CS_232 2005/06
Algorithms and Complexity

(Attempt 2 questions out of 3)

Question 1 Complexity theory

(a) Complexity classes

(i) Explain "decision problems", "languages" and "complexity classes". How are the complexity classes ELTime and PSpace defined?

[6 marks]

(ii) State the SAT problem, and explain what it means that the SAT problem is NP-complete.

[6 marks]

(b) The SAT problem

(i) Describe the backtracking approach to solve the SAT problem, and discuss whether this approach can be generalised to arbitrary problems in NP.

[6 marks]

(ii) A "Latin square" of order $n \in \mathbb{N}$ is a square with entries from $\{1, \ldots, n\}$ such that no row and no column contains the same number two or more times. For example

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

is a Latin square or order 3. Translate the problem of finding a Latin Square of dimension n into a satisfiability problem. (Hint: The basic problem is to find the right notion of (boolean) variables. A suitable notion here is to have variables expressing that a certain field contains a certain number or not; for order 3 this would mean $9 \cdot 3 = 27$ variables.)

[7 marks]

Question 2 Graphs

(a) Fundamental properties

(i) Discuss the distinction between a "graph" and a "graph drawing".

[2 marks]

(ii) Consider a connected graph G. An "articulation point" in G is a vertex $v \in V(G)$ such that removing v from G would render G disconnected, while a "bridge" in G is an edge $e \in E(G)$ such that removing e from G would render G disconnected. Describe polynomial time algorithms determining articulation points, respectively bridges, in G (if they exist); explain in words and using the Big Oh notation how many steps your algorithms take.

[5 marks]

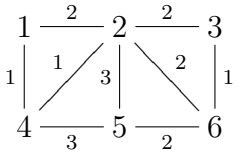
(b) The `graph_traversal` procedure

(i) Describe and explain the `graph_traversal` procedure, including the role of the buffer and the visitor.

[6 marks]

(ii) Show and explain the stepwise application of Dijkstra's algorithm to

$G =$



starting with vertex 1. Show the resulting SPT, and explain its meaning.

[5 marks]

(c) Bipartite graphs

(i) Define "bipartite graphs".

[2 marks]

(ii) Explain the strategy for the efficient algorithm deciding whether a graph is bipartite or not, and apply this algorithm to the grid graphs $\mathrm{Gr}_{m,n}$. Aim for handling general m, n, but you might consider special values for m, n, for example $m = n = 3$, in which case you must explain how your result can be generalised.

[5 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) Compute $6 +_5 8 \in \mathbb{Z}_5$, $3 -_{12} 7 \in \mathbb{Z}_{12}$ and $4 *_7 6 \in \mathbb{Z}_7$.

[3 marks]

(ii) Compute $\mathrm{pow}_{23}(5, 101) \in \mathbb{Z}_{23}$.

[3 marks]

(iii) Compute $\gcd(133, 98)$ with the Euclidean algorithm, showing the Euclidean sequence.

[2 marks]

(iv) Extend the computation of $\gcd(133, 98)$ with the computation of the Euclidean extension sequence, and derive coefficients $x, y \in \mathbb{Z}$ with $x \cdot 133 + y \cdot 98 = \gcd(133, 98)$.

[2 marks]

(v) Decide whether 98 is invertible in $\mathbb{Z}_{133}$ and whether 99 is invertible in $\mathbb{Z}_{133}$; in the affirmative case compute the inverse.

[2 marks]

(b) RSA

(i) Encrypt the plaintext $m = 15$ into the ciphertext $c = \mathrm{RSA}_{(187,7)}(15)$, using the public key $n = 187$, $e = 7$.

[3 marks]

(ii) Decrypt the ciphertext $c = 94$ into the plaintext $m = \mathrm{RSA}^{-1}_{(187,7)}(94)$ (using the same public key $n = 187$, $e = 7$). Hint: You must break the code here!

[5 marks]

(c) Write a (short) "user manual" for RSA, answering in plain words the questions, what kind of encryption can be performed with the help of RSA, and how encryption and decryption is performed in principle (where messages are given as plain text). Do not forget to explain the different types of keys, and how security can be achieved.

[5 marks]