第44卷第12期 中国科学技术大学学报 Vol. 44, No. 12
2014年12月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Dec. 2014

文章编号:0253-2778(2014)12-0991-05

环 $F_q+uF_q+u^2F_q$ 上任意长度的负循环码

黄 磊,朱士信

(合肥工业大学数学学院,安徽合肥 230009)

摘要:根据环 F_q+uF_q 上负循环码的结构,研究了环 $F_q+uF_q+u^2F_q$ 上任意长度的负循环码.利用环同态,给出了环 $F_q+uF_q+u^2F_q$ 上长度为 n 的负循环码的结构,并研究了这些负循环码的对偶码,同时研究了该环上自对偶负循环码.结果表明环 $F_q+uF_q+u^2F_q$ 上自对偶负循环码存在当且仅当 $p=2$.

关键词:负循环码;环同态;对偶码;自对偶码

中图分类号:TN911.22 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2014.12.005

AMS Subject Classification (2000): 94B15

引用格式: Huang Lei, Zhu Shixin. Negacyclic codes of arbitrary lengths over ring $F_q+uF_q+u^2F_q$[J]. Journal of University of Science and Technology of China, 2014,44(12):991-995.
黄磊,朱士信. 环 $F_q+uF_q+u^2F_q$ 上任意长度的负循环码[J]. 中国科学技术大学学报,2014,44(12):991-995.

Negacyclic codes of arbitrary lengths over ring $F_q+uF_q+u^2F_q$

HUANG Lei, ZHU Shixin

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

Abstract: According to the structure of negacyclic codes over ring F_q+uF_q, the negacyclic codes of arbitrary lengths over ring $F_q+uF_q+u^2F_q$ were studied. Bying ring homomorphism, the structure of negacyclic codes over ring $F_q+uF_q+u^2F_q$ of length n were given, the dual codes of these negacyclic codes were studied, and the self-dual negacyclic codes over the ring were also studied. The results show that self-dual negacyclic codes over ring $F_q+uF_q+u^2F_q$ exist if and only if $p=2$.

Key words: negacyclic codes; ring homomorphism; dual codes; self-dual codes

0 引言

有限环上的线性码因为其在代数理论中的地位及在编码中的成功应用而引起了广大编码研究者的极大兴趣.对于结构介于有限域和环之间的有限链环,因其具有某些特殊的性质,其上的纠错码理论研究备受关注.文献[1]研究了 Z_4 上长度为 2^e 的循环码;文献[2]研究了 Z_4 上长度为 $2n$(n 为奇数)的循环码;文献[3]研究了环 $F_{p^m}+uF_{p^m}$ 上任意长度的循环码;文献[4-6]研究了环 $F_{p^m}+uF_{p^m}$ 上的常循环码;文献[7-8]中研究了环 $F_2+uF_2+u^2F_2$ 上的循环码和一类常循环码,给出了它们的结构;文献[9]

收稿日期:2013-12-25;**修回日期**:2014-04-10

基金项目:国家自然科学基金(61370089)资助.

作者简介:黄磊,男,1989年生,硕士. 研究方向:代数编码与密码. E-mail:1306926448@qq.com

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

研究了环 $F_2+uF_2+\cdots+u^{m-1}F_2$ 上的常循环码，而文献[10]研究了环 $F_p+uF_p+\cdots+u^{s-1}F_p$ 上的常循环码. 同循环码一样，负循环码是一类特殊的线性码，有限链环上循环码及其结构的研究获得了丰富的成果，但对有限链环上负循环码的研究相对少些. 文献[11-12]研究了环 Z_4 上负循环码；文献[13-14]研究了环 Z_{2^a} 上的负循环码及其它们的距离，而文献[15]研究了环 Z_{p^a} 上的重根负循环码. 本文基于文献[7-8,10]的理论知识与研究方法，研究了环 $F_q+uF_q+u^2F_q$ 上长度为 n 的负循环码，给出了负循环码的结构，并且研究了这些负循环码的对偶码及环 $F_q+uF_q+u^2F_q$ 上长度为 n 的自对偶负循环码，给出了负循环码是自对偶负循环码的一个充分必要条件.

