EXERCÍCIOS DE MÉTODOS PROBABILÍSTICOS
2o. SEMESTRE DE 2000

1. Prove as seguintes estimativas. Nesta questão, escrevemos $O(f(x))$ para qualquer termo y tal que $|y| \leq C|f(x)|$ para todo x satisfazendo $|x| \leq x_0$, onde C e $x_0 > 0$ são constantes absolutas. (Observe que, nestas estimativas, estamos intessados em uma vizinhança de 0.)
   (*i*) $1 + x \leq \mathrm{e}^x$ para todo $x \in \mathbb{R}$.
   (*ii*) $1 + x > \exp\left\{x - x^2/2\right\}$ para todo $0 < x \leq 1$.
   (*iii*) $1 - x > \exp\left\{-x - x^2\right\}$ para todo $0 < x < x_0$, para algum $x_0 > 0$. De fato, podemos tomar, por exemplo, $x_0 = 0.68$.
   (*iv*) $1 + x \geq \exp\left\{x + O(x^2)\right\}$ para todo $x > -1$.
   (*v*) $1 + x \geq \exp\left\{x - x^2/2 + O(x^3)\right\}$ para todo $x > -1$.
   [*Sugestão.* Lembre que $1/(1-x) = 1 + x + x^2 + \dots$ uniformemente se $|x| \leq x_0$ e $x_0 < 1$. Integre ambos os lados para obter
   $$-\log(1-x) = x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \dots]$$
   {*Data de entrega*: 4/9/2000}
2. Prove as seguintes estimativas para $\binom{a}{b}$, onde a e b são inteiros não-negativos.
   (*i*)
   $$\binom{a}{b} \geq \left(\frac{a}{b}\right)^b. \tag{1}$$
   (*ii*)
   $$\binom{a}{b} \leq \frac{a^b}{b!}. \tag{2}$$
   (*iii*) Para todo $b > 0$,
   $$\binom{a}{b} \leq \left(\frac{\mathrm{e}a}{b}\right)^b. \tag{3}$$
   [*Sugestão para* (*iii*). Avalie $(1+x)^a$ por cima e por baixo para $x = b/a$. Use, para tanto, $1 + x \leq \mathrm{e}^x$ e o binômio de Newton.]
   {*Data de entrega*: 4/9/2000}
3. Suponha que n é um inteiro positivo e que $0 \leq p \leq 1$. Seja X uma v.a. binomial de parâmetros n e p: $X \sim \mathrm{Bi}(n, p)$. Isto é,
   $$\mathbb{P}(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$$

Date: Versão de 17 de outubro de 2000.

para todo k inteiro. Prove que

$$\mathbb{P}(X \geq k) \leq \binom{n}{k} p^k \leq \left(\frac{\mathrm{e}\mu}{k}\right)^k, \tag{4}$$

onde $\mu = \mathbb{E}(X)$. $\{$*Data de entrega*: 4/9/2000$\}$

4. Suponha $2 \leq k \leq n$. Prove que existe uma família de conjuntos $\mathcal{F} \subset \binom{[n]}{k}$ *linear* (i.e., $|F \cap F'| \leq 1$ para todo F e $F' \in \mathcal{F}$ distintos) com

$$|\mathcal{F}| \geq c_k \binom{n}{2}, \tag{5}$$

onde c_k é uma constante positiva que depende apenas de k (procure maximizar c_k). Prove que qualquer tal família satisfaz

$$|\mathcal{F}| \leq \binom{k}{2}^{-1} \binom{n}{2}, \tag{6}$$

e portanto a melhor constante possível em (5) é $\binom{k}{2}^{-1}$. [*Sugestão.* Para provar a existência da família $\mathcal{F}$, ponha em uma família auxiliar $\mathcal{G}$ cada elemento de $\binom{[n]}{k}$ com probabilidade p, independentemente. Para cada par $(G, G') \in \mathcal{G} \times \mathcal{G}$ com $1 < |G \cap G'| < k$, remova G' de $\mathcal{G}$. Escolha um p adequado para que a família resultante $\mathcal{F}$ satisfaça (5).] $\{$*Data de entrega*: 4/9/2000$\}$

