环 F_2+uF_2 上长为 2^e 的循环码

李　平　　朱士信
(合肥工业大学应用数学系　合肥　230009)

摘　要：近十多年来，有限环上的循环码一直是编码研究者所关心的热点问题，本文证明了 $R[x]/<x^n-1>$ 不是主理想环，其中 $R=F_2+uF_2$，$u^2=0$ 且 $n=2^e$。分 3 种情形讨论了环 $R[x]/<x^n-1>$ 中的非零理想，并给出了 R 上循环码的可以唯一确定的生成元的表达形式，同时给出了 R 上循环码的李距离的一个上界估计。

关键词：环 F_2+uF_2；循环码；主理想；带余除法；李距离
中图分类号：TN911.22　　**文献标识码**：A　　**文章编号**：1009-5896(2007)05-1124-03

Cyclic Codes of Length 2^e Over F_2+uF_2

Li Ping　Zhu Shi-xin
(*Dept. of Appl. Math.*, *Hefei University of Technology*, *Hefei* 230009, *China*)

Abstract: In the last ten more years, cyclic codes over finite rings have become a hot issue for coding theorists.It is proved that $R[x]/<x^n-1>$ is not a principal ideal domain, where $R=F_2+uF_2$ with $u^2=0$, and $n=2^e$. The nonzero ideals of $R[x]/<x^n-1>$ are discussed in three cases and the expressions of the uniquely determined generators of the cyclic codes are given. An estimate of upper bound of Lee distance of cyclic codes over R is also given.

Key words: F_2+uF_2; Cyclic codes; Principal ideal; Division algorithm; Lee distance

1　引言

文献[1]中引入了一种介于 Z_4 与 F_4 之间的四元环 $R=F_2+uF_2=F_2[u]/<u^2>$，讨论了环 R 上奇长度循环码的结构，并指出了研究 R 上循环码的重要性。文献[2]中给出了 R 上奇长度循环码的简单的译码算法。R 上循环码的研究已成为一个热点[1–8]。

R 的元素是 $\{0,1,u,\ \bar{u}=u+1\}$，具有唯一的极大理想 $\{0,u\}$，F_2 是 R 的一个子环，环 R 上线性码C是指 R-模 R^n 的一个加法子模。

据文献[1,3]，有下面的结论：R 上任一线性码置换等价于具有生成矩阵形如 $\begin{pmatrix} I_{k_1} & A & B_1+uB_2 \\ 0 & uI_{k_2} & uD \end{pmatrix}$ 的码 C，这里 A，B_1，B_2，D 是 (0,1)- 矩阵。C 的剩余码为 $\mathrm{Res(C)}=\{a\in Z_2^n \mid \forall\ a+ub\in \mathrm{C},\ b\in Z_2^n\}$，它是一个二元 $[n,k_1]$ 码；C的挠码 $\mathrm{Tor(C)}$ 为 $\{c\in Z_2^n \mid \forall\ uc\in \mathrm{C}\}$，它是一个二元 $[n, k_1+k_2]$ 码。我们称上述码C具有类型 $\{k_1, k_2\}$，C具有 $4^{k_1}2^{k_2}$ 个码字。定义C的秩为 k_1+k_2，记成 $\mathrm{rank(C)}=k_1+k_2$，亦即生成C的最小数目的生成元的个数。定义C的自由秩为 k_1，记成 $f\text{-rank(C)}=k_1$，亦即C的 R-自由子模的秩的最大值。如果 $k_2=0$，则称C是一个自由码，定义 R 中元素 0，1，u，$1+u$ 的李重量(Lee weight)依次为 0，1，2，1。R^n 中向量的李重量为其各分量的李重量的有理和。定义 R 到 Z_2^2 的一个映射 $\phi:\phi(x+uy)=(y,\ x+y)$，$\forall\ x,\ y\in Z_2$，则 ϕ 是一个从(R，Lee distance)到(Z_2^2，Hamming distance)的距离保持映射，且为线性映射。很自然地，可将 ϕ 扩展成从 R^n 到 Z_2^{2n} 的线性的距离保持映射，ϕ 也称为Gray映射。R 上长为 n 的循环码是指具有如下性质的 R 上线性码：$\forall(c_0,c_1,\cdots,c_{n-1})\in \mathrm{C}$ 均有 $(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in \mathrm{C}$。$c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ 称为码字 $(c_0,c_1,\cdots,c_{n-1})$ 的多项式表示，通常不加区分，从而 R 上循环码即环 $R_n=R[x]/<x^n-1>$ 中的理想。就偶长度而言，R_n 中循环码的结构远比奇长度情形复杂，这里限制 $n=2^e$，e 是正整数。