1 基本概念

设 $\mathscr{R}$ 为有限链环，环 $\mathscr{R}$ 上长度为 n 的线性码是 $\mathscr{R}^n$ 的子模. 设 C 为环 $\mathscr{R}$ 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 $\mathscr{R}$ 上长度为 n 的负循环码. C 为环 $\mathscr{R}$ 上长度为 n 的负循环码当且仅当其多项式表示为 $\mathscr{R}[x]/\langle x^n+1\rangle$ 的理想. 对于向量表示与多项式表示，它们是等同的，本文不加以区分.

在不混淆的情况下，后文 $f(x)$ 等多项式一律用 f 等字母表示. 对任意的 $x,y\in\mathscr{R}^n$：

$$x=(x_0,x_1,\cdots,x_{n-1}),y=(y_0,y_1,\cdots,y_{n-1}),$$

定义 x 与 y 的内积为

$$x\cdot y=x_0y_0+x_1y_1+\cdots+x_{n-1}y_{n-1},$$

若 $x\cdot y=0$，则称 x 与 y 正交. 定义环 $\mathscr{R}$ 上长度为 n 的负循环码 C 的对偶码为

$$C^{\perp}=\{x\mid x\cdot y=0,\forall\, y\in C\},$$

显然它也是环 $\mathscr{R}$ 上长度为 n 的负循环码. 若 $C=C^{\perp}$，则称 C 为自对偶码.

定义 C 的零化子为

$$A(C)=\{g\mid gf=0,\forall\, f\in C\},$$

易证 $A(C)$ 为 $\mathscr{R}[x]/\langle x^n+1\rangle$ 的理想. 对任意的多项式 $f\in\mathscr{R}[x]$，其互反多项式为 $f^*=x^{\deg f}f(x^{-1})$. 易证 $C^{\perp}=A(C)^*=\{f^*\mid\forall\, f\in A(C)\}$.

设环

$$R=F_q+uF_q+u^2F_q=\{a+ub+u^2d\mid a,b,d\in F_q\},$$

$u^3=0$；环 $S=F_q+uF=\{a+ub\mid a,b\in F_q\}$，$u^2=0$. 显然 R 和 S 都是有限链环，R 和 S 上长度为 n 的负循环码分别可以看成 $R_n=R[x]/\langle x^n+1\rangle$ 和 $S_n=S[x]/\langle x^n+1\rangle$ 的理想. 本文中 $q=p^m$，$n=p^sk$，其中，$(p,k)=1$，p 为域 F_q 的特征.

若 $f\mid(x^n+1)$，则记 $\hat{f}=(x^n+1)/f$. 后文出现 $\hat{f}$ 等形式时不再说明.

2 R 上的负循环码的结构

设 C 是环 R 上长度为 n 的负循环码. 定义 R 到 S 的映射 $\phi_1:\phi_1(a+ub+u^2d)=a+ub$，其中 $a,b\in F_q$. 易证它为环同态映射. 可以将 ϕ_1 扩展为 C 到 S_n 的同态映射 $\psi_1:\psi_1(c)=a+ub$. 其中，$c=a+ub+u^2d\in C$，$a,b,d\in F_q[x]/\langle x^n+1\rangle$. 有 $\ker\psi_1=\{u^2r\mid u^2r\in C,\forall\, r\in F_q[x]\}$，记 $T_1(C)=\{r\mid u^2r\in\ker\psi_1\}$，易证它是域 F_q 上长度为 n 的负循环码. 根据有限域上纠错码理论可知存在唯一的满足 $a_2\mid x^n+1$ 的首一多项 $a_2\in F_q[x]$，使得 $T_1(C)=\langle a_2\rangle$ 和 $\ker\psi_1=\langle u^2a_2\rangle$.

设 C 在 ψ_1 下的像为 $R_1(C)$，它显然 $R_1(C)$ 是 $S_n=S[x]/\langle x^n+1\rangle$ 的一个理想. 要得到负循环码 C 的结构，必须知道 $R_1(C)$ 的结构，即我们需要了解环 S 上长度为 n 的负循环码的结构.