5. Prove que existe uma família linear $\mathcal{F} \subset \binom{[n]}{3}$ com

$$|\mathcal{F}| \geq \left(\frac{1}{3} - o(1)\right) \binom{n}{2},$$

onde $o(1)$ denota um termo que tende a 0 conforme $n \to \infty$. Note que, em vista de (6), tal família $\mathcal{F}$ tem tamanho assintoticamente ótimo. [*Sugestão.* Para cada $\{a, b, c\} \in \binom{[n]}{3}$, considere $a + b + c \pmod{n}$.] $\{$*Data de entrega*: 4/9/2000$\}$

6. Generalize o resultado da questão anterior, mostrando que existe uma família $\mathcal{F}$ de k-subconjuntos de $[n]$ tal que quaisquer dois de seus membros têm no máximo $k - 2$ elementos em comum e

$$|\mathcal{F}| \geq \left(\frac{1}{k} - o(1)\right) \binom{n}{k-1}.$$

Mostre que tal $\mathcal{F}$ tem tem tamanho assintoticamente ótimo. $\{$*Data de entrega*: 4/9/2000$\}$

7. Suponha que $p = p(n) = \omega n^{-1/3}$, onde $\omega = \omega(n) \to \infty$ conforme $n \to \infty$, e considere o grafo aleatório $G(n,p)$. Seja $0 < \varepsilon < 1$ uma constante arbitrária. Mostre que para quase todo $G = G(n,p)$ (i.e., que com probabilidade tendendo a 1 conforme $n \to \infty$) temos que todo conjunto de vértices $S \subset V(G)$ com $|S| \geq \varepsilon n$ induz um triângulo K^3 em G. [*Sugestão.* Considere famílias lineares de triplas em S.] $\{$*Data de entrega*: 11/9/2000$\}$

8. Seja G um grafo. Escrevemos $\chi_3(G)$ para o *número K^3-cromático* de G, i.e., o número mínimo de partes em uma partição $V(G) = \bigcup_i V_i$, onde cada V_i induz um subgrafo livre de K^3 em G. Equivalentemente, $\chi_3(G)$ é o número mínimo de cores com que podemos colorir os vértices de G de forma que não haja nenhum triângulo monocromático.
   (i) Mostre que K^7 é tal que $\chi_3(K^7) > 3$.
   (ii) Mostre que existem grafos G com $\chi_3(G) > 3$ livres de K^7 (i.e., que não contêm K^7 como subgrafo).
   {*Data de entrega*: 11/9/2000}
9. Lembre que escrevemos $\nu(n)$ para o número de primos que dividem n. Seja N um inteiro positivo, e considere $[N]$ como um espaço de probabilidade, com todos os seus elementos equiprováveis. Mostramos que
$$\mathbb{E}(\nu) = \log\log N + O(1) \tag{7}$$
   e que
$$\mathrm{Var}(\nu) \leq \log\log N + O(1). \tag{8}$$
   (i) Deduza cuidadosamente de (7) e (8) que se $\lambda > 1$ é uma constante, então
$$\mathbb{P}\left\{|\nu - \log\log N| > \lambda\sqrt{\log\log N}\right\} \leq \lambda^{-2} + o(1) \tag{9}$$
   conforme $N \to \infty$.
   (ii) Deduza de (9) que
$$\nu(n) \sim \log\log N$$
   para quase todo $n \in [N]$, isto é,
$$\lim_{N\to\infty} \mathbb{P}\left\{|\nu - \log\log N| > \varepsilon \log\log N\right\} = 0.$$
   para todo $\varepsilon > 0$ fixo.
   {*Data de entrega*: 11/9/2000}
10. Suponha que
$$p = p(n) = \frac{\log n + f}{n}, \tag{10}$$
   onde $f = f(n)$, e considere o grafo aleatório $G(n,p)$. Prove que as seguintes asserções valem para quase todo $G = G(n,p)$.
   (i) Se $f = f(n) \to \infty$, então G não tem vértices isolados.
   (ii) Se $f = f(n) \to -\infty$ e $|f| \leq \log n$, então G tem vértices isolados. De fato, o número de vértices isolados $X = X(G)$ em G satisfaz
$$X \sim \exp\{-f\}.$$
   (iii) O que você consegue dizer sobre o caso em que $f = f(n) \to f_0$ para alguma contante f_0?
   {*Data de entrega*: 11/9/2000}

