Galois 环上循环码新的表示

张莉娜
ZHANG Li-na

安徽理工大学 数理系,安徽 淮南 232001
Department of Mathematics,Anhui University of Science and Technology,Huainan,Anhui 232001,China
E-mail:lnzhang@aust.edu.cn

ZHANG Li-na.New description of cyclic codes over galois rings.Computer Engineering and Applications,2010,46(2):104-105.

Abstract: Galois rings may be of interesting in coding theory,which have already been studied by many coding theorists.In this paper,discrete Fourier transform and MS polynomial are defined for cyclic codes over Galois rings.A new description of cyclic codes over Galois rings is given.

Key words: cyclic code;Galois rings;Discrete Fourier Transform(DFT)

摘 要:近年来,在编码理论中,Galois 环上码的研究成为编码理论工作者研究的一个热点。定义了 Galois 环上循环码的离散傅里叶变换及 Mattson-Solomon(MS)多项式,证明了 Galois 环上的循环码同构于 Galois 环的 Galois 扩张的理想。

关键词:循环码;Galois 环;离散傅里叶变换
DOI:10.3778/j.issn.1002-8331.2010.02.032 **文章编号**:1002-8331(2010)02-0104-02 **文献标识码**:A **中图分类号**:O236.2

1 引言

循环码是一类最重要的纠错码,目前利用纠错码降低各类数字通信系统以及计算机存贮和运算系统中的误码率,提高通信质量,延长计算机无故障运行时间等,都有着非常重要的作用。

Hammons 等人在文献[1]中,通过对 Z_4 环上线性码的 Gray 映射的定义,得到了非常著名的非线性二元 Kerdock 码和 Delsarte-Goethals 码。而且还解决了在编码理论中一个古老而公开的问题,即证明了非线性二元 Kerdock 码和 Preparata 码满足 MacWilliams 等式关系。这些发现导致了近年来环上码的研究成为编码理论学家研究的一个热点。

在文[2]中,Abualrub 等人研究了 Z_4 环上的循环码及其离散傅里叶变换。在文[3]中,Dougherty 等人将这一结果推广到 Z_{p^i} 环上。该文,研究 Galois 环上的循环码,即定义循环码的离散傅里叶变换及 Mattson-Solomon(MS)多项式,给出 Galois 环上循环码另一种表示方式。

2 基本概念

令 p 是任意素数,e,m 是正整数。特征为 p^e,元素个数为 p^{em} 的 Galois 环 $R=GR(p^e,m)$ 是指剩余类环 $Z_{p^e}[x]/(h(x))$,这里 $h(x)$ 是 $Z_{p^e}[x]$ 上次数为 m 的首一多项式,它在模 p 的映射像是 $F_p[x]$ 上不可约多项式。R 是一个局部的主理想环,它的理想为 p^iR,$i=0,1,\cdots,e$,pR 为其最大的理想,$R\backslash pR$ 的元素为其单位。当 $m=1$ 时,即 $R=GR(p^e,m)$ 为整数环 Z_{p^e},当 $e=1$ 时,$R=GR(p^e,m)$ 即为有限域 F_{p^m}。

定义 1 R 上长度为 n 的线性码 C 称为循环码,是指如果 $c=(c_0,c_1,\cdots,c_{n-1})\in C$,那么 c 循环移位得到的 $c'=(c_1,c_2,\cdots,c_{n-1},c_0)\in C$。

令 $R[x]$ 为 R 的环多项式,通过模 p 从 R 到 F_p 有自然同态 φ,把这个映射自然地扩展至 $R[x]$ 到 $F_p[x]$,仍用 φ 表示。

定义 2 设首项系数为 1 的多项式 $h(x)\in R[x]$,如果 $\varphi(h(x))$ 为 F_p 上不可约多项式,则称 $h(x)$ 为 $R[x]$ 上基本不可约多项式。

设 $h(x)$ 是 R 上首项系数为 1 的 s 次基本不可约多项式,则 R 的维数为 s 的 Galois 扩张表示为 $GR(R,s)=R[x]/(h(x))$。

类似于 Galois 域,$GR(R,s)$ 是由 s 唯一决定的,$GR(R,s)$ 的单位群记为 $GR^*(R,s)$,则 $GR^*(R,s)=G_C\times G_A$,其中 G_C 是阶为 $p^{ms}-1$ 的循环群,而 G_A 是阶为 $p^{(e-1)ms}$ 的 Ablian 群。

