**King Fahd University of Petroleum and Minerals**
College of Computer Sciences and Engineering
Information and Computer Science Department

ICS 254: Discrete Structures II
Spring semester 2015-2016 (152)
Major Exam #2, Wednesday March 30, 2016
Time: **90** Minutes

**Name:** ______________________________________________

**ID#:** ____________________

**Instructions:**
1. The exam consists of 6 pages, including this page, containing 5 questions.
2. Answer all questions. **Show all the steps.**
3. Make sure your answers are **clear** and **readable**.
4. The exam is closed book and closed notes. No calculators or any helping aides are allowed. Make sure you turn off your mobile phone and keep it in your pocket.
5. If there is no space on the front of the page, use the back of the page.

| Question | Maximum Points | Earned Points |
|---|---|---|
| 1 | 30 | |
| 2 | 20 | |
| 3 | 15 | |
| 4 | 15 | |
| 5 | 20 | |
| **Total** | **100** | |

**Q1**: [30 points]

(a) (6 points) Suppose you received these bit strings over a communications link, where the last bit is a parity check bit.

$x = 00000111111$
$y = 10101010101$
$z = 11111100000$
$w = 10111101111$

i. (3 points) Which string are you sure there is an error?

String W = 1011101111

ii. (3 points) Are you sure that the rest of the strings are correct? Justify your answer.

No. If there are exactly 2 errors (2 bits), then the parity check will be correct although the string is not.

(b) (8 points) Encrypt the message TOO EASY using blocks of three letters and the transposition cipher based on the permutation of {1, 2, 3} with $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 2$.

OOT ASE XXY

(c) (10 points) Decrypt the message OAYU EORD NGIG OPOD which is the ciphertext produced by encrypting a plaintext message using the transposition cipher with blocks of four letters and the permutation $\sigma$ of {1, 2, 3, 4} defined by $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, and $\sigma(4) = 2$.

1. Find $\sigma^{-1}$.

4 $\sigma^{-1}(1)=2$ $\sigma^{-1}(2)=4$ $\sigma^{-1}(3)=1$ $\sigma^{-1}(4)=3$

4 YOUA REDO INGG OODP

2 You are doing good.

(d) (6 points) What is the decryption function for an affine cipher if the encryption function is $c = (15p + 13)$ **mod** 26?

$c = 15p + 13 \pmod{26}$

$c - 13 = 15p \pmod{26}$

$\therefore (15)(7) = 1 \pmod{26}$

$\therefore 7c - 13(7) = p \pmod{26}$

$\therefore p = 7c + 13 \pmod{26}$

$26 = 15(1) + 11$
$15 = 11(1) + 4$
$11 = 4(2) + 3$
$4 = 3(1) + 1$

$1 = 4 - 3$
$= 4 - [11 - 2(4)]$
$= 3(4) - 11$
$= 3[15 - 11] - 11$
$= 3(15) - 4(11)$
$= 3(15) - 4(26 - 15)$
$= 7(15) - 4(26)$

$13 \times 7 = 91$

$-91 + 78 = -13 \pmod{x}$
$= 13 \pmod{26}$

**Q2**: [20 points]

(a) (6 points) Consider the relation $R$ on the set of all real numbers where

$(x, y) \in R$ if and only if $x = 2y$.

i. (4 points) Determine whether the relation $R$ is reflexive, irreflexive, symmetric, asymmetric, antisymmetric, and/or transitive.

| | Yes/No | | Yes/No |
|---|---|---|---|
| Reflexive 0.5 | No | Irreflexive | 1 No |
| Symmetric 0.5 | No | Asymmetric | 1 NO |
| Antisymmetric 0.5 | Yes | Transitive | 0.5 NO |

ii. (2 points) Specify the inverse relation $R^{-1}$.

$R^{-1}$ is the relation on the set of all real numbers where $(x, y) \in R^{-1}$ if and only if

$x = \frac{1}{2}y$

(b) (9 points) Let $A = \{a, b, c, d$, e$\}$ and let $R$ be a relation on $A$ defined by

$R = \{(a, c), (b, a), (b, b), (c, a), (c, d), (d, e), (e, e)\}$

i. (5 points) List the ordered pairs of $R \circ R$.

