Vol. 35 (2015)
No. 2

数 学 杂 志
J. of Math. (PRC)

环 $\frac{\mathbb{F}_{p^m}[u]}{\langle u^a\rangle}$ 上一类常循环码

刘花璐
(湖北理工学院数理学院, 湖北 黄石 435003)

摘 要: 本文研究有限链环上一类 λ - 常循环码. 利用 x^n-1 在 $R_a[x]$ 上可唯一分解为两两互素的首一基本不可约多项式乘积, 刻画了 R_a 中长为 p^sn 的所有 λ - 常循环码, 推广了开晓山等人在文献 [4] 中的结果.

关 键 词: 重根常循环码; 对偶码; 有限链环
MR(2010) **主题分类号**: 11T71 **中 图 分 类 号**: O157.4
文 献 标 识 码: A **文 章 编 号**: 0255-7797(2015)02-0412-07

1 引言

常循环码是一类非常重要的码. 可是, 大多数对常循环码的研究只涉及到码长 N 与域 $\mathbb{F}$ 的特征互素的情形. 在这种情形下, 长为 N 的 $\lambda-$ 常循环码是剩余类环 $\frac{\mathbb{F}[x]}{\langle x^N-\lambda\rangle}$ 的理想 $\langle f(x)\rangle$, 其中 $x^N-\lambda=f(x)g(x)$. 当码长 N 被域的特征整除时, 就产生所谓的重根常循环码. 重根常循环码最初是由 Berman 于 1967 年引入的 [1]. 在 1991 年, Castagnoli 与 Lint 等人证明了有几种情形的重根循环码是极优的 [2,3]. 从而促使研究者进一步对重根循环码进行研究. 最近, 开晓山等人研究了有限链环 $\mathbb{F}_p+u\mathbb{F}_p+\cdots+u^{a-1}\mathbb{F}_p(u^a=0)$ 中长为 p^sn 的 $(1+\rho u)$ - 重根常循环码, 这里 ρ 是 $\mathbb{F}_p$ 的非零元, 给出了这里重根常循环码的结构 [4]. 刘修生等人在文献 [5] 中利用中国剩余定理给出了有限链环 $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ 上长为 $2p^s$ 的循环码及负循环码的代数结构及码字个数, 且它们的研究方法可推广到有限链环 $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+\cdots+u^{a-1}\mathbb{F}_{p^m}$.

本文将采用类似于 [4] 的方法, 研究更一般的有限链环 $R_a=\frac{\mathbb{F}_{p^m}[u]}{\langle u^a\rangle}=\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+\cdots+u^{a-1}\mathbb{F}_{p^m}$ 的长为 p^sn 的更一般 $\lambda-$ 重根常循环码, 其中

$$\lambda=1+u\lambda_1+\cdots+u^{a-1}\lambda_{a-1},\lambda_1\neq 0,\lambda_1,\cdots,\lambda_{a-1}\in\mathbb{F}_{p^m}$$

且包含了 [4] 中 $\lambda=1+\rho u$ 的情形. 第 2 节, 回顾了有限链环与有限环上码的一些基本知识, 这些知识是后续各节的研究基础; 第 3 节, 研究了 R_a 上长为 p^s 的 $\lambda-$ 重根常循环码, 给出了这类码与它的对偶码的结构. 最后, 在第 4 节, 假设 n,p 为奇数且 $(n,p)=1$ 的情形下, 刻画了 R_a 上长为 p^sn 的 $\lambda-$ 重根常循环码.

2 基础知识

*收稿日期: 2014-08-08 接收日期: 2014-11-20
基金项目: 湖北理工学院自然科学研究项目 (11yjz37B); 湖北理工学院重点教学研究项目 (2013A04); 湖北省高等学校教学研究项目 (2011371); 湖北省教育厅自然科学基金 (D20144401).
作者简介: 刘花璐 (1981–), 男, 湖北荆州, 讲师, 主要研究方向: 矩阵论, 代数编码.

设 R 是一个有限交换环, 如果 R 有唯一的最大理想, 则称 R 为局部环. 进而, 如果 R 的所有理想在集合论意义下有线性包含关系, 则称 R 为链环. 下面事实可以在文献 [7] 中找到.

