有限非链环 $F_{p^m}+vF_{p^m}$ 上循环码的迹码和子环子码

高 健,李 娟
(山东理工大学数学与统计学院,山东淄博 255000)

摘 要: 给出了有限非链环 $F_{p^m}+vF_{p^m}$ 的 Galois 扩环相关理论,明确了有限非链环 $F_{p^m}+vF_{p^m}$ 上循环码的迹码和子环子码的生成元结构.

关键词: 有限非链环; 迹码; 子环子码
中图分类号: TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2019)01-0241-04
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.01.032

On Trace Codes and Subring Subcodes of Cyclic Codes Over Finite Non-Chain Ring $F_{p^m}+vF_{p^m}$

GAO Jian, LI Juan
(*School of Mathematics and Statistics, Shandong University of Technology, Zibo, Shandong* 255000, *China*)

Abstract: In this paper, we give some results on the Galois extension of the finite non-chain ring $F_{p^m}+vF_{p^m}$. We also determine the generators of trace codes and subring subcodes of cyclic codes over the finite non-chain ring $F_{p^m}+vF_{p^m}$.

Key words: finite non-chain ring; trace codes; subring subcodes

1 引言

有限交换环上的编码理论始于上个世纪六十年代. 1994 年 Hammons 等编码学者发现一些性能良好的二元非线性码可以看作四元有限环 Z_4 上某些循环码的二元象[1]. 从此,有限环上的编码理论成为了编码理论中的一个热点研究领域. 随着有限链环上的编码理论研究的不断深入,部分编码学者开始关注有限非链环上的编码理论的研究[2~8]. 有限非链环上编码理论的研究有助于对有限域上的编码有更清楚的认识,从而将纠错码理论应用到密码设计和网络安全等实际领域[9,10].

编码理论中子域子码是一类重要的线性码. 常见的子域子码有: Hamming 码、Goppa 码等. Delsarte 给出有限域上迹码和子域子码的关系[7]. Gao 和 Fu 利用有限域上循环码和线性移位序列的关系,给出了有限域上循环码的迹码和子域子码的生成多项式[11].

在本文中,首先我们给出了有限非链环 $F_{p^n}+vF_{p^n}$ 上循环码的一些基本结果,其次明确了该非链环上循环码的迹码和子环子码的生成元.

2 基本结果

令 $\Re=F_{p^n}+vF_{p^n}$, $R=F_p+vF_p$, 其中 $v^2=v$. 设 $a(x)\in F_p[x]$ 为 m 次基本不可约多项式,则称剩余类环 $R[x]/\langle a(x)\rangle$ 为 R 的 m 次 Galois 扩张. 显然 R 是 $\Re$ 的一个子环.

定义 1 环 $\Re$ 上的 Frobenius 映射定义为

$$f:\Re\to\Re$$
$$r=(1-v)a+vb\to f(r)=(1-v)a^p+vb^p$$

显然, f 的阶为 m, f 固定的元素恰为 R 中的元素. 易证环 $\Re$ 的 Galois 群为由 Frobenius 映射 f 生成的 m 阶循环群 $<f>$.

定义 2 $\Re$ 到 R 的迹映射定义为

$$T_r:\Re\to R$$
$$r\to T_r(r)=\sum_{\varphi\in<f>}\varphi(r)=r+f(r)+\cdots+f^{m-1}(r)$$

易知迹映射 T_r 为 $\Re$ 到 R 的满射.

定义 3 设 C 是环 $\Re$ 上码长为 n 的线性码,令

收稿日期:2017-07-25;修回日期:2018-04-21;责任编辑:孙瑶
基金项目:国家自然科学基金(No. 11701336, No. 11626144, No. 11671235)

$$T_r(C)=\{T_r(\boldsymbol{c})=(T_r(c_0),T_r(c_1)\cdots T_r(c_{n-1}))\mid \forall \boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})\in C\}$$

则称 $T_r(C)$ 为线性码 C 的迹码.

