物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于数模混合的混沌映射实现

党小宇 李洪涛 袁泽世 胡文

Chaotic map implementation based on digital-analog hybrid method

Dang Xiao-Yu Li Hong-Tao Yuan Ze-Shi Hu Wen

引用信息 Citation: Acta Physica Sinica, 64, 160501 (2015) DOI: 10.7498/aps.64.160501
在线阅读 View online: http://dx.doi.org/10.7498/aps.64.160501
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2015/V64/I16

基于数模混合的混沌映射实现*

党小宇[1)] 李洪涛[2)†] 袁泽世[2)] 胡文[1)]

1) (南京航空航天大学电子信息工程学院, 南京 210016)

2) (南京理工大学电子工程与光电技术学院, 南京 210094)

(2015 年 2 月 5 日收到; 2015 年 4 月 16 日收到修改稿)

混沌随机序列发生器在数字实现时面临有限字长效应, 无法严格保证伪随机序列的非周期性. 构建了一类包含最少模拟器件的新数模混合系统, 分析比较了此类系统的非线性动力学行为. 利用现场可编程逻辑门阵列和 *RC* 电路实现了混沌映射, 构造了稳定的高速随机序列发生器, 可产生 100 Gbit/s 以上速率的随机数. 研究表明, 数模混合系统的混沌性对元件参数变化不敏感, 数模实现验证了新系统的存在性和物理上的可实现性. 系统易于集成在数字加密、保密通信和雷达波形产生等应用系统中.

关键词: 随机序列发生器, 有限字长, 数模混合, 非线性动力学

PACS: 05.45.–a, 05.45.Gg, 05.45.Pq, 05.45.Ra **DOI:** 10.7498/aps.64.160501

1 引 言

随机序列产生在数字加密 [1]、保密通信 [2,3] 以及雷达波形产生等 [4] 领域都有着重要的作用. 随机序列可以由物理熵源或基于混沌的确定性算法产生, 然而基于经典或量子光电子噪声的物理熵源在比特率上难以满足现代数据处理的应用需求 [5]. 基于混沌的伪随机序列可以由各类宏观或纳米尺度的微波振荡器 [5] 和光振荡器 [6] 现, 然而不论用何种器件实现, 所有的模拟实现方案 [7] 都面临着混沌系统对参数和初始值敏感的问题 [8]. 两个模拟混沌系统之间由于参数误差和干扰噪声, 难以保持长时间的稳定同步. 此外, 模拟系统无法避免参数和初始值误差通常会显著地改变混沌系统状态 [9–11], 从而影响所产生序列的统计特性的问题.

基于数字实现的混沌系统能减小模拟实现混沌系统时系统对参数和初始值误差敏感的影响, 然而数字系统的有限字长效应必然会引起动力退化 [12,13]. 数字混沌系统的动力特性退化问题成为严重影响基于数字混沌系统应用发展的瓶颈. 因此, 研究者试图通过多种方法尝试减小数字混沌系统的动力特性退化问题, 然而所有单一基于数字系统的方案都无法从根本上避免动力特性退化问题. 基于数字模拟混合实现的方案 [14–19] 由于需要引入模拟混沌系统的扰动, 因此模拟混沌系统部分将面临系统参数与初始值必然存在误差的问题.

Deng 等 [14] 设计了一个脉冲式的控制器, 与状态反馈控制器共同保证了不确定连续混沌系统同步的鲁棒性, 同时解决了数字系统动力退化的问题. Ergün 和 Güler 等 [15–17] 均采用了连续时间混沌振荡器为核心的思路, 借助部分数字器件, 实现了高速随机序列发生器. 但是由于在整体电路的设计中运用了运算放大器等模拟器件, 因此其序列产生速度和系统鲁棒性受到了限制. Hu 等 [18] 归纳了解决数字系统动力特性退化常用的方法, 包括增加计算精度、级联多个混沌系统、利用伪随机序列对系统进行扰动、切换多个混沌系统以及误差补偿方法等. 同时 Hu 等 [18] 提出了一个新的方法, 即将给定的数字混沌映射与一模拟混沌系统进行耦合, 让

* 国家自然科学基金 (批准号: 61401204, 61401198)、江苏省自然科学基金青年基金 (批准号: K2014041565)、中央高校基本科研业务费 (批准号: NP2015504) 和南京航空航天大学基本科研业务费 (批准号: NS2013025) 资助的课题.

† 通信作者. E-mail: liht@njust.edu.cn

模拟系统反控制数字映射. 虽然这一方法能有效解决系统动力特性退化问题, 但是由于其引入了一个完整的模拟混沌系统, 而模拟系统又容易受到外界条件的影响, 因此系统的鲁棒性也受到了限制. Yeniçéri 和 Yalcín [19] 提出了一种时延采样数据反馈系统, 利用模拟元器件产生动力学行为的同时, 利用数字器件组成采样和时延线作为系统反馈. 该设计思路同样采用了模拟放大器, 也存在着序列产生速度和系统鲁棒性受限的问题.

