MAC 338 - Análise de Algoritmos

Departamento de Ciência da Computação
Primeiro semestre de 2003

Terceira Prova

1. **(Valor: 2.5)** Considere n tarefas identificadas pelos inteiros de 1 a n. Uma *relação de precedência* entre estas tarefas é uma coleção de pares (i, j), com i e j em $\{1, \ldots, n\}$, indicando que a tarefa i deve ser executada antes da tarefa j. Uma relação de precedência pode ser dada por meio de uma matriz que contém 1 na posição (i, j) se o par (i, j) está na relação, 0 em caso contrário. Um *escalonamento de 1 a n* é uma permutação de 1 a n. Um escalonamento $\pi(1), \ldots, \pi(n)$ *satisfaz* uma relação de precedência dada por uma matriz $a_{n\times n}$ se $\pi(i) < \pi(j)$ para todo (i, j) tal que $a(i, j) = 1$. Uma *função penalidade* é uma função f não-decrescente que associa um número não-negativo a cada natural. Se uma dada tarefa tem associada a ela uma função penalidade f, podemos interpretar $f(i)$ como a penalidade por terminar a execução dessa tarefa no instante i.

   Considere o seguinte problema de escalonamento. Dadas n tarefas identificadas pelos inteiros de 1 a n, uma relação de precedência entre elas, um tempo de duração p_i e uma função penalidade f_i para cada tarefa i, determinar um escalonamento $\pi(1), \ldots, \pi(n)$ de 1 a n que satisfaça a relação de precedência e minimize a maior das penalidades, ou seja, que minimize $\max_{i=1}^{n} f_{\pi(i)}(t_i)$, onde $t_i := \sum_{j=1}^{i} p_{\pi(j)}$.

   Um tal escalonamento é chamado de *ótimo*. O seguinte algoritmo guloso resolve o problema acima. Prove que o algoritmo de fato calcula um escalonamento ótimo.

   Algoritmo Acha_Escalonamento (n, a, f)
   1. para i de 1 até n faça $n(i) := \sum_{j=1}^{n} a(i, j)$
   2. $S := \{1, \ldots, n\}$
   3. $p := \sum_{i=1}^{n} p_i$
   4. para k de n até 1 faça
   5. seja j em S com $n(j) = 0$ tal que $f_j(p)$ é mínimo
   6. $S := S \setminus \{j\}$
   7. $\pi(k) := j$
   8. $p := p - p_j$
   9. para i de 1 até n faça
   10. se $i \in S$ e $a(i, j) = 1$ então $n(i) := n(i) - 1$
   11. devolva π

   Dica: Dados dois escalonamentos, denote por r a última posição em que eles diferem; se os escalonamentos forem idênticos, deixe $r := 0$. Tome um escalonamento ótimo que tenha r mínimo em relação ao escalonamento produzido pelo algoritmo acima. Se $r = 0$, não há nada a provar. Senão, modifique o escalonamento ótimo obtendo um outro escalonamento ótimo com r menor (uma contradição). Observe que o valor do escalonamento é o **máximo** das penalidades, não a soma delas.

2. **(Valor: 2.5)** Abaixo está o pseudo-código da função `Calcula_Função_Prefixo` usada no algoritmo KMP, no pré-processamento de um padrão $P[1\,..\,m]$.

   Algoritmo Calcula_Função_Prefixo (P, m)
   1. $\pi[1] := 0$
   2. $k := 0$
   3. para q de 2 até m faça
   4. enquanto $k > 0$ e $P[k + 1] \neq P[q]$ faça
   5. $k := \pi[k]$
   6. se $P[k + 1] = P[q]$
   7. então $k := k + 1$
   8. $\pi[q] := k$
   9. devolva π

   Prove que a função acima consome tempo $O(m)$.

   Dica: Primeiro mostre que $\pi(i) < i$ para todo i. Então faça uma análise amortizada do enquanto das linhas 4 e 5.

