计算机工程与应用　2009 45 (35): 114-119　ISSN: 1002-8331　CN: 11-2127/TP

网络、通信、安全

扩展在上*GF*（3）新型自缩序列模型及研究

王锦玲，陈亚华，兰娟丽

郑州大学 数学系，郑州 450001

收稿日期 2008-7-9　修回日期 2008-10-23　网络版发布日期 2009-12-16　接受日期

摘要　自收缩序列是一类重要的伪随机序列，而周期和线性复杂度是序列伪随机性的经典量度。如何构造自缩序列的新模型，使生成序列具有大的周期和高的线性复杂度是一个重要的问题。针对这一问题，构造了*GF*（3）上一种新型的自缩序列模型，利用有限域理论，研究了生成序列的周期和线性复杂度，得到一些主要结论：周期上界3^n，下界$3^{2[n/3]}$；线性复杂度上界3^n，下界$3^{2[n/3]-1}$。进一步讨论了基于*GF*（3）上本原三项式和四项式的自缩序列的周期和线性复杂度。

关键词　自缩序列　周期　线性复杂度　本原三项式　本原四项式

分类号　TN918.4

New model and studying of self-shrinking sequence developed on *GF*（3）

WANG Jin-ling，CHEN Ya-hua，LAN Juan-li

Department of Mathematics，Zhengzhou University，Zhengzhou 450001，China

Abstract

Self-shrinking sequence is an important kind of pseudo-random sequences.Period and linear complexity are classic measures of pseudo-random sequences.So，it becomes an important issue to construct new models of self-shrinking sequence that could generate sequences with great period and high linear complexity.In view of this question，a new model of self-shrinking sequence over *GF*（3） is constructed.After the study of the period and linear complexity of the generated sequence using the theory of finite fields，there are some main conclusions：The upper bound of the period is $3n$，the lower bound is $3^{2[n/3]}$；The upper bound of linear complexity is 3^n，the lower bound is $3^{2[n/3]-1}$.Moreover，the period and linear complexity of the generated sequence based on primitive trinomials and quarternomials of degree *n* over *GF*（3） are discussed.

Key words　self-shrinking sequence　period　linear complexity　primitive trinomials　primitive quarternomials

DOI:　10.3778/j.issn.1002-8331.2009.35.035

扩展功能

本文信息

Supporting info

PDF(672KB)

[HTML全文](0KB)

参考文献

服务与反馈

把本文推荐给朋友

加入我的书架

加入引用管理器

复制索引

Email Alert

文章反馈

浏览反馈信息

相关信息

本刊中 包含“自缩序列”的相关文章

本文作者相关文章

- 王锦玲
- 陈亚华
- 兰娟丽

通讯作者　王锦玲 wang63227@sohu.com