DMP221
Discrete Mathematics – Fall 2013
Final Exam – Form A – Solution

120 Minutes

<u>**Instructions:**</u>

- **The exam consists of 7 problems on 6 pages. Most problems are subdivided into sections like 1(a), 1(b), etc. The last problem is 7b. Make sure your exam is complete before you begin.**
- **Show all work in detail or your answer will not receive any credit. All answers without supporting work receive ZERO credit.**
- **Write neatly and box all answers.**
- **Include appropriate units on all questions that apply. When drawing graphs, make sure to clearly label axes, scale, and curves.**
- **Do not use your own scratch paper. You may ask for scratch paper at the front desk (or from your instructor if the exam is conducted in class).**
- **Turn off your handy phone. Leave all electronic devices in your backpack, and leave your backpack at the front of the room.**
- **No calculators with QWERTY keyboards or ones like the Casio FX-2, TI-89 or TI-92 that do symbolic algebra may be used.**
- **Add your student ID, name, signature and submit this form together with your answer sheet.**

Honor Statement:
By signing below you confirm that you have neither given nor received any unauthorized assistance on this exam. This includes any use of a graphing calculator beyond those uses specifically authorized by the Faculty of Information Technology (FIT) and your instructor. Furthermore, you agree not to discuss this exam with anyone until the exam testing period is over. In addition, your calculator's program memory and menus may be checked at any time and cleared by any testing center proctor or FIT's instructor.

Student ID	Student Name	Signature

1. **Multiple Choices (20 points):** Select the best answer for the question.

   (a) (2 points) Suppose h and c are these propositions:

   $$h\text{: "I go hiking"},\ c\text{: "It is a cold day."}$$

   Express in symbols the compound proposition "I don't go hiking when it is a cold day."

   i. $h \to c$. ii. $c \to \neg h$. iii. $\neg c \to h$. iv. $\neg h \to c$.

   (b) (2 points) Consider the statement:

   "If the product of two integers is even, then their sum is also even."

   Which of the following assertions is correct?

   i. The statement is true and can be proved easily using either a direct proof or a proof by contraposition.
   ii. The statement is true and can be proved most easily using a proof by contradiction.
   iii. The statement is true and can be proved most easily using a proof by contraposition.
   iv. The statement is false as can be shown by finding a counterexample.

   (c) (2 points) Suppose you are examining a conjecture of the form $\forall x(P(x) \to Q(x))$. If you are looking for a counterexample, you need to find a value x such that:

   i. $P(x)$ and $Q(x)$ are true.
   ii. $P(x)$ and $Q(x)$ are false.
   iii. $Q(x)$ is true and $P(x)$ is false.
   iv. $P(x)$ is true and $Q(x)$ is false.

   (d) (2 points) Which one of these statements is true? Assume that the universe for x and y consists of all numbers.

   i. $\forall x \exists y\ (-x < y < x)$.
   ii. $\forall x \exists y\ ((x \neq 0) \to (-x < y < x))$.
   iii. $\exists x \exists y\ (x < y + 1 < x + 1 < y)$.
   iv. $\exists y \forall x\ (x \leq y \leq x^2)$.
   v. $\forall x \exists y\ (x^2 \leq x + y)$.

   (e) (2 points) Which one of these rules defines a function f from the set of all strings of length six of letters of the alphabet to the set $\{1, 2, 3, 4, 5, 6\}$?

   i. The rule that assigns to each string the number of vowels in the string. For example, f(TAZNAV)=2.
   ii. The rule that assigns to each string the number of times Z is an element of the string. For example, f(RZVZQC)=2.

iii. The rule that assigns to each string the reverse of the string. For example, f(BAQKDU)=UDKQAB.

iv. The rule that assigns to each string the position in which the first Z occurs. For example, f(PPABZY)=5.

v. The rule that assigns to each string the number of distinct letters appearing in the string. For example, f(TNVRRN)=4.

(f) (2 points) Suppose $f : \mathbf{R} \to \mathbf{R}$ has the following property for all real numbers x and y: if $x < y$ then $f(x) < f(y)$. (A function with this property is called a strictly increasing function.) Which of the following is true?

i. f must be one-to-one but is not necessarily onto $\mathbf{R}$.

ii. f is onto $\mathbf{R}$, but is not necessarily one-to-one.

iii. f must be both one-to-one and onto $\mathbf{R}$.

iv. f is not necessarily one-to-one and not necessarily onto $\mathbf{R}$.

(g) (2 points) Which of the following is true for all sets A and B?

i. $A \cup \overline{B} = \overline{A \cap B}$.

ii. $A \cup \overline{B} = (A \cap B) \cup B$.

iii. $(A \cup B) \cap B = B \cup (A \cap B)$.

iv. $A - (B - A) = A \cap \overline{B}$.

