1. Simulação Estocástica e Números Pseudoaleatórios

USP/ICMC

1º/2026

Simulação

Simulação estocástica é a arte de gerar amostras de variáveis aleatórias em um ambiente computacional e usar essas amostras para a obtenção de um certo resultado (Bustos & Frery, 1992, *Simulação Estocástica – Teoria e Algoritmos*, ABE, São Paulo-SP).

Simulação

Simulação estocástica é a arte de gerar amostras de variáveis aleatórias em um ambiente computacional e usar essas amostras para a obtenção de um certo resultado (Bustos & Frery, 1992, *Simulação Estocástica – Teoria e Algoritmos*, ABE, São Paulo-SP).
Arte? Necessitamos de muitas técnicas para atingir o(s) objetivo(s) (Teoria dos Números, Probabilidade, Processos Estocásticos, Estatística, Computação, Análise Numérica, . . .)

Simulação

Simulação estocástica é a arte de gerar amostras de variáveis aleatórias em um ambiente computacional e usar essas amostras para a obtenção de um certo resultado (Bustos & Frery, 1992, *Simulação Estocástica – Teoria e Algoritmos*, ABE, São Paulo-SP).
Arte? Necessitamos de muitas técnicas para atingir o(s) objetivo(s) (Teoria dos Números, Probabilidade, Processos Estocásticos, Estatística, Computação, Análise Numérica, . . .)
Variáveis aleatórias? Muitos problemas ou são de natureza não determinística ou porque é mais apropriado o tratamento estocástico.

Simulação

Simulação estocástica é a arte de gerar amostras de variáveis aleatórias em um ambiente computacional e usar essas amostras para a obtenção de um certo resultado (Bustos & Frery, 1992, *Simulação Estocástica – Teoria e Algoritmos*, ABE, São Paulo-SP).
Arte? Necessitamos de muitas técnicas para atingir o(s) objetivo(s) (Teoria dos Números, Probabilidade, Processos Estocásticos, Estatística, Computação, Análise Numérica, . . .)
Variáveis aleatórias? Muitos problemas ou são de natureza não determinística ou porque é mais apropriado o tratamento estocástico.
Ambiente computacional? A complexidade e/ou o volume de dados impedem a busca de uma solução manual.

Simulação

Simulação estocástica é a arte de gerar amostras de variáveis aleatórias em um ambiente computacional e usar essas amostras para a obtenção de um certo resultado (Bustos & Frery, 1992, *Simulação Estocástica – Teoria e Algoritmos*, ABE, São Paulo-SP).
Arte? Necessitamos de muitas técnicas para atingir o(s) objetivo(s) (Teoria dos Números, Probabilidade, Processos Estocásticos, Estatística, Computação, Análise Numérica, . . .)
Variáveis aleatórias? Muitos problemas ou são de natureza não determinística ou porque é mais apropriado o tratamento estocástico.
Ambiente computacional? A complexidade e/ou o volume de dados impedem a busca de uma solução manual.
Certo resultado? O bom uso da simulação estocástica fornece resultados aproximados.

Geração de Variáveis Aleatórias

Variáveis aleatórias i.i.d. Uniforme(0,1).

Geração de Variáveis Aleatórias

Variáveis aleatórias i.i.d. Uniforme(0,1).
Procedimentos para geração de números pseudoaleatórios: as sequências geradas, embora sejam determinísticas, devem ter a "aparência" de aleatoriedade.

Geração de Variáveis Aleatórias

Variáveis aleatórias i.i.d. Uniforme(0,1).
Procedimentos para geração de números pseudoaleatórios: as sequências geradas, embora sejam determinísticas, devem ter a "aparência" de aleatoriedade.
Testes de geradores de números aleatórios.

Geração de Variáveis Aleatórias

Variáveis aleatórias i.i.d. Uniforme(0,1).
Procedimentos para geração de números pseudoaleatórios: as sequências geradas, embora sejam determinísticas, devem ter a "aparência" de aleatoriedade.
Testes de geradores de números aleatórios.
Período da sequência, precisão, repetibilidade e portabilidade.

Alguns geradores

G1. Gerador de von Neumann (1949)

Alguns geradores

G1. Gerador de von Neumann (1949)

1. x_0: número de quatro algarismos decimais (semente). Faça $i = 0$.

