GERADORES PSEUDO-ALEATÓRIOS: MEDIÇÃO DE ALEATORIEDADE

Ramon F. Figueira[1], Larissa M. Soares[2], Cleonilson P. Souza[3]

[1]UFPB, João Pessoa, Brasil, ramonformiga.ee@gmail.com
[2]UFPB, João Pessoa, Brasil, larimeloo@hotmail.com
[3]UFPB, João Pessoa, Brasil, protasio@ct.ufpb.br

Resumo: Neste artigo é descrita um método de medição de aleatoriedade de geradores de sequências pseudo-aleatórias. Baseando-se neste método, foi realizada uma análise comparativa entre Autômatos Celulares e LFSRs (*Linear Feedback Shift Registers)*, geradores muito utilizados nos testes aplicados em circuitos integrados auto-testáveis, BISTs (da expressão, *Built-In Self Test*). Para verificar a eficiência desses geradores forma realizados experimentos simulaçionais para medir a aleatoriedade dos geradores.

Palavras-chave: medição de aleatoriedade, LFSR e Autômato Celular.

1. INTRODUÇÃO

A geração de sequências pseudo-aleatórias possui uma aplicabilidade bastante vasta. Em alguns circuitos autotestáveis, por exemplo, é necessária a presença de um dispositivo capaz de gerar vetores de teste com a maior aleatoriedade possível. Na maioria dos casos a obtenção dessas sequências de vetores se dá por meio de fontes determinísticas conhecidas como geradores automáticos de sequências pseudo-aleatórias. Esses geradores são desenvolvidos de modo a apresentarem sequências que se assemelham às puramente aleatórias [1], e devem, portanto, ser submetidos a diversos testes de verificação de aleatoriedade. Em geral, os geradores de sequências pseudo-aleatórias mais utilizados em testes de circuitos digitais são os autômatos celulares e os registradores de deslocamento com realimentação linear (LFSRs, da expressão em inglês *Linear Feedback Shift Register*) [1].

Nas Seções 2 e 3 serão apresentados os conceitos básicos referentes aos dois geradores citados. Os métodos de análise de aleatoriedade usados para testá-los estão explicitados na Seção 4. Na Seção 5 serão discutidos os resultados experimentais obtidos.

2. *LINEAR FEEDBACK SHIFT-REGISTER* (LFSR)

O LFSR é um circuito registrador de deslocamento com realimentação feita através de operações lineares [2]. Em se tratando de operações em campo binário, essa realimentação é realizada com a utilização de portas lógicas do tipo 'ou-exclusivo'. Geralmente, os LFSRs são representados por um polinômio de realimentação, o qual caracteriza completamente o LFSR e define todas as conexões envolvidas na realimentação do sistema. Esse polinômio é dado por:

$$\Phi(x) = \Phi_q x^q + \Phi_{q-1} x^{q-1} + \cdots + \Phi_2 x^2 + \Phi_1 x^1 \qquad (1)$$

Na Figura 1 é apresentado um LFSR generalizado em que se pode ver as conexões Φ_i e o vetor de estado dado por:

$$\vec{t} = (t_0, t_1, \cdots, t_{q-1}) \qquad (2)$$

É denominado de semente (*seed*), o estado inicial do LFSR.

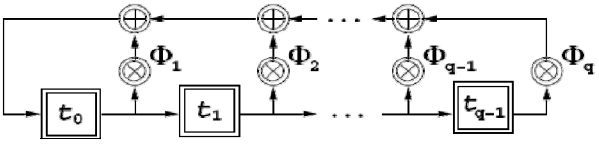

Fig. 1 Forma Generalizada do LFSR.

3. AUTÔMATO CELULAR

O autômato celular (CA, da expressão em inglês *Cellular Automaton*) é um conjunto de células que interagem com operação lógica "ou-exclusivo" com sua vizinhança de acordo com certas regras [2]. Estas regras tentam emular as interações celulares que ocorrem em organismos vivos [1]. Essas interações com operações lógicas são no campo binário, dentre as regras mais comuns estão a Regra de 90 e a Regra de 150. O nome de cada regra é obtido o valor decimal do código binário gerado para o próximo estado do registro x_i como resultado da operação lógica "ou-exclusivo" com seus dois vizinhos mais próximos, x_{i-1} e x_{i+1} [3]. Por exemplo, a Regra de 128 é a operação lógica ´AND' de x_{i-1}, x_{i+1} e x_i.

