形式幂级数环中的循环码

刘修生

（黄石理工学院 数理学院，湖北 黄石 435003）

摘 要：研究了形式幂级数环与有限链环上的循环码与负循环码，利用环同构与交换图技术得到这 2 类环上循环码与负循环码，以及 Dougherty 等得到的形式幂级数环上的循环码的投影码也是循环码的结果，给出了形式幂级数环上码为循环码的一个充要条件。借助这一条件，得到了含有形式幂级数环的中国积中循环码的投影码的循环性。

关键词：形式幂级数环；循环码；投影码；中国积

中图分类号：O157.4 **文献标识码**：A **文章编号**：1000-436X(2011)02-0068-04

Cyclic codes over formal power series rings

LIU Xiu-sheng

(School of Math.and Physics, Huangshi Institute of Technology, Huangshi 435003, China)

Abstract: Cyclic and negacyclic codes over formal power series and finite chain rings were studied. By using ring isomorphism and exchange graph, an obtained results of cyclic and negacyclic codes over two classes ,Dougherty, Liu and Park gave that the projective codes of cyclic codes over the formal power series ring were cyclic codes, sufficient and necessary conditions for cyclic codes gave over this class of rings.Thus it is obvious that projective codes of the cyclic codes over the Chinese product with formal power serious ring are cyclic code.

Key words: formal power series rings; cyclic codes; projective codes; Chinese product

1 引言

循环码是一类非常重要的码，首先是在二元域 $\mathbb{F}_2$ 中研究循环码，然后扩充到有限域 F_q 上（$q=p^r, p$ 为素数，$r\geqslant 1$）。由于有限域 F_q 上长度为 n 的循环码可以看成环 $F_q[x]\Big/\langle x^n-1\rangle$ 的一个理想，在文献[1]中给出了这种域上循环码的构造。在文献[2]中，Norton 和 Salagean 应用环同构技术扩充了文献[1]与文献[3]得到的定理推广到有限链环。接下来，Dinh 和 Lopez-permouth 在文献[4]中用不同于文献[2]的方法研究了有限链环上循环码的生成元。近年来，Dougherty 等研究了形式幂级数环 R_∞ 上循环码的投影码的循环性，得到了一系列的结果[5]。本文的目的是：由形式幂级数环 R_∞ 上码 C 投影码的循环性来研究码 C 的循环性，以及含有形式幂级环 R_∞ 的中国积中循环码来研究它的投影码的循环性。

2 有限链环与形式幂级数环

一个环 R 称为链环，如果它的所有理想在包含关系上是线性有序的，显然链环上的理想都是主理想，且是局部主理想环，因此它有唯一的最大理想。

设 R 是一个有限链环，I 是它唯一的最大理想，让 $\bar{\gamma}$ 是的 I 生成元，则

$$I=\langle\bar{\gamma}\rangle=R\bar{\gamma}=\{\beta\bar{\gamma}|\beta\in R\}$$

于是

收稿日期：2010-03-11；修回日期：2010-06-25

$$R=\left\langle \bar{\gamma}^{0}\right\rangle \supseteq \left\langle \bar{\gamma}^{1}\right\rangle \supseteq \cdots \supseteq \left\langle \bar{\gamma}^{i}\right\rangle \supseteq \cdots \tag{1}$$

由于 R 为有限环，所以在式(1)中的链不可能是无限的。因此，存在正整数 i 使 $\left\langle \bar{\gamma}^{i}\right\rangle =\{0\}$。设 e 是使 $\left\langle \bar{\gamma}^{e}\right\rangle =\{0\}$ 的最小正整数，这个数 e 叫做 $\bar{\gamma}$ 的幂零指数。

使用 $R^{\times}$ 表示 R 中所有在乘法运算下的单位作为的集合。记 $F=R/I=R/\left\langle \bar{\gamma}\right\rangle$，则 F 是一个域，称为主理想环 I 的剩余类域。设它的特征为素数 p，则存在正整数 q 和 r，使 $|F|=q=p^{r}$。显然 $\left|F^{\times}\right|=p^{r}-1$。