Alguns geradores

G1. Gerador de von Neumann (1949)

1. x_0: número de quatro algarismos decimais (semente). Faça $i = 0$.
2. Calcular x_i^2. Se necessário, acrescentar zeros à esquerda para que x_i^2 seja escrito como $d_7 d_6 d_5 d_4 d_3 d_2 d_1 d_0$, em que $d_j \in \{0, 1, \ldots, 9\}$, para $j = 0, 1, \ldots, 7$.

Alguns geradores

G1. Gerador de von Neumann (1949)

1. x_0: número de quatro algarismos decimais (semente). Faça $i = 0$.
2. Calcular x_i^2. Se necessário, acrescentar zeros à esquerda para que x_i^2 seja escrito como $d_7 d_6 d_5 d_4 d_3 d_2 d_1 d_0$, em que $d_j \in \{0, 1, \ldots, 9\}$, para $j = 0, 1, \ldots, 7$.
3. Fazer $x_{i+1} = d_5 d_4 d_3 d_2$ (meio do quadrado).

Alguns geradores

G1. Gerador de von Neumann (1949)

1. x_0: número de quatro algarismos decimais (semente). Faça $i = 0$.
2. Calcular x_i^2. Se necessário, acrescentar zeros à esquerda para que x_i^2 seja escrito como $d_7 d_6 d_5 d_4 d_3 d_2 d_1 d_0$, em que $d_j \in \{0, 1, \ldots, 9\}$, para $j = 0, 1, \ldots, 7$.
3. Fazer $x_{i+1} = d_5 d_4 d_3 d_2$ (meio do quadrado).
4. Faça $i = i + 1$ e retorne ao passo 2 até que $i = n$.

Alguns geradores

G1. Gerador de von Neumann (1949)

1. x_0: número de quatro algarismos decimais (semente). Faça $i = 0$.
2. Calcular x_i^2. Se necessário, acrescentar zeros à esquerda para que x_i^2 seja escrito como $d_7 d_6 d_5 d_4 d_3 d_2 d_1 d_0$, em que $d_j \in \{0, 1, \ldots, 9\}$, para $j = 0, 1, \ldots, 7$.
3. Fazer $x_{i+1} = d_5 d_4 d_3 d_2$ (meio do quadrado).
4. Faça $i = i + 1$ e retorne ao passo 2 até que $i = n$.
5. Divida os elementos da sequência por 10.000.

Exemplos:
(a) $\{2100, 4100, 8100, 6100, 2100, \ldots\}$,

Alguns geradores

G1. Gerador de von Neumann (1949)

1. x_0: número de quatro algarismos decimais (semente). Faça $i = 0$.
2. Calcular x_i^2. Se necessário, acrescentar zeros à esquerda para que x_i^2 seja escrito como $d_7 d_6 d_5 d_4 d_3 d_2 d_1 d_0$, em que $d_j \in \{0, 1, \ldots, 9\}$, para $j = 0, 1, \ldots, 7$.
3. Fazer $x_{i+1} = d_5 d_4 d_3 d_2$ (meio do quadrado).
4. Faça $i = i + 1$ e retorne ao passo 2 até que $i = n$.
5. Divida os elementos da sequência por 10.000.

Exemplos:
(a) {2100, 4100, 8100, 6100, 2100, ...},
(b) {3792, 3792, ...},

Alguns geradores

G1. Gerador de von Neumann (1949)

1. x_0: número de quatro algarismos decimais (semente). Faça $i = 0$.
2. Calcular x_i^2. Se necessário, acrescentar zeros à esquerda para que x_i^2 seja escrito como $d_7 d_6 d_5 d_4 d_3 d_2 d_1 d_0$, em que $d_j \in \{0, 1, \ldots, 9\}$, para $j = 0, 1, \ldots, 7$.
3. Fazer $x_{i+1} = d_5 d_4 d_3 d_2$ (meio do quadrado).
4. Faça $i = i + 1$ e retorne ao passo 2 até que $i = n$.
5. Divida os elementos da sequência por 10.000.

Exemplos:
(a) {2100, 4100, 8100, 6100, 2100, ...},
(b) {3792, 3792, ...},
(c) Considere x_0 = ano de seu nascimento.

G2. Geradores congruenciais lineares (Lehmer, 1951)

G2. Geradores congruenciais lineares (Lehmer, 1951)
Gerar uma sequência de inteiros $x_1, x_2, \ldots, x_n \in \{0, 1, \ldots, \mathrm{M}-1\}$, M deve ser "grande".