当 p 整除 n 时，特征为 p 的域上的长为 n 的循环码叫做重根循环码。Castagnoli 和 Van Lint 等人在文献[9,10]中对二元域 F_2 上偶长度循环码进行了深入的研究。Abualrub 和 Blackford 在文献[11，12]中研究了有限环 Z_4 上偶长度循环码。某些情形下，它们是最优码。

就偶数 n 而言，x^n-1 在 $R[x]$ 中的分解并不唯一。例如：$x^4-1=(x-1)^4=(x-1)^2[x-(1+u)]^2$。本文约定零多项式次数为 $+\infty$。不引起混淆时，任一多项式 $f(x)$ 可简记成 f。

2　主要结果

引理 1(文献[13])　设 F 是有限域，C是 F 上长为 n 的任一循环码(即 $F[x]/<x^n-1>$ 中的理想)，则C中次数最低的首一多项式必唯一且整除 x^n-1。且该多项式是C的生成多项式。

2005-10-08 收到，2006-03-13 改回
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(2006jql002 zd)和合肥工业大学科研发展基金项目(061003F)资助课题

值得注意的是该引理对码长 n 无限制，n 可奇可偶。

引理 2(交换环的特征公式)　设 G 是特征为 $p\neq 0$ 的交换环，则 $\forall a,b\in G,\ (a-b)^{p^e}=a^{p^e}-b^{p^e}$。

在引理 2 中取 $G=Z_2[x]$，则 G 是特征为 2 的环，则 $n=2^e$ 时，$x^n-1=(x-1)^n$。而 $Z_2[x]$ 是单一分解整环，从而 x^n-1 的所有因子为 $(x-1)^i$，$0\le i\le n$。在引理 1 中取 $F=Z_2$，则可知 $Z_2[x]/<x^n-1>$ 的所有理想共有 $n+1$ 个。它们是 $<(x-1)^i>, 0\le i\le n$。又由于 $<(x-1)^i>\supset<(x-1)^{i+1}>$，$0\le i\le n-1$，故 $<(x-1)>$ 是 $Z_2[x]/<x^n-1>$ 的唯一的极大理想。

引理 3(文献[14])　设 ϕ 是环 A 到 A' 的满同态，D' 是 A' 的一个理想，$D=\phi^{-1}(D')$ 是 D' 的完全原象，则 D 是 A 的理想，且环 A/D 与 A'/D' 同构。

引理 4(文献[15])　设 ϕ 是环 A 到 A' 的满同态，$\ker\phi=K$，则 A' 的极大理想与 A 中包含 K 的极大理想是一一对应的。

命题 1　设 $n=2^e$，则 R_n 具有唯一的极大理想 $M=<u,x-1>$。

证明　定义 ϕ：$R_n\to Z_2[x]/<x^n-1>$，$a_0+a_1x+\cdots+a_{n-1}x^{n-1}\to\overline{a}_0+\overline{a}_1x+\cdots+\overline{a}_{n-1}x^{n-1}$ 其中 $a_i\in R$，$\overline{0}=\overline{u}=0$，$\overline{1}=\overline{v}=1$ (v即 $1+u$)。

从而 ϕ 是环满同态。又已证得 $Z_2[x]/<x^n-1>$ 具有唯一的极大理想 $<x-1>$，再根据引理 3，$\phi^{-1}(<x-1>)=<u,x-1>$ 是 $R_n=R[x]/<x^n-1>$ 中的极大理想。再根据引理 4，$<x-1>$ 的原象集合 $\phi^{-1}(<x-1>)=<u,x-1>$ 是 R_n 的唯一极大理想。

引理 5　如果 R_n 具有唯一极大理想 $M=<f(x),g(x)>$，若 M 是主理想，则 $M=<f(x)>$ 或 $M=<g(x)>$。

证明　设 $M=<h(x)>$，$\exists\ s(x)\in R_n$ 使得 $f(x)=h(x)\cdot s(x)$。如果 $s(x)$ 是 R_n 中可逆元，则 $h(x)=s(x)^{-1}f(x)$，$M=<f(x)>$。否则，由于 R_n 是具有单位元的有限可换环，$s(x)\in M$，$s(x)=ft_1+gt_2$，$t_1,t_2\in R_n$，$sh=ft_1h+gt_2h$，$f=ft_1h+gt_2h$，$f(1-t_1h)=gt_2h$。又 $1-t_1h\notin M=<h>$，故 $1-t_1h$ 是 R_n 中可逆元，从而 $f=(1-t_1h)^{-1}gt_2h\in<g>$，从而 $M=<g>$。

