，并且 p 为 F_q 的特征。在第二部分，给出了我们需要的一些基本结果。在第三部分，对于任意的 $\lambda\in F_q^*$，我们给出了 $x^{klmp^n}-\lambda$ 的不可约分解。最后，我们得到了在 F_q 上长度为 $klmp^n$ 的常循环码的生成多项式。

2. 预备知识

定义 2.1 令 n 是一个正整数。对于 F_q^* 中的任意元素 λ 和 μ，如果多项式 $\lambda x^n-\mu$ 在 F_q 中有一个根，那么我们称 λ 与 μ 在 F_q^* 中 n 等价，记为 $\lambda\sim_n\mu$。

命题 2.2 [8]对 F_q^* 中的任意元素 λ 和 μ，下面的四个陈述是相互等价的：

1) $\lambda^{-1}\mu\in\langle\xi^n\rangle$，其中 ξ 是 F_q 的本原元。

2) $(\lambda^{-1}\mu)^d=1$，其中 $d=\dfrac{q-1}{\gcd(n,q-1)}$。

3) λ 与 μ 在 F_q^* 中 n 等价，即存在一个元素 $a\in F_q^*$ 使得 $a^n\lambda=\mu$。

4) 存在一个元素 $a\in F_q^*$ 使得

$$\varphi_a: F_q[x]/\langle x^n-\mu\rangle\to F_q[x]/\langle x^n-\lambda\rangle$$
$$f(x)\to f(ax)$$

是一个 F_q 代数同构。

特别地，在 F_q^* 上的 n 等价类的个数等于 $\gcd(n,q-1)$。

引理 2.3 [10]对于任意的 $\lambda\in F_q^*$，如果 $\gcd(ord(\lambda),n)=1$，那么存在一个整数 s 使得 $\lambda^{ns+1}=1$。

由定义 2.1，如果 $\lambda\in F_q^*$ 满足 $\gcd(ord(\lambda),n)=1$，那么 $\lambda\sim_n 1$ 并且 λ^s 是 $\lambda x^n-1=0$ 的一个根。根据命题 2.2 (4)中的表述我们有 $a=\lambda^s$，由于 s 和 $ord(\lambda)$ 互素，因此 $ord(a)=ord(\lambda)$。

引理 2.4 [10]令 k，l，m 为不同的素数，且 q 为一个素数的幂次。令 $\gcd(e,f)=d$。那么 $ord_{kl}(q)=\dfrac{ef}{d}$ 且所有不同的 q 模 kl 的分圆陪集为 $C_0=\{0\}$，

$$C\left(g_1^i,0\right)=\left\{\theta\left(g_1^i,0\right),\theta\left(g_1^i,0\right),\cdots,\theta\left(g_1^i,0\right)q^{e-1}\right\}\left(\mathrm{mod}\,kl\right),$$

$$C\left(0,g_2^j\right)=\left\{\theta\left(0,g_2^j\right),\theta\left(0,g_2^j\right)q,\cdots,\theta\left(0,g_2^j\right)q^{f-1}\right\}\left(\mathrm{mod}\,kl\right),$$

$$C\left(g_1^i,g_2^jq^t\right)=\left\{\theta\left(g_1^i,g_2^jq^t\right),\theta\left(g_1^i,g_2^jq^t\right)q,\cdots,\theta\left(g_1^i,g_2^jq^t\right)q^{\frac{ef}{d}-1}\right\}\left(\mathrm{mod}\,kl\right).$$

其中 $0\le i\le\frac{k-1}{e}-1$，$0\le j\le\frac{l-1}{f}-1$，$0\le t\le d-1$。

引理 2.5 [11]令整数 $t\ge 2$ 并且 $a\in F_q^*$。那么二项式 x^t-a 在 $F_q\left[x\right]$ 上不可约当且仅当满足下面的两个条件：

1) 在 F_q^* 中，t 的每一个素因子能够整除 a 的阶 e，但不能整除 $\frac{q-1}{e}$；

2) 如果 $t\equiv 0\left(\mathrm{mod}\,4\right)$，那么 $q\equiv 1\left(\mathrm{mod}\,4\right)$。

假设 $f\left(x\right)\in F_q\left[x\right]$ 是首项系数 $a_n\ne 0$ 的多项式。我们把首一多项式 $a_n^{-1}f\left(x\right)$ 记为 $\widehat{f\left(x\right)}$。

3. 主要结果

为了表述需要，我们给出下面的一些记号：

- $F_q^*=\left\langle\xi\right\rangle$；
- $ord_k\left(q\right)=e$； $ord_l\left(q\right)=f$； $ord_m\left(q\right)=g$；
- $Z_k^*=\left\langle g_1\right\rangle$； $Z_l^*=\left\langle g_2\right\rangle$； $Z_m^*=\left\langle g_3\right\rangle$；
- $\gcd\left(e,f\right)=d_1$， $\gcd\left(e,g\right)=d_2$， $\gcd\left(f,g\right)=d_3$， $\gcd\left(e,f,g\right)=d$。

由中国剩余定理，我们可以定义一个从 $Z_k\times Z_l\times Z_m$ 到 Z_{klm} 的同构，记为 φ。

定理 3.1 令 k, l, m 为不同的奇素数，并且 q 为一个素数的幂次。根据 $\gcd\left(e,f\right)=d_1$，$\gcd\left(e,g\right)=d_2$，$\gcd\left(f,g\right)=d_3$，$\gcd\left(e,f,g\right)=d$，那么 $ord_{kl}\left(q\right)=\frac{ef}{d_1}$，$ord_{km}\left(q\right)=\frac{eg}{d_2}$，$ord_{lm}\left(q\right)=\frac{fg}{d_3}$，$ord_{klm}\left(q\right)=\frac{efg}{d^2}$ 并且所有不同的 q 模 klm 的分圆陪集为 $C_0=\left\{0\right\}$，

$$C_{\left(g_1^h,0,0\right)}=\left\{\phi\left(g_1^h,0,0\right),\phi\left(g_1^h,0,0\right)q,\cdots,\phi\left(g_1^h,0,0\right)q^{e-1}\right\}\left(\mathrm{mod}\,klm\right),$$

$$C_{\left(0,g_2^r,0\right)}=\left\{\phi\left(0,g_2^r,0\right),\phi\left(0,g_2^r,0\right)q,\cdots,\phi\left(0,g_2^r,0\right)q^{e-1}\right\}\left(\mathrm{mod}\,klm\right),$$

$$C_{\left(0,0,g_3^t\right)}=\left\{\phi\left(0,0,g_3^t\right),\phi\left(0,0,g_3^t\right)q,\cdots,\phi\left(0,0,g_3^t\right)q^{g-1}\right\}\left(\mathrm{mod}\,klm\right),$$

$$C_{\left(g_1^h,g_2^rq^{s_1},0\right)}=\left\{\phi\left(g_1^h,g_2^rq^{s_1},0\right),\phi\left(g_1^h,g_2^rq^{s_1},0\right)q,\cdots,\phi\left(g_1^h,g_2^rq^{s_1},0\right)q^{\left(\frac{ef}{d_1}-1\right)}\right\}\left(\mathrm{mod}\,klm\right),$$

$$C_{\left(g_1^h,0,g_3^tq^{s_2}\right)}=\left\{\phi\left(g_1^h,0,g_3^tq^{s_2}\right),\phi\left(g_1^h,0,g_3^tq^{s_2}\right)q,\cdots,\phi\left(g_1^h,0,g_3^tq^{s_2}\right)q^{\left(\frac{eg}{d_2}-1\right)}\right\}\left(\mathrm{mod}\,klm\right),$$

$$C_{\left(0,g_2^r,g_3^tq^{s_3}\right)}=\left\{\phi\left(0,g_2^r,g_3^tq^{s_3}\right),\phi\left(0,g_2^r,g_3^tq^{s_3}\right)q,\cdots,\phi\left(0,g_2^r,g_3^tq^{s_3}\right)q^{\left(\frac{fg}{d_3}-1\right)}\right\}\left(\mathrm{mod}\,klm\right),$$

$$C_{\left(g_1^h,g_2^rq^{s'},g_3^tq^s\right)}=\left\{\phi\left(g_1^h,g_2^rq^{s'},g_3^tq^s\right),\phi\left(g_1^h,g_2^rq^{s'},g_3^tq^s\right)q,\cdots,\phi\left(g_1^h,g_2^rq^{s'},g_3^tq^s\right)q^{\left(\frac{efg}{d^2}-1\right)}\right\}\left(\mathrm{mod}\,klm\right).$$

其中 $0\le h\le\frac{k-1}{e}-1$，$0\le r\le\frac{l-1}{f}-1$，$0\le t\le\frac{m-1}{g}-1$，$0\le s_1\le d_1-1$，$0\le s_2\le d_2-1$，$0\le s_3\le d_3-1$，$0\le s'\le d-1$，$0\le s\le d-1$。

证明假设 $C_{\left(g_1^h,g_2^rq^{s_1},0\right)}=C_{\left(g_1^{h'},g_2^{r'}q^{s_1'},0\right)}$，其中 h,h',r,r',s_1,s_1' 都为整数且满足 $0\le h,h'\le\frac{k-1}{e}-1$，$0\le r,r'\le\frac{l-1}{f}-1$，$0\le s_1,s_1'\le d_1-1$。因此存在整数 v，$0\le v\le\frac{ef}{d_1}-1$，使得

$$\phi\left(g_1^h,g_2^rq^{s_1},0\right)=\phi\left(g_1^h,g_2^rq^{s_1},0\right)q^v.$$