因为迹映射是 R-线性映射,因此迹码 $T_r(C)$ 是环 R 上码长为 n 的线性码.

若对线性码 C 中任意码字 $(c_0,c_1,\cdots,c_{n-1})$,有 $(c_{n-1},c_0,\cdots,c_{n-2})$ 仍是线性码 C 中的码字,则称 C 为码长为 n 的循环码. 定义从 $\Re^n$ 到 $\Re[x]/\langle x^n-1\rangle$ 的 $\Re$-模同构,$\psi(\boldsymbol{c})=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$,其中 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})$ 是 $\Re^n$ 中任意元素. 线性码 C 是 $\Re$ 上码长为 n 的循环码当且仅当 $\psi(C)$ 是 $\Re[x]/\langle x^n-1\rangle$ 的一个理想.

对于环 $\Re$ 上码长为 n 的循环码 C,它可以表示为

$$C=(1-v)C_1\oplus vC_2$$

其中 C_1 和 C_2 是有限域 F_{p^m} 上码长为 n 的循环码[6]. 令 $f(x)$ 和 $g(x)$ 分别是 C_1 和 C_2 的生成多项式,则有 $C=<(1-v)f(x)+vg(x)>$. 令 $\deg(f(x))=t_1$,$\deg(g(x))=t_2$,则 C 作为 $\Re$-子模,有极小生成元集 $S_1\cup S_2$,其中

$$S_1=\{(1-v)f(x),(1-v)xf(x),\cdots,(1-v)x^{n-t_1-1}f(x)\}$$

$$S_2=\{vg(x),vxg(x),\cdots,vx^{n-t_2-1}g(x)\}$$

定义 4 令 C 是环 $\Re$ 上码长为 n 的循环码,则称 $(C|_R)=C\cap R^n$ 为 C 的子环子码.

显然,$C|_R$ 是环 R 上码长为 n 的循环码. 由迹映射的定义,环 $\Re$ 上循环码的迹码是环 R 上的循环码. 下面我们将给出环 $\Re$ 上循环码的迹码 $T_r(C)$ 的生成元和其子环子码的具体表达.

3 循环码的迹码和子环子码

令 $\{\alpha_0,\alpha_1,\cdots,\alpha_{m-1}\}$ 是 F_{p^m} 在 F_p 上的一组基,则 $\{\alpha_0,\alpha_1,\cdots,\alpha_{m-1}\}$ 亦是 $\Re$ 在 R 上的一组基. 对于任意 $i=0,1,\cdots,m-1$,定义 $\Re^n$ 到 R^n 上的映射

$$h_i:\Re^n\to R^n$$

$$\sum_{j=0}^{m-1}\alpha_jc_j\mapsto c_i$$

其中 $c_j\in R^n$. 显然,h_i 是环 R 上的线性映射.

引理 1 令 C 是环 $\Re$ 上码长为 n 的线性码则对于 $i=0,1,\cdots,m-1$,有 $h_i(C)=T_r(C)$.

证明 令 $\{\alpha_0,\alpha_1,\cdots,\alpha_{m-1}\}$ 是 $\Re$ 在 R 上的一组基,$\{\beta_0,\beta_1,\cdots,\beta_{m-1}\}$ 是其对偶基. 故当 $i=j$ 时,$T_r(\alpha_j\beta_i)=1$,否则 $T_r(\alpha_j\beta_i)=0$. 令 $c=\sum_{i=0}^{m-1}h_i(c)\alpha_i\in C$,则对于任意的 $i=0,1,\cdots,m-1$,$j=0,1,\cdots,m-1$ 及 $c\in C$,有下面等式成立

$$\begin{aligned}T_r(\beta_jc)&=T_r(\beta_j\sum_{i=0}^{m-1}h_i(c)\alpha_i)\\&=T_r(h_0(c)\alpha_0\beta_j+\cdots+h_{m-1}(c)\alpha_{m-1}\beta_j)\\&=T_r(h_i(c))\\&=h_i(c)\end{aligned}$$

从而 $h_i(C)=T_r(C)$.

