文章编号:0253-2778(2015)06-0465-05

环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上的负循环码

陈晓静, 朱士信

(合肥工业大学数学学院, 安徽合肥 230009)

摘要:研究了多项式剩余类环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上任意长度的负循环码.运用有限环理论,给出了该环上任意长的负循环码的结构,并研究了该环上长度为 p^s 的负循环码的 Hamming 距离.

关键词:负循环码;有限环理论;Hamming 距离

中图分类号:TN911.22 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2015.06.006

2010 Mathematics Subject Classification: 94B15

引用格式: Chen Xiaojing, Zhu Shixin. Negacyclic codes over $F_q+uF_q+\cdots+u^{k-1}F_q$ [J]. Journal of University of Science and Technology of China, 2015,45(6):465-469,516.

陈晓静, 朱士信. 环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上的负循环码[J]. 中国科学技术大学学报,2015,45(6):465-469,516.

Negacyclic codes over $F_q+uF_q+\cdots+u^{k-1}F_q$

CHEN Xiaojing, ZHU Shixin

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

Abstract: Negacyclic codes of arbitrary lengths over the polynomial residue ring $F_q+uF_q+\cdots+u^{k-1}F_q$ were studied. By means of the finite ring theory, the structure of negacyclic codes over the ring of arbitrary lengths was given. The Hamming distance of negacyclic codes of length p^s over the ring was also studied.

Key words: negacyclic codes; finite ring theory; Hamming distance

0 引言

1994 年 Hammons 等[1]证明了某些高效的二元非线性码可以看作 Z_4 线性码在 Gray 映射下的象,使得有限环上的码受到广泛的关注.循环码具有严谨的代数结构,而且具有循环的特性,因此性能易于分析,其编译码电路尤其是编码电路简单易于实现.常循环码作为循环码的推广具有循环码的一切优良性质,同时多项式剩余类环的结构介于域和环之间,因此多项式剩余类环上的常循环码尤为引人注目.Bonnecaze 等[2]首先研究了环 F_2+uF_2 上奇长的循环码.随后 Qian 等[3]将其推广到环 $F_p+uF_p+\cdots+u^{k-1}F_p$. Abualrub 等[4]研究了环 Z_2+uZ_2 和 $Z_2+uZ_2+u^2Z_2$ 上的任意长的循环码.Qian 等[5]首先研究了环 F_2+uF_2 上的常循环码.随后,学者们在此基础上展开了一系列的研究[6-11].线性码的 Hamming 距离是衡量纠错码可靠性的一个重要参数,其与纠错码的纠错能力息息相关,因此研究码的距离分布是非常有意义的.施敏加等[12]研究了环 $F_2+uF_2+\cdots+u^{k-1}F_2$ 上长度为 2^s 的 $(1+u)$ 常

收稿日期:2015-02-04;**修回日期**:2015-04-08

基金项目:国家自然科学基金(61370089)资助.

作者简介:陈晓静,女,1990 年生,硕士. 研究方向:代数编码与密码. E-mail: chenxiaojing0909@126.com

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

循环码的 Hamming 距离和 Homogeneous 距离分布. 随后,他们又研究了环 F_2+uF_2 上长度为 2^s 的循环码的 Hamming 距离和 Lee 距离分布[13]. 最近,黄磊等[14]给出了环$F_q+uF_q+u^2F_q$上任意长度的负循环码的结构,Abhay 等[15]研究了环 $Z_p[u]/\langle u^k\rangle$ 上长度为 p^s 的循环码的 Hamming 距离.

本文利用有限环理论,将文献[14-15]的结论加以推广,研究了环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上任意长度的负循环码,得到了其上负循环码的结构以及该环上长度为 p^s 的负循环码的 Hamming 距离.

1 预备知识

设 R 为多项式剩余类环,环 R 上长度为 n 的码 C 是 R^n 的非空子集,若它是 R^n 的 R 子模,则称 C 为线性码. 设 C 为环 R 上长度为 n 的线性码,若对任意的 $c=(c_0,c_1,\cdots,c_{n-1})\in C$,有$(-c_{n-1},c_0,\cdots,c_{n-2})\in C$,则称 C 为环R 上长度为n 的负循环码. 令

