GF(3)上新型自缩控序列的周期与线性复杂度

王锦玲 崔静静*

(郑州大学数学与统计学院 郑州 450001)

摘 要：自缩控(SSC)序列是一类重要的伪随机序列，而伪随机序列在通信加密、编码技术等很多领域中有着广泛的应用。在这些应用中，通常要求序列具有大周期和高的线性复杂度。为了构造出周期更大、线性复杂度更高的伪随机序列，该文基于GF(3)上的m-序列构造了一种新型自缩控序列模型，利用有限域理论研究了生成序列的周期和线性复杂度，得到的生成序列周期和线性复杂度大大提高，且得到生成序列线性复杂度更精确的一个上界值，从而提高了生成序列在通信加密中的防攻击能力和安全性能。

关键词：自缩控序列；线性复杂度；周期；特征多项式；m-序列

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2021)08-2149-07

DOI: 10.11999/JEIT200676

The Period and the Linear Complexity of a New Self-shrinking Control Sequence on GF(3)

WANG Jinling CUI Jingjing

(*School of Mathematics and Statistics*, *Zhengzhou University*, *Zhengzhou* 450001, *China*)

Abstract: Self-Shrinking Control (SSC) sequences are a class of important pseudo-random sequences, and pseudo-random sequences are widely used in many fields, such as communication encryption, recoding technology. In these applications, sequences are usually required to have large periods and high linear complexity. In order to construct pseudo-random sequences with higher period and higher linear complexity, a new SSC sequence model based on the m-sequence in GF (3) is constructed, the period and the linear complexity of the generated sequence are studied by using finite domain theory, this model greatly improves the period and the linear complexity of the generated sequence, and obtains a more accurate upper bound value of the linear complexity of the generated sequence. Thus, the anti-attack ability and security performance of the generated sequence in communication encryption are improved.

Key words: Self-Shrinking Control (SSC) sequence; Linear complexity; Period; Characteristic polynomial; m-sequence

1 引言

线性复杂度和周期是衡量序列伪随机性的两个重要指标。序列的线性复杂度已经在很多文献中被研究过[1]，比如文献[1]研究了一种特殊2元序列的线性复杂度，文献[2–4]讨论了周期不同的2元广义分圆序列的线性复杂度，文献[5,6]研究了不同周期的4元广义分圆序列的线性复杂度，文献[7,8]分别讨论了2元割圆序列和广义割圆序列的线性复杂度，文献[9,10]讨论了不同周期序列的线性复杂度。本文主要研究的是新型自缩控序列的线性复杂度，自缩序列有许多密码学优点，比如构造方式简单、周期较大、线性复杂度较高、对驱动序列有强力保护，而成为密码学中一类重要的伪随机序列。文献[11]定义了自缩序列的构造方式，给出了其线性复杂度的上界值等于周期的上界值：2^{n-1}，文献[12]给出了自缩序列线性复杂度的一个上界值：$2^{n-1}-(n-2)$，此界值较文献[11]中更精确，文献[13]提出通过模加来构造一种新的自缩序列，这虽然提高了生成序列的安全性能，但与文献[11,12]相比，其给出的周期和线性复杂度的上界并没有更精确，如何使得生成的自缩序列周期更大，线性复杂度更高且更精确，一直是研究自缩序列生成方式的一个重要问题，文献[14–16]分别在GF(3)上构造了不同的自缩序列模型，虽然得到的周期比文献[11–13]中的更大，但线性复杂度并没有突破文献[12]中的界值。而本文在GF(3)上构造的新型自缩控序列模型，不但更大地提高了

收稿日期：2020-08-04；改回日期：2020-12-09；网络出版：2020-12-21
*通信作者： 崔静静 17335569258@163.com
基金项目：国家自然科学基金 (61772476)
Foundation Item: The National Natural Science Foundation of China (61772476)

生成序列的周期和线性复杂度，而且得到了生成序列线性复杂度更精确的一个上界，给出新型自缩控序列的周期上界：3^n，下界：$3^{2\cdot\lfloor n/3\rfloor}$；线性复杂度的上界：$3^n-\lfloor(n-3)/4\rfloor-1$，下界：$3^{2\cdot\lfloor n/3\rfloor-1}$。

下面定义新型自缩控序列。

定义 1 设$a^\infty=(a_0,a_1,a_2,\cdots)$是一$n$级$m$-序列，将序列$a^\infty$的输出比特依次按照如式(1)方式分组

$$(a_0,a_1,a_2)(a_3,a_4,a_5)\cdots(a_{3k},a_{3k+1},a_{3k+2})\cdots \tag{1}$$

若$a_{3k}\oplus a_{3k+1}\oplus a_{3k+2}=0$，则放弃输出；若$a_{3k}\oplus a_{3k+1}\oplus a_{3k+2}=1$，则输出$a_{3k+1}$；若$a_{3k}\oplus a_{3k+1}\oplus a_{3k+2}=2$，则输出$a_{3k+1}$, a_{3k+2}；这样得到的输出序列为$s^\infty=(s_0,s_1,s_2,\cdots)$，称为由序列$a^\infty$导出的新型自缩控序列(Self-Shrinking Control sequence, SSC)，以下简记为SSC(模3)-序列。

2 SSC(模3)-序列的理论基础

引理1[17] 设$a^\infty=(a_0,a_1,a_2,\cdots)$是GF(3)上一$n$级$m$-序列，对于$0<k\le n$，设GF(3)上任意$k$元组$(b_1,b_2,\cdots,b_k)$在$a^\infty$的一个周期中出现的次数

$$N(b_1,b_2,\cdots,b_k)=\begin{cases}3^{n-k}, & (b_1,b_2,\cdots,b_k)\ne(0,0,\cdots,0)\\ 3^{n-k}-1, & (b_1,b_2,\cdots,b_k)=(0,0,\cdots,0)\end{cases} \tag{2}$$

证明：考虑在序列a^∞的一个周期圆中，每个非0的n元组(n维向量)只出现1次，对每个非0的k维向量扩充为n维向量共有3^{n-k}种扩充方式，同样对于k长的0向量也有3^{n-k}种扩充为n维向量的方式，但要去掉一个全0的n维向量(这是因为n级m-序列无n长0向量)，故此时有$3^{n-k}-1$种方式。 证毕