下面给出 2 个引理[6]。

引理 1[6]　记号如上，对任意 $0\neq r\in R$，存在唯一整数 i 且 $0\leqslant i\leqslant e$，使得 $r=\mu\bar{\gamma}^{i}$，这里 μ 是一个单位且在模 $\bar{\gamma}^{e-i}$ 下是唯一的。

引理 2[6]　设 R 是具有最大理想 $I=\left\langle \bar{\gamma}\right\rangle$ 的有限链环，$\bar{\gamma}$ 的幂零指数为 e。设 $V\subseteq R$ 是 R 中元素在 $\bar{\gamma}$ 的模同余关系的等价类的代表元作成的集合。则：

1) $\forall r\in R$, 存在唯一的 $r_0,r_1,\cdots,r_{e-1}\in V$，使得 $r=\sum_{i=0}^{e-1}r_i\bar{\gamma}^{i}$；

2) $|V|=|F|$；

3) $\left|\left\langle \bar{\gamma}^{j}\right\rangle\right|=|F|^{e-j}$, $0\leqslant j\leqslant e-1$。

从引理 2 知道 $\forall a\in R$ 有唯一的表达式。

$$a=a_0+a_1\bar{\gamma}+\cdots+a_{e-1}\bar{\gamma}^{e-1} \tag{2}$$

其中，$a_i\in F$。

下面 2 个定义是由 Dougherty 和刘宏伟在文献[5]中给出的。

定义 1[5]　设 i 是一个任意正整数，令

$$R_i=\left\{a_0+a_1\gamma+\cdots+a_{i-1}\gamma^{i-1}\,|\,a_i\in F\right\}$$

其中，在 R_i 中，$\gamma^{i-1}\neq 0$，但 $\gamma^{i}=0$。在 R_i 中，定义 2 种运算

$$\sum_{l=0}^{i-1}a_l\gamma^{l}+\sum_{l=0}^{i-1}b_l\gamma^{l}=\sum_{l=0}^{i-1}(a_l+b_l)\gamma^{l}$$

$$\sum_{l=0}^{i-1}a_l\gamma^{l}\sum_{l'=0}^{i-1}b_{l'}\gamma^{l'}=\sum_{s=0}^{i-1}\Big(\sum_{l+l'=s}a_lb_{l'}\Big)\gamma^{s}$$

则 R_i 是一个有限环。

注意到，当 $i=1$ 时，$R_1=F$；当 $i=e$ 时，$R_e\cong R$。

易证明，对于任意 $i<\infty$，环 R_i 是有唯一最大理想 $\langle\gamma\rangle$ 的有限链环。

定义 2[5]　记号如上，设

$$R_\infty=F[[\gamma]]=\left\{\sum_{l=0}^{\infty}a_l\gamma^{l}\,|\,a_l\in F\right\}$$

则称 R_∞ 为形式幂级数环，显然 $R_\infty^{\times}=\left\{\sum_{j=0}^{\infty}a_j\gamma^{j}\,|\,a_0\neq 0\right\}$，且 R_∞ 为主理想数环。

定义 3　对于任意正整数 $i<\infty$，定义映射

$$R_\infty\to R_i \tag{3}$$

$$\Psi_i:\sum_{l=0}^{\infty}a_l\gamma^{l}\mapsto\sum_{l=0}^{i-1}a_l\gamma^{l} \tag{4}$$

称 Ψ_i 为 R_∞ 到 R_i 的投射映射。

对于任意 $\forall a,b\in R_\infty$，易验证

$$\begin{cases}\Psi_i(a+b)=\Psi_i(a)+\Psi_i(b)\\ \Psi_i(ab)=\Psi_i(a)\Psi_i(b)\end{cases} \tag{5}$$

注意到，映射 Ψ_i 可以很自然地扩充成 R_∞^{n} 到 R_i^{n} 的映射。

定义 4　如果 C 是 R_∞ 上码，对于任意 $i<\infty$，称 $\Psi_i(C)$ 是码 C 在环 R_i 上的投影码。有时，用 C^{i} 表示 $\Psi_i(C)$。

