第37卷 第19期 计 算 机 工 程 2011年10月
Vol.37 No.19 Computer Engineering October 2011

·安全技术· 文章编号：1000—3428(2011)19—0133—02 文献标识码：A 中图分类号：TP301.6

GF(3)上新一类广义自缩序列的伪随机性

王锦玲，崔雪晴

(郑州大学数学系，郑州 450001)

摘 要：提出GF(3)上新一类广义自缩序列。分析游程分布情况，得到在序列 b 连续 $2\times3^{n-1}$ 个符号中，1长1游程、1长2游程、1长0游程、k 长1游程($2\leqslant k\leqslant(n-6)/2$)的数目所在范围，通过 n=8 时的实例验证定理1~定理3的正确性，及此类序列的符号平衡。实验结果表明，该序列能获得最小周期的最大值，即 $2\times3^{n-1}$，并能得到 $n=5,6,7$ 时此类序列的线性复杂度，其结构简单且具有较好的伪随机性。

关键词：流密码；m-序列；广义自缩序列；游程分布；最小周期

Pseudo Random of New Class Generalized Self-shrinking Sequence on GF(3)

WANG Jin-ling, CUI Xue-qing

(Department of Mathematic, Zhengzhou University, Zhengzhou 450001, China)

【Abstract】This paper proposes a new class of generalized self-shrinking sequences on GF(3). The run distribution is analysed. It gets that the range of the number of 1-run 2-run 0-run whose length is 1 and 1-run whose length is $k(2\leqslant k\leqslant(n-6)/2)$ in consecutive $2\times3^{n-1}$ symbols of sequence b. It is verified that the theorems 1、2、3 are right by the example of $n=8$. It is proved that the sequences are balanced. Experimental results show that the minimum period of the sequences can reach the maximum(that is, $2\times3^{n-1}$) and gets the linear complexities of the sequences when n=5,6,7. This sequences can get good pseudo random and have simpleness structure.

【Key words】stream cipher; m-sequence; generalized self-shrinking sequence; run distribution; minimum period

DOI: 10.3969/j.issn.1000-3428.2011.19.043

1 概述

随着信息时代的到来，伪随机序列广泛应用于通信、密码等诸多领域，则设计具有伪随机特性的密钥流序列生成机制成为信息时代的热点和难点。文献[1]提出自缩序列，但其密钥选择范围较小；文献[2]提出广义自缩序列的概念，扩大了密钥选择范围；文献[3-4]对某些类型的广义自缩序列进行了详细的研究；文献[5-6]将广义自缩序列的概念扩展到GF(3)；文献[5]提到的生成序列存在短游程数量少的不足；文献[6]提到的生成序列，虽然短游程数量有所增加，但是实现的难度较大。基于以上观点，本文提出新一类广义自缩序列。

2 基础知识介绍与游程分布定义

2.1 基础知识介绍

下面给出输出序列的模型：

定义 设 $a=a_0a_1\mathrm{L}$ 是GF(3)上的 m-序列。对于 $k=0,1,\mathrm{L}$ 如果 $a_k=1$，那么输出 a_{k-2}，如果 $a_k=2$，那么输出 $a_{k-1}+a_k$，否则放弃输出。这样得到的输出序列记为 $b=b_0b_1\mathrm{L}$，称序列 b 为GF(3)上一类广义自缩序列。

以下列出平凡事实：

若序列 a 是GF(3)上的 n 级 m-序列，则：

(1)序列 a 的最小周期为 3^n-1；

(2)在序列 a 的一个最小周期内，1 和 2 各出现 3^{n-1} 次，0 出现 $3^{n-1}-1$ 次；

(3)将序列 a 的一个最小周期首尾相连，则游程分布如下：对于 $1\leqslant k\leqslant n-2$，长为 k 的 0 游程 1 游程 2 游程各出现 $2^2\times3^{n-k-2}$ 次；长为 $n-1$ 的 0 游程出现 2 次，1 游程 2 游程各出现一次；长为 n 的 0 游程不出现，1 游程 2 游程各出现一次。由以上模型定义及事实知，序列 b 以 $2\times3^{n-1}$ 为一个周期。