引理2[17] 设$a^\infty=(a_0,a_1,a_2,\cdots)$是GF(3)上一$n$级$m$-序列，则有：

(1) 序列a^∞的最小周期是3^n-1;

(2) 序列a^∞是平衡的，即在序列a^∞的一个最小周期内，1, 2各出现3^{n-1}次，0出现$3^{n-1}-1$次。

证明 由n级m-序列的定义知序列a^∞的最小周期为3^n-1，即(1)成立；(2)的结果由引理1中$k=1$即可得。

为了得到SSC(模3)-序列线性复杂度更精确的上界值，先从序列的特征多项式入手来展开讨论。设序列u^∞是GF(3)上周期整除3^n的一个序列，则$1-x^{3^n}=(1-x)^{3^n}$是序列u^∞的一个特征多项式，则序列的极小多项式可表示为$(1-x)^a$，其中$0\le a\le 3^n$，若$0\le L\le 3^n-\lfloor(n-3)/4\rfloor-1$，这里$L$表示序列的线性复杂度，则只需证$(1-x)^{3^n-\lfloor(n-3)/4\rfloor-1}$是序列$u^\infty$的一个特征多项式，由特征多项式的定义知：只需证明

$$\sum_{i=0}^{v}\binom{v}{v-i}(-1)^{v-i}\bmod 3\cdot u_i=0 \tag{3}$$

即等价于证明

$$\sum_{i=0}^{v}\binom{v}{i}(-1)^{v-i}\bmod 3\cdot u_i=0 \tag{4}$$

其中$v=3^n-\lfloor(n-3)/4\rfloor-1$。所以也需要下面的引理。

引理3[18] 设T是GF(3^n)到GF(3)上的任一线性投射，则存在$c\in$GF(3^n)，使$T(x)=\mathrm{Tr}(cx)$，其中对任意$x\in$GF(3^n)，满足$\mathrm{Tr}(x)=\sum_{i=0}^{n-1}x^{3^i}$。

证明 为了证明简便，不妨设$F=$GF(3^n)$K=$GF(3)$T(x)\triangleq L_c(x)\mathrm{Tr}(x)\triangleq\mathrm{Tr}_{F/K}(x)L_c$是线性变换(线性投射)，则$T(x)=\mathrm{Tr}(cx)$等价于$L_c(x)=\mathrm{Tr}_{F/K}(cx)$，本文先来证明$c\ne d$时，有$L_c\ne L_d$。由于$\mathrm{Tr}_{F/K}$是$F$到$K$上的线性变换，所以$\exists x\in F$使得$\mathrm{Tr}_{F/K}((c-d)x)\ne 0$，因此有$L_c(x)-L_d(x)=\mathrm{Tr}_{F/K}((c-d)x)\ne 0$，从而$L_c\ne L_d$。这样$\{L_c:c\in F\}$共给出了$3^n$个线性变换。但由于$F\to K$的任何一个线性变换都可以由该变换作用在某一组基上的像完全确定，而且这些像可以在K中任意取值，因此$F\to K$的线性变换共有3^n个，所以$\{L_c:c\in F\}$就是线性变换的全体。即F到K的任一线性变换都可以写成$L_c(x)=\mathrm{Tr}_{F/K}(cx)$的形式，也即可以写成$T(x)=\mathrm{Tr}(cx)$的形式。 证毕

定义2[18] 设i是任一正整数，$w_3(i)$表示i的三进制展开中非0位的个数。

定义3[18] 设R表示次数小于3^n的多项式环，对所有的非负整数k，定义：$P_3(k)=\left\{\sum_{i=0}^{3^n-1}a_ix^i\in R\middle|\text{当}w_3(i)\ge k+1\text{时，}a_i=0\right\}$；$P_3{}^*(k)=\left\{\sum_{i=0}^{3^n-1}a_ix^i\in R\middle|\text{当}w_3(i)\ge k+1\text{时，}a_i=0a_0=0\right\}$。

引理4[18] 设T是GF(3^n)到GF(3)上的任意一个线性投射，则$T\in P_3^*(1)$。

证明 由引理3知$\exists c\in$GF(3^n)有$T(x)=\mathrm{Tr}(cx)$，且$\mathrm{Tr}(cx)=\sum_{j=0}^{n-1}c^jx^{3^j}\ a_{3^j}=c^j$，所以只有当$\mathrm{Tr}(cx)$的系数是第$3^i$项时非0，即$w_3(i)\ge 2$时$a_i=0$且$a_0=0$，所以$T\in P_3^*(1)$。 证毕

引理5[18] 设$f\in P_3(k_1)g\in P_3(k_2)$，则有$fg\in P_3(k_1+k_2)$，如果$f\in P_3^*(k_1)g\in P_3(k_2)$，则$fg\in P_3^*(k_1+k_2)$。

证明 f, g中x的次数有以下情况：当$i_1+i_2\le 3^n-1$时，有$x^{i_1}x^{i_2}=x^{i_1+i_2}$；当$i_1+i_2\ge 3^n$时，有$x^{i_1}x^{i_2}=x^{i_1+i_2-3^n+1}$，其中当$i_1+i_2\le 3^n-1$时，$w_3(i_1+i_2)\le w_3(i_1)+w_3(i_2)\le k_1+k_2$，当$i_1+i_2$

$\geq 3^n$时，$w_3(i_1+i_2-3^n+1) \leq w_3(i_1+i_2)-1+1 \leq k_1+k_2$，得$fg \in P_3(k_1+k_2)$;

当 $f \in P_3{}^*(k_1)$ 时，$f(0)=0$ 且$fg(0)=f(0)g(0)=0$，所以$fg \in P_3^*(k_1+k_2)$。　　证毕

引理 6[18]　设 $\alpha \in \mathrm{GF}(3^n)$ 是一个本原元，$f \in P_3^*(k)$，则存在一个元素$g \in P_3(k)$，对所有的$i \in \{0,1,\cdots,3^n-2\}$，有$g(\alpha^i)=\sum_{j=0}^{i} f(\alpha^j)$。

