第38卷第12期 中国科学技术大学学报 Vol. 38, No. 12
2008年12月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Dec. 2008

文章编号:0253-2778(2008)12-1392-05

环 F_q+uF_q 上任意长度的循环码

李　平,朱士信

(合肥工业大学应用数学系,安徽合肥 230009)

摘要:最近,环 F_q+uF_q 上的码引起编码学家极大的兴趣.为此研究了该环上任意长度的循环码及其对偶码,并运用有限环理论,给出了这些循环码及其对偶码的可以唯一确定的生成元的表达形式,并确定了这些循环码的秩.

关键词:环 F_q+uF_q;环同态;循环码;对偶码;秩

中图分类号:TN911.22　　**文献标识码**:A

AMS Subject Classification (2000): 94B15

Cyclic codes of arbitrary lengths over the ring F_q+uF_q

LI Ping, ZHU Shi-xin

(*Department of Applied Mathematics, Hefei University of Technology, Hefei* 230009, *China*)

Abstract: Recently codes over the ring F_q+uF_q have received a great deal of interest among coding researchers. Cyclic codes and their duals of arbitrary lengths over the ring F_q+uF_q are studied. By using the theory of finite rings, the uniquely determined generators for these codes are obtained and the rank of these cyclic codes is also determined.

Key words: ring F_q+uF_q; ring homomorphism; cyclic codes; dual codes; rank

0 引言

最近,编码学与密码学的爱好者对剩余类环 $F_q[u]/\langle u^k\rangle=F_q+uF_q+\cdots+u^{k-1}F_q$ 产生极大的兴趣(q 为素数 p 的方幂,该环的特征是素数 p,本文多数情况下 $p(x)$或 p 表示多项式,不会引起混淆).文献[1]利用环 $F_p+uF_p=F_P[u]/\langle u^2\rangle$上的线性码进行了格的构造;文献[2,3]利用环 $F_P[u]/\langle u^k\rangle$构造了最佳跳频序列;文献[4]利用环 F_2+uF_2 上码进行了厄米特模形式的构造;文献[5]等利用环 F_q+uF_q上的码通过线性的 gray 映射构造了一大批域 F_q 上的最优码($q=3,5$ 等);文献[6]给出环 F_q+uF_q 上关于厄米特内积的自对偶码计数公式;文献[7]研究了 $F_P[u]/\langle u^k\rangle$上单根循环码及自对偶码的结构;文献[8]证明了环 $F_q[u]/\langle u^s\rangle$上所有的单根循环码皆为最大秩距离码.特别地,已有大量文献对环 F_2+uF_2 上的码进行了研究[9~16].其中文献[9]对环F_2+uF_2 上具有奇素数阶自同构的自对偶码进行了分类;文献[10]研究了环 F_2+uF_2 上$(1+u)$-常循环码及循环码的 gray 像性质;文献[11]讨论了环 F_2+uF_2 上码关于李距离的覆盖半径;文献[12]讨论了环 F_2+uF_2 上循环码的构造及其对偶码和汉明距离;文献[13]讨论了环 F_2+uF_2 和 $F_2+uF_2+u^2F_2$ 上循环码的构造及关系.

收稿日期:2007-08-24;**修回日期**:2008-05-15

基金项目:国家自然科学基金(60673074),教育部科学技术研究重点项目(107065),安徽省高校青年教师科研资助计划重点项目(2006JQl002ZD),合肥工业大学科研发展基金项目(061003F)资助.

作者简介:李平,男,1971年生,讲师.研究方向:编码理论与信息安全.E-mail:lpmath@126.com

通讯作者:朱士信,博士/教授.E-mail:sxinzhu@tom.com

大量文献研究了含幺有限交换环上的单根循环码(即码长与该环的特征互素的情形,否则叫做重根循环码)及其对偶码的结构,而重根循环码的研究相比较还很不完善.文献[14]研究了环 F_2+uF_2 上长为 2^e 的循环码;文献[15]给出了环 F_2+uF_2 上长为 $2n$ 的循环码的计数.本文运用环同态理论研究了 $F_q[u]/\langle u^2\rangle=F_q+uF_q$ 上任意长度的循环码及其对偶码.该环的结构见文献[2,8],它是一类特殊的有限链环,文献[17,18]运用相同的方法独立地给出了有限链环上单根循环码的结构.本文还研究了 F_q+uF_q 上任意长度的循环码的秩,当码长 n 较大时,它在计算码的距离分布时可大大简化计算的复杂度.

