第30卷第6期 电子与信息学报 Vol.30No.6
2008年6月 Journal of Electronics & Information Technology Jun. 2008

环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上一类重根常循环码

朱士信[①] 李 平[①] 吴 波[②]
[①](合肥工业大学应用数学系 合肥 230009)
[②](安徽大学数学与计算科学学院 合肥 230039)

摘 要：记 $R=F_q+uF_q+\cdots+u^{k-1}F_q$，$G=R[x]/<x^t-\alpha>$，且 λ 是 R 中可逆元。定义了从 G^n 到 R^{tn} 的新的Gray映射 ϕ，证明了 J 是 G 上长为 n 的线性的 x-常循环码当且仅当 $\phi(J)$ 是 R 上长为 tn 的线性的 α-常循环码。使用有限环理论，获得了环 R 上长为 p^e 的所有的 $(u\lambda-1)$-常循环码的结构及其码字个数。特别地，获得了环 $F_{2^m}+uF_{2^m}$ 上长为 2^e 的 $(u\lambda-1)$-常循环码的对偶码的结构及其码字个数。推广了环 Z_{2^a} 上重根负循环码的若干结果。

关键词：重根常循环码；Gray映射；极大理想；有限链环

中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2008)06-1394-03

A Class of Repeated-root Constacyclic Codes over the Ring $F_q+uF_q+\cdots+u^{k-1}F_q$

Zhu Shi-xin[①] Li Ping[①] Wu Bo[②]
[①](*Dept. of Appl. Math., Hefei University of Technology, Hefei* 230009, *China*)
[②](*School of Math. and Compu. Science, Anhui University, Hefei* 230039, *China*)

Abstract: Let $R=F_q+uF_q+\cdots+u^{k-1}F_q$, $G=R[x]/<x^t-\alpha>$, and λ be an invertible element in R. A new Gray map ϕ from G^n to R^{tn} is defined. It is proved that J is a linear x-constacyclic code of length n if and only if $\phi(J)$ is a linear α-constacyclic code over R of length tn. By means of the theory of finite rings the structure and sizes of all $(u\lambda-1)$-constacyclic codes over R of length p^e are obtained. Especially, the structure and sizes of the duals of all $(u\lambda-1)$-constacyclic codes of length 2^e over the ring $F_{2^m}+uF_{2^m}$ are also obtained. Some of the results about repeated-root negacyclic codes over the ring Z_{2^a} are generalized.

Key words: Repeated-root constacyclic codes; Gray map; Maximal ideal; Finite chain rings

1 引言

最近，编码学与密码学的爱好者对剩余类环 $F_q[u]/<u^k>=F_q+uF_q+\cdots+u^{k-1}F_q$ 产生极大的兴趣(q为素数p的方幂)。文献[1]中利用环 $F_p+uF_p=F_p[u]/<u^2>$ 上的线性码进行格的构造；文献[2]中利用环 $F_p[u]/<u^k>$ 来构造最佳跳频序列；文献[3]中研究了 $F_p[u]/<u^k>$ 上单根循环码及自对偶码的结构；文献[4]中证明了环 $F_q[u]/<u^s>$ 上所有的单根循环码皆为最大秩距离码。特别地，已有大量的文献对环 F_2+uF_2 上的码进行了研究[5−9]，文献[7]中利用线性的Gray映射构造了一批二元最优码。值得注意的是：当 $q=2,k=2,\lambda=1$ 时，本文实际上获得了环 F_2+uF_2 上长为 2^e 的所有的 $(u-1)$-常循环码及其对偶码的结构。

从上世纪70年代Massey和Van Lint等人开始研究有限域上的重根循环码[10−12]，某些情形下也获得了一些最优码。编码理论的一个突破性进展是Nechaev在1989年发现二元Kerdock-码可视为 Z_4 上的循环码，随后Hammons等五人小组在1993年通过 Z_4 上线性码的研究解决了困扰编码学家们30多年的一个问题，即非线性二元Preparata码与二元同码长Kerdock码的形式对偶问题[13, 14]。自此，Z_4 上乃至更一般的有限环上码的研究成为编码方向的一个新的热点。

