环上 $F_{p^k}+uF_{p^k}$ 的循环码 *

梁 华[1], 唐元生[2]

(1. 淮阴师范学院 数学科学学院, 江苏 淮安 223300; 2. 扬州大学 数学科学学院, 江苏 扬州 225002)

摘 要: 利用 Gray 映射 Φ 的性质,研究了交换环 $R=F_{p^k}+uF_{p^k}$ 上任意长的循环码。其中 p 是素数,k 是一给定的正整数。证明了环 R 上长为 n 的码 C 是循环码当且仅当 $\Phi(C)$ 是 F_{p^k} 上指标为 p^k 长为 np^k 的准循环码。特别地,环 R 上长为 n 的线性循环码的 Gray 像是有限域 F_{p^k} 上指标为 p^k 长为 np^k 的线性准循环码。

关键词: 循环码; 准循环码; 格雷映射

中图分类号: O236.2;TP391 **文献标志码**: A **文章编号**: 1001-3695(2010)06-2026-02

doi:10.3969/j.issn.1001-3695.2010.06.007

Cyclic codes over ring $F_{p^k}+uF_{p^k}$

LIANG Hua[1], TANG Yuan-sheng[2]

(1. *School of Mathematical Science, Huaiyin Teachers College, Huaian Jiangsu* 223300, *China*; 2. *School of Mathematical Science, Yangzhou University, Yangzhou Jiangsu* 225002, *China*)

Abstract: Based on the property of Gray map Φ, studied cyclic codes of arbitrary length over the commutative ring $R=F_{p^k}+uF_{p^k}$, where p was a prime and $k\geq 1$ was a positive integer. Proved that a code C of length n over R was a cyclic code if and only if its Gray image was a quasi-cyclic code over F_{p^k} of index p^k and length np^k. In particular, the Gray image of a linear cyclic code of length n over R was a linear quasi-cyclic code over F_{p^k} of index p^k and length np^k.

Key words: cyclic code; quasi-cyclic code; Gray map

0 引言

随着信息产业的飞速发展,信息的传输、变换、压缩和储存等信息处理中的有效性、可靠性和安全性等问题已经成为了亟待解决的重要问题,而各种形式的编码和密码则是解决上述这些问题的基本理论和方法。

近年来,随着有限域上纠错码理论的成熟,很多从事编码理论研究的学者将研究兴趣从有限域上编码理论转移到有限环上编码理论上来。Wolfmann 在文献[1]中证明了环 Z_4 上长为 n 的线性负循环码的 Gray 像是 F_2 上长为 $2n$ 的循环码;若 n 为奇数,则环 Z_4 上长为 n 的线性循环码的 Gray 像置换等价于 F_2 上的线性循环码。文献[2]中,Ling 等人将文献[1]的结论推广至环 $Z_{p^{k+1}}$ 上。钱建发等人在文献[3]中采用同文献[1]中类似的方法研究了环 F_2+uF_2 上 $(1+u)$-循环码以及长度为奇数的循环码。文献[4]的,Amarra 等人将文献[3]的结果推广到环 $F_{p^k}+uF_{p^k}$ 上。其中 $F_{p^k}=GF(p^k)$。文献[5]则将文献[4]的结论进一步推广到有限链环上。

文献[1~5]仅讨论了相应环上码长 n 与 p 互素的循环码,而对于相应环上任意长的循环码则没有讨论。本文将文献[4]中的结论作了进一步的推广,得到了环 $F_{p^k}+uF_{p^k}$ 上的码是循环码的一个充分必要条件,这里码长 n 与 p 不必互素。

1 基本概念

设 p 为素数,k 是给定正整数。R 是指交换环 $F_{p^k}+uF_{p^k}$,其中 $F_{p^k}=GF(p^k)$,$u^2=0$。R 是有限链环,其极大理想为 uR。