$$R_k = F_q + uF_q + \cdots + u^{k-1}F_q, u^k = 0$$

且 $R_{k,n}=R_k[x]/\langle x^n+1\rangle$. 对 R_k 中任意的元素 r,都可以唯一地表示成

$$r = r_0 + ur_1 + u^2r_2 + \cdots + u^{k-1}r_{k-1},$$

其中,$r_i\in F_q$,$0\leqslant i\leqslant k-1$. 对每个固定的正整数 k,任意 $r\in R_k$,$\bar{r}$ 表示 r 模 u^{k-1}约化. 设 C_k 是 R_k 上长度为 n 的负循环码,则 C_k 是 $R_{k,n}$的一个理想. 对任意的 $c=(c_0,c_1,\cdots,c_{n-1})\in C_k$,其多项式表示为 $c_0+c_1x+\cdots+c_{n-1}x^{n-1}$. 码 C_k 是 R_k 上长度为 n 的负循环码当且仅当其多项式表示是环 $R_{k,n}$的一个理想. 本文视码字的向量表示和多项式表示为同一概念,不加以区分. 在不混淆的情况下,多项式 $f(x)$均用字母 f 表示.

设 $c=(c_0,c_1,\cdots,c_{n-1})$是线性码 C_k 中的一个码字,定义码字 c 的 Hamming 重量为其非零分量的个数,记为 $w(c)$,即 $w(c)=|\{i|0\leqslant i\leqslant n-1,c_i\neq 0\}|$. 对于 C_k 中的任意两个码字 $a=(a_0,a_1,\cdots,a_{n-1})$和 $b=(b_0,b_1,\cdots,b_{n-1})$,定义它们的 Hamming 距离为其对应不相等分量的个数,记为 $d(a,b)$,即 $d(a,b)=|\{i|0\leqslant i\leqslant n-1,a_i\neq b_i\}|=w(a-b)$. 码 C_k 的最小 Hamming 重量为 $\min\{w(c)|0\neq c\in C_k\}$,码 C_k 的最小 Hamming 距离定义为 $\min\{d(c_1,c_2)|c_1,c_2\in C_k,c_1\neq c_2\}$. 若 C_k 是线性码,C_k 的最小 Hamming 距离就等于它的最小 Hamming 重量,并且下文中的距离均指 Hamming 距离.

本文中,$q=p^m$,p 为域 F_q 的特征. 在 $F_q[x]$中,若 $f|(x^n+1)$,则记 $\hat{f}=(x^n+1)/f$,后文出现 $\hat{f}$ 等记号不再说明.

定义 1.1 令 $t=b_{s-1}p^{s-1}+b_{s-2}p^{s-2}+\cdots+b_1p+b_0$,$b_i\in F_q$,$0\leqslant i\leqslant s-1$,是 t 的 p 进制展开.

① 若对所有 $1\leqslant i\leqslant l$,$l<s$,$b_{s-i}\neq 0$,且对所有 i,$l+1\leqslant i\leqslant s$,$b_{s-i}=0$,则称 t 有一个长度为 l 的 p 进制零展开.

② 若对所有 $1\leqslant i\leqslant l$,$l<s$,$b_{s-i}\neq 0$,$b_{s-l-1}=0$,且对所有 $l+2\leqslant i\leqslant s$,$b_{s-i}\neq 0$,则称 t 有一个长度为 l 的 p 进制非零展开.

③ 若对所有 $1\leqslant i\leqslant s$,$b_{s-i}\neq 0$,则称 t 有一个长度为 s 的 p 进制全展开.

2 R_k 上的负循环码

令 $R_k=F_q+uF_q+\cdots+u^{k-1}F_q$,$u^k=0$ 且 $R_{k,n}=R_k[x]/\langle x^n+1\rangle$,则 R_k 是极大理想为$\langle u\rangle$的局部环,其剩余域为 F_q. 定义映射

$$\varphi_k: R_k \to R_{k-1} \tag{1}$$

$$\varphi_k(r_0+ur_1+\cdots+u^{k-1}r_{k-1}) = r_0+ur_1+\cdots+u^{k-2}r_{k-2} \tag{2}$$

式中,$r_i\in F_q$,$0\leqslant i\leqslant k-1$. 显然,$\varphi_k$ 是 R_k 到 R_{k-1}的环同态映射,将 φ_k 扩展到同态映射

$$\Phi_k: C_k \to R_{k-1,n} \tag{3}$$

$$\Phi_k(c_0+c_1x+\cdots+c_{n-1}x^{n-1}) = \varphi_k(c_0)+\varphi_k(c_1)x+\cdots+\varphi_k(c_{n-1})x^{n-1} \tag{4}$$

式中,$c_i\in R_k$,$0\leqslant i\leqslant n-1$. 令 $J_k=\{r\in F_q[x]|u^{k-1}r\in \ker\Phi_k\}$. 易见 J_k 是 $R_{1,n}$的一个理想. 因为 $R_{1,n}$是一个主理想环,所以由经典纠错码理论知:在 $F_q[x]$中,存在唯一的 x^n+1 的首一因子 $a_{k-1,k-1}$,使得

$$J_k = \langle a_{k-1,k-1}\rangle,\ \ker\Phi_k = \langle u^{k-1}a_{k-1,k-1}\rangle.$$

