产生 2^k 元伪随机序列的准混沌 Mealy 型有限状态机方法 [1]

张申如 王庭昌 * 邓晓燕

(解放军理工大学理学院 南京 211101)
*(总参第 63 研究所 南京 210007)

摘 要 该文利用 m 状态序列稳定的长周期，以及混沌序列流的高线性复杂度，研究了一种将 m 状态序列作为准混沌 Mealy 型有限状态机输入的 2^k 元伪随机序列产生方法，分析了系统的周期特性，进行了序列流随机性的测试，介绍了系统作为跳频码发生器在 FPGA 的仿真和综合结果。

关键词 混沌，有限状态机，伪随机序列
中图号 TN918.2

1 引 言

q 元伪随机数序列可应用于序列流密码和扩跳频码中。产生伪随机数序列最简单、最经济的方法是线性反馈移位寄存器，所产生的最大长度二进制序列称 m 序列。对于非素数的 $q = 2^k$ 元伪随机数序列可以从线性反馈移位寄存器的状态序列中得到，但是 m 序列及其 m 状态序列通常并不能安全地直接应用于流密码和扩跳频码，最重要的原因之一是其线性复杂度低，所以人们提出了许多非线性组合，反馈和前馈的方法。

从 90 年代起，人们开始研究混沌序列流的产生方法，主要是看好它有高的线性复杂度，良好的均匀性和自相关、互相关性，但仍担忧其周期点的存在和有限字节下短周期的影响。另一方面，混沌算法的非线性对硬件实现来说也是一个难题。

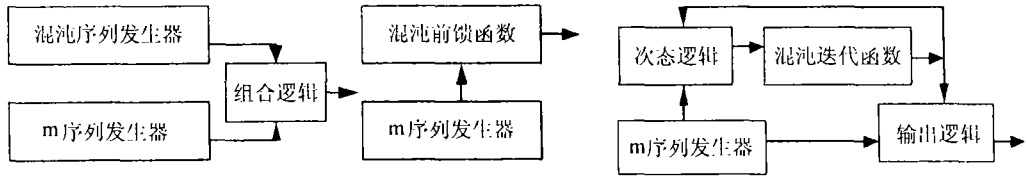
本文在文献 [1-3] 基础上，利用 m 序列及其状态序列稳定的长周期，并结合混沌序列流的高线性复杂度，研究一种可在 FPGA (Field Programmable Gate Array) 上实现的长周期 $q = 2^k$ 元伪随机序列产生方法。第 2 节说明了系统的设计思想，第 3 节分析了系统的周期特性，第 4 节对序列流进行了测试，第 5 节介绍了系统在 FPGA 的仿真和综合结果。

2 混沌的 Mealy 型有限状态机设计思想

将产生 m 状态序列的线性反馈移位寄存器和运行在有限字长下的准混沌 [1,2] 序列发生器综合成一体，有三种可考虑的方式 (如图 1(a), 1(b), 1(c))，借用密码学 [4] 通常的说法它们是组合，前馈和 Mealy 型有限状态机 [5] 方式。

组合方式中 m 状态序列和混沌序列各自独立运行，只要组合逻辑得当，其输出序列周期可为 m 状态序列和准混沌序列周期的最小公倍数；前馈方式中混沌函数仅作为独立运行的 m 状态序列的非线性前馈，若前馈函数合适，其输出序列的周期可等于 m 状态序列的周期，文献 [6] 研究了这种方式。第 3 种实质上为有限状态机方式，文献 [3] 是作为微扰引入的。

[1] 2001-11-30 收到，2002-05-20 改回
复旦大学专用集成电路国家重点实验室访问学者基金和成都电子科技大学战术通信抗干扰技术国防科技重点实验室项目基金资助



(a) m状态序列和混沌序列的组合方式　(b)混沌函数作为m状态序列的前馈方式　(c) m状态序列作为混沌迭代函数组成的Mealy型有限状态机方式的输入

图 1　线性反馈移位寄存器和准混沌序列发生器 3 种综合方式

本文发展了有限状态机方式，系统如图 2 。它由两部分组成：第一部分是 L 级线性反馈移位寄存器，用它产生 m 状态序列；第二部分为运行在准混沌状态的字长为 k 位 s 阶的非线性数字滤波器 [1]，选择这种数字滤波器主要考虑它只用到了模 2^k 加法器，而不必使用其它混沌函数通常所需要的、更耗费资源的乘法器或除法器等，这利于芯片实现。次态 / 输出逻辑也已采用了易于芯片实现的位 "异或" 方式。研究表明：根据输出字长的要求选择 k，适当选择的次态 / 输出逻辑，可稳定地保证输出序列的周期是 m 状态序列周期的整数倍。