下文中环 R 总是指环 $F_{p^k}+uF_{p^k}$。

定义 1 R^n 上的循环移位 σ 定义为 $\sigma(r_0,r_1,\cdots,r_{n-1})=(r_{n-1},r_0,\cdots,r_{n-2})$。

定义 2 $F_{p^k}^{np^k}$ 到 $F_{p^k}^{np^k}$ 的映射 $\tilde{\sigma}^{\otimes p^k}$ 定义为 $\tilde{\sigma}^{\otimes p^k}(a^{(1)}|a^{(2)}|\cdots|a^{(p^k)})=(\tilde{\sigma}(a^{(1)})|\tilde{\sigma}(a^{(2)})|\cdots|\tilde{\sigma}(a^{(p^k)}))$。其中:$a^{(1)},a^{(2)},\cdots,a^{(p^k)}\in F_{p^k}^n$ 而 $\tilde{\sigma}$: $F_{p^k}^n\to F_{p^k}^n$ 表示 $F_{p^k}^n$ 上的循环移位。

环 R 上长为 n 的线性码是指 R-模 R^n 的一个加法子模。若 R^n 的子集 C 满足 $\sigma(C)=C$,则称 C 为环 R 上长为 n 的循环码;若 $F_{p^k}^{np^k}$ 的子集 $\tilde{C}$ 满足 $\tilde{\sigma}^{\otimes p^k}(\tilde{C})=\tilde{C}$,则称 $\tilde{C}$ 是 F_{p^k} 上指标为 p^k 长为 np^k 的准循环码。显然,指标为 1 的准循环码是循环码。

本文中,循环码以及准循环码不必是线性码。

2 Gray 映射及其性质

集合 $\{0,1,2,\cdots,p^k-1\}$ 中任一元素 ε 都可以惟一标志为

$$\varepsilon=r_0(\varepsilon)+r_1(\varepsilon)p+\cdots+r_{k-1}(\varepsilon)p^{k-1}$$

其中:$r_0(\varepsilon),r_1(\varepsilon),\cdots,r_{k-1}(\varepsilon)\in\{0,1,2,\cdots,p-1\}$。

设 α 是 F_{p^k} 的一个本原元,则对任意的 $\varepsilon\in\{0,1,2,\cdots,p^k-1\}$,$F_{p^k}$ 中有相应的元 $\alpha_\varepsilon=r_0(\varepsilon)+r_1(\varepsilon)\alpha+\cdots+r_{k-1}(\varepsilon)\alpha^{k-1}$。

定义 3[4] 环 R^n 到 $F_{p^k}^{np^k}$ 的 Gray 映射定义为

$$\Phi(r)=(y,\alpha_1x\oplus y,\cdots,\alpha_{p^k-1}x\oplus y)$$

收稿日期: 2009-10-19; **修回日期**: 2009-12-22 **基金项目**: 国家自然科学基金资助项目(60971123);国家教育部科学技术研究重点项目(208045);东南大学移动通信国家重点实验室开放课题(W200819);江苏省自然科学基金资助项目(BK2008208)

作者简介: 梁华(1977-),男,江苏滨海人,讲师,硕士,主要研究方向为代数编码、信息安全等(lianghua@hytc.edu.cn);唐元生(1965-),男,教授,博士,主要研究方向为编码密码学、信息安全.

这里 $r=x+uy\in R^n$,$x,y\in F_{p^k}^n$,而⊕表示 F_{p^k} 和 $F_{p^k}^n$ 中元素的加法。

当 $p=2,k=1$ 时,得到 $(F_2+uF_2)^n\to F_2^{n2}$ 的 Gray 映射[3]。

根据定义 3,容易得到如下命题:

命题 1　设 $r,r'\in R^n$,则有

a) $\Phi(r+r')=\Phi(r)\oplus\Phi(r')$;

b) $\Phi(\beta r)=\beta\Phi(r)$。其中 $\beta\in F_{p^k}$。

从现在起,用 $(l)_n$ 表示 l 模 n 的最小非负剩余,这里 $l\in Z$。

集合 $\{0,1,\cdots,np^k-1\}(\subset Z)$ 中任一元素 N 均可惟一标志成 $N=\varepsilon n+j$。其中 $j=(N)_n$,$\varepsilon\in\{0,1,2,\cdots,p^k-1\}$。