定理 1 令 C 是环 $\Re$ 上码长为 n 的循环码,$\{\alpha_0,\alpha_1,\cdots,\alpha_{m-1}\}$ 是 $\Re$ 在 R 上的一组基且 $\{\mu_0,\mu_1,\cdots,\mu_k\}$ 是码 C 的极小生成元集,则 $T_r(C)$ 的极小生成元集为 $\{h_i(\mu_j),0\leqslant i\leqslant m-1,1\leqslant j\leqslant k\}$.

证明 令 $c=\sum_{j=1}^{k}\lambda_j\mu_j\in C$,其中 $\lambda_j\in\Re$,$1\leqslant j\leqslant k$. 令 $\{\alpha_0,\alpha_1,\cdots,\alpha_{m-1}\}$ 是 $\Re$ 在 R 上的一组基,则 λ_j,μ_j 均可由该基唯一表示,即

$$\lambda_j=\sum_{r=0}^{m-1}\lambda_{jr}\alpha_r,\quad \mu_j=\sum_{s=0}^{m-1}h_s(\mu_j)\alpha_s$$

且 $\alpha_s\alpha_r=\rho_{sri}\alpha_i$,其中 $\lambda_{jr},\rho_{sri}\in R$. 于是

$$\begin{aligned}c&=\sum_{j=1}^{k}\lambda_j\mu_j\\&=\sum_{j=1}^{k}\sum_{r=0}^{m-1}\lambda_{jr}\alpha_r\mu_j\\&=\sum_{j=1}^{k}\sum_{r=0}^{m-1}\sum_{s=0}^{m-1}\lambda_{jr}h_s(\mu_j)\alpha_s\\&=\sum_{j=1}^{k}\sum_{r=0}^{m-1}\sum_{s=0}^{m-1}\sum_{i=0}^{m-1}\lambda_{jr}h_s(\mu_j)\rho_{sri}\alpha_i\end{aligned}$$

因此,对任意 $i=0,1,\cdots,m-1$ 我们有

$$h_i(c)=\sum_{j=1}^{k}\sum_{r=0}^{m-1}\sum_{s=0}^{m-1}\lambda_{jr}h_s(\mu_j)\rho_{sri}$$

综上,$\{h_i(\mu_j),0\leqslant i\leqslant m-1,1\leqslant j\leqslant k\}$ 生成 $h_i(C)$. 由引理 1,$T_r(C)$ 的极小生成元集为

$$\{h_i(\mu_j),0\leqslant i\leqslant m-1,1\leqslant j\leqslant k\}$$

推论 1 令 C 是环 $\Re$ 上码长为 n 的循环码,且

$$C=<(1-v)f(x)+vg(x)>$$

其中 $\deg(f(x))=t_1$,$\deg(g(x))=t_2$. 令

$$f(x)=f_0(x)\alpha_0+f_1(x)\alpha_1+\cdots+f_{m-1}(x)\alpha_{m-1}$$

$$g(x)=g_0(x)\alpha_0+g_1(x)\alpha_1+\cdots+g_{m-1}(x)\alpha_{m-1}$$

定义

$$F(x)=\gcd(f_0(x),f_1(x),\cdots,f_{m-1}(x))$$

$$G(x)=\gcd(g_0(x),g_1(x),\cdots,g_{m-1}(x))$$

则

$$T_r(C)=<(1-v)F(x)+vG(x)>$$

证明 令 $C=<(1-v)f(x)+vg(x)>$,其中 $\deg(f(x))=t_1$,$\deg(g(x))=t_2$,则 C 的极小生成元集 $S_1\cup S_2$,其中

$$S_1=\{(1-v)f(x),(1-v)xg(x),\cdots,(1-v)x^{n-t_1-1}f(x)\}$$

$$S_2=\{vg(x),vxg(x),\cdots,vx^{n-t_2-1}g(x)\}$$

令 $S_1\cup S_2=\{(1-v)x^{m_1}f(x),0\leqslant m_1\leqslant n-t_1-1\}\cup\{vx^{m_2}g(x),0\leqslant m_2\leqslant n-t_2-1\}$