证明　若 $k \leq n-1$，设$f=\sum_{r=1}^{3^n-2} a_r x^r (f \in P_3^*(k))$，设$g(x)=\left(\sum_{r=1}^{3^n-2} a_r \frac{\alpha^r}{\alpha^r-1} x^r\right)-\sum_{r=1}^{3^n-2} a_r \frac{1}{\alpha^r-1} g(\alpha^i)=\left(\sum_{r=1}^{3^n-2} a_r \frac{\alpha^r}{\alpha^r-1}\alpha^{ir}\right)-\sum_{r=1}^{3^n-2} a_r \frac{1}{\alpha^r-1}=\sum_{j=0}^{i}\left(\sum_{r=1}^{3^n-2} a_r (\alpha^j)^r\right)=\sum_{j=0}^{i} f(\alpha^j)$。　　证毕

引理7[18]　设 $f \in P_3^*(k)$ $(k<n)$，则$\sum_{x \in \mathrm{GF}(3^n)\setminus\{0\}} f(x)=0$。

证明　因为 $f \in P_3^*(k)$，所以$f(0)=0$，设$f=\sum_{r=1}^{3^n-2} a_r x^r$ $(a_0=0 a_{3^n-1}=0)$ $\sum_{\alpha^k \in \mathrm{GF}(3^n)} f(\alpha^k)=\sum_{r=1}^{3^n-2} a_r\left(\frac{\alpha^r}{\alpha^r-1}\alpha^{(3^n-2)r}-\frac{1}{\alpha^r-1}\right)=\sum_{r=1}^{3^n-2} a_r\left(\frac{1}{\alpha^r-1}-\frac{1}{\alpha^r-1}\right)=0$。

引理 8　设 f_1 $f_2 \in P_3^*(k)(k<n)$，则$\sum_{x \in \mathrm{GF}(3^n)\setminus\{0\}} f_1(x)+2f_2(x)=0$。

证明　因为 f_1 $f_2 \in P_3^*(k)$，所以$f_1(0)=0$ $f_2(0)=0$，若要证明$\sum_{x \in \mathrm{GF}(3^n)\setminus\{0\}} f_1(x)+2f_2(x)=0$成立，则等价于证明$\sum_{x \in \mathrm{GF}(3^n)} f_1(x)+2f_2(x)=0$成立即可。设$f_1(x)=\sum_{r=1}^{3^n-2} a_r x^r f_2(x)=\sum_{r=1}^{3^n-2} b_r x^r$，其中$a_r b_r \in \mathrm{GF}(3^n)$，由$1 \leq r \leq 3^n-2$，得$\sum_{x \in \mathrm{GF}(3^n)} x^r=0$，(见参考文献[19])，因此有

$$\begin{aligned}&\sum_{x \in \mathrm{GF}(3^n)} f_1(x)+2f_2(x)\\&=\sum_{x \in \mathrm{GF}(3^n)}\left(\sum_{r=1}^{3^n-2} a_r x^r+\sum_{r=1}^{3^n-2} 2b_r x^r\right)\\&=\sum_{r=1}^{3^n-2}(a_r+2b_r)\sum_{x \in \mathrm{GF}(3^n)} x^r=0\end{aligned} \tag{5}$$

证毕

为了得到周期为3^n的序列线性复杂度更精确的上界值，本文引入GF(3^n)到GF(3)上两个非0的线性映射T_1 T_2具体定义如下。

定义4　设n是任一正整数，设T_1 T_2分别是GF(3^n) $\to$ GF(3)上两个不同的，且非0的线性映射，设$\alpha \in \mathrm{GF}(3^n)$是$n$次本原多项式的根，则定义

$$T_1:\sum_{i=0}^{n-1} a_i\alpha^i \to a_{n-2},\ T_2:\sum_{i=0}^{n-1} a_i\alpha^i \to a_{n-2},a_{n-1} \tag{6}$$

由以上T_1, T_2和α的定义，通过以下方式可得到GF(3^n)中周期为3^n的序列u^∞：

当$0 \leq i < 3^{n-1}$时，定义u_i为序列$1,\alpha,\alpha^2,\cdots,\alpha^{3^n-2}$中使$T_1(x)=1$的第$i+1$个元素；当$3^{n-1} \leq i < 2\cdot 3^{n-1}$时，定义$u_i$为序列$1,\alpha,\alpha^2,\cdots,\alpha^{3^n-2}$中使$T_2(x)=a_{n-2}=2$，$u_i=2\cdot u_{i-3^{n-1}}$的$3^{n-1}$个元素；当$2\cdot 3^{n-1} \leq i < 3^n$时，定义$u_i$为序列$1,\alpha,\alpha^2,\cdots,\alpha^{3^n-2}$中使$T_2(x)=a_{n-1}=2$的第$2\cdot 3^{n-1}-i+1$个元素。

定理1　设u_i是上述序列u^∞中的元素，且$u_i \in \mathrm{GF}(3^n)$，则

$$\sum_{i=0}^{v}\binom{v}{i}(-1)^{v-i} \bmod 3 \cdot u_i=0 \tag{7}$$

其中，$v=3^n-\lfloor (n-3)/4\rfloor-1$。

证明　u_i是式(7)中的被加项当且仅当i满足$\binom{3^n-\lfloor (n-3)/4\rfloor-1}{i} \bmod 3 \neq 0$，等价于$\lfloor (n-3)/4\rfloor$的三进制展开中的第$k$位是2时，$i$的三进制展开中的第$k$位是0; $\lfloor (n-3)/4\rfloor$的三进制展开中的第k位是1时，i的三进制展开中的第k位是1或0。对于式(7)中被加项的系数：$\binom{v}{i}(-1)^{v-i} \bmod 3$，在GF(3)上有$\binom{v}{i}(-1)^{v-i} \bmod 3$=1或2，当被加项系数为1时，记此时对应的被加项为u_{t_i}；当被加项系数为2时，记此时对应的被加项为u_{t_j}，则要证明式(7)成立，即要证明式(8)成立

$$\sum_{i,j=0,i\neq j}^{v} c_{t_i}u_{t_i}+c_{t_j}u_{t_j}=0 \tag{8}$$

即等价于证明式(9)成立

$$\sum_{i,j=0,i\neq j}^{v} u_{t_i}+2u_{t_j}=0 \tag{9}$$

为了证明式(9)成立，需要定义以下两个映射，设σ_1为GF(3^n) $\to$ GF(3^n)的一个映射，具体定义如下：当$x=u_{t_i}$为式(9)中的被加数时，有$\sigma_1(x)=x$，此时被加项对应的系数为1；其他情形时，有$\sigma_1(x)=0$。同样定义σ_2如下：当$x=u_{t_j}$为式(9)中的被加数时，$\sigma_2(x)=x$，此时被加项对应的系数为2；其他情形时，有$\sigma_2(x)=0$。由$\sigma_1\sigma_2$的定义可得

$$\sum_{i,j=0,i\neq j}^{v} u_{t_i}+2u_{t_j}=\sum_{x \in \mathrm{GF}(3^n)\setminus\{0\}} \sigma_1(x)+2\sigma_2(x)=0 \tag{10}$$