命题 2.1 设 R 为有限交换环, 则下列条件等价:

(i) R 是局部环且 R 的最大理想 M 是主理想, 即存在 $\gamma \in R$, 使 $M = \langle\gamma\rangle$;

(ii) R 是局部主理想环;

(iii) R 是链环, 其理想为 $R = \langle\gamma^0\rangle \supset \langle\gamma\rangle \supset \cdots \supset \langle\gamma^{e-1}\rangle \supset \langle\gamma^e\rangle = \langle 0\rangle$, 其中 $\gamma^{e-1} \neq 0$, 称 e 为 γ 的幂零指数.

记 $\overline{R} = \frac{R}{M}$. 用 "$^-$" 表示 $R \to \overline{R}$ 的自然环同态: $r \mapsto r + M$. 将其扩充 $R[x] \to \overline{R}[x]$ 自然同态, 仍用 "$^-$" 表示, 即 $f(x) = a_l x^l + \cdots + a_1 x + a_0 \mapsto \overline{f}(x) = \overline{a}_l x^l + \cdots + \overline{a}_1 x + \overline{a}_0$.

设 $f_1(x), f_2(x) \in R[x]$, 如果 $\langle f_1(x)\rangle + \langle f_2(x)\rangle = R[x]$, 则称 $f_1(x)$ 与 $f_2(x)$ 是互素的, 记为 $(f_1(x), f_2(x)) = 1$ (见文献 [6]).

引理 2.2 [8] 设 R 为有限交换链环, $f_1(x), f_2(x) \in R[x]$. 则 $(f_1(x), f_2(x)) = 1$ 当且仅当 $(\overline{f}_1(x), \overline{f}_2(x)) = 1$.

下面 Hensel 引理在有限链环上编码的研究中起着非常重要的作用.

引理 2.3 [9] (Hensel 引理) 设 $f(x) \in R[x]$ 且 $\overline{f}(x) = g_1(x)\cdots g_t(x)$, 其中 $g_1(x), \cdots, g_t(x)$ 是 $\overline{R}[x]$ 中两两互素的多项式, 则 $R[x]$ 上存在两两互素的多项式 $f_1(x), \cdots, f_t(x)$ 使得 $f(x) = f_1(x)\cdots f_t(x)$ 且 $\overline{f}_1(x) = g_1(x), \cdots, \overline{f}_t(x) = g_t(x)$.

接下来, 我们给出有限交换链环 R 上相关码的概念与性质.

设 R 为有限交换链环, λ 为 R 的一个单位. $\forall(x_0, x_1, \cdots, x_{N-1}) \in R^N$, 在 R^N 上的 λ - 常循环位移 τ_λ 定义为 $\tau_\lambda(x_0, x_1, \cdots, x_{N-1}) = (\lambda x_{N-1}, x_0, x_1, \cdots, x_{N-2})$. 若 $\tau_\lambda(C) = C$, 则称码 C 为 R 上的 λ - 常循环码. 当 $\lambda = 1$, λ - 常循环码为循环码; 当 $\lambda = -1$, λ - 常循环码为负循环码.

作映射

$$\begin{aligned} \varphi : R^N &\longrightarrow \frac{R[x]}{\langle x^N - \lambda\rangle} \\ (c_0, c_1, \cdots, c_{N-1}) &\longmapsto c_0 + c_1 x + \cdots + c_{N-1} x^{N-1} \end{aligned}$$

则 φ 是 R^N 到 $\frac{R[x]}{\langle x^N-\lambda\rangle}$ 的一个环同构. 下面命题是显然的.

命题 2.4 C 为 R 上长为 N 的 $\lambda-$ 常循环码当且仅当 $\varphi(C)$ 为 $\frac{R[x]}{\langle x^N-\lambda\rangle}$ 的理想.

设 C 为 R 上的 $\lambda-$ 常循环码, 称 $\{f | fg = 0, \forall g \in C\}$ 为 C 的零化子, 记为 $\mathrm{Ann}(C)$. 即 $\mathrm{Ann}(C) = \{f | fg = 0, \forall g \in C\}$.

设 $f(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + a_k x^k$, 称 $x^k f(x^{-1}) = a_k + a_{k-1}x + \cdots + a_0 x^k$ 为 $f(x)$ 互反多项式, 记为 $f^*(x)$. 显然 $(f^*(x))^* = f(x)$ 当且仅当 $f(x)$ 的常数项非零. 记 $\mathrm{Ann}(C)^* = \{f^*(x) | f(x) \in \mathrm{Ann}(C)\}$.

以下 3 个引理可以在文献 [10] 中找到.

