第44卷第3期 中国科学技术大学学报 Vol. 44,No. 3
2014年3月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Mar. 2014

文章编号:0253-2778(2014)03-0203-04

R_k 上的常循环码

宋贤梅[1,2],朱士信[2]

(1.安徽师范大学数学计算机科学学院,安徽芜湖 241003;2.合肥工业大学数学学院,安徽合肥 230009)

摘要:主要讨论了 R_k 上的常循环码.证明了 R_k 上长为 n 的 $(1+u_k)$ 循环码在 ϕ 下的像是指数为 2^{k-1} 长为 $2^k n$ 的二元拟循环码.研究了环 $R_k[x]/(x^n-(1+u_k))$,得到了当 $n=2^m$ 时,$R_{k,n}$ 是局部环,当 $n=2^m s$,$s>1$ 是奇数时,$R_{k,n}$ 不是局部环.

关键词:R_k 环;常循环码;Gray 映射

中图分类号:TN911.2 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2014.03.006

AMS Subject Classification (2000): Primary 94B05; Secondary 94B15

引用格式:Song Xianmei, Zhu Shixin. Constacyclic codes over R_k [J]. Journal of University of Science and Technology of China, 2014,44(3):203-206.
宋贤梅,朱士信. R_k 上的常循环码[J]. 中国科学技术大学学报,2014,44(3):203-206.

Constacyclic codes over R_k

SONG Xianmei[1,2], ZHU Shixin[2]

(1. *School of Mathematics and Computer Science, Anhui Normal University, Wuhu 241003, China*;
2. *School of Mathematics, Hefei University of Technology, Hefei 23009, China*)

Abstract: Constacyclic codes over R_k were mainly discussed. It was proved that the image of a $(1+u_k)$-constacyclic code of length n over R_k under ϕ is a binary quasi-cyclic of index 2^{k-1} and length $2^k n$. $R_k[x]/(x^n-(1+u_k))$ ring was studied. It was obtained that $R_{k,n}$ is local when $n=2^m$, that $R_{k,n}$ is not local when $n=2^m s$, where $s>1$ is an odd number.

Key words: R_k rings; Constacyclic codes; Gray maps

0 引言

在文献[1-2]中作者证明了高效的二元非线性 Preparate 码与 Kerdock 码可以看作是 Z_4 上线性码的二元象,由此解决了 Preparate 码与 Kerdock 码关于距离计数器具有形式对偶性这一困扰人们二十多年的疑惑.自此,有限环上的纠错码理论研究成为编码理论研究的一个热点[3-11].在这些研究中,有限链环上码的相关问题研究已得到一些好的成果[3-8].最近环 R_k 上的线性码和循环码已经被 Dougherty 等研究,且一些好的二元码已通过两种 Grap 映射像得到[10-11]. R_k 环是 $F_2+uF_2+vF_2+uvF_2$ 的推广,但 R_k 不是有限链环,因此有限链环上研究码的方法对于 R_k 环未必有效.

本文主要研究 R_k 环上的一类常循环码,即 $(1+u_k)$ 循环码,其中,$u_k^2=0$.我们证明了 R_k 上长为

收稿日期:2012-05-18;**修回日期**:2012-08-26

基金项目:国家自然科学基金(60973125,11326062),安徽省自然科学基金(1408085QA01)资助.

作者简介:宋贤梅,女,1977年生,博士/副教授.研究方向:代数学与编码. E-mail:xianmeisongahnu@163.com

通讯作者:朱士信,博士/教授. E-mail:zhushixin@hfut.edu.cn

n的$(1+u_k)$循环码在ϕ下的像是指数为2^{k-1}长为$2^k n$的二元拟循环码;研究了环$R_k[x]/(x^n-(1+u_k))$,得到了当$n=2^m$时,$R_{k,n}$是局部环,$n=2^m s$时,$R_{k,n}$不是局部环,其中$s>1$是奇数.

1 预备知识

文献[10]中环R_k的定义如下:对$k\geqslant 1$,

$$R_k = F_2[u_1, u_2, \cdots, u_k]/\langle u_i^2 = 0, u_i u_j = u_j u_i\rangle.$$

对任意子集$A\subseteq\{1,2,\cdots,k\}$,令

$$u_A = \prod_{i\in A} u_i.$$

约定$u_\emptyset=1$,于是R_k的元素可以表示成形式

$$\sum_{A\subseteq\{1,2,\cdots,k\}} c_A u_A,\ c_A \in F_2.$$

引理1.1[10] R_k是可换环且$|R_k|=2^{(2^k)}$.