G2. Geradores congruenciais lineares (Lehmer, 1951)
Gerar uma sequência de inteiros $x_1, x_2, \ldots, x_n \in \{0, 1, \ldots, \mathrm{M}-1\}$, M deve ser "grande". Fazer $u_i = x_i/M$, $i = 1, \ldots, n$,

G2. Geradores congruenciais lineares (Lehmer, 1951)
Gerar uma sequência de inteiros $x_1, x_2, \ldots, x_n \in \{0, 1, \ldots, \text{M}-1\}$, M deve ser "grande". Fazer $u_i = x_i/M$, $i = 1, \ldots, n$, em que

$$x_i = (ax_{i-1} + c) \; mod \; M,$$

sendo que $a, c, x_0 \in \{0, 1, \ldots, M-1\}$, x_0 é chamado de semente e *mod* representa o resto da divisão inteira.

G2. Geradores congruenciais lineares (Lehmer, 1951)
Gerar uma sequência de inteiros $x_1, x_2, \ldots, x_n \in \{0, 1, \ldots, \text{M}-1\}$, M deve ser "grande". Fazer $u_i = x_i/M$, $i = 1, \ldots, n$, em que

$$x_i = (ax_{i-1} + c) \; mod \; M,$$

sendo que $a, c, x_0 \in \{0, 1, \ldots, M-1\}$, x_0 é chamado de semente e *mod* representa o resto da divisão inteira.
O terno (a, c, M) caracteriza o gerador.

G2. Geradores congruenciais lineares (Lehmer, 1951)
Gerar uma sequência de inteiros $x_1, x_2, \ldots, x_n \in \{0, 1, \ldots, \text{M}-1\}$, M deve ser "grande". Fazer $u_i = x_i/M$, $i = 1, \ldots, n$, em que

$$x_i = (ax_{i-1} + c) \; mod \; M,$$

sendo que $a, c, x_0 \in \{0, 1, \ldots, M-1\}$, x_0 é chamado de semente e *mod* representa o resto da divisão inteira.
O terno (a, c, M) caracteriza o gerador. Exemplos:
(a) Gerador do IMSL: $a = 16807$, $c = 0$, $M = 2^{31} - 1$, período $= 2^{31} - 2$ $= 2.147.483.646$.

G2. Geradores congruenciais lineares (Lehmer, 1951)
Gerar uma sequência de inteiros $x_1, x_2, \ldots, x_n \in \{0, 1, \ldots, \text{M}-1\}$, M deve ser "grande". Fazer $u_i = x_i/M$, $i = 1, \ldots, n$, em que

$$x_i = (ax_{i-1} + c) \; mod \; M,$$

sendo que $a, c, x_0 \in \{0, 1, \ldots, M-1\}$, x_0 é chamado de semente e *mod* representa o resto da divisão inteira.
O terno (a, c, M) caracteriza o gerador. Exemplos:
(a) Gerador do IMSL: $a = 16807$, $c = 0$, $M = 2^{31} - 1$, período $= 2^{31} - 2$ $= 2.147.483.646$.
(b) RANDU (IBM, DEC, ...): $a = 2^{16} + 3$, $c = 0$, $M = 2^{31}$.

G2. Geradores congruenciais lineares (Lehmer, 1951)
Gerar uma sequência de inteiros $x_1, x_2, \ldots, x_n \in \{0, 1, \ldots, \text{M}-1\}$, M deve ser "grande". Fazer $u_i = x_i/M$, $i = 1, \ldots, n$, em que

$$x_i = (ax_{i-1} + c) \; mod \; M,$$

sendo que $a, c, x_0 \in \{0, 1, \ldots, M-1\}$, x_0 é chamado de semente e *mod* representa o resto da divisão inteira.
O terno (a, c, M) caracteriza o gerador. Exemplos:
(a) Gerador do IMSL: $a = 16807$, $c = 0$, $M = 2^{31} - 1$, período $= 2^{31} - 2 = 2.147.483.646$.
(b) RANDU (IBM, DEC, ...): $a = 2^{16} + 3$, $c = 0$, $M = 2^{31}$.
`randu` em R: *400 triples of successive random numbers were taken from the VAX FORTRAN function RANDU running under VMS 1.5.*