为了减小模拟部分参数对整个数字模拟混合系统的影响, 本文尝试用尽可能少的模拟器件构造数字模拟混合系统, 探讨仅用一个模拟器件的数模混合系统产生混沌随机序列的可能. 本文采用单个电容器和数字器件组成反馈结构, 构造混沌系统, 本质上解决了数字混沌系统动力退化问题, 同时最大程度地减小模拟部分参数对系统混沌性的影响, 降低模拟器件对随机序列产生速率和系统鲁棒性的限制, 仅采用单个模拟器件也使得系统更加容易集成. 经实验验证, 本文提出的数字模拟混合实现系统以现场可编程逻辑门阵列 (FPGA) 实现时, 可产生 100 Gbit/s 以上速率的随机数, 性能远优于已有的系统.

2 基于单电容反馈的数模混合混沌系统

2.1 数模混合系统动力学模型的构建

基于单电容反馈的数模混合系统框图如图 1 所示, 数字部分输出的信号经过数模转换器 D/A 转换为模拟信号激励电容器, 产生的电压响应经过模数转换器 A/D 的采集反馈回数字部分. 模拟电容的引入将在本质上避免纯数字系统的有限状态相空间问题.

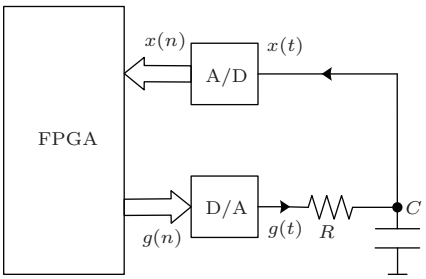

图 1 基于单电容反馈的数模混合系统框图

Fig. 1. Block diagram of digital-analog hybrid system based on single capacitance feedback.

数模混合系统可以看成带有连续时间系统反馈的离散时间系统. 反馈部分可以作为采样和保持模块, 级联采样和保持将对反馈路径上的信号进行延时. 因此, 整个系统可以称为延时数据采样反馈系统, 系统两个采样瞬间的动力学行为可以表示为 [19]

$$\begin{aligned}\dot{x}(t) = & -x(t)+\alpha g\left[x\left(t_k-\tau\right)\right], \\ & t_k \leqslant t \leqslant t_k+T_{\mathrm{s}},\end{aligned} \tag{1}$$

其中 x 为状态变量, α 为反馈权重, g 为非线性反馈函数, τ 为 x 第 t_k 个采样点处的延时总数, T_{s} 为采样周期. 在 t_k 和 t_k+T_{s} 时刻之间, 系统保持固定的采样和延时反馈 $x\left(t_k-\tau\right)$.

图 1 所示的电容器处有如下关系:

$$C\frac{\mathrm{d}x(t)}{\mathrm{d}t}=\frac{V(t)-x\left(t\right)}{R}, \tag{2}$$

其中 C 为电容器的容值, $V(t)$ 为 D/A 输出端的电压, R 为电阻的阻值. (2) 式化简后可得

$$\begin{aligned}\dot{x}(t) = & -\frac{1}{RC}x(t)+\frac{1}{RC}V(t) \\ = & -\frac{1}{RC}x(t)+\frac{1}{RC}g\left[x\left(t-\tau\right)\right],\end{aligned} \tag{3}$$

其中 $V(t)=g\left[x\left(t-\tau\right)\right]$. 当 $RC=1$, $\alpha=1$ 时, (1) 式与 (3) 式等价. 求解 (3) 式可得基于单电容反馈的数模混合系统动力学模型:

$$\begin{aligned}& x(t) \\ = & g\left[x\left(t-\tau\right)\right]-\left[g\left(x\left(t-\tau\right)\right)-x\left(t-\tau\right)\right]\mathrm{e}^{\frac{\Delta T}{RC}} \\ = & \left(1-\mathrm{e}^{\frac{\Delta T}{RC}}\right)g\left(x\left(t-\tau\right)\right)+\mathrm{e}^{\frac{\Delta T}{RC}}x\left(t-\tau\right),\end{aligned} \tag{4}$$

其中 ΔT 为采样间隔, $g(x(t-\tau))$ 为数字器件通过 D/A 输出的有限状态变量, $x(t-\tau)\in\mathbb{R}$ 是由电容引入的模拟量. (4) 式的变量本质上是属于实数空间, 从而避免了有限字长效应; 同时作为模拟量的 $x(t-\tau)$ 只有一项线性项, 对整个系统动力学行为的影响易于分析控制.

2.2 基于 Logistic 映射的系统分析

通过将简单的 Logistic 映射分别引入纯数字系统以及本文的数模混合系统, 并将系统进行对比分析, 可初步验证本文方法的正确性和有效性.

已知 Logistic 映射可以表示为

$$\begin{aligned}x(t) = & ax\left(t-\tau\right)\left[1-x\left(t-\tau\right)\right], \\ & a\in[0,4], \quad x\in(0,1),\end{aligned} \tag{5}$$

为了利用基于单电容反馈的数模混合系统实现Logistic映射, 可令(5)式等于(4)式, 得到

$$\begin{aligned} & g\left[x\left(t-\tau\right)\right] \\ &= \frac{a-\mathrm{e}^{\frac{\Delta T}{RC}}}{1-\mathrm{e}^{\frac{\Delta T}{RC}}} x\left(t-\tau\right) - \frac{a}{1-\mathrm{e}^{\frac{\Delta T}{RC}}} x^2\left(t-\tau\right) \\ &= bx\left(t-\tau\right) - cx^2\left(t-\tau\right), \end{aligned} \tag{6}$$

其中 $b = \dfrac{a-\mathrm{e}^{\frac{\Delta T}{RC}}}{1-\mathrm{e}^{\frac{\Delta T}{RC}}}$, $c = \dfrac{a}{1-\mathrm{e}^{\frac{\Delta T}{RC}}}$. 将(6)式代入(4)式中, 即可得到在Logistic映射下数模混合系统动力学模型的输出.