命题 2　$\Phi\sigma=\tilde{\sigma}^{\otimes p^k}\Phi$。

证明　设 $r=(r_0,\cdots,r_{n-1})=x+uy\in R^n$。

其中 $x=(x_0,\cdots,x_{n-1}),y=(y_0,\cdots,y_{n-1})\in F_{p^k}^n$。

设 $\Phi(r)=(a_0,a_1,\cdots,a_{np^k-1})$,对任意的 $N=\varepsilon n+j\in\{0,1,\cdots,np^k-1\}\subset Z$。其中 $j=(N)_n$,$\varepsilon\in\{0,1,2,\cdots,p^k-1\}$。根据定义 3 和 2 得

$$a_N=a_{\varepsilon n+j}=\Big(\sum_{i=0}^{k-1}r_i(\varepsilon)\alpha^i\Big)x_j\oplus y_j$$

$$\tilde{\sigma}^{\otimes p^k}(\Phi(r))=(\tilde{\sigma}(a_0,a_1,\cdots,a_{n-1})\,|\,\tilde{\sigma}(a_n,a_{n+1},\cdots,a_{2n-1})\,|\cdots|\,\tilde{\sigma}(a_{n(p^k-1)},a_{n(p^k-1)+1},\cdots,a_{np^k-1}))=(a_{n-1},a_0,\cdots,a_{n-2}\,|\,a_{2n-1},a_n,\cdots,a_{2n-2}\,|\cdots|\,a_{np^k-1},a_{n(p^k-1)},\cdots,a_{np^k-2})$$

另一方面,设 $\Phi(\sigma(r))=\Phi(r_{n-1},r_0,\cdots,r_{n-2})=(b_0,b_1,\cdots,b_{np^k-1})$。由定义 3 得

$$b_N=\begin{cases}\Big(\sum_{i=0}^{k-1}r_i(\varepsilon)\alpha^i\Big)x_{n-1}\oplus y_{n-1},&j=0\\ \Big(\sum_{i=0}^{k-1}r_i(\varepsilon)\alpha^i\Big)x_{j-1}\oplus y_{j-1},&j\geq 1\end{cases}=$$

$$\begin{cases}a_{\varepsilon n+(n-1)}=a_{N+n-1},&j=0\\ a_{\varepsilon n+(j-1)}=a_{N-1},&j\geq 1\end{cases}$$

故有 $\tilde{\sigma}^{\otimes p^k}(\Phi(r))=\Phi\sigma(r)$,命题得证。

3　环 R 上循环码的 Gray 像

定理 1　环 R 上长为 n 的码 C 是循环码当且仅当它的 Gray 像 $\Phi(C)$ 是有限域 F_{p^k} 上指标为 p^k 长为 np^k 的准循环码。

