第43卷第8期 中国科学技术大学学报 Vol. 43, No. 8
2013年8月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Aug. 2013

文章编号:0253-2778(2013)08-0622-04

Z_{p^s} 上的准循环码

储 强,朱士信

(合肥工业大学数学学院,安徽合肥 230009)

摘要:研究了有限链环 $R=Z_{p^s}$ 上长为 mn 准循环码,其中,p 是素数,s 是任意的正整数.通过对其结构的研究,确定了 R 上长为 mn 准循环码等价于 A^n 的 A 子模,其中,$A=R[x]/(x^m-1)$.然后,研究了以下情形:当 $\gcd(m,p)=1$ 时,R 上准循环码可以分解成有限个不可约循环子模的直和.

关键词:准循环码;不可约模;子模;直和

中图分类号:TN918.1 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2013.08.003

AMS Subject Classification (2000): Primary 94B05; Secondary 94B15

引用格式: Chu Qiang, Zhu Shixin. Quasi-cyclic codes over Z_{p^s} [J]. Journal of University of Science and Technology of China, 2013,43(8):622-625.

储强,朱士信. Z_{p^s} 上的准循环码[J]. 中国科学技术大学学报,2013,43(8):622-625.

Quasi-cyclic codes over Z_{p^s}

CHU Qiang, ZHU Shixin

(*School of Mathematics, Hefei University of Technology, Hefei* 230009, *China*)

Abstract: The quasi-cyclic codes of length mn over $R=Z_{p^s}$ were studied, where p is a prime and s is an arbitrary positive integer. By exploring the structure, the quasi-cyclic codes of length mn over R were shown to be equivalent to A-submodules of A^n, where $A=R[x]/(x^m-1)$. Then the case was studied in which quasi-cyclic codes over R can be decomposed into a direct sum of a fixed number of irreducible cyclic submodules when $\gcd(m,p)=1$.

Key words: quasi-cyclic codes; irreducible modules; cyclic modules; direct sum

0 引言

准循环码是循环码的自然推广,由其可以构造出大量的好码.一些重要的码,如 Turbo 码、卷积码等,与准循环码有着紧密的联系.所以准循环码一直是众多学者研究的热点.有限域上的准循环码理论已经被众多学者研究.Townsend 等[1]第一次给出了自正交准循环的定义,并且给出了一串好码,具有很好的极小距离和高效性.Coman 等[2]讨论了有限域上准循环码的结构和计数.近年来,有限环上的准循环码理论也引起了众多学者的兴趣.Pei 等[3-4]研究了模 4 的整数环上准循环码的结构.文献中[5]讨论了 Z_q 和 Galois 环上准循环码的结构性质和距离的下界等问题.曹永林[6]讨论 Galois 环上广义准循环码的结构性质,并且给出了计数.Ling[7]研究了有限链环上准循环码直和分解的结构,讨论了离散傅

收稿日期:2012-03-22;**修回日期**:2012-05-15

基金项目:国家自然科学基金(60973125)资助.

作者简介:储强,男,1988 年生,硕士. 研究方向:代数编码. E-mail: cq118to632@163.com

通讯作者:朱士信,博士/教授. E-mail: zhushixin@hfut.edu.cn

立叶变换. 本文中采用与文献[6]不同的思想和方法，给出了 Z_{p^s} 上的准循环码代数结构，即可以具体分解成有限个不可约循环子模的直和.

1　预备知识

令 $R=Z_{p^s}$ 是模 p^s 的整数剩余类环，其中，p 是素数. R^n 是 R 上长为 n 的向量集合. R^n 中任意 R 子模叫做长为 n 的 R 线性码. 设 C 是长为 mn 的 R 线性码，如果

$$\begin{aligned}&\forall\, \underline{c}(x)=(c_{00},c_{10},\cdots,c_{n-1,0};c_{01},c_{11},\cdots,c_{n-1,1};\cdots;\\&c_{0,m-1},c_{1,m-1},\cdots,c_{n-1,m-1})\in C\Rightarrow\\&(c_{0,m-1},c_{1,m-1},\cdots,c_{n-1,m-1};c_{00},c_{10},\cdots,c_{n-1,0};\cdots;\\&c_{0,m-2},c_{1,m-2},\cdots,c_{n-1,m-2})\in C\end{aligned}\tag{1}$$

我们就称 C 是 R 上的准循环码.

