环F_2+uF_2的Galois扩张上的迹码

吴　波[①②]　　朱士信[②]
[①②](安徽大学数学系　合肥　230039)
[②](合肥工业大学应用数学系　合肥　230009)

摘　要：环 F_2+uF_2 是介于环 Z_4 与域 F_4 之间的一种四元素环，因此分享了环 Z_4 与域 F_4 的一些好的性质，此环上的编码理论研究成为一个新的热点。该文给出了环 F_2+uF_2 的 Galois 扩张的相关理论，指出此 Galois 扩环的自同构群不同于 Z_4 环上的 Galois 扩环的自同构群；定义了 Galois 扩环上的迹码的概念及子环子码的概念，证明了此 Galois 扩环上的一个码的对偶码的迹码是该环的子环子码的对偶码。

关键词：Galois 扩张；自同构群；迹码；子环子码
中图分类号：TN911.22　　**文献标识码**：A　　**文章编号**：1009-5896(2007)12-2899-03

Trace Codes over Galois Extensions of Ring F_2+uF_2

Wu Bo[①②]　　Zhu Shi-xin[②]
[①](*Department of Mathematics*, *Anhui University*, *Hefei* 230039, *China*)
[②](*Department of Applied Mathematics*, *Hefei University of Technology*, *Hefei* 230009, *China*)

Abstract: F_2+uF_2 is a ring with four elements which shares some good properties of both Z_4 and F_4. Coding theory over this ring has recently received a great deal of interest among coding theorists. This paper gives the theory of Galois extensions over F_2+uF_2, and shows that the automorphism groups of these Galois extensions are different from the corresponding groups over Z_4. Trace codes and subring subcodes over Galois extensions are defined, and it is proved that the trace codes of dual codes of linear codes are the dual codes of subring subcodes.

Key words: Galois extensions; Automorphism groups; Trace codes; Subring subcodes

1　引言

文献[1-3]中引入一种介于 Z_4 与 F_4 之间的四元素环 $R=F_2+uF_2=F_2[u]/(u^2)$，讨论了环R上循环码的结构、译码问题及类型II码的性质，环R上的纠错码理论的研究已成为一个新热点[1-7]。关于环R上的Galoisk扩环，在文献[1-3]中均有提及，但仅简单给出几个结果，且并未给出完整证明。在有限域上，Delsarte给出了一个非常有名的等式，即子域子码的对偶码是原码对偶码的迹码[8]，此结果在文献[7]中被推广到环 Z_q 上。

本文首先完整给出了环 R 的 Galois 扩环的相关理论，指出此 Galois 扩环的自同构群不同于 Z_4 环上的 Galois 扩环的自同构群(这点未见有文献提及)；定义了 Galois 扩环上的迹码的概念及子环子码的概念，得到了此 Galois 扩环上的一个码的对偶码的迹码是该环的子环子码的对偶码。

2　环 R 上的 Galois 扩环

环 R 是有唯一极大理想 $\{0,u\}$ 的局部环，R 中任意元素 λ 都可唯一表示为：$\lambda=r(\lambda)+q(\lambda)$，$r(\lambda),q(\lambda)\in F_2$。称 $\overline{\lambda}=r(\lambda)$ 为元素 λ 的二元约化，称二元多项式 $\overline{f}(x)=\sum_{i=0}^{k}\overline{a}_i x^i\in F_2[x]$ 为 $f(x)=\sum_{i=0}^{k}a_i x^i\in R[x]$ 的二元约化。若 $\overline{f}(x)$ 为 $F_2[x]$ 中不可约多项式，且 $f(x)$ 首项系数可逆，则称 $f(x)$ 为 R 上基本不可约多项式。特别地，如果 $\overline{f}(x)$ 为 $F_2[x]$ 中 m 次本原多项式，称 $f(x)$ 为 R 上 m 次基本本原多项式。