设 C_{k-1}是 R_{k-1}上长度为 n 的负循环码,则 C_{k-1}是 $R_{k-1,n}$的一个理想. 定义映射

$$\varphi_{k-1}: R_{k-1} \to R_{k-2} \tag{5}$$

$$\varphi_{k-1}(r_0+ur_1+\cdots+u^{k-2}r_{k-2}) = r_0+ur_1+\cdots+u^{k-3}r_{k-3} \tag{6}$$

式中,$r_i\in F_q$,$0\leqslant i\leqslant k-2$. 显然,$\varphi_{k-1}$是 R_{k-1}到 R_{k-2}的环同态映射,将 φ_{k-1}扩展到同态映射

$$\Phi_{k-1}: C_{k-1} \to R_{k-2,n} \tag{7}$$

$$\Phi_{k-1}(c_0+c_1x+\cdots+c_{n-1}x^{n-1}) = \varphi_{k-1}(c_0)+\varphi_{k-1}(c_1)x+\cdots+\varphi_{k-1}(c_{n-1})x^{n-1} \tag{8}$$

式中,$c_i\in R_{k-1}$,$0\leqslant i\leqslant n-2$. 令

$$J_{k-1} = \{r\in F_q[x]\mid u^{k-2}r\in\ker\Phi_{k-1}\}.$$

易见 J_{k-1} 是 $R_{1,n}$ 的一个理想. 如上,在 $F_q[x]$ 中,存在唯一的 x^n+1 的首一因子 $a_{k-2,k-2}$,使得 $J_{k-1}=\langle a_{k-2,k-2}\rangle$,且 $\ker\Phi_{k-1}=\langle u^{k-2}a_{k-2,k-2}\rangle$.

继续上面的方法我们可以类似定义 φ_{k-3}, $\varphi_{k-4},\cdots,\varphi_2$ 和 $\Phi_{k-3},\Phi_{k-4},\cdots,\Phi_2$. 定义映射

$$\varphi_2:R_2\to R_1 \tag{9}$$

$$\varphi_2(r_0+ur_1)=r_0 \tag{10}$$

式中,$r_0,r_1\in F_q$. 显然 φ_2 是一个环同态,将 φ_2 扩展到同态映射

$$\Phi_2:C_2\to R_{1,n} \tag{11}$$

$$\Phi_2(c_0+c_1x+\cdots+c_{n-1}x^{n-1})=\varphi_2(c_0)+\varphi_2(c_1)x+\cdots+\varphi_2(c_{n-1})x^{n-1} \tag{12}$$

式中,$c_i\in R_2$, $0\leqslant i\leqslant n-1$. 如上,在 $F_q[x]$ 中,存在唯一的 x^n+1 的首一因子 a_{11} 使得 $\ker\Phi_2=\langle ua_{11}\rangle$. 此外,$\Phi_2(C_2)$ 是 $R_{1,n}$ 的一个理想,即其是 F_q 上的负循环码. 因为 $R_{1,n}$ 是一个主理想环,所以 $\Phi_2(C_2)$ 是由某个 x^n+1 的首一因子 a_{00} 生成的.

为了下文研究需要,我们先给出如下引理.

引理 2.1　设 C_k 是环 R_k 上长度为 n 的负循环码,则 $|C_k|=|J_k||C_{k-1}|$.

证明　由环同态基本定理知 $C_k/\ker\Phi_k\cong C_{k-1}$,所以 $|C_k|=|C_{k-1}||\ker\Phi_k|$,又因为

$$\ker\Phi_k=\{u^{k-1}r\mid\forall r\in F_q[x]\},$$

$$J_k=\{r\in F_q[x]\mid u^{k-1}r\in\ker\Phi_k\},$$

所以有 $|\ker\Phi_k|=|J_k|$,因而

$$|C_k|=|J_k||C_{k-1}|. \qquad \square$$

下面,利用归纳方法给出 R_k 上长度为 n 的负循环码的结构.