(h) (2 points) Suppose you want to use the principle of mathematical induction to prove that

$$1 + 2 + 2^2 + 2^3 + \ldots + 2^n = 2^{n+1} - 1$$

for all nonnegative integers n. Which of these is the correct statement $P(k)$ in the inductive hypothesis?

i. $1+2^1+2^2+2^3+\ldots+2^{k+1} = 2^{k+2}-1$

ii. $2^{k+1} - 1$

iii. $1 + 2^1 + 2^2 + 2^3 + \ldots + 2^k = 2^{k+1} - 1$

iv. $1 + 2^1 + 2^2 + 2^3 + \ldots + 2^k + 2^{k+1}$

(i) (2 points) Let G be a nonempty set with a operation $\bullet$ (multiplication) defined on it: $a, b \mapsto a \bullet b$. $(G, \bullet)$ will be a group if the following axioms are satisfied:

i. Closure, associate law, identity element, inverse element.

ii. Closure, associate law, commutative law, distributive law, additive identity element, additive inverse element.

iii. Closure, associative law, commutative law, distributive law, additive identity element, additive inverse element, multiplicative identity element, multiplicative inverse element.

iv. Closure, associative law, commutative law, distributive law, multiplicative identity element, multiplicative inverse element.

(j) (2 points) Alice set up a secret sharing scheme where she want to distribute five shares to five persons such that any three or more persons can figure out the secret, but two or fewer persons cannot. She employs the polynomial $P(x)$ in $GF(7)$ (where $P(0) = s$ is the secret) with the shares are $P(1) = 6$, $P(2) = 4$, $P(3) = 4$, $P(4) = 6$, and $P(5) = 3$. So, the secrete key must be

i. 1   ii. 3   iii. 2   iv. 4

Solution: $(a).ii; (b).iv; (c).iv; (d).v; (e).v; (f).i; (g).iii; (h).iii; (i).i; (j).ii - P(x) = x^2 + 2x + 3$
Check Self Assessments link in DMP course.

2. **Fill in the Blank (30 points):** Use only one word for each question.

(a) (2 points) A _______ graph (V, E) consists of a nonempty set of vertices V and a set of _______ edges (or arcs) E. Each _______ edge is associated with an ordered pair of vertices. The _______ edge associated with the ordered pair (u, v) is said to start at u and end at v. (directed)

(b) (2 points) A simple graph G is called _______ if its vertex set V can be partitioned into two disjoint sets V_1 and V_2 such that every edge in the graph connects a vertex in V_1 and a vertex in V_2 (so that no edge in G connects either two vertices in V_1 or two vertices in V_2). (bipartite)

(c) (2 points) A path from a to b in the directed graph G is a sequence of edges $(x_0, x_1), (x_1, x_2), (x_2, x_3), \ldots, (x_{n-1}, x_n)$ in G, where n is a nonnegative integer, and $x_0 = a$ and $x_n = b$, that is, a sequence of edges where the terminal vertex of an edge is the same as the initial vertex in the next edge in the path. This path is denoted by $x_0, x_1, x_2, \ldots, x_{n-1}, x_n$ and has length n. We view the empty set of edges as a path of length zero from a to a. A path of length $n \geq 1$ that begins and ends at the same vertex is called a _______. (circuit or cycle)

(d) (2 points) An _______ circuit in a graph G is a simple circuit containing every edge of G. (Euler)

(e) (2 points) A simple path in a graph G that passes through every vertex exactly once is called a _______ path, and a simple circuit in a graph G that passes through every vertex exactly once is called a _______ circuit. (Hamilton)

(f) (2 points) A relation R on a set A is called _______ if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$. (transitive)

(g) (2 points) A _______ spanning tree in a connected weighted graph is a spanning tree that has the smallest possible sum of weights of its edges. (minimum)

(h) (2 points) Let G be a simple graph. A _______ tree of G is a subgraph of G that is a tree containing every vertex of G. (spanning)

(i) (2 points) A tree is a connected undirected graph with no _______ circuits. (simple)

(j) (2 points) A _______ tree is a tree in which one vertex has been designated as the root and every edge is directed away from the root. (rooted)

(k) (2 points) The algebraic properties of _______ polynomials can also be used to help solve problems of counting arrangements. (rook)

(l) (2 points) Two $n \times n$ Latin squares $L_1 = (a_{ij})$ and $L_2 = (b_{ij})$ are called _______ if every ordered pair of symbols (k_1, k_2), $1 \leq k_1 \leq n, 1 \leq k_2 \leq n$, occurs among the n^2 ordered pairs (a_{ij}, b_{ij}). (orthogonal)