引理 2.5 R 上 λ - 常循环码的对偶码为 R 上 λ^{-1} - 常循环码.

引理 2.6 设 C 为有限链环 R 上长为 N 的线性码, 则 $|C| \cdot |C^\perp| = |R|^N$.

引理 2.7 设 R 为有限链环, λ 为 R 上的单位且 $\lambda^2 = 1$. 如果 C 为 R 上长为 N 的 λ - 常循环码, 则 C 的对偶码 $C^\perp = \mathrm{Ann}(C)^*$.

3 R_a 上长度为 p^s 的 λ - 常循环码

令 $\lambda = 1 + u\lambda_1 + \cdots + u^{a-1}\lambda_{a-1}$, 这里 $\lambda_1, \cdots, \lambda_{a-1} \in \mathbb{F}_{p^m}$, 且 $\lambda_1 \neq 0$. 我们来研究 R_a 上长度为 p^s 的 λ - 常循环码. 众所周知, C 为 R_a 上长度为 p^s 的 λ - 常循环码的充要条件

$$\varphi(C) = \{c_0 + c_1 x + \cdots + c_{p^s-1}x^{p^s-1} + \langle x^{p^s} - \lambda\rangle | (c_0, c_1, \cdots, c_{p^s-1}) \in C\}$$

为环 $\widetilde{R}_a(s,\lambda) = \frac{R_a[x]}{\langle x^{p^s}-\lambda\rangle}$ 的理想.

我们首先提供 $x-1$ 在 $\widetilde{R}_a(s,\lambda)$ 中所起作用的一个重要事实.

引理 3.1 对于任意正整数 k, $(x-1)^{p^k} = x^{p^k} - 1 \in R_a[x]$. 特别地, 在 $\widetilde{R}_a(s,\lambda)$ 中, 存在一个单位 b, 使 $(x-1)^{p^s} = u\lambda_1 b$ 且 $x-1$ 具有幂零指数 $p^s a$.

证 对 $1 \leq k \leq p^s - 1$, 有 $p \big| \binom{p^s}{k}$. 因此 $(x-1)^{p^k} = x^{p^k} - 1$. 于是, 在 $\widetilde{R}_a(s,\lambda)$ 中,

$$\begin{aligned}(x-1)^{p^s} &= x^{p^s} - 1 = u\lambda_1 + \cdots + u^{a-1}\lambda_{a-1} \\ &= u\lambda_1(1 + u\lambda_2\lambda_1^{-1} + \cdots + u^{a-2}\lambda_{a-1}\lambda_1^{-1}) \\ &= u\lambda_1 b.\end{aligned}$$

这里 $b = 1 + u\lambda_2\lambda_1^{-1} + \cdots + u^{a-2}\lambda_{a-1}\lambda_1^{-1}$ 显然在 $\widetilde{R}_a(s,\lambda)$ 中是可逆. 因此, 在 $\widetilde{R}_a(s,\lambda)$ 中, $\langle (x-1)^{p^s}\rangle = \langle u\rangle$. 显然, 在 $\widetilde{R}_a(s,\lambda)$ 中, $(x-1)^{p^s a-1} \neq 0$. 故 $x-1$ 在 $\widetilde{R}_a(s,\lambda)$ 中的幂零指数为 $p^s a$.

命题 3.2 环 $\widetilde{R}_a(s,\lambda)$ 是一个链环, 其所有理想为

$$\widetilde{R}_a(s,\lambda) = \langle 1\rangle \supsetneq \langle x-1\rangle \supsetneq \cdots \supsetneq \langle (x-1)^{p^s a-1}\rangle \supsetneq \langle (x-1)^{p^s a}\rangle = \langle 0\rangle.$$

证 显然, $\widetilde{R}_a(s,\lambda)$ 中的元 $f(x)$ 可以表示成

$$f(x) = \sum_{i=0}^{p^s-1} c_{0,i}(x-1)^i + u\sum_{i=0}^{p^s-1} c_{1,i}(x-1)^i + \cdots + u^{a-1}\sum_{i=0}^{p^s-1} c_{a-1,i}(x-1)^i,$$