G2. Geradores congruenciais lineares (Lehmer, 1951)
Gerar uma sequência de inteiros $x_1, x_2, \ldots, x_n \in \{0, 1, \ldots, \text{M}-1\}$, M deve ser "grande". Fazer $u_i = x_i/M$, $i = 1, \ldots, n$, em que

$$x_i = (ax_{i-1} + c) \; mod \; M,$$

sendo que $a, c, x_0 \in \{0, 1, \ldots, M-1\}$, x_0 é chamado de semente e *mod* representa o resto da divisão inteira.
O terno (a, c, M) caracteriza o gerador. Exemplos:
(a) Gerador do IMSL: $a = 16807$, $c = 0$, $M = 2^{31} - 1$, período $= 2^{31} - 2 = 2.147.483.646$.
(b) RANDU (IBM, DEC, ...): $a = 2^{16} + 3$, $c = 0$, $M = 2^{31}$.
`randu` em R: *400 triples of successive random numbers were taken from the VAX FORTRAN function RANDU running under VMS 1.5.*
... the triples fall on 15 parallel planes in 3-space. This can be shown theoretically to be true for all triples from the RANDU generator.

G3. Outros geradores

G3. Outros geradores

(1) Geradores com períodos 2^{60}, 2^{113} e $2^{19937} - 1 \cong 10^{6002}$ (Mersenne-Twister, *default* em R, *equidistribution in 623 consecutive dimensions*).

G3. Outros geradores

(1) Geradores com períodos 2^{60}, 2^{113} e $2^{19937} - 1 \cong 10^{6002}$ (Mersenne-Twister, *default* em R, *equidistribution in 623 consecutive dimensions*).

(2) Gerador natural (Y. Dodge, 1996, *International Statistical Review* 64, 329–344): algarismos decimais de π.

Sugestão: Gravar bilhões de dígitos da parte fracionária de π e usar como gerador.

G3. Outros geradores

(1) Geradores com períodos 2^{60}, 2^{113} e $2^{19937} - 1 \cong 10^{6002}$ (Mersenne-Twister, *default* em R, *equidistribution in 623 consecutive dimensions*).

(2) Gerador natural (Y. Dodge, 1996, *International Statistical Review* 64, 329–344): algarismos decimais de π.

Sugestão: Gravar bilhões de dígitos da parte fracionária de π e usar como gerador.

Obs. 1. Cálculo de π com $12,1 \times 10^{12}$ dígitos decimais em dez/2013 (`http://mathworld.wolfram.com/PiDigits.html`).

G3. Outros geradores

(1) Geradores com períodos 2^{60}, 2^{113} e $2^{19937} - 1 \cong 10^{6002}$ (Mersenne-Twister, *default* em R, *equidistribution in 623 consecutive dimensions*).

(2) Gerador natural (Y. Dodge, 1996, *International Statistical Review* 64, 329–344): algarismos decimais de π.

Sugestão: Gravar bilhões de dígitos da parte fracionária de π e usar como gerador.

Obs. 1. Cálculo de π com $12,1 \times 10^{12}$ dígitos decimais em dez/2013 (`http://mathworld.wolfram.com/PiDigits.html`).

Obs. 2. Cálculo de π com 100 trilhões de dígitos ("Even more pi in the sky: Calculating 100 trillion digits of pi on Google Cloud". Google Cloud Platform, 2022, `https://cloud.google.com/blog/products/compute/calculating-100-trillion-digits-of-pi-on-google-cloud`

G3. Outros geradores

(1) Geradores com períodos 2^{60}, 2^{113} e $2^{19937} - 1 \cong 10^{6002}$ (Mersenne-Twister, *default* em R, *equidistribution in 623 consecutive dimensions*).

(2) Gerador natural (Y. Dodge, 1996, *International Statistical Review* 64, 329–344): algarismos decimais de π.

Sugestão: Gravar bilhões de dígitos da parte fracionária de π e usar como gerador.

Obs. 1. Cálculo de π com $12,1 \times 10^{12}$ dígitos decimais em dez/2013 (`http://mathworld.wolfram.com/PiDigits.html`).

Obs. 2. Cálculo de π com 100 trilhões de dígitos ("Even more pi in the sky: Calculating 100 trillion digits of pi on Google Cloud". Google Cloud Platform, 2022, `https://cloud.google.com/blog/products/compute/calculating-100-trillion-digits-of-pi-on-google-cloud`

Obs. 3. Há indicações de que *the decimal expansion of* π *is not statistically random* (R. E. Ganz, 2014, *Experimental Mathematics* 23, 99–104).