由 ϕ 是一个同构，我们能得到下面的条件：

$$g_1^h\equiv g_1^{h'}q^v\left(\mathrm{mod}\,k\right)\tag{1}$$

$$g_1^rq^{s_1}\equiv g_2^rq^{s_1'}q^v\left(\mathrm{mod}\,l\right)\tag{2}$$

因为 $q^e\equiv1\left(\mathrm{mod}\,k\right)$，由条件(1)可得 $g_1^{(h-h')e}\equiv1\left(\mathrm{mod}\,k\right)$。因此 $\left(k-1\right)\left|\left(h-h'\right)e\right.$。再根据 $0\le h,h'\le\frac{k-1}{e}-1$ 可得 $h=h'$。由此可得，$q^v\equiv1\left(\mathrm{mod}\,k\right)$。因此 $e\left|v\right.$，从而 $d_1\left|v\right.$。同样地，由条件(2)得到 $g_2^{(r-r')f}\equiv1\left(\mathrm{mod}\,l\right)$。因此 $\left(l-1\right)\left|\left(r-r'\right)f\right.$。由于 $0\le r,r'\le\frac{l-1}{f}-1$，我们可以得到 $r=r'$。由此可得，$q^{s_1'-s_1+v}\equiv1\left(\mathrm{mod}\,l\right)$。因此 $f\left|s_1'-s_1+v\right.$。再根据 $d_1\left|f\right.$ 和 $d_1\left|v\right.$ 可以得到 $d_1\left|s_1'-s_1\right.$。由于 $0\le s_1,s_1'\le d_1-1$，所以 $s_1=s_1'$。把 $s_1=s_1'$ 代入 $f\left|s_1'-s_1+v\right.$ 可得 $f\left|v\right.$，由此可得 $\frac{ef}{d_1}\left|v\right.$。再根据 $0\le v\le\frac{ef}{d_1}-1$ 可得 $v=0$。

那么 $C_{\left(g_1^h,g_2^rq^{s_1},0\right)}$，$0\le h\le\frac{k-1}{e}-1$，$0\le r\le\frac{l-1}{f}-1$，$0\le s_1\le d_1-1$ 为 q 模 klm 的互不相同的陪集。同理可证 $C_{\left(g_1^h,0,g_3^tq^{s_2}\right)}$，$C_{\left(0,g_2^r,g_3^tq^{s_3}\right)}$，$0\le h\le\frac{k-1}{e}-1$，$0\le r\le\frac{l-1}{f}-1$，$0\le t\le\frac{m-1}{g}-1$，$0\le s_2\le d_2-1$，$0\le s_3\le d_3-1$ 也为 q 模 klm 的互不相同的陪集。

下面假设 $C_{\left(g_1^{h_4},g_2^{r_4}q^{s_4'},g_3^{t_4}q^{s_4}\right)}=C_{\left(g_1^{h_5},g_2^{r_5}q^{s_5'},g_3^{t_5}q^{s_5}\right)}$，其中 $0\le h_4,h_5\le\frac{k-1}{e}-1$，$0\le r_4,r_5\le\frac{l-1}{f}-1$，$0\le t_4,t_5\le\frac{m-1}{g}-1$，$0\le s_4',s_5'\le d-1$，$0\le s_4,s_5\le d-1$。因此存在整数 ω，$0\le\omega\le\frac{efg}{d^2}-1$，使得

$$\phi\left(g_1^{h_4},g_2^{r_4}q^{s_4'},g_3^{t_4}q^{s_4}\right)=\phi\left(g_1^{h_5},g_2^{r_5}q^{s_5'},g_3^{t_5}q^{s_5}\right)q^{\omega}.$$

由 ϕ 是一个同构，我们能得到下面的条件：

$$g_1^{h_4}\equiv g_1^{h_5}q^{\omega}\left(\mathrm{mod}\,k\right)\tag{3}$$

$$g_2^{r_4}q^{s_4'}\equiv g_2^{r_5}q^{s_5'}q^{\omega}\left(\mathrm{mod}\,l\right)\tag{4}$$

$$g_3^{t_4}q^{s_4}\equiv g_3^{t_5}q^{s_5}q^{\omega}\left(\mathrm{mod}\,m\right)\tag{5}$$

由条件(3)可得到 $g_1^{(h_4-h_5)e}\equiv1\left(\mathrm{mod}\,k\right)$，因此 $\left(k-1\right)\left|\left(h_4-h_5\right)e\right.$。再根据 $0\le h_4,h_5\le\frac{k-1}{e}-1$ 可得 $h_4=h_5$。

由此可得， $q^{\omega}\equiv 1\left(\mathrm{mod}\,k\right)$。因此 $e\mid\omega$，从而 $d\mid\omega$。

由条件(4)可得到 $g_2^{(r_4-r_5)f}\equiv 1\left(\mathrm{mod}\,l\right)$，因此 $(l-1)\mid(r_4-r_5)f$。再根据 $0\le r_4,r_5\le\dfrac{l-1}{f}-1$ 可得 $r_4=r_5$。由此可得， $q^{s_5'-s_4'+\omega}\equiv 1\left(\mathrm{mod}\,l\right)$。因此 $f\mid s_5'-s_4'+\omega$，从而 $d\mid s_5'-s_4'+\omega$。又因为 $d\mid\omega$，所以 $d\mid s_5'-s_4'$。再根据 $0\le s_4',s_5'\le d-1$，可得 $s_4'=s_5'$。

由条件(5)可得到 $g_3^{(t_4-t_5)g}\equiv 1\left(\mathrm{mod}\,m\right)$，因此 $(m-1)\mid(t_4-t_5)g$。再根据 $0\le t_4,t_5\le\dfrac{m-1}{g}-1$ 可得 $t_4=t_5$。且由此可得 $q^{s_5-s_4+\omega}\equiv 1\left(\mathrm{mod}\,m\right)$。因此 $g\mid s_5-s_4+\omega$。再由 $d\mid g$ 与 $d\mid\omega$ 可得 $d\mid s_5-s_4$。从而由 $0\le s_4,s_5\le d-1$，可得 $s_4=s_5$。

我们根据 $e\mid\omega$ 并且 $\gcd(e,f,g)=d$，可得 $\dfrac{efg}{d^2}\mid\omega$。再根据 $0\le\omega\le\dfrac{efg}{d^2}-1$ 可得 $\omega=0$。从而我们得到 C_0，$C_{\left(g_1^h,0,0\right)}$，$C_{\left(0,g_2^r,0\right)}$，$C_{\left(0,0,g_3^t\right)}$，$C_{\left(g_1^h,g_2^rq^{s_1},0\right)}$，$C_{\left(g_1^h,0,g_3^tq^{s_2}\right)}$，$C_{\left(0,g_2^r,g_3^tq^{s_3}\right)}$，$C_{\left(g_1^h,g_2^rq^{s'},g_3^tq^{s}\right)}$ 均为 q 模 klm 不同的陪集，其中 $0\le h\le\dfrac{k-1}{e}-1$，$0\le r\le\dfrac{l-1}{f}-1$，$0\le t\le\dfrac{m-1}{g}-1$，$0\le s_1\le d_1-1$，$0\le s_2\le d_2-1$，$0\le s_3\le d_3-1$，$0\le s'\le d-1$，$0\le s\le d-1$。由于

$$\begin{aligned}&\left|C_0\right|+\sum_{h=0}^{\frac{k-1}{e}-1}\left|C_{\left(g_1^h,0,0\right)}\right|+\sum_{r=0}^{\frac{l-1}{f}-1}\left|C_{\left(0,g_2^r,0\right)}\right|+\sum_{t=0}^{\frac{m-1}{g}-1}\left|C_{\left(0,0,g_3^t\right)}\right|\\&+\sum_{h=0}^{\frac{k-1}{e}-1}\sum_{r=0}^{\frac{l-1}{f}-1}\sum_{s_1=0}^{d_1-1}\left|C_{\left(g_1^h,g_2^rq^{s_1},0\right)}\right|+\sum_{h=0}^{\frac{k-1}{e}-1}\sum_{t=0}^{\frac{m-1}{g}-1}\sum_{s_2=0}^{d_2-1}\left|C_{\left(g_1^h,0,g_3^tq^{s_2}\right)}\right|\\&+\sum_{r=0}^{\frac{l-1}{f}-1}\sum_{t=0}^{\frac{m-1}{g}-1}\sum_{s_3=0}^{d_3-1}\left|C_{\left(0,g_2^r,g_3^tq^{s_3}\right)}\right|+\sum_{h=0}^{\frac{k-1}{e}-1}\sum_{r=0}^{\frac{l-1}{f}-1}\sum_{t=0}^{\frac{m-1}{g}-1}\sum_{s'=0}^{d-1}\sum_{s=0}^{d-1}\left|C_{\left(g_1^h,g_2^rq^{s'},g_3^tq^{s}\right)}\right|=klm\end{aligned}$$

从而，我们就得到了所有 q 模 klm 的分圆陪集。

我们记 $C_{\rho_h}=C_{\left(g_1^h,0,0\right)}$，$C_{\rho_r}=C_{\left(0,g_2^r,0\right)}$，$C_{\rho_t}=C_{\left(0,0,g_3^t\right)}$，$C_{\chi_{j_1}}=C_{\left(g_1^h,g_2^rq^{s_1},0\right)}$，$C_{\chi_{j_2}}=C_{\left(g_1^h,0,g_3^tq^{s_2}\right)}$，$C_{\chi_{j_3}}=C_{\left(0,g_2^r,g_3^tq^{s_3}\right)}$，$C_{\vartheta_{h_r}}=C_{\left(g_1^h,g_2^rq^{s'},g_3^tq^{s}\right)}$。则 C_0，C_{ρ_h}，C_{ρ_r}，C_{ρ_t}，$C_{\chi_{j_1}}$，$C_{\chi_{j_2}}$，$C_{\chi_{j_3}}$，$C_{\vartheta_{h_r}}$ 为所有 q 模 klm 的分圆陪集，其中 $0\le h\le\dfrac{k-1}{e}-1$，$0\le r\le\dfrac{l-1}{f}-1$，$0\le t\le\dfrac{m-1}{g}-1$，$0\le j_1\le\dfrac{k-1}{e}\dfrac{l-1}{f}d_1$，$0\le j_2\le\dfrac{k-1}{e}\dfrac{m-1}{g}d_2$，$0\le j_3\le\dfrac{l-1}{f}\dfrac{m-1}{g}d_3$，$0\le h_r\le\dfrac{k-1}{e}\dfrac{l-1}{f}\dfrac{m-1}{g}d^2$。