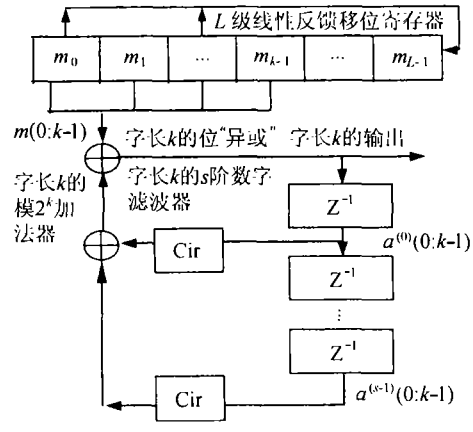


图 2　由 m 状态序列和字长 k 的 s 阶非线性数字滤波器组成的系统

对于设定的初始状态 $m_0(0:L-1)$, $a^{(i)}(0:k-1)(i=0,1,\cdots,s-1)$ 系统第 n 步的迭代运行方式为：

$$m_{n+1}(0:L-2)=m_n(1:L-1) \tag{1}$$

$$m_{n+1}(L-1)=f[m_n(0:L-1)] \tag{2}$$

$$a_{n+1}^{(j+1)}(0:k-1)=a_n^{(j)}(0:k-1),\quad j=0,1,\cdots,s-2 \tag{3}$$

$$a_{n+1}^{(0)}(0:k-1)=\sum_{i=0}^{s-1}\mathrm{Cir}[a_n^{(i)}(0:k-1),\ \text{shift-}i]\mathrm{mod}2^k\oplus m_{n+1}(0:k-1) \tag{4}$$

$$\mathrm{output}_{n+1}=g[a_{n+1}^{(0)}(0:k-1)] \tag{5}$$

式中 $n=0,1,2,\cdots,\oplus$ 为 $\mathrm{GF}(2^k)$ 的位模 2 加，$f[m_n(0:k-1)]$ 为产生 m 序列的线性反馈多项式。$\mathrm{Cir}[a_n^{(i)}(0:k-1),\text{shift-}i]$ 为对 k 比特的 $a_n^{(i)}(0:k-1)$ 进行移 shift-i 位的左循环移位函数，$i=0,1,\cdots,s-1$ 。$\Sigma\cdots\mathrm{mod}2^k$ 为模 2^k 加。$g[a_n^{(0)}(0:k-1)]$ 是对 $\mathrm{GF}(2^k)$ 元素的一个输出映射。

3 系统的周期特性分析

现分析上述系统的周期特性。系统的第一部分为 m 状态序列发生器。对于有 L 位的线性

反馈移位寄存器，其周期为 $T=2^L-1$，例如当选 $L=128$ 时 $T=2^{128}-1$。

系统第二部分为运行在准混沌状态的非线性数字滤波器。文献 [1] 应用的是其 $s=2$ 特殊情况，说明了它的准混沌性质，并给出当其单独运行在字长度 $k=8$ 位， shift-0 = 0, shift-1 = 1 即左循环移 1 位时周期的部分结果。我们已进一步研究了 $s=2$ 时 $k=8,9,10$, shift-0 = 0, shift-1 $=1,2,\cdots,k-1$ 即分别左循环移动 $1,2,\cdots,k-1$ 位时的周期，也研究了 $s=3$, $k=5$ 时， shift-0, shift-1, shift-2 取 $0,1,2,3$ 不同左循环移动量的组合时的周期，得到与文献 [1] 类似的结果。概括起来，这种运行在准混沌状态下的二阶或高阶非线性数字滤波器自身的迭代序列都具有如下特点：(1) 有较长的平均周期，它约为总状态数 2^{sk} 的 1/4 至 1/2；(2) 对某些初态仍然存在有短周期 (例如有不动点)。

