第 57 卷 第 7 期 2008 年 7 月
1000-3290/2008/57(07)/4007-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.57, No.7, July, 2008

将混沌序列变换成均匀伪随机序列的普适算法*

盛利元[1)†] 肖燕予[2)] 盛 [3)]

1)(中南大学物理科学与技术学院,长沙 410083)

2)(Department of Applied Mathematics Science College, University of Western Ontario London, ON, Canada N6A 5B7)

3)(中南大学数学与统计学院,长沙 410075)

(2007 年 8 月 22 日收到;2007 年 10 月 31 日收到修改稿)

提出了一种将混沌序列变换成均匀伪随机序列的普适算法.这种算法基于计算机浮点数表示的 bit 位操作,不针对任何具体对象,可将任意连续或分段连续分布的实型随机变量转换成均匀分布的随机变量.理论分析表明,这种算法源于实型随机变量中普遍存在着的沿 bit 位以指数规律增强的均匀化趋势.任何实型的混沌序列,不论来自混沌映射系统还是混沌微分动力系统,都可以在同一个标准算法下变换成均匀分布的伪随机序列,因而是混沌伪随机数发生器标准化模块设计和硬件实现的关键技术基础.

关键词:混沌,伪随机序列,均匀分布函数

PACC:0545,0250

1. 引 言

高质量伪随机数发生器(pseudo-random number generator, PRNG)广泛地应用于信息加密、数值仿真、电子游戏、统计分析、分布式计算等领域,它的最重要特性之一是伪随机序列必须服从均匀分布,但是,这样的 PRNG 并不多见.混沌系统作为一种随机数源可以构造 PRNG,如用分段线性映射系统和复合离散混沌系统构造的 PRNG 具有均匀性[1—3],但用于信息加密时存在参数空间太小等其他缺陷;又如用 TD-ERCS 混沌系统构造的 PRNG,需要通过一个反余弦函数和一个反正切函数变换才具有均匀分布的特性[4],影响了计算速度,用 FPGA 硬件实现时遇到了极大的困难;文献[5]提出了一种由 z-logistic 映射构造具有均匀性的 PRNG 的新方法,虽然可以精确预测其周期性,但涉及素数、三角函数运算,同样是速度慢而不宜硬件实现.在现有理论下,绝大多数混沌系统目前都还不能构造出具有均匀分布特性的 PRNG,极大地限制了混沌系统在电子信息领域中的应用和相应的理论研究.为了克服混沌系统构造均匀 PRNG 的理论困难和硬件实现的技术困难,本文提出了一种随机数均匀化的普适算法.这种算法基于计算机浮点数表示的 bit 位操作,不针对任何具体对象,可将任意分布(只要求连续或分段连续)的实型随机变量转换成均匀分布的随机变量,并且运算速度快,易于硬件实现,是一种自然的因而也是普适的算法.这种算法的自然性源于实型随机变量中普遍存在的一种均匀化趋势,而它的普适性则是由于这种均匀化趋势沿实型数据的 bit 位以指数规律增强,因而可以通过 bit 位操作得以实现.采用这种普适算法,任何实型的混沌序列,不论是来自于混沌映射系统还是混沌微分动力系统,都可以在同一个标准算法下变换成均匀分布的伪随机序列,这意味着任何混沌系统都可以构造出均匀分布的伪随机序列,因而有望成为混沌 PRNG 标准化模块设计和硬件实现的关键技术基础.

2. 随机数均匀化普适算法描述

2.1. bit 位的移位操作

IEEE754 标准[6] 规定,一个实数的双精度二进制表示由三部分组成(图 1 所示):1-bit 符号位(用 s

* 国家自然科学基金(批准号:60672041)资助的课题.

† E-mail:itpo@mail.csu.edu.cn

表示),11-bit 有偏指数位(用 e 表示),52-bit 尾数位(用 f 表示),由

$$(-1)^s \times 2^{e-1023} \times 1.f,$$
$$0 < e < 2047, s \in \{0,1\} \quad (1)$$

换算到十进制数或二进制数.

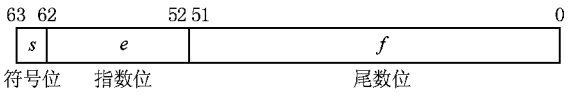

图 1 IEEE754 实数表示法

引入"左移位 b 操作"和"右移位 b 操作".