设 $h(x)\in R[x]$ 为 m 次基本不可约多项式，称剩余类环 $R[x]/(h(x))=\{a_0+a_1x+\cdots+a_{m-1}x^{m-1}+(h(x))|a_i\in R,i=0,1,\cdots,m-1\}$ 为 R 的 Galois 扩张(或 Galois 扩环)，记为 $\mathrm{GR}(R,m)$，简记为 R_m。显然有 $|R_m|=4^m$，且 R_m 的特征为 2。取 $\xi=x+(h(x))$，则 ξ 为 $h(x)$ 的一个根，并且 R_m 中元素都可唯一表示为：$a_0+a_1\xi+\cdots+a_{m-1}\xi^{m-1}$(其中：$a_i\in R$，$i=0,1,\cdots,m-1$)的形式，即 $R_m=R[\xi]$。

映射 $\varphi:R[x]\to F_2[x]$；$f(x)\mapsto\overline{f}(x)$ 为环同态映射。理想 $(h(x))$ 在 φ 下像为 $(\overline{h}(x))$，因此映射：$R[x]/(h(x))\to F_2[x]/(\overline{h}(x))$；$\sum_{i=0}^{m-1}a_ix^i+(h(x))\mapsto\sum_{i=0}^{m-1}\overline{a}_ix^i+(\overline{h}(x))$ 也是环同态映射，也记为 φ，在 φ 下 $\xi=x+(h(x))$ 的像为 $\overline{\xi}=x+(\overline{h}(x))$。故有 $\overline{\xi}$ 是 $\overline{h}(x)$ 的根。从而 $F_2[x]/(\overline{h}(x))=F_2[\overline{\xi}]$，映射 φ 可写作 φ：$R[\xi]\to F_2[\overline{\xi}]$；$\sum_{i=0}^{m-1}a_i\xi^i\mapsto\sum_{i=0}^{m-1}\overline{a}_i\overline{\xi}^i$。

2006-05-15 收到，2007-01-31 改回
国家自然科学基金(60673074)和安徽大学创新团队资助课题

于是有下面定理：

定理 1 设 $h(x)\in R[x]$ 是 m 次基本不可约多项式，剩余类环 $R_m=R[x]/(h(x))$ 是特征为 2 具有 4^m 个元素的有限环。记 $\xi=x+(h(x))$，则 $h(\xi)=0$，且 R_m 中每个元素都可表示为形式：

$$a_0+a_1\xi+\cdots+a_{m-1}\xi^{m-1},\ a_i\in R,\ i=0,1,\cdots,m-1 \tag{1}$$

即 $R_m=R[\xi]$，理想 (u) 是 $R[\xi]$ 的唯一极大理想，它是由 R_m 中所有零因子加上零元素形成。记 $\overline{\xi}=x+(\overline{h}(x))$，那么 $\overline{h}(\xi)=0$，且 $F_2[\overline{\xi}]=F_{2^m}$。

注意到不同于 Z_4 情形，环 F_2 到R的多项式提升是平凡提升[2]，类似于Galois域，可得R的Galois扩环 R_m 对于给定的正整数m是唯一的[8, 9]。

引理 1 对于 Galois 扩环 R_m，有 $R_m/(u)\cong F_{2^m}$ 且 $|R_m|=4^m$。设 $f(x)\in R[x]$，且 $\overline{f}(x)\in F_2[x]$ 有一根 $\overline{\beta}\in F_{2^m}$ 使 $\overline{f}'(\overline{\beta})\neq 0$，则存在唯一 $\alpha\in R_m$ 满足：$f(\alpha)=0$ 且 $\overline{\alpha}=\overline{\beta}$。

