文章编号:1671-8860(2010)05-0566-04　　文献标志码:A

多输出 LFSR 结构均匀分布伪随机数生成器的硬件设计优化

谷晓忱[1]　张民选[1]

(1　国防科学技术大学计算机学院 PDL 重点实验室,长沙市开福区德雅路 54 号,410073)

摘　要:通过公式推导,得出了使用硬件方式实现伪随机数生成器所消耗的硬件资源数量与输出位数和所产生随机数周期之间的关系,从理论层面上证明了多输出 LFSR 结构在硬件资源利用方面存在的优势;通过分析变换矩阵的结构以及反馈系数的特点,给出了提高该类随机数生成器工作速度的方法。在 Xilinx Vertex 4 FPGA 上进行了大量的实验,实验结果验证了理论分析的正确性。

关键词:伪随机数;LFSR;均匀分布伪随机数生成器;FPGA 计算加速

中图法分类号:TP302

均匀分布随机数生成器(uniform random number generator ,URNG)是产生其他分布类型 RNG 的基本组成部件[1]。随着人们对基于 FPGA 的运算加速问题的深入研究[2-4], URNG 的硬件实现问题也逐渐成为研究热点,其中基于 LFSR 的 URNG 就是应用最为广泛的一种结构[5-7]。本文在文献[8]的基础上,对多输出 LFSR 结构的 URNG 进行了更深入的分析。文中的 URNG 指的都是均匀分布伪随机数生成器。

1　多输出 LFSR 结构 URNG 的原理[8]

本文均以外部反馈 LFSR 为理论推导和实验对象。图 1 为单输出外部反馈 LFSR 结构,$C_1 \sim C_n$是反馈系数(即 Tap 值),图中的寄存器状态转换关系可以用如下公式表示:

$$X(t+1) = \boldsymbol{A}X(t) \tag{1}$$

式中, $\boldsymbol{A}$ 是变换矩阵。由式(1)可知,普通的 LFSR 是单输出的,它所生成的是 1 bit 数据流。

多输出 LFSR 是通过改进变换矩阵 $\boldsymbol{A}$ 得到的。由式(1)可进行如下推导:

$$X(t+m) = \boldsymbol{A}X(t+m-1) = \boldsymbol{A}(\boldsymbol{A}X(t+m-2)) = \cdots = \boldsymbol{A}^m X(t) \tag{2}$$

可见,使用变换矩阵 $\boldsymbol{A}^m$ 对 $X(t)$进行变换,就可以

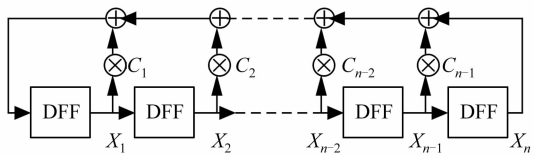

图 1　单输出外部反馈 LFSR 结构

Fig. 1　Basic Structure of Fibonacci LFSR

得到 m 输出 LFSR 的状态转换关系:

$$X(t'+1) = \boldsymbol{A}^m X(t') \tag{3}$$

基于 m 输出 LFSR 结构的 URNG 所产生的随机数仍然是伪随机数,其最大周期公式为[8]:

$$T = [2^n - 1, m]/m \tag{4}$$

式中,$[2^n-1, m]$为 2^n-1 与 m 的最小公倍数。

2　多输出 LFSR 结构 URNG 在硬件资源利用方面的优势分析

变换矩阵 $\boldsymbol{A}$ 是一个特殊的矩阵,可表示为[8]:

$$\boldsymbol{A} = \begin{pmatrix} \boldsymbol{C}_{1\times n} \\ \boldsymbol{I}_{(n-1)\times(n-1)} \quad 0_{(n-1)\times 1} \end{pmatrix} \tag{5}$$

其中,$\boldsymbol{C}_{1\times n}$是反馈系数的向量表示;$\boldsymbol{I}_{(n-1)\times(n-1)}$是一个单位矩阵;$0_{(n-1)\times 1}$是一个零向量。则多输出 LFSR 的变换矩阵 $\boldsymbol{A}^m$ 可表示为:

收稿日期:2010-03-15。

项目来源:国家 863 计划资助项目(2009AA01Z124)。

$$\boldsymbol{A}^m=\begin{pmatrix}\boldsymbol{C}_{1\times n}\times\boldsymbol{A}^{m-1}\\ \boldsymbol{C}_{1\times n}\times\boldsymbol{A}^{m-2}\\ \cdots\\ \boldsymbol{C}_{1\times n}\times\boldsymbol{A}\\ \boldsymbol{C}_{1\times n}\\ \boldsymbol{I}_{(n-m)\times(n-m)}\quad 0_{(n-m)\times m}\end{pmatrix}\tag{6}$$