定义 1 如果尾数 f 中第 51-bit,50-bit,…,$(51-b+1)$-bit 均为"0",而 $(51-b)$-bit 为"1",则将 f 的前 b 位依次移到 f 的右边构成一个新尾数 f,这样的操作称为左移位 b 操作,新尾数 f 记为 $f_{\leftarrow b}$.

例如

移位前 f :**0000010**10100001111…10,

移位后 $f_{\leftarrow 6}$:10100001111…10**0000001**.

左移位 b 操作用于二进制小数转换为 IEEE754 标准的双精度数的尾数.

定义 2 将尾数 f 中第 0-bit 设置为"1",第 1-bit,2-bit,…,$(b-1)$-bit 均设置为"0",然后将此 b 位依次移到 f 的左边构成一个新尾数 f,这样的操作称为右移位 b 操作,新尾数 f 记为 $f_{\rightarrow b}$.

例如

移位前 f :10100001111…10**011000**,

重设置 f :10100001111…10**0000001**,

移位后 $f_{\rightarrow 6}$:**0000001**10100001111…10.

右移位 b 操作用于将 IEEE754 标准的双精度数的尾数转换为二进制小数.

2.2. bit 位变换

(1)式中尾数 f 可视为 52bit 的二进制码

$$f = f_{51}f_{50}\cdots f_2f_1f_0,$$
$$f_i \in \{1,0\}, i = 0,1,2,\cdots,51,52. \quad (2)$$

将其分成高位 26bit 和低位 26bit 的两个码块,记为

$$f_H = f_{51}f_{50}\cdots f_{27}f_{26}, f_L = f_{25}f_{24}\cdots f_1f_0. \quad (3)$$

将 f_L 倒置,记为

$$f'_L = f_0f_1\cdots f_{24}f_{25}. \quad (4)$$

定义 3 f_H 与 f'_L 对应 bit 位进行异或运算,记为

$$f'_H = f_H \oplus f'_L = f'_{51}f'_{50}\cdots f'_{27}f'_{26}, \quad (5)$$

其中

$$f'_i = f_{51-i} \oplus f_i, i = 0,1,2,\cdots,24,25,$$

再将 f'_H 与 f_L 按照高位和低位合并构成一个新的尾数,即

$$f' = f'_Hf_L = f'_{51}f'_{50}\cdots f'_{27}f'_{26}f_{25}f_{24}\cdots f_2f_1f_0. \quad (6)$$

称 f' 为尾数 f 的 bit 位变换,记为 **Bit** $\{f\}$,即 $f' =$ **Bit** $\{f\}$. f'_L 称为 bit 位变换的变换核.

Bit $\{f\}$ 的逆变换记为 **IBit** $\{f\}$.因

$$f_H = (f_H \oplus f'_L) \oplus f'_L = f'_H \oplus f'_L,$$

故 **IBit** $\{f\}$ 与 **Bit** $\{f\}$ 的算法规则相同,即 **IBit** $\{f\}$ = **Bit** $\{f\}$.于是,对任意尾数 f 有

$$f = \textbf{IBit}\{f'\} = \textbf{IBit}\{\textbf{Bit}\{f\}\} = \textbf{Bit}\{\textbf{Bit}\{f\}\}, \quad (7)$$

即尾数 f 进行两次 bit 位变换,其值不变.

2.3. 实数的 bit 位变换

由(1)式知,在计算机中,一个实数 x 的双精度表示为

$$x = (-1)^s \times 2^{e-1023} \times 1.f,$$
$$0 < e < 2047, s \in \{0,1\}. \quad (8)$$

因此,与数学意义的实数性质不同,计算机表示的实数是可数的,实数的数目是有限的.为了研究计算机表示的实数的性质,不仿用 G 表示所有由(8)式给定的实数的集合,即 G 是计算机表示的实数的定义域,并引入一种计算机双精度实数的简单表示法:对于实数 x,若 $x \in G$,则 x 简记为 $\{s,e,f\}$,即(8)式为

$$x = \{s,e,f\}. \quad (9)$$

用计算机来研究实数,实质上就是研究 s,e 和 f 三个数.

定义 4 $\{s,e,\textbf{Bit}\{f\}\}$ 称为 $\{s,e,f\}$ 的第一类 bit 位变换,用 $B_1(x)$ 表示.