当 $k=2$ 时,设 C_2 是 $R_2=F_q+uF_q$ 上长度为 n 的负循环码. 结合文献[14]可得,R_2 上长度为 n 的负循环码 C_2 可以表示为 $C_2=\langle a_{00}+ua_{01},ua_{11}\rangle$,其中 a_{00},a_{11} 是 $F_q[x]$ 中首一且唯一的多项式,$a_{01}\in F_q[x]$, $a_{11}\mid a_{00}\mid x^n+1$, $\deg a_{01}<\deg a_{11}$,且满足整除关系式:$a_{11}\mid a_{01}\hat{a}_{00}$. 进一步,我们有

$$|C_2|=q^{2n-\deg a_{00}-\deg a_{11}}.$$

对于 $k-1$,假设环 R_{k-1} 上长度为 n 的负循环码 C_{k-1} 可以表示为 $C_{k-1}=\langle A_0,A_1,A_2,\cdots,A_{k-2}\rangle$,其中,

$$\begin{pmatrix}A_0\\A_1\\A_2\\\vdots\\A_{k-2}\end{pmatrix}=\begin{pmatrix}a_{00}&a_{01}&a_{02}&\cdots&a_{0,k-2}\\0&a_{11}&a_{12}&\cdots&a_{1,k-2}\\0&0&a_{22}&\cdots&a_{2,k-2}\\\vdots&\vdots&\ddots&\ddots&\vdots\\0&0&\cdots&0&a_{k-2,k-2}\end{pmatrix}\begin{pmatrix}1\\u\\u^2\\\vdots\\u^{k-2}\end{pmatrix} \tag{13}$$

a_{ii} $(0\leqslant i\leqslant k-2)$ 是 $F_q[x]$ 中首一且唯一的多项式,$a_{mj}\in F_q[x]$, $a_{k-2,k-2}\mid\cdots\mid a_{11}\mid a_{00}\mid x^n+1$, $\deg a_{mj}<\deg a_{jj}$, $1\leqslant j\leqslant k-2$, $0\leqslant m<j$,且满足整除关系式:

$a_{11}\mid a_{01}\hat{a}_{00}$,

$a_{22}\mid a_{12}\hat{a}_{11}$, $a_{22}\mid a_{02}\hat{a}_{00}\hat{a}_{11}$,

$a_{33}\mid a_{23}\hat{a}_{22}$, $a_{33}\mid a_{13}\hat{a}_{12}\hat{a}_{11}$, $a_{33}\mid a_{03}\hat{a}_{00}\hat{a}_{11}\hat{a}_{22}$,

$\cdots$

$a_{k-2,k-2}\mid a_{k-3,k-2}\hat{a}_{k-3,k-3},\cdots,a_{k-2,k-2}\mid a_{1,k-2}\hat{a}_{1,k-3}\cdots\hat{a}_{12}\hat{a}_{11},a_{k-2,k-2}\mid a_{0,k-2}\hat{a}_{00}\hat{a}_{11}\hat{a}_{22}\cdots\hat{a}_{k-3,k-3}$.

进一步,我们有 $|C_{k-1}|=q^{(k-1)n-\sum_{i=0}^{k-2}\deg a_{ii}}$,则对 R_k 上长度为 n 的负循环码,可以证明如下结论:

定理 2.2　设 C_k 是 R_k 上长度为 n 的负循环码,若 $C_{k-1}=\langle A_0,A_1,A_2,\cdots,A_{k-2}\rangle$,其中,$A_0,A_1,\cdots,A_{k-2}$ 的定义如式(13),则 C_k 可以表示为

$$C_k=\langle A_0+u^{k-1}a_{0,k-1},A_1+u^{k-1}a_{1,k-1},\cdots,u^{k-1}a_{k-1,k-1}\rangle \tag{14}$$

式中,$a_{k-1,k-1}$ 是 $F_q[x]$ 中首一且唯一的多项式,$a_{i,k-1}\in F_q[x]$, $0\leqslant i\leqslant k-2$, $a_{k-1,k-1}\mid a_{k-2,k-2}\mid\cdots\mid a_{11}\mid a_{00}\mid x^n+1$, $\deg a_{m,k-1}<\deg a_{k-1,k-1}$, $0\leqslant m<k-1$. 此外,还满足如下整除关系式:

$$a_{k-1,k-1}\mid a_{k-2,k-1}\hat{a}_{k-2,k-2},$$

$$\cdots$$

$$a_{k-1,k-1}\mid a_{1,k-1}\hat{a}_{1,k-2}\cdots\hat{a}_{12}\hat{a}_{11},$$

$$a_{k-1,k-1}\mid a_{0,k-1}\hat{a}_{00}\hat{a}_{11}\cdots\hat{a}_{k-2,k-2}.$$

进一步,我们有 $|C_k|=q^{kn-\sum_{i=0}^{k-1}\deg a_{ii}}$.