由式(6)可见,输出位数 m 每增加一位,URNG 反馈网络中就会相应地增加一条反馈链路,该反馈链路的具体结构由 $\boldsymbol{C}_{1\times n}\times\boldsymbol{A}^{m-i}$ 决定。

作为参照对象,由单输出 LFSR 构成的 m 位 URNG 使用的硬件数量可以表示为:

$$S=m\times n\times S_{\text{register}}+m\times S_{\text{Tap}}\tag{7}$$

其中,S_{register} 为每一级寄存器对应的硬件数量;S_{Tap} 为反馈网络 $\boldsymbol{C}_{1\times n}$ 对应的硬件数量;n 是 LFSR 的级数。该复用结构的 URNG 可以保证每拍输出一个 m 位整数随机数,周期为 2^n-1。

当使用 m 输出 LFSR 结构时,为了得到相同的随机数周期,使用的 LFSR 级数 n' 应该满足如下关系式:

$$[2^{n'}-1,m]/m=2^n-1\tag{8}$$

按照最差情况计算,为了得到大小为 2^n-1 的输出周期,m 输出 LFSR 结构的级数需要满足的条件为:

$$n'=n+\log_2 m\tag{9}$$

所以,m 输出 LFSR 结构 URNG 使用的硬件数量可以表示为:

$$S'=n'\times S_{\text{register}}+m\times S_{\text{Tap}}=n\times S_{\text{register}}+\log_2 m\times S_{\text{register}}+m\times S_{\text{Tap}}\tag{10}$$

进而可以得到如下关系式:

$$\Delta S=S-S'=(m\times n-n-\log_2 m)\times S_{\text{register}}\tag{11}$$

在式(11)中,m 的值恒大于 1,n 的值一般要大于 10。因此,综合式(7)、式(10)和式(11)的内容,可以得出如下结论:

1) 当输出位数 m 增加时,相对于单输出 LFSR 结构的 URNG,多输出 LFSR 结构的 URNG 所使用的硬件资源数量将以 $(m\times n-\log_2 m)\times S_{\text{register}}$ 的趋势减少。

2) 当输出的随机数周期增加,即 n 值增大时,相对于单输出 LFSR 结构的 URNG,多输出 LFSR 结构的 URNG 所使用的硬件资源数量将以 $(m-1)\times n\times S_{\text{register}}$ 的趋势减少。

3) 输出位数 m 越大,产生的随机数周期越长时,多输出 LFSR 结构的 URNG 在硬件资源消耗方面的优势就越明显。

3　多输出 LFSR 结构的 URNG 工作速度的优化方法

反馈网络的延时决定了外部反馈 LFSR 的工作速度。通过对比式(5)和式(6)中变换矩阵的形式可以看出,多输出 LFSR 结构 URNG 的反馈网络比单输出 LFSR 结构 URNG 的要复杂得多。这种复杂性对工作速度的影响主要体现在如下两个方面:① 导致关键路径变长,从而造成反馈网络的延迟时间变大,进而降低工作速度;② 导致参与反馈的寄存器输出负载变大,从而增大信号翻转所需的时间,进而降低工作速度。

通过对式(6)中变换矩阵 $\boldsymbol{A}^m$ 的进一步分析可以得出,当反馈系数满足关系 $C_1=C_2=\cdots=C_{m-1}=0$ 时,$\boldsymbol{A}^m$ 的行向量可以表示为:

$$\boldsymbol{C}_{1\times n}\times\boldsymbol{A}^{m-1}=(C_m,C_{m+1},C_{m+2},\cdots,C_{n-1},1,\underbrace{0,0,\cdots,0}_{(m-1)\text{个}})_{1\times n}\tag{12}$$

可见,此时 $\boldsymbol{C}_{1\times n}\times\boldsymbol{A}^{m-1}$ 的结果只是简单地将 $\boldsymbol{C}_{1\times n}$ 进行了 $m-1$ 位的逻辑左移而已。因此,与变换矩阵 $\boldsymbol{A}^m$ 相对应的反馈网络并没有使关键路径变长,也就不会造成 URNG 工作速度变慢。但是,从式(12)中也可以看出,与变换矩阵 $\boldsymbol{A}^m$ 相对应的反馈网络确实有可能导致参与反馈的寄存器输出负载变大。其中最坏的情况出现在变换矩阵 $\boldsymbol{A}^m$ 中的某一列存在最多 1 时,此时对应该列的寄存器的输出负载最大,它所需要的信号翻转时间也最长,进而成为 URNG 工作速度提升的瓶颈。