假设 $A=R[x]/(x^m-1)$，A^n 是 n 个 A 的直积. 定义

$$\psi:\underline{c}(x)\mapsto \underline{c}(x)=(c_0(x),c_1(x),\cdots,c_{n-1}(x)),$$

其中，$c_i(x)=\sum_{j=0}^{m-1}c_{ij}x^j$，是 R^m 到 A^n 一一映射，则式(1)等价于 $\forall\, \underline{c}(x)\in\psi(C)\Rightarrow \underline{xc}(x)\in\psi(C)$. 则 C 是准循环码当且仅当 $\psi(C)$ 是 A^n 的 A 子模.

定义“$-$”是 R 到 Z_p 的模 p 的映射. 映射“$-$”可以自然地推广至 $R[x]$ 到 $Z_p[x]$ 上的映射，即

$$-:R[x]\mapsto Z_p[x]$$

$$a_0+a_1x+\cdots+a_nx^n\to \bar{a}_0+\bar{a}_1x+\cdots+\bar{a}_nx^n.$$

对 $\forall\, f(x)\in R[x]$ 是首项系数为 1 的多项式，若 $\bar{f}(x)\in Z_p[x]$ 是不可约的，由 Hensel 引理[3]，那么 $f(x)$ 是基本不可约多项式.

2　准循环码的代数结构

设 $\gcd(m,p)=1$，那么在 $R[x]$ 中 x^m-1 唯一分解成 $x^m-1=h_1(x)h_2(x)\cdots h_r(x)$，其中，$h_i(x)$ $(i=1,2,\cdots r)$ 是 R 上次数为 e_i、首项系数为 1 的基本不可约多项式.

令 $\hat{h}_i(x)=(x^m-1)/h_i(x)$. 因为 $h_i(x)$ 和 $\hat{h}_i(x)$ 互素，那么存在 $\lambda_{i1}(x)$，$\lambda_{i2}(x)\in R[x]$ 使得 $\lambda_{i1}(x)h_i(x)+\lambda_{i2}(x)\hat{h}_i(x)=1$. 设

$$\theta_i(x)=\lambda_{i2}(x)\hat{h}_i(x),\ i=1,2,\cdots,r,$$

同文献[1，定理 2]，我们有如下结论：

定理 2.1　① 对 $i=1,2,\cdots,r$，$\theta_i(x)$ 是 $A\hat{h}_i(x)$ 的单位元，且 $A\hat{h}_i(x)=A\theta_i(x)$；

② $A=A\hat{h}_1(x)\oplus A\hat{h}_2(x)\oplus\cdots\oplus A\hat{h}_r(x)$；

③ 对 $i=1,2,\cdots,r$，$R[x]/(h_i(x))$ 到 $A\hat{h}_i(x)$ 上的映射：$f(x)+(h_i(x))\mapsto f(x)\hat{h}_i(x)$ 是环同构.

对任意 $\underline{a}(x)=(a_0(x),a_1(x),\cdots,a_{n-1}(x))\in A^n$，定义 $\underline{a}(x)$ 的阶是满足 $f(x)\underline{a}(x)=\underline{0}$ 的次数最低的非零首项系数为 1 的多项式 $f(x)$，记为 $\mathrm{ord}(\underline{a}(x))$. 我们约定 $\mathrm{ord}(\underline{0})=1$. 对任意的 $\underline{a}(x)\in A^n$，有 $(x^m-1)\underline{a}(x)=\underline{0}$，故 $\mathrm{ord}(\underline{a}(x))\mid(x^m-1)$.

设 M 是 A^n 的子模，定义 M 的阶 $\mathrm{ord}(M)$ 是对 $\forall\, \underline{a}(x)\in M$ 满足 $f(x)\underline{a}(x)=\underline{0}$ 的次数最低非零首项系数为 1 的多项式 $f(x)$. 显然，$\mathrm{ord}(M)\mid(x^m-1)$. 如果存在 $\underline{a}(x)\in M$ 使得 $M=A\,\underline{a}(x)$，那么称 M 是循环模. 如果 $\mathrm{ord}(M)$ 是 R 上基本不可约多项式，则称 M 是不可约模.

对 $i=1,2,\cdots,r$，令 $Q_i=A^n\hat{h}_i(x)$，并称其为做 A^n 的准素分量，则 $\mathrm{ord}(Q_i)=h_i(x)$，且由定理 2.1 得 Q_i 的类型是 p^{se_i}. 易知 $A^n=Q_1\oplus Q_2\oplus\cdots\oplus Q_r$. 设 C 是 R 上准循环码，$C_i=C\cap Q_i$ 是 C 的准素分量，那么

$$C=C_1\oplus C_2\oplus\cdots\oplus C_r.$$

引理 2.1　设 $h(x)$ 是 x^m-1 次数为 e 的基本不可约因子，$Q=A^n\hat{h}(x)$ 是 A^n 的准素分量. 对 $i=0,1,\cdots,s-1$，如果 $p^i\,\underline{a}_i(x)\in p^iQ$ 且 $p^{s-1}\underline{a}_i(x)\neq\underline{0}$，那么 $M_i=p^iA\,\underline{a}_i(x)$ 是阶为 $h(x)$ 类型为 $p^{(s-i)e}$ 不可约循环子模.