实数的第一类 bit 位变换中,s 和 e 保持不变,尾数 f 用 **Bit** $\{f\}$ 代换,实数 $\{s,e,\textbf{Bit}\{f\}\} \in G$,且由(7)式知,$\{s,e,\textbf{Bit}\{\textbf{Bit}\{f\}\}\} = \{s,e,f\} \in G$,故 $B_1(x)$ 是一对一的 $G \mapsto G$ 映射,逆变换存在.

定义 5 对 **Bit** $\{f\}$ 进行左移位 b 操作后得 **Bit** $\{f\}_{\leftarrow b}$,且令 $e' = 1023 - b$,$s = 0$,新的实数 $\{0,e',\textbf{Bit}\{f\}_{\leftarrow b}\}$ 称为 $\{s,e,f\}$ 的第二类 bit 位变换,用 $B_2(x)$ 表示.

实数的第二类 bit 位变换由 bit 变换,左移位 b 操作完成,且 $\{0,e',\textbf{Bit}\{f\}_{\leftarrow b}\} \in [0,1]$,故 $B_2(x)$ 是多对一的 $G \mapsto [0,1]$ 映射,逆变换不存在.

定义 6 若 $\{s,e,f\} \in [-1,1]$,$\{0,1023-b,\textbf{Bit}\{f_{\rightarrow(1023-e)}\}_{\leftarrow b}\}$ 称为 $\{s,e,f\}$ 的标准第二类 bit 位变换,仍用 $B_2(x)$ 表示.

实数的标准第二类 bit 位变换由右移位 b 操

作，bit 变换，左移位 b 操作完成，是多对一的 $[-1,1]\mapsto[0,1]$ 映射，逆变换不存在.

2.4. 随机数均匀化普适算法

定理 1　设实型随机变量 $\xi\in G$ 的分布函数 $F_\xi(x)=P\{\xi<x\}$ 连续(或分段连续)，若对 ξ 进行第二类 bit 位变换(或标准的第二类 bit 位变换)成随机变量 η，则 $\eta\in[0,1]$，且其分布函数 $F_\eta(x)$ 以不大于 2^{-52} 的理想偏差服从均匀分布，即

$$p_\eta(x)=\frac{\mathrm{d}}{\mathrm{d}x}F_\eta(x)=1.$$

该定理表明，对一个实数表示的随机变量只要采用第二类 bit 位变换(或标准的第二类 bit 位变换)，就能获得均匀分布的随机数，简单地说，若 ξ 是一个实的随机变量，则 $\eta=B_2(\xi)$ 是 $[0,1]$ 上均匀分布的随机变量，这就是随机数均匀化普适算法.

3. 随机数均匀化普适算法之证明

为了证明定理 1，先引入随机变量分布均匀性的判断标准.

定义 7　设 ξ 为 0-1 二值随机变量，$P\{\xi=0\}$ 和 $P\{\xi=1\}$ 分别为 $\xi=0$ 和 $\xi=1$ 的概率，且 $\min(P\{\xi=0\},P\{\xi=1\})>0$，令

$$Y=\frac{\min(P\{\xi=0\},P\{\xi=1\})}{\max(P\{\xi=0\},P\{\xi=1\})},\quad Y\in(0,1],\qquad(10)$$

则称 Y 为 ξ 的概率均匀性指数.

概率均匀性指数表征了二值随机变量 ξ 的概率分布的均匀性优劣. 若 $Y=1$，则 $P\{\xi=0\}=P\{\xi=1\}$，ξ 均匀分布；Y 越大，ξ 的均匀性越好.

定理 2　设 ξ 和 η 为两个相互独立的 0-1 二值随机变量，构造一个新的二值随机变量 $\tau=\xi+\eta(\mathrm{mod}2)$，则 τ 的均匀性优于 ξ 和 η 的均匀性，即 $Y_\tau\geqslant Y_\xi$，$Y_\tau\geqslant Y_\eta$.

证明　设 $P\{\xi=0\}=\alpha$，$P\{\eta=0\}=\beta$，则有 $P\{\xi=1\}=1-\alpha$，$P\{\eta=1\}=1-\beta$，于是由 $\tau=\xi+\eta(\mathrm{mod}2)$ 及 ξ 和 η 的相互独立性，得

$$\begin{aligned}P\{\tau=0\}&=P\{\xi=0,\eta=0\}+P\{\xi=1,\eta=1\}\\&=\alpha\beta+(1-\alpha)(1-\beta)\\&=\alpha+(1-\beta)(1-2\alpha),\\P\{\tau=1\}&=P\{\xi=0,\eta=1\}+P\{\xi=1,\eta=0\}\\&=\alpha(1-\beta)+(1-\alpha)\beta\\&=\alpha+\beta(1-2\alpha),\end{aligned}$$