As Regras de 90 e 150 são geradas por operações lógicas "ou-exclusivas" do próprio registro e dos seus dois vizinhos mais próximos. A Regra de 90 é construída com *flip-flop* recebendo o resultado do "ou-exclusivo" dos seus vizinhos mais próximos: $x_i(t+1) = x_{i-1}(t) \oplus x_{i+1}(t)$, como mostrado na Fig. 2.a. A Regra de 150 é construída com *flip-flop* recebendo o resultado do ´ou-exclusivo´ dos seus vizinhos mais próximos e do próprio registro:

$x_i(t+1) = x_{i-1}(t) \oplus x_i \oplus x_{i+1}(t)$, como mostrado na Fig. 2.b [2].

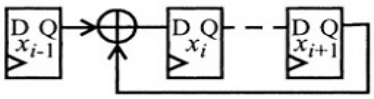

Fig. 2.a Regra de 90 para o *flip-flop* x_i.

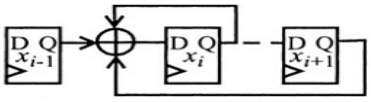

Fig. 2.b Regra de 150 para o *flip-flop* x_i.

4. MÉTODOS DE ANÁLISE DE ALEATORIEDADE

Para a análise da aleatoriedade dos geradores descritos foram realizados os seguintes testes: o **Teste de Corrida** e o **Teste de Kolmogorov-Smirnov.**

O Teste de Corrida é utilizado para verificar independência entre valores gerados e consiste em testar os desvios de valores crescentes e decrescentes e dos valores acima e abaixo da média comparando os valores atuais com os esperados [5]. Esse teste segue os seguintes passos:

1. Verifica-se se o número antecessor da sequência é maior ou menor que o próximo. Se for maior, coloca-se sinal +; se for menor, coloca-se sinal -.
2. Conta-se o número de *corridas,* número de positivos ou negativos em sequência, se há três positivos em sequência é uma corrida, ao ver um sinal negativo, se torna outra sequência e assim por diante. O número de corridas será atribuído a *a.*
3. Verifica-se a quantidade de números na sequência e atribui-se esse valor a *N.*
4. Aplica-se os valores encontrados nos passos 2 e 3 às seguintes fórmulas:

$$\mu_0 = \frac{2N-1}{3}$$

$$\sigma_0 = \frac{16N-29}{90}$$

$$Z_0 = \frac{(a-\mu_0)}{\sqrt{\sigma_0}}$$

em que, $Z \sim (0,1)$ $-Z_{\alpha/2} \leq Z_0 \leq Z_{\alpha/2}$ com $\alpha = 0{,}05\,\%$.

5. Se as condições do passo 4 forem satisfeitas, a hipótese de independência não pode ser rejeitada, se não forem, a hipótese pode ser rejeitada.

O Teste de Kolmogorov-Smirnov é utilizado para verificar a uniformidade entre valores gerados e consiste em medir o grau de aproximação entre a distribuição da amostra do gerador de números aleatórios e a distribuição uniforme teórica [4]. O desvio entre as duas distribuições não pode ser maior que o $D\alpha$, onde D é conhecido e tabelado em função de *N,* que é o número de valores decimais e α = 0,05%. Esse teste segue os seguintes passos:

1. Ordena-se os valores decimais em ordem crescente
   $R(1) < R(2) \cdots R(N)$
2. $D+= max|(i/N) - R(i)|$
   Onde: $1 < i < N$
   $D-= max|R(i) - (i-1)/N|$
   Onde: $1 < i < N$
3. Escolhe-se o maior valor entre $D+$ e $D-$
4. Determina-se o valor crítico $D\alpha$, por nível de significância e tamanho da amostra N.
5. Compara-se de D e $D\alpha$:
   $D > D\alpha$ – Hipótese é rejeitada
   $D < D\alpha$ – Hipótese não pode ser rejeitada

5. RESULTADOS EXPERIMENTAIS

Para verificar a aleatoriedade dos geradores descritos e ter uma avaliação quantitativa dos resultados, foi elaborado um simulador em linguagem C, que executa os seguintes procedimentos:

1. Aplica-se uma semente aleatória no gerador desejado;
2. Executa-se o gerador a fim de gerar uma sequência de valores (estado);
3. Executa-se o **Teste de Corrida** e verifica se passou;
4. Executa-se o **Teste de Kolmogorov-Smirnov** e verifica se passou;
5. Novo teste? Se sim, volta ao passo 1. Se não, **FIM**.

Nas Tabelas 1, 2 e 3 são mostrados os resultados dos testes realizados em LFSRs e CAs , em que: T é o tamanho do gerador (número de registros), C é o comprimento da sequência geradas e E é a quantidade de testes.

Tabela 1. Resultado do Teste de Kolmogorov-Smirnov.