设 D 是环 S 上长度为 n 的负循环码，定义 S 到 F_q 的映射 $\phi_2:\phi_2(a+ub)=a$，其中 $a,b\in F_q$. 它为环同态映射. 将 ϕ_1 扩展为 D 到 $F_q[x]/\langle x^n+1\rangle$ 的同态映射 $\psi_2:\psi_2(c)=a$. 其中，$c=a+ub\in D$，$a,b\in F_q[x]/\langle x^n+1\rangle$. 我们有 $\ker\psi_2=\{ut\mid ut\in D,\forall\, t\in F_q[x]\}$，记 $T_2(D)=\{t\mid ut\in\ker\psi_2\}$，易证它也是域 F_q 上长度为 n 的负循环码，则由有限域上纠错码理论可知：存在唯一的满足 $a_1\mid x^n+1$ 的首一多项式 $a_1\in F_q[x]$，使得 $T_2(D)=\langle a_1\rangle$.

设 D 在 ψ_2 下的像为 $R_2(D)$，它显然是 $F_q[x]/\langle x^n+1\rangle$ 的一个理想，则由有限域上纠错码理论可知：存在唯一的满足 $g\mid x^n+1$ 的首一多项式 $g\in F_q[x]$，使得 $R_2(D)=\langle g\rangle$.

设 $g+up_1$ 为 g 关于 ψ_2 在 D 中的原像，易证 $D=\langle g+up_1,ua_1\rangle$. 因为对任意的多项式 $e\in S[x]$，$\langle a,b\rangle=\langle a+be,b\rangle$，则可约定 $\deg p_1<\deg a_1$，此时易证 p_1 是唯一的.

引理 2.1 设 C 是环 R 上长度为 n 的负循环码，D 是环 S 上长度为 n 的负循环码，定义如下两个映射：① C 到 $R_1(C)$ 的映射 φ_1：对任意的 $c\in C$，$\varphi_1(c)=\psi_1(c)$；② D 到 $R_2(D)$ 的映射 φ_2：对任意的

$c\in D,\varphi_1(e)=\psi_2(c)$. 则 φ_1,φ_2 为满同态映射,且

$$|C|=|R_1(C)||T_1(C)|,$$
$$|D|=|R_2(D)||T_2(D)|.$$

定理 2.2　设 C 是环 R 上长度为 n 的负循环码,存在唯一满足 $a_2|a_1|g|x^n+1$,$\deg p_1<\deg a_1$,$\deg p_2<\deg a_2$,$\deg q_1<\deg a_2$ 且 a_2,a_1,g 首一的多项式 $a_1,g,a_2,p_1,p_2,q_1\in F_q[x]$,使得

$$C=\langle g+up_1+u^2p_2,ua_1+u^2q_1,u^2a_2\rangle,$$

且 $|C|=p^{m(3n-\deg a_2-\deg g-\deg a_1)}$.

证明　因为 $u^2a_1\in\ker\varphi_1$,则 $a_2|a_1$,因此 $a_2|a_1|g|x^n+1$. 设 $g+up_1+u^2p_2,ua_1+u^2q_1$ 分别为 $g+up_1,ua_1$ 关于 ϕ_1 在 C 中的原像,利用引理 2.1 易证 $C=\langle g+up_1+u^2p_2,ua_1+u^2q_1,u^2a_2\rangle$. 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 $\deg p_2<\deg a_2$,$\deg q_1<\deg a_2$. 前面已知 a_2,a_1,g,p_1 是唯一的. 设

$$\langle g+up_1+u^2p_2,ua_1+u^2q_1,u^2a_2\rangle=\langle g+up_1+u^2r_2,ua_1+u^2t_1,u^2a_2\rangle,$$

则必存在 $\alpha_1,\alpha_2\in R[x]$,使得

$$g+up_1+u^2p_2=g+up_1+u^2r_2+\alpha_1(ua_1+u^2q_1)+\alpha_2u^2a_2,$$

即有 $u^2(p_2-r_2)=\alpha_1(ua_1+u^2q_1)+\alpha_2u^2a_2\in C$,则 $p_2-r_2\in T_1(C)$,推知 $a_2|(p_2-r_2)$. 而 $\deg r_2<\deg a_2$,$\deg p_2<\deg a_2$,则 $p_2=r_2$. 同理可证 $q_1=t_1$. 则证唯一性.