其中 $c_{0,i}, c_{1,i}, \cdots, c_{a-1,i} \in \mathbb{F}_{p^m}, i = 0, 1, \cdots, p^s - 1$. 由引理 3.1, $u = (x-1)^{p^s}\lambda_1^{-1}b^{-1}$, 则可将 $f(x)$ 改写为 $f(x) = c_{0,0} + (x-1)g(x)$, $g(x)$ 是 $\widetilde{R}_a(s,\lambda)$ 中某一多项式. 因为 $(x-1)$ 是幂零的, 所以 $f(x)$ 不可逆当且仅当 $c_{0,0} = 0$, 即若 $f(x)$ 不可逆, 则 $f(x) \in \langle x-1\rangle$. 因此 $\widetilde{R}_a(s,\lambda)$ 是有最大理想 $\langle x-1\rangle$ 的局部环. 由命题 2.1 知, $\widetilde{R}_a(s,\lambda)$ 是链环, 且所有理想为

$$\widetilde{R}_a(s,\lambda) = \langle 1\rangle \supsetneq \langle x-1\rangle \supsetneq \cdots \supsetneq \langle (x-1)^{p^s a-1}\rangle \supsetneq \langle (x-1)^{p^s a}\rangle = \langle 0\rangle.$$

将引理 3.1 与命题 3.2 相结合，我们马上得到下列定理.

定理 3.3 R 中长度为 p^s 的 $\lambda-$ 常循环码有且仅有 $p^s a+1$ 个. 它们对应有限链环 $\widetilde{R}_a(s,\lambda)$ 中的理想 $\langle (x-1)^i\rangle, i = 0, 1, \cdots, p^s a$. 每一个 $\lambda-$ 常循环码 $\langle (x-1)^i\rangle$ 有 $p^{m(p^s a-i)}$ 个码字.

命题 3.4 对 $0 \leq i \leq p^s a$, λ - 常循环码 $C = \langle (x-1)^i\rangle \subset \widetilde{R}_a(s,\lambda)$ 的对偶码是 $\widetilde{R}_a(s,\lambda^{-1})$ 上的 λ^{-1} - 常循环码 $C^\perp = \langle (x-1)^{p^s a-i}\rangle \subset \widetilde{R}_a(s,\lambda^{-1})$, 且 $|C^\perp| = p^{mi}$.

证 由引理 2.5 知 $C^\perp$ 是 R_a 上长度为 p^s 的 λ^{-1} - 常循环码. 令 $L = [\log_p a]$, 则 $p^L \geq a$. 从而 $u^{p^L} = 0$. 因此 $\lambda^{p^L} = 1$. 故 $\lambda^{-1} = \lambda^{p^L-1}$. 由 $\lambda = 1 + u\lambda_1 + \cdots + u^{a-1}\lambda_{a-1}$, 可令 $\lambda^{-1} = 1 + u\lambda_1' + \cdots + u^{a-1}\lambda_{a-1}'$. 从而引理 3.1 及定理 3.3 能够用到 $C^\perp$ 和 $\widetilde{R}_a(s,\lambda^{-1})$ 中. 因此 $C^\perp$ 是有限链环 $\widetilde{R}_a(s,\lambda^{-1})$ 中形为 $\langle (x-1)^j\rangle, 0 \leq j \leq p^s a$ 的理想.

另一方面, 由引理 2.6, $|C|\cdot|C^{\perp}|=|R_a|^{p^s}=p^{p^sam}$, 可得

$$|C^{\perp}|=\frac{p^{p^sam}}{|C|}=\frac{p^{p^sam}}{p^{m(p^sa-i)}}=p^{mi}.$$

因此 $C^{\perp}=\langle(x-1)^{p^sa-i}\rangle$.

推论 3.5 R_a 上存在长为 p^s 的自对偶 $\lambda-$ 常循环码的充要条件是 $a=2$ 且 $p=2$.

证 因为 $C=\langle(x-1)^i\rangle\subset\widetilde{R}_a(s,\lambda)$ 的对偶码是 $C^{\perp}=\langle(x-1)^{p^sa-i}\rangle\subset\widetilde{R}_a(s,\lambda^{-1})$, 所以 $C=C^{\perp}$ 当且仅当 $\lambda=\lambda^{-1}$ 和 $i=p^sa-i$, 即 $\lambda^2=1$ 且 a 为偶数. 从而 $C=C^{\perp}$ 当且仅当 $a=2$ 且 $p=2$. 于是 $i=2^s$, 进而 $\langle(x-1)^{2^s}\rangle=\langle u\rangle$ 是唯一的自对偶码.