故当 $\alpha\leqslant\frac{1}{2}$，即 $1-\alpha\geqslant\frac{1}{2}$ 时，有

$$\begin{aligned}\alpha&\leqslant\alpha+(1-\beta)(1-2\alpha)\\&=1-\alpha-(1-2\alpha)\beta\leqslant1-\alpha,\\\alpha&\leqslant\alpha+\beta(1-2\alpha)\\&=1-\alpha-(1-2\alpha)(1-\beta)\leqslant1-\alpha,\end{aligned}$$

反之，当 $\alpha\geqslant\frac{1}{2}$，即 $1-\alpha\leqslant\frac{1}{2}$ 时，上面两个不等式仍然成立，当且仅当 $\alpha=\frac{1}{2}$ 时等号成立.

综合上述两种情况有

$$\begin{aligned}\min(\alpha,1-\alpha)&\leqslant\min(P\{\tau=0\},P\{\tau=1\})\\&\leqslant\max(P\{\tau=0\},P\{\tau=1\})\\&\leqslant\max(\alpha,1-\alpha).\end{aligned}$$

同理

$$\begin{aligned}\min(\beta,1-\beta)&\leqslant\min(P\{\tau=0\},P\{\tau=1\})\\&\leqslant\max(P\{\tau=0\},P\{\tau=1\})\\&\leqslant\max(\beta,1-\beta).\end{aligned}$$

由此，结合定义式(10)，得 $1\geqslant Y_\tau\geqslant Y_\xi$，$1\geqslant Y_\tau\geqslant Y_\eta$，故 τ 的均匀性优于 ξ 和 η 的均匀性. 证毕.

推论　设 ξ 和 η 为两个相互独立的 0-1 二值随机变量，若 ξ 与 η 中任意一个是均匀分布的，则二值随机变量 $\tau=\xi+\eta(\mathrm{mod}2)$ 也是均匀分布的.

此结论成立显然.

定理 3　设实型随机变量 $\xi\in[0,1]$ 具有连续(或分段连续)的概率密度函数 $p_\xi(x)$，将 ξ 表示成二进制形式

$$\xi=0.\xi_1\xi_2\xi_3\cdots\xi_i\cdots,\qquad(11)$$

则 $\xi_i\in\{0,1\}$，$i=1,2,3,\cdots$ 是一个二值随机变量序列，且当 $i\to\infty$ 时，ξ_i 趋于均匀分布，即 $\lim\limits_{n\to\infty}P(\xi_n=0)=\lim\limits_{n\to\infty}P(\xi_n=1)$.

证明　因概率密度函数 $p_\xi(x)$ 是连续(或分段连续)的，对于 ξ_i，$i=1,2,3,\cdots$，有

$$\begin{aligned}i=1:\quad P(\xi_1=0)&=\int_0^{\frac{1}{2}}p_\xi(x)\mathrm{d}x,\\P(\xi_1=1)&=\int_{\frac{1}{2}}^1p_\xi(x)\mathrm{d}x,\\i=2:\quad P(\xi_2=0)&=\int_0^{\frac{1}{4}}p_\xi(x)\mathrm{d}x+\int_{\frac{2}{4}}^{\frac{3}{4}}p_\xi(x)\mathrm{d}x,\\P(\xi_2=1)&=\int_{\frac{1}{4}}^{\frac{2}{4}}p_\xi(x)\mathrm{d}x+\int_{\frac{3}{4}}^1p_\xi(x)\mathrm{d}x,\\&\cdots\cdots\end{aligned}$$

$$i = n:\ P(\xi_n = 0) = \sum_{k=1}^{2^{n-1}} \int_{\frac{2(k-1)}{2^n}}^{\frac{2k-1}{2^n}} p_\xi(x)\,\mathrm{d}x,$$

$$P(\xi_n = 1) = \sum_{k=1}^{2^{n-1}} \int_{\frac{2k-1}{2^i}}^{\frac{2k}{2^n}} p_\xi(x)\,\mathrm{d}x, \quad (12)$$

