一种混沌密码序列周期特性检测新方法*

郑艳斌[1)] 宋煜[2)] 杜宝祥[1)] 潘晶[1)] 丁群[1)†]

1) (黑龙江大学电子工程学院, 哈尔滨 150080)

2) (哈尔滨工业大学计算机学院, 哈尔滨 150001)

(2012 年 4 月 1 日收到; 2012 年 6 月 18 日收到修改稿)

针对数字混沌密码序列发生器产生的二值序列局部范围内存在的周期特性评价难问题, 提出一种新的周期特性分析方法 ——BSPD (binary sequence's periodic detection) 方法, 用于评价二值序列具有的周期特性. 该方法除可用于检测二值序列是否存在精确周期, 或在部分时域范围内存在周期现象; 还可检测出序列局部出现的周期性重叠模板, 用于具体分析二值序列中周期现象的统计特征. 一个基于经典 Logistical 映射的 BSPD 检验表明, 该方法可以有效地定位一个类似随机混沌二值序列中蕴含的周期现象.

关键词: 混沌, 二值序列, 周期, 检测

PACS: 05.45.–a, 02.30.Lt, 43.55.Cs, 02.60.–x

1 引 言

混沌系统由于具有良好的统计特性、初值敏感性和伪随机性, 使得其在通信系统和加密系统的设计方面具有显著优势 [1−4], 这主要表现在混沌系统采用某些计算代价很小的方法, 就可能得到随机性较高的二值序列 [4,5]. 目前由混沌系统获取二值序列的关键因素可概括为两个方面 [6−18]: 一是混沌系统演化过程中的计算精度, 如浮点精度、定点精度和字长精度等; 二是混沌映射过程与二值序列之间的映射关系即量化方法. 数字混沌系统在由模拟转向数字的过程中, 其统计特性和随机性将会发生变化.

早在 1997 年 Kohda 和 Tsuneda 已经考虑到计算精度对混沌序列随机性的影响 [19]. 后来的文献 [20−24] 中也提到由于动力学退化数字混沌序列最终将演化为一个周期序列, 文献 [24] 则明确指出由于计算精度的问题会导致混沌序列退化到 "0 序列". 相较其他类型的随机数生成器, 数字系统的截断误差和舍入误差对混沌随机数生成器的影响更加明显. 这使得一些通信系统或加密系统仅应用混沌序列的某个局部时, 其随机性和安全性受到一定的威胁. 目前很多研究者 [25−29] 利用一些常见的随机性检验标准, 如 SP800-22[30] 和 TestU01[31,32], 来研究上述因素对混沌序列的影响. 一些具有良好随机性的混沌序列生成器 [16−18] 随之产生. 然而, 人们在关注序列随机性的同时, 往往忽略了序列还应具有的稳定性. 一些整体上看似随机性良好的混沌序列往往在局部范围内分布着大量的周期性出现的 "0" "1" 编码块. 文献 [33] 从加密应用角度提醒我们, 除了关注序列随机性还应关注序列稳定性对混沌序列加密应用的影响. 由此, 讨论数字混沌序列局部范围内的周期现象具有实际意义.

根据文献 [5, 15, 19, 22, 25, 26, 29—33], 我们将现有的周期检测方法归纳为两类: 一类是针对序列精确周期和近似周期现象的检验方法, 如自相关函数、傅里叶变换、功率谱以及各种熵的分析法. 另一类是基于周期模板的检验与挖掘方法. 这两类方法在评价序列周期现象时, 均只能针对在序列全局出现的周期现象给出响应, 应用范围较小. 目前, 讨论数字混沌序列局部范围内与某些潜在的周期特

* 国家自然科学基金 (批准号: 60672011) 资助的课题.

† E-mail: qunding@yahoo.cn

性相关的研究较少, 特别是缺乏对二值数字混沌序列在局部范围内存在的周期现象的分析、讨论和检测方法.

本文依据二值随机序列自身涵含的逻辑联系, 首先提出了一种扩展的周期现象定义, 使得精确周期现象、近似周期现象和仅在序列局部出现的周期现象均可以作为这种定义的特例. 其次, 按照所提出的定义, 证明了随机序列局部范围内出现的周期现象的统计特性, 并在二值随机序列的局部周期特性与特定重构序列的游程特性之间建立了对应关系. 最后, 根据这种对应关系, 结合广泛应用的 SP800-22 中针对游程特性的测试方法, 给出了检测序列周期现象的一种新方法, 即 BSPD (binary sequence's periodic detection) 方法. 该方法不但可以判断二值序列是否具有精确周期现象、近似周期现象, 还能够对序列局部范围内的周期现象进行分析和检测, 从而定位实验序列的局部周期模板, 判定其是否能导致混沌序列在某个局部出现低随机性、低安全性等问题, 即检测序列是否存在显著的周期现象.

2 周期现象评测原理

在本文中, 我们令 N 表示自然数的集合, $\odot$ 表示同或运算, $f(t)$ 表示一个二值序列, $P\{A\}$ 表示事件 A 的概率, $\lfloor K \rfloor$ 表示对小数 K 取整.

2.1 定义扩展的目标

一般意义上, 人们对周期现象的理解为在某一时域范围内, 若序列 $f(t)$ 均有 $f(t+nT)=f(t)$ 存在, 则称序列 $f(t)$ 存在一个严格的 T 周期现象. 按照上述定义, 一方面, 人们很难对二值序列局部范围内周期性出现的符号串进行定量评价. 如图 1 所示, 如果一个由数字混沌系统生成的二值序列仅在某一时域范围内每间隔 11 比特 (bits) 重复出现连续的 5 比特二值串 '10111', 目前就很难通过有效的方法评价.

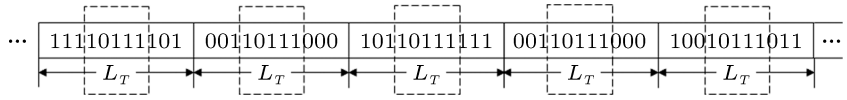

图 1 局部范围内出现的周期现象

另一方面, 混沌系统由于通常具有短期可预测性, 导致在二值混沌序列中必然存在大量的局部周期现象, 从而对序列造成随机性弱化; 同时由于混沌系统的长期不可预测性, 人们很难利用已有的周期现象检测方法和随机性检查方法, 找出这些局部周期现象的统计特征.

例如: 在由经典 Logistic 映射 (1) 式描述的二值混沌序列生成器 [4], (2) 式及 (3) 式反应了 (1) 式中存在的一种短期可预测特性:

$$\begin{cases} x_{n+1}=4x_n(1-x_n), \\ f(n)=\begin{cases} 0, & x_n<c, \\ 1, & x_n\geqslant c, \end{cases} \quad c=0.5. \end{cases} \tag{1}$$

若用 M 比特对其状态进行观察与记录. 假设 Δx_n 为截断误差, X_n 为观察值, (1) 式中任意 x_n 也可用 (2) 式表示:

$$x_n=2^{-M}(X_n+\Delta x_n), \quad -1<\Delta x_n<1. \tag{2}$$

将 (2) 式代入 (1) 式, 则该混沌系统下一状态可以用条件不等式 (3) 进行预测:

$$\begin{aligned} &2^{2-2M}X_n\overline{X_n}-2^{2-M} \\ &\leqslant x_{n+1}\leqslant 2^{2-2M}X_n\overline{X_n}+2^{2-M}, \end{aligned} \tag{3}$$

其观察值必在 $2^{2-M}X_n\overline{X_n}-2^2<X_{n+1}<2^{2-M}X_n\overline{X_n}+2^2$ 范围内.

由 (3) 式可证, 在 $M=32$ 的系统中, 只要系统状态 $0.5<x_n<0.5005$ 时, 符号 "11000000000000000" 将被编入二值序列. 显然在伯努利试验序列中符号 "11000000000000000" 的出现概率要远小于混沌系统处于值域 $0.5<x_n<0.5005$ 的概率, 这使得在经典 Logistic 映射描述的二值混沌序列生成器必然存在一些局部时域, 在这些时域上, 符号 "11000000000000000" 将被反复编入序列, 从而成为局部的随机性弱化区间.

