08

Mat2274
Estatística Computacional

Prof. Lorí Viali, Dr.
viali@mat.ufrgs.br
http://www.ufrgs.br/~viali/

Número (pseudo) aleatórios

Conceitos Básicos

Conceito

Números aleatórios (NA) são elementos básicos necessários na simulação de quase todos os sistemas discretos. Eles podem ser utilizados diretamente ou então utilizados para gerar valores de variáveis aleatórias.

Métodos de geração de NA e de variáveis aleatórias são normalmente denominados de Métodos de Monte Carlo. A denominação é uma homenagem ao Cassino de Monte Carlo, onde a roleta é um dos mecanismos mais simples de geração de NA.

O trabalho pioneiro nesta área remonta a Ulam, que o teria inventado em 1946 ao estudar as possibilidades de ganhar no jogo de cartas “Solitário”.

Stanislaw Marcin Ulam (1909 - 1984)

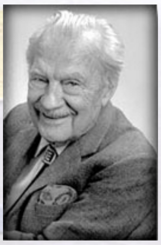
John Von Neumann (1903 - 1957)

Trabalhando com Von Neuman e Metropolis ele desenvolveu algoritmos computacionais. Explorou meios de transformar problemas não aleatórios em aleatórios para que pudesse resolvê-los através da amostragem.

Esse trabalho transformou a amostragem estatística de uma curiosidade matemática para um metodologia formal aplicável a uma grande variedade de problemas.

Foi Metropolis que denominou a nova metodologia de Monte Carlo. Ulam e Metropolis publicaram o primeiro artigo sobre o método em 1949.

Nicholas Constantine Metropolis (1915 - 1999)



Existem várias maneiras ou mecanismos de geração de NA. O objetivo é a geração por computador. Embora falar em NA gerados por computador não seja apropriado, pois a característica de qualquer seqüência de NA é não ser reproduzível e todos os procedimentos computacionais fornecem seqüências que podem ser reproduzidas.

Propriedades

Uma seqüência de números aleatórios U_1, U_2, ..., U_n deve apresentar três propriedades básicas:

(i) Uniformidade;

(ii) Aleatoriedade e

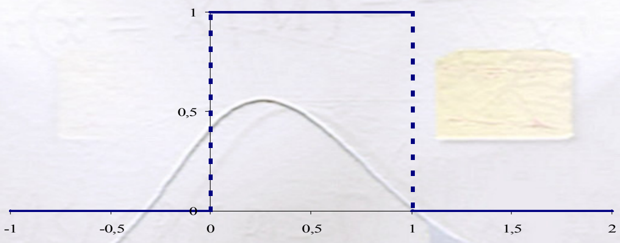
(iii) Ausência de autocorrelação.

Definição:

Cada número aleatório U_i é um valor de uma VAC uniforme em [0; 1], isto é, de uma função densidade de probabilidade (fdp) dada por:

$$f(u) = \begin{cases} 1 & \text{se } 0 \leq u \leq 1 \\ 0 & \text{c.c.} \end{cases}$$

fdp da U(0; 1)

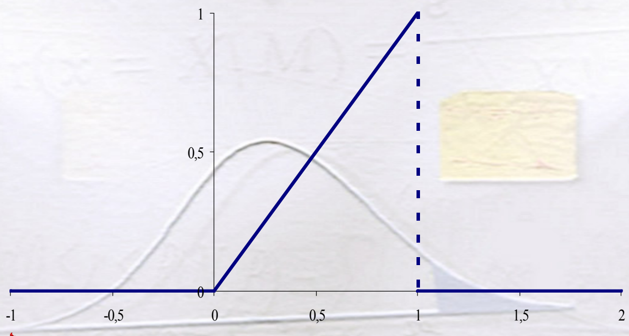


Exemplo

Se X é uniforme no intervalo [0; 1], então a FDA de X é dada por:

$$F(x) = \begin{cases} 0 & \text{se } x < 0 \\ x & \text{se } 0 \le x \le 1 \\ 1 & \text{se } x > 1 \end{cases}$$

FDA da U(0;1)



Expectância

$$E(X) = \int_{-\infty}^{+\infty} x.f(x)dx = \int_0^1 xdx =$$

$$= \left[\frac{x^2}{2}\right]_0^1 = \frac{1}{2} = 0,50$$

Variância

$\sigma^2 = V(X) = E(X^2) - E(X)^2$

$$E(X^2) = \int_{-\infty}^{+\infty} x^2.f(x)dx = \left[\frac{x^3}{3}\right]_0^1 = \frac{1}{3}$$

$$\sigma^2 = V(X) = E(X^2) - E(X)^2 =$$

$$= \frac{1}{3} - \left(\frac{1}{2}\right)^2 = \frac{1}{3} - \frac{1}{4} = \frac{1}{12}$$

Conseqüências

Duas conseqüências da uniformidade e independência são:

(a) Se o intervalo [0, 1] é dividido em k classes de igual tamanho, então o número esperado de observações em cada classe é n/k onde n é o total de valores gerados.