则由引理8知，要证明式(10)成立，只需证明$\sigma_1(x) \in P_3^*(z_1')$ $\sigma_2(x) \in P_3^*(z_2')$ $z_1', z_2'=n-1$，即可证明式(10)成立，那么说明式(7)也是成立的，下面来证$\sigma_1(x) \in P_3^*(z_1')\sigma_2(x) \in P_3^*(z_2')$，其中$z_1', z_2'=n-1$。

定义函数$\kappa_k(x):\mathrm{GF}(3^n)\to\mathrm{GF}(3^n)$，具体定义如下：当$x=u_{t_i}$或$x=u_{t_j}$时，且此时$t_it_j$被$3^k$整除，有$\kappa_k(x)=1$；其他情形时，有$\kappa_k(x)=0$。为了证明方便，把$u_{t_i}u_{t_j}$统一记为$u_i$，下面用数学归纳法来证$\kappa_k(x)\in P_3^*(3^k)$，当$k=0$时，$\kappa_0(x)=T_1\in P_3^*(1)=P_3^*(3^0)$，此时结论成立；下面假设有$\kappa_{k-1}\in P_3^*(3^{k-1})$，则由引理6知，存在$g(x)\in P_3(3^{k-1})$，使得$g(\alpha^i)=\sum_{j=0}^{i}\kappa_{k-1}(\alpha^j)$，再由$\kappa_k(x)=1\Leftrightarrow\kappa_{k-1}(x)=1$，且$g(x)\neq 0$，则可得到$\kappa_k(x)=\kappa_{k-1}(x)g^2(x)$，那么由引理5可知$\kappa_k(x)\in P_3^*(3^k)$。

设$\sigma_k(x)=1+g^2(x)\sigma_k(x)\in P_3(2\cdot 3^{k-1})$，$i$的三进制展开中的第$k$位非零时，有$\sigma_k(u_i)=1$，其他情形时，$\sigma_k(u_i)=0$，再记$h_{1k}=\sigma_{1k}$，其中$1k$表示$\lfloor(n-3)/4\rfloor$的三进制展开中的第$k$位是1时的下标；$h_{2k}=\sigma_{2k}$，其中$2k$表示$\lfloor(n-3)/4\rfloor$的三进制展开中的第$k$位是2时的下标，设$n-3$的三进制表示为：$n-3=\sum_{i=0}^{n-4}a_i3^i$，其中$a_i\in\{0,1,2\}$，(注意此处$n-3<3^{n-3}$，所以该定义有意义。)则可得到两个函数：

$$\left.\begin{aligned}P_1&=XT_1\prod\left(h_{1k}+1\right)^2\prod\left(h_{2k}^4+1\right)\\P_2&=\frac{1}{2}XT_2\prod\left(h_{1k}+1\right)^2\prod\left(h_{2k}^4+1\right)\end{aligned}\right\}\tag{11}$$

其中，X是恒同映射，T_1T_2是定义4中的映射。且有$\prod\left(h_{1k}+1\right)^2\prod\left(h_{2k}^4+1\right)\in P_3^*(z_1)$，其中$z_1=n-3$，再由引理5知，$P_1\in P_3^*(z_1')$，其中$z_1'=z_1+2=n-1$，则$P_1(x)=x$的充要条件为$T_1(x)=1\prod(h_{1k}+1)^2=1\prod\left(h_{2k}^4+1\right)=1$，即充要条件为$T_1(x)=1$ $h_{1k}(x)\neq 2h_{2k}(x)=0$。由此可以看出$P_1(x)=\sigma_1(x)$，且$P_1(x)=\sigma_1(x)\in P_3^*(z_1')$；同样对于$P_2(x)$，有$\prod\left(h_{1k}+1\right)^2\prod\left(h_{2k}^4+1\right)\in P_3^*(z_2)$，其中$z_2=n-3$，再由引理5知$P_2\in P_3^*(z_2')$，其中$z_2'=z_2+2=n-1$，则有$P_2(x)=x$的充要条件是$T_2(x)=2\prod\left(h_{1k}+1\right)^2=1\prod\left(h_{2k}^4+1\right)=1$，即$T_2(x)=2h_{1k}(x)\neq 2h_{2k}(x)=0$。由此可得到$P_2(x)=\sigma_2(x)P_2(x)=\sigma_2(x)\in P_3^*(z_2')$，则由引理8得$\sum_{x\in\mathrm{GF}(3^n)\backslash\{0\}}\sigma_1(x)+2\sigma_2(x)=0$，那么则有等式$\sum_{i=0}^{v}\binom{v}{i}(-1)^{v-i}\bmod 3\cdot u_i=0$成立，其中的$v$为$3^n-\lfloor(n-3)/4\rfloor-1$。证毕

3 SSC(模3)-序列的周期和线性复度

本部分给出GF(3)上SSC(模3)-序列的周期与线性复杂度的界，为叙述方便，本文用$P(\cdot)$来表示序列的最小周期，用$L(\cdot)$来表示序列的线性复杂度。

3.1 周期

设$a^\infty=(a_0,a_1,a_2,\cdots)$是GF(3)上一$n$级$m$-序列，将序列$a^\infty$的输出比特依次分组如下：$(a_0,a_1,a_2)$, $(a_3,a_4,a_5),\cdots,(a_{3^n-2},a_0,a_1),(a_2,a_3,a_4),\cdots,(a_{3^n-3},a_{3^n-2},a_0),(a_1,a_2,a_3),\cdots,(a_{3^n-4},a_{3^n-3},a_{3^n-2}),(a_0,a_1,a_2),\cdots$