定理 2 (1)在 Galois 扩环 R_m 中，存在 2^m-1 阶元素 ξ，ξ 为 R 上 m 次基本不可约多项式 $h(x)$ 的根，使得 $R_m=R[\xi]$，并且 $h(x)$ 是满足：$\deg(h(x))\le m$，$h(x)\in R[x]$ 且 $h(\xi)=0$ 的唯一一个首一多项式。(2)设 $\mathbf{T}=\{0,1,\xi,\cdots,\xi^{2^m-2}\}$，那么对任意 $c\in R_m$ 都能被唯一表示为

$$c=a_0+ua_1,\ a_0,a_1\in\mathbf{T} \tag{2}$$

推论 1 设 $c\in R_m$，$c=a_0+ua_1$，$a_0,a_1\in\mathbf{T}$，当且仅当 $a_0\neq 0$ 时，c 为 R_m 中可逆元，R_m 中所有可逆元形成一个阶为 $(2^m-1)2^m$ 的乘法群，记为 R_m^*，则 $R_m^*=(\xi)\times\mathcal{E}$，其中 (ξ) 是由 ξ 生成的 2^m-1 阶循环群，$\mathcal{E}=\{1+ua_1|a_1\in\mathbf{T}\}$ 是 2^m 阶 Abelian 群。

推论 2 设 $c_1,c_2\in\mathbf{T}$，若记 $c_1+c_2=a+ub$，$a,b\in\mathbf{T}$，则 $b=0$，$a=c_1+c_2$。

定义 1[2] 称映射 $f:R_m\to R_m$；$c=a_0+ua_1\mapsto c^f=a_0^2+ua_1^2$ 为 R_m 中的Frobenius映射。

定理 3 Frobenius 映射 f 是环 R_m 的环自同构，f 固定的元素恰为 R 中全部元素，且 f 的阶为 m。

证明 由 $(2,2^m-1)=1$，循环群 (ξ) 中每一个元素都可表示为其中某个元素的平方，故 f 是满射，又 R_m 为有限环，从而 f 是双射。对任意 $c,c'\in R_m$，其中 $c=a_0+ua_1$，$c'=a_0'+ua_1'$，$a_0,a_1,a_0',a_1'\in\mathbf{T}$，根据 Frobenius 映射的定义及推论 2，易有 $(c+c')^f=c^f+c'^f$，$(cc')^f=c^f\cdot c'^f$，因此映射 f 是环 R_m 的环自同构。由于 ξ 的阶为 2^m-1 易见 f 的阶为 m。对 $a\in\mathbf{T}$，如果 $a^2=a$，那么 $a=0$ 或 1，所以 f 固定的元素恰为 0，1，u，$1+u$。 证毕

定义映射 $\sigma_i:R_m\to R_m$；$a+ub\mapsto a+u\xi^ib$，其中 $i\in\{0,1,\cdots,2^m-2\}$。

为给出环 R_m 的所有环自同构，先介绍两个引理。

引理 2 映射 σ_i 是环 R_m 的环自同构，且 $\{\sigma_i|i=0,1,\cdots,2^m-2\}$ 关于映射的复合运算构成一个 2^m-1 阶的循环群 (σ_1)。

根据定理 3 及引理 2 可得下面引理：

引理 3 映射 $\sigma_if^j:R_m\to R_m$；$a+ub\mapsto a^{2^j}+u\xi^ib^{2^j}$ 为环 R_m 的环自同构，这里 $i\in\{0,1,\cdots,2^m-2\}$，$j\in\{0,1,\cdots,m-1\}$。

定理 4 设 σ 是环 R_m 的任意一个环自同构，则存在 $i\in\{0,1,\cdots,2^m-2\}$，$j\in\{0,1,\cdots,m-1\}$，使得 $\sigma=\sigma_if^j$；从而环 R_m 的自同构群为 $(\sigma_1)\times(f)$，其阶为 $(2^m-1)m$。