由引理 2.1 可知

$$|C|=|u^2T_1(C)|\cdot|R_1(C)|=|u^2T_1(C)|\cdot|R_2(R_1(C))|\cdot|T_2(R_1(C))|.$$

而 $T_1(C)=\langle a_2\rangle$,$R_2(R_1(C))=\langle g\rangle$,$T_2(R_1(C))=\langle a_1\rangle$,且它们均为域 F_q 上长度为 n 的负循环码,则可求得 $|C|=p^{m(3n-\deg a_2-\deg g-\deg a_1)}$,定理得证. □

推论 2.3　在定理 2.2 中,若 $a_2=g$,则 $C=\langle g+up_1+u^2p_2\rangle$,且 $(g+up_1+u^2p_2)|(x^n+1)$. 若 $a_1=g$,则 $C=\langle g+up_1+u^2p_2,u^2a_2\rangle$.

推论 2.4　在定理 2.2 中,$a_2|a_1|p_1\hat{g},a_2|q_1\hat{a}_1,a_2|p_1\hat{a}_1\hat{g}$.

证明　因为 $(g+up_1)\hat{g}=up_1\hat{g}\in R_1(C)$,则有 $p_1\hat{g}\in T_2(R_1(C))$,又因为 $a_2|a_1$,即有 $a_2|a_1|p_1\hat{g}$. 而这可推知 $u\hat{a}_1\hat{g}p_1=u\hat{a}_1a_1h$,其中,$h\in F_q[x]$,则 $\hat{a}_1\hat{g}(g+up_1+u^2p_2)=u^2\hat{a}_1\hat{g}p_1\in C$,由此可以推知 $a_2|p_1\hat{a}_1\hat{g}$. 因为 $\hat{a}_1(ua_1+u^2q_1)=u^2\hat{a}_1q_1\in C$,则 $a_2|q_1\hat{a}_1$. □

推论 2.5　在定理 2.2 中,若 $(n,p)=1$,则 $C=\langle g,ua_1,u^2a_2\rangle$.

3　对偶码及自对偶码

关于定理 2.2 中的长度为 n 的负循环码 C,因为 C 的零化子 A(C)为 $R[x]/\langle x^n+1\rangle$ 的理想,可设 $A(C)=\langle h+us_1+u^2s_2,ur_1+u^2t_1,u^2r_2\rangle$,且有 h,r_1,r_2 首一,$\deg s_1<\deg r_1$,$\deg s_2<\deg r_2$,$\deg t_1<\deg r_2$.

因为 $(h+us_1+u^2s_2)u^2a_2=0$,则 $ha_2=0$,即有 $\hat{h}|a_2$. 又 $(h+us_1+u^2s_2)u^2\hat{h}=0$,则必有 $a_2|\hat{h}$. 而 $a_2,\hat{h}$ 均首一,则 $a_2=\hat{h}$,即 $h=\hat{a}_2$. 同理可知 $r_2=\hat{g}$.

因为 $(ur_1+u^2t_1)(ua_1+u^2q_1)=0$,则有 $r_1a_1=0,t_1g+r_1p_1=0$. 而 $(u\hat{a}_1-u^2p_1\hat{a}_1/g)C=0$,即 $u\hat{a}_1-u^2p_1\hat{a}_1/g\in A(C)$,且 r_1,a_1 首一,则易知 $r_1=\hat{a}_1$,$t_1=-p_1\hat{a}_1/g$.