11. Considere a identidade

$$\sum_{0\le k\le n} \binom{n}{k} = 2^n, \tag{11}$$

e seja $\omega = \omega(n)$ uma função com $\omega \to \infty$ conforme $n \to \infty$. Podemos dizer que a soma em (11) está 'concentrada' nos termos com k satisfazendo

$$\left| k - \frac{n}{2} \right| \le \omega\sqrt{n}, \tag{12}$$

pois

$$\sum\nolimits_k^* \binom{n}{k} \sim 2^n, \tag{13}$$

onde $\sum_k^*$ indica soma sobre todos os k satisfazendo (12) e escrevemos $f(n) \sim g(n)$ se $\lim_n f(n)/g(n) = 1$.

Suponha agora que $\varepsilon > 0$ é um número real fixo. Podemos dizer que a soma em (11) está 'exponencialmente concentrada' nos termos com k satisfazendo

$$\left| k - \frac{n}{2} \right| \le \varepsilon n, \tag{14}$$

pois

$$\sum\nolimits_k' \binom{n}{k} \le 2^n \exp\{-c_\varepsilon n\}, \tag{15}$$

onde $\sum_k'$ indica soma sobre todos os k para os quais (14) *não vale*, e $c_\varepsilon > 0$ é uma constante que depende apenas de ε.

(i) Prove (13).

(ii) Prove que a condição de que $\omega \to \infty$ é necessária para que (13) valha. Para tanto, use a fórmula de Stirling. Uma versão desta fórmula é como segue: para todo $n \ge 1$, existe α_n com $1/(12n+1) < \alpha_n < 1/12n$ tal que

$$\begin{aligned} n! &= \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n \mathrm{e}^{\alpha_n} \\ &= \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n \left(1 + \frac{1}{12n} + O\left(\frac{1}{n^2}\right)\right). \end{aligned} \tag{16}$$

Use (16) para provar que se $k = k(n) = n/2 + c_n\sqrt{n}$, onde $c_n \to c$ $(n \to \infty)$ e c é uma constante, então

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \sim \frac{d}{\sqrt{n}} 2^n, \tag{17}$$

onde $d = d(c) > 0$ é uma constante que depende apenas de c.

(iii) Prove (15).