最近，有限环上重根常循环码引起编码学家的兴趣，Abualrub 等在文献[15]中从生成元的角度讨论了 Z_4 上长为 2^e 的循环码的结构，Blackford分别在文献[16，17]中讨论了 Z_4 上奇偶长度(oddly even)的循环码和偶长度的负循环码的结构，Dougherty和Ling San则在文献[18]中研究了 Z_4 上任意长度的循环码。Salagean 在文献[19]中研究了有限链环上的重根循环码和重根负循环码。Dinh在文献[20]中获得了环 Z_{2^m} 上长为 2^e 的负循环码的结构，随后在文献[21]中将其推广到Galois环GR(2^a，m)上，并讨论了这些重根负循环码的汉明距离和重量分布。本文将Dinh的结果推广到剩余类环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上的一类重根常循环码，即该环上长为 p^e 的 $(u\lambda-1)$-常循环码，其中 λ 是该环中的可逆元。有关该环的结构，可参考文献[2，4]。有关有限链环的知识，可参考文献[20，22]。文献[20，22]运用相同的方法独立地给

2006-12-18收到，2007-07-23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(2006jql002zd)和合肥工业大学科研发展基金项目(061003F)资助课题

出了有限链环上单根循环码的结构。

2　主要结果

首先，通过定义 Gray 映射来研究 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上任意长度的 $(u\lambda-1)$ -常循环码。下面记 $R=F_q+uF_q+\cdots+u^{k-1}F_q$，且 $G=R[x]/<x^t-\alpha>$，其中 α 是 R 中的可逆元。设 C 是 R 上长为 t 的线性码，则 $C^{\perp}=\{(d_0,d_1,\cdots,d_{t-1})\mid c_0\cdot d_0+c_1\cdot d_1+\cdots+c_{t-1}\cdot d_{t-1}=0,\forall(c_0,c_1,\cdots,c_{t-1})\in C\}$，这里的运算为环 R 中的加法和乘法。若 $\forall(c_0,c_1,\cdots,c_{t-1})\in C$，均有 $(\alpha c_{t-1},c_0,c_1,\cdots,c_{t-2})\in C$，则 C 叫做 R 上长为 t 的线性的 α -常循环码。若将任一码字 $(c_0,c_1,\cdots,c_{t-1})$ 等同于它的多项式表示 $c_0+c_1x+\cdots+c_{t-1}x^{t-1}$，则 R 上长为 t 的线性的 α -常循环码即 G 的理想。当环 R 的特征 p 整除码长 t 时，则 α -常循环码叫做重根常循环码，否则叫做单根常循环码。记 θ 是 G 上一个不定元，则剩余类环 $G[\theta]/<\theta^n-x>$的理想即为 G 上长为 n 的线性的 x -常循环码。$\forall\ b\in G^n$，其中 $b=(b_0^{(0)}+b_0^{(1)}x+\cdots+b_0^{(t-1)}x^{t-1},b_1^{(0)}+b_1^{(1)}x+\cdots+b_1^{(t-1)}x^{t-1},\cdots,b_{n-1}^{(0)}+b_{n-1}^{(1)}x+\cdots b_{n-1}^{(t-1)}x^{t-1})$，这里 $b_i^{(j)}\in R,0\le i\le n-1,\ 0\le j\le t-1$。记 $b^{(j)}=(b_0^{(j)},b_1^{(j)},\cdots,b_{n-1}^{(j)}),0\le j\le t-1$。定义 G^n 到 R^{tn} 的 Gray 映射 ϕ 如下：$\phi\ (b)=(b^{(0)},b^{(1)},\cdots,b^{(t-1)})$，该等式右边表示 t 个 n 维行向量的连接。

K 是任意环，$\forall y\in K,\sigma_y$ 表示 K^m 中的一个 y -右循环变换，即 $\sigma_y(\alpha_0,\alpha_1,\cdots,\alpha_{m-1})=(y\alpha_{m-1},\alpha_0,\alpha_1,\cdots,\alpha_{m-2})$，$\forall(\alpha_0,\alpha_1,\cdots,\alpha_{m-1})\in K^m$。