由此看到，把序列a^∞的3个周期段内输出的比特依次重排后，(a_0,a_1,a_2)将会重复出现，所以SSC(模3)-序列s^∞是周期的。

定理2 设$a^\infty=(a_0,a_1,a_2,\cdots)$是GF(3)上一$n$级$m$-序列，序列$s^\infty$为$a^\infty$导出的SSC(模3)-序列，则$s^\infty$是平衡的且$P(s^\infty)|3^n$。

证明 由新型自缩控序列的定义知，只有当$a_{3k}\oplus a_{3k+1}\oplus a_{3k+2}=1$或2时，才会有输出比特作为序列$s^\infty$的元素，由引理1知，每个3元组 (0, 0, 1) (1, 0, 0)(0, 1, 0)(2, 0, 2)(0, 2, 2)(2, 2, 0)(1, 1, 2)(1, 2, 1)(2, 1, 1)各出现3^{n-3}次，此时a^∞输出$9\cdot 3^{n-3}$个比特,其中0 1 2个数均为$3\cdot 3^{n-3}$；每个3元组(0, 0, 2)(0, 2, 0)(2, 0, 0)(1, 1, 0)(1, 0, 1)(0, 1, 1)(2, 2, 1)(2, 1, 2)(1, 2, 2)各出现3^{n-3}次，此时a^∞输出$9\cdot 2\cdot 3^{n-3}$个比特，其中0, 1, 2个数均为$3\cdot 2\cdot 3^{n-3}$；

故$9\cdot 3^{n-3}+9\cdot 2\cdot 3^{n-3}=3^n$是序列$s^\infty$的一个周期，且0,1,2均出现$3^{n-1}$次。如果记$s^\infty$的最小周期为$P(s^\infty)$，则序列$s^\infty$是平衡的且$P(s^\infty)|3^n$。 证毕

定理3 对于任意正整数$n\geq 3$，SSC(模3)-序列s^∞的最小周期满足$P(s^\infty)\geq 3^{2\cdot\lfloor n/3\rfloor}$。

证明 设$m=3\cdot\lfloor n/3\rfloor$，当$n=3k$时，$m=n$；当$n=3k+1$时，$m=n-1$；当$n=3k+2$时，$m=n-2$。因为$a^\infty=(a_0,a_1,a_2,\cdots)$为$n$级$m$-序列，所以$a(3t)=(a_{3t},a_{3t+1},\cdots,a_{3t+m-1})$跑遍$\mathrm{GF}(3)^m$上所有向量，特别跑遍了如下形式的向量：

(1) $(a_0,b_0,c_0),(a_1,b_1,c_1),\cdots,(a_{m/3-1},b_{m/3-1},c_{m/3-1})$，其中$a_i\oplus b_i\oplus c_i=1(\bmod 3)$，$i=0,1,\cdots,m/3-1$。

(2) $(a_0',b_0',c_0'),(a_1',b_1',c_1'),\cdots,(a_{m/3-1}',b_{m/3-1}',c_{m/3-1}')$，其中$a_i'\oplus b_i'\oplus c_i'=2(\bmod 3)$，$i=0,1,\cdots,m/3-1$。

在第(1)种情况下，$z(t)=(b_0,b_1,\cdots,b_{m/3-1})$ $t=0,1,\cdots$,跑遍$\mathrm{GF}(3)^{m/3}$上所有向量，所以此时有$P(s^\infty)\geq 3^{m/3}=3^{\lfloor n/3\rfloor}$；在第(2)种情况下，$z(t)=(b_0',c_0',b_1',c_1',\cdots,b_{m/3-1}',c_{m/3-1}')t=0,1,\cdots$，跑遍$\mathrm{GF}(3)^{2m/3}$上所有向量，所以此时有$P(s^\infty)\geq 3^{2m/3}=3^{2\lfloor n/3\rfloor}$。综上有$P(s^\infty)\geq 3^{2\lfloor n/3\rfloor}$。 证毕

由上述定理可知$3^{2\cdot\lfloor n/3\rfloor}\leq P(s^\infty)\leq 3^n$，且SSC(模3)-序列的周期上界可以达到。

3.2 线性复杂度

设$a^\infty=(a_0,a_1,a_2,\cdots)$是GF(3)上一$n$级$m$-序

列，则存在非0元$c\in \mathrm{GF}(3^n)$和本原元$\alpha\in \mathrm{GF}(3^n)$使得$a_i=\mathrm{Tr}(c\alpha^i)$，对所有的非负整数$i$成立，设序列$s^\infty$是由序列$a^\infty$导出的自缩控序列，记

$$s^\infty=(s_{00},s_{10},s_{20},\cdots,s_{3^{n-1}-1,0},s_{3^{n-1},0},\cdots,s_{2\cdot 3^{n-1}-1,0},s_{2\cdot 3^{n-1},1},\cdots,s_{3\cdot 3^{n-1}-1,1}) \tag{12}$$

则有

当$0\le i<3^{n-1}$$s_{im}=a_{3\tau(i)+1}$，其中$\tau(i)$是序列$a_0\oplus a_1\oplus a_2(\mathrm{mod}3)a_3\oplus a_4\oplus a_5(\mathrm{mod}3)\cdots$中使得下面3项和，即$a_{3\tau(i)}\oplus a_{3\tau(i)+1}\oplus a_{3\tau(i)+2}(\mathrm{mod}3)$为1的第$i+1$个1，这里令$m=0$；

当$3^{n-1}\le i<2\cdot 3^{n-1}$$s_{im}=a_{3\tau(i)+1}$，其中$\tau(i)$是序列$a_0\oplus a_1\oplus a_2(\mathrm{mod})3a_3\oplus a_4\oplus a_5(\mathrm{mod}3)\cdots$中使得下面3项和，即$a_{3\tau(i)}\oplus a_{3\tau(i)+1}\oplus a_{3\tau(i)+2}(\mathrm{mod}3)$为2的第$i-3^{n-1}+1$个2，这里令$m=0$；