4 R 上长为 p^sn 的 λ - 常循环码

设 $\lambda=1+u\lambda_1+\cdots+u^{a-1}\lambda_{a-1}$, 其中 $\lambda_1,\cdots,\lambda_{a-1}\in\mathbb{F}_{p^m}$, 且 $\lambda_1\neq0$. 令 $(n,p)=1$ 且 n 与 p 都为奇数. 这一节, 我们来讨论 R 上长为 p^sn 的 λ - 常循环码. 这类码是环 $T_a(s,n,\lambda)=\frac{R_a[x]}{\langle x^{p^sn}-\lambda\rangle}$ 的理想.

引理 4.1 对于任意正整数 k, $(x^n-1)^{p^k}=x^{p^kn}-1\in R_a[x]$. 特别地, 在 $T_a(s,n,\lambda)$ 中, 有 $(x^n-1)^{p^s}=u\lambda_1w$ 和 x^n-1 是幂零的且幂零指数为 p^sa, 这里 $w=1+u\lambda_2\lambda_1^{-1}+\cdots+u^{a-2}\lambda_{a-1}\lambda_1^{-1}$ 为 $T_a(s,n,\lambda)$ 中的单位.

证 对 $1\leq i\leq p^k-1$, 有 $p\big|\binom{p^s}{k}$. 所以, 在 $R_a[x]$ 中, 有 $(x-1)^{p^k}=x^{p^k}-1$. 注意到, 在 $T_a(s,n,\lambda)$ 中,

$$\begin{aligned}(x^n-1)^{p^s}&=x^{p^sn}-1=u\lambda_1+\cdots+u^{a-1}\lambda_{a-1}\\&=u\lambda_1(1+u\lambda_2\lambda_1^{-1}+\cdots+u^{a-2}\lambda_{a-1}\lambda_1^{-1})\\&=u\lambda_1w,\end{aligned}$$

其中 $w=1+u\lambda_2\lambda_1^{-1}+\cdots+u^{a-2}\lambda_{a-1}\lambda_1^{-1}$ 显然是 $T_a(s,n,\lambda)$ 中的单位. 因此, 在 $T_a(s,n,\lambda)$ 中, 有 $\langle(x^n-1)^{p^s}\rangle=\langle u\rangle$. 显然在 $T_a(s,n,\lambda)$ 中, $(x^n-1)^{p^sa-1}\neq0,(x^n-1)^{p^sa}=0$. 故 x^n-1 的幂零指数为 p^sa.

引理 4.2 设 $f(x)\in R_a[x]$ 且 $(f(x),x^n-1)=1$, 则 $f(x)$ 是 $T_a(s,n,\lambda)$ 中的单位.

证 因为 $(f(x),x^n-1)=1$, 所以存在 $g(x),h(x)\in R_a[x]$, 使 $f(x)g(x)+(x^n-1)h(x)=1$, 即 $f(x)g(x)=1-(x^n-1)h(x)$. 由引理 4.1 知, $[(x^n-1)h(x)]^{p^sa}=0$. 故

$$\begin{aligned}1&=1-[(x^n-1)h(x)]^{p^sa}\\&=[1-(x^n-1)h(x)][1+(x^n-1)h(x)+\cdots+((x^n-1)h(x))^{p^sa-1}].\end{aligned}$$

因此 $f(x)g(x)$ 是单位, 从而 $f(x)$ 也是单位.

设 I 表示模 n 的 p^m- 分割陪集的代表元作成的集合. 由于 $(n,p)=1$, 故 x^n-1 在 $R_a[x]$ 中可以唯一分解为两两互素的首 1 的基本不可约多项式 $f_i(x)$ 的乘积 $(i\in I)$, 即 $x^n-1=\prod_{i\in I}f_i(x)$, 记 $f_i'(x)=\frac{x^n-1}{f_i(x)}$. 我们有

引理 4.3 设 $x^n-1=\prod_{i\in I}f_i(x)$, 其中 $f_i(x)$ 为 $R_a[x]$ 上两两互素的首 1 的基本不可约多项式. 则在 $T_a(s,n,\lambda)$ 中, 对任意 $i\in I$ 和任意非负整数 k, 有 $\langle f_i^{p^sa}(x)\rangle=\langle f_i^{p^sa+k}(x)\rangle$.