(m) (2 points) Let $G = (V, E)$ be any bipartite graph with $V = V_1 \cup V_2$. A subset of edges M contained in E is called a _______ matching if every vertex in V is contained in exactly one edge of M. (perfect)

(n) (2 points) The n-tuple _______ number of a graph G, denoted by $\chi_n(G)$, is the minimum number of colors required for an n-tuple coloring of G. (chromatic)

(o) (2 points) Let G be a graph in which there are two designated vertices, one the *source* of all flow, and the other the *sink*, or recipient of all flow. At every other vertex, the amount of flow into the vertex equals the amount of flow out of the vertex. The flows are limited by weights, or _______, on the edges. The edges may be undirected or directed. (capacities)

Questions 2.(k) to 2.(o): 2^{nd} round projects.

3. **Congruence (10 points):** Find x in the following equations:

   (a) (5 points) $24x \equiv 27 \pmod{33}$. ($gcd(24, 33) = 3; x_0 = 8; x = x_0 + k\frac{33}{3} = 8, 19, 30$)

   (b) (5 points) $31x \equiv 1 \pmod{57}$. ($x = 46$)

4. **RSA or Error Correcting Code (10 points):** Select only ONE question to solve

   (a) (10 points) What is the original message encrypted using the RSA system with $p = 7, q = 11$ and $e = 13$ and the codes of the encrypted message is 25 02 08. *Student must use the ASCII tables to look up for ASCII codes and find the characters (See Figure 2).* ($d = 37, m = 539$)

   (b) (10 points) We received data through a transmission line with general error rate is 1 over 5 packages. The received packages are $\{0, 4, 4, 4, 0\}$ and the encryption employs polynomials over $GF(7)$.

      i. Which package has been changed? (Package 3)

ii. What is the corrected value of the error package? ($P(x) = x^2 + x + 5; Q(x) = x^3 + 5x^2 + 2x + 6;$

$$x = \begin{pmatrix} 9/16 \\ -11/16 \\ -3/16 \\ 5/16 \\ 13/16 \end{pmatrix};$$

corrected value is 3.)

5. **Shortest Path Algorithms (10 points):** find the shortest path from A to all other vertices by using

   (a) (5 points) Dijkstra's algorithm in the Figure 1(a)

   (b) (5 points) Bellman-Ford's algorithm in the Figure 1(b).

6. **Search Algorithms (10 points):** Start from vertex A in the Figure 1(c), show visiting process and the final level graph by using

   (a) (5 points) Depth-First-Search (DFS) algorithm with pre-order traversal (root, left, right).

   (b) (5 points) Breadth-First-Search (BFS) algorithm.

7. **Binary Tree Application (10 points):** Given a data source of 8 characters A, B, C, D, E, F with probability of appearance as follows:

A	B	C	D	E	F
0.15	0.24	0.31	0.09	0.10	0.11

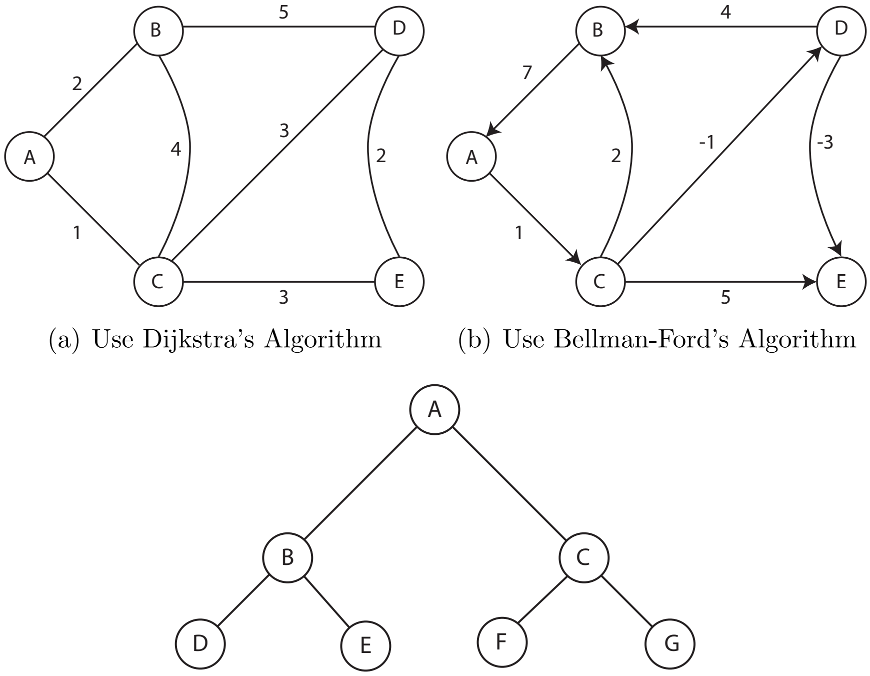
   (a) (5 points) Encode the source and find the codewords for those characters. Draw the Huffman tree.