2.2 游程分布

引理 1 某个固定的 t，使得 $a_t=1$，则当且仅当序列 a 的相应符号为以下情形时，得到序列 b 中 1 长 1 游程如下：

(1) $0*101\bar{0}001$
(2) $0*1011$
(3) $0*1012$
(4) $0*101\bar{0}02$
(5) $0111\bar{0}001$
(6) 01112
(7) $0111\bar{0}02$
(8) $121\bar{0}001$
(9) 1212
(10) $121\bar{0}02$
(11) 1211
(12) $2*101\bar{0}001$
(13) $2*1011$
(14) $2*1012$
(15) $2*101\bar{0}02$
(16) $2111\bar{0}001$

基金项目：河南省教育厅自然科学指导性计划基金资助项目(2005 10459003)

作者简介：王锦玲(1963－)，女，教授，主研方向：密码学，信息安全；崔雪晴，硕士研究生

收稿日期：2011-04-12 **E-mail：**cuixq0807@sina.com

(17) 21112

(18) 2111$\bar{0}$02

其中，$\bar{0}$ 的长度大于等于 0；$*$ 可以是 0、1、2 中的任何一个数字。

引理 2 设某个固定的 t，使得 $a_t=2$，当且仅当序列 a 的相应符号为以下情形时，得到序列 b 中 1 长 1 游程如下：

(1) 122$\bar{0}$001

(2) 122$\bar{0}$02

(3) 12201

(4) 1221

(5) 022$\bar{0}$001

(6) 022$\bar{0}$02

(7) 02201

(8) 0221

其中，$\bar{0}$ 的长度大于等于 0。

定理 1 若 $n\geqslant 8$，则在序列 b 的连续 $2\times 3^{n-1}$ 个符号中，1 长 1 游程的个数所在范围为：$86\times 3^{n-6}-11\sim 86\times 3^{n-6}+11$。

证明过程如下：

(1)引理 1 的情形

当符号串长不超过 n 时，引理 1 的(1)、(12)中的 $\bar{0}$ 的长度可以从 $0\sim n-8$，故 $*$ 有 3 种选择，此时 1 长 1 游程的数目为下式：

$$3\times\sum_{i=0}^{n-8}3^{n-(i+8)}=3\times\frac{3^{n-7}-1}{2}$$

引理 1 的(4)、(15)中的 $\bar{0}$ 的长度可以从 $0\sim n-7$，故 $*$ 有 3 种选择，此时 1 长 1 游程的数目为下式：

$$3\times\sum_{i=0}^{n-7}3^{n-(i+7)}=3\times\frac{3^{n-6}-1}{2}$$

引理 1 的(5)、(16)中的 $\bar{0}$ 的长度可以从 $0\sim n-7$，此时 1 长 1 游程的数目为下式：

$$\sum_{i=0}^{n-7}3^{n-(i+7)}=\frac{3^{n-6}-1}{2}$$

引理 1 的(7)、(8)和(18)中的 $\bar{0}$ 的长度可以从 $0\sim n-6$，此时 1 长 1 游程的数目为下式：

$$\sum_{i=0}^{n-6}3^{n-(i+6)}=\frac{3^{n-5}-1}{2}$$

引理 1 的(10)中的 $\bar{0}$ 的长度可以从 $0\sim n-5$，则此时 1 长 1 游程的数目为下式：

$$\sum_{i=0}^{n-5}3^{n-(i+5)}=\frac{3^{n-4}-1}{2}$$

另外，引理 1 的(2)、(3)、(6)、(9)、(11)、(13)、(14)和(17)的情形下，共有 $4\times 3^{n-4}$ 个 1 长 1 游程。此时 1 长 1 游程的个数为 $50\times 3^{n-6}-9$。故当符号串长超过 n 时，引理 1 的(1)、(4)、(5)、(7)、(8)、(10)、(12)、(15)、(16)和(18)的情形下一共至多有 18 个 1 长 1 游程。

(2)引理 2 的情形

当符号串长不超过 n 时，引理 2 的(1)、(5)中的 $\bar{0}$ 的长度可以从 $0\sim n-6$，此时 1 长 1 游程的数目为下式：

$$\sum_{i=0}^{n-6}3^{n-(i+6)}=\frac{3^{n-5}-1}{2}$$

引理 2 的(2)、(6)中 $\bar{0}$ 的长度可以从 $0\sim n-5$，此时 1 长 1 游程的数目为下式：

$$\sum_{i=0}^{n-5}3^{n-(i+5)}=\frac{3^{n-4}-1}{2}$$

另外，引理 2 的(3)、(4)、(7)和(8)情形下共有 $24\times 3^{n-6}$ 个。此时 1 长 1 游程的个数为 $36\times 3^{n-6}-2$。当符号串长超过 n 时，引理 2 的(1)、(2)、(5)和(6)的情形下，一共至多有 4 个 1 长 1 游程。