通过以上分析,可以得出以下优化多输出 LFSR 结构 URNG 工作速度的方法:① 为了不影响反馈网络中关键路径的长度,在选取反馈系数时,应满足 $C_1=C_2=\cdots=C_{m-1}=0$ 的关系;② 变换矩阵 $\boldsymbol{A}^m$ 中的某一列中 1 的个数最大值等于反馈系数 $C_1\sim C_n$ 中 1 的个数。因此,为了尽可能减小寄存器的输出负载,在选取反馈系数时,应该尽量减少 1 的个数;③ 通过式(6)和式(12)可知,当反馈系数 $C_1\sim C_n$ 中 1 的间距比较小时,变换矩阵 $\boldsymbol{A}^m$ 中的某一列才容易出现多个 1 的现象。因此,在选取反馈系数时,应该尽可能地加大 1 出现的间距。

4　实验结果

为了验证上述理论分析的正确性,本文在 Xil-

inx Vertex 4 FPGA上进行了一系列的实验。第一个实验验证了当URNG所产生随机数的周期不变时,随着输出位数 m 的增加,单输出LFSR结构和多输出LFSR结构在硬件使用量方面的变化趋势以及差异情况。实验中,n 取固定值13,而 m 值从2递增到8。相关的参数选取如表1所示。

表1 实验1中的相关参数

Tab. 1 Parameters of Simulation 1

m	单输出LFSR级数	单输出LFSR的Tap	多输出LFSR级数	多输出LFSR的Tap
2	13	[13,12,10,9]	14	[14,13,11,9]
3,4	13	[13,12,10,9]	15	[15,14,13,11]
5,6,7,8	13	[13,12,10,9]	16	[16,11,9,8]

从图2可见,随着输出位数 m 的增加,单输出LFSR结构硬件消耗的增长速度远大于多输出LFSR结构,这点完全符合式(7)和式(10)的描述。为了保证产生随机数的周期不变,多输出结构会以 $\log_2 m$ 的速度适当地增加LFSR的级数。但是从表1和图2的实验结果可见,这种增长并没有导致很大的硬件消耗。所以,当输出位数 m 增加时,相对于单输出LFSR结构,多输出LFSR结构在硬件消耗方面存在明显的优势。从图2还可以看出,随着 m 的增加,ΔS 变化趋势的实测结果与理论推断结果非常接近。

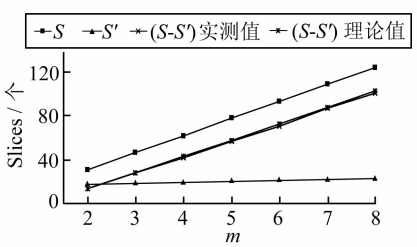

图2 硬件资源消耗与输出位数的关系

Fig. 2 Relationship Between Hardware Resources and m

第二个实验验证了当URNG所产生随机数的位数不变时,随着产生随机数周期的增加,单输出LFSR结构和多输出LFSR结构在硬件使用量方面的变化趋势以及差异情况。实验中,m 取固定值8,而 n 值从13递增到20。相关的参数选取如表2所示。

图3所示是实验结果的折线图。根据式(7)和式(10)的描述,当 m 不变时,单输出LFSR结构URNG的硬件消耗随着 n 的变化以 $m \times S_{\text{register}}$ 的速度增长,而多输出LFSR结构URNG的硬件消耗随着 n 的变化以 S_{register} 的速度增长。图3的实验结果基本符合这一规律。同时,图3的结果也同样表明,随着 n 的增加,ΔS 变化趋势的实测结果与理论推导结果非常接近。

表2 实验2中的相关参数

Tab. 2 Parameters of Simulation 2

单输出LFSR级数	单输出LFSR的Tap	多输出LFSR级数	多输出LFSR的Tap
13	[13,12,10,9]	16	[16,11,9,8]
14	[14,13,11,9]	17	[17,16,15,14]
15	[15,14,13,11]	18	[18,17,16,13]
16	[16,11,9,8]	19	[19,18,17,14]
17	[17,16,15,14]	20	[20,19,16,14]
18	[18,17,16,13]	21	[21,20,19,16]
19	[19,18,17,14]	22	[22,21,16,15]
20	[20,19,16,14]	23	[23,22,20,18]