证明　显然，M_i 是阶为 $h(x)$ 的不可约循环子模. 下面证明其类型为 $p^{(s-i)e}$. 对于 $i=0,1,\cdots,s-1$，定义映射

$$\varphi:\quad A\to M_i,$$

$$f(x)+(x^m-1)\mapsto p^if(x)\,\underline{a}_i(x).$$

显然，φ 是模满同态，且

$$\ker\varphi\supseteq(p^{s-i},h(x)+(x^m-1)).$$

同时对 $\forall\, f(x)+(x^m-1)\in A$ 且满足 $p^if(x)\underline{a}(x)=\underline{0}$. 由于 $h(x)$ 是首项系数为 1 的基本不可约多项式，有 $f(x)=q(x)h(x)+r(x)$，则

$$p^ir(x)\,\underline{a}_i(x)=p^if(x)\,\underline{a}_i(x)-p^iq(x)h(x)\,\underline{a}_i(x)=\underline{0}.$$

若 $r(x)=0$，那么该结论显然成立. 若 $r(x)\neq0$，则 $\deg r(x)<e$. 若 $\bar{r}(x)\neq0$，有 $(\bar{r}(x),\bar{h}(x))=1$，则 $(r(x),h(x))=1$. 所以存在 $\lambda_1(x)$，$\lambda_2(x)\in Z_{p^s}[x]$，有

$$1=\lambda_1(x)r(x)+\lambda_2(x)h(x),$$

则 $p^i\,\underline{a}_i(x)=\underline{0}$，矛盾！即 $\bar{r}(x)=0$. 所以

$$r(x) = pr_1(x).$$

同理,有 $\overline{r}_1(x)=p^2 r_2(x)$. 这样一直继续下去,最后我们可以得到

$$r(x) = p^{s-i}r_{s-i}(x).$$

综合上述,

$$\ker\varphi=(p^{s-i},h(x)+(x^m-1)).$$

根据环同态基本定理,

$$M\cong A/(\ker\varphi)\cong Z_{p^{s-i}}[x]/(h(x)),$$

那么 $|M|=p^{(s-i)e}$,从而得证. □

引理 2.2 $h(x)$和 Q 由引理 2.1 给出,设 M 是 Q 的子模. 则 M 可分解为 $k_1+k_2+\cdots+k_s$ 个不可约循环子模的直和,即

$$M=\bigoplus_{i=1}^{k_1} A\,\underline{a}_{1i}(x)\oplus\bigoplus_{i=1}^{k_2} pA\,\underline{a}_{2i}(x)\oplus\cdots\oplus\bigoplus_{i=1}^{k_s} p^{s-1}A\,\underline{a}_{ri}(x),$$

其中,$k_1,k_2,\cdots,k_s$ 分别表示类型为 $p^s,p^{(s-1)e},\cdots,p^e$ 的不可约循环子模个数.

证明 设 $\overline{M}_1=\{\underline{a}(x)\in M\mid p^{s-1}\underline{a}(x)=\underline{0}\}$. 首先任取 $\underline{a}_{11}(x)\in M\backslash\overline{M}_1$. 假设取定 $\underline{a}_{11}(x),\underline{a}_{12}(x),\cdots,\underline{a}_{1i}(x)\in M\backslash\overline{M}_1$,使得 $\sum_{j=1}^{i}A\,\underline{a}_{1j}(x)$ 是直和. 若 $M\neq\sum_{j=1}^{i}A\,\underline{a}_{1j}(x)+\overline{M}_1$,取 $\underline{a}_{1,i+1}(x)\in M$,且 $\underline{a}_{1,i+1}(x)\notin\sum_{j=1}^{i}A\,\underline{a}_{1j}(x)+\overline{M}_1$,则 $\sum_{j=1}^{i+1}A\,\underline{a}_{1j}(x)$ 是直和.