以下记 $R=F_q[u]/\langle u^2\rangle=F_q+uF_q$.设 C 是 R 上长为 n 的线性码,则 C 的对偶码为

$$C^{\perp}=\{(d_0,d_1,\cdots,d_{n-1})\mid c_0\cdot d_0+c_1\cdot d_1+\cdots+c_{n-1}\cdot d_{n-1}=0,\forall(c_0,c_1,\cdots,c_{n-1})\in C\} \tag{1}$$

式中,运算为环 R 中的加法和乘法.

1　主要结果

域 F_q 是环 R 的子环,x 是 R 及 F_q 上的未定元.$\forall f(x)\in R[x]$,则 $f(x)$ 可唯一地表示为 $f(x)=f_1(x)+uf_2(x)$.其中,$f_1(x),f_2(x)\in F_q[x]$.定义映射 ϕ 如下

$$\phi:R[x]/\langle x^n-1\rangle\to F_q[x]/\langle x^n-1\rangle,$$
$$f(x)+\langle x^n-1\rangle\to f_1(x)+\langle x^n-1\rangle \tag{2}$$

则 ϕ 是商环 $R[x]/\langle x^n-1\rangle$ 到 $F_q[x]/\langle x^n-1\rangle$ 的环满同态.为简洁起见,下文 $s(x)+\langle x^n-1\rangle$ 可以简写成 $s(x)$.多项式 $s(x)$ 也可简写成 s.设 C 是 $R[x]/\langle x^n-1\rangle$ 中的任意理想(即 R 上长为 n 的任意循环码,码长 n 无任何限制),限制 ϕ 作用在 C 上:即

$$\phi:C\to F_q[x]/\langle x^n-1\rangle,$$
$$f(x)+\langle x^n-1\rangle\to f_1(x)+\langle x^n-1\rangle,$$
$$\forall f(x)+\langle x^n-1\rangle=$$
$$f_1(x)+uf_2(x)+\langle x^n-1\rangle\in C \tag{3}$$

式中,$f_1(x),f_2(x)\in F_q[x]$.则 ϕ 是 C 到 $F_q[x]/\langle x^n-1\rangle$ 的环同态,由环同态基本定理可得,$\phi(C)$ 是 $F_q[x]/\langle x^n-1\rangle$ 的理想(该商环中零理想的生成元约定用 x^n-1 表示),即域 F_q 上长为 n 的循环码.从而 $\phi(C)$ 中存在唯一的次数最低的首一多项式 $g(x)$ 满足:$g(x)\mid x^n-1$ 且 $\phi(C)=\langle g(x)\rangle$.此外,该环同态的核 $\mathrm{Ker}\,\phi=\{uh(x):h(x)\in F_q[x],uh(x)\in C\}$ 是 C 的理想,记 $T=\{h(x):h(x)\in F_q[x],uh(x)\in \mathrm{Ker}\,\phi\}$,则易证得 T 是 $F_q[x]/\langle x^n-1\rangle$ 的理想.同理可知,T 中存在唯一的次数最低的首一多项式 $a(x)$ 满足:$a(x)\mid x^n-1$ 且 $T=\langle a(x)\rangle$.从而 $\mathrm{Ker}\,\phi=\langle ua(x)\rangle$.设 $g(x)$ 关于 ϕ 在 C 中的某个原像是 $g(x)+up(x)$,$\langle g(x)+up(x),ua(x)\rangle$ 是 C 的理想,当 $\deg a\leqslant\deg p$ 时,可将 $ua(x)$ 乘上 $x^{\deg p-\deg a}$,再乘上 $p(x)$ 的首项系数的相反数,加到 $g(x)+up(x)$ 上去,获得 $g(x)+up_1(x)$,则 $\langle g(x)+up_1(x),ua(x)\rangle=\langle g(x)+up(x),ua(x)\rangle$;若 $\deg a\leqslant\deg p_1$,类似的运算继续进行,故 C 的理想 $\langle g(x)+up(x),ua(x)\rangle$ 中不妨设 $\deg a>\deg p$.我们断言:$C=\langle g(x)+up(x),ua(x)\rangle$,且满足 $\deg a>\deg p$ 的 $p(x)\in F_q[x]$ 也是唯一确定的.由于 $ug(x)\in C$,$ug(x)\in \mathrm{Ker}\,\phi$,故 $g(x)\in T$,从而 $a(x)\mid g(x)$.由 $\deg p<\deg a\leqslant\deg g$ 知,$g(x)+up(x)$ 是首一多项式.$\forall f(x)\in C$,若 $f(x)\notin \mathrm{Ker}\,\phi$,则 $\phi(f(x))=g(x)\alpha(x)\neq0$,记 $f(x)=g(x)\alpha(x)+u\beta(x)$.由于 $g(x)+up(x)$ 是首一多项式,根据带余除法