直接经过计算，可获得下面命题：

命题 1　$\forall b\in R^n$，均有 $\phi(\sigma_x(b))=\sigma_\alpha(\phi(b))$。

定理 1　J 是 G 上长为 n 的线性的 x -常循环码当且仅当 $\phi(J)$ 是 R 上长为 tn 的线性的 α -常循环码。

证明　显然 ϕ 是线性的双射，再据命题 1：$\forall b\in J$，则 $\sigma_x(b)\in J\Leftrightarrow\phi(\sigma_x(b))\in\phi(J)\Leftrightarrow\sigma_\alpha(\phi(b))\in\phi(J)$，故定理成立。　证毕

引理 1[20]　R 是阶为 q^k 的交换环，q 是素数幂，则 R 上长为 n 的任一线性码 C 所含码字个数为 q^i，其中 $i\in\{0,1,2,\cdots,kn\}$。而且 C 的对偶码所含码字个数为 q^{kn-i}。

引理 2[20]　任一含幺有限交换环 K 若具有唯一的极大理想，且该极大理想为主理想，则 K 是有限链环。

引理 3　$x+1$ 是剩余类环 $R[X]/<x^{p^e}+1-u\lambda>$ 中的幂零元，幂零指数为 p^ek。这里 λ 是 R 中的可逆元。(约定：$f(x)+<x^{p^e}+1-u\lambda>$ 简记为 $f(x)$。)

证明　由交换环的特征公式知 $(x+1)^{p^e}=x^{p^e}+1$，而 $x^{p^e}+1=u\lambda$，$u\lambda$ 的幂零指数为 k，故引理成立。

引理 4　若 β 是含幺交换环 K 中的可逆元，而 γ 是 K 中的幂零元，则 $\beta+\gamma$ 一定是 K 中的可逆元。

证明　由于 $\beta+\gamma=\beta(1+\beta^{-1}\gamma)$，只需证 $1+\omega$ 是 K 中可逆元，其中 ω 是 K 中的幂零元。设 ω 的幂零指数是 m，则 $(1+\omega)[1-\omega+\omega^2-\omega^3+\cdots+(-1)^{m-1}\omega^{m-1}]=1$。

引理 5　$R[X]/<x^{p^e}+1-u\lambda>$ 中每个多项式 $f(x)$ 可唯一地表示成 $f(x)=\sum_{j=0}^{p^e-1}a_{0j}(x+1)^j+u\sum_{j=0}^{p^e-1}a_{1j}(x+1)^j+\cdots+u^{k-1}\sum_{j=0}^{p^e-1}a_{k-1,j}(x+1)^j$，其中 $a_{ij}\in F_q$，$0\le i\le k-1,0\le j\le p^e-1$。并且，$f(x)$ 是 $R[X]/<x^{p^e}+1-u\lambda>$ 中的可逆元当且仅当 $a_{00}\neq0$。

证明　由于 $f(x)$ 可表成 $f_0(x)+uf_1(x)+\cdots+u^{k-1}f_{k-1}(x)$ 的形式，其中 $f_i(x)\in F_q[x]$，$0\le i\le k-1$。易知引理前半部分成立。下面证后半部分：$(\Rightarrow)$ 反证法：若 $a_{00}=0$，$f(x)=(x+1)g(x)+uh(x)$，由引理 3，$x+1$ 是 $R[X]/<x^{p^e}+1-u\lambda>$ 中的幂零元，且 u 也是其中的幂零元，从而 $f(x)$ 是 $R[X]/<x^{p^e}+1-u\lambda>$ 中的幂零元，当然不是其中的可逆元。$(\Leftarrow)$：若 $a_{00}\neq0$，则 $f(x)=a_{00}+(x+1)g(x)+uh(x)$，由必要性的证明知 $(x+1)g(x)+uh(x)$ 是 $R[X]/<x^{p^e}+1-u\lambda>$ 中的幂零元，而 a_{00} 是 R 的子环 F_q 中的可逆元，且 R 与 F_q 有相同的单位元，从而 a_{00} 是 R 中的可逆元，由引理 3 的约定，a_{00} 是 $R[X]/<x^{p^e}+1-u\lambda>$ 中的可逆元。也就是说 $f(x)$ 可表为 $R[X]/<x^{p^e}+1-u\lambda>$ 中的可逆元与幂零元的和，由引理 4，$f(x)$ 是 $R[X]/<x^{p^e}+1-u\lambda>$ 中的可逆元。