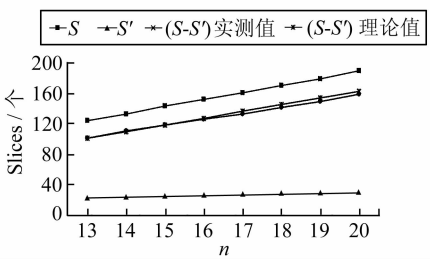

图3 硬件资源消耗与随机数周期的关系

Fig. 3 Relationship Between Hardware Resources and Period

第三个实验验证了不同的Tap值对多输出LFSR结构URNG工作速度的影响。实验以17级2输出LFSR为例,对6组不同Tap值所对应的URNG的工作速度进行了测试。实验中选取的6组Tap值(Tap1、Tap2、Tap3、Tap4、Tap5、Tap6)分别为[17,14,13,10]、[17,16,15,14]、[17,16,15,13,9,8]、[17,16,15,14,13,12]、[17,15,13,11,9,6,5,2]、[17,16,15,14,13,12,11,9]。这6组Tap值的选取原则是:① 按反馈系数的级数(即1出现的个数)从4级到6级的顺序,每级选取两组;② 在每级的两组Tap中,按照反馈系数中1出现的间距关系,分别在间距紧密和间距宽松的Tap中各选择了一组。

图4是实验结果的折线图。从实验结果中可得:① 随着反馈系数级数的增加,URNG的工作速度逐渐降低;② 在相同级数的条件下,反馈

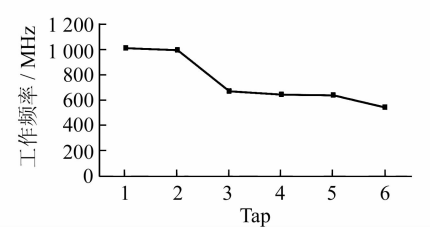

图4 不同Tap对速度的影响

Fig. 4 Relationship Between Speed and Taps

系数中 1 出现间距大的 Tap 对应的 URNG 的工作速度快。

5 结　语

本文分析了多输出 LFSR 结构 URNG 在硬件资源使用方面的优势,提出了优化多输出 LFSR 结构 URNG 工作速度的方法。实验证明了该方法的正确性。因为本文的主要目的是对基于 LFSR 结构的 URNG 在从单输出结构改进为多输出结构后的优势进行讨论,因此文中并没有将多输出 LFSR 结构 URNG 的硬件实现结果与其他类型 URNG 的硬件实现结果进行比对。

参 考 文 献

[1] Thomas D B, Luk W, Leong P H W, et al. Gaussian Random Number Generators [J]. ACM Computing Surveys (CSUR), 2007, 39(4): 11

[2] Che Shuai, Li Jie, Sheaffer J W, et al. Accelerating Compute-Intensive Applications with GPUs and FPGAs[C]. Symposium on Application Specific Processors, Anaheim, CA, 2008

[3] Kaganov A, Chow P, Lakhany A. FPGA Acceleration of Monte-Carlo Based Credit Derivative Pricing [C]. International Conference on Field Programmable Logic and Applications, Heidelberg, 2008

[4] Thomas D B, Luk W. FPGA-optimised High-quality Uniform Random Number Generators [C]. The 16th International ACM/SIGDA Symposium on Field Programmable Gate Arrays, USA, 2008

[5] Mucci C, Vanzolini L, Mirimin I, et al. Implementation of Parallel LFSR-based Applications on an Adaptive DSP Featuring a Pipelined Configurable Gate Array [C]. Conference on Design, Automation and Test in Europe, Germany, 2008

[6] Mascagni M. Random Number Generation for Serial, Parallel, Distributed, and Grid-based Financial Computations [C]. IEEE International Symposium on Parallel and Distributed Processing, Miami, FL, 2008

[7] Singh B, Khosla A, Bindra S. Power Optimization of Linear Feedback Shift Register (LFSR) for Low Power BIST [C]. IEEE International Advance Computing Conference, Patiala, 2009

[8] Gu Xiaochen, Zhang Minxuan. Multi-output Fibonacci Type LFSR Based Uniform Random Number Generator: Design and Analysis [J]. Computer Engineering and Science, 2009 31(A1):80-83

第一作者简介:谷晓忱,博士生,主要研究方向为可重构计算、数模混合集成电路设计、射频集成电路设计等。

E-mail:xc.gu0612@gmail.com

Multi-output LFSR Based Uniform Pseudo Random Number Generator

GU Xiaochen[1]　*ZHANG Minxuan*[1]

(1　PDL, School of Computer, National University of Defense Technology, 54 Deya Road, Kaifu District, Changsha 410073, China)

Abstract: Through the systematic analysis, we derive the expressions that represents the relations between the amount of the utilized hardware and the bit-width of the output or the period of the generated random numbers, and prove the advantages of multi-output LFSR based UPRNG in hardware utilization in theory. Through the analysis of the transform matrix and the taps of LFSR, we propose several novel methods to improve the speed of the UPRNG. The experiments verify the expressions and the methods mentioned above in Xilinx Vertex 4 FPGA.

Key words: pseudo random number; LFSR; uniform pseudo random number generation; sceleration in FPGA

About the first author: GU Xiaochen, Ph.D candidate, majors in reconfigurable computing, mixed IC design and RF IC design.

E-mail: xc.gu0612@gmail.com