当$2\cdot 3^{n-1}\le i<3^n$$s_{im}=a_{3\tau(i)+2}$，其中$\tau(i)$是序列$a_0\oplus a_1\oplus a_2(\mathrm{mod}3)a_3\oplus a_4\oplus a_5(\mathrm{mod}3)\cdots$中使得下面3项和，即$a_{3\tau(i)}\oplus a_{3\tau(i)+1}\oplus a_{3\tau(i)+2}(\mathrm{mod}3)$为2的第$i-2\cdot 3^{n-1}+1$个2，这里令$m=1$。

为了更方便地来表示序列的线性复杂度，下面我们利用迹映射的相关性质和上述u^∞来重新定义。设$T:\mathrm{GF}(3^n)\to\mathrm{GF}(3)$，$T(x)=\mathrm{Tr}((c^{3^{n-1}}+(c\alpha+c\alpha^2)^{3^{n-1}})x)$，因为迹映射在3次方自同构下不变，所以有$\mathrm{Tr}(x)=\mathrm{Tr}(x^3)$，则有

$$\begin{aligned}T(\alpha^k)&=\mathrm{Tr}((c^{3^{n-1}}+(c\alpha+c\alpha^2)^{3^{n-1}})\alpha^k)\\&=\mathrm{Tr}(((c^{3^{n-1}}+(c\alpha+c\alpha^2)^{3^{n-1}})\alpha^k)^3)\\&=\mathrm{Tr}(c\alpha^{3k}+c\alpha^{3k+1}+c\alpha^{3k+2})\\&=a_{3k}+a_{3k+1}+a_{3k+2}\end{aligned} \tag{13}$$

设$T_1{}':\mathrm{GF}(3^n)\to\mathrm{GF}(3)$，$T_1{}'(x)=\mathrm{Tr}((c\alpha)^{3^{n-1}}x)$，则有

$$\begin{aligned}T_1{}'(\alpha^k)&=\mathrm{Tr}((c\alpha)^{3^{n-1}}\alpha^k)\\&=\mathrm{Tr}((c\alpha)^{3^n}\alpha^{3k})=\mathrm{Tr}(c^{3^n}\alpha^{3^n}\alpha^{3k})\\&=\mathrm{Tr}(c\alpha\alpha^{3k})=\mathrm{Tr}(c\alpha^{3k+1})=a_{3k+1}\end{aligned} \tag{14}$$

设$T_2{}':\mathrm{GF}(3^n)\to\mathrm{GF}(3)$，$T_2{}'(x)=\mathrm{Tr}((c\alpha^{m+1})^{3^{n-1}}x)$，则有

$$\begin{aligned}T_2{}'(\alpha^k)&=\mathrm{Tr}((c\alpha^{m+1})^{3^{n-1}}\alpha^k)=\mathrm{Tr}((c\alpha^{m+1})^{3^n}\alpha^{3k})\\&=\mathrm{Tr}(c^{3^n}\alpha^{3^n(m+1)}\alpha^{3k})\\&=\mathrm{Tr}(c\alpha^{m+1}\alpha^{3k})=\mathrm{Tr}(c\alpha^{3k+(m+1)})\\&=a_{3k+(m+1)}\end{aligned} \tag{15}$$

其中，$m=0$或1。

以下为了叙述方便，当$m=0$时，记T_2'为T_{20}'；当$m=1$时，记T_2'为T_{21}'；重新记

$$u^\infty=(u_{00},u_{10},u_{20},\cdots,u_{3^{n-1}-1,0},u_{3^{n-1},0},\cdots,u_{2\cdot 3^{n-1}-1,0},u_{2\cdot 3^{n-1},1},\cdots,u_{3\cdot 3^{n-1}-1,1}) \tag{16}$$

对所有的非负整数i有：当$0\le i<3^{n-1}$时，有$s_{im}=T_1'(u_{im})$；当$3^{n-1}\le i<2\cdot 3^{n-1}$时，有$s_{im}=T_{20}'(u_{im})$；当$2\cdot 3^{n-1}\le i<3^n$时，$s_{im}=T_{21}'(u_{im})$。若我们重新记 $s^\infty=(s_0,s_1,s_2,\cdots,s_{3k},s_{3k+1},s_{3k+2},\cdots)$ 和$u^\infty=(u_0,u_1,u_2,\cdots,u_{3k},u_{3k+1},u_{3k+2},\cdots)$分别与上述所记的$s^\infty$和$u^\infty$一一对应，则此时有：当$0\le i<3^{n-1}$时，有$s_i=T_1'(u_i)$；当$3^{n-1}\le i<2\cdot 3^{n-1}$时，有$s_i=T_{20}'(u_i)$；当$2\cdot 3^{n-1}\le i<3^n$时，有$s_i=T_{21}'(u_i)$。

由前述定理1和上边的记法可得下面的式子是成立的，即有

$$\begin{aligned}0=T'(0)&=T'\left(\sum_{i=0}^{3^n-\lfloor\frac{n-3}{4}\rfloor-1}c_iu_i\right)\\&=T'_1\left(\sum_{i=0}^{3^{n-1}-1}c_iu_i\right)+T'_{20}\left(\sum_{i=3^{n-1}}^{2\cdot 3^{n-1}-1}c_iu_i\right)\\&\quad+T'_{21}\left(\sum_{i=2\cdot 3^{n-1}}^{3^n-\lfloor\frac{n-3}{4}\rfloor-1}c_iu_i\right)\\&=\sum_{i=0}^{3^{n-1}-1}c_iT'_1(u_i)+\sum_{i=3^{n-1}}^{2\cdot 3^{n-1}-1}c_iT'_{20}(u_i)\\&\quad+\sum_{i=2\cdot 3^{n-1}}^{3^n-\lfloor\frac{n-3}{4}\rfloor-1}c_iT'_{21}(u_i)\\&=\sum_{i=0}^{3^{n-1}-1}c_is_i+\sum_{i=3^{n-1}}^{2\cdot 3^{n-1}-1}c_is_i+\sum_{i=2\cdot 3^{n-1}}^{3^n-\lfloor\frac{n-3}{4}\rfloor-1}c_is_i\\&=\sum_{i=0}^{3^n-\lfloor\frac{n-3}{4}\rfloor-1}c_is_i=0\end{aligned} \tag{17}$$