本文针对二值混沌系统可能在局部存在随机性弱化问题, 对周期现象的定义进行扩展, 期望使

一些广泛存在的周期现象及其引起的随机性弱化得到解释与评价.

2.2 周期现象的扩展定义

定义 1 若存在连续的自然数集合 $\phi_\varepsilon = \{\varepsilon_i | 0 \leqslant \varepsilon_1 < \varepsilon_i < \varepsilon_\omega \leqslant L_T, \varepsilon_i \in N, 1 \leqslant i \leqslant \omega, i \in N, L_T \in N\}$, 使得二值序列 $f(t)$ 在 $[L_0, L_n]$ 上, 对于任意的 ε_i 以及 $[1, (L_n - L_0)/L_T]$ 上任意的整数 k, 均有

$$\begin{aligned} & f\left(L_0 + (k-1)\cdot L_T + \varepsilon_i\right) \\ & = f\left(L_0 + k\cdot L_T + \varepsilon_i\right) \odot C, \end{aligned} \tag{4}$$

则称序列 $f(t)$ 在 $[L_0, L_n]$ 上存在一个 L_T 周期现象. "$f(L_0+\varepsilon_1)f(L_0+\varepsilon_2)\cdots f(L_0+\varepsilon_\omega)$" 为该现象中周期性出现的符号串 (以下简称周期模板), 符号串长度 ω 称为周期模板长度. 其中 C 为常数 0 或 1, ε_i 表示周期模板中第 i 位元素在一个周期范围内的相对位置.

1) 若 $L_0 = 0, L_n \to +\infty$ 且 $\varepsilon_i = i$, i 为 $[1, L_T]$ 连续的自然数, (4) 式描述了一个周期为 L_T 的精确周期现象.

2) 若 $L_0 \to 0, L_n \to +\infty$, 且 $\omega \to L_T$, (4) 式描述了一个周期为 L_T 的近似周期现象.

3) 若 $[L_0, L_n]$ 为二值序列中的某一局部, 且 $0 < \omega < L_T$, (4) 式描述了一个在局部范围内周期性出现的局部周期现象.

由上述定义可知, 1) 若一个二值序列存在精确周期现象或近似周期现象, 则该现象均可视为其局部周期现象在 $[L_0, L_n]$ 范围内的某种特例: 2) 若一个二值序列存在精确周期现象或近似周期现象, 则其任意范围内存在的局部周期现象对应的最小周期均不超过已知的精确周期或近似周期.

2.3 周期现象的统计特征

为评价序列存在的周期现象, 本节以二值伯努利实验序列中各种局部周期现象出现次数的数学期望为基本参照, 给出了随机性弱化区间的一种统计特征.

引理 1 在一组二值伯努利试验序列中, 假设 L 为局部周期现象存在的时序区间长度, L_T 为周期, ω 为周期模板长度, 若 $1 \leqslant \omega < L_T \ll L$, 令 $k = \lfloor L/L_T \rfloor$, 则在任意长度为 L 的区间上以 L_T 为周期的局部周期现象出现次数的数学期望为

$$\begin{aligned} E(L, L_T, \omega) = {} & (L_T - \omega - 1)\cdot 2^{-(k-1)\omega} \\ & \times \left(1 - 2^{-k+1}\right)^2 \\ & + 2\cdot 2^{-(k-1)\omega}\cdot\left(1 - 2^{-k+1}\right). \end{aligned} \tag{5}$$

证明 首先讨论二值伯努利实验序列在长度为 L 的区间 $[L_0, L_n]$ 上指定位置出现以 L_T 为周期, 以 ω 为周期模板长度的局部周期现象概率.

假设二值序列 $f(t)$ 为伯努利实验序列, 若 $f(t)$ 在 $[L_0, L_n]$ 上存在周期为 L_T 的 ω 长的周期模板的局部周期现象. 由定义 1 可知, 无论周期模板在 $[1, L_T]$ 上的什么位置, 如图 2 所示, 都至少有 $(k-1)\omega$ 个相互独立的等式成立.

$$\begin{array}{c|l}
1 & \omega\left\{\begin{array}{l} f(L_0+\varepsilon_1)=f(L_0+L_T+\varepsilon_1)\odot C \\ f(L_0+\varepsilon_2)=f(L_0+L_T+\varepsilon_2)\odot C \\ \cdots \\ f(L_0+\varepsilon_\omega)=f(L_0+L_T+\varepsilon_\omega)\odot C \end{array}\right. \\
\downarrow & \omega\left\{\begin{array}{l} f(L_0+L_T+\varepsilon_1)=f(L_0+2\cdot L_T+\varepsilon_1)\odot C \\ f(L_0+L_T+\varepsilon_2)=f(L_0+2\cdot L_T+\varepsilon_2)\odot C \\ \cdots \\ f(L_0+L_T+\varepsilon_\omega)=f(L_0+2\cdot L_T+\varepsilon_\omega)\odot C \end{array}\right. \\
 & \cdots \\
k-1 & \omega\left\{\begin{array}{l} f(L_0+(k-2)\cdot L_T+\varepsilon_1)=f(L_0+(k-1)\cdot L_T+\varepsilon_1)\odot C \\ f(L_0+(k-2)\cdot L_T+\varepsilon_2)=f(L_0+(k-1)\cdot L_T+\varepsilon_2)\odot C \\ \cdots \\ f(L_0+(k-2)\cdot L_T+\varepsilon_\omega)=f(L_0+(k-1)\cdot L_T+\varepsilon_\omega)\odot C \end{array}\right.
\end{array}$$

图 2 $(k-1)\omega$ 个等式

更进一步, 根据周期模板在 $[1, L_T]$ 范围内的相对位置, 还可将局部周期现象归为下述三类事件之一.

事件 A 描述一个周期为 L_T 的局部周期现象中, 其周期模板中任意元素的位置 ε_i 满足 $0 < \varepsilon_1 \leqslant \varepsilon_i \leqslant \varepsilon_\omega < L_T$, 并在 $[1, k]$ 内存在整数 k_1, k_2 满足 (6) 式成立的事件:

$$\begin{cases} f\left(L_0 + (k_1 - 1)L_T + \varepsilon_1 - 1\right) \\ \neq f\left(L_0 + k_1 L_T + \varepsilon_1 - 1\right) \odot C, \\ f\left(L_0 + (k_2 - 1)L_T + \varepsilon_\omega + 1\right) \\ \neq f\left(L_0 + k_2 L_T + \varepsilon_\omega + 1\right) \odot C, \end{cases} \tag{6}$$

即对于二值伯努利实验序列 $f(t)$, 该事件发生的条件概率: $P(A) = 2^{-(k-1)\omega} \cdot \left(1 - 2^{-k+1}\right)^2$. 该事件可在 $[1, L_T]$ 范围内 $(L_T - \omega - 1)$ 个位置上发生.

事件 B 描述一个周期为 L_T 的局部周期现象中, 其周期模板中任意元素的位置 ε_i 满足 $0 < \varepsilon_1 \leqslant \varepsilon_i \leqslant \varepsilon_\omega = L_T$, 并在 $[1, k]$ 内存在整数 k_1 使得 (7) 式成立的事件:

$$\begin{aligned} &f\left(L_0 + (k_1 - 1)L_T + \varepsilon_1 - 1\right) \\ &\neq f\left(L_0 + k_1 L_T + \varepsilon_1 - 1\right) \odot C, \end{aligned} \tag{7}$$

即对于二值伯努利实验序列 $f(t)$, 该事件发生的条件概率: $P(B) = 2^{-(k-1)\omega} \cdot \left(1 - 2^{-k+1}\right)$. 该事件可在 $[1, L_T]$ 范围内 1 个位置上发生.

事件 C 描述一个周期为 L_T 的局部周期现象中, 其周期模板中任意元素的位置 ε_i 满足 $0 = \varepsilon_1 \leqslant \varepsilon_i \leqslant \varepsilon_\omega < L_T$, 并有 $[1, k]$ 内存在整数 k_1 使得 (8) 式成立的事件:

$$\begin{aligned} &f\left(L_0 + (k_1 - 1)L_T + \varepsilon_\omega + 1\right) \\ &\neq f\left(L_0 + k_1 L_T + \varepsilon_\omega + 1\right) \odot C, \end{aligned} \tag{8}$$

即对于二值伯努利实验序列 $f(t)$, 该事件发生的条件概率: $P(C) = 2^{-(k-1)\omega} \cdot \left(1 - 2^{-k+1}\right)$. 该事件可在 $[1, L_T]$ 范围内 1 个位置上发生.