由于循环码与多项式的剩余类环有密切关系。为此将等式(5)定义的映射引入到形式幂级数环 R_∞ 与有限链环 R_i 的多项式中。

设

$$R_\infty[x]=\left\{\sum_{l=0}^{n}a_lx^{l}\,|\,a_l\in R_\infty,n\geqslant 0\right\}$$

是环 R_∞ 上的多项式环。由于 R_∞ 为整环，因此 $R_\infty[x]$ 也为整环。

设 $f(x)=a_0+a_1x+\cdots+a_nx^{n}\in R_\infty[x]$，有下列映射：

$$\Psi_i:\begin{array}{c}R_\infty[x]\to R_i[x]\\ f(x)\mapsto\Psi_i(f(x))\end{array}$$

其中，$\Psi_i(f(x))=\Psi_i(a_0)+\Psi_i(a_1)x+\cdots+\Psi_i(a_n)x^{n}$。

3　R_∞ 上的循环码与负循环码

本节利用 R_∞ 上码 C 的投影码 $\Psi_i(C)$ 的循环性来研究码 C 的循环性。

设 λ 是 R_∞ 上的任一单位，令

$$R_\infty[x]/\left\langle x^{n}-\lambda\right\rangle=\left\{f(x)+\left\langle x^{n}-\lambda\right\rangle\,|\,f(x)\in R_n[x]\right\}$$

对于 $f(x)+\langle x^n-\lambda\rangle, g(x)+\langle x^n-\lambda\rangle \in R_\infty[x]/\langle x^n-\lambda\rangle$，若 $0\leqslant \deg(f(x))<n$，$0\leqslant \deg(g(x))<n$ 且 $f(x)+\langle x^n-\lambda\rangle = g(x)+\langle x^n-\lambda\rangle$，则 $f(x)-g(x)\in \langle x^n-\lambda\rangle$，从而 $f(x)=g(x)$。因此

$$R_\infty[x]/\langle x^n-\lambda\rangle = \{f(x)+\langle x^n-\lambda\rangle \mid f(x)\in R_n[x], \deg(f(x))<n \text{或} f(x)=0\}$$

定义映射 P_λ 如下

$$P_\lambda: \begin{array}{c} R_\infty^n \to R_\infty[x]/\langle x^n-\lambda\rangle \\ (a_0,a_1,\cdots,a_{n-1}) \mapsto a_0+a_1x+\cdots+a_{n-1}x^{n-1}+\langle x^n-\lambda\rangle \end{array}$$

特别地，如果取 $\lambda=1$ 或 $\lambda=-1$，得到下面 2 个映射 P_1 和 P_{-1}。

$$P_1: \begin{array}{c} R_\infty^n \to R_\infty[x]/\langle x^n-\lambda\rangle \\ (a_0,a_1,\cdots,a_{n-1}) \mapsto a_0+a_1x+\cdots+a_{n-1}x^{n-1}+\langle x^n-1\rangle \end{array}$$

$$P_{-1}: \begin{array}{c} R_\infty^n \to R_\infty[x]/\langle x^n-\lambda\rangle \\ (a_0,a_1,\cdots,a_{n-1}) \mapsto a_0+a_1x+\cdots+a_{n-1}x^{n-1}+\langle x^n+1\rangle \end{array}$$

设 C 是 R_∞^n 的任意集合，记

$$P_\lambda(C) = \left\{c_0+c_1x+\cdots+c_{n-1}x^{n-1}+\langle x^n-\lambda\rangle \mid (c_0,c_1,\cdots,c_{n-1})\in C\right\}$$

定义 5 设 C 是 R_∞ 上长度 n 的线性码，如果对于任意 $c=(c_0,c_1,\cdots,c_{n-1})\in C$，有 $(\lambda c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$，则称 C 为 R_∞ 上的 λ 循环码。当 $\lambda=1$ 时，称 C 为 R_∞ 上的循环码。当 $\lambda=-1$ 时，称 C 为 R_∞ 上的负循环码。

引理 3 R_∞ 上一个长度为 n 的线性码 C 是 λ 循环码，当且仅当 $P_\lambda(C)$ 是 $R_\infty[x]/\langle x^n-\lambda\rangle$ 的理想。