证明　因为 $u^{k-1}a_{k-2,k-2}\in\ker\Phi_k$,所以 $a_{k-1,k-1}\mid a_{k-2,k-2}$. 由归纳假设知 $a_{k-2,k-2}\mid a_{k-3,k-3},\cdots,a_{22}\mid a_{11}$,所以

$$a_{k-1,k-1}\mid a_{k-2,k-2}\mid\cdots\mid a_{11}\mid a_{00}\mid x^n+1.$$

设 $A_0,A_1,\cdots,A_{k-2}$ 在 C_k 中一个原象分别为 $A_0+u^{k-1}a_{0,k-1},A_1+u^{k-1}a_{1,k-1},\cdots,A_{k-2}+u^{k-1}a_{k-2,k-1}$, J_k 为 F_q 上长度为 n 的负循环码,所以存在唯一 $a_{k-1,k-1}\mid x^n+1$ 使得 $J_k=\langle u^{k-1}a_{k-1,k-1}\rangle$. 从而,$\langle A_0+u^{k-1}a_{0,k-1},A_1+u^{k-1}a_{1,k-1},\cdots,u^{k-1}a_{k-1,k-1}\rangle\subseteq C_k$. 记

$D=\langle A_0+u^{k-1}a_{0,k-1},A_1+u^{k-1}a_{1,k-1},\cdots,u^{k-1}a_{k-1,k-1}\rangle$,则 $\overline{D}\subseteq\overline{C}_k=C_{k-1}$ 显然. 因为 $A_0,\cdots,A_{k-2}\in\overline{D}$,所以 $\overline{D}=C_{k-1}$. 容易由 $J_k\subseteq\ker D$,得

$$|D|=|\overline{D}||\ker D|\geqslant|C_{k-1}||J_k|=|C_k|,$$

从而 $D=C_k$.

因为对任意的多项式 $e\in R[x]$,$\langle a,b\rangle=$

$\langle a+be,b\rangle$，则可约定 $\deg a_{m,k-1}<\deg a_{k-1,k-1}$，$0\leqslant m<k-1$. 前面已知 a_{ii}，$0\leqslant i\leqslant k-1$，$a_{mj}$，$1\leqslant j\leqslant k-2$，$0\leqslant m<j$，是唯一的，设

$$\langle A_0+u^{k-1}a_{0,k-1},A_1+u^{k-1}a_{1,k-1},\cdots,u^{k-1}a_{k-1,k-1}\rangle=\langle A_0+u^{k-1}r_{0,k-1},A_1+u^{k-1}r_{1,k-1},\cdots,u^{k-1}a_{k-1,k-1}\rangle,$$

则必存在 $\alpha_1,\alpha_2,\cdots,\alpha_{k-1}\in R_k[x]$，使得

$$A_0+u^{k-1}a_{0,k-1}=A_0+u^{k-1}r_{0,k-1}+\alpha_1(A_1+u^{k-1}r_{1,k-1})+\cdots+\alpha_{k-1}u^{k-1}a_{k-1,k-1}\quad(15)$$

即

$$u^{k-1}(a_{0,k-1}-r_{0,k-1})=\alpha_1(A_1+u^{k-1}r_{1,k-1})+\alpha_2(A_2+u^{k-1}r_{2,k-1})+\cdots+\alpha_{k-1}u^{k-1}a_{k-1,k-1}\in C_k\quad(16)$$

则 $a_{0,k-1}-r_{0,k-1}\in J_k$，故 $a_{k-1,k-1}\mid a_{0,k-1}-r_{0,k-1}$. 又因为

$$\deg a_{0,k-1}<\deg a_{k-1,k-1},$$
$$\deg r_{0,k-1}<\deg a_{k-1,k-1},$$

所以 $a_{0,k-1}=r_{0,k-1}$. 同理可证 $a_{1,k-1}=r_{1,k-1}$，$a_{2,k-1}=r_{2,k-1}$，$\cdots$，$a_{k-2,k-1}=r_{k-2,k-1}$，唯一性得证.

易得

$$a_{k-1,k-1}\mid a_{k-2,k-1}\hat{a}_{k-2,k-2},a_{k-1,k-1}\mid a_{2,k-1}\hat{a}_{2,k-2}\cdots\hat{a}_{23}\hat{a}_{22},a_{k-1,k-1}\mid a_{1,k-1}\hat{a}_{1,k-2}\cdots\hat{a}_{12}\hat{a}_{11}.$$

由于 $a_{11}\mid a_{01}\hat{a}_{00}$，故存在 $h\in F_q[x]$，使得 $a_{11}h=a_{01}\hat{a}_{00}$. 类似的，我们有 $a_{22}t=a_{02}\hat{a}_{00}\hat{a}_{11}$，其中，$t\in F_q[x]$. 因而有

$$(A_0+u^{k-1}a_{0,k-1})\hat{a}_{00}\hat{a}_{11}\cdots\hat{a}_{k-2,k-2}=u^{k-1}a_{0,k-1}\hat{a}_{00}\hat{a}_{11}\cdots\hat{a}_{k-2,k-2}\in\ker\Phi_k\quad(17)$$

从而 $a_{k-1,k-1}\mid a_{0,k-1}\hat{a}_{00}\hat{a}_{11}\cdots\hat{a}_{k-2,k-2}$.