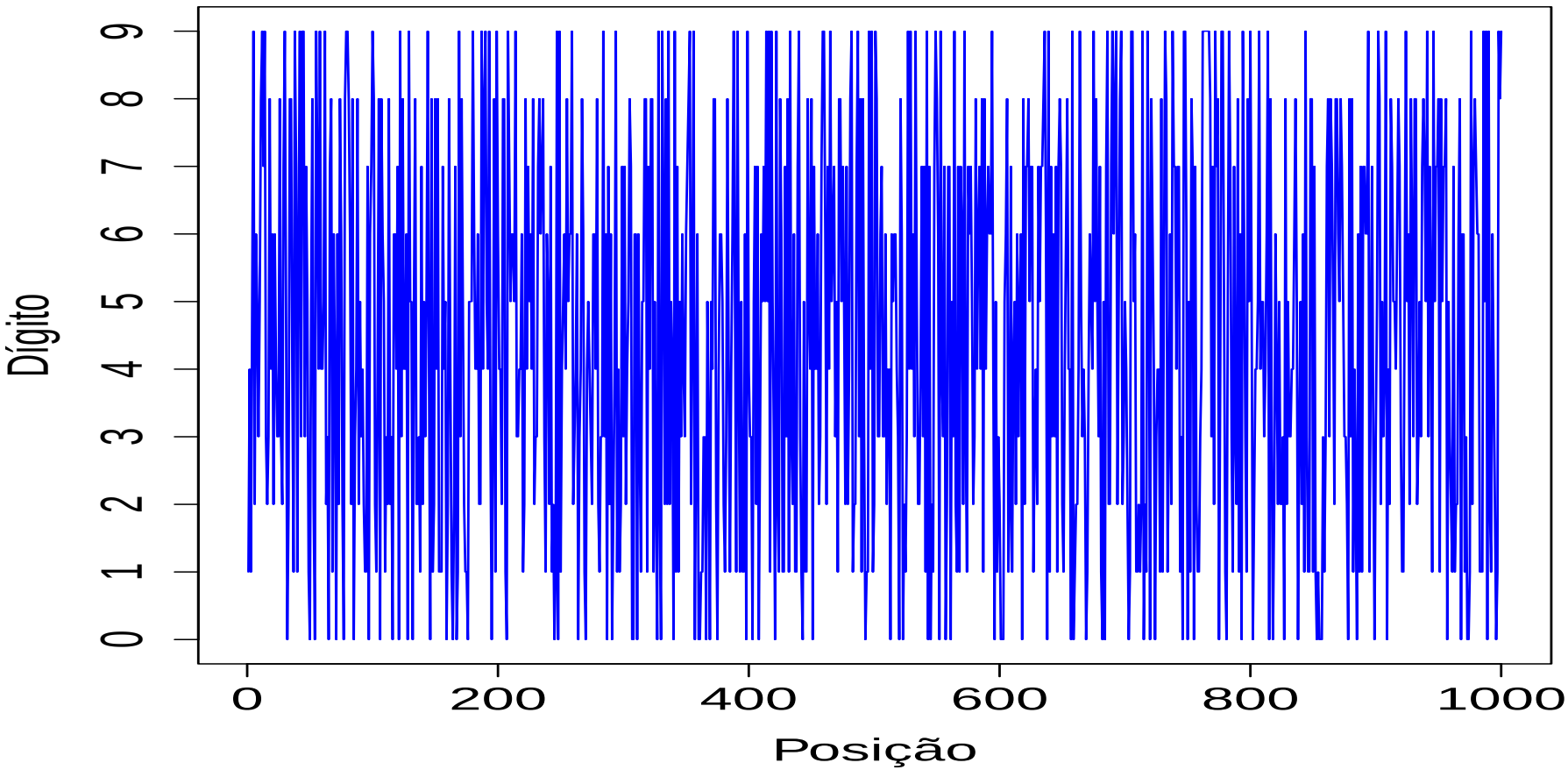

Figura 1: Sequência dos primeiros 1000 dígitos de π.