为了避免短周期的出现，又使系统能运行在准混沌状态，从而使它具有对初始值敏感的依赖性和长期行为的不可预测性，我们现将两部分耦合起来。具体地说是用 m 状态序列的前 k 位“异或”非线性数字滤波器的输出，并反馈为非线性数字滤波器的新状态。这种方式可以看成是用 m 状态序列作为 Mealy 有限状态机的输入，以混沌迭代函数进行状态变换。下述定理证明：它的输出保持了 m 状态序列稳定的长周期性质。测试也表明，它还保留了准混沌的非线性所带来的高复杂度。

定理 1 由线性反馈移位寄存器和非线性数字滤波器组成的图 2 联合系统，迭代映射是一对一的，即系统的每个前导状态有唯一的一个后续状态，反过来每个后续状态也只有唯一的一个前导状态。(证明参见附录)

定理 2 由线性反馈移位寄存器和非线性数字滤波器组成的图 2 联合系统，迭代映射的输出 $a^{(0)}(0:k-1)$ 的周期 p 是 m 状态序列周期 T 的整数倍，即 $p=NT$，此处 $1\le N\le 2^{sk}$。(证明参见附录)。

我们用计算机模拟测定了联合系统的周期。第一个系统 $L=10$, $s=2$, $k=5$，取 shift-0 = 0, shift-1 = 1 循环左移一位，迭代的结果如表 1。联合系统可选初态数为 $(2^L-1)2^{sk}=1047552$ (m 状态序列非全零)，系统的状态转换仅由 4 条封闭环组成。对循环左移 2, 3, 4 位也得到了类似结果。

表 1 $L+sk=(10+2\times 5)=20$ 位联合系统的周期测试

环长 $(NT)\times$ 条数	6138× 1	72633×1	233244× 1	735537× 1
N 数 $(T=1023)$	6	71	228	719

第二个系统 $L=8$, $s=3$, $k=4$，取 shift-0 =shift-1 = 0, shift-2 = 1 循环左移一位。迭代的结果如表 2。联合系统可选初态数为 $(2^L-1)2^{sk}=1044480(m$ 状态序列非全零)，系统的状态转换仅由 8 条封闭环组成。对 shift-0, shift-1, shift-2 取 $0,1,2,3$ 不同左循环移动量的组合，也得到了类似结果。实际使用 k 位输出时，还可进一步考虑序列安全性，将 $a^{(0)}(0:k-1)$ 通过某个一对一 g 函数加以映射，输出序列仍将保持定理 2 保证的 (长) 周期。

表 2 $L+sk=(8+3\times 4)=20$ 位联合系统的周期测试

环长 $(NT)\times$ 条数	735420× 1	135915× 1	117300× 1	44625× 1	6630× 1	1530× 3
N 数 $(T=255)$	2884	533	460	175	26	6

4 输出 $q=2^k$ 元序列的测试

我们使用 $L=128$ 位， $k=8$ 位， $s=4$ 阶，左循环移位数 shift-0 = 0, shift-1 = 1, shift-2 = 2, shift-3 = 3 模型，将 $L+4\times k=160$ 位的任选的 5 个密钥值赋给线性反馈移位寄存

器和数字滤波器作初值，迭代得到长度为 1,000,000 的 256 元序列，对它的随机特性进行了测试。

4.1 输出 256 元序列一维分布的均匀性测试

表 3 列出了对 5 个序列样本的 256 元出现次数均匀性测试得到的 χ^2 值. 在显著性水平取为 0.05 时，一维均匀性假设成立的 χ^2 为 293.2464，而对由相邻的两个序列元素可组成的 65536 图案，序列二维均匀性 χ^2 通过值为 66131.63，可见 5 条序列都通过了测试. 图 3 示出了其中一条序列样本各元素出现次数的一维均匀性分布图。

表 3　5 个序列样本的均匀性测试表

序列 1 的 χ^2	序列 1 的 χ^2	序列 1 的 χ^2	序列 1 的 χ^2	序列 1 的 χ^2
一维分布均匀性 $\chi^2 \le 293.2464$ 通过				
218.1222	271.7543	273.4208	231.8617	240.3937
二维分布均匀性 $\chi^2 \le 66131.63$ 通过				
65780.93	65551.99	65812.49	66201.99	65603.02