设 $\xi\in GR(R,s)$ 是本原的 $p^{ms}-1$ 次单位根,$T=\{0,1,\xi,\cdots,\xi^{p^{ms}-2}\}$,那么 $GR(R,s)$ 中任何元素 α 能唯一表示为:

$\alpha=\alpha_0+\xi\alpha_1+\cdots+\xi^{s-1}\alpha_{s-1}$,其中 $\alpha_i\in T$

定义 Frobenius 映射 f 如下:

$f(\alpha)=\alpha_0+\alpha_1\xi^p+\cdots+\xi^{(s-1)p}\alpha_{s-1}$

由有限环理论[4]可知,$GR(R,r)$ 的 Galois 自同构群是由 f 生成的次数为 s 的循环群。

基金项目:安徽省教育厅自然科学基金项目(No.KJ2008B241)。
作者简介:张莉娜(1977-),女,讲师,主要研究领域为信息安全、编码密码学。
收稿日期:2008-07-24 **修回日期**:2008-10-20

3 主要结论

选择正整数 s,使得 F_{p^s} 包含 n 次本原单位根,则 $GR(R,s)$ 中也包含 n 次本原单位根 δ。

定义 3 p 模 n 的分圆陪集是指集合 $cl_p(i,n)=\{i,ip,\cdots,ip^{m_i-1}\}$,其中 m_i 为使 $ip^{m_i}\equiv i(\mathrm{mod}\ n)$ 成立的最小正整数。

记 $m_i=|cl_p(i,n)|$,I 为 p 模 n 的分圆陪集代表的完全集合。

定义 4 设 $c=(c_0,c_1,\cdots,c_{n-1})\in R^n$,定义 c 的离散傅里叶变换为向量

$(C_0,C_1,\cdots,C_{n-1})\in GR(R,s)^n$,其中 $C_i=c(\delta^i)=\sum_{i=0}^{n-1}c_j\delta^{ij}$

定义 c 的 Mattson-Solomon(MS)多项式为 $C(Z)=\sum_{i=0}^{n-1}C_{n-i}Z^i$。

容易验证,$C_i\in GR(R,m_i)$,且对 i 有 $C_{ip}=C_i^f$。

定理 1(反转公式) 如果 $c=(c_0,c_1,\cdots,c_{n-1})\in R^n$ 的 MS 多项式为 $C(Z)$,那么 $c_t=\frac{1}{n}C(\delta^t)$,其中 $0\leqslant t\leqslant n-1$。

证明 对于 $0\leqslant t\leqslant n-1$

$$C(\delta^t)=\sum_{i=0}^{n-1}c(\delta^{-i})\delta^{it}=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}c_j\delta^{i(t-j)}=\sum_{j=0}^{n-1}c_j\sum_{i=0}^{n-1}\delta^{i(t-j)}=nc_t$$

故定理得证。

引理 1 如果 $a(x),b(x)\in R[x]/(x^n-1)$,$A(Z),B(Z)$ 分别为它们的 MS 多项式,那么有:

(1)$a(x)+b(x)$ 的 MS 多项式为 $A(Z)+B(Z)$。

(2)$a(x)b(x)(\mathrm{mod}\ x^n-1)$ 的 MS 多项式为 $A(Z)*B(Z)=\sum A_iB_iZ^i$

(* 记为多项式的卷积运算)。

证明 由定义 4 可知,结论显然成立。

令 A 为所有变换向量 $(C_0,C_1,\cdots,C_{n-1})\in GR(R,s)^n$ 的集合,且对所有的 i,有 $C_{ip}=C_i^f$。在 A 中定义对加法和乘法的卷积运算,使其成为一个环,那么可直接验证:

$A\cong\oplus_{i\in I}GR(R,m_i)$

则有下面定理:

定理 2 映射 $\gamma:R[x]/(x^n-1)\to A$ 是环同构,其中 $\gamma(c(x))=(C_0,C_1,\cdots,C_{n-1})$。

证明 由引理 1 及反转公式知,γ 是环同态。下证 γ 是单射,如果 $\gamma(c(x))=0$,那么由反转公式可知

$\sum_{j=0}^{n-1}c_j\delta^{ij}=0$,则由该式可得 $c(x)=0$,即 γ 是单射。故定理得证。

由定理 2,显然有下面推论:

