关于"停走"生成器输出序列的中心极限定理*

黄晓英 李世取

(信息工程大学信息安全学院 郑州 450002)

E-mail: huangxy@zhengzhou.cgw.net.cn

摘要 建立了"停走"生成器输出序列的概率模型,讨论了由这类序列构成的随机变量序列的概率分布、独立性、数学期望和方差等概率性质,在得到此类随机变量序列是强平稳的和 α 混合的这一结论的基础上证明了它们服从中心极限定理.

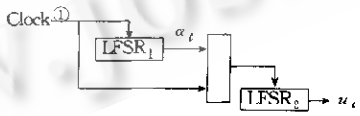
关键词 "停走"生成器,随机变量,强平稳,α-混合序列,中心极限定理.

中图法分类号 TP301

人们对钟控序列的研究始于 Kjeldsen 和 Jennings[1]. 他们分别提出了级联序列和复合序列的概念,人们称这类序列为钟控序列. 人们对钟控序列的研究表明,钟控序列因其所具有的较高的、较稳定的球性复杂度和较强的伪随机性而具有密码学的应用价值. 而"停走"生成器[2]作为一种基本的钟控生成器,由于对它目前尚无有效的相关攻击方法[3],因此,它常常是作为较复杂的钟控生成器(如袭特生成器[4]、钟控非线性组合生成器[3]、钟控滤波生成器[4]等)的基本构件. 可见,分析"停走"生成器输出序列的性质、特征和其相关序列之间的关系是研究其他生成器输出序列的基础和条件. 我们试图用概率的方法对"停走"生成器输出序列的基本性质和特征进行必要的分析和研究,希望能以此从概率的角度说明为什么"停走"生成器的输出序列具有良好的密码学价值,从而为进一步分析钟控序列的性质、特征和应用价值奠定基础. 而中心极限定理作为概率论的基本理论,是考察随机变量序列诸多性质的前提和条件. 因此,本文首先利用"停走"生成器输出序列的伪随机性来建立"停走"生成器的概率模型,并验证此序列是强平稳的[5]和 α-混合[6]的这样一种相依随机变量序列,最后证明此序列服从中心极限定理. 本文的工作为今后进一步讨论和分析"停走"生成器输出序列的弱不变原理及其收敛的速度奠定了必要的基础.

1 "停走"生成器的概率模型

"停走"生成器由两个线性反馈移位寄存器(LFSR)组成,其中一个 LFSR 和一个时钟用来控制另一个 LFSR. 其构造如图 1 所示[3].



①时钟.

Fig. 1
图1

假定 $LFSR_1$ 的输出序列为 $\{a_t\}$,$LFSR_2$ 的输出序列为 $\{b_t\}$. 那么,"停走"生成器的输出序列 $\{u_t\}$ 可表示为[3]

---

* 作者黄晓英,女,1962 年生,讲师,主要研究领域为概率统计的密码学应用. 李世取,1945 年生,教授、博士生导师,主要研究领域为概率统计的密码学应用.

本文通讯联系人:黄晓英,郑州 450002,信息工程大学信息安全学院

本文 2000-05-31 收到原稿,2000-06-30 收到修改稿

$$\begin{cases} v_0 = b_0 \\ v_t = b_{t-1}, & t \geqslant 1. \end{cases}$$

由于许多具有实用性的LFSR的输出序列都具有良好的伪随机性,因此,可以利用随机变量序列的概念来讨论"停走"生成器的输出序列的概率性质.

设 $a^\infty = \{a_0, a_1, a_2, \ldots\}, b^\infty = \{b_0, b_1, b_2, \ldots\}$ 都是同一概率空间 (Ω, F, P) 上取值为0,1的独立随机变量序列,且满足:

(1) 对一切 $i \geqslant 0$,都有

$$P\{a_i = 0\} = P\{a_i = 1\} = P\{b_i = 0\} = P\{b_i = 1\} = \frac{1}{2};$$

(2) a^∞ 与 b^∞ 之间也是相互独立的,

$$\begin{cases} u_0 = b_0 \\ u_n = b_{n-1}, & n \geqslant 1. \end{cases} \qquad (*)$$

这里,$\sum$ 表示在实数域上求和,则产生的序列为

$$u^\infty = \{u_0, u_1, \ldots, u_n, \ldots\} = \{b_0, b_{a_0}, b_{a_0+a_1}, \ldots, b_{a_0+a_1+\ldots+a_{n-1}}, \ldots\}.$$

易见,u_n 是以 $a_0, a_1, \ldots, a_{n-1}; b_0, b_1, \ldots, b_n$ 为自变量的复合函数,它显然关于由 $a_0, a_1, \ldots, a_{n-1}; b_0, b_1, \ldots, b_n$ 生成的 σ-代数[6]可测.因而 u^∞ 仍是同一概率空间 (Ω, F, P) 上的取值为0,1的随机变量序列.故可以利用 a^∞ 与 b^∞ 的一系列概率性质来考察 u^∞ 是否服从中心极限定理.