$$f(x)=g(x)\alpha(x)+u\beta(x)=$$
$$[g(x)+up(x)]\gamma(x)+t(x) \tag{4}$$

式中,$\gamma(x),t(x)\in R[x]$,$t(x)=0$,或者 $\deg t<\deg(g+up)=\deg g$.若 $t(x)\neq0$,则 $\deg t<\deg g$;又由于 $t(x)\in C$,$\phi(t(x))\in\phi(C)=\langle g(x)\rangle$,从而 $\deg g\leqslant\deg\phi(t(x))\leqslant\deg t$,推出矛盾.故必然 $t(x)=0$,$f(x)\in\langle g(x)+up(x)\rangle$.故 $C\subseteq \mathrm{Ker}\,\phi\cup\langle g(x)+up(x)\rangle\subseteq\langle g(x)+up(x),ua(x)\rangle$,而 $\langle g(x)+up(x),ua(x)\rangle$ 是 C 的理想,故 $C=\langle g(x)+up(x),ua(x)\rangle$.若 $C=\langle g(x)+up(x),ua(x)\rangle=\langle g(x)+u\lambda(x),ua(x)\rangle$.其中,$\deg p<\deg a$,$\deg\lambda<\deg a$.则比较 $g(x)+u\lambda(x)=[g(x)+up(x)]\theta(x)+ua(x)\upsilon(x)$ 两边系数,必然 $\theta(x)=1$,$u\{[\lambda(x)-p(x)]-a(x)\upsilon(x)\}=0$;因为 $[\lambda(x)-p(x)]-a(x)\upsilon(x)\in F_q[x]$,故其必然为 0,从而有 $a(x)\mid\lambda(x)-p(x)$,比较多项式次数,得 $\lambda(x)=p(x)$.综合以上讨论,我们有下面的定理.

定理 1.1　设 C 是 $R[x]/\langle x^n-1\rangle$ 的任意理想(即 R 上长为任意正整数 n 的任意循环码),则存在唯一的满足 $a(x)\mid g(x)\mid x^n-1$,$\deg a>\deg p$ 的 $F_q[x]$ 中的多项式 $g(x),a(x),p(x)$,使得 $C=\langle g(x)+up(x),ua(x)\rangle$.

注　若在定理 1.1 中取 $n=p^e$,由于 $x^n-1=(x-1)^n$,而 $F_q[x]$ 是单一分解整环,$a(x),g(x)$ 具

有形式 $a(x)=(x-1)^m$，$g(x)=(x-1)^s$，且 $m\leqslant s$. 从而 C 可分三种情形讨论：

（Ⅰ）$m=s$ 时

$$C=\langle g(x)+up(x)\rangle=\langle (x-1)^s+u\sum_{i=0}^{s-1}c_i(x-1)^i\rangle$$

（Ⅱ）$m<s$ 且 $s\neq n$ 时

$$C=\langle g(x)+up(x),ua(x)\rangle=\langle (x-1)^s+u\sum_{i=0}^{m-1}c_i(x-1)^i,u(x-1)^m\rangle$$

（Ⅲ）$m<s$ 且 $s=n$ 时，$g(x)=x^n-1$，由下面的引理 1.1 知 $a(x)\mid p(x)$，而 $\deg p<\deg a$，必然 $p(x)=0$，从而 $C=\langle u(x-1)^m\rangle$. 当 $p=2$ 时，该结果与文献[14]的一个主要定理是一致的.

引理 1.1 上述定理中 $a(x)\mid p(x)\dfrac{x^n-1}{g(x)}$.

证明 $\phi\left(\dfrac{x^n-1}{g(x)}[g+up]\right)=\phi\left(up\dfrac{x^n-1}{g}\right)=0$，从而 $up\dfrac{x^n-1}{g}\in\mathrm{Ker}\,\phi$，故 $p\dfrac{x^n-1}{g}\in T$，引理得证.