故 $\xi_i, i = 1,2,3,\cdots$ 是一个二值随机变量序列. 进一步,利用中值定理,(12)式改写成

$$P(\xi_n = 0) = \sum_{k=1}^{2^{n-1}} p_\xi(x_{k_0}) \cdot \frac{1}{2^n} = \frac{1}{2^n} \cdot \sum_{k=1}^{2^{n-1}} p_\xi(x_{k_0}),$$

$$\frac{2(k-1)}{2^n} \leqslant x_{k_0} \leqslant \frac{2k-1}{2^n};$$

$$P(\xi_n = 1) = \sum_{k=1}^{2^{n-1}} p_\xi(x_{k_1}) \cdot \frac{1}{2^n} = \frac{1}{2^n} \cdot \sum_{k=1}^{2^{n-1}} p_\xi(x_{k_1}),$$

$$\frac{2(k-1)}{2^n} \leqslant x_{k_1} \leqslant \frac{2k}{2^n}.$$

故有

$$\begin{aligned}
&|P(\xi_n = 0) - P(\xi_n = 1)| \\
&= \frac{1}{2^n} \cdot \left| \sum_{k=1}^{2^{n-1}} (p_\xi(x_{k_0}) - p_\xi(x_{k_1}) \right| \\
&\leqslant \frac{1}{2^n} \cdot \sum_{k=1}^{2^{n-1}} |p_\xi(x_{k_0}) - p_\xi(x_{k_1})| \\
&\leqslant \frac{1}{2^n} \cdot \sum_{k=1}^{2^{n-1}} |p'_\xi(x_k)| \cdot \frac{2}{2^n} \\
&\leqslant \frac{1}{2^n} \cdot 2^{n-1} \\
&\quad \times \max\{p'_\xi(x_1), p'_\xi(x_2), \cdots, p'_\xi(x_n)\} \cdot \frac{2}{2^n} \\
&= \frac{1}{2^n} \max\{p'_\xi(x_1), p'_\xi(x_2), \cdots, p'_\xi(x_n)\},
\end{aligned}$$

其中 $x_{k_0} \leqslant x_k \leqslant x_{k_1}$, $p'_\xi(x_k)$ 为 $p_\xi(x)$ 在 x 处的导数. 取极限,得

$$\lim_{n\to\infty} |P(\xi_n = 0) - P(\xi_n = 1)| = 0,$$

即

$$\lim_{n\to\infty} P(\xi_n = 0) = \lim_{n\to\infty} P(\xi_n = 1).$$

证毕.

称 ξ_i 为 ξ 的第 i 随机位,简称随机位. 定理 3 表明实型随机变量 ξ 中的随机位 ξ_i 存在均匀化的一种自然趋势,这种趋势与 ξ 自身的分布无关. 几何上解释为,随机变量 ξ 在间隔 $\frac{1}{2^n}$ 区间上具有偏差 $|p'_\xi(x_k)| \cdot \frac{1}{2^n}$ 的近似均匀分布,其平均偏差

$$\begin{aligned}
\Delta_n &= \overline{\left| p'_\xi(x_k) \cdot \frac{1}{2^n} \right|} \\
&\approx \frac{1}{2^n} \int_0^1 |p'_\xi(x)|\,\mathrm{d}x \\
&= \frac{1}{2^n} \cdot \int_0^1 |\mathrm{d}p_\xi(x)| \\
&= \frac{1}{2^n} \cdot [\mathrm{up_sum}(p_\xi(x)) \\
&\quad + \mathrm{down_sum}(p_\xi(x))], \quad (13)
\end{aligned}$$

其中 $\mathrm{up\_sum}(p_\xi(x))$ 为 $p_\xi(x)$ 增量的总和, $\mathrm{down\_sum}(p_\xi(x))$ 为 $p_\xi(x)$ 减量的总和.

显然, $p_\xi(x)$ 的变化程度影响了随机位 ξ_n 均匀分布的近似程度,但不会改变它的均匀化趋势. 为了表征随机位 ξ_n 的均匀化趋势,不妨假定 $\Delta_n = 2^{-n}$,称为理想偏差,并称随机位 ξ_n 是 n 级均匀化的,以 2^{-n} 理想偏差服从均匀分布. 随机位 n 级越高,均匀化越好.

若随机变量 $\xi \in G$, $[0,1] \subset G$,定理 3 也同样适应. 只需将 ξ 写成类似(1)式的形式

$$\xi = (-1)^s \times 2^{-b} \times 1.\xi_1\xi_2\xi_3\cdots, \quad (14)$$

其中 s 对应符号位, $b = 1023 - e$ 对应有偏指数, $\xi_1\xi_2\xi_3\cdots$ 对应尾数. 与(11)式相比,无论 $|\xi| \leqslant 1$(即 $b \geqslant 0$)还是 $|\xi| > 1$(即 $b < 0$), b 均隐含至少 1 个随机位,故 ξ_n 具有不低于 n 级的均匀化趋势.