证 显然 $(f_i(x), f_i'(x)) = 1$, 故由引理 2.2 知, $(\overline{f}_i(x), \overline{f}_i'(x)) = 1$. 从而

$$(\overline{f}_i(x)^k, \overline{f}_i'(x)^{p^s a}) = 1.$$

由引理 2.2 知 $(f_i^k(x), (f_i'(x))^{p^s a}) = 1$. 因此存在 $g(x), h(x) \in R_a[x]$, 使

$$f_i^k(x)g(x) + (f_i'(x))^{p^s a}h(x) = 1.$$

故在 $T_a(s, n, \lambda)$ 中,

$$f_i^{p^s a+k}(x)g(x) = (1 - f_i'^{p^s a}(x)h(x))f_i^{p^s a}(x) = f_i^{p^s a}(x) - (x^n - 1)^{p^s a}h(x) = f_i^{p^s a}(x).$$

这意味着 $\langle f_i^{p^s a}(x)\rangle = \langle f_i^{p^s a+k}(x)\rangle$.

有了以上准备，我们来证明如下定理.

定理 4.4 记号如上. 环 $T_a(s, n, \lambda)$ 是主理想环, 它的理想为 $\langle\prod_{i\in I} f_i^{t_i}(x)\rangle$, 其中 $0 \le t_i \le p^s a$, 即 R_a 中长为 $p^s n$ 的 $\lambda-$ 常循环码有形式 $C = \langle\prod_{i\in I} f_i^{t_i}(x)\rangle, 0 \le t_i \le p^s a$. 进而

$$|C| = p^{ma[p^s a - \sum_{i\in I} t_i \deg(f_i(x))]}.$$

证 设 C 是 R_a 中长为 $p^s n$ 的 $\lambda-$ 常循环码. 记

$$C_u = \{\overline{c} = (c_1 \pmod u, \cdots, c_{p^s a} \pmod u) | \forall c = (c_1, \cdots, c_{p^s a}) \in C\}.$$

则 C_u 是 $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s n}-1\rangle}$ 的理想. 根据 Hensel 引理, $x^n - 1$ 在 $\mathbb{F}_{p^m}$ 上可以分解为两两互素的首 1 的不可约多项式的乘积 $\prod_{i\in I} g_i(x)$, 其中 $g_i(x) = \overline{f}_i(x)$, 且 $C_u = \langle\prod_{i\in I} g_i^{l_i}(x)\rangle, 0 \le l_i \le p^s$. 因此, 对任意 $c \in C$, 存在 $h(x), q(x) \in T_a(s, n, \lambda)$, 使得 $c = h(x)\prod_{i\in I} f_i^{l_i}(x) + uq(x)$. 由引理 4.1, $u \in \langle(x^n - 1)^{p^s}\rangle = \langle\prod_{i\in I} f_i^{p^s}(x)\rangle$. 故

$$c = \prod_{i\in I} f_i^{l_i}(x)[g(x) + \prod_{i\in I} f_i^{p^s - l_i}(x)\widetilde{q}(x)] \in \langle\prod_{i\in I} f_i^{l_i}(x)\rangle.$$

即 $C \subset \langle\prod_{i\in I} f_i^{l_i}(x)\rangle$. 对每个 $i \in I$, 选择 t_i 为 $f_i(x)$ 中的幂 j_i 中的最大者, 这里 $C \subset \langle\prod_{i\in I} f_i^{j_i}(x)\rangle$. 因此 $0 \le t_i \le p^s a$ 和 $C \subset \langle\prod_{i\in I} f_i^{t_i}(x)\rangle$. 由每个 t_i 的最大性知, 存在 $r(x) \in C$, 使 $r(x) = e(x)\prod_{i\in I} f_i^{t_i}(x)$, 这里 $e(x) \in T_a(s, n, \lambda)$, 使得对每个 i 有 $(e(x), f_i(x)) = 1$. 因此

$$(e(x), x^n - 1) = (e(x), \prod_{i\in I} f_i(x)) = 1.$$

于是由引理 4.2 知, $e(x)$ 是 $T_a(s, n, \lambda)$ 中的单位, 故 $\prod_{i\in I} f_i^{t_i}(x) \in C$. 从而 $C = \langle\prod_{i\in I} f_i^{t_i}(x)\rangle$. 由引理 4.3, 可取 $0 \le t_i \le p^s a$, 进一步, 对 $C = \langle\prod_{i\in I} f_i^{t_i}(x)\rangle$, 有

$$|C| = |R_a|^{p^s n - \sum_{i\in I} t_i \deg(f_i(x))} = p^{ma[p^s a - \sum_{i\in I} t_i \deg(f_i(x))]}.$$

下面推论是定理 4.4 的显然结果.