推论 1 映射 $\gamma:R[x]/(x^n-1)\to\oplus_{i\in I}GR(R,m_i)$ 是环同构。

推论 2 如果 C 是环 R 上长度为 n 的循环码,那么 C 同构于 $\oplus_{i\in I}C_i$,其中对 $i\in I$,C_i 是 $GR(R,m_i)$ 的理想。

4 结束语

目前,对环上的循环码的研究是一个新的课题,如何设计出快速,简单,经济和译码错误概率小的译码方法,是纠错码或循环码是否实用的关键,也是环上码研究的一个新的方向。

参考文献:

[1] Hammons A R,Kumar P V,Calderbank A R,et al.The Z_4-linearity of kerdock,preparata,goethals,and related codes[J].IEEE Trans Inform Theory,1994,40(3):301-319.

[2] Abualrub T,Oehmke R.On the generators of Z_4 cyclic codes of length 2^e[J].IEEE Trans Inform Theory,2003,49(9):2126-2133.

[3] Dougherty S T,Park Y H.On modular cyclic codes[J].Finite Fields and Their Applications,2007,13:31-57.

[4] McDonald B R.Finite rings with identity,pure and applied mathematics[M].New York:Marcel Dekker,1974.

[5] MacWilliams F J,Sloane N J A.The theory of error correcting codes[J].Amsterdam,The Netherlands:North-Holland,1977.

(上接 78 页)

参考文献:

[1] 刘郁恒,陈广文,胡严,等.一种在接收端实现的 TCP-Friendly 拥塞控制机制[J].电子学报,2005,33(5):835-841.

[2] 孙丹丹,李新,苗建松,等.基于时延和跳数的 Ad hoc 网络流量分配算法[J].吉林大学学报:工学版,2007,37(4):881-884.

[3] Hu N N,Steenkiste P.Evaluation and characterization of available bandwidth probing techniques[J].IEEE Journal on Selected Areas in Communications,2003,21(6):879-894.

[4] 卢利琼,陈元琰,吴东,等.高带宽时延乘积网络中的拥塞控制端算法研究[J].计算机应用研究,2006(3):8-10.

[5] 卞静,王泽强,张光昭,等.基于时延的分层多播拥塞控制协议设计[J].通信学报,2007,28(5):55-60.

[6] 姚兰,曾锋,王东.一种满足时延和时延抖动约束的多播路由算法[J].计算机工程与应用,2006,42(17):132-135.

[7] 黎文伟,张大方,曾彬.基于仿真分析的端到端最小包时延测量方法[J].计算机应用,2007,27(6):1304-1309.

[8] 李仁发,莫铁强,刘钰锋,等.随机早期诊断(RED)队列管理算法的改进研究[J].小型微型计算机系统,2003,24(3):491-494.

[9] 文宏,朱培栋,唐玉华.随机早期检测主动队列管理算法的改进研究[J].计算机工程与设计,2005,26(10):2572-2575.

[10] 王辉,李津生,洪佩琳.一种基于循环队列的分布式公平队列调度算法[J].电子与信息学报,2004,26(10):1540-1547.

[11] 扈红超,伊鹏,郭云飞,等.一种公平服务的动态轮询调度算法[J].软件学报,2008,19(7):1856-1864.

[12] 杨帆,刘增基,邱智亮,等.一种具有低时延的分组公平循环调度[J].电子与信息学报,2007,29(4):785-788.

[13] Faber T.ACC:Using active networking to enhance feedback congestion control mechanisms[J].IEEE Network,1998,12(3):61-65.

[14] Sisalem D,Wolisz A.MLDA:A TCP-friendly congestion control framework for heterogeneous multicast environments[C]//8th International Workshop on Quality of Service(IWQoS 2000),Pittsburgh,PA,June 2000.

[15] Papagiannaki K,Moon S,Fraleigh C.Measurement and analysis of single-hop delay on all IP backbone network[J].IEEE Journal on Selected Areas in Communications,2003,21(6):908-921.

[16] Gruber F,Karrenberg D.Providing active measurements as a regular service for ISP'S[C]//Proc of the Passive and Active Measurement Workshop 2001(PAM 2001).Amsterdam:RIPE NCC,2001:51-62.

[17] Jain M,Dovorlis C.End-to-end available bandwidth:Measurement methodology,dynamics,and relation with TCP throughput[J].IEEE/ACM Transactions on Networking,2003,11(4):537-549.