由此二值伯努利实验序列在长度为 L 的区间 $[L_0, L_n]$ 指定位置上出现以 L_T 为周期、ω 为周期模板长度的局部周期现象的数学期望可表示为

$$\begin{aligned} E(L, L_T, \omega) &= (L_T - \omega - 1) \cdot P\{A\} + 1 \cdot P\{B\} \\ &\quad + 1 \cdot P\{C\} \\ &= (L_T - \omega - 1) \cdot 2^{-(k-1)\omega} \\ &\quad \times \left(1 - 2^{-k+1}\right)^2 \\ &\quad + 2 \cdot 2^{-(k-1)\omega} \cdot \left(1 - 2^{-k+1}\right). \end{aligned}$$

引理 1 得证.

引理 2 对于任意二值伯努利试验序列 $f(t)$, 其游程长度的数学期望为 3.

证明 由文献 [34] 知, 对于任意二值伯努利试验序列 $f(t)$, 长度为 ω 的游程出现的概率为 $\omega \cdot 2^{-\omega-1}$.

即引理 2 所讨论的数学期望可以表示为 $E = \sum_{\omega=1}^{+\infty} \omega^2 \cdot 2^{-\omega-1}$. 故 (9) 式

$$\begin{aligned} 2 \cdot E &= \sum_{\omega=1}^{+\infty} \omega^2 \cdot 2^{-\omega} \\ &= \frac{1}{2} + \sum_{\omega=2}^{+\infty} \omega^2 \cdot 2^{-\omega} \\ &= \frac{1}{2} + \sum_{\omega=1}^{+\infty} (\omega + 1)^2 \cdot 2^{-\omega-1} \\ &= \frac{1}{2} + \sum_{\omega=1}^{+\infty} \omega^2 \cdot 2^{-\omega-1} + \sum_{\omega=1}^{+\infty} 2 \cdot \omega \cdot 2^{-\omega-1} \\ &\quad + \sum_{\omega=1}^{+\infty} 1 \cdot 2^{-\omega-1} \\ &= \frac{1}{2} + E + 2 + \frac{1}{2} = E + 3 \end{aligned} \tag{9}$$

成立.

可得游程长度的数学期望 $E = 3$.

引理 2 得证.

由于混沌退化原因造成了二值混沌序列随机性弱化, 那么这些序列就将在某些时域范围内出现一系列模板长度较长的局部周期现象. 假设周期为 L_T 的局部周期现象在长度为 L 的局部范围内有长度为 ω 的周期模板, 那么当 $\omega > 3$, $L > L_T \cdot \left(1 + \dfrac{\mathrm{lb}^{L_T}}{\omega}\right)$ 时, 该现象的数学期望具有明显的统计特征即 $E(L, L_T, \omega) < 1$. 本文称这一类局部周期现象为: 以 L_T 为周期的显著局部周期现象.

定义 2 对于给定二值序列, 如其在长度为 L 的区间上存在一系列以 L_T 为周期, 以 ω 为模板长度的局部周期现象, 并且这类局部周期现象出现次数大于 $E(L, L_T, \omega) + \Delta(L, L_T, \omega)$, 则称该序列中存在以 L_T 为周期的显著局部周期现象, $\Delta(L, L_T, \omega)$ 为显著水平的检测量.

显然定义 1 中的精确周期现象和近似周期现

象也是显著局部现象的特例, 并且有显著的统计特性 $E(L, L_T, \omega) \ll 1 - \Delta(L, L_T, \omega)$.

2.4 周期现象与序列重构

由周期现象定义可知, 若序列 $f'(t)$ 是由二值序列 $f(t)$ 经方法

$$f'(t) = f(t) \odot f(t + L_T), \quad L_T \in N,$$

重构生成的二值序列, 则序列 $f(t)$ 与 $f'(t)$ 间应具有如下性质.

引理 3 若序列 $f(t)$ 为二值伯努利实验序列, 其重构序列 $f'(t)$ 也应具有二值伯努利实验序列的统计特性.

证明 首先对于重构序列 $f'(t)$ 中的任意时序 i 位置上的元素, 其取值为 "0" 的概率可以由 (10) 式得出

$$\begin{aligned} & P\{f'(i) = 0\} \\ &= P\{f(i) \odot f(i + L_T) = 0\} \\ &= P\{f(i) = 0 \ \& \ f(i + L_T) = 1\} \\ &\quad + P\{f(i) = 1 \ \& \ f(i + L_T) = 0\} \\ &= P\{f(i) = 0\} \cdot P\{f(i + L_T) = 1\} \\ &\quad + P\{f(i) = 1\} \cdot P\{f(i + L_T) = 0\}. \end{aligned} \tag{10}$$

由于 $f(t)$ 为二值伯努利实验序列, 必有 $P\{f(i) = 0\} = P\{f(i) = 1\} = 1/2$.

由此可得, $P\{f'(i) = 0\} = 1/2$. 同理可得 $P\{f'(i) = 1\} = 1/2$. 显然重构序列中任意元素取值为 0 或 1 的概率均为 1/2. 同理可证 $f'(t)$ 中任意时序位置 i 和位置 j 上元素存在如下关系

$$\begin{aligned} P\{f'(i) \ \& \ f'(j) = 1\} &= P\left\{f'(i) \ \& \ \overline{f'(j)} = 1\right\} \\ &= P\left\{\overline{f'(i)} \ \& \ f'(j) = 1\right\} \\ &= P\left\{\overline{f'(i)} \ \& \ \overline{f'(j)} = 1\right\} \\ &= 1/4, \end{aligned}$$

即重构序列 $f'(t)$ 中任意元素 $f'(i)$ 与 $f'(j)$ 相互独立.

由此可知, 重构序列 $f'(t) = f(t) \odot f(t + L_T)$ 可同样视为二值伯努利实验序列的一个近似.

引理 3 得证.

引理 4 对于任意二值伯努利试验序列 $f(t)$, 在 L_T 长的区间 $[L_0, L_n]$ 上, 一个长度为 ω ($1 \leqslant \omega \leqslant L_T - 1$) 的游程出现次数的数学期望为 $(L_T - \omega - 1) \cdot 2^{-\omega-1} + 2^{-\omega+1}$.

证明 首先假设 "$f(L_0 + \varepsilon_1) f(L_0 + \varepsilon_2) \cdots f(L_0 + \varepsilon_\omega)$" 为一个在二值伯努利实验序列指定区间 $[L_0, L_n]$ 上出现的游程, 该游程的长度为 ω, 指定区间长度为 $L_n - L_0$.

与引理 1 的证明过程类似, 我们同样按游程在区间中的位置, 将事件分成三种情况: 游程从区间的起始位置开始 {head}、游程到区间的结束位置结束 {tail}、其他情况 {middle}.

对于从区间起始位置开始的游程, 共有下述 ω 个等式成立

$$\begin{aligned} f(L_0 + \varepsilon_1) = f(L_0 + \varepsilon_2) = \cdots = f(L_0 + \varepsilon_\omega) \\ \neq f(L_0 + \varepsilon_\omega + 1). \end{aligned}$$

由此 $P\{\text{head}\} = 2^{-\omega}$, 同理可知 $P\{\text{tail}\} = 2^{-\omega}$.

其他情况下, 则共有下述 $\omega + 1$ 个等式成立

$$\begin{aligned} f(L_0 + \varepsilon_1 - 1) \neq f(L_0 + \varepsilon_1) &= f(L_0 + \varepsilon_2) \\ &= \cdots = f(L_0 + \varepsilon_\omega) \\ &\neq f(L_0 + \varepsilon_\omega + 1). \end{aligned}$$

由此 $P\{\text{middle}\} = 2^{-\omega-1}$, 这样共有 $(L_T - \omega - 1)$ 种可能.