引理1.2[10] R_k中元素是单位当且仅当且$u_\emptyset$的系数是1.每个单位是自身的乘法逆.

由文献[10]可知,R_k环既不是主理想环也不是链环.回忆局部环是指有唯一极大理想的环.则有如下结果:

引理1.3[10] R_k是极大理想为$\langle u_1, u_2, \cdots, u_k\rangle$的局部环.

R_k^n的非空子集称为R_k上长为n的码,R_k^n的R子模称为R_k上长为n的线性码.对单位$\lambda\in R_k$,R_k^n上的λ常循环置换是指置换

$$\tau_\lambda(c_0, c_1, \cdots, c_{n-1}) = (\lambda c_{n-1}, c_0, \cdots, c_{n-2}).$$

如果R_k上长为n的线性码C在λ常循环置换τ_λ下是不变的,则称C是λ常循环码.我们经常将码字$c=(c_0, c_1, \cdots, c_{n-1})$等同于多项式$c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$,于是环$R_k[x]/(x^n-\lambda)$中$c(x)$在$\lambda$常循环置换下对应于多项式$xc(x)$.因此$R_k$上长为$n$的$\lambda$常循环码等同于环$R_k[x]/(x^n-\lambda)$的理想.

定义$\phi_k: R_k\to R_{k-1}^2$使得$\phi_k(c)=(b, a+b)$,其中,$c=a+u_kb$, $a,b\in R_{k-1}$.易知这个映射可扩张为$\phi_k: R_k^n\to R_{k-1}^{2n}$使得

$$\phi_k(c_0, c_1, \cdots, c_{n-1}) = (b_0, b_1, \cdots, b_{n-1}, a_0+b_0, a_1+b_1, \cdots, a_{n-1}+b_{n-1}).$$

令$\phi=\phi_1\phi_2\cdots\phi_k: R_k^n\to F_2^{2^k}$,则$\phi$是$R_k$上的Gray映射.

2 Gray映射与R_k上的$(1+u_k)$循环码

引理2.1 设τ是R_k上$(1+u_k)$循环置换,σ是R_{k-1}^{2n}上循环码,则$\phi_k\tau=\sigma\phi_k$.

证明 设$c=(c_0, c_1, \cdots, c_{n-1})\in R_k^n$,令$c_i=a_i+u_kb_i$,其中,$a_i, b_i\in R_{k-1}$, $i=0,1,\cdots,n-1$.由于

$$\tau(c) = ((1+u_k)c_{n-1}, c_0, \cdots, c_{n-2}) = (a_{n-1}+u_k(a_{n-1}+b_{n-1}), a_0+u_kb_0, \cdots, a_{n-2}+u_kb_{n-2}),$$

于是有

$$\phi_k\tau(c) = (a_{n-1}+b_{n-1}, b_0, b_1, \cdots, b_{n-1}, a_0+b_0, a_1+b_1, \cdots, a_{n-2}+b_{n-2}).$$

易知

$$\sigma\phi_k(c) = (a_{n-1}+b_{n-1}, b_0, b_1, \cdots, b_{n-1}, a_0+b_0, a_1+b_1, \cdots, a_{n-2}+b_{n-2}).$$

因此$\phi_k\tau=\sigma\phi_k$. □

定理2.1 R_k上长为n的线性码C是$(1+u_k)$循环码当且仅当$\phi_k(C)$是R_{k-1}上长为$2n$的循环码.

证明 如果C是$(1+u_k)$循环码,由引理2.1知

$$\sigma(\phi_k(C)) = \phi_k(\tau(C)) = \phi_k(C)$$

成立,于是$\phi_k(C)$是R_{k-1}上长为$2n$的循环码.反过来,如果$\phi_k(C)$是R_{k-1}上长为$2n$的循环码,则

$$\phi_k(\tau(C)) = \sigma(\phi_k(C)) = \phi_k(C)$$

成立.注意到ϕ_k是单射,因此$\tau(C)=C$,即C是$(1+u_k)$循环码. □

推论2.3 R_k上长为n的$(1+u_k)$循环码在ϕ_k下的像是R_{k-1}上长为$2n$的循环码.