证明 设线性码 C 是 R_∞ 上 λ 循环码，则对于任意 $c=(c_0,c_1,\cdots,c_{n-1})\in C$，有 $(\lambda c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$。于是 $\forall\ c_0+c_1x+\cdots+c_{n-1}x^{n-1}+\langle x^n-\lambda\rangle \in P_\lambda(C)$，由于

$$\left(x+\langle x^n-\lambda\rangle\right)\left(c_0+c_1x+\cdots+c_{n-1}x^{n-1}+\langle x^n-\lambda\rangle\right) = \lambda c_{n-1}+c_0x+c_1x^2+\cdots+c_{n-2}x^{n-1}+\langle x^n-\lambda\rangle$$

知 $\left(x+\langle x^n-\lambda\rangle\right)\left(c_0+c_1x+\cdots+c_{n-1}x^{n-1}+\langle x^n-\lambda\rangle\right) \in P_\lambda(C)$，从而 $P_\lambda(C)$ 是 $R_\infty[x]/\langle x^n-\lambda\rangle$ 的理想。

反之，当 $P_\lambda(C)$ 是 $R_\infty[x]/\langle x^n-\lambda\rangle$ 的理想时，线性码 C 是 R_∞ 上一个长度为 n 的 λ 循环码，这是显然的事实。

推论 1

1) R_∞ 上一个长度为 n 的线性码 C 是循环码，当且仅当 $P_1(C)$ 是 $R_\infty[x]/\langle x^n-1\rangle$ 的理想；

2) R_∞ 上一个长度为 n 的线性码 C 是负循环码，当且仅当 $P_{-1}(C)$ 是 $R_\infty[x]/\langle x^n+1\rangle$ 的理想。

接下来，研究 R_∞ 上循环码与负循环码以及这类码的投影码。

设

$$R_\infty[x]/\langle x^n-1\rangle \to R_i[x]/\langle x^n-1\rangle \tag{6}$$

$$\Psi_i:\ f(x)+\langle x^n-1\rangle \mapsto \Psi_i(f(x))+\langle x^n-1\rangle \tag{7}$$

易验证 Ψ_i 是一个 $R_\infty[x]/\langle x^n-1\rangle$ 到 $R_i[x]/\langle x^n-1\rangle$ 的一个同态。这意味着若 I 是 $R_\infty[x]/\langle x^n-1\rangle$ 的理想，则 $\Psi_i(I)$ 是 $R_i[x]/\langle x^n-1\rangle$ 的理想。因此有下面交换图：

$$\begin{array}{ccc} R_\infty^n & \xrightarrow{P_1} & R_\infty[x]/\langle x^n-1\rangle \\ \Psi_i\downarrow & & \downarrow\Psi_i \\ R_i^n & \xrightarrow{P_1} & R_i[x]/\langle x^n-1\rangle \end{array}$$

即 $\Psi_iP_1=P_1\Psi_i$。

有了以上准备，就可以证明下面定理。

定理 1 记号如上。R_∞ 上一个长度为 n 的线性码 C 是循环码，当且仅当对于所有 $i<\infty$，$\Psi_i(C)$ 是 R_i 上的循环码。

证明 先证明必要性。设 C 是 R_∞ 上的循环码，则由推论 1 知 $P_1(C)$ 是 $R_\infty[x]/\langle x^n-1\rangle$ 的理想。再由同态式 (6) 及上面的交换图，知道 $\Psi_i(P_1(C)) = P_1(\Psi_i(C))$ 是 $R_i[x]/\langle x^n-1\rangle$ 的理想。从而对于所有 $i<\infty$，$\Psi_i(C)$ 是 R_i 上的循环码。

再来证明充分性。假设 C 不是循环码，则存在 $(a_0,a_1,\cdots,a_{n-1})\in C$，但 $(a_{n-1},a_0,a_1,\cdots,a_{n-2})\notin C$。

令 $a_j=\sum_{i=1}^{\infty} b_{ji}\gamma^j\ (j=0,1,2,\cdots,n-1)$，由于 $(a_{n-1},a_0,a_1,\cdots,a_{n-2})\notin C$，因此存在一个 k，使 $\Psi_k(a_{n-1},a_0,a_1,\cdots,a_{n-2})\notin \Psi_k(C)$ 与假设矛盾，从而 C 是循环码。

