Aluna: Beatriz Bastos Assis Matrícula: 933 1ª Lista

① Gerador Linear Congruente (GLC) misto $X_{n+1} = (aX_n + c) \bmod m$

$a = 5 \quad c = 3 \quad m = 16 \quad X_0 = 7$

a) $X_0 = 7$

$X_1 = (5*7+3) \bmod 16 = 38 \bmod 16 = 6$

$X_2 = (5*6+3) \bmod 16 = 33 \bmod 16 = 1$

$X_3 = (5*1+3) \bmod 16 = 8 \bmod 16 = 8$

$X_4 = (5*8+3) \bmod 16 = 43 \bmod 16 = 11$

$X_5 = (5*11+3) \bmod 16 = 58 \bmod 16 = 10$

$38 \,|\, 16$: -32, 06, quociente 2 $\quad$ $33 \,|\, 16$: -32, 01, quociente 2 $\quad$ $8 \,|\, 16$: -0, 8, quociente 0

$43 \,|\, 16$: -32, 11, quociente 2 $\quad$ $58 \,|\, 16$: -48, 10, quociente 3

b) $X_6 = (5*10+3) \bmod 16 = 53 \bmod 16 = 5$

$X_7 = (5*5+3) \bmod 16 = 28 \bmod 16 = 12$

$X_8 = (5*12+3) \bmod 16 = 63 \bmod 16 = 15$

$X_9 = (5*15+3) \bmod 16 = 78 \bmod 16 = 14$

$X_{10} = (5*14+3) \bmod 16 = 73 \bmod 16 = 9$

$X_{11} = (5*9+3) \bmod 16 = 48 \bmod 16 = 0$

$X_{12} = (5*0+3) \bmod 16 = 3 \bmod 16 = 3$

$X_{13} = (5*3+3) \bmod 16 = 18 \bmod 16 = 2$

$X_{14} = (5*2+3) \bmod 16 = 13 \bmod 16 = 13$

$X_{15} = (5*13+3) \bmod 16 = 68 \bmod 16 = 4$

$X_{16} = (5*4+3) \bmod 16 = 23 \bmod 16 = 7$

$53 \,|\, 16$: -48, 5, quociente 3 $\quad$ $28 \,|\, 16$: -16, 12, quociente 1 $\quad$ $63 \,|\, 16$: -48, 15, quociente 3

$78 \,|\, 16$: -64, 14, quociente 4 $\quad$ $73 \,|\, 16$: -64, 9, quociente 4 $\quad$ $48 \,|\, 16$: -48, 0, quociente 3

$13 \,|\, 16$: -0, 13, quociente 0 $\quad$ $68 \,|\, 16$: -64, 04, quociente 4 $\quad$ $23 \,|\, 16$: -16, 7, quociente 1

Como voltou ao valor inicial $X_0 = 7$ após 16 iterações. O período é igual a 16

c) Este GCL misto não é adequado para aplicações criptográficas pois como o módulo é $m = 16$ então todos os valores estão no conjunto $\{0, 1, \ldots, 15\}$ sendo este espaço de estados pequeno este GCL misto é vulnerável a força bruta, pois é necessário testar apenas 16 possibilidades para descobrir a sequência criptográfica. Outro fator é que se o atacante descobrir os parâmetros a, c, e m ele irá descobrir os outros valores subsequentes, logo há uma previsibilidade

Para que a computação seja eficiente $m = 2^k$, k deve ser grande, valores como exemplo $k = 8 \to m = 256$ bits, ou mais; e não um $k = 4 \to m = 16$ bits como no exercício

---

② $\lambda = 3$ [chamadas/min] Distribuição Poisson

a) $Pr[X=5] = ?$

$$Pr[X=x] = \frac{\lambda^x e^{-\lambda}}{x!} \quad \therefore \quad Pr[X=5] = \frac{3^5 e^{-3}}{5!} = 0{,}1008188134 \cong 10{,}08\%$$

b) $Pr[X \leq 2] = ?$

$Pr[X \leq 2] = P(X=0) + P(X=1) + P(X=2)$

$$Pr[X \leq 2] = \frac{3^0 e^{-3}}{0!} + \frac{3^1 e^{-3}}{1!} + \frac{3^2 e^{-3}}{2!} = 0{,}04978 + 0{,}14936 + 0{,}224041$$