证明 对 $\forall a\in\mathbf{T}$，有 $a^{2^m}-a=0$。即 $\mathbf{T}$ 中 2^m 个元素都是 $x^{2^m}-x$ 的根，而 $x^{2^m}-x$ 的根都在 R_m 中，因此有 $\mathbf{T}^{\sigma}=\mathbf{T}$。由 $0=(u^2)^\sigma=(u^\sigma)^2$，得 $u^\sigma\in(u)$，所以存在 $i\in\{0,1,\cdots,2^m-2\}$ 使得 $u^\sigma=u\xi^i$；于是对 $\forall c=a+ub$，有：$c^\sigma=a^\sigma+u\xi^ib^\sigma$。故有 σ 由其在 $\mathbf{T}$ 上的作用确定。因为 $u^\sigma\in(u)$，所以 $(u^\sigma)=(u)$，从而映射 $\overline{\sigma}:R_m/(u)\to R_m/(u)$；$\overline{c}\mapsto\overline{c^\sigma}$ 为域 $R_m/(u)$ 的自同构。可令 $\overline{\xi}^{\overline{\sigma}}=\overline{\xi}^{2^j}$，某 $j(0\le j\le m-1)$。设 $\xi^\sigma=\xi^l$，$l\in\{1,2,\cdots,2^m-2\}$，则有 $\overline{\xi^l}=\overline{\xi}^l=\overline{\xi^\sigma}=\overline{\xi}^{\overline{\sigma}}=\overline{\xi}^{2^j}$，从而 $l=2^j$。因此 $\sigma=\sigma_if^j$。 证毕

定义 2 设 σ 为环 R_m 的自同构，如果 σ 固定 R 中所有元素，称 σ 为 R_m 的 R-自同构。称 R_m 的所有 R-自同构所构成的群为环 R_m 的 Galois 自同构群，简称 Galois 群。

由定理可得下面推论：

推论 3 环 R_m 的 Galois 群为由 Frobenius 映射 f 生成的 m 阶循环群。

注 Z_4 环上的 Galois 扩环的自同构群恰为其 Galois 群[10]，但对于环 R，Galois扩环 R_m 的Galois群为其自同构群的子群。

3 Galois 扩环 R_m 上的迹码

对于环 $\mathcal{R}$（$\mathcal{R}$ 为 R 或 R_m）。称 $\mathcal{R}^n$ 的任一非空子集 C 为 $\mathcal{R}$ 上的码，n 称为码长，C 中元素称为码字。若 $C'\subseteq C$。则称 C' 为 C 的子码。对 $\forall x=(x_1,x_2,\cdots,x_n)$，$\forall y=(y_1,y_2,\cdots,y_n)\in\mathcal{R}^n$，定义 x 与 y 的加法：$x+y=(x_1+y_1,x_2+y_2,\cdots,x_n+y_n)$；$x$ 与 y 的内积：$x\cdot y=x_1y_1+x_2y_2+\cdots+x_ny_n$；如果 $x\cdot y=0$ 称 x 与 y 正交。称 $C^\perp=\{x\in R^n\mid x\cdot y=0,\forall y\in C\}$ 为 C 的对偶码。

在有限域中，有从 F_{p^m} 到 F_p 的一个迹映射 Tr，即 $\mathrm{Tr}(a)=a+a^p+a^{p^2}+\cdots+a^{p^{m-1}}$，$\forall a\in F_{p^m}$。下面将迹映射推广到环 R_m 上。

设 $a\in R_m$，由 f 的阶为 m，有 $(a+a^f+a^{f^2}+\cdots+a^{f^{m-1}})^f=a+a^f+a^{f^2}+\cdots+a^{f^{m-1}}$，由定理 3 知 $a+a^f+a^{f^2}+\cdots+a^{f^{m-1}}\in R$。因此可给出如下定义：

定义 3 称 $\mathrm{Tr}(a)=a+a^f+a^{f^2}+\cdots+a^{f^{m-1}}$（$\forall a\in R_m$）为 R_m 到 R 的迹映射。

关于迹映射直接验证可得如下性质：

性质 1 (1) $\mathrm{Tr}(c+c')=\mathrm{Tr}(c)+\mathrm{Tr}(c')$，$\forall c,c'\in R_m$；

(2) $\mathrm{Tr}(\alpha c)=\alpha\mathrm{Tr}(c)$，$\forall c\in R_m,\forall\alpha\in R$，