所以, 引理 4 所求的数学期望

$$\begin{aligned} E &= (L_T - \omega - 1) \cdot P\{\text{middle}\} \\ &\quad + P\{\text{head}\} + P\{\text{tail}\} \\ &= (L_T - \omega - 1) \cdot 2^{-\omega-1} + 2^{-\omega+1}. \end{aligned}$$

引理 4 得证.

此外, 按照定义 1 和定义 2, 还可以得到序列 $f(t)$ 以及重构序列 $f'(t)$ 之间存在的一些其他性质.

性质 1 若序列 $f(t)$ 存在以 L_T 为周期的精确周期现象或近似周期现象, 则序列 $f'(t)$ 也存在以 L_T 为周期的精确周期现象或近似周期现象.

证明 由假设序列 $f(t)$ 存在以 L_T 为周期的精确周期现象. 由定义 1 知对任意时序 i 位置上的的元素 $f(i + L_T) = f(i) \odot C$.

由序列 $f'(t)$ 定义知

$$\begin{aligned} f'(i) &= f(i) \odot f(i + L_T) \\ &= f(i) \odot (f(i) \odot C) = C = f'(i + L_T), \end{aligned}$$

$f'(t)$ 也存在以 L_T 为周期的精确周期现象.

同理, 若序列 $f(t)$ 存在以 L_T 为周期的近似周期现象. 由定义 1 知存在 $L_0 \to 0$, $L_n \to +\infty$ 以及连续的自然数集合 $\phi_\varepsilon = \{\varepsilon_i | 0 \leqslant \varepsilon_1 < \varepsilon_i < \varepsilon_\omega \leqslant L_T, \varepsilon_i \in N, 1 \leqslant i \leqslant \omega, i \in N, L_T \in N, \omega \to L_T\}$, 使得序列 $f(t)$ 中元素满足: $f(L_0 + (k-1)\cdot L_T + \varepsilon_i) = f(L_0 + k\cdot L_T + \varepsilon_i) \odot C$.

由序列 $f'(t)$ 定义知

$$\begin{aligned} & f'(L_0 + (k-1)\cdot L_T + \varepsilon_i) \\ = & f(L_0 + (k-1)\cdot L_T + \varepsilon_i) \\ & \odot f(L_0 + k\cdot L_T + \varepsilon_i) \\ = & f(L_0 + k\cdot L_T + \varepsilon_i) \\ & \odot (f(L_0 + k\cdot L_T + \varepsilon_i) \odot C) \\ = & C \\ = & f'(L_0 + k\cdot L_T + \varepsilon_i), \end{aligned}$$

即 $f'(t)$ 也存在以 L_T 为周期的近似周期现象.

性质 1 得证.

性质 2 若序列 $f(t)$ 在 $[L_0, L_n]$ 上存在一个以 L_T 为周期的局部周期现象, 则序列 $f'(t)$ 在 $[L_0, L_n - L_T]$ 上同样存在一个以 L_T 为周期的局部周期现象.

证明 若序列 $f(t)$ 在 $[L_0, L_n]$ 上存在以 L_T 为周期的局部周期现象. 由定义 1 知存在连续的自然数集合 $\phi_\varepsilon = \{\varepsilon_i | 0 \leqslant \varepsilon_1 < \varepsilon_i < \varepsilon_\omega \leqslant L_T, \varepsilon_i \in N, 1 \leqslant i \leqslant \omega, i \in N, L_T \in N\}$, 使得序列 $f(t)$ 中元素满足: $f(L_0 + (k-1)\cdot L_T + \varepsilon_i) = f(L_0 + k\cdot L_T + \varepsilon_i) \odot C$.

由序列 $f'(t)$ 定义知, 在 $[L_0, L_n - L_T]$ 上,

$$\begin{aligned} & f'(L_0 + (k-1)\cdot L_T + \varepsilon_i) \\ = & f(L_0 + (k-1)\cdot L_T + \varepsilon_i) \\ & \odot f(L_0 + k\cdot L_T + \varepsilon_i) \\ = & f(L_0 + k\cdot L_T + \varepsilon_i) \\ & \odot (f(L_0 + k\cdot L_T + \varepsilon_i) \odot C) \\ = & C \\ = & f'(L_0 + k\cdot L_T + \varepsilon_i), \end{aligned}$$

即 $f'(t)$ 在 $[L_0, L_n - L_T]$ 也存在一个以 L_T 为周期的局部周期现象.

性质 2 得证.

性质 3 若序列 $f'(t)$ 在 $[L_0, L_n - L_T]$ 上存在一个以 L_T 为周期的局部周期现象, 则序列 $f(t)$ 在 $[L_0, L_n]$ 上必存在一个以 $2\cdot L_T$ 为周期的局部周期现象.

证明 若序列 $f'(t)$ 在 $[L_0, L_n - L_T]$ 上存在以 L_T 为周期的局部周期现象. 由定义 1 知存在连续的自然数集合 $\phi_\varepsilon = \{\varepsilon_i | 0 \leqslant \varepsilon_1 < \varepsilon_i < \varepsilon_\omega \leqslant L_T, \varepsilon_i \in N, 1 \leqslant i \leqslant \omega, i \in N, L_T \in N\}$, 使得序列 $f(t)$ 中元素满足: $f'(L_0 + (k-1)\cdot L_T + \varepsilon_i) = f'(L_0 + k\cdot L_T + \varepsilon_i) \odot C$.

由序列 $f'(t)$ 定义知, 在 $[L_0, L_n]$ 上,

$$\begin{aligned} & f'(L_0 + (k-1)\cdot L_T + \varepsilon_i) \\ = & f(L_0 + (k-1)\cdot L_T + \varepsilon_i) \\ & \odot f(L_0 + k\cdot L_T + \varepsilon_i) \\ = & f'(L_0 + k\cdot L_T + \varepsilon_i) \odot C \\ = & f(L_0 + k\cdot L_T + \varepsilon_i) \\ & \odot f(L_0 + (k+1)\cdot L_T + \varepsilon_i) \odot C, \end{aligned}$$

即 $f(L_0 + (k-1)\cdot L_T + \varepsilon_i) = f(L_0 + (k+1)\cdot L_T + \varepsilon_i) \odot C$.

即 $f(t)$ 在 $[L_0, L_n]$ 也存在一个以 $2\cdot L_T$ 为周期的局部周期现象.

性质 3 得证.

引理 5 对于任意二值序列 $f(t)$ 及其重构序列 $f'(t) = f(t) \oplus f(t + L_T)$, 若序列 $f'(t)$ 的游程变化与二值伯努利试验序列的游程变化相比显著变慢时 [25], 则序列 $f(t)$ 中必存在以 L_T 为周期的显著局部周期现象.

证明 若 $f'(t)$ 与二值伯努利试验序列的游程变化相比显著变慢时, 由引理 2 可知, 必存在区间 $[L_0, L_0 + L_T]$, 以及一系列长度 ($\omega \geqslant 3$) 相同的游程时, 使得这些游程在区间 $[L_0, L_0 + L_T]$ 上的出现次数大于 $(L_T - \omega - 1)\cdot 2^{-\omega-1} + 2^{-\omega+1}$. 由定义 1 可知, 序列 $f(t)$ 在 $[L_0, L_0 + 2\cdot L_T]$ 上存在一系列以 L_T 为周期, 以 ω 为模板长度的局部周期现象, 它们的出现次数大于 $E(2\cdot L_T, L_T, \omega) = (L_T - \omega - 1)\cdot 2^{-\omega-1} + 2^{-\omega+1}$.

由定义 2 可知, 这些在 $[L_0, L_0 + 2\cdot L_T]$ 上存在、以 ω 为模板长度的局部周期现象构成了序列 $f(t)$ 以 L_T 为周期的显著局部周期现象.

引理 2 得证.