定理 1.2 若 $(p,n)=1$，则定理 1.1 中 $C=\langle g(x),ua(x)\rangle=\langle g(x)+ua(x)\rangle$. 进一步，若 $a(x)=g(x)$，则 $C=\langle g(x)\rangle$，且是秩为 $n-\deg g$ 的自由模，具有基 $\{g,xg,\cdots,x^{n-\deg g-1}g,\}$；否则 C 不是自由模，但其秩为 $n-\deg a$，具有最小生成元集 $\{g,xg,\cdots,x^{n-\deg g-1}g,ua,xua,\cdots,x^{\deg g-\deg a-1}ua\}$.

证明 由于 $(p,n)=1$，x^n-1 可唯一地分解为 F_q 上两两不同的不可约多项式的乘积，从而 $\left(g,\dfrac{x^n-1}{g}\right)=1$；又 $a(x)\mid g(x)$，故 $\left(a,\dfrac{x^n-1}{g}\right)=1$，再据引理 1.1，$a(x)\mid p(x)\dfrac{x^n-1}{g(x)}$，必然 $a(x)\mid p(x)$，而 $\deg a>\deg p$，故 $p(x)=0$，$C=\langle g(x),ua(x)\rangle$. 再由 $\left(g,\dfrac{x^n-1}{g}\right)=1$ 知，存在 $m_1(x),m_2(x)\in F_q[x]$，使得 $gm_1+\dfrac{x^n-1}{g}m_2=1$，$ugm_1a+ua\dfrac{x^n-1}{g}m_2=ua$. 考察该等式左边，显然 $ug\in\langle g+ua\rangle$；又由于 $ua\dfrac{x^n-1}{g}=\dfrac{x^n-1}{g}(g+ua)\in\langle g+ua\rangle$，故 $ua\in\langle g+ua\rangle$，也就有 $g\in\langle g+ua\rangle$. 从而 $\langle g,ua\rangle\subseteq\langle g+ua\rangle$，并且 $\langle g,ua\rangle\supseteq\langle g+ua\rangle$，故 $C=\langle g,ua\rangle=\langle g+ua\rangle$. 进一步，若 $a(x)=g(x)$，则显然 $C=\langle g(x)\rangle$. 由于 $g(x)\mid x^n-1$，关于 C 是秩为 $n-\deg g$ 的自由模的证明与域上循环码的生成矩阵的证明是类似的，这里不再给出. 若 $a(x)\neq g(x)$，则 C 的最小生成元集的证明与下面定理 1.3 的证明是类似的，这里也不再给出.

注 上述定理中存在唯一的 $a(x)$，$g(x)$ 使得 $C=\langle g(x),ua(x)\rangle$，且 $a(x)\mid g(x)\mid x^n-1$ 与文献[18]的定理 2.5 是完全一致的. 据本文后面定理 1.4 的第（Ⅱ）种情形的证明方法，可证得 $C^{\perp}=\left\langle\left(\dfrac{x^n-1}{a}\right)^*,u\left(\dfrac{x^n-1}{g}\right)^*\right\rangle$，进一步，$\left(\dfrac{x^n-1}{g}\right)^*\mid\left(\dfrac{x^n-1}{a}\right)^*\mid x^n-1$，从而不难理解 $C^{\perp}=\left\langle\left(\dfrac{x^n-1}{a}\right)^*+u\left(\dfrac{x^n-1}{g}\right)^*\right\rangle$.

定理 1.3 若 $(n,p)\neq 1$，关于定理 1.1 中循环码 C：（Ⅰ）若 $a(x)=g(x)$，则 $C=\langle g+up\rangle$，且在 $R[x]$ 中，$(g+up)\mid x^n-1$，从而 C 是秩为 $n-\deg g$ 的自由模，具有基 $\{g+up,x(g+up),\cdots,x^{n-\deg g-1}(g+up)\}$；（Ⅱ）否则，$C$ 不是自由模，但其秩为 $n-\deg a$，具有最小生成元集 $\Gamma=\{g+up,x(g+up),\cdots,x^{n-\deg g-1}(g+up),ua,xua,\cdots,x^{\deg g-\deg a-1}ua\}$.