因为 $(h+us_1+u^2s_2)(g+up_1+u^2p_2)=0$,$(h+us_1+u^2s_2)(ua_1+u^2q_1)=0$,推知 $a_1s_1+q_1h=0$,$s_1g+p_1h=0$,即 $a_1s_1+q_1\hat{a}_2=0$,$s_1g+p_1\hat{a}_2=0$,而 $\deg s_1<\deg r_1$,$\deg q_1<\deg a_2$,则 $s_1=-q_1\hat{a}_2/a_1$. 因为 $s_1g+p_1\hat{a}_2=0$,即 $-q_1\hat{a}_2g/a_1+p_1\hat{a}_2=0$,则容易验证

$$(\hat{a}_2-uq_1\hat{a}_2/a_1+u^2q_1p_1\hat{a}_2/(ga_1)-u^2\hat{a}_2p_2/g)C=0,$$

则

$$\hat{a}_2-uq_1\hat{a}_2/a_1+u^2q_1p_1\hat{a}_2/(ga_1)-u^2\hat{a}_2p_2/g\in A(C).$$

设

$$D=\left\langle\hat{a}_2-uq_1\hat{a}_2/a_1+u^2q_1p_1\hat{a}_2/(ga_1)-u^2\hat{a}_2p_2/g,\ u\hat{a}_1-u^2p_1\hat{a}_1/g,u^2\hat{g}\right\rangle,$$

则有 $D\subseteq A(C)$. 容易验证 $|D|=p^{m(\deg g+\deg a_1+\deg a_2)}$. 而

$$|A(C)|=p^{m(3n-\deg h-\deg r_1-\deg r_2)}=p^{m(\deg g+\deg a_1+\deg a_2)},$$

则有 $D=A(C)$.

引用文献[16]的引理 5.2 的研究方法,有下面定理:

定理 3.1　设 C 是环 R 上长度为 n 的负循环码,且唯一表示为

$$C=\langle g+up_1+u^2p_2,ua_1+u^2q_1,u^2a_2\rangle,$$

则它的对偶码为

$$C^{\perp}=\left\langle(\hat{a}_2-uq_1\hat{a}_2/a_1+u^2q_1p_1\hat{a}_2/(ga_1)-u^2\hat{a}_2p_2/g)^*,\ (u\hat{a}_1-u^2p_1\hat{a}_1/g)^*,u^2\hat{g}^*\right\rangle,$$

且 $|C^{\perp}|=p^{m(\deg g+\deg a_1+\deg a_2)}$.

证明 令

$$D'=\left\langle\begin{matrix}(\hat{a}_2-uq_1\hat{a}_2/a_1+u^2q_1p_1\hat{a}_2/(ga_1)-u^2\hat{a}_2p_2/g)^*,\\(u\hat{a}_1-u^2p_1\hat{a}_1/g)^*,u^2\hat{g}^*\end{matrix}\right\rangle,$$

因为 $a_2\mid a_1\mid g\mid x^n+1$,则 $\deg\hat{a}_2=\deg\hat{a}_2^*$,$\deg\hat{a}_1=\deg\hat{a}_1^*$,$\deg\hat{g}=\deg\hat{g}^*$,容易证明 $|D'|=p^{m(3n-\deg\hat{g}-\deg\hat{a}_1-\deg\hat{a}_2)}$,即 $|D'|=p^{m(\deg g+\deg a_1+\deg a_2)}$. 由 $\hat{a}_2-uq_1\hat{a}_2/a_1+u^2q_1p_1\hat{a}_2/(ga_1)-u^2\hat{a}_2p_2/g\in A(C)$,$u^2\hat{g}\in A(C)$,$u\hat{a}_1-u^2p_1\hat{a}_1/g\in A(C)$,有 $(\hat{a}_2-uq_1\hat{a}_2/a_1+u^2q_1p_1\hat{a}_2/(ga_1)-u^2\hat{a}_2p_2/g)^*\in A(C)^*$,$u^2\hat{g}^*\in A(C)^*$,$(u\hat{a}_1-u^2p_1\hat{a}_1/g)^*\in A(C)^*$,推知 $D'\subseteq A(C)^*=C^{\perp}$. 而

$$|C^{\perp}|=p^{3m}/|C|=p^{m(\deg g+\deg a_1+\deg a_2)},$$
$$|D'|=p^{m(\deg g+\deg a_1+\deg a_2)},$$

