

**CS\_232 2007/08**  
**Algorithms and Complexity**

*(Attempt 2 questions out of 3)*

**Question 1** Graphs

- (a) Define the notion of a *general graph*, and explain the differences to the notion of a *graph*.

**[3 marks]**

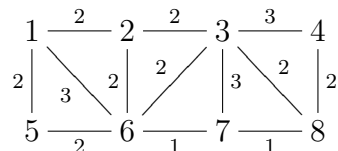
- (b) Give an example for a non-2-colourable graph  $G$ , such that  $G$  has at least 4 vertices and becomes 2-colourable after removal of any edge. Justify your example.

**[4 marks]**

- (c) Explain the generic procedure `graph_traversal` in your own words, with emphasis on the role of the visitor object and the buffer object.

**[6 marks]**

- (d) Run the efficient algorithm for finding an SPT (Shortest Path Tree) we discussed in the lecture (Dijkstra's algorithm) on the following graph, using the root 1 and showing the single steps of your computation; display the final resulting SPT:



**[6 marks]**

- (e) The *girth* of a general graph  $G$  with (arbitrary) edge weights is the minimal length of a circuit in  $G$  if  $G$  has a circuit (that is,  $G$  is not a forest), while otherwise the girth of  $G$  is  $+\infty$ . For example, the girth of the graph under (d) is 6. Assuming nonnegative edge weights, show how to compute the girth of  $G$  in polynomial time. (Hint: run through all the edges.)

**[6 marks]**

**Question 2** Complexity theory

- (a) Define as precisely as possible the complexity classes P and NP. **[6 marks]**
- (b) Define as precisely as possible when a language is NP-complete. **[3 marks]**
- (c) It is the case that professor X either always gives extremely interesting lectures or always gives extremely boring lectures. The following rules may help us to find out what is the case:
- i. If a professor always gives extremely interesting lectures, then he must be a strange guy.
  - ii. If a person is not a strange guy, then he has a dog.
  - iii. X has a dog or a wife, but not both.
  - iv. Strange guys are married.
  - v. If a professor always gives extremely boring lectures, then he has a dog.
- (i) Formulate the problem as a propositional satisfiability problem. Solve this satisfiability problem to the necessary degree, and state explicitly your findings about the lectures of professor X (we would like to know which kind of lectures professor X gives). **[6 marks]**
- (ii) What is the relation to the notion of NP-completeness? Discuss as thoroughly as possible. **[6 marks]**
- (d) State two decision problems which are not in NP and discuss your reasons. **[4 marks]**

### Question 3 Cryptology

For all the following computations it is essential that you show all details of your computations.

(a) Modular arithmetic and the Euclidean algorithm

- (i) Give the addition table and the multiplication for  $\mathbb{Z}_5$  (arithmetic modulo 5). Explain how to obtain additive and multiplicative inverses using these tables. **[6 marks]**
- (ii) Compute  $\text{pow}_{19}(8, 135) \in \mathbb{Z}_{19}$ . **[3 marks]**
- (iii) Compute  $\text{gcd}(144, 56)$  with the Euclidean algorithm, showing the Euclidean sequence. **[2 marks]**
- (iv) Extend the computation of  $\text{gcd}(144, 56)$  with the computation of the Euclidean extension sequence, and derive coefficients  $x, y \in \mathbb{Z}$  with  $x \cdot 144 + y \cdot 56 = \text{gcd}(144, 56)$ . **[2 marks]**
- (v) Decide whether 56 is invertible in  $\mathbb{Z}_{144}$  and whether 59 is invertible in  $\mathbb{Z}_{144}$ ; in the affirmative case compute the inverse. **[2 marks]**

(b) RSA

- (i) State the requirements on a public key (pair)  $n, e$ . **[2 marks]**
- (ii) Encrypt the plaintext  $m = 33 \in \mathbb{Z}_{299}$  into  $c = \text{RSA}_{(299,61)}(33)$ , using the public key  $n = 299, e = 61$ . **[3 marks]**
- (iii) Decrypt the ciphertext  $c = 3$ , given the same public key as before. **[5 marks]**