一种数字化混沌扩频序列发生器的设计 [1]

饶妮妮

(电子科技大学生命科学与技术学院 成都 610054)

摘 要 该文给出了一种基于 FPGA 芯片的数字化分段线性混沌映射系统的设计方法，该方法利用了 m 序列的扰动来克服有限精度下混沌序列的短周期行为；对用 VHDL 实现的分段线性混沌序列发生器进行了门级仿真；将数字混沌序列的平衡性、相关性和线性复杂度等与实值混沌序列进行了比较，结论为：数字混沌序列的平衡性略比实值混沌序列差；自相关特性略好；N=63, 255 时，互相关特性略好，而 N=31, 127 时互相关特性略差；二者的线性复杂度相当，为分段线性映射系统应用于扩频通信领域探索了一条途径。

关键词 数字混沌扩频序列，有限精度效应， VHDL，自顶向下，统计特性

中图号 TN914.4, TN711.4

1 引 言

理论上，混沌序列在扩 / 跳频通信领域中具有作扩频码的应用价值 [1−3] 。例如， Logistic 映射、 Tent 映射以及 Chebyshev 映射等已被建议作为扩频码 [4] 。大多数混沌映射系统是模拟的，然而，许多实际应用系统需要的却是数字混沌序列。在数字化混沌映射系统的具体实现中，会遇到有限精度问题。有关研究表明：有限精度效应限制了数字混沌序列的各项特性，如果实现精度越高，数字混沌序列的各项特性与实值混沌序列的特性就越接近，但同时也提高了电路的硬件复杂度和运算代价。有限精度效应是目前混沌系统从理论走向应用的一大难题。在众多的混沌系统中有一类被称为 “分段线性映射” 的系统，多年的研究表明它们具有均匀的分布函数及可控的统计特性 [5,6] 。文献 [7] 证实了分段线性化映射作为扩频码的可行性。本文给出了一种基于 FPGA 芯片的数字化分段线性混沌映射系统的设计方法，该方法利用了 m 序列的扰动来克服有限精度下混沌序列的短周期行为；对用 VHDL 实现的分段线性混沌序列发生器进行了门级仿真；将数字混沌序列的平衡性、相关性和线性复杂度等与实值混沌序列进行了比较，为分段线性映射系统应用于扩频通信领域探索了一条途径。

2 混沌发生器算法原理

2.1 *算法* 本文采用的分段线性离散混沌系统的算法如下：

$$x_{t+1}=F(x_t)=\begin{cases}-1+2(x_t+1)/p, & x_t\le -1+p\\ -1+2(x_t+1-p)/(1-p), & -1+p<x_i\le 0\\ F(-x_t), & x_t>0\end{cases} \tag{1}$$

其中 $p\in(0,1)$, $I=[-1,1]$, $x_t\in I$ 。文献 [5] 已经证明，迭代系统 (1) 式是混沌的；它的输出信号 $\{x_t\}$ 在 I 上遍历且具有均匀的不变分布函数 $f(x)=0.5$ 。

对上述模拟信号进行量化得到 0–1 二进制混沌序列 $\{b_n(t)\}|_{t=1}^{\infty}$ 。不同的量化函数对混沌二进制序列的自相关、互相关和平衡性产生的影响不同。现有多种量化方法，为了便于硬件实现，本文选用的量化方法是：将实值 $\{x_t\}$ 的绝对值的有效值用 m 比特来表示：

$$|x_t|=0.b_1(x_t)b_2(x_t)\cdots b_n(x_t)\cdots b_m(x_t), \qquad b_n(x_t)\in(0,1) \tag{2}$$

取每一个实值 $\{x_t,t=1,2,\cdots,\infty\}$ 的第 n 比特，可得二进制混沌序列 $\{b_n(t)\}|_{t=1}^{\infty}$ 。$\{b_n(t)\}|_{t=1}^{\infty}$ 称为实值混沌序列。文献 [7] 的结论表明，这类混沌序列适于作扩频通信系统的扩频码。