3 周期特征检测算法

3.1 BSPD 原理概述

鉴于本文 2.2 和 2.3 节中提出的周期现象扩展定义及其统计特征的证明, 若从序列随机性检测角度观察, 对于二值序列中长度为 ω 的子串在 L 长的局部时序范围内以 $\dfrac{1}{L_T}$ 的频率反复出现的现象, 当 $E(L,L_T,\omega)\ll 1$ 时 (表明上述现象在二值伯努利实验序列中的出现概率非常小), 可知该现象的存在降低了序列的随机性. 另一方面, 若从序列周期检测角度考虑, 当测得上述现象中存在的子串个数远大于二值伯努利实验序列中该现象的期望 $E(L,L_T,\omega)$ 时, 可知序列在 L 长范围内存在以 L_T 为周期的显著局部周期现象.

然而, 仅利用 2.2, 2.3 节的结论对二值序列进行检验, 需要穷举大量的变长时序区间 L 和长度为 ω 的子串以及可能存在的周期数 L_T, 随着序列长度的增大, 该方法的计算需要消耗大量的计算资源. 对局部周期现象的进一步研究中 (如 2.4 节所述), 我们发现原二值序列逐位同或操作形成的二维重构矩阵的下三角矩阵的第 L_T 条对角线, 即序列与其右移 L_T 位的序列同或操作后形成的重构序列, 具有的游程特性和原序列以 L_T 为周期的周期特性之间存在明确的对应关系. 根据这种对应关系, 本文借助 SP800-22 中随机性检验方法对重构矩阵对角线相关游程参数进行检测与判断, 实现了对二值序列周期现象的快速检测. 通过对检出序列的进一步分析, 给出了确定显著局部周期现象时序位置的具体方法, 并在 3.4 节中给出了正确性分析, 最终达到了对周期现象检测与定位的目的.

3.2 周期检测矩阵定义和性质

定义 3 对于长度为 n 的任意二值序列 $f(t)$, 定义二维 $n\times n$ 矩阵 $\boldsymbol{R}: R_{i,j}=f(i)\odot f(j)$ 为序列 $f(t)$ 的周期检测矩阵, 其中 $f(i)$ 和 $f(j)$ 分别为二值序列 $f(t)$ 中第 i 和第 j 个元素.

令矩阵下三角元素有效, 则二值序列 $f(t)$ 与其周期检测矩阵 $\boldsymbol{R}$ 之间具有如下性质.

性质 4 若二值序列 $f(t)$ 为二值伯努利试验序列, 由引理 3 及引理 5 可知, 利用序列 $f(t)$ 生成的周期检测矩阵 $\boldsymbol{R}$ 中任意一条对角线构成二值序列均可以作为一个二值伯努利试验序列的近似, 其游程变化速度与二值伯努利试验序列相比较没有显著差异.

性质 5 若二值序列 $f(t)$ 中存在关系: $f(i)\cdots f(i+\omega-1)=f(i+j)\cdots f(i+j+\omega-1)$. 即二值序列中从第 i 位和第 $i+j$ 位开始有连续 ω 位元素取值相同, 则在周期检测矩阵中, 沿矩阵 $\boldsymbol{R}$ 第 j 条对角线前进 i 步后必有连续长度为 ω, 并且取值为 1 的游程.

性质 6 若二值序列 $f(t)$ 中存在关系: $f(i)\cdots f(i+\omega-1)=\overline{f(i+j)}\cdots\overline{f(i+j+\omega-1)}$. 即二值序列中从第 i 位和第 j 位开始有连续 ω 位元素取值相反, 则在其周期检测矩阵, 沿矩阵 $\boldsymbol{R}$ 中第 j 条对角线前进 i 步后必有连续长度为 ω, 并且取值为 0 的游程.

以序列 $f_{10}=1100101000$ 为例, 设二维 $n\times n$ 矩阵 $\boldsymbol{Q}$ 中任意元素 $Q_{i,j}=\omega$ 表示从二值序列第 i 位和第 j 位起有 ω 位连续元素相同的现象, 则矩阵 $\boldsymbol{Q}$ 和周期检测矩阵 $\boldsymbol{R}$ (按定义 3 构造) 可分别表示为

$$\boldsymbol{R}=\begin{bmatrix}
1 & & & & & & & & & \\
0 & 0 & & & & & & & & \\
0 & 0 & 1 & & & & & & & \\
1 & 1 & 0 & 0 & & & & & & \\
0 & 0 & 1 & 1 & 0 & & & & & \\
1 & 1 & 0 & 0 & 1 & 0 & & & & \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & & & \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & & \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 &
\end{bmatrix},$$

$$\boldsymbol{Q}=\begin{bmatrix}
1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 2 & 0 & 3 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 2 & 2 & 1 & 0 & 0 \\
0 & 3 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}.$$

从上述矩阵中可以明确性质 5, 性质 6 对应关系, 如矩阵 $\boldsymbol{Q}$ 中有 $Q_{4,2}=3$, 则矩阵 $\boldsymbol{R}$ 中沿第 2

条对角线走 4 步则有 3 个连续的 1 出现: 由沿矩阵 $\boldsymbol{R}$ 中第 5 条对角线走 2 步后有 3 个连续的 1 出现; 则矩阵 $\boldsymbol{Q}$ 中有 $Q_{2,5}=3$. 同理, 若矩阵 $\boldsymbol{Q}$ 中任意元素 $Q_{i,j}=\omega$ 表示从二值序列第 i 位和第 j 位起有 ω 位连续元素相反的现象, 矩阵 $\boldsymbol{Q}$ 同样具有与矩阵 $\boldsymbol{R}$ 中相应对角线元素的对应关系, 这里不再赘述.

上述性质表明, 任意二值序列的周期模板出现的位置与周期检测矩阵具有明确的对应关系. 依据引理 5, 当周期检测矩阵第 j 条对角线的游程变化较二值伯努利实验序列显著变慢时, 待检序列中必存在以 j 为周期的精确周期、近似周期或显著局部周期现象.

3.3 BSPD 算法描述

在检查二值序列游程特性的已知算法中, 被广泛引用的典型算法是 SP800-22[25] 标准中的 RUN Test 方法 [15,16,18,35]. BSPD 方法利用 RUN Test 对周期检测矩阵的对角线逐条进行游程检验, 从而形成统计指标集 $\{\pi, \mathrm{Vobs}\}$ 判断游程变化的速度, 根据第 j 条对角线的指标集与序列周期特性和游程变化之间的关系判定序列是否存在周期为 j 的周期现象.

首先介绍周期检测过程中指标集的参数设置.

假设待验二值序列 $f(t)$ 的长度为 L, $s_j(t)$ 为周期检测矩阵中第 j 条对角线, l_j 为第 j 条对角线长度, s_j^i 为 $s_j(t)$ 中的第 i 个元素值, $0<i<l_j$, 则令

1) $\pi_j=\sum\limits_i s_j^i/l_j$,

2) $\mathrm{Vobs}_j=\sum\limits_{i=1}^{l_j-1} r_j^i+1$, 若 $s_j^i\neq s_j^{i+1}$ 有 $r_j^i=1$, 反之 $r_j^i=0$.

即 Vobs_j 为对角线 j 中游程 1 和 0 游程总数.

3) $\tau_j=2/\sqrt{l_j}$, $\eta_j=0.01$,

4) $\mathrm{ppvalue}_j=\mathrm{erfc}\left(\dfrac{|\mathrm{Vobs}_j-2l_j\pi_j(1-\pi_j)|}{2\sqrt{2l_j}\pi_j(1-\pi_j)}\right)$.

BSPD 方法对第 j 条对角线周期现象分析判定遵循如下过程.

步骤 1 选取周期检测矩阵 $\boldsymbol{R}$ 中第 j 条对角线. 若 $j-1$ 条对角线为矩阵中最后一条对角线, 转步骤 6; 反之, 转步骤 2.

步骤 2 计算参数 π_j, Vobs_j, τ_j, $\mathrm{ppvalue}_j$.

步骤 3 检验 $\pi_j=1$ 为真时, 判断二值序列 $f(t)$ 存在周期为 j 的精确周期, 结束对第 j 条对角线的检测, 提取周期模板, $j=j+1$, 转步骤 1; 反之, 继续下一步.

步骤 4 检验 $|\pi_j-1/2|>\tau_j$ 为真时, 判断二值序列 $f(t)$ 存在周期为 j 的近似周期, 结束对第 j 条对角线的检测, 提取周期模板, $j=j+1$, 转步骤 1; 反之, 继续下一步.