{*Data de entrega*: 25/9/2000}

12. Para todo N, definimos $\mathcal{R}_N \subset 2^{[N]}$ como sendo o hipergrafo cujos membros são as progressões aritméticas contidas em $[N]$. Ademais, pomos
$$\operatorname{dev}(\mathcal{R}_N) = \min_f \max_P \Big| \sum_{x \in P} f(x) \Big|, \tag{18}$$
onde o mínimo é tomado sobre todas as funções $f\colon [N] \to \{\pm 1\}$ e o máximo é tomado sobre todos membros $P \in \mathcal{R}_N$. Prove que existem $c > 0$ e $N_0 \geq 1$ tais que
$$\operatorname{dev}(\mathcal{R}_N) \leq c(N \log N)^{1/2} \tag{19}$$
para todo $N \geq N_0$. $\{$*Data de entrega*: 25/9/2000$\}$
13. Seja $0 < \eta < 1$ um número real fixo. Mostre que existe uma constante $c = c(\eta) > 0$ para o qual vale o seguinte. Para todo $\varepsilon > 0$, existe um inteiro $N_0 = N_0(\eta, \varepsilon) \geq 1$ tal que se $N \geq N_0$, então existe $A \subset [N]$ tal que (i) $\big||A| - \eta N\big| \leq \varepsilon \eta N$ e (ii) para toda progressão aritmética $P \in \mathcal{R}_N$, temos
$$\big||P \cap A| - \eta |P|\big| \leq c(N \log N)^{1/2}. \tag{20}$$
$\{$*Data de entrega*: 25/9/2000$\}$
14. Mostre que existem constantes absolutas $c > 0$ e $N_0 \geq 1$ para os quais temos
$$\operatorname{dev}(\mathcal{R}_N) \geq cN^{1/4} \tag{21}$$
para todo $N \geq N_0$. Use o teorema de Roth (veja Teorema 25A de Beck e Chen) que afirma que o 'desvio' em (20) (isto é, o lado esquerdo daquela desigualdade) é $\geq c'(\eta(1-\eta))^{1/2} N^{1/4}$ $(c' > 0)$ para algum $P = P_A \in \mathcal{R}_N$ para todo $A \subset [N]$ com $|A| = \eta N$. Para tanto, considere $M = 2N$ e se $f\colon [N] \to \{\pm 1\}$, considere $A \subset [M]$ tal que $A \cap [N] = \{x \in [N]\colon f(x) = +1\}$ e $A \cap ([M] \setminus [N]) = \{x \in [M] \setminus [N]\colon f(x - N) = -1\}$. $\{$*Data de entrega*: 25/9/2000$\}$
15. Suponha que as variáveis aleatórias $X_1, \dots, X_n$ assumem apenas um número finito de valores. Dizemos que estas variáveis são *independentes* se para todo $I \subset [n]$, e para toda família $(R_i)_{i \in I}$ com $R_i \subset \mathbb{R}$ $(i \in I)$, temos
$$\mathbb{P}\Big(X_i \in R_i \text{ para todo } i \in I\Big) = \prod_{i \in I} \mathbb{P}(X_i \in R_i). \tag{22}$$
   (i) Suponha que as variáveis aleatórias $X_1, \dots, X_n$ como acima são independentes. Deduza que
$$\mathbb{E}\Big(\prod_{i \in I} X_i\Big) = \prod_{i \in I} \mathbb{E}(X_i). \tag{23}$$
   (ii) Suponha que $X_1, \dots, X_n$ sejam variáveis aleatórias independentes, que assumem valores em $\{\pm 1\}$, e com $\mathbb{E}(X_i) = 0$ para todo $1 \leq i \leq n$. Mostre que o espaço Ω em que estas variáveis aleatórias estão definidas precisa satisfazer $|\Omega| \geq 2^n$. A hipótese

de que estas variáveis tenham esperança nula é essencial? {*Data de entrega*: 25/9/2000}

16. Dizemos que as variáveis aleatórias $X_1, \ldots, X_n$ sao *k-a-k independentes* se, para todo $I \subset [n]$ com $|I| = k$, as variáveis X_i $(i \in I)$ formam uma família de k variáveis independentes.
    - (i) Fixe $k \geq 1$ e $n = 2^k$. Construa um espaço de probabilidade $(\Omega, \mathbb{P})$ com $|\Omega| = n$ e variáveis aleatórias $X_1, \ldots, X_{n-1}$ definidas sobre Ω, tomando valores em $\{\pm 1\}$, duas-a-duas independentes, e com $\mathbb{E}(X_i) = 0$ para todo $1 \leq i < n$. [*Sugestão.* Considere as matrizes

$$\begin{pmatrix} + & + \\ + & - \end{pmatrix}, \qquad \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix}, \qquad \text{etc.}$$