定理2.4 设$C=\langle f(x)+u_kg(x)\rangle$是$R_k$上长为$n$的$(1+u_k)$循环码,则$\phi_k(C)$是$R_{k-1}$上由$g(x)+x^n(f(x)+g(x))$和$f(x)+x^nf(x)$生成的.

证明 对任意$a(x), b(x)\in R_{k-1}$,

$$(a(x)+u_kb(x))(f(x)+u_kg(x)) = a(x)(f(x)+u_kg(x))+u_kb(x)f(x)$$

成立.由ϕ_k的定义可知

$$\phi_k(f(x)+u_kg(x)) = (g(x), f(x)+g(x)) = g(x)+x^n(f(x)+g(x)),$$

$$\phi_k(u_kf(x)) = (f(x), f(x)) = f(x)+x^nf(x).$$

注意到ϕ_k是线性的,于是有

$$\phi_k(a(x)+u_kb(x))(f(x)+u_kg(x)) = a(x)(g(x)+x^n(f(x)+g(x)))+b(x)(f(x)+x^nf(x)).$$

所以$\phi_k(C)$是R_{k-1}上由$g(x)+x^n(f(x)+g(x))$和$f(x)+x^ng(x)$生成的. □

设σ是循环置换,对任意正整数s,σ_s表示拟循环置换即

$$\sigma_s(a^{(1)} \mid a^{(2)} \mid \cdots \mid a^{(s)}) = (\sigma(a^{(1)}) \mid \sigma(a^{(2)}) \mid \cdots \mid \sigma(a^{(s)})).$$

指数为 s 长度为 $2ns$ 的拟循环码 C 是指 $C \subseteq (F_2^{2n})^s$ 且 $\sigma_s(C)=C$.

引理 2.4　设 τ 是 R_k^n 上 $(1+u_k)$ 循环置换，则 $\phi\tau=\sigma_{2^{k-1}}\phi$.

证明　设 $c=(c_0,c_1,\cdots,c_{n-1})\in R_k^n$，令 $c_i=a_i+u_kb_i$，其中，$a_i,b_i\in R_{k-1}$，$i=0,1,\cdots,n-1$. 于是

$$\begin{aligned}\phi\tau(c) = {} & \phi_1\phi_2\cdots\phi_k(a_{n-1}+u_k(a_{n-1}+b_{n-1}),\\ & a_0+u_kb_0,\cdots,a_{n-2}+u_kb_{n-2}) =\\ & \phi_1\phi_2\cdots\phi_{k-1}(a_{n-1}+b_{n-1},b_0,b_1,\cdots,b_{n-1},\\ & a_0+b_0,a_1+b_1,\cdots,a_{n-2}+b_{n-2}) =\\ & \phi_1\phi_2\cdots\sigma\phi_{k-1}(b_0,b_1,\cdots,b_{n-1},\\ & a_0+b_0,a_1+b_1,\cdots,a_{n-1}+b_{n-1}) =\\ & \phi_1\phi_2\cdots\sigma\phi_{k-1}\phi_k(c) =\\ & \phi_1\phi_2\cdots\sigma_2\phi_{k-2}\phi_{k-1}\phi_k(c) = \cdots =\\ & \sigma_{2^{k-1}}\phi_1\phi_2\cdots\phi_{k-1}\phi_k(c).\end{aligned}$$

所以 $\phi\tau=\sigma_{2^{k-1}}\phi$ 成立. □

定理 2.5　R_k 上长为 n 的线性码 C 是 $(1+u_k)$ 循环码当且仅当 $\phi(C)$ 是指数为 2^{k-1} 长为 2^kn 的二元拟循环码.

证明　如果 C 是 $(1+u_k)$ 循环码，由引理 2.4 有 $\sigma_{2^{k-1}}\phi(C)=\phi\tau(C)=\phi(C)$ 成立，因此有 $\phi(C)$ 是指数为 2^{k-1} 长为 2^kn 的二元拟循环码. 反过来，如果 $\phi(C)$ 是指数为 2^{k-1} 长为 2^kn 的二元拟循环码，再由引理 2.4 知 $\phi\tau(C)=\sigma_{2^{k-1}}\phi(C)=\phi(C)$ 成立. 而 ϕ 是单的，故 $\tau(C)=C$. □

推论 2.6　R_k 上长为 n 的 $(1+u_k)$ 循环码在 ϕ 下的像是指数为 2^{k-1} 长为 2^kn 的二元拟循环码.