由引理 2.1 知，

$$|C_k|=|J_k||C_{k-1}|=|J_k||J_{k-1}||C_{k-2}|=\cdots=|J_k||J_{k-1}|\cdots|J_1||C_1|\quad(18)$$

而 $J_k=\langle a_{k-1,k-1}\rangle$，$J_{k-1}=\langle a_{k-2,k-2}\rangle$，$\cdots$，$J_2=\langle a_{11}\rangle$，$C_1=\langle a_{00}\rangle$，则易得 $|C_k|=q^{kn-\sum_{i=0}^{k-1}\deg a_{ii}}$. □

根据归纳原理，定理 2.2 给出了 R_k 上长度为 n 的负循环码的生成子及其所含码字的数目. 因此，利用递归的方法可以得到 R_k 上任意长度的负循环码的结构. 下面，考虑两种特殊情况.

推论 2.3 在定理 2.2 中，若 $a_{k-1,k-1}=a_{00}$，则 $C_k=\langle A_0+u^{k-1}a_{0,k-1}\rangle$，并且 $(A_0+u^{k-1}a_{0,k-1})\mid(x^n+1)$. 若 $a_{k-2,k-2}=a_{00}$，则

$$C_k=\langle A_0+u^{k-1}a_{0,k-1},u^{k-1}a_{k-1,k-1}\rangle.$$

推论 2.4 在定理 2.2 中，若 $(n,p)=1$，则 R_k 上长度为 n 的负循环码可以表示成

$$C_k=\langle a_{00},ua_{11},u^2a_{22},\cdots,u^{k-1}a_{k-1,k-1}\rangle\quad(19)$$

式中，a_{ii}（$0\leqslant i\leqslant k-1$）是 $F_q[x]$ 中首一且唯一的多项式，并且满足 $a_{k-1,k-1}\mid a_{k-2,k-2}\mid\cdots\mid a_{11}\mid a_{00}\mid x^n+1$.

证明 因为 R_k 是多项式剩余类环，且 $(n,p)=1$，故由 Hensel 提升可知：x^n+1 在 $R_k[x]$ 中可以唯一分解为两两互素的首一的基本不可约多项式的乘积. 此时，由定理 2.2 中的整除关系式可得 $a_{ij}=0$，$0\leqslant i\leqslant k-2$，$i<j\leqslant k-1$. 因此

$$C_k=\langle a_{00},ua_{11},u^2a_{22},\cdots,u^{k-1}a_{k-1,k-1}\rangle.$$ □

3 Hamming 距离

线性码的 Hamming 距离是衡量纠错码可靠性的一个重要参数，其与纠错码的纠错能力息息相关. 下面我们将研究环 R_k 上长度为 n 的负循环码的 Hamming 距离. 为了下文研究需要，我们先给出如下定理：

定理 3.1 若 C_k 是 R_k 上长度为 n 的负循环码，其中 C_k 的定义如式(14)，则 $w(C_k)=w(J_k)$.

证明 由 $J_k=\langle a_{k-1,k-1}\rangle$，易知 $J_k\subseteq C_k$，因而 $w(C_k)\leqslant w(J_k)$. 若 $t=t_0+ut_1+\cdots+u^{k-1}t_{k-1}\in C_k$，其中 $t_0,t_1,\cdots,t_{k-1}\in F_q[x]$，则 $u^{k-1}t=u^{k-1}t_0$，$w(u^{k-1}t)\leqslant w(t)$，从而 $w(u^{k-1}C_k)\leqslant w(C_k)$. 又因为 $u^{k-1}C_k=\langle u^{k-1}a_{k-1,k-1}\rangle$，所以 $w(J_k)\leqslant w(C_k)$. 故 $w(C_k)=w(J_k)$. □

引理 3.2 若 C_k 是 R_k 上长度为 p^s 的负循环码，其中，s 是正整数. 若 $C_k=\langle a\rangle$，其中，$a=(x^{p^{s-1}}+1)^bh$，$1\leqslant b<p$，则 C_k 的最小距离 $d(C_k)=(b+1)d$，其中，d 是 $C_1=\langle h\rangle\subseteq R_k[x]/\langle x^{p^{s-1}}+1\rangle$ 的最小距离.