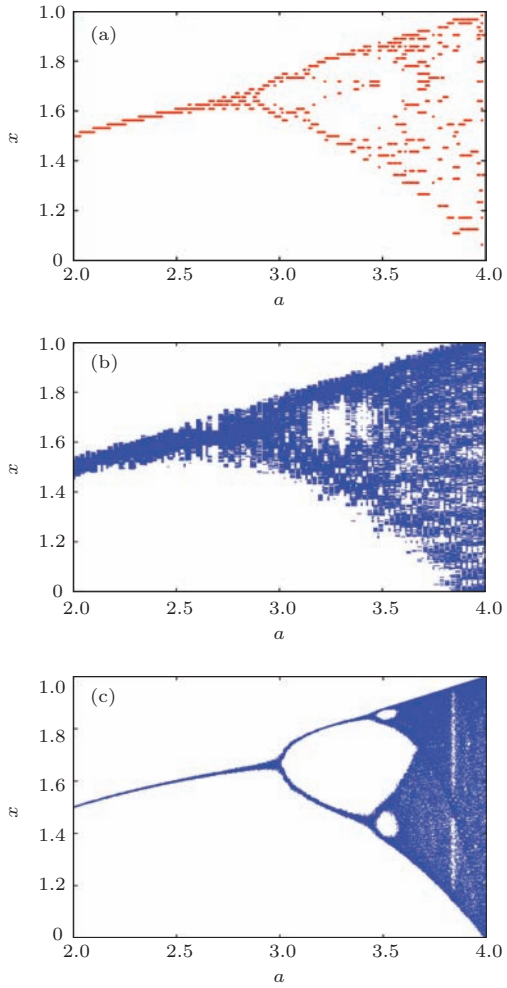

图2 (网刊彩色) Logistic映射的分岔图和Lyapunov指数谱 (a) 纯数字系统(量化位数 $N=6$); (b) 数模混合系统(量化位数 $N=6$); (c) 数模混合系统(量化位数 $N=10$) ($R=100\ \Omega$, $C=1\ \mu\mathrm{F}$, $\Delta T=10^{-4}$ s)

Fig. 2. (color online) Bifurcation diagram and Lyapunov exponent spectrum of Logistic map: (a) digital system (digitalizing bit $N=6$); (b) hybrid system (digitalizing bit $N=6$); (c) hybrid system (digitalizing bit $N=10$); ($R=100\ \Omega$, $C=1\ \mu\mathrm{F}$, $\Delta T=10^{-4}$ s).

图2分别给出了采用纯数字系统(量化位数为 $N=6$)以及本文数模混合系统(量化位数分别为 $N=6$ 和 $N=10$)所得到的Logistic映射分岔图. 采用纯数字系统时, 因为其映射斜率均为0, 此时求得系统的Lyapunov指数为负无穷大, 系统始终不会产生混沌现象; 采用数模混合系统时, 计算可得数模混合系统的Lyapunov指数为 $\mathrm{e}^{\frac{\Delta T}{RC}}$, 为一仅与电阻、电容值以及时间参数的选取有关的值. 当电阻、电容值以及时间参数给定时, Lyapunov指数为一恒定值且始终大于零, 系统始终处于混沌状态.

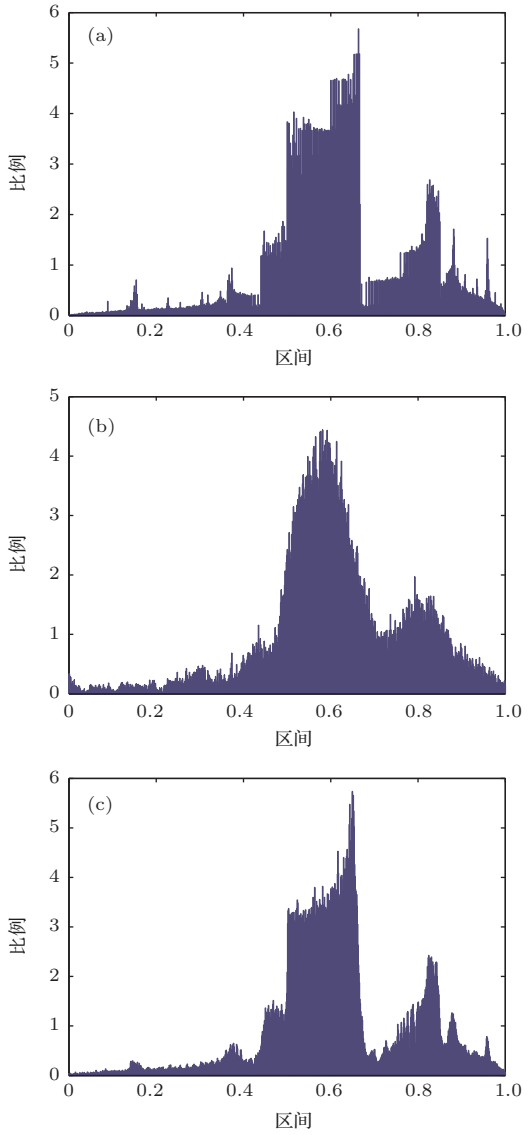

图3 (网刊彩色) 统计直方图 (a) 理想映射; (b) 数模混合系统(量化位数 $N=6$); (c) 数模混合系统(量化位数 $N=10$)

Fig. 3. (color online) Statistical histogram: (a) ideal mapping; (b) hybrid system (quantization length $N=6$); (c) hybrid system (quantization length $N=10$).