事实上,设

$$\underline{b}(x)\in\Big(\sum_{j=1}^{i}A\,\underline{a}_{1j}(x)\Big)\cap A\,\underline{a}_{1,i+1}(x)$$

且 $\underline{b}(x)\neq 0$. 如果 $\underline{b}(x)\notin\overline{M}_1$,那么 $A\,\underline{b}(x)\subseteq A\,\underline{a}_{1,i+1}(x)$,类型均为 p^s,故 $A\underline{b}(x)=A\,\underline{a}_{1,i+1}(x)$. 那么 $\underline{a}_{1,i+1}(x)\in A\,\underline{b}(x)\subseteq\sum_{j=1}^{i}A\,\underline{a}_{1j}(x)$,矛盾!若 $\underline{b}(x)=p^l\underline{b}_1(x)\in\overline{M}_1$,且 $p^{s-1}\underline{b}_1(x)\neq 0$,$1\leqslant l\leqslant s-1$,那么 $p^lA\,\underline{b}_1(x)\subseteq p^lA\,\underline{a}_{i+1}(x)$,且类型都为 $p^{(s-l)e}$,所以 $p^lA\,\underline{b}_1(x)=p^lA\,\underline{a}_{1,i+1}(x)$. 那么存在 $\underline{d}_{1,i+1}(x)\in A^n$,$c_{1,i+1}(x)\in A$ 使得

$$\underline{a}_{1,i+1}(x)=c_{1,i+1}(x)\,\underline{b}_1(x)+p^{(s-l)}\,\underline{d}_{1,i+1}(x).$$

另外,因为

$$p^l\,\underline{b}_1(x)\in p^l\sum_{j=1}^{i}A\,\underline{a}_{1j}(x),$$

所以

$$\underline{b}_1(x)=\sum_{j=1}^{i}c_{1j}(x)\,\underline{a}_{1j}(x)+p^{s-l}\,\underline{d}(x),$$

其中,$\underline{d}(x)\in A^n$,$c_{1i}(x)\in A$. 那么有

$$\underline{a}_{1,i+1}(x)\in\sum_{j=1}^{i}A\,\underline{a}_{1j}(x)+\overline{M}_1,$$

矛盾! 所以可取 $\underline{a}_{11}(x),\underline{a}_{12}(x),\cdots,\underline{a}_{1k_1}(x)$ 使

$$M=\bigoplus_{i=1}^{k_1}A\,\underline{a}_{1i}(x)+\overline{M}_1.$$

考虑 $\overline{M}_1$,设

$$\overline{M}_2=\{\underline{a}(x)\in\overline{M}_1\mid p^{s-2}\,\underline{a}(x)=\underline{0}\}.$$

同理,取

$$pa_{21}(x),pa_{22}(x),\cdots,pa_{2k_2}(x)\in\overline{M}_1\backslash\Big(\sum_{i=1}^{k_1}pA\,\underline{a}_{1i}(x)+\overline{M}_2\Big)$$

使得

$$M=\bigoplus_{i=1}^{k_1}A\,\underline{a}_{1i}(x)+\bigoplus_{i=1}^{k_2}pA\,\underline{a}_{2i}(x)+\overline{M}_2.$$

这样一直继续,最后得到

$$M=\bigoplus_{i=1}^{k_1}A\,\underline{a}_{1i}(x)\oplus\bigoplus_{i=1}^{k_2}pA\,\underline{a}_{2i}(x)\oplus\cdots\oplus\bigoplus_{i=1}^{k_s}p^{s-1}A\,\underline{a}_{ri}(x).$$

若 M 分解不唯一,即

$$M=\bigoplus_{i=1}^{l_1}A\,\underline{a}_{1i}(x)\oplus\bigoplus_{i=1}^{l_2}pA\,\underline{a}_{2i}(x)\oplus\cdots\oplus\bigoplus_{i=1}^{l_s}p^{s-1}A\,\underline{a}_{ri}(x).$$

由于 M 类型不变,

$$p^{sk_1e}p^{(s-1)k_1e}\cdots p^{k_se}=p^{sl_1e}p^{(s-1)l_1e}\cdots p^{l_se},$$

那么 $k_i=l_i$,$i=1,2,\cdots,s$. 从而得证. □

定理 2.2 任意的准循环码 C 可分解成 $k_{11}+k_{12}+\cdots+k_{1s}+\cdots+k_{r1}+k_{r2}+\cdots+k_{rs}$($0\leqslant k_{i1}+k_{i2}+\cdots+k_{is}\leqslant n$)个不可约循环子模的直和. 其中,$k_{i1},k_{i2},\cdots,k_{is}$,$1\leqslant i\leqslant r$,是 P_i 中类型分别为 $p^s,p^{(s-1)e},\cdots,p^e$ 不可约循环模的个数. 定义 C 的指数是向量

$$\underline{k}=(k_{11},k_{12},\cdots,k_{1s},\cdots,k_{r1},k_{r2},\cdots,k_{rs}),$$

且具有不变性.