由以上的讨论可以得到以下定理4。

定理4　新型自缩控序列(SSC(模3)-序列)s^∞的线性复杂度上界为

$$L(s^\infty)\le 3^n-\lfloor(n-3)/4\rfloor-1 \tag{18}$$

定理5　新型自缩控序列(SSC(模3)-序列)s^∞的线性复杂度下界为$L(s^\infty)>3^{2\cdot\lfloor n/3\rfloor-1}$。

证明　设$g(x)$为序列s^∞的极小多项式，利用序列的极小多项式整除特征多项式，来证$L(s^\infty)>3^{2\cdot\lfloor n/3\rfloor-1}$，若有$L(s^\infty)\le 3^{2\cdot\lfloor n/3\rfloor-1}$，那么由$1-x^{3^{2\cdot\lfloor n/3\rfloor-1}}=(1-x)^{3^{2\cdot\lfloor n/3\rfloor-1}}$，且$g(x)|(1-x)^{3^{2\cdot\lfloor n/3\rfloor-1}}$，得$P(s^\infty)\le 3^{2\cdot\lfloor n/3\rfloor-1}$，与已知的$P(s^\infty)\ge 3^{2\cdot\lfloor n/3\rfloor}$相矛盾，所以$L(s^\infty)>3^{2\cdot\lfloor n/3\rfloor-1}$。　证毕

本文从上边讨论的结果中可以看出：与文献[12–16]中的序列相比，本文中的新型自缩控序列(SSC(模3)-序列)s^∞不但周期有更大的提高，而且线性复杂度也有较大的提高，且有以下几点优势。

(1) 文献[13]中改进的自收缩序列模型是由$a_{3k}\oplus a_{3k+1}$的值来决定该括号内输出比特的个数，但是该序列模型当$a_{3k}\oplus a_{3k+1}=1$时，只输出1个比特，而在本文的模型上，不仅增加了元素相加的项，而且还分类输出，当$a_{3k}\oplus a_{3k+1}\oplus a_{3k+2}=1$时，输出1个比特；当$a_{3k}\oplus a_{3k+1}\oplus a_{3k+2}=2$时，输出2个比特，因而得到的序列周期提高很多；

(2) 文献[15]中GF(3)上多位自收缩序列的模型，只是由a_{3k}的值来决定所在分组是否有输出，但a_{3k}的所在分组中至多输出1个比特，且当$a_{3k}=0$时，没有输出；而本文中的模型是根据$a_{3k}\oplus a_{3k+1}\oplus a_{3k+2}$的取值来决定该括号内的输出比特个数，更好地弥补$a_{3k}=0$时$a^{\infty}$收缩过多的不足，所得到的自缩控序列整体上的平衡性更优；

(3) 本文中的自缩控序列(SSC(模3)-序列)的周期整除3^n，这里是对文献[12,18]的研究方法进行改进，并在取最小周期为3^n的情况下，通过探究，得到了自缩控序列(SSC(模3)-序列)线性复杂度更精确的上界值：$3^n-\lfloor(n-3)/4\rfloor-1$。

(4) 通过此种方式得到的自缩控序列的信息利用率更高，达到1/3，与之前了解过的自缩序列模型相对比，信息利用率明显提高，使原来的数据得到了更充分的利用。

4 结束语

伪随机序列在通信加密、雷达信号设计和编码技术等很多领域中有着广泛的应用。在这些应用中，通常要求序列具有大的周期和高的线性复杂度。衡量伪随机性的指标主要有周期、平衡性、线性复杂度和自相关性等。本文所设计的密码序列，主要是从周期、线性复杂度这两个安全指标来分析所构造序列的安全性，本文基于m-序列构造的新型自缩控序列，从整体上研究了该序列的周期及线性复杂度，分析结果发现新型自缩控序列具有更大的周期和较高的线性复杂度。虽然输出不规则，但是破坏了序列的代数结构，由此输出的序列隐蔽性较好且防攻击能力较强，从安全性指标来看，新型自缩控序列具有较好的密码学性质，是一种较好的伪随机序列。接下来可以进一步研究新型自缩控序列的游程分布、自相关性等密码学特性，完善理论结果，为自缩控序列在各领域的应用提供更好的理论基础。

参 考 文 献

[1] 杜小妮, 李丽, 张福军. 基于模$2p^m$的欧拉商的二元序列的线性复杂度[J]. 电子与信息学报, 2019, 41(12): 3000–3005. doi: 10.11999/JEIT190071.

DU Xiaoni, LI Li, and ZHANG Fujun. Linear complexity of binary sequences derived from euler quotients modulo $2p^m$[J]. *Journal of Electronics & Information Technology*, 2019, 41(12): 3000–3005. doi: 10.11999/JEIT190071.

[2] 王艳, 薛改娜, 李顺波, 等. 一类新的周期为$2p^m$的q阶二元广义分圆序列的线性复杂度[J]. 电子与信息学报, 2019, 41(9): 2151–2155. doi: 10.11999/JEIT180884.

WANG Yan, XUE Gaina, LI Shunbo, *et al*. The linear complexity of a new class of generalized cyclotomic sequence of order q with period $2p^m$[J]. *Journal of Electronics & Information Technology*, 2019, 41(9): 2151–2155. doi: 10.11999/JEIT180884.

[3] YANG Bo, DU Tianqi, and XIAO Zibi. Linear complexity of generalized cyclotomic binary sequences of period pq[J]. *Journal.of Mathematics*, 2020, 40(2): 139–148. doi: 10.13548/j.sxzz.2020.02.004.

[4] 李瑞芳, 柯品惠. 一类新的周期为$2pq$的二元广义分圆序列的线性复杂度[J]. 电子与信息学报, 2014, 36(3): 650–654. doi: 10.3724/SP.J.1146.2013.00751.

LI Ruifang and KE Pinhui. The linear complexity of a new class of generalized cyclotomic sequence with period $2pq$[J]. *Journal of Electronics & Information Technology*, 2014, 36(3): 650–654. doi: 10.3724/SP.J.1146.2013.00751.

[5] 杜小妮, 赵丽萍, 王莲花. Z_4上周期为$2p^2$的四元广义分圆序列的线性复杂度[J]. 电子与信息学报, 2018, 40(12): 2992–2997. doi: 10.11999/JEIT180189.