从图2 (a) 和 (b) 可以看出, 数模混合系统所得到的Logistic映射分岔图其效果比纯数字系统所得到的要好得多, 且随着量化位数 N 的增加, 数模混合系统得到的分岔图精度越来越高, 越来越逼近理想的Logistic映射分岔图. 为了精确地描述分岔图的逼近程度, 本文引入比较直方图间距的图像相似度检测方法来量化这一程度. 图3给出了理想的Logistic映射分岔图和不同量化位数的数模混合系统分岔图所对应的直方图.

直方图间的距离可使用一般的欧氏距离函数来衡量, 即

$$M_{\mathrm{E}}(Q,D)=\sqrt{\sum_{i=1}^{L}\left[H_Q(i)-H_D(i)\right]^2},$$

其中 $H(k)$ 为图像特征的统计直方图. 仿真可得量化位数 $N=6$ 时, 数模混合系统与理想映射直方图间的距离为19.1734, 量化位数 $N=10$ 时, 距离为11.1837, 可知量化位数 $N=10$ 时数模混合系统的直方图与理想映射的直方图更加接近, 也即分岔图更加逼近理想映射的分岔图.

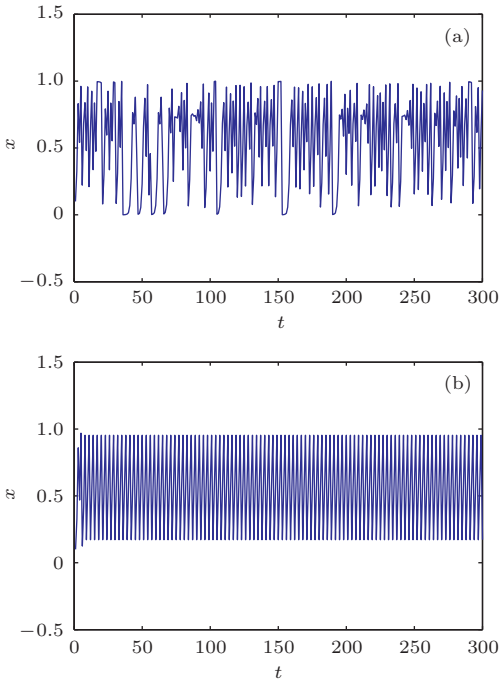

图4 (网刊彩色) 序列时序图 (量化位数 $N=6$, $a=3.9$) (a) 数模混合系统; (b) 纯数字系统

Fig. 4. (color online) Sequence diagram of x (quantization length $N=6$): (a) hybrid system; (b) digital system.

图4给出了当量化位数 $N=6$, $a=3.9$ 时, 本文数模混合系统和纯数字系统所产生的序列时域图. 从图4中可看出, 纯数字系统在较短的时间内即转变为周期序列, 而本文数模混合系统则保证了系统始终处于混沌状态中, 进一步验证了之前对两种系统Lyapunov指数的分析.

3 随机数发生器

本文第2部分给出了采用基于单电容反馈的数模混合系统实现Logistic映射的输出结果, 并与纯数字系统相比较验证了本文方法正确性和有效性. 然而在实际应用中, Logistic映射过于简单, 难以产生性能优异的伪随机序列, 因此本文将采用更为复杂的耦合锯齿映射[20]来设计随机数发生器.

近邻耦合单峰映像格子模型可以表示为

$$\begin{aligned}&x_n(i)\\&=(1-\eta)f(x_{n-1}(i))+\frac{\varepsilon}{2}\big[f(x_{n-1}(i-1))\\&\quad+f(x_{n-1}(i+1))\big],\end{aligned}\tag{7}$$

其中, n 表示离散时间步数; $i=1,2,\cdots,L$ 为离散格点坐标, L 为系统级数; η 为耦合系数, 且满足 $0<\eta<1$. 边界条件服从 $x_n(L)=x_n(0)$, 初始条件取 [0, 1] 内的随机数. (7) 式中非线性函数 $f(x)$ 为锯齿映射, 其迭代方程如下:

$$x_{n+1}=F(x_n)=\beta x_n\,(\mathrm{mod}1),\tag{8}$$

其中 $F:[0,1]\to[0,1]$, 当 $1<\beta\in\mathbb{R}$ 时, 系统处于混沌状态.

令 (7) 式与 (4) 式相等, 可以得到近邻耦合锯齿映射下数模混合系统的输出 $x(t)$, 其中 $g(x(t-\tau))$ 的表达式如下:

$$\begin{aligned}&g(x(t-\tau))\\&=-\frac{\mathrm{e}^{\frac{\Delta T}{RC}}}{1-\mathrm{e}^{\frac{\Delta T}{RC}}}x(t-\tau)+\frac{1}{1-\mathrm{e}^{\frac{\Delta T}{RC}}}x_{n+1}(i)\\&=bx(t-\tau)+c\Big\{(1-\varepsilon)f(x(i))\\&\quad+\frac{\varepsilon}{2}\left[f(x(i-1))+f(x(i+1))\right]\Big\},\end{aligned}\tag{9}$$

式中

$$b=-\frac{\mathrm{e}^{\frac{\Delta T}{RC}}}{1-\mathrm{e}^{\frac{\Delta T}{RC}}},\qquad c=\frac{1}{1-\mathrm{e}^{\frac{\Delta T}{RC}}},$$

$x_{n+1}(i)$ 为近邻耦合单峰映像格子模型.