证明 （Ⅰ）由 $ua=ug\in\langle g+up\rangle$ 知 $C=\langle g+up,ua\rangle=\langle g+up\rangle$. 由带余除法，$x^n-1=(g+up)\omega(x)+\mu(x)$，其中 $\mu(x)=0$，或者 $\deg\mu<\deg g$. 由于 $\mu(x)\in C$，若 $\mu(x)\neq 0$，则 $\deg\phi(\mu(x))\leqslant\deg\mu<\deg g$，而 $g\mid\phi(\mu(x))$，必然 $\phi(\mu(x))=0$，$\mu(x)=u\mu_1(x)\in\mathrm{Ker}\,\phi$，$\mu_1(x)\in T$，$a(x)\mid\mu_1(x)$，又 $\mu_1(x)\neq 0$，从而 $\deg a\leqslant\deg\mu_1$，即 $\deg g\leqslant\deg\mu_1=\deg\mu$，矛盾. 故必然 $\mu(x)=0$，从而 $(g+up)\mid x^n-1$. 由于 $(g+up)\mid x^n-1$，关于 C 是秩为 $n-\deg g$ 的自由模的证明与域上循环码的生成矩阵的证明是类似的.

（Ⅱ）显然 $\{g+up,x(g+up),\cdots,x^{n-\deg g-1}(g+up),ua,xua,\cdots,x^{n-\deg a-1}ua\}$ 是 C 的一个生成元集；现证明 $ux^{\deg g-\deg a}a(x)$ 可由 Γ 生成. 设 $x^{\deg g-\deg a}a(x)=g(x)+\delta(x)$，由于 $a(x)\mid g(x)\mid x^n-1$，故 $\delta(x)\neq 0$，且 $a(x)\mid\delta(x)$. 设 $\delta(x)=a(x)\pi(x)$，由 $\deg a\leqslant\deg\delta\leqslant\deg g-1$ 知，$\deg\pi\leqslant\deg g-1-\deg a$. 从而

$$\begin{aligned}ux^{\deg g-\deg a}a(x)&=u(g+up)+u\delta(x)=\\&u(g+up)+ua(x)(\pi_0+\pi_1x+\cdots+\\&\pi_{\deg g-\deg a-1}x^{\deg g-\deg a-1})\end{aligned}\tag{5}$$

这就证明了 Γ 确实是 C 的一个生成元集. 现在只需证明 Γ 中任一个元素皆不可能由 Γ 中其余的元素线性表示. 当 $0\leqslant i\leqslant n-\deg g-1$ 时，假设

$$x^i(g+up)=(g+up)c_0+\cdots+$$

$$x^{i-1}(g+up)c_{i-1}+x^{i+1}(g+up)c_{i+1}+\cdots+$$
$$x^{n-\deg g-1}(g+up)c_{n-\deg g-1}+ua(x)d_0+$$
$$xua(x)d_1+\cdots+x^{\deg g-\deg a-1}ua(x)d_{\deg g-\deg a-1}$$

这里 $c_j,d_j\in R$. 由左边多项式次数知，$c_{i+1}=\cdots=c_{n-\deg g-1}=0$，从而右边多项式次数不大于 $i-1+\deg g$，而左边多项式次数为 $i+\deg g$，推出矛盾. 当 $0\leqslant k\leqslant \deg g-\deg a-1$ 时，假设

$$x^k ua(x)=(g+up)b_0+x(g+up)b_1+\cdots+$$
$$x^{n-\deg g-1}(g+up)b_{n-\deg g-1}+ua(x)e_0+\cdots+$$
$$x^{k-1}ua(x)e_{k-1}+x^{k+1}ua(x)e_{k+1}+\cdots+$$
$$x^{\deg g-\deg a-1}ua(x)e_{\deg g-\deg a-1}$$

这里 $b_j,e_j\in R$. 由左边多项式次数不大于 $\deg g-1$，推出 $b_0=b_1=\cdots=b_{n-\deg g-1}=0$. 再比较两边最高次幂的系数知，$e_{\deg g-\deg a-1}=0$，依次比较下去，可得 $e_{\deg g-\deg a-2}=0,\cdots,e_{k+1}=0$，由此再比较等式两边得：左边多项式次数为 $k+\deg a$，而右边多项式次数不大于 $k-1+\deg a$，推出矛盾. 这就证明了 Γ 确为 C 的一个最小生成元集，码 C 的秩为 $n-\deg a$.