证明　必要性。设 C 为环 R 上长为 n 的循环码,则有 $\Phi(C)=C$。由命题 2 得

$$\tilde{\sigma}^{\otimes p^k}(\Phi(C))=\Phi(\sigma(C))=\Phi(C)$$

故 $\Phi(C)$ 是有限域 F_{p^k} 上指标为 p^k 长为 np^k 的准循环码。

充分性。设 $\Phi(C)$ 是有限域 F_{p^k} 上指标为 p^k 长为 np^k 的准循环码,由命题 2 得

$$\Phi(\sigma(C))=\tilde{\sigma}^{\otimes p^k}(\Phi(C))=\Phi(C)$$

又 Φ 是单射,故有 $\Phi(C)=C$,即 C 为环 R 上长为 n 的循环码。

推论 1　环 R 上长为 n 的线性循环码的 Gray 像是有限域 F_{p^k} 上指标为 p^k 长为 np^k 的线性准循环码。

证明　设 C 为环 R 上长为 n 的线性循环码,则由定理 1 得,$\Phi(C)$ 是 F_{p^k} 上指标为 p^k 长为 np^k 的准循环码。

再由命题 1 知,$\Phi(C)$ 是有限域 F_{p^k} 上指标为 p^k 长为 np^k 的线性准循环码。

4　结束语

本文刻画了环 R 上循环码的 Gray 像的特征,解决了文献[3]和[5]的 conclusion 中提出的问题。本文结果可以推广到有限链环文献[5]中去,这将有助于进一步研究有限链环上的循环码。

参考文献:

[1] WOLFMANN J. Negacyclic and cyclic codes over Z_4[J]. IEEE Trans on Information Theory,1999,45(7):2527-2532.

[2] LING S, BLACKFORD J. Z_{pk+1}-linear codes[J]. IEEE Trans on Information Theory,2002,48(9):2592-2605.

[3] QIAN Jian-fa, ZHANG Li-na, ZHU Shi-xin. $(1+u)$-cyclic and cyclic codes over F_2+uF_2[J]. Applied Mathematics Letters,2006,19:820-823.

[4] AMARRA M C V, NEMENZO F R. On $(1-u)$-cyclic codes over $F_{pk}+uF_2$[J]. Applied Mathematics Letters,2008,21(11):1129-1133.

[5] QIAN Jian-fa, MA Wen-ping. Constacyclic and cyclic codes over finite chain rings[J]. Journal of China Universities of Posts and Telecommunications,2009,16(3):122-125.

(上接第 2025 页)了一种新算法——分合粒子群优化算法,它克服了算法出现早熟现象,提高了算法全局搜索能力。严格地讲,该算法是一种新的范式,目前笔者在国内外文献中还没有发现。该范式可以与任何一种智能算法结合,从理论和实际上来讲都有很大的探索空间,但本文只局限于实验阶段,缺乏理论的研究,这些是笔者未来努力的方向。

参考文献:

[1] KENNEDY J, EBERHART R C. Particle swarm optimization[C]// Proc of IEEE International Conference on Neural Networks. Piscataway:IEEE Press,1995:1942-1948.

[2] LOVBJERG M, RASMUSSEN T K, KRINK T. Hybrid particle swarm optimizer with breeding and subpopulations[C]//Proc of the 3rd Genetic and Evolutionary Computation Conference. San Francisco:[s.n.],2001:469-476.

[3] HU Wang, LI Zhi-shu. A simpler and more effective particle swarm optimization algorithm[J]. Journal of Software,2007,18(4):861-868.

[4] SHI Yu-hui, EBERHART R C. Fuzzy adaptive particle swarm optimization[C]//Proc of Congress on Evolutionary Computation. Piscataway:IEEE Press,2001:101-106.

[5] ANGELINE P J. Evolutionary optimization versus particle swarm optimization:philosophy and performance differences[C]//Proc of the 7th Annual Conference on Evolutionary Programming. Berlin:Springer-Verlag,1998:601-610.

[6] LV Zhen-su, HOU Zhi-rong. Particle swarm optimization with adaptive mutation[J]. Acta Electronica Sinica,2004,32(3):416-420.

[7] van den BERGH F, ENGELBRECHT A P. Cooperative learning in neural networks using particle swarm optimizers[J]. South African Computer Journal,2000,26(11):84-90.

[8] RATNAWEERA A, HALGAMUGE S K, WATSON H C. Self-organizing hierarchical particle swarm optimizer with time-varying acceleration coefficients[J]. IEEE Trans on Evolutionary Computation,2004,8(3):240-255.

[9] SHARMA K D, CHATTERJEE A, RAKSHIT A A. A hybrid approach for design of stable adaptive fuzzy controllers employing lyapunov theory and particle swarm optimization[J]. IEEE Trans on Fuzzy Systems,2009,17(2):329-341.