   (b) (5 points) Calculate the average length of codewords ($\overline{L}$) and the entropy (H) of the source by the following equations

$$\overline{L} = \sum_{i=1}^{m} L_i \times p_i;\ H = \sum_{i=1}^{m} p_i \times \log_2\left(\frac{1}{p_i}\right)$$

   where m is number of different characters, L_i and p_i are length and probability of the ith codeword.

Solution:

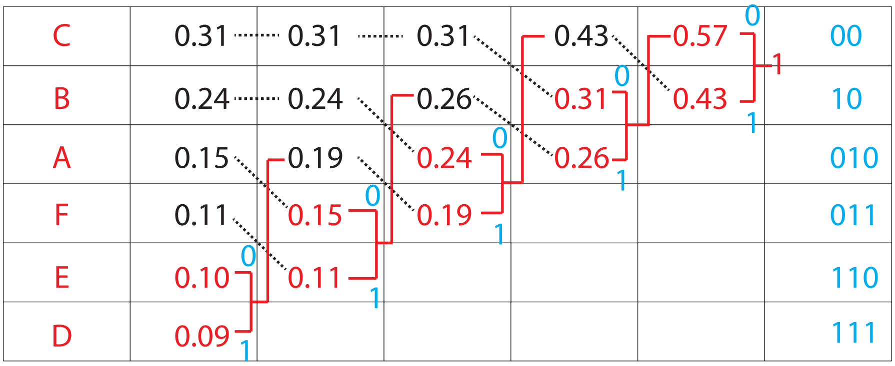


(a) Use Dijkstra's Algorithm (b) Use Bellman-Ford's Algorithm

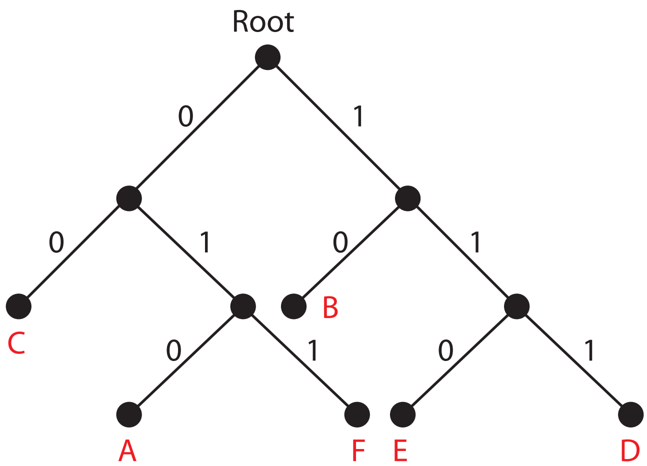
(c) Use DFS & BFS Algorithms

Figure 1: Graphs

$$\begin{aligned}
\overline{L} &= 0.31 \times 2 + 0.24 \times 2 + 0.15 \times 3 + 0.11 \times 3 + 0.1 \times 3 + 0.09 \times 3 = 2.45; \\
H &= 0.31 \times \log_2 \frac{1}{0.31} + 0.24 \times \log_2 \frac{1}{0.24} + 0.15 \times \log_2 \frac{1}{0.15} \\
&\quad + 0.11 \times \log_2 \frac{1}{0.11} + 0.1 \times \log_2 \frac{1}{0.1} + 0.09 \times \log_2 \frac{1}{0.09} = 2.4236.
\end{aligned}$$



(a) Encode



(b) Huffman tree

Figure 2: ASCII Table

Notes:

- Use ASCII Table (Figure 3) for question 4.a
- Use this inverse matrix for question 4.b

$$A^{-1} = \begin{pmatrix} -1/40 & -3/80 & 7/40 & -11/80 & 1/40 \\ -1/8 & 5/16 & -1/8 & -3/16 & 1/8 \\ -1/8 & -3/16 & -1/8 & 5/16 & 1/8 \\ 51/40 & -7/80 & 3/40 & 1/80 & -11/40 \\ -1/8 & 1/16 & 1/8 & 1/16 & -1/8 \end{pmatrix}$$

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(	72	48	H	104	68	h
9	09	Horizontal tab	41	29	)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

(a) Code 0 → 127

Figure 3: ASCII Table