unibz
Fakultät für Informatik
Facoltà di Scienze e Tecnologie informatiche
Faculty of Computer Science

Advanced Algorithms

Written Examination

20th February 2015

FIRST NAME		**LAST NAME**	
STUDENT NUMBER		**SIGNATURE**	

Instructions for students

Write First Name, Last Name, Student Number and Signature where indicated. If not, the examination cannot be marked.

Use a pen, not a pencil.

Write neatly and clearly.

Student Code Ethics

Students are expected to maintain the highest standards of academic integrity. Work that is not the students' own creation will receive no credit. Remember that you cannot give or receive unauthorized aid on any assignment, quiz, or exam. Students cannot use others' ideas and declare that they belong to them. Students are required to properly cite the original sources of the ideas and information used in their work.

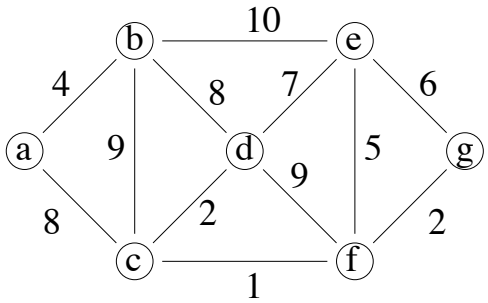
Exercise 1 (4 points)
Explain the typical scenario of the RSA cryptosystem, in which Alice and Bob want to communicate in private and Eve attempts to decrypt the messages they exchange. In particular, explain why the encryption and decryption of messages is easy for Alice and Bob, while decryption is extremely difficult for Eve.

Solution
Suppose that Alice wants to send a message m to Bob. She encrypts m using Bob's public key, obtaining m_{enc} and then sends m_{enc} over the communication channel. Bob can then decrypt m_{enc} using his private key, obtaining back m.
Bob's public key is (N, e) and can be calculated in polynomial time by selecting two prime numbers p and q, setting $N=p*q$, and selecting e as a number relatively prime to $(p-1)*(q-1)$. Bob's private key d is the inverse of e mod $(p-1)*(q-1)$, also calculated in polynomial time using the extended Euclid algorithm. The encryption $m_{enc}=m^e \ mod \ N$ is calculated in polynomial time. The decryption $m = m_{enc}^{\ d} \ mod \ N$ is also calculated in polynomial time.
In order to decrypt m_{enc} without knowing d, Eve could experiment with all possible values of m, each time checking whether $m^e \equiv m_{enc} \ mod \ N$, but this would take exponential time. Or she could try to factor N to retrieve p and q, and then figure out d by calculating the inverse of e mod $(p-1)*(q-1)$, but factoring would also take exponential time.

Exercise 2 (3 points)
Make examples of: supervised learning, unsupervised learning, classification problem, and regression problem.

Solution
See lecture 11.

Exercise 3 (4 points)
The Prim's algorithm finds a minimum spanning tree (MST) on a connected graph. For the graph below, show the steps in executing Prim's algorithm. Draw the partial MST identified at each step.



In general, can a connected graph have more than one MST? If not, explain why; if yes, does the graph above have more than one MST?

Solution
The application of the Prim's algorithm to the given graph finds a MST including the following edges:

ab, bd, dc, cf, fg, fe

The edges are in the order of inclusion in the MST. The starting node of the algorithm is node a. In general, a connected graph can have more than 1 MST. The given graph has another MST:

ab, ac, cd, cf, fg, fe

Exercise 4 (3.5 points)
Under a Huffman encoding of n symbols with frequencies $f_1, f_2, ..., f_n$, what could the maximum length of a codeword possibly be? Give a sample set of frequencies that would produce this case.

Solution
The longest codeword can be of length $n-1$. An encoding of n symbols with $n-2$ of them having probabilities $1/2, 1/4, \ldots, 1/2^{n-2}$ and two of them having probability $1/2^{n-1}$ achieves this value.

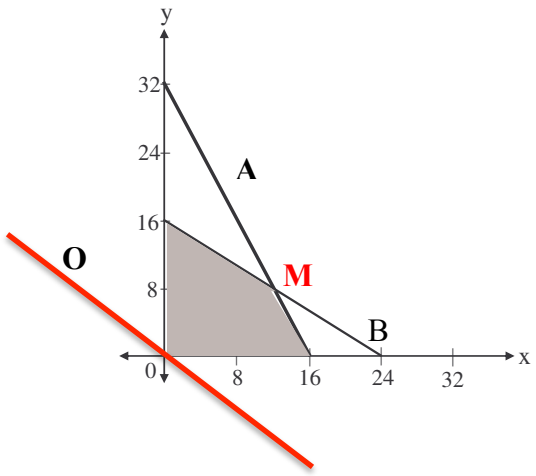
Exercise 5 (3.5 points)
A small business enterprise makes dresses and trousers. To make a dress requires 1/2 hour of cutting and 20 minutes of sewing. To make a pair of trousers requires 15 minutes of cutting and 1/2 hour of sewing. The profit on a dress is 40 € and on a pair of trousers is 50 €. The business operates for a maximum of 8 hours per day. Determine how many dresses and trousers should be made to maximize the daily profit and what the maximum profit is.

1. Formulate a linear programming model for this problem;
2. Use the graphical method to solve this model.

Solution
Let x be the number of dresses and y the number of trousers.

(A) Constraint on cutting time:	$1/2x + 1/4y \leq 8$	→	$2x+y\leq 32$
(B) Constraint of sewing time:	$1/3x+1/2y \leq 8$	→	$2x+3y\leq 48$
Trivial constraints:	$x\geq 0, y\geq 0$		
(O) Objective function:	max $40x+50y$		

Feasible region:



The line corresponding to all the pairs (x,y) for which the objective is equal to 0 is denoted by O. Given the slope of this line, we can visually determine that the maximum of the objective function is the vertex of the feasible region indicated by M. The coordinates of M can be found calculating the intersection of lines A and B; M=(12, 8). The value of the objective function in M is 880.