步骤 5 检测 $\mathrm{Vobs}_j<2l_j\pi_j(1-\pi_j)\&\ \mathrm{ppvalue}_j<\eta_j$ 为真时, 判断二值序列 $f(t)$ 存在周期为 j 的显著局部周期现象, 提取周期模板, 结束对第 j 条对角线的检测; 反之, 判断没有检出周期为 j 的显著局部周期现象. $j=j+1$, 转步骤 1.

步骤 6 若检测矩阵中所有对角线均未检出显著周期现象时, 认为二值序列 $f(t)$ 为二值伯努利试验的一个近似序列; 反之, 列举序列存在的不同周期现象.

BSPD 方法的检测优势不仅体现在能够挖掘出二值序列上存在的各种周期现象, 还表现出对序列不同周期范围内的周期模板的简便提取. 以长度为 L 的二值序列 $f(t)$ 周期检测矩阵 $\boldsymbol{R}$ 中第 j 条对角线为例, 若其上检出具有显著局部周期现象, 则采取如下步骤, 定位和提取局部周期模板.

步骤 1 抽取该对角线上全部 l_j 个元素组成序列 $S(t)$.

步骤 2 将序列 $S(t)$ 以 j 为周期折叠, 建立具有 k 行 j 列元素的矩阵 $\boldsymbol{G}$, 并有

$$k=\begin{cases} l_j/j, & l_j \bmod j=0,\\ \lfloor l_j/j\rfloor+1, & l_j \bmod j>0,\end{cases} \tag{11}$$

其中 $l_j=L-j$, 则 $\boldsymbol{G}$ 中第 o 行 p 列的元素可以表示为

$$\boldsymbol{G}_{o,p}=\begin{cases} S(o\cdot j+p) & o\cdot j+p\leqslant l_j,\\ 0 & o\cdot j+p>l_j,\end{cases} \tag{12}$$

步骤 3 在矩阵 $\boldsymbol{G}$ 中, 对所有 "0" 块或 "1" 块进行面积检验, 提取所有面积不小于 $\mathrm{lb}^{\max(L-j,j)}+\Delta(j)$ 的 "0" 块或 "1" 块, 并将它加入集合 $\{\mathrm{Block}\}$. 其中 $\Delta(j)$ 为显著性检验条件, 在本文所有实验中取 $\Delta(j)=\mathrm{lb}^j/2$. 所有集 $\{\mathrm{Block}\}$ 中块, 均对应一个显著周期现象.

3.4 BSPD 算法正确性分析

首先假设, 集合 $\{\mathrm{Block}\}$ 中的元素 Block_i 表示

矩阵 $\boldsymbol{G}$ ($\boldsymbol{G}$ 为 $\boldsymbol{R}$ 中第 i 条对象构造的折叠矩阵)中的一个面积不小于 $\mathrm{lb}^{\max(L-j,j)}+\Delta(j)$ 的 "0" 块或 "1" 块, Block_i 的宽度为 $\omega(1<\omega<j)$, 高度为 $h(1<h\leqslant k)$, 面积 $\omega\cdot h$ 不小于 $\mathrm{lb}^{\max(L-j,j)}+\Delta(j)$ 的 "0" 块或 "1" 块.

由定义 1 及引理 1 可知, 在长度为 $j\cdot(h+1)$ 的二值伯努利试验序列上, 以 j 为周期, 周期模板长度为 ω 的局部周期现象, 其出现次数的数学期望可表示为

$$E(j(h+1),j,\omega)=(j-\omega+1)\cdot 2^{-\omega h}\cdot(1-2^{-h})^2+2\cdot 2^{-\omega h}\cdot(1-2^{-h}).$$

当 $\omega h\geqslant \mathrm{lb}^j+\dfrac{\mathrm{lb}^j}{2}$, 并且 $j>1$ 时, 下式

$$\begin{aligned}&E(j(h+1),j,\omega)\\&\leqslant(j-\omega+1)\cdot 2^{-1.5\mathrm{lb}^j}\cdot(1-2^{-h})^2+2\cdot 2^{-1.5\mathrm{lb}^j}(1-2^{-h})\\&=(j-\omega+1)\cdot j^{-1.5}\cdot(1-2^{-h})^2+2\cdot j^{-1.5}(1-2^{-h})\\&<1\end{aligned}\tag{13}$$

成立.

即由定义 1 及引理 1, 定理 5 可知, 当 $\omega\cdot h\geqslant \mathrm{lb}^j+\dfrac{\mathrm{lb}^j}{2}$, $j>1$ 时, 在序列 $f(t)$ 中必存在一个区间 $[o\cdot j+p, o\cdot j+p+j\cdot(h+1)]$, 在这个区间上有以 j 为周期, ω 为模板长度的局部周期现象的出现, 但这种局部周期现象在二值伯努利试验序列中出现次数的数学期望 $E(j\cdot(h+1),j,\omega)<1$.

同时, 由于周期检测矩阵第 j 条对角线的长度 $L_j=L-j$, 所以矩阵 $\boldsymbol{G}$ 中任意面积为 ωh 的块出现次数的期望的最大值为 $E(L-j,L-j,\omega h)=(L-j-\omega h+1)\cdot 2^{-\omega h}\cdot(1-2^{-1})^2+2\cdot 2^{-\omega h}\cdot(1-2^{-1})$.

当 $\omega h\geqslant \mathrm{lb}^{L-j}+\dfrac{\mathrm{lb}^j}{2}$, 并且 $j>1$ 时, 下式

$$\begin{aligned}&E(L-j,L-j,\omega h)\\&\leqslant\frac{(L-j-\omega h+1)}{4}\cdot 2^{-(\mathrm{lb}^{L-j}+\mathrm{lb}^j)}+2^{-\left(\mathrm{lb}^{L-j}+\frac{\mathrm{lb}^j}{2}\right)}\\&=\frac{(L-j-\omega h+1)}{4}\cdot\frac{1}{(L-j)\sqrt{j}}+\frac{1}{(L-j)\sqrt{j}}\\&<1\end{aligned}\tag{14}$$

成立.

由此可知, 对于一个长度为 L 的二值序列 $f(t)$, BSPD 在其周期检测矩阵的对角线提取的所有 "0" 块或 "1" 块, 均将对应序列 $f(t)$ 中一个精确周期、近似周期或显著局部周期现象. 若块在序列 $S(t)$ 中的起始时序位置为 L_0, 结束位置 L_n, 块的宽度为 ω, 那么 $[L_0, L_n+j]$ 为 BSPD 定位的显著周期现象存在区间, 符号串 "$f(L_0)f(L_0+1)\cdots f(L_0+\omega-1)$" 为提取出的周期模板.

4 Logistic 混沌状态的局部周期现象

在通信和加密应用过程中许多混沌系统不可避免的需要转化为二值序列, 特别是一些基于混沌映射生成的随机序列. 然而鲜有相关方法用于阐述和分析混沌二值序列内部存在的局部周期特性及其对应用的影响. 本文正是出于对上述问题的考虑, 设计了 BSPD 方法, 用以检测和定位任意二值序列的周期现象. 为了详细说明 BSPD 的检测效果, 仿真实验设计通过下述方法生成待检序列: 利用经典 logistic 方程 (1) 式, 将从初值 x_0 开始迭代, 当采用 M 位定点精度, 经过量化函数分别生成的长度为 10^4 二值序列, 称为待检混沌序列 $f_M(x_0,t)$.

本文采用 BSPD 共对 $M=16$, 24, 32, 64, $x_0=i/255$, $i=1, 2, 3, \cdots, 254$, 共 1016 个不同待检序列进行了实际检验. 表 1 为检验结果, 表明这些待检序列中均存在精确周期、近似周期或显著局部周期现象.