      Calcule o quadrado das matrizes acima.]
    - (ii) Suponha que $X_1, \ldots, X_{n-1}$ é uma seqüência de variáveis aleatórias definidas sobre $(\Omega, \mathbb{P})$, com $|\Omega| = n = 2^k$ e $k \geq 1$ é um inteiro. Suponha que, para um certo inteiro ℓ, a família X_i $(1 \leq i < n)$ é uma família de variáveis aleatórias ℓ-a-ℓ independentes. Dê um limitante superior para ℓ.
    - (iii) Suponha que $X_1, \ldots, X_m$ é uma seqüência de variáveis aleatórias definidas sobre Ω, com $|\Omega| = n$, tomando valores em $\{\pm 1\}$, duas-a-duas independentes, e com $\mathbb{E}(X_i) = 0$ para todo $1 \leq i \leq m$. Mostre que $m < n$. [*Sugestão.* Considere o espaço vetorial sobre $\mathbb{R}$ das funções reais definidas em Ω. Observe que $\langle X_i, X_j \rangle = |\Omega| \, \mathbb{E}(X_i X_j)$, onde $\langle f, g \rangle$ denota o produto escalar canônico. Prove que, devido às hipóteses sobre os X_i, temos que a variável constante igual a 1 e os X_i $(1 \leq i \leq m)$ são linearmente independentes.]

    {*Data de entrega*: 25/9/2000}

17. Sejam $Y_1, \ldots, Y_n$ variáveis aleatórias independentes com $\mathbb{P}(Y_i = 1) = 1 - \mathbb{P}(Y_i = 0) = p_i$ $(1 \leq i \leq n)$. Ponha $Y = \sum_{1 \leq i \leq n} Y_i$. Seja

$$\bar{p} = \frac{1}{n} \sum_{1 \leq i \leq n} p_i,$$

    e considere uma variável aleatória binomial X de parâmetros n e $\bar{p}$, isto é, $X \sim \mathrm{Bi}(n, \bar{p})$.
    - (i) Use um argumento de convexidade para provar que

$$\begin{aligned} \mathbb{E}(\mathrm{e}^{uY}) &= \prod_{1 \leq i \leq n} \big(1 + p_i(\mathrm{e}^u - 1)\big) \\ &\leq \big(1 + \bar{p}(\mathrm{e}^u - 1)\big)^n = \mathbb{E}(\mathrm{e}^{uX}) \end{aligned} \tag{24}$$

      para todo $u \in \mathbb{R}$.

(*ii*) Deduza de (24) que se $\mu = \mathbb{E}(Y)$, então, para todo $0 \le t \le n-\mu$, temos

$$\mathbb{P}\big(Y \ge \mathbb{E}(Y) + t\big) \le \left(\frac{\mu}{\mu+t}\right)^{\mu+t}\left(\frac{n-\mu}{n-\mu-t}\right)^{n-\mu-t}.$$

Note que podemos portanto concluir as desigualdades

$$\mathbb{P}\big(Y \ge \mathbb{E}(Y) + t\big) \le \exp\left(-\frac{t^2}{2(\mu+t/3)}\right) \tag{25}$$

e

$$\mathbb{P}\big(Y \le \mathbb{E}(Y) - t\big) \le \exp\left(-\frac{t^2}{2\mu}\right) \tag{26}$$

para todo $t \ge 0$. Ademais, para todo $0 \le \varepsilon \le 3/2$, temos

$$\mathbb{P}\big(|Y - \mathbb{E}(Y)| \ge \varepsilon\,\mathbb{E}(Y)\big) \le 2\exp\left(-\frac{\varepsilon^2}{3}\,\mathbb{E}(Y)\right). \tag{27}$$

(Não é necessário deduzir (25)–(27) explicitamente.)

{*Data de entrega*: 2/10/2000}

18. Dado um conjunto $A = \{a_1 < a_2 < \dots\} \subset \mathbb{N}$, escrevemos $f_A(n)$ para o número de pares (i,j) tais que $i < j$ e $a_i + a_j = n$ $(n \in \mathbb{N})$. Ademais, pomos $A(n) = \#\{a \in A : a \le n\}$. Seja $0 < \varepsilon < 1/2$ um número real fixo. Mostre que existe um conjunto A satisfazendo as seguinte duas condições:

(P_1) Temos

$$\lim_{n\to\infty} A(n)n^{-1/2+\varepsilon} = \infty. \tag{28}$$

(P_2) Existe uma constante $C = C(\varepsilon)$ para a qual temos

$$f_A(n) \le C \text{ para todo } n \ge n_0, \tag{29}$$

onde $n_0 = n_0(A)$ é uma constante.