$Pr[X \leq 2] \cong 0{,}423181 \cong 42{,}32\%$

③ 10 questões. Cada questão 4 alternativas → 1 correta   X = acerto

a) $Pr = \binom{n}{x} q^{x}(1-q)^{n-x}$ $q = \frac{1}{4} = 0,25$

$Pr[X=3] = \binom{10}{3} 0,25^{3}(1-0,25)^{10-3} = \binom{10}{3} 0,25^{3} * 0,75^{7} = \frac{10!}{3!\,7!} 0,25^{3} * 0,75^{7}$

$Pr[X=3] = \frac{10 \cdot 9 \cdot 8 \cdot \cancel{7!}}{3!\,\cancel{7!}} * 0,25^{3} * 0,75^{7} \cong 0,250282 \cong \boxed{25,03\%}$

b) $Pr[X \le 2] = P[X=0] + P[X=1] + P[X=2]$

$Pr[X \le 2] = \binom{10}{0} 0,25^{0}(1-0,25)^{10} + \binom{10}{1} 0,25^{1}(1-0,25)^{9} + \binom{10}{2} 0,25^{2}(1-0,25)^{8}$

$Pr[X \le 2] = \frac{10!}{0!\,10!} 0,75^{10} + \frac{10!}{1!\,9!} 0,25 * 0,75^{9} + \frac{10!}{2!\,8!} 0,25^{2} 0,75^{8}$

$Pr[X \le 2] = 0,75^{10} + \frac{10 \cdot \cancel{9!}}{1 \cdot \cancel{9!}} 0,25 * 0,75^{9} + \frac{\overset{5}{\cancel{10}} \cdot 9 \cdot \cancel{8!}}{\cancel{2} \cdot \cancel{8!}} \cdot 0,25^{2} 0,75^{8}$

$Pr[X \le 2] = 0,75^{10} + 2,5 * 0,75^{9} + 45 * 0,25^{2} 0,75^{8}$

$Pr[X \le 2] = 0,525592804 \cong \boxed{52,56\%}$

c) $\mu = nq = 10 * 0,25 = 2,5$

$\sigma = \sqrt{nq(1-q)} = \sqrt{10 * 0,25(1-0,25)} \cong 1,3693$

média = 2,5 questões

desvio padrão ≅ 1,3693 questões

---

④ Distribuição de Poisson $\lambda = 6$ falhas a cada 2 semanas $P[X=x] = \frac{\lambda^{x} e^{-\lambda}}{x!}$

$Pr[X \ge 3]$ em 1 semana = ?

$\lambda = \frac{6}{2} = 3$ falhas/semana

$Pr[X \ge 3] = 1 - P[X < 3] = 1 - \left[P[X=0] + P[X=1] + P[X=2]\right]$

$Pr[X \ge 3] = 1 - \left[\frac{3^{0} e^{-3}}{0!} + \frac{3^{1} e^{-3}}{1!} + \frac{3^{2} e^{-3}}{2!}\right]$

$Pr[X \ge 3] = 1 - 0,4231900811 = 0,5768099189 \cong \boxed{57,68\%}$

5) Distribuição exponencial $\beta = 2$

a) $\beta = \frac{1}{\lambda} \rightarrow \lambda = \frac{1}{\beta} = \frac{1}{2} = 0{,}5 \frac{\text{chegadas}}{\text{minuto}}$

b) $Pr[X < 1] = ?$

$F(x) = P(X \leq x) = 1 - e^{-\lambda x} \rightarrow P[X<1] = 1 - e^{-0{,}5 * 1} \cong 0{,}393469 \cong \boxed{39{,}35\%}$

c) $Pr[X \geq 4] = ?$

$Pr[X \geq 4] = 1 - P[X \leq 4] = 1 - (1 - e^{-0{,}5*4}) = 0{,}1353352832 \cong \boxed{13{,}53\%}$

6) $pmf = f(x) = p(1-p)^{x-1}$ $p = \text{sucesso}$ $x = \text{nº tentativas}$

Distribuição geométrica $P[X=x] = (1-p)^{x-1} p$

a) $p = \frac{1}{6}$ $1 - p = \frac{5}{6}$ $P[X=3] = ?$

$P[X=3] = \frac{5}{6}^{3-1} * \frac{1}{6} = 0{,}1157407407 \cong \boxed{11{,}57\%}$

b) $P[X \geq 4] = ?$

Como os lançamentos são independentes

$P[X \geq 4] = (1^{\text{a}}\ \text{falha})(2^{\text{a}}\ \text{falha})(3^{\text{a}}\ \text{falha}) = \left(\frac{5}{6}\right)\left(\frac{5}{6}\right)\left(\frac{5}{6}\right) = \frac{5}{6}^3$