2 u^∞ 是强平稳α-混合相依随机变量序列

由于"停走生成器"的输出序列所产生的随机变量序列是同分布的,但不是相互独立的[7],因此,为了利用混合相依随机变量的极限理论考查这类随机变量序列是否服从中心极限定理,首先必须考察它们的平稳性和混合性.

定理1[7]. 设 $a^\infty = \{a_0, a_1, a_2, \ldots\}, b^\infty = \{b_0, b_1, b_2, \ldots\}$ 都是同一概率空间 (Ω, F, P) 上取值为0,1的独立随机变量序列,且满足:

(1) 对一切 $i \geqslant 0$,都有

$$P\{a_i = 0\} = P\{a_i = 1\} = P\{b_i = 0\} = P\{b_i = 1\} = \frac{1}{2};$$

(2) a^∞ 与 b^∞ 之间也相互独立.若 $u_n (n \geqslant 0)$ 的定义如式(*),则对一切 $n \geqslant 0$,都有

$$P\{u_n = 0\} = P\{u_n = 1\} = \frac{1}{2}. \qquad (1)$$

定理2[7]. 设条件同定理1,则对一切 n 和 $k (n \geqslant 0, k \geqslant 1)$,都有

$$P\{u_n = i, u_{n+k} = j\} \to \begin{cases} \dfrac{2^k+1}{2^{k+2}}, & i = j \\ \dfrac{2^k-1}{2^{k+2}}, & i \neq j \end{cases} = \frac{2^k + (-1)^{i+j}}{2^{k+2}}. \qquad (2)$$

显然,式(2)表明了 $\{u_n\}$ 不是独立的随机变量序列.利用上述结果容易得到以下数字特征.

定理3[7]. 设条件同定理1,则对一切 $n \geqslant 0, k \geqslant 1$,都有

(1) 数学期望 $E(u_n) = \frac{1}{2}$;

(2) 方差 $D(u_n) = \frac{1}{4}$;

(3) $E(u_n u_{n+k}) = \frac{2^k+1}{2^{k+2}}$;

(4) 相关系数 $\rho(u_n,u_{n+k})=\frac{1}{2^k}$, $n\geqslant 0,k\geqslant 1$.

定理 4. 设条件同定理 1,则 u^∞ 是强平稳的.

证明:由定理 2 可得,u_n 的 $k(k\geqslant 1)$步转移概率为

$$p_{ij}^{(k)}=P\{u_{n+k}=j\mid u_n=i\}=2P\{u_{n+k}=j,u_n=i\}=\frac{1}{2}+\frac{(-1)^{i+j}}{2^{k+1}},$$

故根据随机变量的联合分布与转移概率的关系式[8]:

$$P\{u_{n_1}=i_1,\dots,u_{n_k}=i_n\}=P\{u_{n_1}=i_1\}p_{i_1i_2}^{(n_2-n_1)}\cdots p_{i_{k-1}i_k}^{(n_k-n_{k-1})}=\frac{1}{2}p_{i_1i_2}^{(n_2-n_1)}\cdots p_{i_{k-1}i_k}^{(n_k-n_{k-1})}$$

及 $p_{ij}=\frac{2+(-1)^{i+j}}{4}$,就有对一切自然数 n,

$$P\{u_0=i_0,u_1=i_1,\dots,u_k=i_k\}=P\{u_n=i_0,u_{n+1}=i_1,\dots,u_{n+k}=i_k\}$$

成立. 故 u^∞ 是强平稳的. □

定义 1[6]. 设$\{X_n,n\geqslant 1\}$是定义在概率空间(Ω,F,P)上的随机变量序列,若

$$\alpha(n)=\sup_{k\in N}\alpha(F_1^k,F_{k+n}^\infty)\to 0,n\to\infty,$$

其中 $\alpha(F_1^k,F_{k+n}^\infty)=\sup_{A\in F_1^k,B\in F_{n+k}^\infty}|P(AB)-P(A)P(B)|$, $F_1^k=\sigma(X_1,\dots,X_k)$, $F_{n-k}^\infty=\sigma(X_{n+k},X_{n+k+1},\dots,)$为 F 的子 σ-代数,则序列$\{X_n,n\geqslant 1\}$是 α-混合或强混合的.