图5给出了近邻耦合单峰映像格子模型原分岔图以及经过数模混合系统后的分岔图, 其中分

岔参数为$\beta \in (0,4]$, 耦合系数$\eta = 0.01$, 系统级数$L = 15$, 分岔输出级数$L = 5$. 数模混合系统中$R = 100\ \Omega$, $C = 1\ \mu\text{F}$, $\Delta T = 10^{-4}\ \text{s}$, 量化位数分别为$N = 8$和$N = 16$. 从图5 (a)中可以看出, 当$\beta > 1$时, 原系统处于混沌状态; 从图5 (b)和(c)中可以看出, 数模混合系统输出始终处于混沌状态, 与第二部分的分析一致. 但是当量化位数较低时, 明显看出分岔图呈条带状, 与原系统混沌状态时的分岔图差距较大, 而随着量化位数的提高, 分岔图则更接近原系统的分岔图. 图6给出了数模混合系统的相轨图, 输出级数$L = 5$.

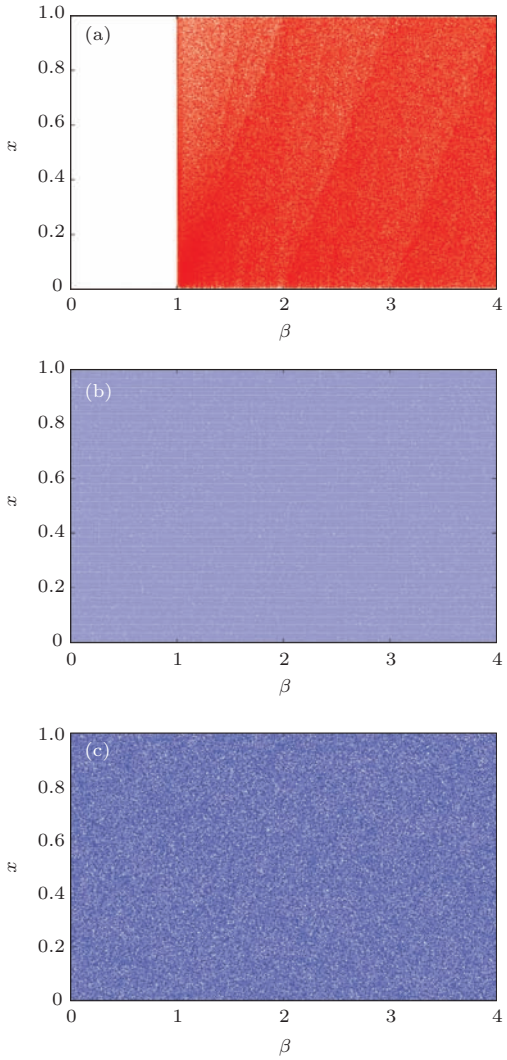

图5 (网刊彩色) 近邻耦合单峰映像格子模型分岔图 (a) 原系统; (b) 数模混合系统$N = 8$; (c) 数模混合系统$N = 16$

Fig. 5. (color online) Bifurcation diagram of two-way coupled saw tooth map lattice: (a) original system; (b) hybrid system $N = 8$; (c) hybrid system $N = 16$.

为了得到只包含0和1元素的随机信号序列, 还需要对混合系统输出进行量化, 得到0/1二进制序列$\{s_n(t)\}|_{t=1}^{\infty}$, 其量化函数$T_n(x_i)$定义如下:

$$\{s_n(t)\}|_{t=1}^{\infty} = T_n(x_i) = \begin{cases} 0, & x \in U_{d=0}^{2^{n-1}-1} I_{2d}^n, \\ 1, & x \in U_{d=0}^{2^{n-1}-1} I_{2d+1}^n, \end{cases} \tag{10}$$

其中n为正整数, $I_0^n, I_1^n, \cdots, I_{2^n-1}^n$为$[0,1]$间的$2^n$个连续等分区间, $U_{d=0}^{2^{n-1}-1} I_{2d}^n$, $U_{d=0}^{2^{n-1}-1} I_{2d+1}^n$分别代表偶数区间和奇数区间取并集. 随着$n$的增大, 等分区间增多, 使得这种量化函数可以保证序列有着良好的统计特性.

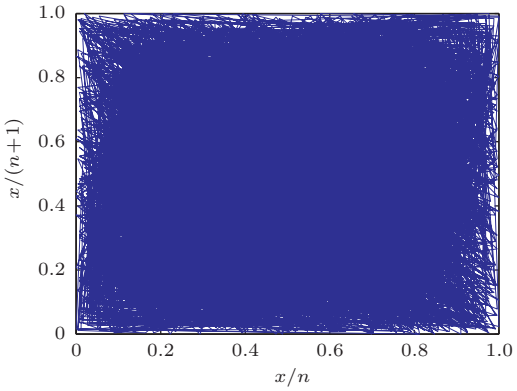

图6 (网刊彩色) 近邻耦合单峰映像格子模型相轨图

Fig. 6. (color online) Phase portrait of two-way coupled saw tooth map lattice.