评注：若 R_1 是 R_2 的子环，且皆为幺环，但单位元不同，则 R_1 中的可逆元未必是 R_2 中的可逆元，比如 $\overline{4}$ 是模 6 的剩余类环 Z_6 的理想 $<\overline{2}>$ 中的可逆元，却不是 Z_6 中的可逆元。

定理 2　环 $R[X]/<x^{p^e}+1-u\lambda>$ 具有唯一的极大理想，且该极大理想为 $<x+1>$。

证明　设 I 是 $R[X]/<x^{p^e}+1-u\lambda>$ 的任一极大理想，$\forall f(x)\in I$，由引理 5，记 $f(x)=\sum_{j=0}^{p^e-1}a_{0j}(x+1)^j+u\sum_{j=0}^{p^e-1}a_{1j}\cdot(x+1)^j+\cdots+u^{k-1}\sum_{j=0}^{p^e-1}a_{k-1,j}(x+1)^j$，其中 $a_{ij}\in F_q$，$0\le i\le k-1,0\le j\le p^e-1$。由于极大理想中不含可逆元，再由引理 5，必有 $a_{00}=0$，从而 $f(x)\in<u,x+1>$，又 $R[X]/<x^{p^e}+1-u\lambda>$ 中 $(x+1)^{p^e}=x^{p^e}+1$，而 $x^{p^e}+1=u\lambda$，从而 $u=\lambda^{-1}(x+1)^{p^e}$，也就有 $<u,x+1>=<x+1>$，故 $I\subseteq<x+1>$。又 $<x+1>\subset R[X]/<x^{p^e}+1-u\lambda>$，故 $I=<x+1>$。

定理 3　$R[X]/<x^{p^e}+1-u\lambda>$ 是个有限链环，其所有的理想(即 R 上长为 p^e 的 $(u\lambda-1)$ -常循环码)是 $<(x+1)^i>$，$i=0,1,2,\cdots,p^e\cdot k$。

证明　依次使用定理 2，引理 2 及引理 3 即可获证。

推论 1　当 $n=p^s$ 时，J 是 G 上长为 p^s 的线性的 x -常循环码当且仅当存在 $i\in\{0,1,2,\cdots,p^{e+s}\}$，使得 $\phi(J)=<(x+1)^i>$，其中 $x+1\in R[X]/<x^{p^{e+s}}+1-u\lambda>$。

证明　在定理 1 中取 $t=p^e,\alpha=u\lambda-1$，再使用定理 3 即可。

定理 4　$\forall i\in\{0,1,2,\cdots,p^e\cdot k\}$，理想 $<(x+1)^i>$ 中恰好

含有 $q^{p^e\cdot k-i}$ 个码字。

证明 $R[X]/<x^{p^e}+1-u\lambda>$ 的全部 $p^e\cdot k+1$ 个理想按集合的包含关系形成严格的升链：$<0>=<(x+1)^{p^e\cdot k}>\subset<(x+1)^{p^e\cdot k-1}>\subset\cdots\subset<x+1>\subset<(x+1)^0>=<1>$。由引理 1，这些理想所含码字的个数皆为 q 的方幂，即形如 q^i，$i\in\{0,1,2,\cdots,p^e\cdot k\}$。又 $q^0\prec q^1\prec\cdots\prec q^{p^e\cdot k}$，由对应关系，必然理想 $<(x+1)^i>$ 中恰好含有 $q^{p^e\cdot k-i}$ 个码字，$i\in\{0,1,2,\cdots,p^e\cdot k\}$。 证毕

定理 5 环 $R_0=F_{2^m}+uF_{2^m}$ 上长为 2^e 的 $(u\lambda-1)$-常循环码 $C=<(x+1)^i>$ 恰好含有 $2^{m\cdot 2^{e+1}-m\cdot i}$ 个码字；它的对偶码 $C^\perp$ 是 $R_0[X]/<x^{2^e}+1-u\lambda>$ 中理想 $<(x+1)^{2^{e+1}-i}>$，且恰好含有 $2^{m\cdot i}$ 个码字。