(b) A probabilidade de observarmos um valor em uma classe é independente do valor obtido anteriormente.

Métodos de Geração

1. Métodos Históricos

São as primeiras tentativas feitas para encontrar geradores de números aleatórios. Foram aceitos e válidos na sua época. Com o tempo e a sofisticação teórica e computacional as falhas foram aparecendo e foram substituídos por métodos mais eficientes.

O método do meio do quadrado

Foi desenvolvido por Von Neumann e Metropolis em meados de 1940. Consiste em elevar o número anterior ao quadrado e extrair os dígitos do meio.

Exemplo

Se desejamos NA de três dígitos e o valor da semente fosse $\lambda_0 = 252$, teríamos:

$225^2 = 63504$, que produziria o valor $\lambda^1 = 350$ e assim por diante.

Exercício

Suponhamos que uma seqüência de 4 dígitos aleatórios seja necessária. Seja X_i o i-ésimo valor a ser elevado ao quadrado e U_i o i-ésimo NA. Seja X_0 = 5497 (semente). Determinar os primeiros 200 valores.

Faça o mesmo com os seguintes valores: 5197 e 6500.

Prof. Lorí Viali, Dr. - UFRGS - Instituto de Matemática - Departamento de Estatística

O método do meio do produto

Entre outras técnicas semelhantes à técnica **do meio do quadrado** está a do **meio-produto**. Este método parte de duas sementes com o mesmo número de dígitos: x_0 e x_0'.

Prof. Lorí Viali, Dr. - UFRGS - Instituto de Matemática - Departamento de Estatística

Multiplica-se o número x_0 por x_0' para obter o valor x_1 do qual é selecionado o meio, fornecendo o valor x_{i+1}.

Prof. Lorí Viali, Dr. - UFRGS - Instituto de Matemática - Departamento de Estatística

Exemplo

Usar a técnica do Meio-Produto para gerar uma seqüência aleatória de 40 dígitos com x_0 = 2938 e x_0' = 7229.

Prof. Lorí Viali, Dr. - UFRGS - Instituto de Matemática - Departamento de Estatística

Exercício

Encontre dois valores iniciais. Determine 200 valores pelo método meio-produto e faça um diagrama de dispersão dos resultados tomando metade dos resultados como valores "x" e a outra metade como valores "y".

Prof. Lorí Viali, Dr. - UFRGS - Instituto de Matemática - Departamento de Estatística

A constante multiplicativa

A técnica da constante multiplicativa é uma leve variação da técnica do meio do quadrado. Utiliza uma constante multiplicativa “k”.

A constante é multiplicada por um valor semente x_0. Ambos, constante e NA, têm “d” dígitos. O resultado é um valor R_1. Os “d” dígitos do meio do resultado são tomados para obtermos o valor x_1, e assim por diante.

Exemplo

Usar a técnica constante multiplicativa para gerar uma seqüência aleatória de 40 dígitos com $k = 3987$ e $x_0 = 7223$.

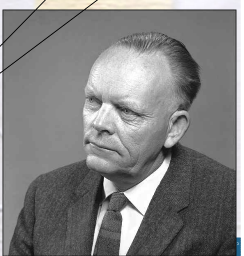
Exercício

Encontre dois valores iniciais. Determine 200 valores pelo método da constante multiplicativa e faça um diagrama de linha dos resultados.

O método aditivo congruencial

Um último processo de interesse histórico é o Método Aditivo Congruencial (MAC) que foi proposto por Lehmer em 1951.

