

## Lista de soluções 6

### Exercício 1

Para demonstrar que um problema pertence a NP, é suficiente mostrar que uma solução pode ser verificada em tempo polinomial. Uma solução do ISO é uma permutação dos vértices em  $G$ , e podemos verificar em tempo  $O(m)$  se  $G$  com essa permutação de vértices é isomórfico com  $H$ .

### Exercício 2

SAT-DUPLO pertence a NP, porque podemos verificar em tempo polinomial se duas atribuições dadas são diferentes e satisfazem uma dada fórmula  $\varphi$ . Para demonstrar que SAT-DUPLO é NP-difícil, vamos reduzir SAT para SAT-DUPLO. Para uma dada fórmula  $\varphi$  constrói uma fórmula  $\psi = \varphi \wedge (x \vee \neg x)$  com uma nova variável  $x$ . A fórmula  $\varphi$  é satisfatível se e somente se  $\psi$  é satisfatível por pelo menos duas atribuições diferentes.

### Exercício 3

**Ida:** Supõe que  $L \in \text{coNP}$  com  $\text{coNP}$  de acordo com a primeira definição. Logo  $\bar{L} \in \text{NP}$  e existe uma MTND existencial que decide  $\bar{L}$  em tempo  $p(|x|)$  para um polinômio  $p$ . Cria uma nova MTND  $M'$  que aceita caso  $M$  rejeita e *vice versa*.  $M'$  executa igualmente em tempo polinomial  $p(|x|)$ .

Agora  $x \in L$  se e somente se  $x \notin \bar{L}$  (por definição), se e somente se todas computações de  $M$  rejeitam (por definição da MTND existencial), sse todas computações de  $M'$  aceitam (por definição de  $M'$ ).

**Volta:** Supõe que  $L \in \text{coNP}$  com  $\text{coNP}$  de acordo com a segunda definição. Logo existe uma MTND universal que decide  $L$  em tempo polinomial  $p(|x|)$ . Com a mesma modificação anterior obtemos uma MTND  $M'$  existencial que decide  $\bar{L}$  em tempo polinomial. Logo  $L \in \text{coNP}$  pela primeira definição.

### Exercício 4

A soma de quadrados mínima (SQM) pertence a NP porque podemos verificar que uma partição respeita o limite  $L$  em tempo polinomial. Para demonstrar que ele é NP-difícil vamos reduzir PARTITION para SQM.

Para facilitar a prova vamos introduzir a notação  $\sum X = \sum_{i \in X} t_a$  e abreviar  $S = \sum A$ .

Para uma instância de PARTITION gera uma instância de SQM com os mesmos itens,  $k = 2$  e  $L = (\sum A)^2/2$ . Caso existe um  $A'$  com  $\sum A' = \sum A \setminus A'$ , temos  $\sum A' = \sum A \setminus A' = S/2$  e logo existem  $A_1 = A'$ ,  $A_2 = A \setminus A'$  tal que  $(\sum A_1)^2 + (\sum A_2)^2 = S^2/2 = L$ . Conversamente, caso existem  $A_1, A_2$  tal que  $(\sum A_1)^2 + (\sum A_2)^2 = (\sum A_1)^2 + (S - \sum A_1)^2 \leq L$  temos  $(\sum A_1)^2 + (\sum A_2)^2 = L$  porque a função  $f(x) = x^2 + (S - x)^2$  atinge o mínimo no intervalo  $[0, S]$  para  $x = S/2$  com valor  $S^2/2$ . Logo temos também  $(\sum A_1) = (\sum A_2) = S/2$ .

### Exercício 5

A redução recebe duas expressões regulares, transforma-las para autômatos finitos e depois testa se os dois autômatos são isomórficos. Caso sim, de fato as linguagens dos autômatas, e consequentemente das expressões regulares são iguais. Caso contrário, os autômatos não são isomórficos, mas isso não implica que eles não reconhecem a mesma linguagem. De fato, já expressões equivalentes simples como  $aa^*$  e  $a \cup aaa^*$  geram autômatos não isomórficos.