$P[X \geq 4] = 0{,}5787037037 \cong \boxed{57{,}87\%}$

c) $\text{média} = \frac{1}{p} = \frac{1}{\frac{1}{6}} = 6$ lançamentos

desvio padrão $(\sigma) = \sqrt{\frac{1-p}{p^2}} = \sqrt{\frac{5/6}{(1/6)^2}} = \sqrt{\frac{5}{6} \cdot 6^2} = 5{,}477225575$

$\sigma \cong 5{,}4772$ lançamentos

7) Método da inversa $f(x) = 3x^2$ $0 \leq x \leq 1$

$F(x) = \int 3t^2\, dt = 3 \int t^2\, dt = \frac{3t^3}{3} = t^3$

$F(x) = (t^3)\Big|_0^x = x^3 - 0^3 = x^3$

$F(x) = (t^3)\Big|_0^1 = 1^3 - 0^3 = 1$ $0 \leq x \leq 1$

$\left.\begin{array}{l} F(0) = 0^3 = 0 \\ F(1) = 1^3 = 1 \end{array}\right\} \rightarrow F(x) = x^3$

$U = x^3 \rightarrow x = \sqrt[3]{U}$ $\therefore F^{-1}(U) = U^{1/3}$

$\boxed{\begin{array}{l} pdf = f(x) = 3x^2 \\ cdf = F(x) = x^3 \end{array}}$

⑧ $\begin{cases} f(x) = 3x^2 & , 0 \leq x \leq 1 \\ f(x) = 0 & , \text{caso contrário} \end{cases}$ Método da aceitação-rejeição.

a) Para ser uma função densidade válida $f(x)$ precisa ser sempre não negativa e a área total sob a curva da função densidade deve ser igual a 1.

Então: Como x está ao quadrado então é sempre positivo dada a $f(x)=3x^2$ caso contrário, é sempre 0 que também é positivo $\boxed{\text{OK!}}$

$$\int_0^1 3x^2\,dx = \frac{3x^3}{3}\Big|_0^1 = x^3\Big|_0^1 = 1^3 - 0^3 = 1 \quad \boxed{\text{OK!}}$$

Como ambas as condições são verdadeiras, tem uma densidade válida

b) Escolhendo $g(x) = 2x$, $0 \leq x \leq 1$

$$\int_0^1 2x\,dx = \frac{2x^2}{2}\Big|_0^1 = x^2\Big|_0^1 = 1^2 - 0^2 = 1 \quad \text{OK!}$$

$$\frac{f(x)}{g(x)} = \frac{3x^2}{2x} \qquad c = \max\left(\frac{3x^2}{2x}\right)$$ Como o intervalo é de 0 a 1 então o valor máximo é quando $x=1$

$$c = \frac{3 \cdot 1^2}{2 \cdot 1} = \frac{3}{2} = 1{,}5$$

c) 1º) Gerar uma variável aleatória Y de uma distribuição conhecida $g(x)$. Para isso a variável deve ser uniforme entre 0 e 1 : $Y \sim U(0,1)$

Exemplo: $g(x) = 2x$ $\quad G(x) = x^2$ $\quad Y = \sqrt{U}$ $\quad$ Se $U' = 0{,}81$ $\quad Y = \sqrt{0{,}81} = 0{,}9$

2º) Gerar U independente de Y: Gerar outro valor aleatório independente $U \sim U(0,1)$

Exemplo: $U'' = 0{,}6$

3º) Teste de aceitação: Se $U \leq \dfrac{f(Y)}{c \cdot g(Y)}$ Então aceita-se a amostra $(X=Y)$

Senão rejeita e volta ao passo 1

Aplicando no exercício:

$$U \leq \frac{3Y^2}{1{,}5 \cdot (2Y)} = \frac{3Y^2}{Y} = Y \quad \therefore U \leq Y$$

Gerou-se $Y = 0{,}9$ e $U'' = 0{,}6$

Como $U'' = 0{,}6 \leq Y = 0{,}9$ aceita-se o valor $X = 0{,}9$

Caso a condição acima $(U \leq Y)$ não seja satisfeita $(U > Y)$, que não é o caso desse exemplo, rejeita o valor e volta para o 1º passo para gerar os novos valores