至此,利用定理 2 和定理 3,定理 1 可证明如下:

根据定理 3,实型随机变量 $\xi \in G$,通过(14)式及(8)式和(9)式,可以表示成 $\{s, e, f\}$,其中尾数由 52 位随机位组成,即

$$f = \xi_1\xi_2\xi_3\cdots\xi_{51}\xi_{52}, \quad (15)$$

且随机位 ξ_i 以不低于 2^{-i} $(i = 1,2,\cdots,52)$ 的理想偏差服从均匀分布. 对 f 进行 bit 位变换,得

$$\mathbf{Bit}\{f\} = \xi'_{52}\xi'_{51}\cdots\xi'_{27}\xi_{27}\cdots\xi_{52}, \quad (16)$$

其中

$$\xi'_i = \xi_{53-i} \oplus \xi_i, i = 52,51,\cdots,27.$$

根据定理 2, ξ'_i 的均匀性优于 ξ_i 和 ξ_{53-i} $(i = 52,51,\cdots,27)$,即以不低于 2^{-i} $(i = 52,51,\cdots,27)$ 的理想偏差服从均匀分布. 因此,对 ξ 进行第二类 bit 位变换,得到新的随机变量 η,其值

$$\begin{aligned}
\eta = B_2(\xi) &= \{0, 1023 - b, \mathbf{Bit}\{f\}_{\leftarrow b}\} \\
&= 0.\xi'_{52}\xi'_{51}\cdots\xi'_{27}\xi_{27}\cdots\xi_{52}. \quad (17)
\end{aligned}$$

设 η 将以理想偏差 Δ_η 服从均匀分布,则由(17)式表示的随机位位置及其均匀性可得

$$\begin{aligned}
\Delta_\eta \leqslant \max\{&2^0 \cdot 2^{-52}, 2^{-1} \cdot 2^{-51}, \cdots, \\
&2^{-25} \cdot 2^{-27}, 2^{-26} \cdot 2^{-27}, \cdots, 2^{-51} \cdot 2^{-52}\},
\end{aligned}$$

即

$$\Delta_\eta \leqslant 2^{-52}.$$

随机变量 η 将以不大于理想偏差 2^{-52} 服从均匀分布.

4. 随机数均匀化普适算法的实验

以 logistic 映射，Henon 映射和 Lorenz 系统为例验证随机数均匀化普适算法，前两例是混沌映射系统，后一例是混沌微分动力系统. 都取状态序列 x_n 进行第二类 bit 位变换，分别统计变换前后的概率密度. 系统迭代计算 10 万次，所得 x_n 和 $x'_n = B_2(x_n)$ 分成 100 个盒计数. 实验结果表明，无论是映射系统还是微分动力系统，只要系统是混沌的，状态序列呈现随机性，通过随机数均匀化普适算法变换，都能获得均匀性非常好的伪随机序列.

4.1. logistic 映射

logistic 映射采用形式

$$x_{n+1} = 1 - \mu x_n^2, x_n \in [-1,1], n = 0,1,2,\cdots.$$

当 $\mu = 2$ 时，状态序列 x_n 的概率分布有规律可循，服从[7]

$$p(x_n) = \frac{1}{\pi\sqrt{1 - x_n^2}},$$
$$x_n \in [-1,1], n = 0,1,2,\cdots. \quad (18)$$

通过变量代换 $\theta_n = \frac{\arccos(x_n)}{\pi}$ 可以得到标准的均匀分布 $p(\theta_n) = 1, \theta_n \in [0,1]$，但是，这种变换用 FPGA 硬件实现非常困难，且运算速度慢. 采用随机数均匀化普适算法，可得 $x'_n = B_2(x_n), x'_n \in [0,1], p(x_n)$ 与 $p(x'_n)$ 的统计结果如图 2 所示. 统计表明，$p(x_n)$ 的曲线与(18)式一致；$p(x'_n)$ 则是均匀的，标准差为 0.0288，均匀性好. (18)式中有两个微商无穷的点，即，$p(x_n)|_{x_n = \pm 1} = \infty$，是影响均匀性的主要来源.