表 1 待检序列 BSPD 检验结果

迭代精度	存在周期现象的待检序列数			
M/bits	精确周期现象	近似周期现象	显著局部周期现象	无显著周期现象
16	254	0	0	0
24	19	235	0	0
32	0	2	252	0
64	0	0	254	0

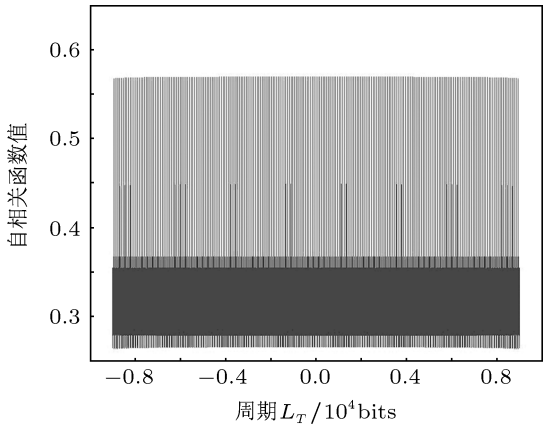

图 3 序列 $f_{16}(15/255,t)$ 自相关算法周期检验结果图

图 3—5 为待检序列 $f_{16}(15/255,t)$ 的检验结果. 在图 3 中, 自相关检验 [29] 显示 $f_{16}(x_0/255,t)$ 存在周期为 79 的周期现象; 在图 4 中, BSPD 表明 $f_{16}(x_0/255,t)$ 存在周期为 79 的精确周期现象; 图 5 为 BSPD 提取的该精确周期现象的信号模板.

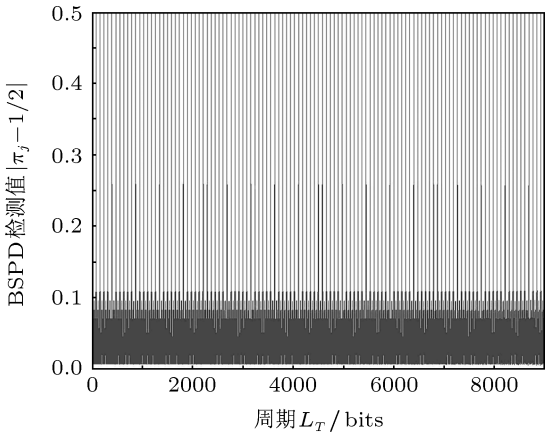

图 4 序列 $f_{16}(15/255,t)$ 周期检验结果图

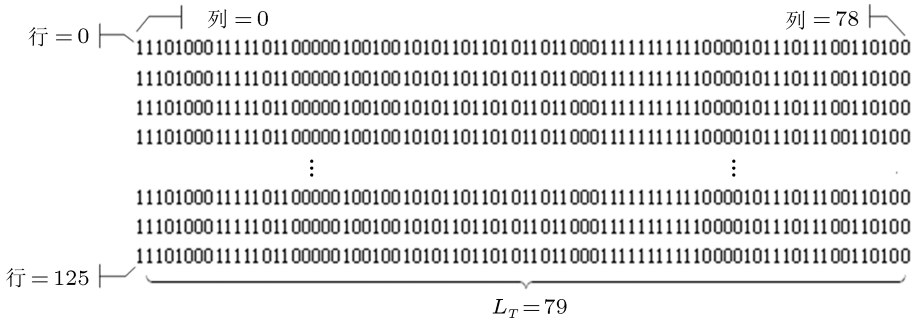

图 5 序列 $f_{16}(15/255,t)$ 周期信号模板

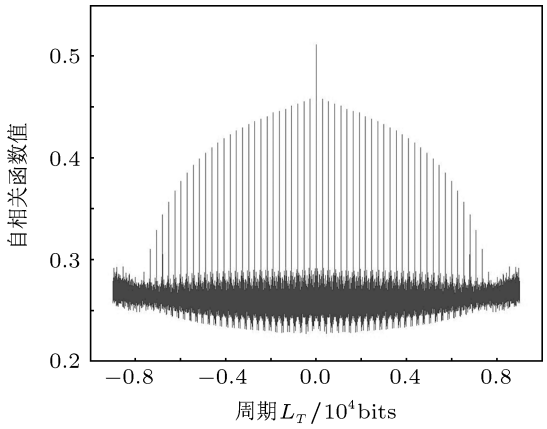

图 6 序列 $f_{24}(28/255,t)$ 自相关算法周期检验结果图

图 6—8 为待检序列 $f_{24}(28/255,t)$ 的检验结果. 在图 6 中, 自相关检验显示 $f_{24}(x_0/255,t)$ 存在周期为 272 的周期现象; 在图 7 中, BSPD 表明 $f_{24}(x_0/255,t)$ 存在周期为 272 的近似周期现象; 图 8 为 BSPD 提取的该精确周期现象的信号模板.

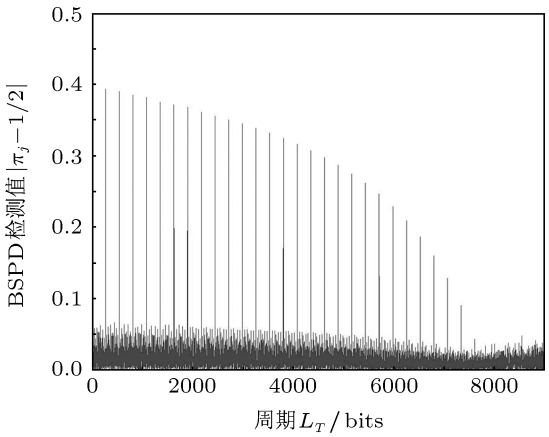

图 7 序列 $f_{24}(28/255,t)$ 周期检验结果图

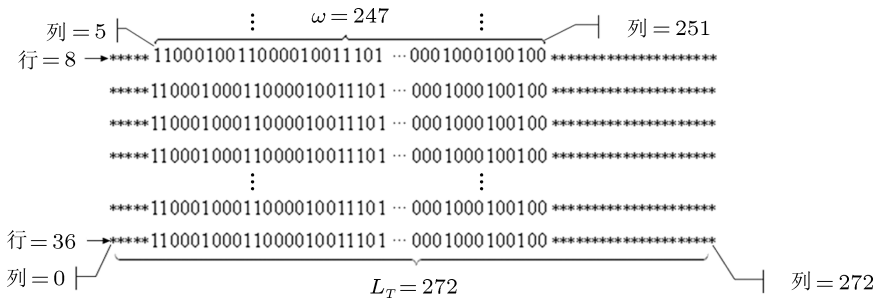

图 8 序列 $f_{24}(28/255, t)$ 周期信号模板

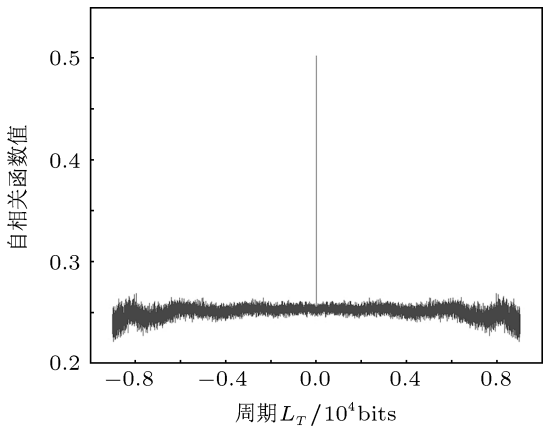

图 9 序列 $f_{32}(179/255, t)$ 自相关算法周期检验结果图

图 9—11 为待检序列 $f_{32}(179/255, t)$ 的检验结果. 在图 9 中, 自相关检验显示 $f_{32}(179/255, t)$ 周期特性与随机现象近似; 在图 10 中, BSPD 表明 $f_{32}(179/255, t)$ 中存在很多显著局部周期现象; 图 11 为 BSPD 从 $f_{32}(179/255, t)$ 提取的两个周期为 610 的显著局部周期现象的信号模板, 其中一个表示在 [6125, 6128], [6735, 6738], [7345, 7348], [7955, 7958] 和 [8565, 8568] 范围内存在的周期模板为 {1111} 的局部周期现象, 另一个则表示在 [8362, 8380] 和 [8872, 8890] 范围内存在的周期模板为 "10101100100011000000" 的局部周期现象.