推论 4.5 R_a 上长为 p^sn 的 λ - 常循环码的个数为 $(p^sa+1)^{|I|}$, 这里 I 是模 n 的 p^m - 分圆陪集的完全代表集.

定理 4.6 设 $C=\langle\prod\limits_{i\in I}f_i^{t_i}(x)\rangle$ 是 R_a 上长为 p^sn 的 λ - 常循环码. 则它的对偶码 $C^\perp$ 是 R_a 上长为 p^sn 的 λ^{-1} - 常循环码, 且 $|C^\perp|=p^{ma\sum\limits_{i\in I}t_i\deg(f_i(x))}$. 特别地, $C^\perp$ 是 λ - 常循环码当且仅当 $a=2$. 在这种情形下, $C^\perp=\langle\prod\limits_{i\in I}(f_i^*(x))^{p^sa-t_i}\rangle$.

证 因为 $|C|\cdot|C^\perp|=|R_a|^{p^sn}$, 所以

$$|C^\perp|=\frac{|R_a|^{p^sn}}{|C|}=\frac{p^{map^sn}}{p^{ma(p^sa-\sum\limits_{i\in I}t_i\deg(f_i(x)))}}=p^{ma\sum\limits_{i\in I}t_i\deg(f_i(x))}.$$

注意到, $C^\perp$ 是 $\lambda-$ 常循环码当且仅当 $\lambda^{-1}=\lambda$. 即 $a=2$. 此时, 取

$$C_1=\langle\prod_{i\in I}f_i^{p^sa-t_i}(x)\rangle\subset T_a(s,n,\lambda).$$

由于

$$\prod_{i\in I}f_i^{p^sa-t_i}(x)\prod_{i\in I}f_i^{t_i}(x)=\prod_{i\in I}f_i^{p^sa}(x)=(x^n-1)^{p^sa}=0.$$

故 $C_1\subset\mathrm{Ann}(C)$. 从而 $C_1^*\subset\mathrm{Ann}^*(C)=C^\perp$. 另一方面, 由定理 4.4, 有

$$|C_1^*|=|C_1|=p^{ma\sum\limits_{i\in I}t_i\deg(f_i(x))}=|C^\perp|.$$

因此, $C^\perp=C_1^*=\left\langle\prod\limits_{i\in I}(f_i^*(x))^{p^sa-t_i}\right\rangle$.

定理 4.7 设 $C=\langle\prod\limits_{i\in I}f_i^{t_i}(x)\rangle$ 是 R_a 上长为 p^sn 的 λ - 常循环码, $0\le t_i\le p^sa$, $x^n-1=\prod\limits_{i\in I}f_i(x)$, 这里 $f_i(x)$ 是 $R_a[x]$ 上两两互素的首 1 的基本不可约多项式. 记 $\overline{C}=\{\overline{f}(x)|u^{a-1}f(x)\in C\}$, $C'=\langle\prod\limits_{i\in I}\overline{f}_i^{k_i}(x)\rangle$, 其中 $k_i=t_i-\min\{p^s(a-1),t_i\}$. 那么,

(i) $C\cap\langle u^{a-1}\rangle=\langle u^{a-1}\prod\limits_{i\in I}f_i^{k_i}(x)\rangle$;

(ii) $\overline{C}=C'$;

(iii) $d(C)=d(C')$.

证 (i) 因为 $\langle u\rangle=\langle(x^n-1)^{p^s}\rangle=\langle\prod\limits_{i\in I}f_i^{p^s}(x)\rangle$, 所以 $\langle u^{a-1}\rangle=\langle\prod\limits_{i\in I}f_i^{p^s(a-1)}(x)\rangle$. 从而,

$$\begin{aligned}C\cap\langle u^{a-1}\rangle &= \langle\prod_{i\in I}f_i^{t_i}(x)\rangle\cap\langle\prod_{i\in I}f_i^{p^s(a-1)}(x)\rangle=\langle\prod_{i\in I}f_i^{\max\{p^s(a-1),t_i\}}(x)\rangle\\ &= \langle\prod_{i\in I}f_i^{p^s(a-1)}(x)\prod_{i\in I}f_i^{t_i-\min\{p^s(a-1),t_i\}}(x)\rangle=\langle u^{a-1}\prod_{i\in I}f_i^{k_i}(x)\rangle.\end{aligned}$$