4.2. Hénon 映射

Hénon 映射[8] 形式为

$$x_{n+1} = 1 - ax_n^2 + y_n,$$
$$y_{n+1} = bx_n, n = 0,1,2,\cdots.$$

取 $a = 1.4, b = 0.3, x_0 = 0.3345, y_0 = 0.01$，状态变量 $|x_n| \leqslant 1.5$. 采用随机数均匀化普适算法，可得 $x'_n = B_2(x_n), x'_n \in [0,1], p(x_n)$ 与 $p(x'_n)$ 的统计结果如图 3 所示. 结果表明，$p(x_n)$ 无规律可循，变化剧烈；$p(x'_n)$ 是均匀的，标准差为 0.0447，均匀性好. 根据

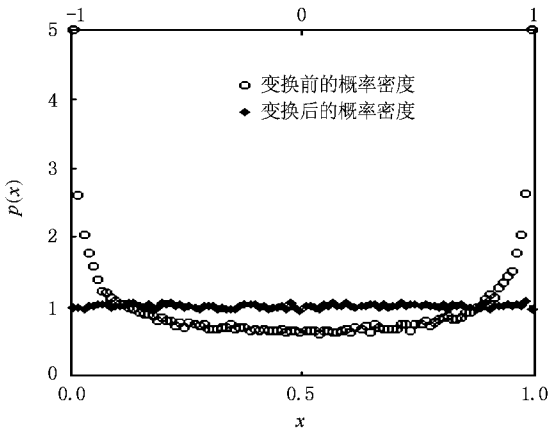

图 2　随机数均匀化普适算法对 logistic 映射序列均匀化的实验结果(系统参数 $\mu = 2$，初始点 $x_0 = 0.3345$)

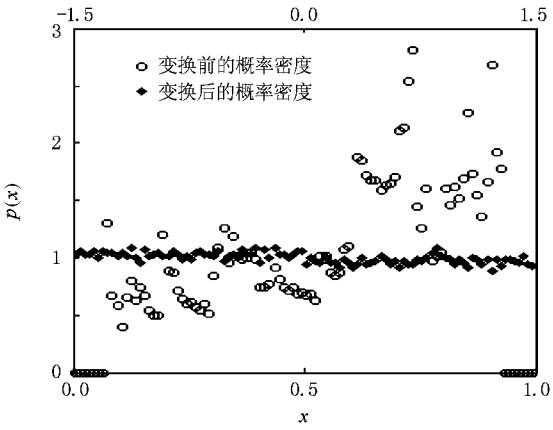

图 3　随机数均匀化普适算法对 Henon 映射序列均匀化的实验结果(系统参数 $a = 1.4, b = 0.3$，初始值 $x_0 = 0.3345, y_0 = 0.01$)

(13)式，$p(x_n)$ 的剧烈变化是影响 $p(x'_n)$ 的均匀性的主要来源，其影响程度已经高于 logistic 映射.

4.3. Lorenz 系统

Lorenz 系统是一组微分动力方程[9]，形式为

$$\dot{x} = \sigma(y - x),$$
$$\dot{y} = rx - xz - y,$$
$$\dot{z} = xy - bz.$$

取系统参数 $\sigma = 10, r = 28, b = \frac{8}{3}$，产生著名的 Lorenz 吸引子；步长取 $\Delta t = 0.01$，初始点 $x_0 = 0.3, y_0 = 0.4, z_0 = 0.5$，状态变量 $|x_n| \leqslant 20$. 采用随机数均匀化普适算法，可得 $x'_n = B_2(x_n)$. $p(x_n)$ 与 $p(x'_n)$ 的统计结果如图 3 所示. 结果表明，$p(x'_n)$ 是均匀的，标准差为 0.0297，均匀性好；除两个不连续点(对应两

个吸引不动点)外,$p(x_n)$是连续性,但也无规律可循,两个不连续点是影响$p(x'_n)$的均匀性的主要来源,影响程度与 logistic 映射相当.