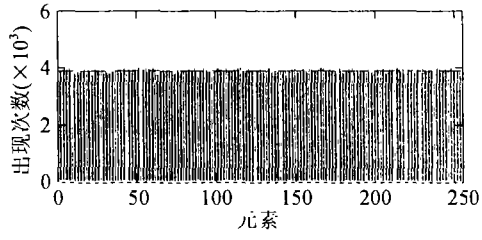


图 3　长度为 1,000,000 的 256 元序列各元素出现次数，一维均匀性分布图

4.2 输出 256 元序列游程分布

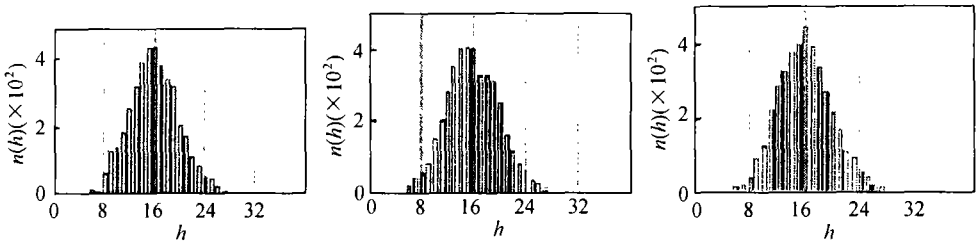
表 4 列出了 5 个序列样本 1 游程 —3 游程的出现次数，与其对比的为文献 [7] 指出的随机序列游程数学期望理论值，它们是十分相近的.

表 4　5 个序列样本的游程分布测试表

	数学期望	序列 1	序列 2	序列 3	序列 4	序列 5
1 游程	992202.8	992176	992345	992068	992243	992294
2 游程	3875.792	3879	3808	3948	3853	3829
3 游程	15.13981	22	13	12	17	16

4.3 汉明自相关和互相关

用作跳频通信，我们要检测它们的汉明自相关和互相关，测试是对两条长度为 4096 的 256 元输出序列进行的，它们的 160 位密钥值每个字节仅 1 位有差异. 测试结果如下：图 4(a) 和图 4(b) 是两条序列的汉明自相关测试结果，横坐标是汉明自相关值 h，纵坐标是出现的次数 $n(h)$，期望的中心值出现在横坐标约为 4096/256=16 处. 在周期汉明自相关旁瓣的 4095 次测试中，均匀分布假设是否成立的 χ^2 测试值为 4097.9 和 4089.6，小于选取显著性水平为 5% 时，χ^2 通过值 4244.98. 类似在图 4(c) 是该两条序列的汉明互相关测试结果，横坐标是汉明互相关值 h，纵坐标是出现的次数 $n(h)$，期望的中心值出现在横坐标为 4096/256=16 处. 在周期汉明互相关的 4096 次测试中，均匀分布假设是否成立的 χ^2 测试值为 3957.6，小于显著性水平取 5% 时，χ^2 通过值 4246.02.