3　环 $R_k[x]/(x^n-(1+u_k))$

命题 3.1　当 n 是奇数时，映射

$$\Psi: R_k[x]/(x^n-1)) \to R_k[x]/(x^n-(1+u_k));$$
$$f(x) \mapsto f((1+u_k)x)$$

是环同构.

证明　易知 $1+u_k$ 是 R_k 中单位，且 $(1+u_k)^2=1$. 由于 n 是奇数，于是 $(1+u_k)^n=1+u_k$. 下证

$$f(x) \equiv g(x) \bmod (x^n-1)$$

当且仅当

$$f((1+u_k)x) \equiv g((1+u_k)x) \bmod (x^n-(1+u_k)).$$

事实上，若

$$f(x) \equiv g(x) \bmod (x^n-1),$$

则

$$f(x)-g(x)=(x^n-1)q(x),$$

其中，$q(x)\in R_k[x]$. 于是

$$\begin{aligned}& f((1+u_k)x)-g((1+u_k)x) =\\ & ((1+u_k)^nx^n-1)q((1+u_k)x) =\\ & ((1+u_k)x^n-(1+u_k)^2)q((1+u_k)x) =\\ & (1+u_k)(x^n-(1+u_k))q((1+u_k)x)).\end{aligned}$$

因此

$$f((1+u_k)x) \equiv g((1+u_k)x) \bmod (x^n-(1+u_k)).$$

反过来，如果

$$f((1+u_k)x) \equiv g((1+u_k)x) \bmod (x^n-(1+u_k)),$$

则存在 $q(x)\in R_k[x]$ 使得

$$f((1+u_k)x)-g((1+u_k)x) = (x^n-(1+u_k))q(x),$$

令 $(1+u_k)x=y$，则有 $x=(1+u_k)y$，且

$$\begin{aligned}& f(y)-g(y) =\\ & ((1+u_k)^ny^n-(1+u_k))q((1+u_k)y) =\\ & ((1+u_k)(y^n-1)q((1+u_k)y).\end{aligned}$$

因此有

$$f(x) \equiv g(x) \bmod (x^n-1).$$

于是 Ψ 是单射. 对任意

$$f(x) \in R_k[x]/(x^n-(1+u_k)),$$

存在

$$f((1+u_k)x) \in R_k[x]/(x^n-(1+u_k))$$

使得

$$\Psi(f(1+u_k)x) = f((1+u_k)^2x) = f(x).$$

容易验证 Ψ 保持同态，所以 Ψ 是环同构. □

推论 3.2　当 n 是奇数时，A 是 R_k 上长为 n 的循环码当且仅当 $\Psi(A)$ 是 R_k 上长为 n 的 $(1+u_k)$ 循环码.

记 $R_{k,n}=R_k[x]/(x^n-(1+u_k))$，下面讨论 n 为何值时，环 $R_{k,n}$ 是局部环.

定理 3.3　当 $n=2^m$，m 是正整数时，$R_{k,n}$ 是局部环.

证明　只要证明环 $R_{k,n}$ 中非单位元组成的子集合是理想即可. $R_{k,n}$ 中非零元或者是单位或者是零因子. 因此 $R_{k,n}$ 中任意元与非单位元的乘积仍是非单位元. 下证两个非单位元的和仍是非单位元. 设

$$\alpha = a_0+a_1x+\cdots+a_{2^m-1}x^{2^m-1},$$
$$\beta = b_0+b_1x+\cdots+b_{2^m-1}x^{2^m-1} \in R_{k,n}$$

是非单位元. 由于 $(1+u_k)^2=1$ 且 $R_{k,n}$ 的特征为 2，于是

$$\alpha^{2^m} = a_0^{2^m} + a_1^{2^m}(1+u_k) + a_2^{2^m}(1+u_k)^2 + \cdots + a_{2^m-1}^{2^m}(1+u_k)^{2^m-1} = a_0^{2^m} + a_1^{2^m} + \cdots + a_{2^m-1}^{2^m} + u_k(a_1^{2^m} + a_3^{2^m} + \cdots + a_{2^m-1}^{2^m}),$$

$$\beta^{2^m} = b_0^{2^m} + b_1^{2^m}(1+u_k) + b_2^{2^m}(1+u_k)^2 + \cdots + b_{2^m-1}^{2^m}(1+u_k)^{2^m-1} = b_0^{2^m} + b_1^{2^m} + \cdots + b_{2^m-1}^{2^m} + u_k(b_1^{2^m} + b_3^{2^m} + \cdots + b_{2^m-1}^{2^m}),$$

