ANEXO A

GERADOR DE NÚMEROS ALEATÓRIOS COM DISTRIBUIÇÃO UNIFORME E REPETITIVIDADE

Conforme definido por L'ECUYER (1994), computadores digitais só podem gerar números pseudo-aleatórios, por se tratarem de máquinas totalmente determinísticas. No entanto, desde que um gerador de números pseudo-aleatórios seja aprovado em testes de aleatoriedade, sua aplicação vai levar a comportamentos equivalentes aos produzidos por geradores puramente aleatórios. Sendo assim, não se faz distinção neste trabalho entre aleatoriedade e pseudo-aleatoriedade.

Um gerador de números (pseudo-)aleatórios em computadores digitais tem um estado que evolui em um espaço *S*. Esse espaço é composto por um número finito de estados e a repetitividade é garantida a partir de uma recorrência na forma: $s_n = f(s_{n-1}),\ n \geq 1$, sendo que $s_o \in S$ será denominado a semente e $f : S \rightarrow S$ será a função determinística de transição. No enésimo passo, a função de saída do gerador será dada por $u_n = g(s_n)$ com $g : S \rightarrow [0,1]$ (essa saída poderia ser mais geral, entretanto está sendo assumido o intervalo *[0,1]*). Observe que a seqüência de saída do gerador será um conjunto de valores representado por $\{u_n, n \geq 0\}$. Como o espaço *S* é finito, a seqüência $\{u_n, n \geq 0\}$ deverá ser periódica (possivelmente após um transitório inicial). Em outras palavras, todas as vezes em que a semente s_o for a mesma, a seqüência aleatória gerada será repetida. Em situações em que é necessário aumentar a periodicidade do gerador, ou seja quando a quantidade de números aleatórios a serem gerados é muito grande, será desejável fazer com que esse período seja o mais próximo possível da cardinalidade do espaço *S*.

Geralmente, os modelos fornecidos pelos sistemas computacionais são os geradores lineares apresentando uma relação de recorrência $I_{j+1} = (aI_j + c) \bmod m,\ j = 1,2,\ldots,$ responsável pela geração de uma seqüência $I_1, I_2, I_3, \ldots$ de inteiros entre 0 e $m-1$, sendo m o módulo, a e c inteiros positivos denominados multiplicador e incremento. A recorrência vai

certamente produzir, para algum $j = p \leq m, I_j = I_k \ (k < j)$, ou seja, ela terá um período $p \leq m$. Se o período for $p = m$, todo inteiro entre 0 e m–1 vai ocorrer em alguma das próximas m–1 iterações, fazendo com que a escolha do valor inicial I_0 da recorrência (semente da geração pseudo-aleatória) não influa de forma significativa no resultado estatístico associado a seqüências longas. Os geradores lineares têm a vantagem de serem rápidos, de simples implementação e repetitivos para uma mesma máquina.