定理 5. u^∞ 是 α-混合的随机变量序列.

证明:记 $I_1\subset\{1,2,\dots,2^{k-1}\}$, $I_2\subset\{1,2,\dots,2^l\}$, $I_1\cup I_2\neq\varnothing$,又记

$$\{(a_1,a_2,\dots,a_{k-1});a_j=0,1,0\leqslant j\leqslant k-1\}\triangleq\{(a_1^{(i)},a_2^{(i)},\dots,a_{k-1}^{(i)});i=1,2,\dots,2^{k-1}\},$$

$$\{(b_1,a_2,\dots,b_l);a_i=0,1,0\leqslant i\leqslant l\}\triangleq\{(b_1^{(j)},b_2^{(j)},\dots,b_l^{(j)});j=1,2,\dots,2^l\}.$$

第 1 步:取 $A=\bigcup_{i\in I_1}\{u_1=a_1^{(i)},\dots,u_{k-1}=a_{k-1}^{(i)},u_k=a\}$,其中 a 取为 0 或 1,则易知 $A\in\sigma(u_1,\dots,u_k)\triangleq F_1^k$,又取 $B=\bigcup_{j\in I_2}\{u_{k+n}=b,u_{k+n+1}=b_1^{(j)},\dots,u_{k+n+l-1}=b_{l-1}^{(j)},u_{k+n+l}=b_l^{(j)}$,其中 b 取为 0 或 1,则同理,$B\in\sigma(u_{k+n},u_{k+n+1},\dots,u_{k+n+l})\triangleq F_{k+n}^{k+n+l}$. 故

$$P(A)=\frac{1}{2}\sum_{i\in I_1}p_{a_1^{(i)}a_2^{(i)}}\cdots p_{a_{k-1}^{(i)}a},\quad P(B)=\frac{1}{2}\sum_{j\in I_2}p_{bb_1^{(j)}}\cdots p_{b_{l-1}^{(j)}b_l^{(j)}},$$

$$P(AB)=\sum_{i\in I_1}\sum_{j\in I_2}P\{u_1=a_1^{(i)}\}p_{a_1^{(i)}a_2^{(i)}}\cdots p_{a_{k-1}^{(i)}a}\cdot p_{ab}^{(n)}\cdot p_{bb_1^{(j)}}\cdots p_{b_{l-1}^{(j)}b_l^{(j)}}=2p_{ab}^{(n)}P(A)P(B).$$

因而,

$$|P(AB)-P(A)P(B)|=|2p_{ab}^{(n)}P(A)P(B)-P(A)(B)|\leqslant 2\left|p_{ab}^{(n)}-\frac{1}{2}\right|.$$

根据定理 4 的结论,$|P(AB)-P(A)P(B)|\leqslant\frac{1}{2^n}$.

第 2 步:对任意 $A\in\sigma(u_1,u_2,\dots,u_k)$, $A\neq\varnothing$,必有

$$A=\Big[\bigcup_{i\in I_{11}}\{u_1=a_1^{(i)},\dots,u_{k-1}=a_{k-1}^{(i)},u_k=0\}\Big]\cup\Big[\bigcup_{i\in I_{12}}\{u_1=a_1^{(i)},\dots,u_{k-1}=a_{k-1}^{(i)},u_k=1\}\Big]\triangleq A_1\cup A_2,$$

其中 $I_{11}\subset\{1,2,\dots,2^{k-1}\}$, $I_{12}\subset\{1,2,\dots,2^{k-1}\}$,且 $I_{11}\cup I_{12}\neq\varnothing$.