且有 $(\alpha+\beta)^{2^m}=\alpha^{2^m}+\beta^{2^m}$. 利用满同态

$$\pi: R_{k,n} \to R_k;$$

$$\alpha = a_0 + a_1 x + \cdots + a_{2^m-1}x^{2^m-1} \mapsto a_0 + a_1 + \cdots + a_{2^m-1},$$

容易得到 α 是非单位当且仅当 a_i 中有偶数个为单位,$0\leqslant i\leqslant 2^m-1$. 而环 R_k 中元素 a 当 a 是单位时有 $a^2=1$,a 是非单位时有 $a^2=0$,于是 $\alpha^{2^m}+\beta^{2^m}=0$. 故$(\alpha+\beta)^{2^m}=0$,$\alpha+\beta$ 是非单位. 所以 $R_{k,n}$是局部环.

定理 3.4 当 $n=2^m s$,$R_{k,n}$不是局部环,其中 m 是正整数,$s>1$ 是奇数.

证明 注意到

$$0 = u_k^2 = (x^{2^m s}-1)^2 = (x^{2^m}-1)^2(x^{2^m(s-1)} + \cdots + x^{2^m+1})^2.$$

记

$$f_1(x) = x^{2^m(s-1)} + \cdots + x^{2^m} + 1 \in R_{k,n},$$

$$f_2(x) = x^{2^m(s-2)} + \cdots + x^{2^m} + 1 \in R_{k,n}.$$

于是 $f_1(x)$是非单位且 $f_1(x)+f_2(x)=x^{2^m(s-1)}$. 利用满同态

$$\pi: R_{k,n} \to R_k;$$

$$\alpha = a_0 + a_1 x + \cdots a_{2^m-1}x^{2^m-1} \mapsto a_0 + a_1 + \cdots a_{2^m-1},$$

有 $\pi(f_2(x))=s-1=0$,因此 $f_2(x)$是非单位. 而 $x^{2^m(s-1)}x^{2^m}=x^{2^m s}=1+u_k$ 是单位,故 $x^{2^m(s-1)}$ 是单位. 所以 $R_{k,n}$不是局部环. □

参考文献(References)

[1] Nechaev A A. Kerdock codes in cyclic form[J]. Dis Math Appl, 1991, 1(4):365-384.

[2] Hammons A R. The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes[J]. IEEE Trans Inform Theory, 1994, 40(2):301-319.

[3] Blackford T. Negacyclic codes over Z_4 of even length [J]. IEEE Trans Inform Theory, 2003, 49(6):1 417-1 424.

[4] Zhu S, Kai X. Dual and self-dual negacyclic codes of even length over Z_{2^a}[J]. Dis Math, 2009, 308:2 382-2 391.

[5] Dinh H Q. Negacyclic codes of even length 2^s over Galois rings[J]. IEEE Trans Inform Theory, 2005, 51(12):4 252-4 262.

[6] Dinh H Q, López-permauth S R. Cyclic and negacyclic codes over finite chain rings[J]. IEEE Trans Inform Theory, 2004, 50(8):1 728-1 744.

[7] Li Ping, Zhu Shixin. Cyclic codes of arbitrary lengths over the ring F_q+uF_q[J]. Journal of University of Science and Technology of China, 2008, 38(12):1 392-1 396.
李平,朱士信. 环 F_q+uF_q 上任意长度的循环码[J]. 中国科学技术大学学报, 2008, 38(12):1 392-1 396.

[8] Zhu S, Kai X. Negacyclic codes over Galois rings of characteristic 2^a[J]. Sci China Math, 2012, 55(4): 869-879.

[9] Yildiz B, Karadeniz S. Linear codes over $F_2+uF_2+vF_2+uvF_2$[J]. Des Codes Cryptogr, 2010, 54(1):61-81.

[10] Dougherth S T, Yildiz B, Karadeniz S. Codes over R_k, Gray maps and their binary images[J]. Finite Fields and Their Applications, 2011, 17:205-219.

[11] Dougherth S T, Yildiz B. Karadeniz S. Cyclic codes over R_k[J]. Des Codes Cryptogr, 2012, 63(1): 113-126.