Este é um resultado de Erdős e Rényi. {*Data de entrega*: 2/10/2000}

19. Seja k um inteiro arbitrário. Mostre que existem grafos G com

$$\chi_3(G) > k$$

livres de K^4_-, o grafo completo com 4 vértices com uma aresta removida. Nesta questão, estamos usando a notação da Questão 8. Note que aqui provamos algo mais forte que o resultado daquela questão. [*Sugestão.* Use a desigualdade de Janson e aprecie o poder deste resultado.] {*Data de entrega*: 2/10/2000}

20. Suponha que $\mathcal{H}$ seja uma família 2-universal de funções $h\colon U \to T$; isto é, para todo $(x,y) \in U \times U$ e para todo $(z_1,z_2) \in T \times T$, temos

$$\mathbb{P}_{h\in_{\mathrm{R}}\mathcal{H}}\big((h(x),h(y)) = (z_1,z_2)\big) = \frac{1}{t^2},$$

onde $t = |T|$. Acima, o índice '$h \in_{\mathrm{R}} \mathcal{H}$' indica que a probabilidade é tomada sobre uma escolha uniforme de um membro h de $\mathcal{H}$.

(*i*) Prove que para todo $x \in U$ e para todo $z \in T$, temos

$$\mathbb{P}_{h \in_{\mathrm{R}} \mathcal{H}}(h(x) = z) = \frac{1}{t}.$$

(*ii*) Fixe x, $y \in U$ e seja $B \subset T$. Ponha $Z_w = [h(w) \in B]$ para $w \in \{x, y\}$, onde $[P] = 1$ se P ocorre e $[P] = 0$ caso contrário. Prove que

$$\mathrm{Cov}(Z_x, Z_y) = \mathbb{E}(Z_x Z_y) - \mathbb{E}(Z_x)\,\mathbb{E}(Z_y) = 0$$

se $x \neq y$.

(*iii*) Seja $A \subset U$ e ponha $Z = \sum_{x \in A} Z_x$, onde a notação é como em (*ii*). Determine $\mathbb{E}(Z)$ e $\mathrm{Var}(Z)$.

{*Data de entrega*: 30/10/2000}

21. Suponha que $\mathcal{H}$ seja uma família 2-universal de funções $h\colon U \to T$. Sejam dados $A \subset U$ e $B \subset T$ e $\varepsilon > 0$. Dizemos que $h \in \mathcal{H}$ é (A, B, ε)-*bom* se

$$\Big| \mathbb{P}_{x \in_{\mathrm{R}} U}\big(x \in A \text{ e } h(x) \in B\big) - \mu(A)\mu(B) \Big| \leq \varepsilon,$$

onde $\mu(A) = |A|/|U|$ e $\mu(B) = |B|/|T|$. Prove que, para quaisquer A, B, e $\varepsilon > 0$ como acima, temos

$$\mathbb{P}_{h \in_{\mathrm{R}} \mathcal{H}}\big(h \text{ é } (A, B, \varepsilon)\text{-bom}\big) \geq 1 - \frac{\mu(A)\mu(B)(1 - \mu(B))}{\varepsilon^2 |U|}.$$