为方便陈述，我们记 $T(x)=M_{\rho_h}(x)M_{\rho_r}(x)M_{\rho_t}(x)M_{\rho_{j_1}}(x)M_{\rho_{j_2}}(x)M_{\rho_{j_3}}(x)M_{\rho_{h_r}}(x)$，则

$$x^{klm}-1=(x-1)\prod_{h=0}^{\frac{k-1}{e}-1}\prod_{r=0}^{\frac{l-1}{f}-1}\prod_{t=0}^{\frac{m-1}{g}-1}\prod_{j_1=0}^{\frac{k-1}{e}\frac{l-1}{f}d_1}\prod_{j_2=0}^{\frac{k-1}{e}\frac{m-1}{g}d_2}\prod_{j_3=0}^{\frac{l-1}{f}\frac{m-1}{g}d_3}\prod_{h_r=0}^{\frac{k-1}{e}\frac{l-1}{f}\frac{m-1}{g}d^2}T(x)$$

定理 3.2 令 k,l,m 为不同的奇素数，并且 q 为一个素数的幂次。则由 $ord(f,g)=d_3$，$ord_{lm}(q)=\dfrac{fg}{d_3}$，$k\mid\dfrac{fg}{d_3}$ 可得 $ord_{lm}\left(q^k\right)=\dfrac{fg}{d_3k}$。

1) 若 $k\mid f$，$k\nmid g$。则所有不同的 q^k 模 lm 的分圆陪集为 $C_0=\{0\}$，

$$C'_{\left(g_2^u q^r,0\right)}=\left\{\theta\left(g_2^u q^r,0\right),\theta\left(g_2^u q^r,0\right)q^k,\cdots,\theta\left(g_2^u q^r,0\right)q^{k\left(\frac{f}{k}-1\right)}\right\}\left(\mathrm{mod}\, lm\right),$$

$$C_{\left(0,g_3^v\right)}=\left\{\theta\left(0,g_3^v\right),\theta\left(0,g_3^v\right)q,\cdots,\theta\left(0,g_3^v\right)q^{(g-1)}\right\}\left(\mathrm{mod}\, lm\right),$$

$$C_{\left(g_2^u,g_3^v q^w\right)q^r}=\left\{\theta\left(g_2^u,g_3^v q^w\right)q^r,\theta\left(g_2^u,g_3^v q^w\right)q^r q^k,\cdots,\theta\left(g_2^u,g_3^v q^w\right)q^r q^{k\left(\frac{fg}{d_3k}-1\right)}\right\}\left(\mathrm{mod}\, lm\right).$$

2) 若 $k\nmid f$， $k\mid g$。则所有不同的 q^k 模 lm 的分圆陪集为 $C_0=\{0\}$，

$$C_{\left(g_2^u q^r,0\right)}=\left\{\theta\left(g_2^u,0\right),\theta\left(g_2^u,0\right)q,\cdots,\theta\left(g_2^u,0\right)q^{(f-1)}\right\}\left(\mathrm{mod}\, lm\right),$$

$$C'_{\left(0,g_3^v\right)}=\left\{\theta\left(0,g_3^v\right),\theta\left(0,g_3^v\right)q^k,\cdots,\theta\left(0,g_3^v\right)q^{k\left(\frac{g}{k}-1\right)}\right\}\left(\mathrm{mod}\, lm\right),$$

$$C_{\left(g_2^u,g_3^v q^w\right)q^r}=\left\{\theta\left(g_2^u,g_3^v q^w\right)q^r,\theta\left(g_2^u,g_3^v q^w\right)q^r q^k,\cdots,\theta\left(g_2^u,g_3^v q^w\right)q^r q^{k\left(\frac{fg}{d_3k}-1\right)}\right\}\left(\mathrm{mod}\, lm\right).$$

3) 若 $k\mid f$， $k\mid g$。则所有不同的 q^k 模 lm 的分圆陪集为 $C_0=\{0\}$，

$$C'_{\left(g_2^u q^r,0\right)}=\left\{\theta\left(g_2^u q^r,0\right),\theta\left(g_2^u q^r,0\right)q^k,\cdots,\theta\left(g_2^u q^r,0\right)q^{k\left(\frac{f}{k}-1\right)}\right\}\left(\mathrm{mod}\, lm\right),$$

$$C'_{\left(0,g_3^v\right)}=\left\{\theta\left(0,g_3^v\right),\theta\left(0,g_3^v\right)q^k,\cdots,\theta\left(0,g_3^v\right)q^{k\left(\frac{g}{k}-1\right)}\right\}\left(\mathrm{mod}\, lm\right),$$

$$C_{\left(g_2^u,g_3^v q^w\right)q^r}=\left\{\theta\left(g_2^u,g_3^v q^w\right)q^r,\theta\left(g_2^u,g_3^v q^w\right)q^r q^k,\cdots,\theta\left(g_2^u,g_3^v q^w\right)q^r q^{k\left(\frac{fg}{d_3k}-1\right)}\right\}\left(\mathrm{mod}\, lm\right).$$

其中 $0\le u\le\frac{l-1}{f}-1$， $0\le v\le\frac{m-1}{g}-1$， $0\le w\le d_3$， $0\le r\le k-1$。

证明：假设 $C_{\left(g_2^{u_1},g_3^{v_1}q^{w_1}\right)q^{r_1}}=C_{\left(g_2^{u_2},g_3^{v_2}q^{w_2}\right)q^{r_2}}$，其中 $u_1,u_2,v_1,v_2,w_1,w_2,r_1,r_2$ 都为整数且满足 $0\le u_1,u_2\le\frac{l-1}{f}-1$，$0\le v_1,v_2\le\frac{m-1}{g}-1$， $0\le w_1,w_2\le d_3-1$， $0\le r_1,r_2\le k-1$。那么存在整数 s， $0\le s\le\frac{fg}{d_3k}-1$ 使得 $\theta\left(g_2^{u_1},g_3^{v_1}q^{w_1}\right)q^{r_1}=\theta\left(g_2^{u_2},g_3^{v_2}q^{w_2}\right)q^{r_2}q^{ks}$。

因为 θ 是一个同构，我们可以得到下面的条件：

1) $g_2^{u_1}q^{r_1}\equiv g_2^{u_2}q^{r_2}q^{ks}\left(\mathrm{mod}\, l\right)$

2) $g_3^{v_1}q^{w_1}q^{r_1}\equiv g_3^{v_2}q^{w_2}q^{r_2}q^{ks}\left(\mathrm{mod}\, m\right)$

因为 $q^f\equiv1\left(\mathrm{mod}\, l\right)$，由条件 1)可得 $g_2^{(u_2-u_1)f}\equiv1\left(\mathrm{mod}\, l\right)$。因此 $(l-1)\mid(u_1-u_2)f$。再根据 $0\le u_1,u_2\le\frac{l-1}{f}-1$ 可得 $u_1=u_2$。更进一步地可得，$q^{r_2-r_1+ks}\equiv1\left(\mathrm{mod}\, l\right)$。所以 $f\mid r_2-r_1+ks$，从而 $d_3\mid r_2-r_1+ks$。

由条件 2)可得，$g_3^{(v_1-v_2)g}\equiv1\left(\mathrm{mod}\, m\right)$。因此 $(m-1)\mid(v_1-v_2)g$。再根据 $0\le v_1,v_2\le\frac{m-1}{g}-1$ 可得 $v_1=v_2$。

更进一步地可得，$q^{w_2-w_1+r_2-r_1+ks}\equiv 1\pmod m$。所以 $g\mid w_2-w_1+r_2-r_1+ks$。又因为 $d_3\mid g$ 且 $d_3\mid r_2-r_1+ks$，所以 $d_3\mid w_2-w_1$。而 $0\le w_1,w_2\le d_3-1$，所以 $w_1=w_2$。

把 $u_1=u_2$，$v_1=v_2$，$w_1=w_2$ 代入到 1)和 2)中，我们可以得到

$$q^{r_1}\equiv q^{r_2}q^{ks}\pmod l,$$

$$q^{r_1}\equiv q^{r_2}q^{ks}\pmod m.$$

又因为 $\gcd(l,m)=1$，从而可以得到 $q^{r_1}\equiv q^{r_2}q^{ks}\pmod{lm}$。所以 $\frac{fg}{d_3}\mid r_2-r_1+ks$。又由于 $k\mid\frac{fg}{d_3}$，我们可以得到 $k\mid r_2-r_1+ks$，因此 $k\mid r_2-r_1$。再根据 $0\le r_1,r_2\le k-1$ 可得 $r_1=r_2$。再把 $r_1=r_2$ 代入 $\frac{fg}{d_3}\mid r_2-r_1+ks$ 可得 $\frac{fg}{d_3}\mid ks$，从而 $\frac{fg}{d_3k}\mid s$。再根据 $0\le s\le\frac{fg}{d_3k}-1$，可得 $s=0$。

从而我们说明了 $C_{\left(g_2^ug_3^vq^w\right)q^r}$，$0\le u\le\frac{l-1}{f}-1$，$0\le v\le\frac{m-1}{g}-1$，$0\le w\le d_3-1$，$0\le r\le k-1$ 为 q^k 模 lm 的互不相同的陪集。

并且对于情况(1)，我们有

$$\left|C_0\right|+\sum_{u=0}^{\frac{l-1}{f}-1}\sum_{r=0}^{k-1}\left|C'_{\left(g_2^uq^r,0\right)}\right|+\sum_{v=0}^{\frac{m-1}{g}-1}\left|C_{\left(0,g_3^v\right)}\right|+\sum_{u=0}^{\frac{l-1}{f}-1}\sum_{v=0}^{\frac{m-1}{g}-1}\sum_{w=0}^{d_3-1}\sum_{r=0}^{k-1}\left|C_{\left(g_2^ug_3^vq^w\right)q^r}\right|=klm.$$

