

Números Randômicos

e

Aplicações

JOSÉ LAÉRCIO DORICIO

DEPARTAMENTO DE MATEMÁTICA

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Orientador: Prof. Dr. Roberto R. Paterlini

PADCT/SPEC/1996-1997; PET/CAPES 1997/1998

1. NÚMEROS RANDÔMICOS

1.1. CONCEITO

O conceito de número randômico ou aleatório é bastante complexo, e em cada época esse conceito pode mudar. Um exemplo do que acabo de dizer é o seguinte: para um homem pré-histórico o estado do tempo (sol, chuva, frio, calor, nublado, etc.) seria um fenômeno aleatório, isto é, ele não sabia o que iria acontecer no próximo dia ou na próxima hora em relação ao tempo. Já para a sociedade científica atual os fenômenos temporais não são considerados tão aleatórios, pois existem eficientes métodos de previsão meteorológica, o que torna o fenômeno mais determinado.

Na verdade, não existe o que se possa chamar de número aleatório. Assim, não tem sentido perguntar se 17 é aleatório. Em vez disso, lidamos com seqüências de números aleatórios, que pode ser entendida como uma *seqüência de números independentes* com uma específica *distribuição*. Assim, em uma seqüência de números aleatórios, cada número aparece independentemente dos anteriores, sem nenhuma possibilidade de previsão.

O tipo de distribuição mais utilizado é a *distribuição uniforme*. Se os números de uma seqüência aleatória são extraídos de um determinado conjunto, os elementos deste conjunto devem ter a mesma chance de serem escolhidos a cada vez que é tomado um número para a seqüência. Em outros termos, cada número do conjunto é igualmente provável em cada posição da seqüência.

Assim, se estamos construindo uma seqüência aleatória com os números 0, 1, 2, 3, 4, e 5 (jogando dados, por exemplo), pode ocorrer que os dez primeiros números dessa seqüência sejam o 0. O 11º número pode ser qualquer um dos dígitos 0, 1, 2, 3, 4, ou 5, com igual chance para todos, inclusive para o próprio 0. Em outro exemplo, se, em uma seqüência aleatória com um bilhão de dígitos decimais, os primeiros 999999999 dígitos forem 0, a chance do último ser 0 é ainda 1/10. Em cada ponto da seqüência cada elemento é absolutamente independente dos anteriores.

O mesmo se pode dizer sobre a seqüência vista como um todo. A seqüência com cem

mil dígitos 0 tem tanta probabilidade de ocorrer como outra seqüência qualquer.

As seqüências de números aleatórios são utilizadas para as mais diversas finalidades. Listamos a seguir alguns tipos de aplicações.

Simulação : a simulação de fenômenos naturais através de modelos científicos pode ser mais realista quando os dados de entrada são gerados randomicamente.

Amostragem : quando um modelo científico tem um número muito grande de casos a serem apreciados, pode-se considerar a conveniência de obter uma amostra aleatória de casos e testá-los.

Análise Numérica : modelos determinísticos numéricos podem fazer uso de seqüências aleatórias para economizar tempo de computação. Um exemplo significativo é o teste probabilístico de primalidade, utilizado por aplicativos computacionais matemáticos.

Programação de computadores : números aleatórios podem ser utilizados para testar a eficiência de algoritmos computacionais.

Teoria da decisão: a escolha aleatória de dados de entrada pode acelerar tomada de decisões (por exemplo, na implementação computacional de um algoritmo muito complexo). A aleatoriedade faz parte também da obtenção de estratégias ótimas na Teoria dos Jogos.

Recreação : É bastante conhecido o uso dos números aleatórios em jogos de azar. Em virtude disso as técnicas que envolvem números randômicos são comumente designadas por "Métodos de Monte Carlo", uma referência ao país que abriga cassinos famosos. Este nome foi criado por John von Neumann quando utilizou o método em projetos em Los Alamos.

1.2. ASPECTOS HISTÓRICOS

Atualmente seqüências de números randômicos são geradas e estocadas em computadores, o que facilita bastante o uso dessas seqüências. Entretanto, antes do advento dos computadores, os números randômicos eram gerados das mais diversas maneiras, em geral muito trabalhosas, como lançamento de dados ou embaralhamento de cartas, aparelhos mecânicos,

etc., e eram estocados em tabelas.

William Sealy Gossett, que trabalhou com o pseudônimo de "*Student*", realizou experimentos de amostragem em Matemática Estatística e descobriu a célebre distribuição-t, assim chamada por ele. Atuou em conjunto com o Colégio Universitário, que publicou os seus resultados e experimentos. Gossett trabalhou com números aleatórios em seus experimentos e, para gerar os números, utilizou o método Top-Hat (rotação de discos).

A partir dessa época a quantidade de números aleatórios necessários nos experimentos era cada vez maior. Passou-se a estocar os números em tabelas que eram publicadas para uso dos que delas precisavam. Essa foi uma idéia de L. H. C. Tippett que, em 1927, publicou uma tabela com 40000 dígitos extraídos aleatoriamente de dados do censo americano. Ela foi publicada em "*Random Sampling Numbers*," Tracts for Computers, nº 15, Cambridge University Press, New York, 1927.

A tabela de Tippett logo se mostrou insuficiente, e, em 1939, M. G. Kendall e B. Babington-Smith publicaram a primeira tabela de números randômicos gerados por uma máquina. A tabela publicada por eles tinha continha 100000 dígitos. Eles também introduziram o teste de frequência, o teste de poker e o teste de abertura para as seqüências de números randômicos. Na mesma época Fisher e Yates trabalharam em Rothamsted produzindo uma pequena tabela com 15000 dígitos que eram extraídos do 15º ao 19º dígito dos logaritmos da *Logarithmica Britannica* de A. J. Thompson.

Por volta de 1930, foi sugerido o uso de aritmética para o cálculo dos números randômicos e em 1946 J. von Neumann e M. Metropolis criaram o primeiro gerador de números randômicos baseado em aritmética que foi denominado por eles de método dos quadrados médios. O método produzia resultados insatisfatórios e devido a isso era necessário uma análise prévia para então ser utilizado nos experimentos. Atualmente se consegue seqüências suficientemente randômicas com esse método.

Utilizando aritmética, foi D. H. Lemer em 1949 que primeiro introduziu a idéia do método de congruência linear que utiliza uma equação de congruência para gerar os números. O gerador de Lemer está descrito em Kruskal, J. B. "*An Extremely Portable Random Number Generator*," Comm. ACM, 12 (1969), 93-94.

As tabelas foram suficientes por muitos anos, e, depois da Segunda Guerra Mundial, em 1955, um expressivo aumento do estoque de números randômicos foi feito pela Rand Corporation da América, que publicou uma tabela com um milhão de dígitos aleatórios, obtidos por aparelhos mecânicos.

Com o desenvolvimento da informática nas últimas décadas os cientistas começaram a utilizar o computador para gerar e estocar números aleatórios, baseados em métodos como o de Lemer, e as tabelas perderam a sua utilidade.

O primeiro método de Monte Carlo publicado foi provavelmente o problema de Buffon (1707 - 1788). A melhor aproximação do número π através do método de Buffon foi feita em

1901 por Italian Lazzerini, que de somente 3408 lançamentos randômicos de agulhas, ele conseguiu aproximar o número π corretamente em seis casas decimais.

A maior façanha dos Métodos de Monte Carlo aconteceu no laboratório científico de Los Alamos durante a segunda guerra Mundial. O método foi utilizado para a construção da bomba atômica, que foi sugerido por J. von Neumann e S. Ulam.