Exame de Qualificação - 30/06/2016
Professoras. Leila Ribeiro e Luciana S. Buriol

A avaliação levará em consideração a abrangência e a profundidade demonstradas nas soluções apresentadas.

Dicas gerais:

- Leia todas as questões antes de começar e pergunte em caso de dúvidas;
- sempre justifique a sua resposta.

Responda apenas duas questões da parte de algoritmos (questões 1 a 3). Responda as duas questões da parte de teoria da computação (questões 4 e 5).

1. (2,5 pts) Dado um grafo completo não direcionado pesado $G = (V, A)$, sendo V o conjunto de vértices, e A o conjunto de arestas com custos $c_a \in \mathcal{R}, \forall a \in A$. O problema do caixeiro viajante consiste em encontrar o ciclo Hamiltoniano (que passa por todos os nós uma única vez) de custo mínimo, onde o custo de um ciclo representa a soma dos custos das arestas que o compõe.
   O Algoritmo 1 encontra uma solução para o problema da seguinte forma: um caminho é formado partindo de um nó aleatório e a cada iteração um nó ainda não visitado mais próximo de um dos extremos do caminho é adicionado, fechando o ciclo ao final.

```
1  Selecione aleatoriamente um nó u ∈ V;
2  Encontre um nó v cujo custo c_(u,v) seja mínimo;
3  Inicie um caminho P composto apenas pelo arco (u, v);
4  custo := c_(u,v);
5  for i=1 to |V| − 2 do
6  |  Selecione o nó w cujo arco (w, x) tenha custo mínimo sendo x um dos extremos de
   |  P e w ∉ P;
7  |  Adicione x ao extremo de P cujo custo seja mínimo;
8  |  custo := custo + c_(w,x);
9  end
10 Adicione o arco a que torna o caminho P um ciclo hamiltoniano;
11 custo := custo + c_a;
12 retorne (custo);
```

Algorithm 1: Algoritmo para o problema do caixeiro viajante

Responda as seguintes questões sobre o Algoritmo 1:

a) (0.5 pt) Qual técnica de projeto de algoritmos foi usada neste algoritmo?

b) (1.0 pt) Analise a complexidade de pior caso do algoritmo. Quando conveniente, informe a estrutura de dados usada.

c) (1.0 pt) O algoritmo é ótimo, ou seja, resolve toda e qualquer instância do problema do caixeiro viajante de forma exata? Prove que sim, ou dê um contra-exemplo.

2. (2.5 pts) É dado um grid nxn com valores em cada célula (i,j), onde i e j representam os indexadores de linha e coluna, respectivamente. Um robô deve partir de uma célula qualquer da primeira linha do grid e se mover até uma célula qualquer da última linha. O robô só pode fazer três tipos de movimentos: para chegar numa célula (i,j) o robô tem que estar na célula (i-1,j-1), (i-1,j+1) ou (i-1,j). Projete um algoritmo de programação dinâmica que encontra o caminho de menor custo, onde o custo seja calculado pela soma do valor das células por onde o robô passar. Analise a complexidade de pior caso do seu algoritmo.

   Exemplo: o caminho mínimo possível no grid abaixo teria custo +1-2+0+1=0.

3	0	1	3
-1	7	0	-2
6	2	3	0
0	3	9	1

3. (2.5 pontos) É dada uma sequência de números arbitrários. Um *swap* representa a troca de posições entre dois elementos vizinhos da sequência. Projete um algoritmo que calcula o número mínimo de swaps necessários para ordenar a sequência de números.
   Por exemplo, para S=[4 2 9 0 4] são necessários 5 swaps: 0/9, 0/2, 0/4, 2/4 e 4/9 para obter [0 2 4 4 9].

4. (2.5 pontos) Disserte sobre *Computabilidade*.

5. (2.5 pontos) RSA é um algoritmo de criptografia baseado em um par de chaves, uma pública e uma privada. Uma mensagem cifrada usando uma chave pública só pode ser decodificada usando a respectiva chave privada. Neste algoritmo a construção das chaves se baseia na geração de dois números primos muito grandes e da sua multiplicação, de tal forma que é uma tarefa computacionalmente custosa dada uma chave pública, encontrar os números primos originais, com os quais a mensagem pode ser decodificada. Hoje em dia, grande parte das transações realizadas na internet usam criptografia RSA.

   Assuma que a chave pública do RSA consiste apenas na multiplicação de dois números primos e a chave privada correspondente é formada pelos dois números primos (na realidade, as chaves são mais complexas que isso no RSA). Neste caso, dada uma chave pública n, o código poderia ser quebrado se fossem encontrados os dois números primos p e q que multiplicados geram a chave pública (ou seja, a fatoração de n em números primos é $n = p \times q$). Considere a seguinte frase de um forum de criptografia:

   "Quebrar o RSA é NP-completo, portanto não existe maneira melhor que usar força bruta para isso."

   Avalie esta frase, levando em consideração as seguintes questões:

   a) O que significa precisamente *"quebrar o RSA é NP-completo"*? Ou seja, qual é o problema de decisão envolvido e o que significa dizer que ele é NP-completo?

   b) O problema pertence à classe NP? Justifique.

   c) Assumindo que a premissa está correta, ou seja, que *"quebrar o RSA é realmente NP-completo"*, a conclusão da frase é uma consequência lógica? Justifique.

   d) Fale sobre o impacto da questão *P=NP?* para criptografia baseada no RSA.