命题 2　设 $n=2^e$，则 R_n 不是主理想环。

证明　假设 R_n 是主理想环，则 $<u,x-1>=<u>$ 或者 $<x-1>$。又 $x-1$ 与 u 互相不整除，从而 $<u,x-1>\neq<u>$，$<u,x-1>\neq<x-1>$。命题由引理 5 获证。

定理 1　设 $n=2^e$ 且 C 是 R_n 的一个非零理想，则 C 共有 3 种可能情形：

(1) 若 C 中不含首一多项式，则 $C=<u(x+1)^m>$，非负整数 m 由 C 唯一确定。

(2) 若 C 中次数最低的多项式中含有首一多项式，比如 $g(x)$，则 $C=<g(x)>$ 且 $g(x)|x^n-1$。实际上，上述 $g(x)$ 是唯一确定的，且 $g(x)$ 可表达成 $g(x)=(x+1)^m+u\sum_{i=0}^{m-1}c_i(x+1)^i$，$c_i\in Z_2$ ($0\le i\le m-1$)，其中 m 是使得 $u(x+1)^m\in C$ 的最小正整数。

(3) 若 C 中次数最低的多项式中不含有首一多项式，则 C 中次数最低的多项式必为 $u(x+1)^m$，其中非负整数 m 是 C 中次数最低的多项式的次数。此时，若 C 中同时含首一多项式，设 $g(x)$ 是 C 中任一次数最低的首一多项式(并不唯一)，则 $C=<g,uf>$，且 C 不是主理想。设 $\deg g(x)=s$，则 $g(x)$ 可取为 $(x+1)^s+u\sum_{i=0}^{m-1}c_i(x+1)^i$，其中 $c_i\in Z_2$ ($0\le i\le m-1$) 皆被唯一确定。

证明

(1) 若 C 中不含首一多项式，则 C 中也不含首项系数是 $1+u$ 的多项式。设 $f(x)$ 是 C 中任一多项式，则 $f(x)$ 可表为 $f(x)=f_1(x)+uf_2(x)$，其中 $f_1(x)$，$f_2(x)\in Z_2[x]$。由于 $f^2(x)=f_1^2(x)\in C$，故必然 $f_1(x)=0$，从而 $f(x)=uf_2(x)$，$f_2(x)\in Z_2[x]$。设 $us(x)$ 是 C 中次数最低的多项式，其中 $s(x)\in Z_2[x]$，记 $\deg s=m$。设 $ug(x)$ 是 C 中任一多项式，其中 $g(x)\in Z_2[x]$。在 $Z_2[x]$ 中使用带余除法，设 $g(x)=q(x)s(x)+r(x)$，其中 $\deg r<\deg s$ 或 $r(x)=0$。则 $ug(x)=uq(x)s(x)+ur(x)$，从而 $ur(x)\in C$。由于 $us(x)$ 是 C 中次数最低的多项式，故 $r(x)=0$，从而 $ug(x)\in<us(x)>$，从而 $C=<us(x)>$。另一方面，设 $s(x)=\sum_{i=0}^{m}a_i(x+1)^i$，$a_i\in Z_2$，$a_m=1$。若存在 i：$0\le i\le m-1$，使得 $a_i\neq 0$，设其中最小的 i 是 k，则 $s(x)=\sum_{i=k}^{m}a_i(x+1)^i=(x+1)^k\sum_{i=k}^{m}a_i(x+1)^{i-k}=(x+1)^k\left[1+\sum_{i=k+1}^{m}a_i(x+1)^{i-k}\right]$。由于 $1+\sum_{i=k+1}^{m}a_i(x+1)^{i-k}\notin<x+1>$，而 $<x+1>$ 是 $Z_2[x]/<x^n-1>$ 的唯一极大理想，故它不是 $Z_2[x]/<x^n-1>$ 的零因子，而是 $Z_2[x]/<x^n-1>$ 中的可逆元，从而 $u(x+1)^k\in C$。这与 $\deg us(x)=m$ 矛盾，故 $s(x)=(x+1)^m$，$C=<u(x+1)^m>$。