Derrick Henry Lehmer
Professor de Matemática da UC Berkeley
(1905 - 1991)



O MAC utiliza uma abordagem diferente dos métodos anteriores. Ele requer uma seqüência de tamanho “n”, $x_1, x_2, \ldots, x_n$. O gerador produz então uma extensão desta seqüência: $x_{n+1}, x_{n+2}, \ldots$, através da expressão:

$$x_i = (x_{i-1} + x_{i-n}) \bmod m$$

Exemplo

Seja a seqüência de inteiros $x_1 = 57$, $x_2 = 34$, $x_3 = 89$, $x_4 = 92$ e $x_5 = 16$ (isto é, n = 5). Seja m = 100. Esta seqüência pode ser ampliada, usando o método aditivo congruencial da seguinte forma:

$x_i = (x_{i-1} + x_{i-n}) \bmod m$

$x_6 = (x_5 + x_1) \bmod 100 = 73 \bmod 100 = 73$

$x_7 = (x_6 + x_2) \bmod 100 = 7 \bmod 100 = 07$

$x_8 = (x_7 + x_3) \bmod 100 = 96 \bmod 100 = 96$

$x_9 = (x_8 + x_4) \bmod 100 = 88 \bmod 100 = 88$

$x_{10} = (x_9 + x_5) \bmod 100 = 04 \bmod 100 = 04$

Exercício

Uma maneira diferente de gerar números aleatórios é através da teoria do caos. Identifique valores iniciais que poderiam render um bom gerador para a seguinte seqüência caótica.

$x_{i+1} = 4x_i(1 - x_i)$

2. Métodos atuais

Aritmética Modular ou Congruência

Karl Friedrich Gauss (1777-1855)

A congruência foi introduzida formalmente por Gauss na obra *Disquisitiones Arithmeticae* para estudar os problemas aritméticos relacionados com a divisibilidade. Posteriormente foi aplicada a problemas da teoria dos números.

Sejam a e b números inteiros e m > 0 um número natural. Se a e b fornecem o mesmo resto quando divididos por m escrevemos:

$a \equiv b \pmod{m}$

Lê-se **a** é congruente a **b** módulo **m**. De forma equivalente pode-se dizer que **m** divide **a – b**.

O valor **m** é denominado de módulo da relação de congruência.

Por exemplo, os números que são congruentes a **0** módulo **m**, são os múltiplos de **m**.

A notação sugere que a relação de congruência é semelhante a relação de igualdade. De fato a congruência módulo m é, tal como a igualdade, uma relação de eqüivalência.

Ela apresenta as seguintes propiedades:

Reflexiva: $a \equiv a \pmod{m}$

Simétrica: $a \equiv b \pmod{m}$ se e só se $b \equiv a \pmod{m}$

Transitiva: $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$ então $a \equiv c \pmod{m}$.

Assim pode-se agrupar os números enteiros em famílias disjuntas formadas pos números que são congruentes módulo m.

Vamos obter m famílias que são denominadas de classes de congruência de m.

Serão as famílias de números congruentes a i módulo m fazendo i variar de 0 a m - 1.

Por exemplo, as classes de congruência módulo 2 são os conjuntos dos números pares e o dos ímpares.

De mesma forma, existem três classes de congruência módulo 3. São formadas pelos números múltiplos de 3, pelos múltiplos de 3 mais 1 e pelos múltiplos de 3 mais 2 (ou menos 1).

As classes de inteiros módulo m serão representadas por Z_m (Z módulo m) Assim, por exemplo:

$Z_3 = \{ 0, 1, 2 \}$.

As principais propriedades da congruência são as relacionadas a soma e a multiplicação de inteiros:

Se $a \equiv b \pmod m$ e $c \equiv d \pmod m$, então $a + c \equiv b + d \pmod m$

Se $a \equiv b \pmod m$ e $c \equiv d \pmod m$, então $ac \equiv bd \pmod m$

Essas propriedades precisam ser provadas. Para verificar se a soma de congruências é também uma congruência precisamos verificar se:

$(a + c) – (b + d)$ é divisível por m.

Tem-se o seguinte:

Se $a \equiv b \pmod m$, então existe $k \in Z$ tal que $a – b = km$.

Se $c \equiv d \pmod m$, então existe $l \in Z$ tal que $c – d = lm$.

Assim $(a + c) - (b + d) =$

$(a - b) + (c - d) =$

$km + lm = (k + l)m$

Ou seja: $a + c \equiv b + d \pmod m$

Exercício

Prove que a subtração de congruências é também uma congruência.

Prova de que o produto de congruências e uma congruência.

Nesse caso é necessário mostrar que ac – bd é divisível por m.

Tem-se que:

Se $a \equiv b \pmod m$, então existe $k \in$ Z tal que $a - b = km$.

Se $c \equiv d \pmod m$, então existe $l \in$ Z tal que $c - d = lm$.

