COSC 4P03 TERM TEST
MARCH 23RD, 2018

Total marks: 50. Total time: 80 minutes.
Answer all questions *in your exam booklet*.
This test is open book; the following materials are allowed:

1. Any handwritten, printed or photocopied material (notes, books, assignments, etc)
2. Calculator

Please write *complete* but *concise* answers.

Part	Question	Value	Mark
1	1	12	
	2	6	
2	1	6	
	2	10	
3	1	6	
	2	10	
Bonus		1	
Total:		50	

PART 1 – DYNAMIC PROGRAMMING AND GREEDY ALGORITHMS [18 MARKS]

Question 1 [2x6 marks] – Answer ***two*** of a, b and c:

a) In a problem for which a dynamic programming algorithm can be successfully used, there is often an implicit ordering to the elements. Give the intuition behind why this ordering makes a dynamic programming algorithm successful.

b) Suppose that an approximation algorithm is to be used for an optimization problem. What is the *approximation ratio*? What is an *approximation scheme*? What is a *polynomial-time* approximation scheme?

c) Suppose that M = (S,I) is a matroid, where S is a finite nonempty set, and I is a nonempty family of subsets of S. What does it mean to say that I is *hereditary*? What is the *exchange property*?

PART 1 – DYNAMIC PROGRAMMING AND GREEDY ALGORITHMS, CONTINUED.

Question 2 [6 marks]

Consider a history exam in which students must give the chronological order of a number of historical events. Students who order all the events correctly will receive full credit, but partial credit is more difficult to determine. You are to determine partial credit according to the following rule:

> "Give 1 point for each event in the longest (not necessarily contiguous) sequence of events which are in the correct order relative to each other."

For example, if the correct order of four events is 1 2 3 4, and a student gives the answer 1 3 2 4, then the student should receive a score of 3: the longest event sequences in which all events are in correct order relative to one another are 1 2 4 and 1 3 4 (both of length 3).

Suppose that the correct sequence of events is $<x_1, \ldots, x_n>$ and that the student's sequence of events is $<y_1, \ldots, y_n>$.

Give a recursive definition for $c[i][j]$, $0 \leq i \leq n$, $0 \leq j \leq n$, the score (length of the longest common subsequence) from $<x_1, \ldots, x_i>$ and $<y_1, \ldots, y_j>$.

PART 2 – COMBINATORIAL ALGORITHMS [16 MARKS]

Question 1 [6 marks] – Answer ***one*** of a and b:

a) What is a *bounding function* and what is it used for? Describe a bounding function that one might use when trying to find a set that has maximum size (from among all those that satisfy certain conditions).

b) What is a *minimal change ordering*? List all subsets of {1,2,3} using a minimal-change ordering. What is the rank of the subset {1,2} in this list?

PART 2 – COMBINATORIAL ALGORITHMS, CONTINUED.

Question 2 [2x5 marks]

The 5-Queens problem can be stated as follows: given a 5x5 chessboard, find all ways to place 5 queens on the chessboard so that no row, column or diagonal contains more than 1 queen. The following questions relate to backtrack search and estimation for the 5-Queens problem.

a) Give the portion of the backtrack search tree that corresponds to all 5x5 chessboards in which there is a queen in row 1 of column 1 as shown below. In this tree you should show all acceptable row indices for the locations of queens in the remaining columns. *Do not* show the portion of the tree that corresponds to other choices for the location of the queen in column 1, because this will take too long.

	1	2	3	4	5
1	Q				
2					
3					
4					
5					

b) Based on the search tree you have provided in part (a) above, give a table indicating the estimated number of nodes at each level of the *entire* search tree (i.e. including all possible choices for column 1). Assume that your estimation program always chooses the first (i.e. leftmost) branch at each level of the search. Show all necessary calculations.

PART 3 – CRYPTOGRAPHY [16 MARKS]

Question 1 [6 marks] – Answer ***one*** of a and b:

a) What are *computational security*, *provable security*, and *unconditional security*, as applied to the problem of establishing the security of a given cryptosystem?

b) What is the difference between *secrecy* and *authenticity*? Why is authenticity more difficult to ensure in a public-key system than in a private-key system?

PART 3 – CRYPTOGRAPHY, CONTINUED.

Question 2 [10 marks]

You wish to set up a Merkle-Hellman Knapsack cryptosystem so that your friends can send private messages to you. You choose n=5, s=(1, 4, 7, 14, 27), p=59 and a=5.

a) [4 marks] What are the public and private keys of this cryptosystem? Show your work.

b) [3 marks] Determine a^{-1} mod 59.

c) [3 marks] What is the plaintext corresponding to the ciphertext 48? Show your work. Note: if you were unable to complete calculations from a previous part, then demonstrate the steps you must go through to decipher the message.

Bonus Question [1 mark] For solving what Computer Science problem can you "win" $1 million?