同理可证如下定理及推论。

定理 2　记号如上，R_∞ 上一个长度为 n 的线性码 C 是负循环码，当且仅当对于所有 $i<\infty$，$\Psi_i(C)$ 是 R_i 上的负循环码。

推论 2　设 $Z_{p^\infty}=\left\{\sum_{l=0}^{\infty}a_l p^l \,\middle|\, a_l\in Z, l=1,2,\cdots\right\}$，其中 p 为素数，则 Z_{p^∞} 上的线性码为循环码当且仅当对所有 $i<\infty$，$\Psi_{p^i}(C)$ 为 Z_{p^i} 上的循环码。这里，$Z_{p^i}=\left\{\sum_{l=0}^{i-1}a_l p^l \,\middle|\, 0\leqslant a_l<p\right\}$，$Z_{p^\infty}$ 到 Z_{p^i} 的映射 Ψ_{p^i} 由 $\Psi_{p^i}(\sum_{l=0}^{\infty}a_l p^l)=\sum_{l=0}^{i-1}a_l p^l$ 定义。

4　中国积中的循环码

中国剩余定理在环上码的研究中有非常重要的应用[1,5,7]。在这一节，将用中国剩余定理研究中国积在什么条件下为循环码。

设 R 是一个环，$I_1,I_2,\cdots,I_s$ 是 R 中两两互质的理想，且 $\bigcap_{j=1}^{s}I_j=\{0\}$。显然，映射

$$\Phi_j:\quad \begin{array}{c} R\to R/I_j \\ r\mapsto r+I_j \end{array}$$

是一个自然同态，它可以自然扩充为下面映射：

$$\Phi:\quad \begin{array}{c} R\to R/I_1\times R/I_2\times\cdots\times R/I_s \\ r\mapsto (r+I_1,r+I_2,\cdots,r+I_s) \end{array}$$

易验证 Φ 是一个 R 模同构。记这个同构的逆为

$$CRT=\Phi^{-1}: R/I_1\times R/I_2\times\cdots\times R/I_s\to R$$

如果 $R_j=R/I_j$，则记 $R=CRT(R_1,\cdots,R_s)$。对 $j=1,2,\cdots,s$，设 C_j 是 R_j 上的码。让 $C=CRT(C_1,\cdots,C_s)=\Phi^{-1}(C_1,\cdots,C_s)=\left\{\Phi^{-1}(v_1,\cdots,v_s)\middle|v_j\in C_j\right\}$，那么称 C 为码 $C_1,\cdots,C_s$ 的中国积。

设 $R_{e_1}^1,\cdots,R_{e_s}^s$ 是链环，其中 $R_{e_j}^j$ 有唯一最大理想 $\langle\gamma_j\rangle$ 和 γ_j 的幂零指数为 e_j，记 $F^j=R_{e_j}^j/\langle\gamma_j\rangle$，$A=CRT(R_{e_1}^1,\cdots,R_{e_j}^j,\cdots,R_{e_s}^s)$。

由于 A 是一个主理想环。对于任意 $1\leqslant i<\infty$，设 $A_i^j=CRT(R_{e_1}^1,\cdots,R_i^j,\cdots,R_{e_s}^s)$，同样地，所有环 A_i^j 都是主理想环。特别地，$A_{e_j}^i=A$。用 A_∞^j 表示 $CRT(R_{e_1}^1,\cdots,R_\infty^j,\cdots,R_{e_s}^s)$。

对于任意正整数 $i<\infty$，由等式(4)定义的映射 Ψ_i，可以得到下面映射（仍记为 Ψ_i）：

$$R_{e_1}^1\times\cdots\times R_\infty^j\times\cdots\times R_{e_s}^s\to R_{e_1}^1\times\cdots\times R_i^j\times\cdots\times R_{e_s}^s \tag{8}$$

$$\Psi_i:(a^1,\cdots,a^j,\cdots,a^s)\to(a^1,\cdots,\Psi_i(a^j),\cdots,a^s) \tag{9}$$