(2) 因为 $g(x)$ 是首一多项式，在 $R[x]$ 中由带余除法，存在唯一的 $k(x)$ 和 $t(x)$ 使得 $x^n-1=k(x)g(x)+t(x)$，其中 $t(x)=0$，或者 $\deg t<\deg g$，又 $g(x)$ 是 C 中次数最低的多项式，而 x^n-1 又可视为 R_n 中理想 C 中零码字，故 $t(x)=0$，从而在 $R[x]$ 中 $g(x)|x^n-1$。$\forall\gamma(x)\in C$，由于 $g(x)$ 是首一多项式，从而由 $R[x]$ 中带余除法，$\gamma(x)=p(x)g(x)+q(x)$，其中 $q(x)=0$ 或 $\deg q<\deg g$。再根据 $g(x)$ 是 C 中次数最低的多项式知 $q(x)=0$，从而 $C=<g(x)>$ 且 $g(x)$ 是唯一确定的。令 $g(x)=g_1(x)+ug_2(x)$，其中 $g_1(x)$，$g_2(x)\in Z_2[x]$。则 $<g_1(x)>$ 是二元循环码，故 $g_1(x)=(x+1)^s$，其中 $0<s<n$。又 $g(x)$ 是首一多项式，从而可令 $g(x)=(x+1)^s+u\sum_{i=0}^{s-1}c_i(x+1)^i$，其中 $c_i\in Z_2$。设 m 是最小正整数，使得 $u(x+1)^m\in C$。由 $ug(x)=u(x+1)^s\in C$ 知 $m\le s$，又 $g(x)$ 是 C 中次数最低的多项式，故 $s\le m$，从而 $m=s$ 且 $g(x)=(x+1)^m+u\sum_{i=0}^{m-1}c_i(x+1)^i$。

(3) 设f_1+uf是C中一个次数最低的多项式，其中f_1，$f\in Z_2[x]$，由题设知$\deg f_1<\deg f$或$f_1=0$。由于$uf_1\in$C，故必然$f_1=0$。由题设，设$\deg g=s$，则$\deg uf<\deg g$。类似于(1)中的证法，必有$f=(x+1)^m$。记集合$M=\{Q(x)|Q(x)\in$C且$\deg Q<s\}$，则$M\neq\phi$，且易知M中多项式首项系数均为u，则M中任一多项式可被uf整除。否则，假设$w(x)$是M中次数最低的不能被uf整除的多项式，记$\deg w=k$，再记$T(x)=w(x)-uf(x)\cdot x^{\deg w-\deg f}$，则$T(x)\in$C，从而若$T(x)\neq 0$，则$T(x)\in M$。又$\deg T<\deg w$，故$T(x)$必然可被$uf$整除，从而$w(x)$必然可被$uf$整除，矛盾。故$M$中任一多项式均可被$uf$整除。$\forall\ c(x)\in$C，由带余除法，$c(x)=p(x)g(x)+r(x)$，其中$r(x)=0$或$\deg r<\deg g=s$。由于$r(x)\in$C，若$\deg r<s$，则$r(x)\in M$，存在$\eta(x)\in Z_4[x]$，使得$r(x)=uf(x)\cdot\eta(x)$。若$r(x)=0$，取$\eta(x)=0$即可。总之，恒有$r(x)=uf(x)\cdot\eta(x)$，故$c(x)=p(x)g(x)+uf(x)\cdot\eta(x)$，故C$=<g(x),uf(x)>$。显然$g$和$uf$互相不整除，由引理 5 此时C不是主理想。类似于(2)中的证法，必有$g(x)=(x+1)^s+u\sum_{i=0}^{s-1}c_i(x+1)^i$，从而C$=<(x+1)^s+u\sum_{i=0}^{s-1}c_i(x+1)^i,\ u(x+1)^m>$，易知C$=<(x+1)^s+u\sum_{i=0}^{m-1}c_i(x+1)^i,\ u(x+1)^m>$。显然$m<s$，且取$g(x)=(x+1)^s+u\sum_{i=0}^{m-1}c_i(x+1)^i$时，$g(x)$是唯一确定的。 证毕

下面我们给出R上长为 2^e的循环码的李距离的一个上界估计公式。

定理 2 设C是R上长为$n=2^e$的循环码，其李距离计为d_L，则$\left\lfloor\frac{d_L-1}{2}\right\rfloor\leqslant m$。其中$m$如定理 1 中所述，即$m$是使得$u(x+1)^m\in$C的最小整数。