注　由定理 1.2 和定理 1.3，立即获得如下结论：设 C 是 R 上长为任意正整数 n 的循环码，则 C 是秩为 $n-k$ 的自由模当且仅当 C 中存在多项式 $\varepsilon(x)$ 满足 $C=\langle\varepsilon(X)\rangle$，且在 $R[x]$ 中，$\varepsilon(x)\mid x^n-1$，$\deg\varepsilon=k$. 该结论对码长 n 无任何限制，即对重根循环码亦成立，是文献[16]中相应结论的推广.

下面研究 R 上循环码的对偶码. 设 I 是 $R[x]/\langle x^n-1\rangle$ 的理想，则集合 $A(I)=\{g(x):f(x)g(x)=0,\forall f(x)\in I\}$ 称为 I 在 $R[x]/\langle x^n-1\rangle$ 中的零化子；r 次多项式 $f(x)=c_0+c_1x+\cdots+c_rx^r$ 的互反多项式定义为 $f^*(x)=c_r+c_{r-1}x+\cdots+c_0x^r$；若与循环码 C 相关的理想记为 $A(C)$，则与 C 的对偶码 $C^\perp$ 相关的理想是 $A(C)^*=\{g^*(x):\forall g(x)\in A(C)\}$.

定理 1.4　若 $(n,p)\neq 1$，关于定理 1.3 中循环码 C：(Ⅰ) 若 $a(x)=g(x)$，则 $C=\langle g+up\rangle$，且在 $R[x]$ 中，$(g+up)\mid x^n-1$，从而 $A(C)=\langle\frac{x^n-1}{g+up}\rangle$，也就有 $C^\perp=\langle\left(\frac{x^n-1}{g+up}\right)^*\rangle$. (Ⅱ) 否则，$C=\langle g+up,ua\rangle$，从而 $A(C)=\langle\frac{x^n-1}{a}-u\frac{p\frac{x^n-1}{g}}{a},u\frac{x^n-1}{g}\rangle$，也就有 $C^\perp=\langle\left(\frac{x^n-1}{a}-u\frac{p\frac{x^n-1}{g}}{a}\right)^*,u\left(\frac{x^n-1}{g}\right)^*\rangle$.

证明　(Ⅰ) 由于 $(g+up)\mid x^n-1$，结论的证明与域上循环码的对偶码的生成元的证明类似.

(Ⅱ) 不难区分以下多项式的运算是在 $R[x]$ 中进行，还是在 $R[x]/\langle x^n-1\rangle$ 中进行. 记 $D=\langle\frac{x^n-1}{a}-u\frac{p\frac{x^n-1}{g}}{a},u\frac{x^n-1}{g}\rangle$，易证 $\frac{x^n-1}{a}-u\frac{p\frac{x^n-1}{g}}{a}\in A(C)$，$u\frac{x^n-1}{g}\in A(C)$，从而 $D\subseteq A(C)$；又由于 $A(C)$ 也是 $R[x]/\langle x^n-1\rangle$ 的理想，据定理 1.1 和引理 1.1 可设，$A(C)=\langle h(x)+u\eta(x),u\sigma(x)\rangle$，且 $\sigma(x)\mid h(x)$，$\sigma(x)\mid\eta(x)\frac{x^n-1}{h(x)}$.

因 $ua(h+u\eta)=uah=0$，从而 $ah=(x^n-1)\varphi(x)$，$h=\frac{x^n-1}{a}\varphi$；$gh=0$，$(g+up)(h+u\eta)=ug\eta+uph=0$，$g\eta+p\frac{x^n-1}{a}\varphi=0$. 由引理 1.1 可设，$am=p\frac{x^n-1}{g}$，从而 $g\eta+mg\varphi=0$，$g(\eta+m\varphi)=(x^n-1)\xi$，$\eta+m\varphi=\frac{x^n-1}{g}\xi$，$\eta=\frac{x^n-1}{g}\xi-m\varphi$. $h+u\eta=\frac{x^n-1}{a}\varphi+u\frac{x^n-1}{g}\xi-um\varphi=\varphi\left(\frac{x^n-1}{a}-um\right)+u\frac{x^n-1}{g}\xi\in D$，易证 $u\sigma\in D$，从而 $A(C)\subseteq D$. 故 $A(C)=\langle\frac{x^n-1}{a}-u\frac{p\frac{x^n-1}{g}}{a},u\frac{x^n-1}{g}\rangle$.