显然
$$x^{m_1}f(x)=x^{m_1}\sum_{i=0}^{m-1}\alpha_i f_i(x)$$
$$x^{m_2}g(x)=x^{m_2}\sum_{i=0}^{m-1}\alpha_i g_i(x)$$
其中$\{\alpha_0,\alpha_1,\cdots,\alpha_{m-1}\}$是$\Re$在$R$上的一组基. 因此,由定理1,$C$的迹码$T_r(C)$的生成元集为
$$\{(1-v)x^{m_1}f_i(x)\mid 0\leqslant m_1\leqslant n-t_1-1,0\leqslant i\leqslant m_1\}$$
$$\cup\{vx^{m_2}g_i(x)\mid 0\leqslant m_2\leqslant n-t_2-1,0\leqslant i\leqslant m_1\}$$
因此
$$T_r(C)=<(1-v)F(x)>\oplus<vG(x)>$$
$$=<(1-v)F(x)+vG(x)>$$

Martínez-Moro 等给出有限链环上线性码的迹码和子环子码的关系[12],下面我们给出有限非链环$\Re$上线性码的迹码和子环子码的关系.

引理 2　令C是环$\Re$上码长为n的线性码,则$(C|_R)^{\perp}=T_r(C^{\perp})$.

证明　我们首先证明$T_r(C^{\perp})\subseteq(C|_R)^{\perp}$. 对于$C^{\perp}$中任意码字$(c_0,c_1,\cdots,c_{n-1})\in C^{\perp}$以及$C|_R$中任意码字$\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})\in C|_R$,我们有
$$aT_r(C)=\sum_{i=0}^{m-1}a_iT_r(c_i)=T_r(ac)=T_r(0)=0$$
因此,$T_r(c)\in(C|_R)^{\perp}$,故$T_r(C^{\perp})\subseteq(C|_R)^{\perp}$.

反之,我们证明$T_r(C^{\perp})\supseteq(C|_R)^{\perp}$,即$T_r(C^{\perp})^{\perp}\subseteq(C|_R)$. 对于任意$\boldsymbol{c}\in C^{\perp}$,令$\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})$,有$\lambda\boldsymbol{c}\in C^{\perp}$,其中$\lambda\in\Re$,则对于任意$\boldsymbol{b}=(b_0,b_1,\cdots,b_{n-1})\in(T_r(C^{\perp}))^{\perp}$,我们有
$$0=\boldsymbol{b}T_r(\lambda\boldsymbol{c})=\sum_{i=0}^{m-1}a_iT_r(\lambda c_i)=T_r(\lambda\sum_{i=0}^{m-1}b_ic_i)$$
因为迹映射T_r是满射,所以$\sum_{i=0}^{n-1}b_ic_i=0$. 这表明$\boldsymbol{ac}=0$. 于是$\boldsymbol{a}\in C|_R$.

由引理2,我们给出有限非链环$\Re$上码长为n的循环码的子环子码的生成元.