推论 2.1 若

$$\underline{k}=(k_{11},k_{12},\cdots,k_{1s},\cdots,k_{r1},k_{r2},\cdots,k_{rs})$$

是准循环码 C 的指数,则 C 是不可约子模,当且仅当对 $1\leqslant i\leqslant r$,除去其中某一个 i 外都有 $k_{i1}=k_{i2}=\cdots=k_{is}=0$.

证明 由 $\prod_{k_{i1}\neq 0\text{或}k_{i2}\neq 0\text{或}\cdots\text{或}k_{is}\neq 0}h_i(x)$ 可知. □

推论 2.2 若

$$\underline{k}=(k_{11},k_{12}\cdots,k_{1s},\cdots,k_{r1},k_{r2},\cdots,k_{rs})$$

是准循环码 C 的指数，则 C 是循环模当且仅当 $(k_{i1},k_{i2},\cdots,k_{is})\in T=\{(0,0,\cdots,0),(1,0,\cdots,0),\cdots,(0,0,\cdots,1)\}$，其中，$i=1,2,\cdots,r$.

证明　如果 $C=A\underline{a}(x)$是循环子模，

$$A\theta_i(x)\ \underline{a}(x)\subseteq C\cap Q_i=C_i,\ i=1,2,\cdots,r,$$

其中，$\theta_i(x)$是由定理 2.1 给出. 另外，$\forall\, b(x)\underline{a}(x)\in C_i$，有

$$b(x)\ \underline{a}(x)=b(x)\theta_i(x)\ \underline{a}(x)\in A\theta_i(x)\ \underline{a}(x).$$

那么 $A\theta_i(x)\underline{a}(x)=C_i$，所以 $(k_{i1},k_{i2},\cdots,k_{is})\in T$，$i=1,2,\cdots,r$.

如果 $(k_{i1},k_{i2},\cdots,k_{is})\in T$，$i=1,2,\cdots,r$，则 C 可以分解成

$$C=A\underline{a}_1(x)\oplus A\underline{a}_2(x)\oplus\cdots\oplus A\underline{a}_r(x),$$

其中，$\underline{a}_i(x)\in Q_i$，某些 $\underline{a}_i(x)$ 可能为 $\underline{0}$. 设 $\underline{a}(x)=\underline{a}_1(x)+\underline{a}_2(x)+\cdots+\underline{a}_r(x)$，则 $A\underline{a}(x)\subseteq C$. 又对 $i=1,2,\cdots,r$，有

$$\underline{a}_i(x)=\underline{a}_i(x)\theta_i(x)=\underline{a}(x)\theta_i(x)\in A\underline{a}(x),$$

则 $C\subseteq A\underline{a}(x)$. 所以 $C=A\underline{a}(x)$. 从而得证. □

3　结论

在本文中，我们研究了 R 上单根情况下准循环码. 基于多项式 x^m-1 在 R 上的分解，给出了 R 上长为 mn 指数为 n 的准循环码在每个分量环上线性码的直和分解. 进一步，证明了准循环可以分解成不可约循环子模上线性码的直和，并且给出了具体的分解公式. 准扭码是准循环码的自然推广. 虽然有限链环上准扭码的分解存在困难，但是在今后的研究中可以考虑某一类有限链环上准扭码的不可约循环子模的分解.

参考文献(References)

[1] Townsend R, Weldon E. Self-orthogonal quasi-cyclic codes[J]. IEEE Trans Inform Theory, 1967, 13: 183-195.

[2] Conan J, Seguin G. Structural properties and enumeration of quasi-cyclic codes [J]. AAECC, 1993, 4: 25-39.

[3] Pei J Y, Zhang X J. Quaternary quasi-cyclic codes [J]. Appl Math J Chinese Univ, 2006, 23(3):359-365.

[4] Pei J Y, Zhang X J. 1-generator quasi-cyclic codes[J]. Jrl Syst Sci & Complexity, 2007, 20: 554-561.

[5] Bhaintwal M, Wasan S K. On quasi-cyclic codes over Z_q[J]. AAECC, 2009, 20: 459-480.

[6] Cao Y L. Generalized quasi-cyclic codes over Galois rings: Structural properties and enumeration [J]. AAECC, 2011, 22:219-233.

[7] Ling S, Sole P. On the algebraic structure of quasi-cyclic codes Ⅱ: Chain rings [J]. Design Codes Cryp, 2003,30:113-130.

[8] Mac Williams F J, Sloane N J A. The Theory of Error-Correcting Codes [M]. Amsterdam: North-Holland, 1977.

[9] Wan Z X. Quaternary Codes [M]. Singapore: World Scientific, 1997.