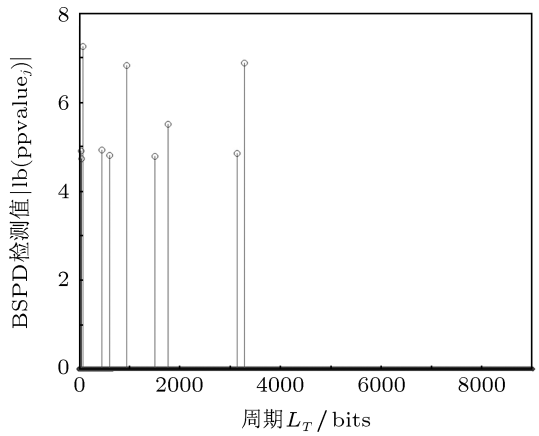

图 10 序列 $f_{32}(179/255, t)$ 周期检验结果图

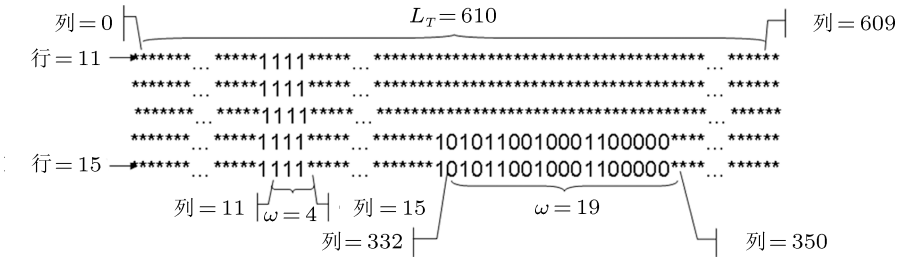

图 11 序列 $f_{32}(179/255, t)$ 局部周期现象定位结果

5 结 论

本文首次提出了对二值序列周期现象的扩展定义. 遵循该扩展定义, 设计并实现了一种用于检验混沌二值序列具有的周期现象的方法 —— BSPD. 文中以伯努利实验序列作为比较对象, 通过

一系列证明, 阐述了混沌二值序列具有的周期现象以及它与其重构序列之间的对应关系. 证明了当周期检测矩阵对角线的游程变慢时, 待验序列必存在显著周期现象, 并进一步给出了显著周期现象的周期模板提取算法, 从而实现了对任意二值序列, 特别是混沌二值序列进行周期现象的检验和定位. 实验结果表明 BSPD 方法既可用于检测二值序列具有的精确周期现象、近似周期现象和局部周期现象, 还能够对序列局部范围内显著存在的周期现象进行有效的时序定位.

[1] Jakimoski G, Kocarev L 2001 *IEEE Trans. Circuits and Systems* I **48** 163

[2] Kocarev L 2001 *IEEE Circuits and Systems Magazine* **1** 6

[3] Baptista M S 1998 *Phys. Lett.* A **240** 50

[4] Kohda T 2002 *Proceedings IEEE* **90** 641

[5] Masuda N, Aihara K 2002 *IEEE Trans. Circuits and Systems* I **49** 28

[6] Mazzini G, Setti G, Rovatti R 1997 *IEEE Trans. Circuits and Systems* I **44** 937

[7] Liao N H, Gao J F 2006 *J. Elec. Inf. Tech.* **28** 1255 (in Chinese) [廖旎焕, 高金峰 2006 电子与信息学报 **28** 1255]

[8] Wu H, Ding Q, Zhou P 2009 *CIMCTC'* 2012 Harbin, July 23–26 2009, pp372–375 (in Chinese) [巫红, 丁群, 周平 2009 中国仪器仪表与测控技术大会, 哈尔滨, 2009 年 7 月 23—26 日, pp372–375]

[9] Van Wiggeren G D, Roy R 1998 *Science* **279** 1198

[10] Pecora L M, Carroll T L 1990 *Phys. Rev. Lett.* **64** 821

[11] Cuomo K M, Oppenheim A V 1993 *Phys. Rev. Lett.* **71** 65

[12] Kocarev L, Parlitz U 1995 *Phys. Rev. Lett.* **74** 5028

[13] Boccaletti S, Kurths J Osipov G, Valladares D L, Zhou C S 2002 *Phys. Rep.* **366** 1

[14] Ruelle D 1989 *Chaotic Evolution and Strange Attractors*: *the Statistical Analysis of Time Series for Deterministic Nonlinear Systems* (New York: Cambridge University Press) pp28–33

[15] Sang T, Wang R L, Yan Y X 2001 *IEEE Trans. Commun.* **49** 620

[16] Kanso A, Smaoui N 2009 *Chaos, Solitons and Fractals* **40** 2557

[17] Jiang H Y, Fu C A 2008 *Proceedings of 2008 International Conference on Intelligent Computation Technology and Automation* (Vol. 2) Changsha, October 20–22 2008 pp60–64

[18] Chen S L, Hwang T T, Lin W W 2010 *IEEE Trans. Circuits and Systems* II **57** 996

[19] Kohda T, Tsuneda A 1997 *IEEE Trans. Information Theory* **43** 104

[20] L'Ecuyer P 2006 *Handbooks in Operations Research and Management Science*: *Simulation* (Amsterdam: Elsevier B V) pp55–81

[21] James F 1990 *Comput. Phys. Commun.* **60** 329

[22] Bresten C L, Jung J H 2009 *Communications in Nonlinear Science and Numerical Simulation* **14** 3076

[23] Cheng L Y, Quan J B 2010 *J. Comut. Appl.* **30** 1802 (in Chinese) [盛利元, 全俊斌 2010 计算机应用 **30** 1802]

[24] Fan J L, Zhang X F 2009 *Acta Electron. Sin.* **4** 720 (in Chinese) [范九伦, 张雪峰 2009 电子学报 **4** 720]

[25] Kohda T, Tsuneda A 1993 *IEICE Trans. Commun.* E **76**_B 855

[26] Liu N S H 2011 *Communications in Nonlinear Science and Numerical Simulation* **16** 761

[27] Tsuneda A 2005 *IEEE Trans. Circuits and Systems* I **52** 454

[28] Jessa M 2002 *IEEE Trans. Circuits and Systems* I **49** 84

[29] Kleiner B 1977 *Technometrics* **19** 343

[30] Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A, Dray J, Vo S 2001 *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (Gaithersburg, MD, USA: NIST) p1, pp18–21

[31] L'Ecuyer P, Simard R 2007 *ACM Trans. Math Software* **33** 1

[32] McCullough B D 2006 *J. Appl. Econ.* **21** 677

[33] Xiang F, Qiu S S 2008 *IEEE Commun. Lett.* **12** 337

[34] Zhang S R, Mei W H, Wang T C, Deng X Y 2000 *Journal of China Institute of Communications* **21** 45 (in Chinese) [张申如, 梅文华, 王庭昌, 邓晓燕 2000 通信学报 **21** 45]

[35] Li C Y, Chen Y H, Chang T Y, Deng L Y, Kiwing T 2012 *IEEE Trans. VLSI Systems* **20** 385

A novel detection of periodic phenomena of binary chaotic sequences*

Zheng Yan-Bin[1)] Song Yu[2)] Du Bao-Xiang[1)] Pan Jing[1)] Ding Qun[1)†]

1) (*Key Laboratory of Electronic Engineering, Heilongjiang University, Harbin* 150080, *China*)

2) (*School of Computer Science and Technology, Harbin Institute of Technology, Harbin* 150001, *China*)

(Received 1 April 2012; revised manuscript received 18 June 2012)

Abstract

For any digital chaotic sequence generator, evaluating periodic characteristics which exist in only part of domains of binary chaotic sequences is extremely difficult. In this paper, we present a method which we name the binary sequence period detection (BSPD). The BSPD is a novel detection which evaluates the periodicity in a binary chaotic sequence, by which both the accurate-periodic phenomena and periodic phenomena in part of domains can be detected. Moreover, any periodic phenomenon pattern of a binary sequence can be located by the BSPD method. The experimental results show that the BSPD can detect and extract the periodic phenomena of the classical Logistic chaotic sequence generators.

Keywords: chaos, binary sequences, period phenomena, detection

PACS: 05.45.–a, 02.30.Lt, 43.55.Cs, 02.60.–x

* Project supported by the National Natural Science Foundation of China (Grant No. 60672011).

† E-mail: qunding@yahoo.cn