同样地,对任意 $B\in\sigma(u_{k+n},u_{k+n+1},\dots,u_{k+n+l})$, $B\neq\varnothing$,也必有

$$B=\Big[\bigcup_{j\in I_{21}}\{u_{k+n}=0,u_{k+n+1}=b_1^{(j)},\dots,u_{k+n+l}=b_l^{(j)}\}\Big]\cup$$

$$\Big[\bigcup_{i\in I_{22}}[u_{k+n}=1,u_{k+n+1}=b_1^{(j)},\dots,u_{k+n+l-1}=b_{l-1}^{(j)},u_{k+n+l}=b_l^{(j)}]\Big]\triangleq B_1\cup B_2,$$

其中 $I_{21}\subset\{1,2,\dots,2^{l-1}\}$, $I_{22}\subset\{1,2,\dots,2^{k-1}\}$,且 $I_{21}\cup I_{22}\neq\varnothing$,则根据第 1 步的结果可知:

$$P(A_1B_1)=2p_{00}^{(n)}P(A_1)P(B_1);\quad P(A_1B_2)=2p_{01}^{(n)}P(A_1)P(B_2);$$

$$P(A_2B_1)=2p_{10}^{(n)}P(A_2)P(B_1);\quad P(A_2B_2)=2p_{11}^{(n)}P(A_2)P(B_2).$$

于是,$|P(AB)-P(A)P(B)|\leqslant\frac{1}{2^{n-2}}$.

第3步:对任意 $A\in\sigma(u_1,u_2,\ldots,u_k)$,$B\in\sigma(u_{k+n},u_{k+n-1},\ldots)$,$A\cup B\neq\varnothing$,取 $B_l\in B\cap\sigma(u_{k+n},u_{k+n+1},\ldots,u_{k+n+l})$,则 B_l 为单调减集列,且 $B=\lim\limits_{l\to\infty}B_l=\bigcap\limits_{l=1}^{\infty}B_l$.

根据概率的连续性易知 $P(AB)=\lim\limits_{l\to\infty}P(AB_l)$;$P(B)=\lim\limits_{l\to\infty}P(B_l)$. 故

$$|P(AB)-P(A)P(B)|=\lim_{l\to\infty}|P(AB_l)-P(A)P(B_l)|\leqslant\lim_{l\to\infty}\frac{1}{2^{n-2}}=\frac{1}{2^{n-2}},$$

综上可得 $\forall k\in N$,$\alpha(F_1^k,F_{n+k}^{\infty})=\sup\limits_{A\in F_1^k,B\in F_{n+k}^{\infty}}|P(AB)-P(A)P(B)|\leqslant\frac{1}{2^{n-2}}\xrightarrow{n\to\infty}0$,所以 $\alpha(n)\xrightarrow{n\to\infty}0$,即 $\{u_n,n\geqslant1\}$ 是 α-混合的. □

3　u^{∞}服从中心极限定理

引理 1[6]. 设 $\{X_n,n\geqslant1\}$ 是强平稳的 α-混合序列,满足 $EX_1=0$ 及 $\sum\limits_{n=1}^{\infty}\alpha(n)<\infty$,那么 $\sigma^2\triangleq EX_1^2+2\sum\limits_{j=2}^{\infty}EX_1X_j<\infty$,且当 $\sigma\neq0$ 时,$\frac{S_n}{\sigma\sqrt{n}}\xrightarrow{d}N(0,1)$,其中 $S_n=\sum\limits_{k=1}^{n}X_k$.

引理 2[8]. 设 $a_n,n=1,2,\ldots$ 是实数序列,且 $\sum\limits_{n=1}^{\infty}a_n$ 收敛,则 $\lim\limits_{n\to\infty}\frac{1}{n}\sum\limits_{i=1}^{n}ia_i=0$.

引理 3. 若 $\{X_n,n\geqslant1\}$ 满足引理1的条件,则 $\{X_n,n\geqslant1\}$ 服从中心极限定理.

证明:为证 $\{X_n,n\geqslant1\}$ 服从中心极限定理,只需证 $\frac{\sigma_n^2}{n}\to\sigma^2$ 即可,其中 $\sigma_n^2=D(S_n)$. 其实,根据 $\{X_n,n\geqslant1\}$ 的平稳性,

$$\sigma_n^2=D(S_n)=N\left\{EX_1^2+2\left[\left(1-\frac{1}{n}\right)EX_1X_2+\left(1-\frac{2}{n}\right)EX_1X_3+\ldots+2EX_1X_{n-1}+EX_1X_n\right]\right\},$$

$$\sigma^2=EX_1^2+2\sum_{j=2}^{n}EX_1X_j+2\sum_{j=n+1}^{\infty}EX_1X_j,$$

故由 σ^2 的收敛性及引理2得 $\frac{\sigma_n^2}{n}-\sigma^2\to0$. □

引理 4. 设 $f_n(x),f(x)$ 为实函数,$f(x)$ 连续且满足 $f_n(x)\xrightarrow{[1]}f(x)$,则当 $x_n\to x$ 时,有 $f_n(x_n)\to f(x)$.