证明 对任意的 $c\in C_k$，我们有

$$c=at=(x^{p^{s-1}}+1)^bht,$$

其中，$t\in R_k[x]/\langle x^{p^{s-1}}+1\rangle$. 又因为

$$C_1=\langle h\rangle\subseteq R_k[x]/\langle x^{p^{s-1}}+1\rangle,$$

所以

$$w(c)=w((x^{p^{s-1}}+1)^bht)=w(x^{p^{s-1}b}ht)+w(c_b^1x^{p^{s-1}(b-1)}ht)+\cdots+w(ht),$$

因而 $d(C_k)=(b+1)d$. □

定理 3.3 若 C_k 是 R_k 上长度为 p^s 的负循环码，其中，C_k 的定义如式(14)，s 是正整数，

$$a_{00}=(x+1)^{t_1},a_{11}=(x+1)^{t_2},\cdots,$$
$$a_{k-1,k-1}=(x+1)^{t_k},0<t_k<\cdots<t_2<t_1.$$

（Ⅰ）若 $t_k\leqslant p^{s-1}$，则 $d(C_k)=2$.

（Ⅱ）若 $t_k>p^{s-1}$，令

$$t_k=b_{s-1}p^{s-1}+b_{s-2}p^{s-2}+\cdots+b_1p+b_0$$

是 t_k 的 p 进制展开且

$$a_{k-1,k-1}=(x+1)^{t_k}=(x^{p^{s-1}}+1)^{b_{s-1}}(x^{p^{s-2}}+1)^{b_{s-2}}\cdots(x^{p^0}+1)^{b_0} \tag{20}$$

① 若 t_k 有一个长度为 l 的 p 进制零展开或全展开($s=l$),则

$$d(C_k)=(b_{s-1}+1)(b_{s-2}+1)\cdots(b_{s-l}+1).$$

② 若 t_k 有一个长度为 l 的 p 进制非零展开,则

$$d(C_k)=2(b_{s-1}+1)(b_{s-2}+1)\cdots(b_{s-l}+1).$$

证明　由定理 3.1,我们有 $d(C_k)=d(u^{k-1}C_k)=d(J_k)=d((x+1)^{t_k})$. 因此,我们只需考察 $u^{k-1}C_k=(x+1)^{t_k}$ 的最小重量.

(Ⅰ) 若 $t_k\leqslant p^{s-1}$,则 $(x+1)^{t_k}(x+1)^{p^{s-1}-t_k}=(x+1)^{p^{s-1}}=(x^{p^{s-1}}+1)\in C_k$,故 $d(C_k)=2$.

(Ⅱ) 若 $t_k>p^{s-1}$,

① 若 t_k 有一个长度为 l 的 p 进制零展开,则有 $t_k=b_{s-1}p^{s-1}+b_{s-2}p^{s-2}+\cdots+b_{s-l}p^{s-l}$ 且

$$a_{k-1,k-1}=(x+1)^{t_k}=(x^{p^{s-1}}+1)^{b_{s-1}}(x^{p^{s-2}}+1)^{b_{s-2}}\cdots(x^{p^{s-l}}+1)^{b_{s-l}}.$$

令 $h=(x^{p^{s-l}}+1)^{b_{s-l}}$,则由 h 生成的负循环码长度为 p^{s-l+1} 且其最小距离为 $(b_{s-l}+1)$. 根据引理 3.2,由 $(x^{p^{s-l+1}}+1)^{b_{s-l+1}}$ h 生成的子码的最小距离为 $(b_{s-l+1}+1)(b_{s-l}+1)$. 对 l 归纳,易得由 $a_{k-1,k-1}$ 生成的负循环码的最小距离为 $(b_{s-1}+1)(b_{s-2}+1)\cdots(b_{s-l}+1)$,所以 $d(C_k)=(b_{s-1}+1)(b_{s-2}+1)\cdots(b_{s-l}+1)$.

② 若 t_k 有一个长度为 l 的 p 进制非零展开,则有 $t_k=b_{s-1}p^{s-1}+b_{s-2}p^{s-2}+\cdots+b_1p+b_0$,$b_{s-l-1}=0$. 令 $r=b_{s-l-2}p^{s-l-2}+b_{s-l-3}p^{s-l-3}+\cdots+b_1p+b_0$,并且

$$h=(x+1)^r=(x^{p^{s-l-2}}+1)^{b_{s-l-2}}(x^{p^{s-l-3}}+1)^{b_{s-l-3}}\cdots(x^{p^1}+1)^{b_1}(x^{p^0}+1)^{b_0}.$$