从而当 $k\mid f$，$k\nmid g$ 时，C_0，$C'_{\left(g_2^uq^r,0\right)}$，$\left|C_{\left(0,g_3^v\right)}\right|$，$C_{\left(g_2^ug_3^vq^w\right)q^r}$ 为所有不同的 q^k 模 lm 的分圆陪集，其中 $0\le u\le\frac{l-1}{f}-1$，$0\le v\le\frac{m-1}{g}-1$，$0\le w\le d_3-1$，$0\le r\le k-1$。

同理可证情况(2)和情况(3)。

定理 3.3 令 k,l,m,p 为不同的奇素数，并且 p 为 F_q 的特征。假设 $k\mid q-1$，$\gcd(l,q-1)=\gcd(m,q-1)=1$。那么对任意的 $\lambda\in F_q^*$ 我们有 $\lambda\in\xi^{ilmp^n}\left\langle\xi^{klmp^n}\right\rangle$，其中 $0\le i\le klm-1$。而且

1) 当 $i=0$，即 $\lambda\in\left\langle\xi^{klmp^n}\right\rangle$ 时，

$$x^{klmp^n}-\lambda=\left(x-a_1^{-1}\right)^{p^n}\prod_{h=0}^{\frac{k-1}{e}-1}\prod_{r=0}^{\frac{l-1}{f}-1}\prod_{t=0}^{\frac{m-1}{g}-1}\prod_{j_1=0}^{\frac{k-1}{e}\frac{l-1}{f}d_1-1}\prod_{j_2=0}^{\frac{k-1}{e}\frac{m-1}{g}d_2-1}\prod_{j_3=0}^{\frac{l-1}{f}\frac{m-1}{g}d_3-1}\prod_{h_r=0}^{\frac{k-1}{e}\frac{l-1}{f}\frac{m-1}{g}d^2-1}\hat{T}\left(a_1x\right)^{p^n}$$

其中 $a_1\in F_q^*$ 并且满足 $\lambda a_1^{klmp^n}=1$。

2) 当 $i\ne 0$ 时，

(2.1)若 $k\nmid\frac{fg}{d_3}$，则

$$x^{klmp^n}-\lambda=\hat{A}\left(a_2x\right)^{p^n}\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\hat{B}_{uvw}\left(a_2x\right)^{p^n}\hat{C}_{uvw}\left(a_2x\right)^{p^n}\hat{D}_{uvw}\left(a_2x\right)^{p^n}.$$

其中 $A(x)=\prod_{j=0}^{k-1}\left(x-\pi_{ij}^{-1}\right)$，$B_{uvw}(x)=\prod_{j=0}^{k-1}\hat{M}_{\rho\left(g_2^u,0\right)}\left(\pi_{ij}x\right)$，$C_{uvw}(x)=\prod_{j=0}^{k-1}\hat{M}_{\rho\left(0,g_3^v\right)}\left(\pi_{ij}x\right)$，

$D_{uvw}(x)=\prod_{j=0}^{k-1}\hat{M}_{\rho\left(g_2^ug_3^vq^w\right)}\left(\pi_{ij}x\right)$。

$a_2 \in F_q^*$ 并且满足 $\lambda a_2^{klmp^n} = \xi^{ilmp^n}$， $\pi_{ij}^{lm}\pi^{ilm+j(q-1)} = 1$， π 和 $\pi_{ij}\,(0 \le j \le k-1)$ 分别为 F_{q^k} 中的 $k(q-1)$ 次和 $\dfrac{k(q-1)}{\gcd(k(q-1),i)}$ 次单位根。

(2.2)当 $k \mid \dfrac{fg}{d_3}$ 时，则有 $k \mid fg$

i) 若 $k \mid f$， $k \nmid g$ 则

$$x^{klmp^n} - \lambda = \hat{E}(a_2x)^{p^n} \prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\prod_{\eta=0}^{k-1}\hat{F}_{uvw\eta}(a_2x)^{p^n}\hat{G}_{uvw\eta}(a_2x)^{p^n}\hat{H}_{uvw\eta}(a_2x)^{p^n}.$$

其中 $E(x) = \prod_{j=0}^{k-1}\left(x - \pi_{ij}^{-1}\right)$， $F_{uvw\eta}(x) = \hat{M}_{\rho'\left(g_2^u,0\right)q^{\overline{\eta}}}\left(\pi_{ij_0}x\right)\hat{M}_{\rho'\left(g_2^u,0\right)q^{\overline{\eta+1}}}\left(\pi_{ij_1}x\right)\cdots\hat{M}_{\rho'\left(g_2^u,0\right)q^{\overline{\eta+k-1}}}\left(\pi_{ij_{k-1}}x\right)$，

$G_{uvw\eta}(x) = \prod_{j=0}^{k-1}\hat{M}_{\rho\left(0,g_3^v\right)}\left(\pi_{ij}x\right)$， $H_{uvw\eta}(x) = \hat{M}_{\rho\left(g_2^ug_3^vq^w\right)q^{\overline{\eta}}}\left(\pi_{ij_0}x\right)\hat{M}_{\rho\left(g_2^ug_3^vq^w\right)q^{\overline{\eta+1}}}\left(\pi_{ij_1}x\right)\cdots\hat{M}_{\rho\left(g_2^ug_3^vq^w\right)q^{\overline{\eta+k-1}}}\left(\pi_{ij_{k-1}}x\right)$。

ii) 若 $k \nmid f$， $k \mid g$。则

$$x^{klmp^n} - \lambda = \hat{E}(a_2x)^{p^n} \prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\prod_{\eta=0}^{k-1}\hat{I}_{uvw\eta}(a_2x)^{p^n}\hat{J}_{uvw\eta}(a_2x)^{p^n}\hat{H}_{uvw\eta}(a_2x)^{p^n}.$$

其中 $I_{uvw\eta}(x) = \prod_{j=0}^{k-1}\hat{M}_{\rho\left(g_2^u,0\right)}\left(\pi_{ij}x\right)$， $J_{uvw\eta}(x) = \hat{M}_{\rho'\left(0,g_3^v\right)q^{\overline{r}}}\left(\pi_{ij_0}x\right)\hat{M}_{\rho'\left(0,g_3^v\right)q^{\overline{r+1}}}\left(\pi_{ij_1}x\right)\cdots\hat{M}_{\rho'\left(0,g_3^v\right)q^{\overline{r+k-1}}}\left(\pi_{ij_{k-1}}x\right)$。

iii) 若 $k \mid f$， $k \mid g$。则

$$x^{klmp^n} - \lambda = \hat{E}(a_2x)^{p^n} \prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\prod_{\eta=0}^{k-1}\hat{F}_{uvw\eta}(a_2x)^{p^n}\hat{J}_{uvw\eta}(a_2x)^{p^n}\hat{H}_{uvw\eta}(a_2x)^{p^n}.$$

证明： 1) 若 $i=0$，即 $\lambda \in \left\langle \xi^{klmp^n} \right\rangle$，由命题 2.2(1)可得 $\lambda \sim_{klmp^n} 1$，所以存在 $a_1 \in F_q^*$ 使得 $\lambda a_1^{klmp^n} = 1$。又因为 $x^{klmp^n} - 1 = \left(x^{klm} - 1\right)^{p^n}$，所以

$$x^{klmp^n} - \lambda = \left(x - a_1^{-1}\right)^{p^n} \prod_{h=0}^{\frac{k-1}{e}-1}\prod_{r=0}^{\frac{l-1}{f}-1}\prod_{t=0}^{\frac{m-1}{g}-1}\prod_{j_1=0}^{\frac{k-1}{e}\frac{l-1}{f}d_1-1}\prod_{j_2=0}^{\frac{k-1}{e}\frac{m-1}{g}d_2-1}\prod_{j_3=0}^{\frac{l-1}{f}\frac{m-1}{g}d_3-1}\prod_{h_r=0}^{\frac{k-1}{e}\frac{l-1}{f}\frac{m-1}{g}d^2-1}\hat{T}(a_1x)^{p^n}.$$

2) 当 $i \ne 0$ 时，令 $\lambda \in \xi^{ilmp^n}\left\langle \xi^{klmp^n} \right\rangle$，其中 $0 \le i \le klm-1$。

则由命题 2.2 (1)可得 $\lambda \sim_{klmp^n} \xi^{ilmp^n}$，所以存在 $a_2 \in F_q^*$ 使得 $\lambda a_2^{klmp^n} = \xi^{ilmp^n}$。令 $\xi = \pi^k$，则 $\pi \in F_{q^k}$ 且 $ord(\pi) = k(q-1)$。因此

$$x^{klmp^n} - \xi^{ilmp^n} = \left(x^{klm} - \xi^{ilm}\right)^{p^n} = \left(x^{klm} - \pi^{iklm}\right)^{p^n} = \prod_{j=0}^{k-1}\left(x^{lm} - \pi^{ilm+j(q-1)}\right)^{p^n}.$$

又因为 $\gcd\left(ord\left(\pi^{ilm+j(q-1)}\right), lm\right) = 1$，由引理 2.3 可知 $\pi^{ilm+j(q-1)} \sim_{lm} 1$，所以存在 $\pi_{ij} \in F_{q^k}^*$ 使得 $\pi_{ij}^{lm}\pi^{ilm+j(q-1)} = 1$ 且 $ord(\pi_{ij}) = ord\left(\pi^{ilm+j(q-1)}\right) = \dfrac{k(q-1)}{\gcd(k(q-1),i)} = ord(\pi^i)$。

因为 $F_{q^k}^*$ 是一个有限循环群，所以存在整数 s_j 使得 $\pi_{ij} = \pi^{is_j}$，并且 s_j 满足 $\gcd\left(s_j, k(q-1)\right) = 1$。根据