2　结论

本文从生成元的角度给出了环 R 上任意长度循环码及其对偶码的结构，并研究了这些循环码的秩. 一个公开的问题是研究环 R 上自对偶的重根循环码及其性质.

参考文献(References)

[1] Bachoc C. Application of coding theory to the construction of modular lattices[J]. Journal of Combinational Theory Series A, 1997, 78(1): 92-119.

[2] Udaya P, Siddiqi M U. Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings[J]. IEEE Transactions on Information Theory, 1998, 44(4): 1 492-1 503.

[3] Eun Y C, Jim S Y, Hong Y P, et al. Frequency hopping sequences with optimal partial autocorrelation properties[J]. IEEE Transactions on Information Theory, 2004, 50(10): 2 438-2 432.

[4] Bannai E, Harada M, Ibukiyama T, et al. Type II codes over $F+uF_2$ and applications to Hermitian modular forms [J]. Abhandlungen aus dem Mathematischen Seminar der Universitat Hamburg, 2003, 73(1): 13-42.

[5] Gulliver T A, Harada M. Codes over F_3+uF_3 and improvements to the bounds on ternary linear codes [J]. Designs, Codes and Cryptography, 2001, 22(1): 89-96.

[6] Gaborit P. Mass formulas for self-dual codes over z_r and F_q+uF_q rings [J]. IEEE Transactions on Information Theory, 1996, 42(4): 1 222-1 228.

[7] Qian J F, Zhang L N, Zhu S X. Cyclic codes over $F_p+uF_P+\cdots u^{k-1}F_p$ [J]. IEICE Transactions on Fundamentals, 2005, E88-A(3): 795-797.

[8] Ozen M, Siap I. Linear codes over $F_q[u]/\langle u^s\rangle$ with respect to the Rosenbloom-Tasfasman metric [J]. Designs, Codes and Cryptography, 2006, 38(1): 17-29.

[9] Huffman W C. On the decomposition of self-dual codes over F_2+uF_2 with an automorphism of odd prime order[J]. Finite Fields and Their Applications, 2007, 13(3): 681-712.

[10] Qian J F, Zhang L N, Zhu S X. (1+u)-constacyclic and cyclic codes over F_2+uF_2 [J]. Applied Mathematics Letters, 2006, 19(8): 820-823.

[11] Li P, Zhu S X, Yu H F. Covering radius of codes over ring F_2+uF_2[J]. Journal of University of Science and Technology of China, 2008, 38(2): 145-148.
李平,朱士信,余海峰. 环 F_2+uF_2 上码的覆盖半径[J]. 中国科学技术大学学报,2008,38(2):145-148.

[12] Abualrub T, Siap I. On the construction of cyclic codes over the ring F_2+uF_2 [J]. Wseas Transactions on mathematics, 2006, 6(5): 750-755.

[13] Abualrub T, Siap I. Cyclic codes over the rings F_2+uF_2 and $F_2+uF_2+u^2F_2$ [J]. Designs, Codes and Cryptography, 2007, 42(3): 273-287.

[14] LI P, ZHU S X. Cyclic codes of length 2^e over F_2+uF_2 [J]. Journal of Electronics and Information Theory, 2007, 29(5): 1 124-1 126.
李平,朱士信. 环 F_2+uF_2 上长为 2^e 的循环码[J]. 电子与信息学报,2007,29(5):1 124-1 126.

[15] WANG D Y, ZHU S X. Number of cyclic codes over F_2+uF_2 of oddly even length[J]. Journal of Hefei University of Technology, 2006, 29(12): 1 470-1 472.
王冬银,朱士信. 环 F_2+uF_2 上长为 $2n$(n 为奇数)的循环码的个数[J]. 合肥工业大学学报,2006,29(12):1 470-1 472.

[16] Li P, Zhu S X. Sufficient and necessary conditions for constacyclic codes over a kind of rings of order four to be free[J]. Journal of Mathematics, 2008, 28(2): 124-128.

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

[18] LI G S, Han W B. Cyclic codes and their Mattson-Solomn polynomials over finite chain rings[J]. Applied Mathematcs—A Journal of Chinese University, 2004, 19(2): 127-134.
李光松,韩文报. 有限链环上的循环码及其 Mattson-Solomn 多项式[J]. 高校应用数学学报 A 辑,2004,19(2):127-134.