[1] 2000-08-04 收到， 2001-03-19 定稿
国防通信抗干扰技术重点实验室预研基金项目资助

2.2 *算法的改进*　由 (1) 式知，所有的计算都是在负数域内进行，给位处理增加了一些麻烦，例如，比较器一般是按无符号数来设计的。为了便于硬件实现，对算法进行对称变换，使所有的计算在正数域内进行，则

$$x_{t+1}=F(x_t)=\begin{cases}1-2(1-x_t)/p, & 1-p<x_t\le 1\\ 1-2(1-p-x_t)/(1-p), & 0<x_t\le 1-p\\ F(-x_t), & x_t<0\end{cases}\tag{3}$$

显然，这种对称变换不会改变混沌序列的特性。

数字电路的有限精度效应使混沌系统产生短周期的混沌序列并且统计特性变差。对混沌系统施加 m 序列扰动，可以增加混沌序列的周期，改善混沌序列特性 [7,8]。改进后的混沌发生器如图 1 所示。

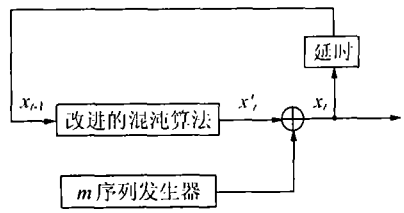

图 1　改进的混沌发生器框图

2.3 *数制的选择*　兼顾数字混沌序列的特性和硬件电路的复杂度，混沌发生器的精度设定为 32bit。由于最终的结果是在 $[-1,1]$ 之间的浮点数，所以量化时应将其均匀量化成 $-2\times10^{31}\sim+2\times10^{31}$ 之间的带符号数参加运算。由于浮点运算在硬件实现上比整数复杂得多，所以本文采用的表数格式为：符号位加数的绝对值。

在 (3) 式的算法中，有大量的 $1-X$ 型算式。不难证明，当 X 分别取 $[0,1]$ 和 $[1,2]$ 两个区间内的值时，采取这种表数方法使 $1-X$ 型的运算分别简化为：若 $X\in[0,1]$，则 $Y=1-X=\overline{X}$；若 $X\in[1,2]$，则 $Y=1-X=X$。

证明　由于文中 32bit 的数是用来表示绝对值小于 1 的带符号数，当 $X\in[1,2]$ 时，若要表示完整的数，可令 $X=1+W$，其中 $W\in[0,1]$。数值 1 若表示成 31bit 的数则是 8000H，最高有效位是 '1'(第 32bit)。若用 31bit 的范围表示大于 1 的数，将会发生溢出，其溢出的那一位则是在符号位上。在这个阶段，出现负数是不可能的。所以可以利用它暂时表示大于 1 的正数，最高位 1 表示其整数位 1，其余 31bit 是小数部分。这样，在实现 $1-X$ 计算时，只需把其最高位清零便实现了 $1-X$ 的操作。当 $X\in[0,1]$，取其相反数即可实现 $1-X$ 型运算。

证毕

在正数域，这种符号位加绝对值的表数方法和补码的意义是一样的，因而也可简化算法中的 $1-(X+P)$ 型运算。

2.4 *算法的硬件设计*　若直接就改进后的算法进行硬件设计，仍然存在硬件电路重复使用的问题。3 个判断分支语句将需要 3 个比较器，判断后将需要至少两个除法器进行数据处理。考虑每一时刻只有一个数据处理单元在工作，因而可先进行数据的判断，将判断后的数据用不同的处理方式处理之后再进行统一计算，以减少硬件上的冗余。具体方法如下：

运算时若 x_t 为负值，则要先计算一次相反数再进入迭代。在开始执行算法之前，可设计一个判断数值正负性的单元。若正则直接进入区间判断；若负则先取其相反数再进入区间判断，相当于再进入下一次迭代。之后加一级比较器，将判断正负后的值和 $1-p$ 进行比较，输出大于

则表示 $x_t > 1-p$；输出小于则表示 $0 < x_t < 1-p$(这种情况有可能是本次的 x_t 大于零后到这一步，也可能是上一次的 x_{t-1} 小于零再取其相反数后进入这一步)。

关于算法中的一些 $1-2X$ 型运算单元，令 $F(X) = 1-2X$，其中，$F(X) \in [-1,1]$，$X \in [0,1]$。(1) 若 $X > 0.5$，则 $F(X) < 0$，令 $X = 0.5 + w$，则 $F(X) = 1-2w$；(2) 若 $X < 0.5$，则 $F(X) > 0$，令 $w = X$，则 $F(X) = 1-2w$；至于 $G(w) = 2w$ 的运算，只需让 w 左移一位，便可实现乘二的功能；按位取反再加一，就可实现 $-X$ 的运算。若 $X \in [0,1]$，$1-X$ 的运算就是 $\overline{X}$。