Assim $a.c - b.d = a.c + 0 - b.d =$
$a.c + (-bc + bc) - b.d =$
$ac - bc + bc - bd =$
$c(a - b) + b(c - d) =$
$ckm + blm =$
$(ck + bl).m =$
pm, onde $p = ck + bl$

Portanto $ac \equiv bd \pmod m$

Um caso particular da regra da multiplicação que é útil é:

Se $a \equiv b \pmod m$ então

$ka \equiv kb \pmod m$, para qualquer inteiro "k".

Sistema completo de restos

Cada inteiro é congruente módulo n com exatamente um dos n números: 0, 1, 2, ... n - 1.

Seja z un inteiro qualquer. Dividindo por n, se obtém:

$z = qn + r, \quad 0 <= r < n,$

Assim que z é congruente módulo n a r, que é um número entre 0 e n - 1.

Suponhamos agora que $0 <= r_1 < r_2 < n$ e que $z \equiv r_1 \pmod n$ e $z \equiv r_2 \pmod n$

Tem-se então que:

$r_1 \equiv r_2 \pmod{n}$ pois n divide a $r_2 - r_1$, mas $0 < r_2 - r_1 <= n - 1 < n$, o que é uma contradição.

Geradores Congruenciais

Prof. Lorí Viali, Dr. - UFRGS - Instituto de Matemática - Departamento de Estatística

O Método Linear Congruencial (*Linear Congruencial Method*), proposto por Lehmer em 1951, é o gerador de NA mais utilizado. Tal gerador é baseado na seguinte relação recursiva:

Prof. Lorí Viali, Dr. - UFRGS - Instituto de Matemática - Departamento de Estatística

$X_i \equiv (a.X_{i-1} + c) \bmod m$,

onde X_i, para i = 1, 2, 3, ... são os números inteiros aleatórios de saída, X_0 é o valor inicial da recursão ou semente e **a**, **c** e **m** são constantes pré-escolhidas.

Prof. Lorí Viali, Dr. - UFRGS - Instituto de Matemática - Departamento de Estatística

Para se obter valores de uma variável aleatória uniforme no intervalo (0, 1), será necessário dividir o valor X_i pelo módulo m, obtendo desta forma o valor $U_i = X_i / m$.

Prof. Lorí Viali, Dr. - UFRGS - Instituto de Matemática - Departamento de Estatística

Se $c \neq 0$ na definição então a expressão é denominada de Método Congruencial Misto.

Quando c = 0 a fórmula é conhecida como Método Congruencial Multiplicativo.

Prof. Lorí Viali, Dr. - UFRGS - Instituto de Matemática - Departamento de Estatística

A rapidez e a eficiência na utilização de geradores é um dos principais fatores a ser considerado na seleção. Isso pode ser obtido pela utilização de um módulo **m** que seja uma potência de 2.

Se o módulo for uma potência de 10, digamos 10^b para $b > 0$ e **c** é zero então a obtenção dos valores X_i é simples.

Ela consistirá em tomar os **b** dígitos à direita do número $X_i = a.X_{i-1}$.

Por analogia, o mesmo pode ser feito, quando o módulo for $m = 2^b$ para $b > 0$.

Essa opção é particularmente eficiente para o uso computacional.

Exemplo:

Sejam:

$X_0 = 10$, $a = 21$, $c = 9$ e $m = 100$

Então:

$X_i \equiv 21X_{i-1} + 9 \pmod{100}$

Exemplo:

$X_1 \equiv (21.10 + 9) \pmod{100} \equiv 219 \bmod 100$

$\equiv 19 \quad \Rightarrow U_1 = 19/100 = 0{,}19$

$X_2 \equiv (21.19 + 9) \pmod{100} \equiv 408 \bmod 100$

$\equiv 8 \quad \Rightarrow U_2 = 08/100 = 0{,}08$

$X_3 \equiv (21.08 + 9) \pmod{100} \equiv 177 \bmod 100$

$\equiv 77 \quad \Rightarrow U_3 = 77/100 = 0{,}77$

....

Propriedades:

01. Em virtude da operação módulo **m**, os valores possíveis do algoritmo são os inteiros: 0, 1, 2, ..., m - 1, se c = 0 ou os inteiros: 1, 2, 3, ..., m - 1, se $c \neq 0$.

02. A mais fina partição do intervalo (0, 1) que esse gerador pode fornecer é $\{0, 1/m, 2/m, ..., (m - 1)/m\}$.

Assim, não se tem uma verdadeira uniforme pois para qualquer $k \in \{0, 1, ... , m - 1\}$ tem-se: $P(k/m < U < (k+1)/m) = 0$ e não $1/m$ como seria requerido.

