应用数学学报
Acta Mathematicae Applicatae Sinica (Chinese Series)

ISSN 0254-3079
CN 11-2040/O1

应用数学学报 英文版

Galois环上极大周期序列的平移等价

张晓磊[1,2,3], 胡磊[1]

1. 中国科学院信息工程研究所 信息安全国家重点实验室, 北京, 100093;
2. 广州大学数学与信息科学学院, 广州, 510006;
3. 数学与交叉科学广东普通高校重点实验室(广州大学), 广州, 510006

The Shift Equivalent of Maximal Period Sequences Over a Galois Ring

ZHANG Xiaolei[1,2,3], Hu Lei[1]

1. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093;
2. College of Mathematical and Information Sciences, Guangzhou University, Guangzhou, 510006;
3. Key Laboratory of Mathematics and Interdisciplinary Sciences of Guangdong Higher Education Institutes, Guangzhou University, GuangZhou, 510006

- 摘要
- 参考文献
- 相关文章

全文: PDF (339 KB) HTML (1 KB) 输出: BibTeX | EndNote (RIS) 背景资料

摘要 本文给出了Galois环上两个具有相同特征多项式的极大周期序列是否平移等价的一个判定方法, 以及在两个序列平移等价的情况下, 利用模p 方幂提升技术, 给出了一个计算它们的平移距离的方法.

关键词: Galois 环 极大周期序列 平移等价

Abstract: In this paper, we study the condition of shift equivalence of two maximal periodic sequences which have the same characteristic polynomial over a Galois rings, and give an algorithm to decide the shift distance between these two sequences when they are shift equivalent.

Key words: Galois ring maximal periodic sequence shift equivalence

收稿日期: 2011-08-22;

基金资助:国家973计划(2013CB834203);国家自然科学基金(61070172,10990011)资助项目

服务
- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- E-mail Alert
- RSS

作者相关文章
- 张晓磊
- 胡磊

引用本文:

张晓磊,胡磊. Galois环上极大周期序列的平移等价[J]. 应用数学学报, 2013, 36(4): 646-655.

ZHANG Xiaolei,Hu Lei. The Shift Equivalent of Maximal Period Sequences Over a Galois Ring[J]. Acta Mathematicae Applicatae Sinica, 2013, 36(4): 646-655.

[1] Calderbank A R, Sloane J A. Modular and p-adic Cyclic Codes. *Designs, Codes and Cryptography*, 1995, 6: 21-35

[2] Interlando J C, Palazzo R, Elia M. On the Decoding of Reed-Solomon and BCH Codes Over Integer Residues Rings. *IEEE Trans. of Information Theory*, 1997, 43(3): 1013-1021

[3] Boztas S, Hammons R, Kumar P V. 4-phase Sequences with Near Optimal Correlation Properties. *IEEE Trans. of Information Theory*, 1991, 37(3): 1101-1113

[4] Kumar P V, Helleseth T, Calderbank A R, Hammons R. Large Families of Quaternary Sequences with Low Correlation. *IEEE Trans. of Information Theory*, 1996, 42(3): 579-592

[5] Udaya P, Siddiqi M. U, Optimal Biphase Sequences with Large Linear Complexities Derived form ML-Sequences over Z_4. *IEEE Trans. of Information Theory*, 1996, 42(1): 206-216

[6] Dai Z D. Binary Sequences Derived form ML-sequences over Rings I: Periods and Minimal Polynomials. *J. of Cryptology*, 1992, 5: 193-207

[7] Dai Z D, Huang M Q. Criteria of Primitive Integral Polynomials Module 2^e. *Chinese Science Bulletin*, 1990, 35(15): 1128-1130

[8] Huang M Q. Maximal Periodic Polynomials over $Z/(p^d)$. *Science in China* (Series A), 1992, 35(3): 270-275

[9] 祝跃飞. Galois 环上本原多项式的一个判别准则. 数学学报, 1996, 39(6): 783-788 (Zhu Y F. A Criterion for Primitive Polynomials over Galois Rings. *Acta Mathematica Sinica* (Chinese Series), 1996, 39(6): 783-788)

[10] Wan Z X. Lectures on Finite Fields and Galois Rings. Beijing: World Publishing Corporation, 2006

[11] McDonald B. R. Finite Rings With Identity. New York: Deek, 1974

[12] 戚文峰, 戴宗铎. 环$Z/(p^d)$ 上序列的迹表示及前馈序列空间结构分析. 应用数学学报, 1997, 20(1): 128-136 (Qi W F, Dai Z D. The Trace-representation of Sequences and the Space of Nonlinear Filtered Sequences over $Z/(p^d)$. *Acat Mathematicae Applicatae Sinica*, 1997, 20(1): 128-136)

[13] Menezes A J, Orschot P G, Vanstone S A. Handbook of Applied Cryptography. Bota Raton: CRC Press, 1996

没有找到本文相关文献