$\pi_{ij}^{lm}\pi^{ilm+j(q-1)}=1$ 可得

$$-is_j lm \equiv ilm + j(q-1)\left(\bmod k(q-1)\right).$$

又因为 $\gcd\left(lm,k(q-1)\right)=1$，所以存在整数 w' 和 v' 使得 $w'lm+v'k(q-1)=1$。因此可得

$$-is_j \equiv i + jw'(q-1)\left(\bmod k(q-1)\right).$$

(2.1)当 $k\nmid\frac{fg}{d_3}$，则所有不同的 q^k 模 lm 的分圆陪集仍为 C_0，$C_{\left(g_2^u,0\right)}$，$C_{\left(0,g_3^v\right)}$，$C_{\left(g_2^u,g_3^v q^w\right)}$，其中 $0\le u\le\frac{l-1}{f}-1$，$0\le v\le\frac{m-1}{g}-1$，$0\le w\le d_3-1$。则

$$x^{lm}-\pi^{ilm+j(q-1)}=\left(x-\pi_{ij}^{-1}\right)\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\hat{M}_{\rho\left(g_2^u,0\right)}\left(\pi_{ij}x\right)\hat{M}_{\rho\left(0,g_3^v\right)}\left(\pi_{ij}x\right)\hat{M}_{\rho\left(g_2^u,g_3^v q^w\right)}\left(\pi_{ij}x\right).$$

所以

$$x^{klmp^n}-\xi^{ilmp^n}=\prod_{j=0}^{k-1}\left(x-\pi_{ij}^{-1}\right)^{p^n}\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\hat{M}_{\rho\left(g_2^u,0\right)}\left(\pi_{ij}x\right)^{p^n}\hat{M}_{\rho\left(0,g_3^v\right)}\left(\pi_{ij}x\right)^{p^n}\hat{M}_{\rho\left(g_2^u,g_3^v q^w\right)}\left(\pi_{ij}x\right)^{p^n}.$$

令 $\pi_{ij_s}^{-q}=\pi_{ij_{s+1}}^{-1}$，$0\le s\le k-1$。则

$$iq + j_s qw'(q-1)\equiv i + j_{s+1}w'(q-1)\left(\bmod k(q-1)\right).$$

因此

$$j_{s+1}\equiv j_s q + ilm\left(\bmod k\right).$$

令 $j_0=0$。那么对所有的 $0\le s\le k-1$，$j_s\equiv silm\left(\bmod k\right)$，且 $j_k=j_0=0$。又因为 $\gcd\left(ilm,k\right)=1$，故当 j 取遍 $[0,k-1]$ 时，$j_0,j_1,\cdots,j_{k-1}$ 取遍 Z_k。令 $A(x)=\prod_{j=0}^{k-1}\left(x-\pi_{ij}^{-1}\right)$，$B_{uvw}(x)=\prod_{j=0}^{k-1}\hat{M}_{\rho\left(g_2^u,0\right)}\left(\pi_{ij}x\right)$，$C_{uvw}(x)=\prod_{j=0}^{k-1}\hat{M}_{\rho\left(0,g_3^v\right)}\left(\pi_{ij}x\right)$，$D_{uvw}(x)=\prod_{j=0}^{k-1}\hat{M}_{\rho\left(g_2^u,g_3^v q^w\right)}\left(\pi_{ij}x\right)$。

$A(x)$ 显然为 $F_q[x]$ 上的不可约多项式。因为 $\hat{M}_{\rho\left(g_2^u,0\right)}\left(\pi_{ij}x\right)=\prod_{t_v\in C_{\left(g_2^u,0\right)}}\left(x-\pi_{ij}^{-1}\eta^{t_v}\right)$，则当 t_v 取遍 $C_{\left(g_2^u,0\right)}$，j 取遍 $[0,k-1]$ 时，$\pi_{ij}^{-1}\eta^{t_v}$ 取遍 $B_{uvw}(x)$ 的所有根。因为 $\left(\pi_{ij_s^{-1}}\eta^{t_v}\right)^q=\pi_{ij_{s+1}^{-1}}\eta^{t_v q}$，且 $t_v q\in C_{\left(g_2^u,0\right)}$。因此 $\left(\pi_{ij_s^{-1}}\eta^{t_v}\right)^q$ 仍然为 $B_{uvw}(x)$ 的根，从而我们可得 $B_{uvw}(x)$ 是 $\pi_{ij_0}^{-1}\eta^{t_v}$ 在 F_q 上的极小多项式，故 $B_{uvw}(x)$ 为 $F_q[x]$ 上的不可约多项式。同理可证 $C_{uvw}(x)$ 和 $D_{uvw}(x)$ 均为 $F_q[x]$ 上的不可约多项式。从而

$$x^{klmp^n}-\lambda=\hat{A}\left(a_2x\right)^{p^n}\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\hat{B}_{uvw}\left(a_2x\right)^{p^n}\hat{C}_{uvw}\left(a_2x\right)^{p^n}\hat{D}_{uvw}\left(a_2x\right)^{p^n}.$$

为 $x^{klmp^n}-\lambda$ 在 F_q 上的不可约分解。

(2.2)当 $k\mid\frac{fg}{d_3}$ 时，

i) 若 $k\mid f$，$k\nmid g$ 则所有不同的 q^k 模 lm 的分圆陪集为 C_0，$C'_{\left(g_2^u q^r,0\right)}$，$C_{\left(0,g_3^v\right)}$，$C_{\left(g_2^u,g_3^v q^w\right)q^r}$，其中

$0\le u\le \frac{l-1}{f}-1$，$0\le v\le \frac{m-1}{g}-1$，$0\le w\le d_3-1$，$0\le r\le k-1$。所以

$$x^{lm}-\pi^{ilm+j(q-1)}=\left(x-\pi_{ij}^{-1}\right)\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\prod_{r=0}^{k-1}\hat{M}_{\rho'\left(g_2^u q^r,0\right)}\left(\pi_{ij}x\right)\hat{M}_{\rho\left(0,g_3^v\right)}\left(\pi_{ij}x\right)\hat{M}_{\rho\left(g_2^u,g_3^v q^w\right)q^r}\left(\pi_{ij}x\right).$$

从而

$$x^{klmp^n}-\xi^{ilmp^n}=\prod_{j=0}^{k-1}\left(x-\pi_{ij}^{-1}\right)^{p^n}\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\prod_{r=0}^{k-1}\hat{M}_{\rho'\left(g_2^u q^r,0\right)}\left(\pi_{ij}x\right)^{p^n}\hat{M}_{\rho\left(0,g_3^v\right)}\left(\pi_{ij}x\right)^{p^n}\hat{M}_{\rho\left(g_2^u,g_3^v q^w\right)q^r}\left(\pi_{ij}x\right)^{p^n}.$$

令 $E(x)=\prod_{j=0}^{k-1}\left(x-\pi_{ij}^{-1}\right)$，$F_{uvw\eta}(x)=\hat{M}_{\rho'\left(g_2^u,0\right)q^{\overline{\eta}}}\left(\pi_{ij_0}x\right)\hat{M}_{\rho'\left(g_2^u,0\right)q^{\overline{\eta+1}}}\left(\pi_{ij_1}x\right)\cdots\hat{M}_{\rho'\left(g_2^u,0\right)q^{\overline{\eta+k-1}}}\left(\pi_{ij_{k-1}}x\right)$，

$G_{uvw\eta}(x)=\prod_{j=0}^{k-1}\hat{M}_{\rho\left(0,g_3^v\right)}\left(\pi_{ij}x\right)$，$H_{uvw\eta}(x)=\hat{M}_{\rho\left(g_2^u,g_3^v q^w\right)q^{\overline{\eta}}}\left(\pi_{ij_0}x\right)\hat{M}_{\rho\left(g_2^u,g_3^v q^w\right)q^{\overline{\eta+1}}}\left(\pi_{ij_1}x\right)\cdots\hat{M}_{\rho\left(g_2^u,g_3^v q^w\right)q^{\overline{\eta+k-1}}}\left(\pi_{ij_{k-1}}x\right)$.

同(2.1)可说明 $E(x)$ 与 $G_{uvw\eta}(x)$ 均在 F_q 不可约。令 $\pi_{ij_0}^{-1}\eta^{t_v}$ 为 $\hat{M}_{\rho'\left(g_2^u,0\right)q^{\overline{\eta}}}\left(\pi_{ij_0}x\right)$ 的一个根，则 $\left(\pi_{ij_0}^{-1}\eta^{t_v}\right)^q=\pi_{ij_1}^{-1}\eta^{t_v q}$。因为 $t_v\in C'_{\left(g_2^u,0\right)q^{\overline{\eta}}}$，所以 $t_v q\in C'_{\left(g_2^u,0\right)q^{\overline{\eta+1}}}$。因此 $\left(\pi_{ij_0}^{-1}\eta^{t_v}\right)^q$ 为 $\hat{M}_{\rho'\left(g_2^u,0\right)q^{\overline{\eta+1}}}\left(\pi_{ij_1}x\right)$ 的一个根。根据数学归纳法可得 $F_{uvw\eta}(x)$ 为 $\pi_{ij_0}^{-1}\eta^{t_v}$ 在 F_q 上的极小多项式，故 $F_{uvw\eta}(x)$ 在 F_q 不可约。同理可证 $H_{uvw\eta}(x)$ 也为 $F_q[x]$ 上的不可约多项式。从而

$$x^{klmp^n}-\lambda=\hat{E}\left(a_2x\right)^{p^n}\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\prod_{\eta=0}^{k-1}\hat{F}_{uvw\eta}\left(a_2x\right)^{p^n}\hat{G}_{uvw\eta}\left(a_2x\right)^{p^n}\hat{H}_{uvw\eta}\left(a_2x\right)^{p^n}.$$

ii) 若 $k\nmid f$，$k\mid g$。则所有不同的模的分圆陪集为 C_0，$C_{\left(g_2^u,0\right)}$，$C'_{\left(0,g_3^v q^r\right)}$，$C_{\left(g_2^u,g_3^v q^w\right)q^r}$，其中 $0\le u\le \frac{l-1}{f}-1$，$0\le v\le \frac{m-1}{g}-1$，$0\le w\le d_3-1$，$0\le r\le k-1$。则

$$x^{klmp^n}-\xi^{ilmp^n}=\prod_{j=0}^{k-1}\left(x-\pi_{ij}^{-1}\right)^{p^n}\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\prod_{r=0}^{k-1}\hat{M}_{\rho\left(g_2^u,0\right)}\left(\pi_{ij}x\right)^{p^n}\hat{M}_{\rho'\left(0,g_3^v q^r\right)}\left(\pi_{ij}x\right)^{p^n}\hat{M}_{\rho\left(g_2^u,g_3^v q^w\right)q^r}\left(\pi_{ij}x\right)^{p^n}$$

令 $I_{uvw\eta}(x)=\prod_{j=0}^{k-1}\hat{M}_{\rho\left(g_2^u,0\right)}\left(\pi_{ij}x\right)$，$J_{uvw\eta}(x)=\hat{M}_{\rho'\left(0,g_3^v\right)q^{\overline{\eta}}}\left(\pi_{ij_0}x\right)\hat{M}_{\rho'\left(0,g_3^v\right)q^{\overline{\eta+1}}}\left(\pi_{ij_1}x\right)\cdots\hat{M}_{\rho'\left(0,g_3^v\right)q^{\overline{\eta+k-1}}}\left(\pi_{ij_{k-1}}x\right)$.