推论 2　令$C=<(1-v)f(x)+vg(x)>$是环$\Re$上码长为n的循环码. 令
$$\hat{f}(x)=\frac{x^n-1}{f(x)}=\sum_{i=0}^{m-1}\hat{f}_i(x)\alpha_i$$
$$\hat{g}(x)=\frac{x^n-1}{g(x)}=\sum_{i=0}^{m-1}\hat{g}_i(x)\alpha_i$$
则
$$C|_R=<(1-v)\frac{x^n-1}{\gcd(\hat{f}_0(x),\hat{f}_1(x),\cdots,\hat{f}_{m-1}(x))}+v\frac{x^n-1}{\gcd(\hat{g}_0(x),\hat{g}_1(x),\cdots,\hat{g}_{m-1}(x))}>$$

证明　由于$C=<(1-v)f(x)+vg(x)>$,则
$$C^{\perp}=<(1-v)\frac{x^n-1}{\tilde{f}(x)}+v\frac{x^n-1}{\tilde{g}(x)}>$$
其中$\tilde{f}$和$\tilde{g}$分别是$f(x)$和$g(x)$的互反多项式. 因此,由推论1和引理2,
$$C|_R=<(1-v)\frac{x^n-1}{\gcd(\hat{f}_0(x),\hat{f}_1(x),\cdots,\hat{f}_{m-1}(x))}+v\frac{x^n-1}{\gcd(\hat{g}_0(x),\hat{g}_1(x),\cdots,\hat{g}_{m-1}(x))}>$$

例 1　令$R=F_5+vF_5$,其中$v^2=v$. 设$f(x)=x^2+4x+2$是F_5上的一个2次本原多项式,则
$$\Re=R[x]/<f(x)>=F_{5^2}+vF_{5^2}$$
令$\omega=x+<f(x)>$是$f(x)$在F_{5^2}中的根且$C=<(1-v)f(x)+vg(x)>$是环$\Re$上码长为24的循环码,其中
$$f(x)=(x^2+4x+1)(x^2+3x+4)(x^2+3x+3)(x^2+4x+2)(x-\omega^9)$$
$$g(x)=(x^2+x+1)(x^2+x+2)(x^2+3)(x+2)(x-\omega^{22})$$
则
$$T_r(C)=<(1-v)(x^8+4x^7+3x^6+3x^4+4x^3+2x^2+x+4)+v(x^7+4x^6+x^5+3x^4+2x^3+2x^2+4x+2)>$$
由推论2,得
$$C|_R=<(1-v)(3+2x+3x^2+4x^3+3x^4+4x^5+4x^6+3x^7+4x^9+x^{10})+v(3+2x^2+4x^3+4x^6+x^9+3x^{10}+x^{11}+4x^{12}+3x^{13}+4x^{14}+x^{15})>$$

例 2　令$R=F_3+vF_3$,其中$v^2=v$. 设$f(x)=x^3+2x+1$是F_3上的一个3次本原多项式,则$\Re=R[x]/<f(x)>=F_{3^3}+vF_{3^3}$. 令$\omega=x+<f(x)>$是$f(x)$在$F_{3^3}$中的根. 令$C=<(1-v)f(x)+vg(x)>$是环$\Re$上码长13的循环码,其中
$$f(x)=(x^3+2x+2)(x-\omega)$$
$$g(x)=(x^3+x^2+2)$$
则
$$T_r(C)=<(1-v)(x^3+2x+2)+v(x^3+x^2+2)>$$
且
$$C|_R=<(1-v)(x^6+x^5+x^2+1)+v(x^3+x^2+2)>$$
定义从R到F_3的Gray映射$\pi(va+(1-v)b)=(a-b,a+b)$,则π是F_3-线性映射且是一个双射. $\pi(T_r(C))$是参数为[26,20,4]的三元最优线性码.

4　结论

生成元的选取对于构造有限域上的好的线性码起决定作用. 本文中,我们给出了有限非链环$F_{p^m}+vF_{p^m}$上循环码的迹码和子环子码的一些结果,明确了它们的生成元具体结构. 但未明确提出构造好的线性码的生成元形式. 虽然与有限域和有限链环相比较,有限非链环结构较复杂,且该环上循环码的代数结构不易处理,

但有限域上一些好的线性码可以由有限非链环上的循环码通过 Gray 映射进行构造,与普通的循环码进行比较,通过有限非链环构造的线性码码长更长.本文的算例指出,有限域上一些好的线性码可以由子环子码或迹码得到.因此,利用有限非链环上子环子码或迹码构造有限域上一些好的线性码是一个有趣的研究问题.另外,利用有限非链环上子环子码与迹码考虑环上的序列结构及码的覆盖半径,深度分布,也是一个值得研究的问题,它们与数据的压缩、传输等实际问题有关.