并且 Tr 为 R_m 到 R 的满射。

定义 4 设 C 为环 R_m 上长为 n 的线性码，称 $C\mid R=$

$\{c \in C \mid c \in R^n\}$ 为 C 关于 R 的子环子码；称 $\mathrm{Tr}(C) = \{\mathrm{Tr}(c) = (\mathrm{Tr}(c_1), \mathrm{Tr}(c_2), \cdots, \mathrm{Tr}(c_n)) \mid c = (c_1, c_2, \cdots, c_n) \in C\}$ 为 R_m^n 中线性码 C 的迹码。

定理 5　设 C 为环 R_m 上的长为 n 的线性码，则 $(C \mid R)^{\perp} = \mathrm{Tr}(C^{\perp})$。

证明　首先证 $(C \mid R)^{\perp} \supseteq \mathrm{Tr}(C^{\perp})$。事实上，对 $\forall c = (c_1, c_2, \cdots, c_n) \in C^{\perp}$ 和 $\forall a = (a_1, a_2, \cdots, a_n) \in C \mid R$，有 $a \cdot \mathrm{Tr}(c) = \sum_{i=1}^{n} a_i \mathrm{Tr}(c_i) = \mathrm{Tr}\left(\sum_{i=1}^{n} a_i c_i\right) = \mathrm{Tr}(a \cdot c) = \mathrm{Tr}(0) = 0$，从而有 $\mathrm{Tr}(c) \in (C \mid R)^{\perp}$。因此 $(C \mid R)^{\perp} \supseteq \mathrm{Tr}(C^{\perp})$。

再证 $(C \mid R)^{\perp} \subseteq \mathrm{Tr}(C^{\perp})$，等价于证明 $(\mathrm{Tr}(C^{\perp}))^{\perp} \subseteq (C \mid R)$。事实上，设 $\forall a \in (\mathrm{Tr}(C^{\perp}))^{\perp}$，$a = (a_1, a_2, \cdots, a_n)$。对 $\forall b = (b_1, b_2, \cdots, b_n) \in C^{\perp}$，有 $\lambda b \in C^{\perp}$，其中 $\forall \lambda \in \mathbf{T}$，则 $0 = a \cdot \mathrm{Tr}(\lambda b) = \sum_{i=1}^{n} a_i \mathrm{Tr}(\lambda b_i) = \mathrm{Tr}(\lambda \sum_{i=1}^{n} a_i b_i)$，再由 λ 的任意性及迹映射 Tr 是满射，必有 $\sum_{i=1}^{n} a_i b_i = 0$，即 $a \cdot b = 0$。所以 $a \in C \mid R$。　　证毕

参 考 文 献

[1] Dougherty S T, Gaborit P, and Harada M. Type II codes over F_2+uF_2. *IEEE Trans. on Info. Theory*, 1999, 45(1): 32–45.

[2] Bonnecaze A and Udaya P. Cyclic codes and self-dual codes over $F_2 + uF_2$. *IEEE Trans. on Info. Theory*, 1999, 45(4): 1250–1255.

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

[4] Dougherty S T, Gaborit P, Harada M, and Munemasa A, *et al.*. Type IV self-dual codes over rings. *IEEE Trans. on Info. Theory*, 1999, 45(7): 2345–2358.

[5] Ling S and Sole P. Duadic codes over $F_2 + uF_2$. *Applicable Algebra in Engineering, Communication and Computing*, 2001, 12(5): 365–379.

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

[7] 朱士信. 信息安全中有限环上的纠错码和序列密码研究. [博士论文], 合肥工业大学，2004.

[8] MacWilliams F J and Sloane N J A. The Theory of Error Correcting Codes. Amsterdam, the Netherlands: North-Holland, 1977: 93–154.

[9] Mcdonald B R. Finite rings with identity. New York: Marcel Dekker, 1974: 291–335.

[10] Wan Zhe-xian. Quaternary Codes. Singapore: World Scientific, 1997: 93–112.

吴　波：　男，1980年生，硕士，主要从事有限环上的纠错码理论和序列密码理论研究.

朱士信：　男，1962年生，博士，教授，主要从事有限环上的纠错码理论和序列密码理论研究.