DU Xiaoni, ZHAO Liping, and WANG Lianhua. Linear complexity of quaternary sequences over Z_4 derived from generalized cyclotomic classes modulo $2p^2$[J]. *Journal of Electronics & Information Technology*, 2018, 40(12): 2992–2997. doi: 10.11999/JEIT180189.

[6] 仲燕, 张胜元, 柯品惠. 一类新的周期为$2p^m$的四元广义分圆序列的线性复杂度研究[J]. 福建师范大学学报: 自然科学版, 2020, 36(1): 7–11. doi: 10.12046/j.issn.1000-5277.2020.01.002.

ZHONG Yan, ZHANG Shengyuan, and KE Pinhui. Research on linear complexity of a new class of quaternary generalized cyclotomic sequence with period $2p^m$[J]. *Journal of Fujian Normal University: Natural Science Edition*, 2020, 36(1): 7–11. doi: 10.12046/j.issn.1000-5277.2020.01.002.

[7] 陈智雄, 吴晨煌. 关于二元割圆序列的k-错线性复杂度[J]. 通信学报, 2019, 40(2): 197–206. doi: 10.11959/j.issn.1000-436x.2019034.

CHEN Zhixiong and WU Chenhuang. k-error linear complexity of binary cyclotomic generators[J]. *Journal on Communications*, 2019, 40(2): 197–206. doi: 10.11959/j.issn.1000-436x.2019034.

[8] 刘龙飞, 杨晓元, 陈海滨. 周期为p^m的广义割圆序列的$\frac{p-1}{2}$-错线性复杂度[J]. 电子与信息学报, 2013, 35(1): 191–195. doi: 10.3724/SP.J.1146.2012.00837.

LIU Longfei, YANG Xiaoyuan, and CHEN Haibin. On the $\frac{p-1}{2}$-error linear complexity of generalized cyclotomic

sequence with length p^m[J]. *Journal of Electronics & Information Technology*, 2013, 35(1): 191–195. doi: 10.3724/SP.J.1146.2012.00837.

[9] 吴晨煌, 许春香, 杜小妮. 周期为p^2的q元序列的k-错线性复杂度[J]. 通信学报, 2019, 40(12): 21–28. doi: 10.11959/j.issn.1000-436x.2019230.

WU Chenhuang, XU Chunxiang, and Du Xiaoni. k-error linear complexity of q-ary sequence of period p^2[J]. *Journal on Communications*, 2019, 40(12): 21–28. doi: 10.11959/j.issn.1000-436x.2019230.

[10] 陈智雄, 牛志华, 吴晨煌. 周期为素数平方的二元序列的k-错线性复杂度[J]. 密码学报, 2019, 6(5): 574–584. doi: 10.13868/j.cnki.jcr.000323.

CHEN Zhixiong, NIU Zhihua, and WU Chenhuang. On k-error linear complexity of prime-square periodic binary sequences[J]. *Journal of Cryptologic Research*, 2019, 6(5): 574–584. doi: 10.13868/j.cnki.jcr.000323.

[11] MEIER W and STAFFELBACH O. The self-shrinking generator[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Perugia, Italy, 1994: 205–214.

[12] BLACKBURN S R. The linear complexity of the self-shrinking generator[J]. *IEEE Transactions on Information Theory*, 1999, 45(6): 2073–2077. doi: 10.1109/18.782139.

[13] KANSO A. Modified self-shrinking generator[J]. *Computers and Electrical Engineering*, 2010, 36(5): 993–1001. doi: 10.1016/j.compeleceng.2010.02.004.

[14] 王锦玲, 邹慧仙. 关于m-序列模加实现的自缩序列[J]. 计算机工程与应用, 2015, 51(19): 110–113. doi: 10.3778/j.issn.1002-8331.1310-0089.

WANG Jinling and ZOU Huixian. Self-shrinking sequence with modular addition on m-sequence[J]. *Computer Engineering and Applications*, 2015, 51(19): 110–113. doi: 10.3778/j.issn.1002-8331.1310-0089.

[15] 王锦玲, 王娟, 陈忠宝. GF(3)上多位自收缩序列的模型与研究[M]. 何大可, 黄月江. 密码学进展——China Cypt'2007: 中国密码学会2007年会论文集. 成都: 西南交通大学出版社, 2007: 299–300.

WANG Jinling, WANG Juan, and CHEN Zhongbao. The model and studying of multi-self-shrinking sequences on GF(3)[M]. HE D K, HUANG Y J. Progress on Cryptography——China Cypt'2007: Proceedings of 2007 Annual Meeting of Chinese Cryptology Society. Chengdu: Southwest Jiaotong University Press, 2007: 299–300.

[16] 王锦玲, 陈亚华, 兰娟丽. 扩展在上$GF(3)$新型自缩序列模型及研究[J]. 计算机工程与应用, 2009, 45(35): 114–119. doi: 10.3778/j.issn.1002-8331.2009.35.035.

WANG Jinling, CHEN Yahua, and LAN Juanli. New model and studying of self-shrinking sequence developed on $GF(3)$[J]. *Computer Engineering and Applications*, 2009, 45(35): 114–119. doi: 10.3778/j.issn.1002-8331.2009.35.035.

[17] 胡予璞, 张玉清, 肖国镇. 对称密码学[M]. 北京: 机械工业出版社, 2002: 66–74.

HU Y P, ZHANG Y Q, XIAO G Z. Symmetric Key Cryptography[M]. Beijing: Machinery Industry Press, 2002: 66–74.

[18] 王慧娟, 王锦玲. $GF(q)$上广义自缩序列的线性复杂度[J]. 电子学报, 2011, 39(2): 414–418.

WANG Huijuan and WANG Jinling. The linear complexity of the generalized self-shrinking generator on $GF(q)$[J]. *Acta Electronica Sinica*, 2011, 39(2): 414–418.

[19] LIDL R and NIEDERREITER H. Finite Fields[M]. Reading, US: Addison-Wesley Publishing Company, 1983: 271–272.

王锦玲：女，1963年生，教授，硕士生导师，研究方向为代数学、密码学.

崔静静：女，1995年生，硕士生，研究方向为代数学、密码学.

责任编辑：余　蓉