证明 如定理 1 所述，C 分 3 种情形：

(1)C$=<u(x+1)^m>$；

(2)C$=<(x+1)^m+u\sum_{i=0}^{m-1}c_i(x+1)^i>$；

(3)C$=<(x+1)^s+u\sum_{i=0}^{m-1}c_i(x+1)^i,\ u(x+1)^m>$

其中m是使得$u(x+1)^m\in$C的最小整数。无论哪种情形，由挠码定义知：Tor(C)的维数为$n-m$，而挠码的维数总等于rank(C)。总之，无论哪种情形，恒有rank(C)$=n-m$。由文献[5]，知：R上长为n的线性码C的李距离d_L满足$\left\lfloor\frac{d_L-1}{2}\right\rfloor\leqslant n-$rank(C)，从而$\left\lfloor\frac{d_L-1}{2}\right\rfloor\leqslant m$。 证毕

当定理 2 中$\left\lfloor\frac{d_L-1}{2}\right\rfloor=m$时，通常称 C 是关于秩的极大李距离码。这是域上最大距离可分码这一概念的推广。

3 结束语

本文证明了$n=2^e$时，R_n不是主理想环，分 3 种情形讨论了环$R[x]/<x^n-1>$中的非零理想，并给出了R上循环码的可以唯一确定的生成元的表达形式，同时给出了R上长为 2^e循环码的李距离的一个上界估计。这些结果对R上循环码进行更深入的研究是有帮助的。比如R上长为 2^e循环码的计数及其对偶码的研究以及R上长为 2^e循环码的距离分布，等等。

参 考 文 献

[1] Bonnecaze A and Udaya P. Cyclic codes and self-dual codes over F_2+uF_2 [J]. *IEEE Trans. on Inform. Theory*, 1999, 45(5): 1250–1255.

[2] Udaya P and Bonnecaze A. Decoding of cyclic codes over F_2+uF_2 [J]. *IEEE Trans. on Inform. Theory*, 1999, 45(6): 2148–2157.

[3] Dougherty S T, Gaborit P, and Harada M. Type II codes over F_2+uF_2 [J]. *IEEE Trans. on Inform. Theory*, 1997, 50(8): 1728–1744.

[4] Ling S and Sole P. Duadic codes over F_2+uF_2 [J]. *Appl. Algebra in Engineering, Communication and Computing*, 2001, 12(2): 365–379.

[5] Dougherty S T and Shiromoto K. Maximum distance codes over rings of order 4[J]. *IEEE Trans. on Inform. Theory*, 2001, 47(1): 400–404.

[6] Dougherty S T, Gaborit P, and Harada M, *et al*.. Type IV self-dual codes over rings [J]. *IEEE Trans. on Inform. Theory*, 1999, 45(7): 2345–2360.

[7] Siap I. Linear codes over F_2+uF_2 and their complete weight enumerators [J]. Codes and Designs, Ohio State Univ. Math Res. Inst. Publ.10, 2000: 259–271.

[8] Gulliver T A and Harada M. Construction of optimal Type IV self-dual codes over F_2+uF_2 [J]. *IEEE Trans. on Inform. Theory*, 1999, 45(7): 2520–2521.

[9] Castagnoli G and Massey J L. On repeated-root cyclic codes[J]. *IEEE Trans. on Inform. Theory*, 1991, 37(3): 337–342.

[10] Van Lint J H. Repeated-root cyclic codes [J]. *IEEE Trans. on Inform. Theory*, 1991, 37(3): 343–345.

[11] Abualrub T and Oehmke T. On the generators of Z_4 cyclic codes [J]. *IEEE Trans. on Inform. Theory*, 2003, 49(9): 2126–2133.

[12] Blackford T. Cyclic codes over Z_4 of oddly even length [C]. in Proc.Int.Workshop on Coding and Crypt., WCC 2001, Paris, France, 2001: 83–92.

[13] Macwilliams F J and Sloane N J A. The Theory of Error-Correcting Codes[M]. Amsterdam: North-Holland publishing company, 1977: 190–191.

[14] 吴品三. 近世代数[M], 北京: 高等教育出版社, 1979: 156–157.

[15] 冯克勤, 李尚志, 查建国. 近世代数引论[M]. 合肥: 中国科技大学出版社, 1988: 106–107.

李 平： 男，1971 年生，讲师，硕士，主要从事代数编码研究.

朱士信： 男，1962 年生，教授，博士，硕士生导师，主要从事代数编码及非线性移位寄存器序列的研究.