定理 6. "停走"生成器的输出序列 $\{u_n,n\geqslant1\}$ 服从中心极限定理.

证明:令 $X_n=u_n-Eu_n,n\geqslant1$,则 $D(X_n)=\frac{1}{4}$,$E(X_nX_{n+k})=\frac{1}{2^{k+2}}$. 根据强混合的证明可知,$0\leqslant\alpha(n)-\sup\limits_{k\in N}\alpha(F_1^k,F_{k+n}^{\infty})\leqslant\frac{1}{2^{n-2}}$,故 $\sum\limits_{n=1}^{\infty}\alpha(n)\leqslant4$.

由引理1,$\frac{S_n}{\sigma\sqrt{n}}\xrightarrow{d}N(0,1)$,注意到 $P\left\{\frac{S_n}{\sigma\sqrt{n}}<x\right\}=P\left\{\frac{S_n}{\sigma_n}<\frac{\sigma\sqrt{n}}{\sigma_n}x\right\}$ 及引理4即得. □

4　结束语

至此,我们对"停走"生成器的输出序列的数字特征、平稳性和相依性问题进行了研究,并利用平稳性和相依性得到了此序列服从中心极限定理的结论. 所得结果有助于我们对此序列的弱不变原理、依分布收敛的速度等问题做进一步的相关分析. 我们的体会是:在建立了"停走"生成器的概率模型后,利用概率的方法对其相关序列进行考察是有效的,利用类似的方法,还可以研究和探讨此类序列的其他诸如相关性、马氏性及服从强大数定理[7]等重要概率性质. 值得指出的是,在证明了序列的马尔可夫性后,利用马氏链的一些结论,也可得到本文的结果,我们将另文叙述. 此外,类似的方法还可以应用于建立衮特生成器的概率模型和对其性质的研究.

参考文献

1　Jennings S M. A special class of binary sequences [Ph.D. Thesis]. London: Westfield College, London University, 1980

2 Beth T, Piper F C. The stop-and-go generator. In: Goos G, Hartmanis J eds. Advances in Cryptology——Proceedings of Eurocrypt'84. Berlin: Springer-Verlag, 1985. 88～92

3 Ding Cun-sheng, Xiao Guo-zhen. Theory of stream cipher and practice. Beijing: National Defense Publishing House, 1994. 189～204
(丁存生,肖国镇.流密码学及其应用.北京:国防工业出版社,1994. 189～204)

4 Gunther C G. A generator of pseudorandom sequences with clock controlled linear feedback shift register. In: Advances in Cryptology——Eurocrypt'87. Berlin: Springer-Verlag, 1988. 5～14

5 Li Zhang-nan, Wu Rong. The theory of random processes. Beijing: Higher Education Press, 1987
(李漳南,吴荣.随机过程论.北京:高等教育出版社,1987)

6 Lu Chuan-rong, Lin Zheng-yan. The limit theorem for mixing and dependant variables. Beijing: Science Press, 1997
(陆传荣,林正炎.混合相依变量的极限理论.北京:科学出版社,1997)

7 Huang Xiao-ying, Li Shi-qu. The law of great numbers in the output-sequences of the stop-and-go generator. Journal of Information Engineering University, 2000,1(2):5～9
(黄晓英,李世取.关于"停走"生成器输出序列的大数定律.信息大学学报,2000,1(2):5～9)

8 Zhongshan University. The basis of measure and probability. Guangzhou: Guangdong Science and Tehnology Press, 1984
(中山大学.测度与概率基础.广州:广东科技出版社,1984)

Central Limit Theorem in Output-Sequences of Stop-and-Go Generator

HUANG Xiao-ying LI Shi-qu

(Information and Security College Information and Engineering University Zhengzhou 450002)

Abstract In this paper, the authors construct the probabilistic model of output sequences of the stop-and-go generator, and discuss the distribution, independency, expected value and variance of the random variables composed by this kind of sequences. It is proved that these random variables are strong stationary and α-mixing random sequences, and these sequences obey the central limit theorem.

Key words Stop-and-Go generator, random variable, strong stationary, α-mixing sequence, central limit theorem.