$R \circ R = \{(a,b) \mid \exists c \text{ with } (a,c) \in R \wedge (c,b) \in R\}$

$= \{(a,a), (a,d), (b,c), (b,a), (c,c), (c,e), (d,e), (b,b), (e,e)\}$

ii. (4 points) Find the smallest relation containing $R$ that is both reflexive and symmetric.

$\hat{R} = \{(a,c), (c,a), (b,a), (a,b), (c,d), (d,c), (d,e), (e,d), (a,a), (b,b), (c,c), (d,d), (e,e)\}$

OR

$\hat{R} = R \cup \{(a,a), (c,c), (d,d), (a,b), (d,c), (e,d)\}$

(c) (5 points) Suppose that $R$ is a symmetric relation on a set $A$. Is $\bar{R}$, the complement relation of R, also symmetric? Prove your answer.

Yes. Let $R$ be symmetric. To show that $\bar{R}$ is symmetric. Let $(x,y) \in \bar{R}$. Then, $(y,x)$ has to be in $\bar{R}$. If not, i.e. $(y,x) \notin \bar{R}$. Then $(y,x) \in R$. Since $R$ is symmetric, $(x,y)$ has to belong to $R$. i.e. $(x,y) \notin \bar{R}$ * contradiction*

$\therefore \bar{R}$ is symmetric

**Q3**: [15 points] Consider the relation $R$ on $\mathbf{Z}\times\mathbf{Z}$ defined by

$(a, b)\ R\ (c, d)$ if and only if $a + d = b + c$

(a) (10 points) Prove that $R$ is an equivalence relation.

1. $R$ is reflexive,

$(a,b) R (a,b)$ ? which is obviously true since $\forall (a,b) \in \mathbb{Z}\times\mathbb{Z}$.

$a+b = b+a$.

2. $R$ is symmetric. Let $(a,b) R (c,d)$ where $(a,b), (c,d) \in \mathbb{Z}\times\mathbb{Z}$

Then $a+d = b+c$

~~[illegible]~~ $(c,d) R (a,b)$ iff $\underset{b+c}{\underset{\shortparallel}{c+b}} = \underset{a+d}{\underset{\shortparallel}{d+a}}$ which is true.

3. $R$ is transitive. Let $(a,b) R (c,d)$ & $(c,d) R (x,y)$.

Then $a+d = b+c$ ① & $c+y = d+x$ ... ②

To show $(a,b) R (x,y)$, we must have $a+y = b+x$

from ① & ② $c = a+d-b = d+x-y$, i.e. $a-b = x-y$, i.e. $a+y = x+b$

(b) (5 points) List 5 elements that belong to the equivalence class of Element (0, 0).

$(0,0) R (c,d)$ iff $d=c$

$<(0,0)> \supseteq \{(0,0), (1,1), (2,2), (-1,-1), (-2,-2)\}$

**Q4**: [15 points]

(a) (5 points) Give the matrix representation of a relation $R$ on $A = \{a, b, c, d\}$ such that R is reflexive and transitive, but neither an equivalence relation nor a partial order, using the minimum number of nonzero entries.

$$R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

(b) (10 points) Use Warshall's algorithm to find the matrix representation of the transitive closure of the relation $R = \{(1, 2), (1,3), (1,4), (2,3), (2,4), (3, 4)\}$ on the set $S = \{1, 2, 3, 4\}$

$$R = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$M_{[R_1]} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$M_{[R_2]} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

They are all equal.

$$M_{[R_3]} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$M_{[R_4]} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

**Q5**: [20 points]

(a) **(6 points) Determine whether the following is a poset. If it is a poset, draw its Hasse diagram. Otherwise, explain why it is not a poset.**

**$(\{1, 2, 3, 4\}, R)$ where $R = \{(1, 1), (1, 2), (2, 2), (3, 2), (3, 3), (4, 1), (4, 4)\}$**

$R$ is not transitive since $(4,1)$ & $(1,2) \in R$ but $(4,2) \notin R$.

$\therefore$ $R$ is not a poset.

(b) **(14 points) Consider the set $S = \{2, 3, 5, 10, 11, 15, 25\}$.**

i. **(8 points) Find the partial order (poset) relation R on S based on the "divides" property.**

$R = \{(2,2),(3,3),(5,5),(10,10),(11,11),(15,15),(25,25),$
$(2,10),(3,15),(5,10),(5,15),(5,25)\}$

ii. **(6 points) Draw the Hasse diagram for the poset in (a).**