证明 考察定理 4 中 $p=2$ 且 $k=2$ 的情形即证得前半部分；此时，由于 $(u\lambda-1)^2=1$，可证得：环 $F_{2^m}+uF_{2^m}$ 上任一 $(u\lambda-1)$-常循环码 C 的对偶码 $C^\perp$ 仍然是 $(u\lambda-1)$-常循环码。又由于 $C=<(x+1)^i>$ 恰好含有 $2^{m\cdot 2^{e+1}-m\cdot i}$ 个码字，根据引理 1，C 的对偶码 $C^\perp$ 恰好含有 $2^{m\cdot i}$ 个码字，再据定理 4 及其证明，$C^\perp=<(x+1)^{2^{e+1}-i}>$。 证毕

推论 2 环 $F_{2^m}+uF_{2^m}$ 上长为 2^e 的自对偶的 $(u\lambda-1)$-常循环码恰好只有一个，即 $C=<u>$。(通常可称作平凡的自对偶码)

证明 由定理 5，$C=C^\perp\Rightarrow i=2^e$，而 $R[X]/<x^{2^e}+1-u\lambda>$ 中，$<(x+1)^{2^e}>=<u\lambda>=<u>$。

参 考 文 献

[1] Bachoc C. Application of coding theory to the construction of modular lattices[J]. *J. Combin. Theory Ser. A*, 1997, 78(1): 92–119.

[2] Udaya P and Siddiqi M U. Optimal large linear complexity frequency hopping patterns derived from polynomial residue rings[J]. *IEEE Trans. on Inform.Theory*, 1998, 44(4): 1492–1503.

[3] Qian J F and Zhu S X. Cyclic codes over $F_p+uF_p+\cdots+u^{k-1}F_p$ [J]. *IEICE Trans. on Fundamentals*, 2005, E88-A(3): 795–797.

[4] Ozen M and Siap I. Linear codes over $F_q[u]/<u^s>$ with respect to the Rosenbloom-Tasfasman Metric[J]. *Designs, Codes and Crypt*, 2006, 38(1): 17–29.

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

[6] 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.* 2000, 10(1): 259–271.

[7] 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.

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

[10] Massey J L and Justesen C. Polynomial weights and code constructions[J]. *IEEE Trans. on Inform.Theory*, 1973, 19(1): 101–110.

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

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

[13] Nechaev A A. Kerdock code in a cyclic form[J](in Russian). *Diskr. Math.* 1989, 1(1): 123–139.

[14] Hammons A R, Kumar P V, and Calderbank A R, *et al.*. The Z_4-linearily of Kerdock, Preparata, Goethals, and related codes[J]. *IEEE Trans. on Inform. Theory*, 1994, 40(1): 301–319.

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

[16] Blackford T. Cyclic codes over Z_4 of oddly even length [J]. *Discrete Mathematics*, 2003, 128(1): 27–46.

[17] Blackford T. Negacyclic codes over Z_4 of even length [J]. *IEEE Trans. on Inform. Theory*, 2003, 49(6): 1417–1424.

[18] Dougherty S T and Ling S. Cyclic codes over Z_4 of even length [J]. *Designs, Codes and Crypt.*, 2006, 39(1): 127–153.

[19] Salagean A. Repeated-root cyclic and negacyclic codes over a finite chain ring[J]. *Discrete Appl. Math.*, 2006, 154(2): 413–419.

[20] Dinh H Q and Lopez-Permouth S K. Cyclic and negacyclic codes over finite chain rings[J]. *IEEE Trans. on Inform. Theory*, 2004, 50(8): 1728–1744.

[21] Dinh H Q. Negacyclic codes of length 2^s over Galois rings[J]. *IEEE Trans. on Inform. Theory*, 2005, 51(12): 4252–4262.

[22] 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.
Li G S and Han W B. Cyclic codes and their Mattson- Solomn polynomials over finite chain rings[J]. *Appl. Math. J. Chinese Univ. Series A*, 2004, 19(2): 127–134.

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

李 平： 男，1971 年生，讲师，博士生，从事代数编码及非线性移位寄存器及序列的研究.

吴 波： 男，1980 年生，讲师，硕士，从事代数编码及非线性移位寄存器及序列的研究.