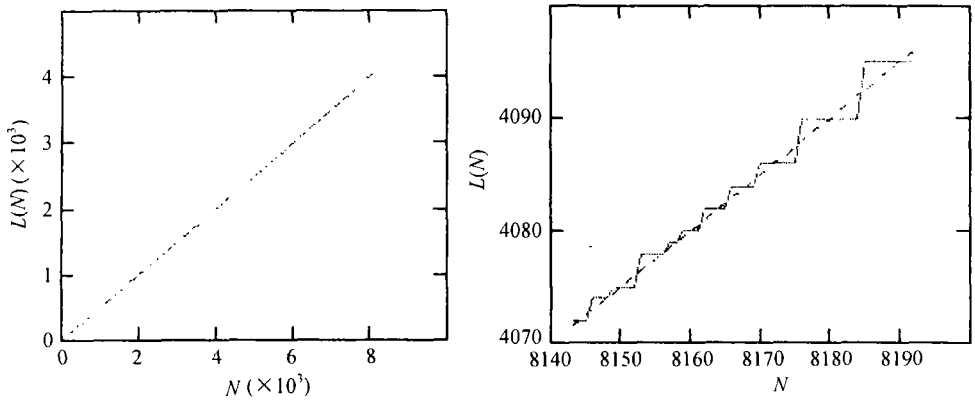


(a) 序列 1 的汉明自相关分布 (b) 序列 2 的汉明自相关分布 (c) 序列 1, 2 的汉明自相关分布

图 4 两条长度为 4096 的 256 元序列汉明自 / 互相关分布测试图

4.4 线性复杂度的测试

由于系统方案中混合了模 2 加、位“异或”、模 2^k 加和循环移位操作等，预期对定义在任一单独域内的线性复杂度都会有较好的性质。例如，我们将一条 256 元长度为 1024 序列段以二进制表示得到的长度为 8192 二元序列，测定在 GF(2) 中的线性复杂度。图 5 中示出了它们动态线性复杂度 $L(N)$-N 关系曲线，其中图 5(b) 为图 5(a) 中某一小局部段进行细节放大的结果。横坐标代表长度 N，纵坐标代表 $L(N)$。图 5(a) 的 N 从 1 至 8192，图 5(b) 的 N 从 8143 至 8192。图示的结果十分相似于理想二元伪随机码序列 $L(N)$-N 曲线要求，它们是以平均斜率 $k = 1/2$ 的增长 (图 5(a))，图像呈骑跨在 $L = N/2$ 直线的阶梯状，阶梯不太规则，各级阶梯的宽，高度比的平均值 [4] 大约是 4 : 2(图 5(b))。



(a) 二元序列的动态线性复杂度 (b) 图 5(a) 的局部细节图

图 5

5 算法在 FPGA 实现的仿真和综合结果

为了验证上述算法在 FPGA 上的实现代价，我们借助硬件描述语言 (VHDL) 编程，在电子设计自动化 (EDA) 软件平台上完成了仿照跳频码发生器的设计，进行了仿真，并针对 Quicklogic 公司有 5000 可用门的 FPGA 芯片 QL2005 实施了综合和布线。器件设计成有 160 位初始值，从 8 个端口按 20 个地址输入，初始化完成后信号 ready=‘1’，此后每个时钟可有 8 位输出。资

源占用约 212cell(仅约 3300 可用门)，时延约为 32ns，即最高时钟频率可达 31MHz，可见此设计资源省，速度高。至于此方案若作为流密码发生器应用，结构的其它密码学特性和抗攻击分析还有待于进一步研究。

附　录

定理 1　证明　如图 2 系统运行的状态可以用 $m_n(0:L-1), a_n^{(i)}(0:k-1), i=0,1,\cdots,s-1$ 来描述。首先，每个前导状态显然只有一个确定的后续状态，这可从迭代关系 (1)–(4) 式的确定性来加以说明。而定理的后半部分现较详细地证明如下：

设有一后续状态为 $m_{n+1}(0:L-1), a_{n+1}^{(i)}(0:k-1), i=0,1,\cdots,s-1$，它们有两个相异的前导状态 $m'_n(0:L-1), a_n^{(i)\prime}(0:k-1)$ 和 $m_n^{(i)\prime\prime}(0:L-1), a_n^{(i)\prime\prime}(0:k-1), i=0,1,\cdots,s-1$。

由 (1) 式应有

$$m'_n(1:L-1)=m''_n(1:L-1) \tag{A1}$$

而由 (3) 式则有

$$a_n^{(i)\prime}(0:k-1)=a_n^{(i)\prime\prime}(0:k-1),\quad i=0,1,\cdots,s-2 \tag{A2}$$

将 (A2) 式代入 (4) 式，由于 $a_{n+1}^{(0)}(0:k-1)$ 的确定性和循环移位运算的唯一性，即

$$\mathrm{Cir}[a_n^{(i)\prime}(0:k-1),\ \text{shift-}i]=\mathrm{Cir}[a_n^{(i)\prime\prime}(0:k-1),\ \text{shift-}i],\quad i=0,1,\cdots,s-2$$