在设计制作实际电路之前, 本文首先利用Matlab仿真产生数模混合系统下近邻耦合锯齿映射所对应的伪随机序列(PN), 然后利用Nist-800-22rev1a测试套件对所得的序列进行测试[15]. 该套件共有15项测试标准, 专用于测试由硬件或软件产生的长随机序列的随机性. 其中Frequency测试主要测试随机序列中的0/1元素数量是否大致相等, 应当首先进行. 在Frequency测试通过的情况下才考虑进行其他测试.

测试时选取序列长度为40 Mbit, 将其分为100个数据流进行测试. 对应于每种测试标准, 都会计算出相应的P值, 然后与已知的显著性水平α相比较, 当$P < \alpha$时, 就判定所测序列未通过测试, 否则判定为通过测试. 本测试套件所选取的显著性水平$\alpha = 0.01$.

利用纯数字系统所得随机序列进行测试, 其中量化位数$N = 8$. 计算得相应P值为0.00439, 此时序列未通过Frequency测试, 因此其他测试均没有进行, 即采用纯数字方法所得的随机序列性能很差, 无法实际应用.

表 1 数模混合系统伪随机序列的 NIST 测试结果

Table 1. NIST test results of hybrid system PN sequence.

测试项目	P	成功比例	测试结果
Frequency	0.514124	100/100	通过
Block frequency	0.304126	99/100	通过
Cumulative sums	0.616305	100/100	通过
Cumulative sums	0.171867	100/100	通过
Runs	0.699313	98/100	通过
Longest run	0.304126	100/100	通过
Rank	0.834308	100/100	通过
FFT	0.816537	100/100	通过
Non-overlapping template	0.350485	95/100	通过
Overlapping template	0.066882	99/100	通过
Universal	0.678686	99/100	通过
Approximate entropy	0.678686	100/100	通过
Random excursions	0.419021	47/50	通过
Random excursions variant	0.383827	49/50	通过
Serial	0.437274	98/100	通过
Serial	0.816537	99/100	通过
Linear complexity	0.978072	98/100	通过

表 1 给出了利用本文基于单电容反馈的数模混合方法所得序列进行测试所得到的结果, 量化位数同样为 $N = 8$, 耦合系数 $\eta = 0.01$, 系统级数 $L = 15$, 分岔参数为 $\beta = 191/17$. 从表 1 可以看出, 仿真采用本文数模混合系统, 结合近邻耦合锯齿映射所产生的伪随机序列, 可以顺利通过 NIST 所有测试, 且 100 个数据流中的成功比例非常高, 即数模混合系统是可行且有效的.

4 电路实现与结果分析

图 7 给出了基于单电容反馈的数模混合系统所实现的随机序列发生器的电路图, 电路实现分为数字模块、数模转换模块以及模拟模块, 其中数字模块又包括序列输出子模块和映射子模块, 映射子模块则由 L 个映射单元组成. 图 8 为映射子模块中每个映射单元的具体结构图, 其中

$$b = -\frac{\mathrm{e}^{\frac{\Delta T}{RC}}}{1-\mathrm{e}^{\frac{\Delta T}{RC}}}, \quad c = \frac{1}{1-\mathrm{e}^{\frac{\Delta T}{RC}}},$$

$x_{n+1}(i)$ 为近邻耦合单峰映像格子模型.

电路的工作流程如下: 数字模块利用 FPGA 来产生出所需要的 $g(n)$ 的值, 经过 D/A 后将值输入到模拟模块, 即 RC 电路以激励电容器, 完成微分运算. 得到的电压响应 $x(t)$ 经过 A/D 转换后, 反馈回数字模块. 其中映射子模块中的 $1, 2, \cdots, L$ 单元分别对应近邻耦合单峰映像格子模型中的 $1, 2, \cdots, L$ 级, 而序列输出子模块则可以根据需求, 从映射子模块中抽取任意单元, 经量化和组合后得到所需的随机序列.

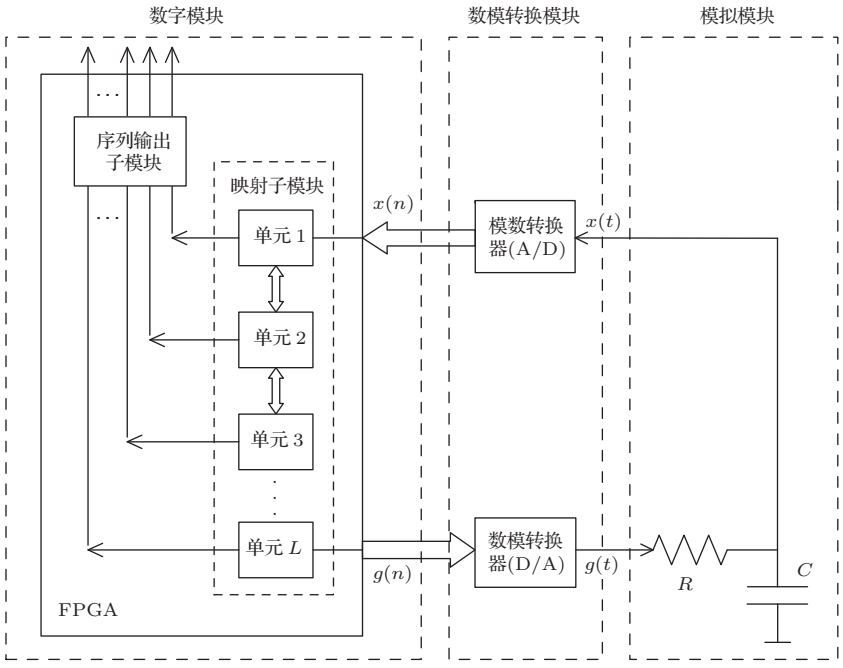

图 7 数模混合系统随机序列发生器电路图

Fig. 7. Circuit diagram of hybrid system random sequence generator.