3. **(Valor: 2.5)**

   (a) Seja U o conjunto de n-uplas de valores de $\mathbf{Z}_p$ e seja p um primo. Para cada n-upla $a = \langle a_0, \ldots, a_{n-1} \rangle$ de valores de $\mathbf{Z}_p$ e para cada b em $\mathbf{Z}_p$, defina a função $h_{a,b} : U \to \mathbf{Z}_p$ sobre a n-upla $x = \langle x_0, \ldots, x_{n-1} \rangle$ por

   $$h_{a,b}(x) = (\textstyle\sum_{j=0}^{n-1} a_j x_j + b) \mod p.$$

   Seja $\mathcal{H}$ a família $\{h_{a,b}\}$. Mostre que a coleção $\mathcal{H}_{a,b}$ é 2-universal.

   (Lembre-se que $\mathcal{H}$ é *k-universal* se, para cada seqüência fixa de k chaves distintas $\langle x^{(1)}, \ldots, x^{(k)} \rangle$ e cada h escolhido aleatoriamente (com distribuição uniforme) de $\mathcal{H}$, a seqüência $\langle h(x^{(1)}), \ldots, h(x^{(k)}) \rangle$ tem a mesma probabilidade de ser qualquer uma das p^k seqüências de comprimento k cujos elementos estão em $\{0, 1, \ldots, p-1\}$.)

   (b) Suponha que Alice e Bob concordam secretamente sobre uma função de hash $h_{a,b}$ de uma família 2-universal $\mathcal{H}$ de funções de hash. Mais tarde, Alice envia pela internet uma mensagem m a Bob na qual $m \in U$. Ela autentica a mensagem para Bob enviando também $t = h_{a,b}(m)$ e Bob verifica se o par (m, t) que ele recebe satisfaz $t = h_{a,b}(m)$. Suponha que um adversário intercepte (m, t) em trânsito e tente iludir Bob substituindo o par (m, t) por um par (m', t') diferente. Mostre que a probabilidade de o adversário ter sucesso na tentativa de fazer Bob aceitar (m', t') é no máximo $1/p$, independente de quanta capacidade de computação o adversário tenha.

4. **(Valor: 2.5)**

   (a) Defina precisamente as classes P e NP de problemas.

   (b) O que significa dizer que um problema Q é NP-completo? (Não dê a definição de NP-completude; diga o que você entende por isso.)

   (c) Marque F, V e O para, respectivamente, *falso*, *verdadeiro* e *não se sabe*.
   ( ) P $\subseteq$ NP
   ( ) P $\neq$ NP
   ( ) Existem problemas NP-completos em P.

   (d) Neste item, usaremos a mesma notação usada com o problema SAT, visto em aula. Em particular, consideramos apenas fórmulas booleanas envolvendo variáveis, suas negações e os operadores $\vee$ (ou) e $\wedge$ (e). O seguinte problema é conhecido como TAUTOLOGIA: dada uma fórmula booleana Φ, com m cláusulas sobre as variáveis $x_1, \ldots, x_n$, determinar se todas as valorações de $x_1, \ldots, x_n$ satisfazem Φ. (Se facilitar, suponha que a fórmula é dada em forma normal conjuntiva, como no SAT.)

   Prove que TAUTOLOGIA está em co-NP.

5. **(Valor: 0.5)** Levando em conta

   - a sua participação em aula, não a presencial, mas a ativa, perguntando, sugerindo, tirando dúvidas, discutindo com o colega do lado, etc;
   - a sua participação ativa, não de leitor apenas, na lista de discussão em assuntos ligados aos tópicos abordados na disciplina (não os administrativos, como sub, critérios de correção, formato da prova, e coisas do gênero);
   - o seu envolvimento geral com a disciplina ao estudar, ao tentar olhar o seu papel em outras disciplinas, ao encarar os exercícios difíceis como desafios, etc, etc,

   que nota de participação na disciplina você se daria, usando um dos conceitos abaixo?

   A - ótimo: participei de tudo um pouco;

   B - bom: participei razoavelmente;

   C - regular: participei pouco;

   D - praticamente não participei nada.