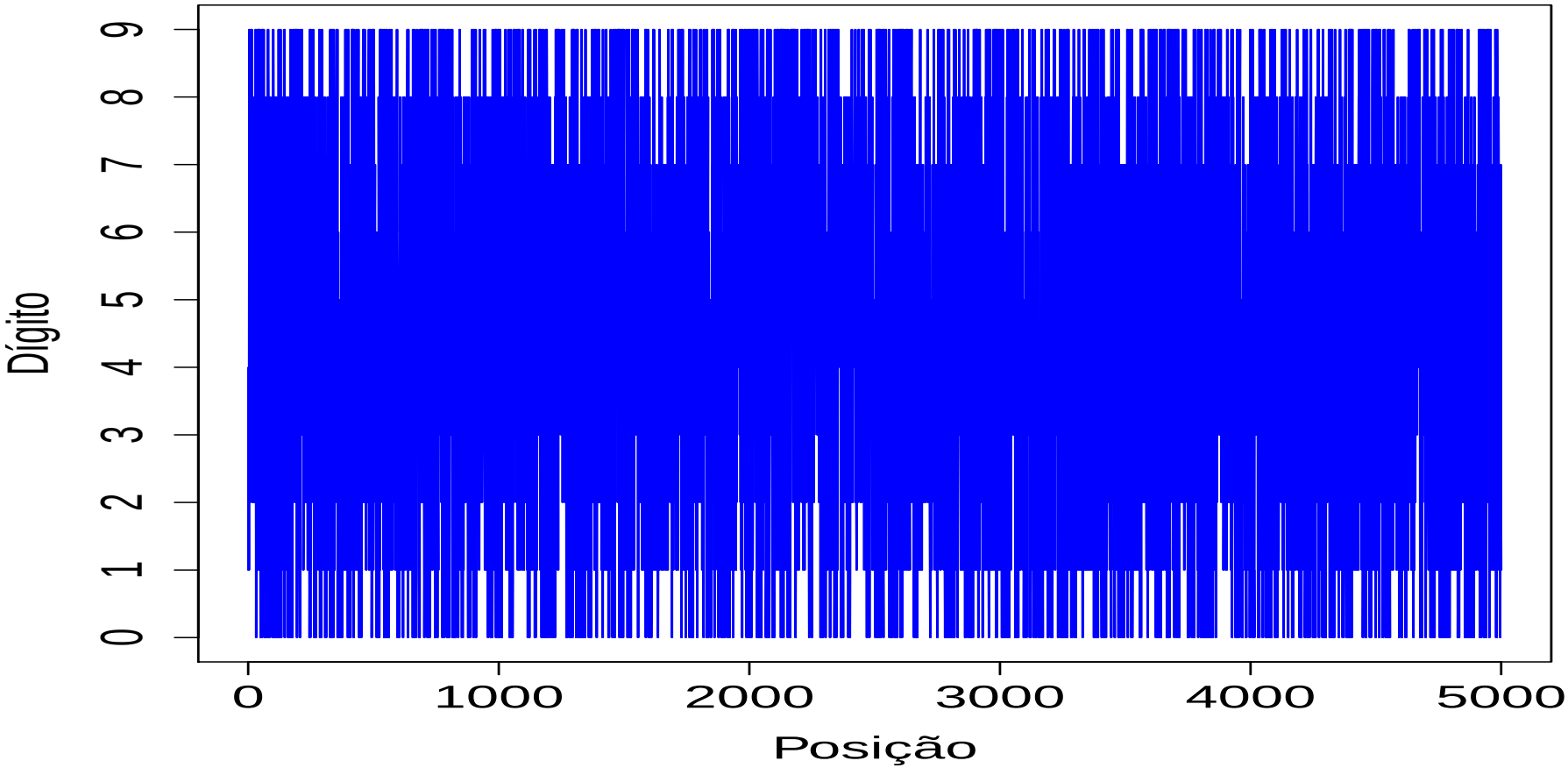

Figura 2: Sequência dos primeiros 5000 dígitos de π.

Frequências relativas dos primeiros 5000 dígitos de π:

0	1	2	3	4	5	6	7	8	9
0,093	0,106	0,099	0,092	0,102	0,105	0,103	0,098	0,098	0,104

Frequências relativas dos primeiros 5000 dígitos de π:

0	1	2	3	4	5	6	7	8	9
0,093	0,106	0,099	0,092	0,102	0,105	0,103	0,098	0,098	0,104

A distribuição é uniforme?