根据以上分析，可得实现算法的硬件结构如图 2 所示。

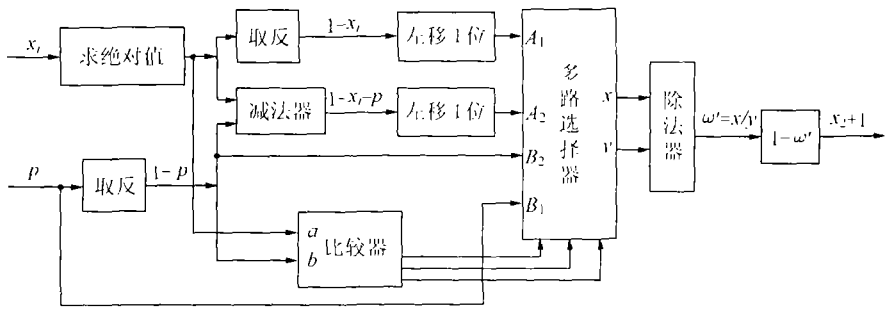

图 2 算法的硬件结构框图

3 混沌发生器的 VHDL 实现

3.1 实现方法 采用自顶向下的设计思想，将混沌发生器按功能分成 7 个模块，如图 3 所示。所有模块均按 IEEE 在 1993 年新修订的 VHDL 标准格式编写；涉及的信号定义、语法均依据 IEEE Standards LRM(Language Reference Manual)[10]；采用了 IEEE 的标准四值逻辑。各模块功能分别是：(1) ISA 总线接口模块：实现和计算机通信与接口，赋初值；(2) 迭代控制模块：实现条件分支的判断、前后两次迭代的控制；(3) 算法产生模块：实现数字化混沌序列的产生；(4) 干扰序列产生模块：实现干扰序列的产生，同时输出 m 序列；(5) 干扰合成模块：把来自算法产生和干扰产生两个模块的信号进行综合，产生混沌序列；(6) 时钟产生模块：实现各模块之间的同步；(7) 输出控制模块：将 m 序列、混沌序列输出，并同时输出和各个序列对应的同步时钟脉冲。

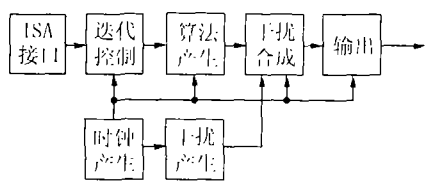

图 3 混沌发生器的 VHDL 实现模块

3.2 仿真结果

3.2.1 行为级仿真 行为级仿真是在 Talent2000 下用其模拟器 Vsim 进行的。对各模块的 VHDL 仿真程序进行验证，结果均符合要求。

3.2.2 门级仿真　门级仿真是在 Max+plusII 下用波形仿真实现的。在混沌发生器的门级仿真中，设置系统工作时钟为：$f_s = 10\text{MHz}, T = 0.1\mu\text{s}$；产生干扰序列的时钟：$f = 0.625\text{MHz}, T = 1.6\mu\text{s}$；产生混沌序列的时钟 $f = 0.15625\text{MHz}, T = 6.4\mu\text{s}$。经反复验证，门级仿真下混沌发生器电路的稳定很好。取初值 $x_0 = 4A7F2456\text{H}, p = 6\text{FD2C431H}$，产生的数字混沌序列局部波形如图 4 所示。仿真实验也表明，用 VHDL 实现的数字化混沌序列发生器仍然保持了对初始值敏感的特性。