类似可证 $I_{uvw\eta}(x)$ 与 $J_{uvw\eta}(x)$ 均为 $F_q[x]$ 上的不可约多项式。从而

$$x^{klmp^n}-\lambda=\hat{E}\left(a_2x\right)^{p^n}\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\prod_{\eta=0}^{k-1}\hat{I}_{uvw\eta}\left(a_2x\right)^{p^n}\hat{J}_{uvw\eta}\left(a_2x\right)^{p^n}\hat{H}_{uvw\eta}\left(a_2x\right)^{p^n}.$$

iii) 若 $k\mid f$，$k\mid g$。则所有不同的 q^k 模 lm 的分圆陪集为 C_0，$C'_{\left(g_2^u q^r,0\right)}$，$C'_{\left(0,g_3^v q^r\right)}$，$C_{\left(g_2^u,g_3^v q^w\right)q^r}$，其中 $0\le u\le \frac{l-1}{f}-1$，$0\le v\le \frac{m-1}{g}-1$，$0\le w\le d_3-1$，$0\le r\le k-1$。则

$$x^{klmp^n}-\lambda=\hat{E}\left(a_2x\right)^{p^n}\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\prod_{\eta=0}^{k-1}\hat{F}_{uvw\eta}\left(a_2x\right)^{p^n}\hat{J}_{uvw\eta}\left(a_2x\right)^{p^n}\hat{H}_{uvw\eta}\left(a_2x\right)^{p^n}.$$

定理 3.4 令 k，l，m，p 为不同的奇素数，并且 p 为 F_q 的特征。假设 $\gcd(k,q-1)=\gcd(l,q-1)=\gcd(m,q-1)=1$。则

$$x^{klmp^n}-\lambda=\left(x-b^{-1}\right)\prod_{h=0}^{\frac{k-1}{e}-1}\prod_{r=0}^{\frac{l-1}{f}-1}\prod_{t=0}^{\frac{m-1}{g}-1}\prod_{j_1=0}^{\frac{k-1}{e}\frac{l-1}{f}d_1-1}\prod_{j_2=0}^{\frac{k-1}{e}\frac{m-1}{g}d_2-1}\prod_{j_3=0}^{\frac{l-1}{f}\frac{m-1}{g}d_3-1}\prod_{h_r=0}^{\frac{k-1}{e}\frac{l-1}{f}\frac{m-1}{g}d^2-1}\hat{T}\left(bx\right)^{p^n}$$

其中 $b\in F_q^*$ 并且满足 $\lambda b^{klmp^n}=1$。

证明：因为 $\gcd(k,q-1)=\gcd(l,q-1)=\gcd(m,q-1)=1$，则 $\gcd\left(q-1,klmp^n\right)=1$。从而根据命题 2.2(2) 可得 $\lambda\sim_{klmp^n}1$，所以存在 $b\in F_q^*$ 使得 $\lambda b^{klmp^n}=1$。又因为 $x^{klmp^n}-1=\left(x^{klm}-1\right)^{p^n}$，所以

$$x^{klmp^n}-\lambda=\left(x-b^{-1}\right)\prod_{h=0}^{\frac{k-1}{e}-1}\prod_{r=0}^{\frac{l-1}{f}-1}\prod_{t=0}^{\frac{m-1}{g}-1}\prod_{j_1=0}^{\frac{k-1}{e}\frac{l-1}{f}d_1-1}\prod_{j_2=0}^{\frac{k-1}{e}\frac{m-1}{g}d_2-1}\prod_{j_3=0}^{\frac{l-1}{f}\frac{m-1}{g}d_3-1}\prod_{h_r=0}^{\frac{k-1}{e}\frac{l-1}{f}\frac{m-1}{g}d^2-1}\hat{T}\left(bx\right)^{p^n}$$

定理 3.5 令 k,l,m,p 为不同的奇素数，并且 p 为 F_q 的特征。假设 $k\mid(q-1)$，$l\mid(q-1)$，$\gcd(m,q-1)=1$。那么对任意的 $\lambda\in F_q^*$ 我们有 $\lambda\in\xi^{imp^n}\left\langle\xi^{klmp^n}\right\rangle$，其中 $0\le i\le kl-1$。而且

1) 当 $i=0$，即 $\lambda\in\left\langle\xi^{klmp^n}\right\rangle$ 时，

$$x^{klmp^n}-\lambda=\left(x-c_1^{-1}\right)^{p^n}\prod_{h=0}^{\frac{k-1}{e}-1}\prod_{r=0}^{\frac{l-1}{f}-1}\prod_{t=0}^{\frac{m-1}{g}-1}\prod_{j_1=0}^{\frac{k-1}{e}\frac{l-1}{f}d_1-1}\prod_{j_2=0}^{\frac{k-1}{e}\frac{m-1}{g}d_2-1}\prod_{j_3=0}^{\frac{l-1}{f}\frac{m-1}{g}d_3-1}\prod_{h_r=0}^{\frac{k-1}{e}\frac{l-1}{f}\frac{m-1}{g}d^2-1}\hat{T}\left(c_1x\right)^{p^n}$$

其中 $c_1\in F_q^*$ 并且满足 $\lambda c_1^{klmp^n}=1$。

2) 当 $i=wl$，$1\le w\le k-1$ 并且 $\gcd(w,k)=1$。则

$$x^{klmp^n}-\lambda=\prod_{j=0}^{l-1}\prod_{v=0}^{k-1}\prod_{u=0}^{\frac{m-1}{g}}\hat{M}_{\sigma_u}\left(c_2\pi_{ij}x\right)^{p^n}.$$

其中 $c_2\in F_q^*$ 并且满足 $\lambda c_2^{klmp^n}=\xi^{wlmp^n}$，$\pi$ 为 F_{q^k} 中的 $k(q-1)$ 次单位根，$\pi_{ij}\in F_q^*$。

证明(1)与定理 3.3(1)的证明类似。

(2) 当 $i=wl$，$1\le w\le k-1$ 并且 $\gcd(w,k)=1$。我们有 $\lambda\in\xi^{wlmp^n}\left\langle\xi^{klmp^n}\right\rangle$。根据命题 2.2(2) 可得 $\lambda\sim_{klmp^n}\xi^{wlmp^n}$，所以存在 $c_2\in F_q^*$ 使得 $\lambda c_2^{klmp^n}=\xi^{wlmp^n}$。同时我们有

$$x^{klmp^n}-\xi^{wlmp^n}=\left(x^{klm}-\xi^{wlm}\right)^{p^n}.$$

令 $\beta=\xi^{\frac{q-1}{l}}$，则 $ord(\beta)=l$。从而

$$x^{klm}-\xi^{wlm}=\prod_{j=0}^{l-1}\left(x^{km}-\xi^{wm+\frac{j(q-1)}{l}}\right).$$

令 $\xi=\pi^k$，$\alpha=\xi^{\frac{q-1}{k}}=\pi^{q-1}$，则 $\pi\in F_{q^k}$ 且 $ord(\pi)=k(q-1)$。则

$$x^{km}-\xi^{wm+\frac{j(q-1)}{l}}=\prod_{v=0}^{k-1}\left[x^m-\pi^{k\left(wm+\frac{j(q-1)}{l}\right)}\alpha^v\right]=\prod_{v=0}^{k-1}\left[x^m-\pi^{k\left(wm+\frac{j(q-1)}{l}\right)+v(q-1)}\right].$$

因为 $\pi^{k\left(wm+\frac{j(q-1)}{l}\right)+v(q-1)}=\pi^{k\left[\left(wm+\frac{j(q-1)}{l}\right)+v\frac{q-1}{k}\right]}=\xi^{\left(wm+\frac{j(q-1)}{l}\right)+v\frac{q-1}{k}}\in F_q^*$。所以存在 $\pi_{ij}\in F_q^*$ 使得

$\pi^{k\left(wm+\frac{j(q-1)}{l}\right)+v(q-1)}\pi_{ij}^{m}=1$。从而我们可以得到

$$x^{klmp^n}-\xi^{wlmp^n}=\prod_{j=0}^{l-1}\prod_{v=0}^{k-1}\prod_{u=0}^{\frac{m-1}{g}}\hat{M}_{\sigma_u}\left(\pi_{ij}x\right)^{p^n}.$$

所以

$$x^{klmp^n}-\lambda=\prod_{j=0}^{l-1}\prod_{v=0}^{k-1}\prod_{u=0}^{\frac{m-1}{g}}\hat{M}_{\sigma_u}\left(c_2\pi_{ij}x\right)^{p^n}.$$

定理 3.6 令 k，l，m，p 为不同的奇素数，并且 p 为 F_q 的特征。假设 $k\mid(q-1)$，$l\mid(q-1)$，$m\mid(q-1)$。那么对任意的 $\lambda\in F_q^*$ 我们有 $\lambda\in\xi^{ip^n}\left\langle\xi^{klmp^n}\right\rangle$，其中 $0\le i\le klm-1$。而且