(ii) 设 $a(x)\in C'$, 则存在 $\overline{r}(x)\in\mathbb{F}_{p^m}[x]$, 使得 $a(x)=\overline{r}(x)\prod\limits_{i\in I}\overline{f}_i^{k_i}(x)$. 因此

$$u^{a-1}r(x)\prod_{i\in I}f_i^{k_i}(x)\in\langle u^{a-1}\prod_{i\in I}f_i^{k_i}(x)\rangle=C\cap\langle u^{a-1}\rangle,$$

故 $u^{a-1}r(x)\prod\limits_{i\in I}f_i^{k_i}(x)\in C$. 从而 $a(x)=\overline{r}(x)\prod\limits_{i\in I}\overline{f}_i^{k_i}(x)\in\overline{C}$. 这就推出 $C'\subset\overline{C}$. 反过来, 设 $\overline{b}(x)\in\overline{C}$, 则 $u^{a-1}b(x)\in C$. 因此

$$u^{a-1}b(x)\in C\cap\langle u^{a-1}\rangle=\langle u^{a-1}\prod_{i\in I}f_i^{k_i}(x)\rangle.$$

故存在 $\overline{h}(x)\in\mathbb{F}_{p^m}[x]$, 使 $\overline{b}(x)=\overline{h}(x)\prod\limits_{i\in I}\overline{f}_i^{k_i}(x)$, 即 $\overline{b}(x)\in C'$. 因此 $\overline{C}\subset C'$. 故 $\overline{C}=C'$.

(iii) $\forall c(x)\in C$, 有 $u^{a-1}c(x)\in C$. 从而 $d(C\cap\langle u^{a-1}\rangle)=d(C)$. 显然 $w(\overline{c}(x))=w(u^{a-1}c(x))$. 故 $d(C)=d(C')$.

参 考 文 献

[1] Berman S D. Semisimple cyclic and Abelian codes Ⅱ (in Russian)[J]. Kibernetika, 1967, 3: 21–30.

[2] Castagnoli G, Massey J L, Schoeller P A, Seemann N V. On repeated-root cyclic codes[J]. IEEE Trans. Inform. Theory, 1991, 37: 337–342.

[3] Van Lint J H. Repeated-root cyclic codes[J]. IEEE Trans. Inform. Theory, 1991, 37: 343–344.

[4] Kai Xiaoshan, Zhu Shixin, Li Ping. $(1+\lambda u)-$ constacyclic codes over $\frac{\mathbb{F}_p[u]}{\langle u^m\rangle}$[J]. J. Franklin Inst., 2010, 347: 751–762.

[5] Liu Xiusheng, Xu Xiaofang. Cyclic and negncyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}[u]+u\mathbb{F}_{p^m}[u]$[J]. Acta Math. Scientia, 2014, 34B(3): 829–839.

[6] 李平, 朱士信. 一类四元环上常循环码是自由码的充要条件 [J]. 数学杂志, 2008, 28(2): 124–128.

[7] Dinh H Q, Lopez-Penmouth S R. Cyclic and negacyclic codes over finite chain rings[J]. IEEE Trans. Inform. Theory, 2004, 51: 1728–1744.

[8] Norton G H, Salagean A. On the structure of linear and cyclic codes over finite chain rings[J]. AAECC, 2000, 10: 489–506.

[9] McDonald B R. Finite rings with identity[M]. New York: Marcal Dakker, 1974.

[10] Dinh H Q, Nguyen D T. On some classes of constacyclic codes over polynomial residue rings[J]. Advances in Math. communications, 2012, 6(2): 125–191.

A CLASS OF CONSTACYCLIC CODES OVER $\frac{\mathbb{F}_{p^m}[u]}{\langle u^a\rangle}$

LIU Hua-lu

(*School of Mathematics and Physics, Hubei Polytechnic University, Huangshi 435003, China*)

Abstract: We study a class of λ -constacyclic codes. By using the unique factorizations of x^n-1 into a product of monic basic irreducible pairwise coprime polynomials over $R_a[x]$, we characterize the structure of λ -constacyclic codes of length p^sn over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^a\rangle}$, which generalizes the result of [4].

Keywords: repeated-constacyclic codes; dual codes; finite chain ring

2010 MR Subject Classification: 11T71