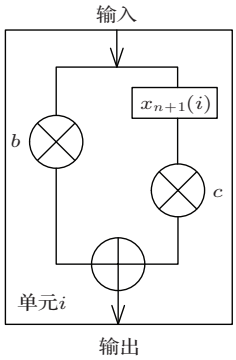

图 8 映射子模块映射单元结构图

Fig. 8. Map unit structure diagram of submodule.

本数模混合随机序列发生电路具有如下优点: 1) 以最少的模拟器件保证系统的混沌性, 同时有效避免了模拟器件参数不稳定且易受环境影响的缺点, 保证了电路的稳定性; 2) 映射子模块占用芯片资源极少, 单元数 L 可以任意扩展, 只需相应改变映射的级数 L 就可以产生更高速率的随机数, 例如 FPGA 工作频率为 200 MHz, 若采用以映射子模块每一级均取出数据进行量化的工作方式, 那么产生的随机序列带宽可达 $200L$ MHz, 根据目前 FPGA 芯片的容量及规模, 可产生 100 Gbit/s 以上速率的随机数, 易于满足各种需求; 3) 系统基于数字芯片和一个模拟器件实现, 结构上兼容且易于集成到现有的电路系统中.

表 2 数模混合系统伪随机序列的 NIST 测试结果

Table 2. NIST test results of hybrid system PN sequence.

测试项目	P	成功比例	测试结果
Frequency	0.724431	100/100	通过
Block frequency	0.436851	99/100	通过
Cumulative sums	0.775489	100/100	通过
Cumulative sums	0.423367	100/100	通过
Runs	0.812365	98/100	通过
Longest run	0.523366	100/100	通过
Rank	0.896587	100/100	通过
FFT	0.912354	100/100	通过
Non-overlapping template	0.425896	97/100	通过
Overlapping template	0.225478	99/100	通过
Universal	0.869954	99/100	通过
Approximate entropy	0.871123	100/100	通过
Random excursions	0.419021	49/50	通过
Random excursions variant	0.383827	49/50	通过
Serial	0.437274	98/100	通过
Serial	0.816537	99/100	通过
Linear complexity	0.978072	98/100	通过

表 2 给出了利用上述电路所产生的随机序列进行 NIST 测试时所得到的结果, 此时选取映射子模块的级数 $L = 500$, 序列长度为 1 Gbit, 将其分为 100 个数据流进行测试. 从表 2 中可以看出, 所产生的随机序列顺利通过所有测试, 且与纯数字系统所得随机序列相比, 实际电路的成功比例更高, 序列的随机性更好.

5 结 论

随着随机序列在各个领域的广泛使用, 对随机序列发生器的要求也日益增高. 基于模拟实现方法的混沌随机序列发生器面临着混沌系统对参数和初始值敏感的问题, 从而影响所产生序列的统计特性, 因此大大限制了其应用范围; 基于数字实现的混沌系统能减小模拟实现混沌系统时系统对参数和初始值误差敏感的影响, 然而数字系统的有限字长效应必然会使混沌序列退化为周期序列, 无法产生真正意义上的随机序列.

基于对以上问题的分析, 本文综合了模拟方法与数字方法的优点, 尝试用尽可能少的模拟器件构造数字模拟混合系统, 提出了仅有一个模拟器件的数模混合系统, 解决了系统动力学行为退化、系统模拟器件过多限制了序列产生速率和系统鲁棒性等问题, 使系统更加易于集成. 给出了基于单电容反馈的数模混合系统框图, 分析了数模混合系统的实现方法和有效性, 并结合多种映射给出了仿真结果图, 利用 NIST 测试套件对仿真产生的混沌随机序列进行了测试. 实际电路验证了强的鲁棒性、无有限字长效应、易于产生高速率随机数以及便于集成的优点. 最终电路产生的随机序列以较高成功率顺利通过 NIST 所有测试, 验证了本文方法的正确性和有效性. 本文方法将能够很好地满足数字加密、保密通信以及雷达波形产生等领域的实际工程需求.