则 $D'=C^{\perp}$,定理得证. □

推论 3.2 在定理 3.1 中,若 $a_2=g$,则

$$C^{\perp}=\langle((x^n+1)/(g+up_1+u^2p_2))^*\rangle.$$

若 $a_1=g$,则

$$C^{\perp}=\langle(\hat{a}_2-uq_1\hat{a}_2/a_1+u^2q_1p_1\hat{a}_2/(ga_1)-u^2\hat{a}_2p_2/g)^*,u\hat{g}^*\rangle.$$

证明 若 $a_2=g$,由推论 2.3 直接可以证明

$$C^{\perp}=\langle((x^n+1)/(g+up_1+u^2p_2))^*\rangle.$$

若 $a_1=g$,由推论 2.3 知 $C=\langle g+up_1+u^2p_2,u^2a_2\rangle$. 设

$$D''=\langle(\hat{a}_2-uq_1\hat{a}_2/a_1+u^2q_1p_1\hat{a}_2/(ga_1)-u^2\hat{a}_2p_2/g)^*,u\hat{g}^*\rangle$$

易证 $\hat{a}_2-uq_1\hat{a}_2/a_1+u^2q_1p_1\hat{a}_2/(ga_1)-u^2\hat{a}_2p_2/g$,$u\hat{g}$ 均属于 $A(C)$,则 $D''\subseteq A(C)$. 易证 $|D''|=p^{m(2\deg g+\deg a_2)}$,$|C|=p^{m(3n-\deg a_2-2\deg g)}$,而

$$|A(C)|=|C^{\perp}|=p^{m(2\deg g+\deg a_2)},$$

则 $D''=A(C)$,因此

$$C^{\perp}=\langle(\hat{a}_2-uq_1\hat{a}_2/a_1+u^2q_1p_1\hat{a}_2/(ga_1)-u^2\hat{a}_2p_2/g)^*,u\hat{g}^*\rangle.$$ □

推论 3.3 在定理 3.1 中,若 $(n,p)=1$,则

$$C^{\perp}=\langle\hat{a}_2^*,u\hat{a}_1^*,u^2\hat{g}^*\rangle.$$

推论 3.4 定义 C 的剩余码与挠码为

$$\mathrm{Res}(C)=\{a\in F_q[x]\mid\exists b,d\in F_q[x],a+ub+u^2d\in C\},$$
$$\mathrm{Tor}(C)=\{f\in S[x]\mid uf\in C\}.$$

则在 S 上有 $\mathrm{Tor}(C^{\perp})=R_1(C)^{\perp}$;在 F_q 上有 $\mathrm{Res}(C^{\perp})=T_1(C)^{\perp}$.

下面研究环 R 上长度为 n 的自对偶负循环码.

设 C 是环 R 上长度为 n 的负循环码,且唯一表示为 $C=\langle g+up_1+u^2p_2,ua_1+u^2q_1,u^2a_2\rangle$. 由定理 2.2 与定理 3.1 可知

$$|C|=q^{(3n-\deg a_2-\deg g-\deg a_1)},$$
$$|C^{\perp}|=q^{\deg g+\deg a_1+\deg a_2}.$$

若 C 是自对偶负循环码,即 $C=C^{\perp}$,则必有

$$3n-\deg g-\deg a_1-\deg a_2=\deg g+\deg a_1+\deg a_2,$$

即 $3n=2(\deg g+\deg a_1+\deg a_2)$,则 n 必须为偶数.

由负循环码的唯一性可得 $a_2=\alpha^{-1}\hat{g}^*$,其中,α 为 $\hat{g}^*$ 的首项系数. 因为 $g\mid(x^n+1)$,必有 $\alpha\neq0$,$\deg a_2=\deg\hat{g}^*=\deg\hat{g}$,即有 $\deg a_2+\deg g=n$. 于是有 $\deg a_1=3n/2-(\deg g+\deg a_2)=n/2$. 又由 $(ua_1+u^2q_1)^2=0$ 可知 $a_1^2=0$. 因为 a_1 首一,则必有 $a_1^2=x^n+1=(x^k+1)^{p^s}$. 若 $p>2$,则 k 为偶数,而 x^k+1 没有重根,x^k+1 为不可能为某一多项式的平方,因此 $p=2$,$n=2^sk$,且 $a_1=x^{n/2}+1$.