1) 当 $i=0$，即 $\lambda\in\left\langle\xi^{klmp^n}\right\rangle$ 时，

$$x^{klmp^n}-\lambda=\left(x-d_1^{-1}\right)^{p^n}\prod_{h=0}^{\frac{k-1}{e}-1}\prod_{r=0}^{\frac{l-1}{f}-1}\prod_{t=0}^{\frac{m-1}{g}-1}\prod_{j_1=0}^{\frac{k-1}{e}\frac{l-1}{f}-1}d_1\prod_{j_2=0}^{\frac{k-1}{e}\frac{m-1}{g}-1}d_2\prod_{j_3=0}^{\frac{l-1}{f}\frac{m-1}{g}-1}d_3\prod_{h_r=0}^{\frac{k-1}{e}\frac{l-1}{f}\frac{m-1}{g}-1}d^2\ \hat{T}\left(d_1x\right)^{p^n}$$

其中 $d_1\in F_q^*$ 并且满足 $\lambda d_1^{klmp^n}=1$。

2) 当 $i=wlm$，$1\le w\le k-1$ 并且 $\gcd(w,k)=1$。那么

$$x^{klmp^n}-\lambda=\prod_{j=0}^{lm-1}\left(\left(d_2x\right)^k-\hat{\xi}^{w+j\frac{q-1}{m}}\right)^{p^n}.$$

其中 $d_2\in F_q^*$ 并且满足 $\lambda d_2^{klmp^n}=\xi^{wlmp^n}$。

3) 当 $i=ym$，$1\le y\le kl-1$ 并且 $\gcd(y,kl)=1$。那么

$$x^{klmp^n}-\lambda=\prod_{u=0}^{m-1}\left(\left(d_3x\right)^{kl}-\hat{\xi}^{y+u\frac{q-1}{m}}\right)^{p^n}.$$

其中 $d_3\in F_q^*$ 并且满足 $\lambda d_3^{klmp^n}=\xi^{wlmp^n}$。

证明(1)与定理 3.3(1)的证明类似。

(2) 当 $i=wlm$，$1\le w\le k-1$ 并且 $\gcd(w,k)=1$。我们有 $\lambda\in\xi^{wlmp^n}\left\langle\xi^{klmp^n}\right\rangle$。根据命题 2.2 可得 $\lambda\sim_{klmp^n}\xi^{wlmp^n}$，所以存在 $d_2\in F_q^*$ 使得 $\lambda d_2^{klmp^n}=\xi^{wlmp^n}$。同时我们有

$$x^{klmp^n}-\xi^{wlmp^n}=\left(x^{klm}-\xi^{wlm}\right)^{p^n}.$$

令 $\zeta=\xi^{\frac{q-1}{lm}}$，则 $ord(\zeta)=lm$。因此可得

$$x^{klm}-\xi^{wlm}=\prod_{j=0}^{lm-1}\left(x^k-\xi^{w+j\frac{q-1}{m}}\right).$$

又因为 $\gcd\left(k,w+j\frac{q-1}{m}\right)=\gcd(k,w)=1$，所以 $ord\left(\xi^{w+j\frac{q-1}{m}}\right)=q-1$。再根据引理 2.4 可知多项式 $x^k-\xi^{w+j\frac{q-1}{m}}\ (0\le j\le lm-1)$ 在 F_q 不可约。所以

$$x^{klmp^n}-\lambda=\prod_{u=0}^{m-1}\left(\left(d_3x\right)^{kl}-\hat{\xi}^{y+u\frac{q-1}{m}}\right)^{p^n}.$$

(3)若 $i=ym$，$1\le y\le kl-1$ 并且 $\gcd(y,kl)=1$。那么 $\lambda\sim_{klmp^n}\xi^{ymp^n}$，所以存在 $d_3\in F_q^*$ 使得 $\lambda d_3^{klmp^n}=\xi^{ymp^n}$。同时我们有

$$x^{klmp^n}-\xi^{ymp^n}=\left(x^{klm}-\xi^{ym}\right)^{p^n}.$$

并且可得 $x^{klm}-\xi^{ym}=\prod_{u=0}^{m-1}\left(x^{kl}-\xi^{y+u\frac{q-1}{m}}\right)$。又因为 $\gcd\left(kl,y+u\dfrac{q-1}{m}\right)=\gcd(kl,y)=1$，所以 $ord\left(\xi^{y+u\frac{q-1}{m}}\right)=q-1$。

再根据引理 2.5 可知多项式 $x^{kl}-\xi^{y+u\cdot\frac{q-1}{m}}\left(0\le u\le m-1\right)$ 在不可约。所以

$$x^{klmp^n}-\lambda=\prod_{u=0}^{m-1}\left(\left(d_3x\right)^{kl}-\hat{\xi}^{y+u\frac{q-1}{m}}\right)^{p^n}.$$

定理 3.7 令 C 是在 F_q 上长度为 $klmp^n$ 的 λ 常循环码。在定理 3.3 的条件下，有下面的结论成立：

1) 当 $\lambda\in\left\langle\xi^{klmp^n}\right\rangle$ 时。记 $\varpi=\varsigma_{h,r,t,j_1,j_2,j_3,h_r}$，则

$$C=\left\langle\left(x-a_1^{-1}\right)^{\varepsilon}\prod_{h=0}^{\frac{k-1}{e}-1}\prod_{r=0}^{\frac{l-1}{f}-1}\prod_{t=0}^{\frac{m-1}{g}-1}\prod_{j_1=0}^{\frac{k-1}{e}\cdot\frac{l-1}{f}d_1}\prod_{j_2=0}^{\frac{k-1}{e}\cdot\frac{m-1}{g}d_2}\prod_{j_3=0}^{\frac{l-1}{f}\cdot\frac{m-1}{g}d_3}\prod_{h_r=0}^{\frac{k-1}{e}\cdot\frac{l-1}{f}\cdot\frac{m-1}{g}d^2}\hat{T}\left(a_1x\right)^{\varpi}\right\rangle.$$

对于任意的 $0\le h\le\dfrac{k-1}{e}-1$，$0\le r\le\dfrac{l-1}{f}-1$，$0\le t\le\dfrac{m-1}{g}-1$，$0\le j_1\le\dfrac{k-1}{e}\cdot\dfrac{l-1}{f}\cdot d_1$，$0\le j_2\le\dfrac{k-1}{e}\cdot\dfrac{m-1}{g}\cdot d_2$，$0\le j_3\le\dfrac{l-1}{f}\cdot\dfrac{m-1}{g}\cdot d_3$，$0\le h_r\le\dfrac{k-1}{e}\cdot\dfrac{l-1}{f}\cdot\dfrac{m-1}{g}\cdot d^2$，都有 $0\le\varepsilon,\varpi\le p^n$。

2) 当 $i\ne0$ 时，

(2.1)若 $k\nmid\dfrac{fg}{d_3}$，则

$$C=\left\langle\hat{A}\left(a_2x\right)^{\delta}\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\hat{B}_{uvw}\left(a_2x\right)^{\varepsilon_{u,v,w}}\hat{C}_{uvw}\left(a_2x\right)^{\varepsilon_{u,v,w}}\hat{D}_{uvw}\left(a_2x\right)^{\varepsilon_{u,v,w}}\right\rangle.$$

对于任意的 $0\le u\le\dfrac{l-1}{f}-1$，$0\le v\le\dfrac{m-1}{g}-1$，$0\le w\le d_3-1$ 都有 $0\le\delta,\varepsilon_{u,v,w}\le p^n$。

(2.2)当 $k\mid\dfrac{fg}{d_3}$ 时，则有 $k\mid fg$

i) 若 $k\mid f$，$k\nmid g$ 则

$$C=\left\langle\hat{E}\left(a_2x\right)^{\vartheta}\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\prod_{\eta=0}^{k-1}\hat{F}_{uvw\eta}\left(a_2x\right)^{\varepsilon_{u,v,w,\eta}}\hat{G}_{uvw\eta}\left(a_2x\right)^{\varepsilon_{u,v,w,\eta}}\hat{H}_{uvw\eta}\left(a_2x\right)^{\varepsilon_{u,v,w,\eta}}\right\rangle.$$

对于任意的 $0\le u\le \frac{l-1}{f}-1$， $0\le v\le \frac{m-1}{g}-1$， $0\le w\le d_3-1$， $0\le r_1\le k-1$ 都有 $0\le \vartheta,\varepsilon_{u,v,w,r_1}\le p^n$。

ii) 若 $k\nmid f$， $k\mid g$。则

$$C=\left\langle \hat{E}\left(a_2x\right)^{\tau}\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\prod_{r_1=0}^{k-1}\hat{I}_{uvwr_1}\left(a_2x\right)^{\zeta_{uvwr_1}}\hat{J}_{uvwr_1}\left(a_2x\right)^{\zeta_{uvwr_1}}\hat{H}_{uvwr_1}\left(a_2x\right)^{\zeta_{uvwr_1}}\right\rangle.$$

对于任意的 $0\le u\le \frac{l-1}{f}-1$， $0\le v\le \frac{m-1}{g}-1$， $0\le w\le d_3-1$， $0\le r_1\le k-1$ 都有 $0\le \tau,\zeta_{u,v,w,r_1}\le p^n$。

iii) 若 $k\mid f$， $k\mid g$。则

$$C=\left\langle \hat{E}\left(a_2x\right)^{\varsigma}\prod_{u=0}^{\frac{l-1}{f}-1}\prod_{v=0}^{\frac{m-1}{g}-1}\prod_{w=0}^{d_3-1}\prod_{r_1=0}^{k-1}\hat{F}_{uvwr_1}\left(a_2x\right)^{\sigma_{uvwr_1}}\hat{J}_{uvwr_1}\left(a_2x\right)^{\sigma_{uvwr_1}}\hat{H}_{uvwr_1}\left(a_2x\right)^{\sigma_{uvwr_1}}\right\rangle.$$

对于任意的 $0\le u\le \frac{l-1}{f}-1$， $0\le v\le \frac{m-1}{g}-1$， $0\le w\le d_3-1$， $0\le r_1\le k-1$ 都有 $0\le \varsigma,\sigma_{u,v,w,r_1}\le p^n$。