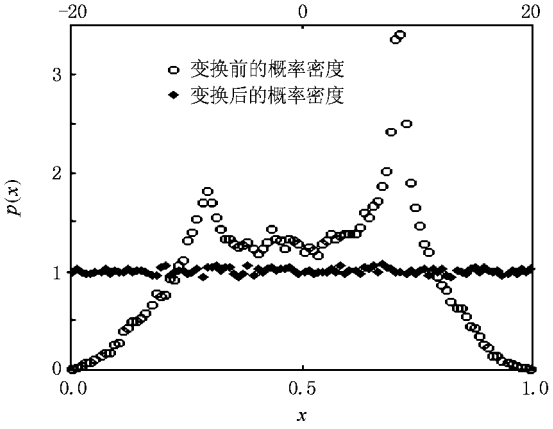

图 4 随机数均匀化普适算法对 Lorenz 系统序列均匀化的实验结果(系统参数 $\sigma=10, r=28, b=\frac{8}{3}$,步长 $\Delta t=0.01$,初始点 $x_0=0.3, y_0=0.4, z_0=0.5$)

5. 结 论

理论分析和实验表明,随机数均匀化普适算法的确是一种优异算法.由于这种算法不依赖随机变量的具体分布,理论上仅利用随机变量中随机位的均匀化趋势,技术上只需进行相关的位操作,故这种算法具有普适的价值,也为硬件实现解决了关键技术中的理论问题.

随机数均匀化普适算法主要用来将混沌序列变换成性能优异的均匀伪随机序列,本文限于篇幅,没有展开讨论其他均匀性质.但我们首次将这种算法用于 FPGA 硬件实现 TD-ERCS 混沌系统的 PRNG,伪随机序列的各种均匀性质,如游程、局部均匀性、整体均匀性等均得到改善,使之能够通过极为严格的 NIST 800-22 测试[10].

[1] Stojanoski T, Kovarev L 2001 *IEEE Trans*. CAS-Ⅰ **48** 281

[2] Wang X S, Gan J R 2002 *Chinese J*. *Comput*. **25** 352 (in Chinese) [王相生、甘骏人 2002 计算机学报 **25** 352]

[3] Li H D, Feng D G 2003 *Journal of Software* **14** 991 (in Chinese) [李红达、冯登国 2003 软件学报 **14** 991]

[4] Sheng L Y, Cao L L, Sun K H, Wen J 2005 *Acta Phys*. *Sin*. **54** 4031 (in Chinese) [盛利元、曹莉凌、孙克辉、闻 姜 2005 物理学报 **54** 4031]

[5] Wang L, Wang F P, Wang Z J 2006 *Acta Phys*. *Sin*. **55** 3964 (in Chinese) [王 蕾、汪芙平、王赞基 2006 物理学报 **55** 3964]

[6] 754-1985 *IEEE Standard for Binary Floating-Point Arithmetic* http ://standards.ieee.org/

[7] Ulan S M, Von Neumann 1947 *J*. *Bull*. *AMS* **53** 1120

[8] Hénon M 1976 *Comm*. *Math*. *Phys*. **50** 69

[9] Lorenz E N 1963 *J*. *Atmos*. *Sci*. **20** 130

[10] 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 http ://csrc.nist.gov/rng/SP800-22b.pdf

A universal algorithm for transforming chaotic sequences into uniform pseudo-random sequences*

Sheng Li-Yuan[1)†] Xiao Yan-Yu[2)] Sheng Zhe[3)]

1)(*School of Physics Science and Technology, Central South University, Changsha* 410083, *China*)

2)(*Department of Applied Mathematics Science College, University of Western Ontario London, ON, Canada* N6A 5B7)

3)(*School of Mathematical Science and Computing Technology, Central South University, Changsha* 410075, *China*)

(Received 22 August 2007; revised manuscript received 31 October 2007)

Abstract

We present a universal algorithm for transforming chaotic sequences of either chaotic map systems or chaotic differential dynamic systems into uniform pseudo-random sequences. Theoretically, the algorithm is based on bit-operations represented by floating-point algorithm, not aiming at any definite physical chaotic systems. It has been proved that, any real random variable generally has a type of natural tendency of homogenization which exponentially increases bitwise with random variable. As a result, any real chaotic sequence can be completely transformed into the pseudo-random sequence having uniform identical independent distribution. Adopting logistic map, Hénon map and Lorenz system as examples to test the universal validity of the algorithm, respectively, the experiments demonstrate that the algorithm is correct. We can reasonably expect that the universally valid algorithm should become the technological basis of standardized modular design of chaotic pseudo-random sequence generator in hardware implementation.

Keywords: chaos, pseudo-random sequences, uniform distribution function

PACC: 0545, 0250

* Project supported by the National Natural Science Foundation of China (Grant No. 60672041).

† E-mail: itpo@mail.csu.edu.cn