于是，有下面交换图

$$\begin{cases} A_\infty^j=CRT(R_{e_1}^1,\cdots,R_\infty^j,\cdots,R_{e_s}^s) & \xrightarrow{\Phi} & R_{e_1}^1\times\cdots\times R_\infty^j\times\cdots\times R_{e_s}^s \\ \Phi^{-1}\Psi_i\Phi=CRT\Psi_i\Phi\downarrow & & \downarrow\Psi_i \\ A_i^j=CRT(R_{e_1}^1,\cdots,R_i^j,\cdots,R_{e_s}^s) & \xrightarrow{\Phi} & R_{e_1}^1\times\cdots\times R_i^j\times\cdots\times R_{e_s}^s \end{cases} \tag{10}$$

因此，环 A_i^j 可以看成环 A_∞^j 的投影。

对 $1\leqslant i<\infty$，设 C_i^j 是 R_i^j 上的码，而 C_∞^j 是 R_∞^j 上的码。记 $\boldsymbol{C}_i^j=CRT(C_{e_1}^1,\cdots,C_i^j,\cdots,C_{e_s}^s)$，$\boldsymbol{C}_\infty^j=CRT(C_{e_1}^1,\cdots,C_\infty^j,\cdots,C_{e_s}^s)$。则由交换图(10)得到下面交换图

$$\begin{cases} \boldsymbol{C}_\infty^j=CRT(C_{e_1}^1,\cdots,C_\infty^j,\cdots,C_{e_s}^s) & \xrightarrow{\Phi} & C_{e_1}^1\times\cdots\times C_\infty^j\times\cdots\times C_{e_s}^s \\ \Phi^{-1}\Psi_i\Phi=CRT\Psi_i\Phi\downarrow & & \downarrow\Psi_i \\ \boldsymbol{C}_i^j=CRT(C_{e_1}^1,\cdots,C_i^j,\cdots,C_{e_s}^s) & \xrightarrow{\Phi} & C_{e_1}^1\times\cdots\times C_i^j\times\cdots\times C_{e_s}^s \end{cases} \tag{11}$$

因此，对于所有 $i<\infty$，在 A_i^j 上的码 $\boldsymbol{C}_i^j$ 可以看作 A_∞^j 上码 $\boldsymbol{C}_\infty^j$ 的投影。

定理 3　设 $C_{e_1}^1,\cdots,C_\infty^j,\cdots,C_{e_s}^s$ 分别是 $R_{e_1}^1,\cdots,R_\infty^j,\cdots,R_{e_s}^s$ 的长为 n 的线性码，$\boldsymbol{C}_\infty^j=CRT(C_{e_1}^1,\cdots,C_\infty^j,\cdots,C_{e_s}^s)$ 是 A_∞^j 上长为 n 循环码，对所有 $i<\infty$，$\boldsymbol{C}_i^j$ 是 A_i^j 长为 n 的循环码。

证明　记号如上，有交换图

$$\begin{array}{ccc} (A_\infty^j)^n & \xrightarrow{P_1} & A_\infty^j[x]/\langle x^n-1\rangle \\ CRT\Psi_i\Phi\downarrow & & \downarrow CRT\Psi_i\Phi \\ (A_i^j)^n & \xrightarrow{P_1} & A_i^j[x]/\langle x^n-1\rangle \end{array} \tag{12}$$

即 $(CRT\Psi_i\Phi)P_1=P_1(CRT\Psi_i\Phi)$。

设 $\boldsymbol{C}_\infty^j$ 是 A_∞^j 上的循环码，则 $P_1(\boldsymbol{C}_\infty^j)$ 是 $A_\infty^j[x]/\langle x^n-1\rangle$ 上的理想，故对于任意正整数 $i<\infty$，结合同态式(5)及交换图(12)知道

$$(CRT\Psi_i\Phi)P_1(\boldsymbol{C}_\infty^j)=P_1(CRT\Psi_i\Phi(\boldsymbol{C}_\infty^j))$$

是 $A_i^j[x]/\langle x^n-1\rangle$ 的理想。再由交换图(11)知，$(CRT\Psi_i\Phi)(\boldsymbol{C}_\infty^j)=\boldsymbol{C}_i^j$ 是 A_i^j 的循环码。

（下转第 76 页）