参考文献

[1] HAMMONS A, KUMAR P, CALDERBANK A, et al. The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes[J]. IEEE Transactions on Information Theory, 1994, 40(2): 301 – 319.

[2] 吴波,朱世信,李平. 环 $F_p + uF_p$ 上的 Kerdock 码和 Preparata 码[J]. 电子学报,2008,36(7):1364 – 1367.
WU Bo, ZHU Shi-xin, LI Ping. Kerdock code and Preparata code over ring $F_p + uF_p$[J]. Acta Electronica Sinica, 2008, 36(7): 1364 – 1367. (in Chinese)

[3] 施敏加,刘艳. 环 $F_p + vF_p + v^2F_p$ 上线性码的各种重量计数器及其 MacWilliams 恒等式[J]. 电子学报,2014,42(7):1387 – 1391.
SHI Min-jia, LIU Yan. Several weight enumerators of linear codes and their MacWilliams identities over ring $F_p + vF_p + v^2F_p$[J]. Acta Electronica Sinica, 2014, 42(7): 1387 – 1391. (in Chinese)

[4] GAO J. Some results on linear codes over $F_p + uF_p + u^2F_p$[J]. Journal of Applied Mathematics and Computing, 2015, 47(1): 473 – 485.

[5] 张光辉. 环 $F_p + vF_p$ 上线性码的极小支座谱[J]. 电子学报,2015,43(8):1621 – 1626.
ZHANG Guang-hui. On the minimum support hierarchy of linear codes over $F_p + vF_p$[J]. Acta Electronica Sinica, 2015, 43(8): 1621 – 1626. (in Chinese)

[6] ZHU S, WANG Y, SHI M. Some results on cyclic codes over $F_2 + vF_2$[J]. IEEE Transations on Information Theory, 2010, 56(4): 1680 – 1684.

[7] DELSARTE P. On subfield subcodes of modified Reed-Solomon codes[J]. IEEE Transations on Information Theory, 1975, 21(5): 575 – 576.

[8] 朱士信,黄磊. 环 $R + vR + v^2R$ 上线性码的 MacWilliams 恒等式[J]. 电子学报,2016,44(7):1567 – 1573.
ZHU S-X, HUANG L. Mac Williams identities of linear codes over ring $R + vR + v^2R$[J]. Acta Electronica Sinica, 2016, 44(7): 1567 – 1573. (in Chinese)

[9] WANG L, WANG Z, HUANG Q, et al. Balanced gray codes with flexible lengths[J]. IEEE Communications Letters, 2016, 20(5): 894 – 897.

[10] 宋云,李志慧,李永明. 基于极小线性码上的秘密共享方案[J]. 电子学报,2013,41(2):220 – 226.
SONG Y, LI Z-H, LI Y-M. Secret sharing schemes on minimal linear codes[J]. Acta Electronica Sinica, 2013, 41(2): 220 – 226. (in Chinese)

[11] GAO Z, FU F-W. Linear recurring sequences and subfied subcodes of cyclic codes[J]. Science China Mathematics, 2013, 56(7): 1413 – 1420.

[12] MARTÍNEZ-MORO E, NICOLÍS A P, RUA I F. On trace codes and Galois invariance over finite commutative chain rings[J]. Finite Fields and Their Applications, 2013, 22: 114 – 121.

作者简介



高 健 男,1987 年生于山东德州.博士、讲师.研究方向为编码理论及其应用.
E-mail:dezhougaojian@163.com



李 娟 女,1991 年生于山东临沂.硕士研究生.研究方向为编码理论及其应用.