[*Sugestão*. Use os resultados da Questão 20.] {*Data de entrega*: 30/10/2000}

22. No que segue, pomos $\Sigma = \{0, 1\}$. Uma linguagem $\mathcal{L} \subset \Sigma^*$ pertence à classe **RP** se existem uma constante $c_{\mathrm{SIM}} > 0$, um polinômio $r(n) = r_{\mathcal{L}}(n)$, e um predicado $q(x, y) = q_{\mathcal{L}}(x, y)$ verificável em tempo polinomial para os quais temos que se $x \in \mathcal{L}$, então $|W_x| \geq c_{\mathrm{SIM}} 2^n$ e se $x \notin \mathcal{L}$, então $W_x = \emptyset$, onde

$$W_x = \{y \in \Sigma^r : q(x, y) = 1\}, \tag{30}$$

$r = r(n)$, e $n = |x|$ é o comprimento de x. Mostre que se $\mathcal{L} \in \mathbf{RP}$ e $\varepsilon > 0$ é uma constante positiva, então existe um algoritmo probabilístico de tempo polinomial $\mathcal{A}$ para o qual temos que

$$\text{se } x \in \mathcal{L} \text{ então } \mathbb{P}(\mathcal{A}(x) = 1) \geq 1 - \varepsilon, \tag{31}$$

e

$$\text{se } x \notin \mathcal{L} \text{ então } \mathbb{P}(\mathcal{A}(x) = 0) = 1. \tag{32}$$

Formalmente, um *algoritmo probabilístico de tempo polinomial* $\mathcal{A}$ é uma máquina de Turing com duas fitas de entrada que admite um polinômio $r(n) = r_{\mathcal{A}}(n)$ que se comporta como segue: $\mathcal{A}$ recebe um par de palavras x e $y \in \Sigma^*$ como entrada, com cada palavra em uma fita, com $|y| = r(|x|)$; a máquina $\mathcal{A}$ devolve 0 ou 1 em tempo polinomial em $|x| + |y|$. Para cada $n \geq 0$, consideramos Σ^r, onde $r = r(n)$, como um espaço de probabilidade uniforme. (Intuitivamente,

x é a instância e $y \in \{0,1\}^{r(|x|)}$ é um string de 'bits aleatórios.') Podemos considerar os eventos '$\mathcal{A}(x,y) = u$' ($u \in \{0,1\}$). Assim, por exemplo, a probabilidade que ocorre em (31) é

$$\mathbb{P}_{y \in_{\mathrm{R}} \Sigma^r}(\mathcal{A}(x,y) = 1).$$

$\{$*Data de entrega*: 30/10/2000$\}$

23. Uma linguagem $\mathcal{L} \subset \Sigma^*$ pertence à classe **BPP** se existem constantes $0 \leq c_{\mathrm{NAO}} < c_{\mathrm{SIM}} \leq 1$, um polinômio $r(n) = r_{\mathcal{L}}(n)$, e um predicado $q(x,y) = q_{\mathcal{L}}(x,y)$ verificável em tempo polinomial para os quais temos que se $x \in \mathcal{L}$, então $|W_x| \geq c_{\mathrm{SIM}} 2^r$ e se $x \notin \mathcal{L}$, então $|W_x| \leq c_{\mathrm{NAO}} 2^r$, onde W_x é como em (30). Mostre que se $\mathcal{L} \in \mathbf{BPP}$ e $\varepsilon > 0$ é uma constante positiva, então existe um algoritmo probabilístico de tempo polinomial $\mathcal{A}$ para o qual temos que

$$\text{se } x \in \mathcal{L} \text{ então } \mathbb{P}(\mathcal{A}(x) = 1) \geq 1 - \varepsilon, \tag{33}$$

e

$$\text{se } x \notin \mathcal{L} \text{ então } \mathbb{P}(\mathcal{A}(x) = 0) \geq 1 - \varepsilon. \tag{34}$$

$\{$*Data de entrega*: 30/10/2000$\}$

24. Defina a classe $\mathbf{BPP}''$ como sendo a família das linguagens $\mathcal{L} \in \Sigma^*$ que admitem um polinômio $r(n)$ e um predicado $q(x,y)$ para os quais temos que se $x \in \mathcal{L}$, então $|W_x| > (1/r)2^r$ e se $x \notin \mathcal{L}$, então $|W_x| \leq (1/r^2)2^r$. Mostre que $\mathbf{BPP} = \mathbf{BPP}''$. $\{$*Data de entrega*: 30/10/2000$\}$