由 $C=C^{\perp}$ 可得

$$(g+up_1+u^2p_2)^2=0,$$
$$(g+up_1+u^2p_2)u^2a_2=0,$$

可推知 $p_1^2=0$,$ga_2=0$. 而 $\deg p_1<\deg a_1=n/2$,$\deg a_2+\deg g=n$,且 g,a_2 均首一,则必有 $p_1=0$,$a_2=\hat{g}=\alpha^{-1}\hat{g}^*$. 于是由定理 3.1 可知

$$C^{\perp}=\langle(g+u^2p_2)^*,ua_1,u^2\alpha a_2\rangle=\langle(g+u^2p_2)^*,ua_1,u^2a_2\rangle.$$

由 C 的唯一表示有 $(g+u^2p_2)^*=\beta(g+u^2p_2)$,$q_1=0$,其中 β 为 $g+u^2p_2$ 的最低次项系数.

现在我们有 $C=\langle g+u^2p_2,u(x^{n/2}+1),u^2\hat{g}\rangle$,于是我们有下面定理:

定理 3.5 设 C 是 R 上长度为 n 的负循环码,且唯一表示为

$$C=\langle g+up_1+u^2p_2,ua_1+u^2q_1,u^2a_2\rangle,$$

则 C 为自对偶负循环码当且仅当 R 的特征 $p=2$,且 $q_1=p_1=0$,$a_1=x^{n/2}+1$,$a_2=\hat{g}=\alpha\hat{g}^*$,$(g+u^2p_2)^*=\beta(g+u^2p_2)$,其中,$\alpha$ 为 $\hat{g}^*$ 的首项系数,β 为 $g+u^2p_2$ 的最低次项系数.

例 设 $q=4$,$n=6$,有

$$x^6+1=(x^2+x+1)^2(x+1)^2.$$

设 C 是环 $F_4+uF_4+u^2F_4$ 上长度为 6 的负循环码,若它是自对偶负循环码,则可唯一表示为

$C=\langle g+u^2p_2, u(x^2+x+1)(x+1), u^2\hat{g}\rangle$，其中，$g\mid x^6+1$ 且 $\hat{g}\mid g$，$\deg g\geqslant 3$，$\deg p_2<\deg \hat{g}$，$(g+u^2p_2)^*=\beta(g+u^2p_2)$，$\beta$ 为 $g+u^2p_2$ 的最低次项系数. 则我们可以给出环 $F_4+uF_4+u^2F_4$ 上所有长度为 6 的自对偶负循环码，如下：

$\langle x^3+1+u^2(x^2+x), u(x^3+1), u^2(x^3+1)\rangle$；

$\langle (x^3+1)(x+1), u(x^3+1), u^2(x^2+x+1)\rangle$；

$\langle u(x^3+1), u^2\rangle$；

$\langle (x^2+x+1)^2(x+1), u(x^3+1), u^2(x+1)\rangle$.

4　结论

本文主要对环 $F_q+uF_q+u^2F_q$ 上任意长度的负循环码及其对偶码进行了研究，得到了负循环码及其对偶码的结构，并在此基础上研究了环 $F_q+uF_q+u^2F_q$ 上的自对偶负循环码. 对于有限链环上负循环码理论的研究，本文具有很好的推广价值及借鉴意义. 但本文没有具体研究这些码的重量分布及其距离的性质，这是以后一个重要的研究方向.

参考文献(References)

[1] Abualrub T, Oehmke R. On the generators of Z_4 cyclic codes of length 2^e [J]. IEEE Transactions on Information Theory, 2003, 49(9): 2 126-2 133.

[2] Blackford T. Cyclic codes over Z_4 of odely even length [J]. Discrete Applied Mathematics, 2003, 128(1): 27-46.

[3] Li Ping, Zhu Shixin. Cyclic codes of arbitrary lengths over the ring F_q+uF_q [J]. Journal of University of Science and Technology of China, 2008, 38(12): 1 392-1 396.
李平，朱士信. 环 F_q+uF_q 上任意长度的循环码[J]. 中国科学技术大学学报，2008，38(12)：1 392-1 396.