可得 $\mathrm{Cir}[a_n^{(s-1)\prime}(0:k-1),\text{shift-}(s-1)]=\mathrm{Cir}[a_n^{(s-1)\prime\prime}(0:k-1),\ \text{shift-}(s-1)]$，则循环移位运算的可逆性可立即得到

$$a_n^{(s-1)\prime}(0:k-1)=a_n^{(s-1)\prime\prime}(0:k-1) \tag{A3}$$

至于 $m_n(0)$ 可利用形成 m 序列的反馈多项式必定是非奇异的，即 $f[m_n(0:L-1)]=m_n(0)\oplus f'[m_n(1:L-1)]$ 利用此式及 (A1) 式，代入 (2) 式便可得到

$$m'_n(0)=m''_n(0) \tag{A4}$$

(A1)—(A4) 证明了前面假设的两个相异状态是完全相同的，映射是一对一的。　　证毕

定理 2　证明　定理的第一部分证明如下。设输出序列的周期为 p，即为状态 a 的周期，有 $a_{j+p}^{(0)}(0:k-1)=a_j^{(0)}(0:k-1), \forall j$，由 (3) 式知状态 $a^{(i)}$，$i=1,2,\cdots,s-1$ 的周期也为 p，即 $a_{j+p}^{(i)}(0:k-1)=a_j^{(i)}(0:k-1), \forall j$，将 (4) 式改写为 $m_{n+1}(0:k-1)=\sum_{i=0}^{s-1}\mathrm{Cir}(a_n^{(i)}(0:k-1),\text{shift-}i)\bmod 2^k\oplus a_{n+1}^{(0)}(0:k-1)$，所以必有 $m_{j+p}(0:k-1)=m_j(0:k-1)$，即 m 状态序列的周期 T 应能整除 p, $p=NT$ 成立。

定理的第二部分要证明 $1\le N\le 2^{sk}$。首先因为 m 状态序列运行是独立进行的，m 状态序列 $m(0:k-1)$ 要返回初始状态的周期为 T，所以包括 $a^{(i)}(0:k-1)i=0,1,\cdots,s-1, m(0:k-1)$ 在内的全状态从某一初态起又回到与初态相同的状态，只可能是经历了由 $a^{(i)}(0:k-1)$, $i=0,1,\cdots,s-1$，这 $s\times k$ 位构成的子状态序列中 N 个 (整数) 的结果，$1\le N\le 2^{sk}$ 是必然的。　　证毕

参 考 文 献

[1] D. R. Frey, Chaotic digital encoding: An approach to secure communication, IEEE Trans. on CAS., 1993, CAS-40(10), 660-666.

[2] M. Itoh, Chai Wan Wu, L. O. Chua, Communication system via chaotic signal from a reconstruction viewpoint, International Journal of Bifurcation and Chaos, 1997, 7(2), 275–286.

[3] 周红，罗杰，凌燮亭，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.

[4] 王育民，何大可，保密学—基础与应用，西安，西安电子科技大学出版社，1990, 6.4, 7.2, 7.3 节.

[5] A. D. 弗莱德曼，著，刘春和，译，数字系统逻辑设计，北京，人民邮电出版社，1982, 5.1 节.

[6] 周红，俞军，凌燮亭，混沌前馈型流密码的设计，电子学报，1998, 26(1), 98–101.

[7] 张申如，梅文华，王庭昌，邓晓燕，非周期 q 元随机序列的游程特性，通信学报，2000, 21(1), 45–48.

GENERATING 2^k PSEUDO-RANDOM SEQUENCES USING QUASI-CHAOTIC MEALY LIMITED STATE MACHINE

Zhang Shenru Wang Tingchang* Deng Xiaoyan

(*Science Institute, PLA University of Sci. and Tech., Nanjing* 211101, *China*)

*(*The 63th Institute of PLA General Staff, Nanjing* 210007, *China*)

Abstract In this paper a method of generating 2^k pseudo-random sequences to obtain stable long period of m-sequences and high complexity of chaotic sequences is discussed. A quasi-chaotic function acts as Mealy limited state machine and m-sequence acts as its input. The periodic nature of sequences is analyzed and the randomness of sequences is tested. The simulation results in chip of FPGA for frequency hopping code generator are reported.

Key words Chaos, Limited state machine, Pseudo-random sequences

张申如： 男，1946 年生，教授，研究方向为光电信息处理、扩展频谱通信及专用集成电路设计等.

王庭昌： 男，1943 年生，研究员，中国电子学会通信专业委员会委员，研究方向为语音压缩、混沌信号处理及模块化设计等.

邓晓燕： 女，1948 年生，教授，研究方向为扩展频谱通信及专用集成电路设计等.