因为 $r<p^{s-l-1}$,所以对非零的 j,有 $p^{s-l-1}=r+j$. 故

$$(x+1)^{p^{s-l-1}-j}h=(x^{p^{s-l-1}}+1)\in C_k.$$

因此,由 h 生成的子码的最小距离为 2. 根据引理 3.2,由 $(x^{p^{s-l}}+1)^{b_{s-l}}h$ 生成的子码的最小距离为 $2(b_{s-l}+1)$. 对 l 归纳,易得由 $a_{k-1,k-1}$ 生成的负循环码的最小距离为 $2(b_{s-1}+1)(b_{s-2}+1)\cdots(b_{s-l}+1)$. 因此,

$$d(C_k)=2(b_{s-1}+1)(b_{s-2}+1)\cdots(b_{s-l}+1).\ \square$$

4　例子

例 4.1　考虑 $R_2=F_3+uF_3$ 上长度为 4 的非零的负循环码和最小距离. 容易得到

$$x^4+1=(x^2+x+2)(x^2+2x+2),$$

记 $g_1=x^2+x+2$,$g_2=x^2+2x+2$,则 R_2 上长度为 4 的非零的负循环码和最小距离如表 1 所列.

表 1　R_2 上长度为 4 的非零的负循环码和最小距离

Tab. 1　**Negacyclic codes and $d(C)$ of length 4 over R_2**

R_2 上长度为 4 的非零的负循环码	$d(C)$
$\langle 1\rangle,\langle u\rangle,\langle g_1,u\rangle,\langle g_2,u\rangle$	1
$\langle g_1\rangle,\langle g_2\rangle,\langle ug_1\rangle,\langle ug_2\rangle$	3

例 4.2　考虑 $R_3=F_5+uF_5+u^2F_5$ 上长度为 9 的非零的负循环码和最小距离. 容易得到

$$x^9+1=(x+1)(x^2+4x+1)(x^6+4x^3+1),$$

记 $g_1=x+1$,$g_2=x^2+4x+1$,$g_3=x^6+4x^3+1$,则 R_3 上长度为 9 的非零的负循环码和最小距离如表 2 所列.

表 2　R_3 上长度为 9 的非零的负循环码和最小距离

Tab. 2　**Negacyclic codes and $d(C)$ of length 9 over R_3**

R_3 上长度为 9 的非零的负循环码	$d(C)$
$\langle 1\rangle,\langle u\rangle,\langle u^2\rangle,\langle g_i,u\rangle,\langle g_i,u^2\rangle,\langle\hat{g}_i,u\rangle,\langle\hat{g}_i,u^2\rangle,\langle ug_i,u^2\rangle,\langle u\hat{g}_i,u^2\rangle,\langle\hat{g}_j,ug_1,u^2\rangle,\langle\hat{g}_t,ug_2,u^2\rangle,\langle\hat{g}_m,ug_3,u^2\rangle$	1
$\langle g_m\rangle,\langle ug_m\rangle,\langle u^2g_m\rangle,\langle\hat{g}_j,ug_1\rangle,\langle\hat{g}_j,u^2g_1\rangle,\langle u\hat{g}_j,u^2g_1\rangle,\langle\hat{g}_t,ug_2\rangle,\langle\hat{g}_t,u^2g_2\rangle,\langle u\hat{g}_t,u^2g_2\rangle,\langle g_1g_2\rangle,\langle ug_1g_2\rangle,\langle u^2g_1g_2\rangle$	2
$\langle g_3\rangle,\langle ug_3\rangle,\langle u^2g_3\rangle,\langle\hat{g}_m,ug_3\rangle,\langle\hat{g}_m,u^2g_3\rangle,\langle u\hat{g}_m,u^2g_3\rangle$	3
$\langle g_1g_3\rangle,\langle ug_1g_3\rangle,\langle u^2g_1g_3\rangle$	6
$\langle g_2g_3\rangle,\langle ug_2g_3\rangle,\langle u^2g_2g_3\rangle$	9

【注】　$i=1,2,3$;$j=2,3$;$t=1,3$;$m=1,2$.

通过上面两个例题的计算,我们发现在给定长度上存在许多极小距离不小于 3 的负循环码,从而这些负循环码就具有了一定的纠错能力. 因此,它们不仅可以用于无线通信网络中的纠错方案设计,还为在等距映射下构造有限域上参数较好的纠错码提供了码源.

5　结论

本文主要研究了环 $R_k=F_q+uF_q+\cdots+u^{k-1}F_q$ 上任意长度的负循环码的结构,并研究了该环上长度为 p^s 的负循环码的最小 Hamming 距离. 对于多项式剩余类环上负循环码的研究,本文具有一定的推广与借鉴价值. R_k 上长度为 n 的负循环码的对偶码及其性质是今后的研究方向.

(下转第 516 页)