[4] Dinh H Q. Constacyclic codes of length p^s over $F_{p^m}+uF_{p^m}$ [J]. Journal of Algebra, 2010, 324(5): 940-950.

[5] Ding Jian, Li Hongju, Liu Jiabao. A class of constacyclic codes over the ring $F_{p^m}+uF_{p^m}$ [J]. Journal of Hefei University of Technology (Natural Science), 2011, 34(4): 634-640.
丁健，李红菊，刘家保. 环 $F_{p^m}+uF_{p^m}$ 上的一类常循环码[J]. 合肥工业大学学报(自然科学版)，2011，34(4)：634-640.

[6] Ding Jian, Li Hongju, Li Haixia. On the equivalence of constacyclic codes over the ring $F_{p^m}+uF_{p^m}$ [J]. Journal of University of Science and Technology of China, 2013, 43(4): 334-339.
丁健，李红菊，李海霞. 关于环 $F_{p^m}+uF_{p^m}$ 上常循环码的等价性[J]. 中国科学技术大学学报，2013，43(4)：334-339.

[7] Abualrub T, Siap I. Cyclic codes over the ring Z_2+uZ_2 and $Z_2+uZ_2+u^2Z_2$ [J]. Designs Codes and Cryptography, 2007, 42(3): 273-287.

[8] Yu Haifeng, Zhu Shixin. $(1+u+u^2)$-cyclic codes over ring $F_2+uF_2+u^2F_2$ [J]. Application Research of Computers, 2010, 27(5): 1 845-1 846.
余海峰，朱士信. 环 $F_2+uF_2+u^2F_2$ 上的$(1+u+u^2)$-循环码[J]. 计算机应用研究，2010，27(5)：1 845-1 846.

[9] Shi Minjia. Constacyclic self-dual codes over ring $F_2+uF_2+\cdots+u^{m-1}F_2$ [J]. Acta Electronica Sinica, 2013, 41(6): 1 088-1 092.
施敏加. 环 $F_2+uF_2+\cdots+u^{m-1}F_2$ 上的常循环自对偶码[J]. 电子学报，2013，41(6)：1 088-1 092.

[10] Shi Minjia, Zhu Shixin. Constacyclic codes over ring $F_p+uF_p+\cdots+u^{s-1}F_p$ [J]. Journal of University of Science and Technology of China, 2009, 39(6): 583-587.
施敏加，朱士信. 环 $F_p+uF_p+\cdots+u^{s-1}F_p$ 上的常循环码[J]. 中国科学技术大学学报，2009，39(6)：583-587.

[11] Dinh H Q, López-Permouth S R. Cyclic and negacyclic codes over finite chain rings[J]. IEEE Transactions on Information Theory, 2004, 50(8): 1 728-1 744.

[12] Blackford T. Negacyclic codes over Z_4 of even length [J]. IEEE Transactions on Information Theory, 2003, 49(6): 1 417-1 424.

[13] Dinh H Q. Complete Distances of all negacyclic codes of length 2^s over Z_{2^a} [J]. IEEE Transactions on Information Theory, 2007, 53(1): 147-161.

[14] Zhu Shixin, Kai Xiaoshan. On the homogeneous distance of negacyclic codes over Z_{2^a} [J/OL]. Sciencepaper Online, [2012-02-28]. http://www.paper.edu.cn/releasepaper/content/201202-1048.
朱士信，开晓山. 关于 Z_{2^a} 上的负循环码的齐次距离[J/OL]. 中国科技论文在线，[2012-02-28]. http://www.paper.edu.cn/releasepaper/content/201202-1048.

[15] Xi Hongqi, Zheng Xiying, Kong Bo. Repeated-root negacyclic codes over Z_{p^a} [J]. Journal of Zhengzhou University (Natural Science Edition), 2012, 44(3): 26-28.
席红旗，郑喜英，孔波. 环 Z_{p^a} 上的重根负循环码[J]. 郑州大学学报(理学版)，2012，44(3)：26-28.

[16] Al-Ashker M M, Chen J Z. Cyclic codes of arbitrary length over $F_p+uF_p+\cdots+u^kF_p$ [J]. Palestine Journal of Mathematics, 2013, 2(1): 72-80.