参考文献

[1] Gallager R G 2008 *Principles of Digital Communication* (Vol. 1) (Cambridge: Cambridge University Press)

[2] van Wiggeren G D, Roy R 1998 *Phys. Rev. Lett.* **81** 3547

[3] Uchida A 2012 *Optical Communication with Chaotic Lasers: Applications of Nonlinear Dynamics and Synchronization* (New York: John Wiley & Sons)

[4] Gini F, Maio A D, Patton L 2012 *Waveform Design and Diversity for Advanced Radar Systems* (UK: The Institution of Engineering and Technology)

[5] Li W, Reidler I, Aviad Y, Huang Y Y, Song H L, Zhang Y H, Rosenbluh M Kanter I 2013 *Phys. Rev. Lett.* **111** 044102

[6] Naruse M, Kim S J, Aono M, Hori H, Ohtsu M 2014 *Sci Rep.* **4** 6039

[7] Petrie C S, Connelly J A 2000 *IEEE Trans. Circuits-I* **47** 5

[8] Bao B C, Hu W, Xu J P, Liu Z, Zou L 2011 *Acta Phys. Sin.* **60** 120502 (in Chinese) [包伯成, 胡文, 许建平, 刘中, 邹凌 2011 物理学报 **60** 120502]

[9] Li C B, Sprott J C 2014 *Int. J. Bifurc. Chaos* **24** 1450131

[10] Li C B, Sprott J C, Thio W 2014 *J. Exp. Theor. Phys.* **118** 494

[11] Li C B, Sprott J C 2014 *Phys. Lett. A* **378** 178

[12] Shao S Y, Min F H, Wu X H, Zhang X G 2014 *Acta Phys. Sin.* **63** 060501 (in Chinese) [邵书义, 闵富红, 吴薛红, 张新国 2014 物理学报 **63** 060501]

[13] Wang G Y, Bao X L, Wang Z L 2008 *Chin. Phys. B* **17** 3596

[14] Deng Y S, Hu H P, Xiong N X, Xiong W, Liu L F 2015 *Inform. Sci.* **305** 146

[15] Ergün S, Özoğuz S 2010 *Int. J. Circ. Theor. Appl.* **38** 1

[16] Güler Ü, Ergün S 2010 *ICECS 17th IEEE International Conference* Athens, December 12–15, 2010 p1037

[17] Ergün S 2014 *Circuits and Systems (APCCAS), 2014 IEEE Asia Pacific Conference* Ishigaki, November 17–20, 2014 p217

[18] Hu H P, Deng Y S, Liu L F 2014 *Commu. Nonlinear Sci.* **19** 1970

[19] Yeniçéri R, Yalçín M E 2013 *Electron. Lett.* **49** 543

[20] Tong Q Y, Zeng Y C 2003 *Acta Phys. Sin.* **52** 285 (in Chinese) [童勤业, 曾以成 2003 物理学报 **52** 285]

Chaotic map implementation based on digital-analog hybrid method*

Dang Xiao-Yu[1)] Li Hong-Tao[2)†] Yuan Ze-Shi[2)] Hu Wen[1)]

1) (*Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China*)

2) (*Nanjing University of Science and Technology, Nanjing 210094, China*)

(Received 5 February 2015; revised manuscript received 16 April 2015)

Abstract

Random number generator plays an important role in many domains, including secret communication, radar waveform generation, etc. However, the existing methods for generating random numbers cannot meet the actual demand for speed. Even worse, the use of analog device will restrict the speed of generator and robustness of system. As a result, researchers start to turn their eyes to digital implementation which is stabler and more efficient than the analog counterpart. Unfortunately, digital methods still have the disadvantages of dynamical degradation because of word length limitation effect. Though some remedies, such as increasing computing precision, cascading multiple chaotic systems, pseudo-randomly perturbing the chaotic system, the switching multiple chaotic systems and error compensation method are proposed, but the limitations are still inevitable. In recent researches, continuous-time chaotic oscillators are used with digital devices to realize random number generator, and a new approach is proposed to solve the dynamical degradation of digital chaotic system by coupling the given digital chaotic map with an analog chaotic system, where the analog chaotic system is applied to anti-control the given digital chaotic map. However, this method also requires a whole continuous-time system realized with analog devices, which confines the system performance.

In this paper, a new digital-analog hybrid chaotic map with only one analog capacitor is constructed to produce random numbers. Firstly, the block diagram of digital-analog hybrid system based on the single capacitance feedback is given, and the model of the system is derived from the block diagram. Secondly, the simple logistic map is applied to the model and its nonlinear dynamics behaviors are analyzed and compared to verify the correctness and effectiveness of the proposed method. Then a more complex two-way coupled saw tooth map is used to produce pseudorandom sequences through simulation smoothly.

When designing the circuits of the system, a digital-analog hybrid implementation with field programmable logic gate array and a single analog capacitor is used to realize chaotic maps, showing that it can overcome the finite word length effect of digital implementation. NIST, a general statistical test suiting for random and pseudorandom number generator cryptographic applications, is used to test the sequences produced by the new system. The results show that the new hybrid system is insensitive to the evolution of circuit parameters and the randomness of sequence is in accordance with the practical application. The circuit implementation verifies the numerical simulation and theoretical results. The high speed digital devices and a single analog capacitance are applied to the proposed random sequence generator, and therefore it can be integrated easily into the systems of digital encryption, secure communication and radar waveform generation.

Keywords: random number generator, limited word length, digital-analog hybrid, nonlinear dynamics

PACS: 05.45.–a, 05.45.Gg, 05.45.Pq, 05.45.Ra **DOI:** 10.7498/aps.64.160501

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61401204, 61401198), the Natural Science Foundation Youth Foundation of Jiangsu Province, China (Grant No. K2014041565), the Fundamental Research Funds for the Central Universities, China (Grant No. NP2015504), and the Fundamental Research Funds of Nanjing University of Aeronautics and Astronautics, Chian (Grant No. NS2013025).

† Corresponding author. E-mail: liht@njust.edu.cn