RESULTADO PERCENTUAL						
				Teste de Kolmogorov		
	T	**C**	**E**	**CA 90**	**CA 150**	**LFSR**
1	7	30	12	0%	50%	100%
2	7	20	10	0%	50%	80%
3	9	20	15	80%	73%	93%
4	8	10	20	85%	100%	80%
5	10	40	25	84%	92%	92%
6	11	20	20	65%	75%	85%
7	12	15	20	95%	90%	95%
8	13	15	40	90%	93%	93%
9	14	20	12	92%	92%	100%
10	15	15	40	93%	98%	85%
11	16	10	20	85%	90%	85%
12	17	12	15	73%	100%	80%
13	17	20	15	100%	93%	87%
14	18	20	12	87%	100%	67%
15	18	30	10	80%	100%	90%
16	19	20	15	93%	100%	93%
17	19	30	25	92%	80%	92%
18	20	60	40	88%	88%	73%
19	21	12	12	75%	83%	75%
Média das %				77%	87%	87%

Tabela 2. Resultado do Teste de Corrida.

RESULTADO PERCENTUAL						
				Teste de Corrida		
	T	**C**	**E**	**CA 90**	**CA 150**	**LFSR**
1	7	30	12	0%	42%	50%
2	7	20	10	0%	70%	60%
3	9	20	15	73%	80%	60%
4	8	10	20	90%	100%	95%
5	10	40	25	56%	88%	24%
6	11	20	20	85%	40%	55%
7	12	15	20	95%	80%	80%
8	13	15	40	95%	95%	73%
9	14	20	12	92%	83%	67%
10	15	15	40	90%	95%	73%
11	16	10	20	90%	85%	80%
12	17	12	15	80%	80%	60%
13	17	20	15	80%	93%	93%
14	18	20	12	75%	92%	58%
15	18	30	10	100%	90%	30%
16	19	20	15	93%	80%	53%
17	19	30	25	80%	88%	60%
18	20	60	40	58%	78%	15%
19	21	12	12	75%	100%	58%
Média das %				74%	82%	60%

6. CONCLUSÃO

Ao analisar os dados apresentados na Tabela 1, pode-se observar que para alguns tamanhos de vetores e tipos de geradores não há aleatoriedade, pois nenhuma sequência de vetores passou nos testes. Isso acontece no autômato celular da Regra de 90 para 7 registros. Em outros, há uma porcentagem maior de sequências que passaram no teste, como por exemplo para 18 registros, que no autômato celular de 150 passa em 90% dos testes. Em geral, pode-se constatar que, ao realizar 19 testes com número de registros, comprimento e eventos diferentes, o CA150 foi o que obteve mais sequências que passaram em ambos os testes, pois obteve uma média percentual de 78% de sequências que passaram em ambos os testes.

REFERÊNCIAS

[1] SOUZA, Cleonilson P. **Uma Arquitetura Autotestável para Circuitos Digitais baseada no Algoritmo de Berlekamp-Massey e em Sistemas Imunológicos Artificiais**. **Tese de Doutorado** UFCG. Campina Grande. 2005.

[2] STROUD, Charles E.. ***A Designer´s Guide to Built-in-Self Test.*** 1ª Edição, Editora Springer, 2002.

[3] MEYER, Paul L. **PROBABILIDADE – Aplicações à Estatística.** 2ª Edição, Livros Técnicos e Científicos Editora, 1994.

[4] WANG, Faggang. ***Fast and Robust Modulation Classification via Kolmogorov-Smirnov Test.*** Artigo IEEE, pags 2324-2332, Agosto 2010.

[5] **Testes de Aleatoriedade**. Disponível em <www.webinbox.com.br/.../Simulação%20-%20Aula%207%20**Testes**%20de%20Aderencia1.ppt> Acessado em: <31 de Mar. 2011>.

Tabela 3. Resultado do Teste de Corrida e Kolmogorov, quando são aleatórios ao mesmo tempo.

RESULTADO PERCENTUAL						
				Ambos os testes		
	T	**C**	**E**	**CA 90**	**CA 150**	**LFSR**
1	7	30	12	0%	42%	50%
2	7	20	10	0%	50%	60%
3	9	20	15	60%	67%	53%
4	8	10	20	85%	100%	75%
5	10	40	25	52%	88%	24%
6	11	20	20	60%	40%	50%
7	12	15	20	90%	80%	80%
8	13	15	40	88%	90%	73%
9	14	20	12	92%	83%	67%
10	15	15	40	83%	93%	65%
11	16	10	20	80%	85%	70%
12	17	12	15	67%	80%	53%
13	17	20	15	80%	93%	80%
14	18	20	12	67%	92%	58%
15	18	30	10	80%	90%	20%
16	19	20	15	87%	80%	47%
17	19	30	25	72%	72%	60%
18	20	60	40	55%	78%	15%
19	21	12	12	67%	83%	58%
Média das %				67%	78%	56%