No entanto qualquer outro algoritmo computacional apresentará o mesmo problema, em virtude da precisão da máquina. Por exemplo, em uma computador com palavra de 32 bits a partição mais refinada de [0, 1] é:

$$\{0, 1/2^{32}, 2/2^{32}, ..., (2^{32} - 1)/2^{32}\}.$$

03. Como o valor X_i depende apenas do valor anterior X_{i-1}, uma vez que um valor se repita, a seqüência inteira se repetirá.

Tal repetição é dita ciclo e o tamanho da seqüência é dita período.

O período máximo de um gerador congruencial é **m**. Ainda, a **resolução** de um gerador é a menor diferença possível entre dois valores diferentes produzidos pelo gerador.

04. As escolhas de **a**, **c**, e **m** (bem como a aritmética particular da máquina), determinarão a resolução da partição [0, 1] bem como o comprimento do ciclo (período) e, portanto, a uniformidade da distribuição e a propriedade de independência da seqüência de saída.

A escolha apropriada de **a**, **c** e **m** é uma técnica com resultados teóricos e testes empíricos.

A primeira regra é selecionar o módulo **m** "tão grande quanto possível“.

Entretanto, m grande pode não ser o bastante, pois e o gerador pode ter muitos ciclos pequenos ou a seqüência não ser independente.

Exemplos:

$X_i \equiv 2X_{i-1} \pmod{2^{32}}$, onde uma semente da forma 2^k cria um ciclo contendo somente inteiros que são potências de 2.

$X_i \equiv (X_{i-1} + 1) \bmod 2^{32}$, que gera uma seqüência não aleatória de inteiros crescentes. Essa equação fornece um gerador que tem um ciclo de período máximo, mas ela é inútil para simular uma seqüência aleatória.

Teorema:

Um gerador linear congruencial terá um período máximo se e somente se:

(i) **c** é não nulo e é primo relativo de **m.**

(ii) (a mod q) = 1, para cada fator primo q de m ou de forma equivalente b = a - 1 é um múltiplo de p, para cada primo p dividindo m.

(iii) (a mod 4) = 1 se 4 é um fator de m, ou de forma equivalente b é múltiplo de 4, se m é múltiplo de 4.

Pelo teorema um gerador com c = 0, não pode ter um período de tamanho m, mas ele poderá ter um período de tamanho m – 1.

Conhecidas as limitações e propriedades dos geradores congruenciais, tem-se ainda a questão de como escolher a terna (a, c, m) do melhor modo possível. Para isto é aconselhado o seguinte roteiro direto, apesar de lento [LEW89]:

(a) Escolher valores (a, c, m) que forneçam um ciclo conhecido e suficientemente longo e utilizar este gerador para obter variáveis uniformemente distribuídas em [0, 1].

(c) Sujeitar o gerador a testes teóricos. O teste espectral de Coveyou e MacPherson é bastante utilizado e reconhecido como um teste estrutural sensível para distinguir entre bons e maus geradores.

Prof. Lorí Viali, Dr. – UFRGS – Instituto de Matemática – Departamento de Estatística

(d) Aplicar ao gerador os novos testes, que estão continuamente surgindo. Vários de tais testes são encontrados em [LEW89].

Prof. Lorí Viali, Dr. – UFRGS – Instituto de Matemática – Departamento de Estatística

Estes testes são aplicáveis a quaisquer geradores e não somente aos do tipo congruencial. Geradores que passam pelo procedimento acima, em geral, tem sido considerados bons geradores.

Prof. Lorí Viali, Dr. – UFRGS – Instituto de Matemática – Departamento de Estatística

Referências

KNUTH, Donald E. ***The Art of Computer Programing. Volume 2 - Seminumerical Algorithms.*** Reading (Massachusetts): Addison Wesley, 1981.

LEWIS, P. A. W., ORAV, E. J. ***Simulation Methodology for Statisticians, Operations Analysts and Engineers. Volume I.*** Belmont (California): Wadsworth, Inc., 1989.

Prof. Lorí Viali, Dr. – UFRGS – Instituto de Matemática – Departamento de Estatística

SOBOL, I. **O método de Monte Carlo**. Moscou: Editora Mir, 1983.

TOCHER, K. D. ***The Art of Simulation***. London: Universities Press, 1963.

Prof. Lorí Viali, Dr. – UFRGS – Instituto de Matemática – Departamento de Estatística