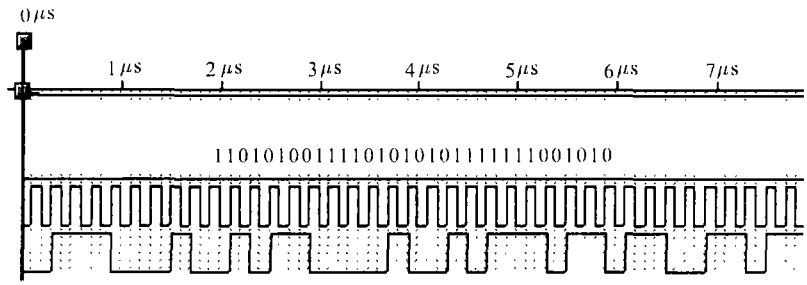

图 4　数字混沌序列波形

3.2.3 统计特性检验　在各种参数下，分别采集 10000 组长度为 N 的数字混沌序列，对其平衡性、自相关、互相关、线性复杂度等统计特性进行检验，并与实值混沌序列的对应特性进行比较，结果如表 1 所示。

表 1　数字与实值混沌序列的统计特性

序列长度 N	平衡性检验通过率		自相关最大旁瓣值 θ_{am}		互相关最大值 θ_{cm}		线性复杂度 LC	
	数字	实值	数字	实值	数字	实值	数字	实值
31	82%	85%	0.33	0.35	0.388	0.355	15	15
63	83%	85%	0.263	0.285	0.324	0.333	31	32
127	90%	92%	0.213	0.226	0.237	0.213	63	63
255	93%	95%	0.163	0.178	0.196	0.205	128	127

由表 1 可知，数字混沌序列的平衡性略比实值混沌序列差，自相关特性略好，$N = 63$，255 时，互相关特性略好，而 $N = 31$，127 时互相关特性略差，二者的线性复杂度相当。因此，数字混沌序列具有十分接近于实值混沌序列的统计特性。

4 结　论

采用数字系统的“自顶向下”的设计方法，运用 VHDL 成功地实现了改进的分段线性混沌映射，经过逻辑综合和仿真，产生了稳定输出的数字混沌序列。统计分析表明，数字混沌序列具有十分接近于实值混沌序列的统计特性，因此，数字混沌序列能够应用于实际的扩频通信系统中。同时，本文的工作也为混沌系统的研究从理论走向实际应用探索了一条途径。

参　考　文　献

[1] D. Sandoval-Morantes, D. Munoz-Rodriguez, Chaotic sequences for multiple access, Electronics letters., 1998, 34(3), 235–237.

[2] 甘良才，等，一类混沌映射产生调频序列的方法，电子学报，2000, 28(4), 109–111.

[3] 金红，等，一种用于 CDMA 系统的混沌多值数字序列及其性能，电子学报，2000, 28(4), 131–134.

[4] 胡健栋，等，码分多址与个人通信，北京，人民邮电出版社，1996 年 10 月，90–134.

[5] L. O. Chua, Y. Yao, Q. Yang, Generating randomness from chaos and constructing chaos with desired randomness, Int. J. Circuit Theory and Applications, 1990, 18(3), 215–240.

[6] A. Baranousky, D. Daems, Bifucation and Chaos, 1995, 5(6), 1585–1598.

[7] 饶妮妮，一种适于作 A-CDMA 系统扩频码的混沌序列，电子科技大学学报， 2000, 29(5), 465–468.

[8] 周红，等，有限精度混沌系统的 m 序列扰动实现，电子学报， 1997, 25(7), 95–97.

[9] 周红，等，混沌非线性反馈密码序列的理论设计和有限精度实现，电子学报， 1997, 25(10), 57–60.

[10] IEEE Std, VHDL Language Reference Manual, IEEE Standard, 1076-1993.

DESIGN FOR A DIGITAL CHAOTIC SPREADING SEQUENCE GENERATOR

Rao Nini

(*Department of Automation, UEST of China, Chengdu* 610054, *China*)

Abstract The design method is given for the digital piecewise linear mapping system based on FPGA chip. In this method, the perturbation of m-sequence is used to overcome the short period of chaotic sequence caused by the finite precision effect. The piecewise linear chaotic generator is realized by means of VHDL and the simulations are made. The balance, the correlation and the linear complexity are compared between digital chaotic sequence and analogue chaotic sequence. A road is explored to apply the piecewise linear mapping system to practical spreading spectrum system.

Key words Digital Chaotic spreading sequence, Finite precision effect, VHDL, Top-to-down, Statistical property

饶妮妮： 女， 1963 年生，教授，硕士， 1997-1998 为英国百拉德福德大学电子工程系访问学者，目前主要研究方向：移动通信、信号与信息处理、生物医学信息技术.