综上所述，在序列 b 的连续 $2\times 3^{n-1}$ 个符号中，1 长 1 游程的个数所在范围为：$86\times 3^{n-6}-11\sim 86\times 3^{n-6}+11$。

由类似引理 1、引理 2、定理 1 的分析方法可以得出在序列 b 的连续 $2\times 3^{n-1}$ 个符号中，1 长 2 游程、1 长 0 游程、k 长 1 游程($2\leqslant k\leqslant (n-6)/2$)的个数，此处不再详述。

定理 2 若 $n\geqslant 8$，在序列 b 的连续 $2\times 3^{n-1}$ 个符号中，1 长 2 游程的个数所在范围为：$(82+1/2)\times 3^{n-6}-4n+21/2\sim(82+1/2)\times 3^{n-6}+4n+3/2$。

定理 3 若 $n\geqslant 8$，在序列 b 的连续 $2\times 3^{n-1}$ 个符号中，1 长 0 游程的个数所在范围为：$(83+1/2)\times 3^{n-6}-4n+25/2\sim(83+1/2)\times 3^{n-6}+4n-1/2$。

定理 4 设 $2\leqslant k\leqslant (n-6)/2$，在序列 b 的连续 $2\times 3^{n-1}$ 个符号中，k 长 1 游程的个数所在范围为：$54\times 3^{n-k-5}+32\times 3^{n-2k-4}-2k-9\sim 54\times 3^{n-k-5}+32\times 3^{n-2k-4}+2k+9$。

通过实验发现，当序列 a 以 8 次本原多项式为极小多项式时，基于序列 a 的这一类广义自缩序列 b 的连续 $2\times 3^{8-1}$ 个符号中，1 长 0 游程的个数范围为 745~758，1 长 1 游程的个数为 774，1 长 2 游程的个数范围为 735~751，符合定理 1~定理 3 的结论。

3 符号平衡性、最小周期和线性复杂度

定理 5 在序列 b 连续 $2\times 3^{n-1}$ 个符号中，符号 0、1、2 出现次数相等，均为 $2\times 3^{n-2}$ 次。

证明：若要得到序列 b 中的符号为 0，则当且仅当序列 a 的相应符号为以下情形时：0$*$1，12。若要得到序列 b 中的符号为 1，则当且仅当序列 a 的相应符号为以下情形时：1$*$1，22。若要得到序列 b 中的符号为 2，则当且仅当序列 a 的相应符号为以下情形时：2$*$1，02。由于这 3 组符号串在序列 a 的一个最小周期内出现次数均为 $2\times 3^{n-2}$，因此，在序列 b 的连续 $2\times 3^{n-1}$ 个符号中，符号 0、1、2 出现次数相等，均为 $2\times 3^{n-2}$。其中，$*$ 可以是 0、1、2 中的任何一个数字。

当序列 a 以 n 次($5\leqslant n\leqslant 7$)本原多项式为极小多项式时，基于序列 a 的这一类广义自缩序列 b 的最小周期为 $2\times 3^{n-1}$，及对应的线性复杂度结果如表 1 所示。此类序列的最小周期可以达到最大值，且线性复杂度也较大。

表 1 序列 b 的最小周期和线性复杂度

本原多项式次数	序列 b 的最小周期	序列 b 的线性复杂度
5	162	153~158
6	486	475~481
7	1 458	1 447~1 452

4 结束语

本文提出 GF(3)上新一类广义自缩序列，并研究其伪随机性。可以看出，该序列生成方式简单，由于只用到控制序列当前位及与其单方向相邻 2 位符号的信息，因此便于实现。实验结果表明，该序列具有良好的短游程分布、符号平衡等伪随机性，在信息时代应用广泛。

参考文献

[1] Meier W, Staffelbach O. The Self-shrinking Generator[EB/OL]. (2011-01-21). http://en.wikipedia.org/wiki/Self-shrinking_generator.

(下转第 140 页)