定理 3.8 令 C 是在 F_q 上长度为 $klmp^n$ 的 λ 常循环码。在定理 3.4 的条件下，记 $\varpi=\varsigma_{h,r,t,j_1,j_2,j_3,h_r}$，有下面的结论成立：

$$C=\left\langle \left(x-b^{-1}\right)^{\varepsilon}\prod_{h=0}^{\frac{k-1}{e}-1}\prod_{r=0}^{\frac{l-1}{f}-1}\prod_{t=0}^{\frac{m-1}{g}-1}\prod_{j_1=0}^{\frac{k-1}{e}\cdot\frac{l-1}{f}\cdot d_1}\prod_{j_2=0}^{\frac{k-1}{e}\cdot\frac{m-1}{g}\cdot d_2}\prod_{j_3=0}^{\frac{l-1}{f}\cdot\frac{m-1}{g}\cdot d_3}\prod_{h_r=0}^{\frac{k-1}{e}\cdot\frac{l-1}{f}\cdot\frac{m-1}{g}\cdot d^2}\hat{T}\left(bx\right)^{\varpi}\right\rangle.$$

对于任意的 $0\le h\le \frac{k-1}{e}-1$， $0\le r\le \frac{l-1}{f}-1$， $0\le t\le \frac{m-1}{g}-1$， $0\le j_1\le \frac{k-1}{e}\cdot\frac{l-1}{f}\cdot d_1$，

$0\le j_2\le \frac{k-1}{e}\cdot\frac{m-1}{g}\cdot d_2$， $0\le j_3\le \frac{l-1}{f}\cdot\frac{m-1}{g}\cdot d_3$， $0\le h_r\le \frac{k-1}{e}\cdot\frac{l-1}{f}\cdot\frac{m-1}{g}\cdot d^2$， 都有 $0\le \varepsilon,\varpi\le p^n$。

定理 3.9 令 C 是在 F_q 上长度为 $klmp^n$ 的 λ 常循环码。在定理 3.5 的条件下，有下面的结论成立：

1) 当 $\lambda\in\left\langle \xi^{klmp^n}\right\rangle$ 时，

$$C=\left\langle \left(x-c_1^{-1}\right)^{\varepsilon}\prod_{h=0}^{\frac{k-1}{e}-1}\prod_{r=0}^{\frac{l-1}{f}-1}\prod_{t=0}^{\frac{m-1}{g}-1}\prod_{j_1=0}^{\frac{k-1}{e}\cdot\frac{l-1}{f}\cdot d_1}\prod_{j_2=0}^{\frac{k-1}{e}\cdot\frac{m-1}{g}\cdot d_2}\prod_{j_3=0}^{\frac{l-1}{f}\cdot\frac{m-1}{g}\cdot d_3}\prod_{h_r=0}^{\frac{k-1}{e}\cdot\frac{l-1}{f}\cdot\frac{m-1}{g}\cdot d^2}\hat{T}\left(c_1x\right)^{\varpi}\right\rangle.$$

其中 $\varpi=\varsigma_{h,r,t,j_1,j_2,j_3,h_r}$。的 $0\le h\le \frac{k-1}{e}-1$， $0\le r\le \frac{l-1}{f}-1$， $0\le t\le \frac{m-1}{g}-1$， $0\le j_1\le \frac{k-1}{e}\cdot\frac{l-1}{f}\cdot d_1$，

$0\le j_2\le \frac{k-1}{e}\cdot\frac{m-1}{g}\cdot d_2$， $0\le j_3\le \frac{l-1}{f}\cdot\frac{m-1}{g}\cdot d_3$， $0\le h_r\le \frac{k-1}{e}\cdot\frac{l-1}{f}\cdot\frac{m-1}{g}\cdot d^2$， 都有 $0\le \varepsilon,\varpi\le p^n$。

2) 当 $i=wl$， $1\le w\le k-1$ 并且 $\gcd\left(w,k\right)=1$。则

$$C=\left\langle \prod_{j=0}^{l-1}\prod_{v=0}^{k-1}\prod_{u=0}^{\frac{m-1}{g}}\hat{M}_{\sigma_u}\left(c_2\pi_{ij}x\right)^{\varsigma_{j,v,u}}\right\rangle.$$

对于任意的 $0\le j\le l-1$， $0\le v\le k-1$， $0\le u\le \frac{m-1}{g}$ 都有 $0\le \varsigma_{j,v,u}\le p^n$。

定理 3.10 令 C 是在 F_q 上长度为 $klmp^n$ 的 λ 常循环码。在定理 3.6 的条件下，有下面的结论成立：

1) 当 $\lambda \in \left\langle \xi^{klmp^n} \right\rangle$ 时，

$$C = \left\langle \left(x - d_1^{-1}\right)^{\varepsilon} \prod_{h=0}^{\frac{k-1}{e}-1} \prod_{r=0}^{\frac{l-1}{f}-1} \prod_{t=0}^{\frac{m-1}{g}-1} \prod_{j_1=0}^{\frac{k-1}{e}\frac{l-1}{f}} d_1 \prod_{j_2=0}^{\frac{k-1}{e}\frac{m-1}{g}} d_2 \prod_{j_3=0}^{\frac{l-1}{f}\frac{m-1}{g}} d_3 \prod_{h_r=0}^{\frac{k-1}{e}\frac{l-1}{f}\frac{m-1}{g}} d^2 \hat{T}\left(d_1 x\right)^{\varpi} \right\rangle.$$

其中 $\varpi = \varsigma_{h,r,t,j_1,j_2,j_3,h_r}$。且 $0 \le h \le \frac{k-1}{e} - 1$，$0 \le r \le \frac{l-1}{f} - 1$，$0 \le t \le \frac{m-1}{g} - 1$，$0 \le j_1 \le \frac{k-1}{e} \cdot \frac{l-1}{f} \cdot d_1$，$0 \le j_2 \le \frac{k-1}{e} \cdot \frac{m-1}{g} \cdot d_2$，$0 \le j_3 \le \frac{l-1}{f} \cdot \frac{m-1}{g} \cdot d_3$，$0 \le h_r \le \frac{k-1}{e} \cdot \frac{l-1}{f} \cdot \frac{m-1}{g} \cdot d^2$，都有 $0 \le \varepsilon, \varpi \le p^n$。

2) 当 $i = wlm$，$1 \le w \le k-1$ 并且 $\gcd(w,k) = 1$。那么

$$C = \left\langle \prod_{j=0}^{lm-1} \left(\left(d_2 x\right)^k - \xi^{w + j \cdot \frac{q-1}{m}} \right)^{\varsigma_j} \right\rangle.$$

对于任意的 $0 \le j \le lm-1$ 都有 $0 \le \varsigma_j \le p^n$。

3) 当 $i = ym$，$1 \le y \le kl-1$ 并且 $\gcd(y,kl) = 1$。那么

$$C = \left\langle \prod_{u=0}^{m-1} \left(\left(d_3 x\right)^{kl} - \xi^{y + u \cdot \frac{q-1}{m}} \right)^{\varsigma_u} \right\rangle.$$

对于任意的 $0 \le u \le m-1$ 都有 $0 \le \varsigma_u \le p^n$。

参考文献

[1] Chen, B., Dinh, H.Q. and Liu, H. (2012) Constacyclic Codes over Finite Fields. *Finite Fields and Their Applications*, **18**, 1217-1231. https://doi.org/10.1016/j.ffa.2012.10.001

[2] Huffman, W.C. and Pless, V. (2003) Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9780511807077

[3] MacWilliams, F.J. and Sloane, N.J.A. (1998) The Theory of Error-Correcting Codes. 10th Impression, North-Holland, Amsterdam.

[4] Dinh, H.Q. (2012) Repeated-Root Constacyclic Codes of $2p^s$. *Finite Fields and Their Applications*, **18**, 133-143. https://doi.org/10.1016/j.ffa.2011.07.003

[5] Dinh, H.Q. (2013) Structure of Repeated-Root Constacyclic Codes of Length $3p^s$ and Their Duals. *Discrete Mathematics*, **313**, 983-991. https://doi.org/10.1016/j.disc.2013.01.024

[6] Dinh, H.Q. (2014) Structure of Repeated-Root Cyclic and Negacyclic Codes of Length $6p^s$ and Their Duals. *Contemporary Mathematics*, **609**, 69-87. https://doi.org/10.1090/conm/609/12150

[7] Chen, B., Dinh, H.Q. and Liu, H. (2014) Repeated-Root Constacyclic Codes of Length lp^s and Their Duals. *Discrete Applied Mathematics*, **177**, 60-70. https://doi.org/10.1016/j.dam.2014.05.046

[8] Chen, B., Dinh, H.Q. and Liu, H. (2015) Repeated-Root Constacyclic Codes of Length $2l^m p^n$. *Finite Fields and Their Applications*, **33**, 137-159. https://doi.org/10.1016/j.ffa.2014.11.006

[9] Tong, H. (2016) Repeated-Root Constacyclic Codes of Length $kl^a p^b$ over a Finite Field. *Finite Fields and Their Applications*, **41**, 159-173. https://doi.org/10.1016/j.ffa.2016.06.006

[10] Zhao, W., Tang, X.L. and Gu, Z. (2018) Constacyclic Codes of Length $kl^m p^n$ over a Finite Field. *Finite Fields and Their Applications*, **52**, 51-66. https://doi.org/10.1016/j.ffa.2018.03.004

[11] Lidl, R. and Niederreiter, H. (1983) Finite Fields. In: Rota, G.-C., Ed., *The Encyclopedia of Mathematics*, *Vol.* 20, Addison-Wesley, Reading, MA.

知网检索的两种方式：

1. 打开知网页面 http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD
   下拉列表框选择：[ISSN]，输入期刊 ISSN：2160-7583，即可查询
2. 打开知网首页 http://cnki.net/
   左侧“国际文献总库”进入，输入文章标题，即可查询

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：pm@hanspub.org