Philadelphia University Faculty of Engineering Department of Computer Engineering		Second Semester 2017/2018 Date:- 29/05/2018 Allowed time:- 2 Hours

Discrete Mathematics (630260) Final Exam

Student Name: - ……………………………………………….................. ID: - ……………………………

Question 1: **6 points**

A). State the converse, contrapositive, and inverse of the following statements

If n is odd then 1-n is even

Converse: $\rightarrow p$: if 1-n is even then n is odd

Contrapositive: $\neg q \rightarrow \neg p$: if 1-n is odd then n is even

Inverse: $\neg p \rightarrow \neg q$: if n is even then 1-n is odd

B). Show that $\neg(p \oplus q)$ *and* $(p \leftrightarrow q)$ are logically equivalent.

Left side	Right side
$\neg(p \oplus q)$ $\neg((p \wedge \neg q) \vee (\neg p \wedge q))$ $(\neg(p \wedge \neg q) \wedge \neg(\neg p \wedge q))$ $(\neg p \vee q) \wedge (\neg q \vee p)$ $(p \rightarrow q) \wedge (q \rightarrow p)$ $(p \leftrightarrow q)$	$(p \leftrightarrow q)$ $(p \rightarrow q) \wedge (q \rightarrow p)$ $(\neg p \vee q) \wedge (\neg q \vee p)$ $\neg(p \wedge \neg q) \wedge \neg(q \wedge \neg p)$ $\neg((p \wedge \neg q) \vee (q \wedge \neg p))$ $\neg(p \otimes q)$

Question 2: Prove that if n is an integer and $n^3 + 5$ is odd, then n is even using: **6 points**

1- a proof by contrapositive.
The contrapositive statement is " if n is odd then $n^3 + 5$ is even"
$n = 2k + 1$ *where k some integer (becouse n is odd)* Then $n^3 + 5 = (2k + 1)^3 + 5 = 8k^3 + 12k^2 + 6k + 1 + 5 = 8k^3 + 12k^2 + 6k + 6 = 2(4k^3 + 6K^2 + 3k + 3)$ which is even

2- a proof by contradiction.
If $n^3 + 5$ is odd then n is odd. If n is odd then $n = 2k + 1$
Then $n^3 + 5 = (2k + 1)^3 + 5 = 8k^3 + 12k^2 + 6k + 6 = 2(4k^3 + 6K^2 + 3k + 3)$ which is even: which is contradict the premise that $n^3 + 5$ is odd.

Question 3: **8 points**

A). Let A = {1, 2, 3, 4, 5} and B = {0, 3, 6}. Find

a) $A \cup B$. $A \cup B = \{1,2,3,4,5,0,6\}$
b) $A \cap B$. $A \cap B = \{3\}$
c) $A - B$. $A - B = \{1,2,4,5\}$
d) $B - A$. $B - A = \{0,6\}$

B). What can you say about the sets A and B if we know that

a) $A \cup B = A$ (B is a subset of A $B \subseteq A$)
b) $A \cap B = A$ (A is a subset of B $A \subseteq B$)
c) $A - B = A$ ($A \cap B = \phi$)
d) $A - B = B - A$ (A=B)

Question 4: **6 points**

A).Determine whether each of these functions is a bijection from **R** to **R**.

1. $f(x) = -3x + 4$ bijection (one-to-one and onto)
2. $f(x) = -3x^2 + 7$ not bijection (neither one-to-one nor onto)
3. $f(x) = \frac{x+1}{x+2}$ not bijection (onto but not one-to-one)
4. $f(x) = 2x^3 - 5$ bijection (one-to-one and onto)

Question 5: **15 points**

A). Use chines reminder theorem to find the solution of the following system of linear congruence's

$$x \equiv 1 \ (mod\ 2)$$
$$x \equiv 2 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 5)$$
$$x \equiv 4 \ (mod\ 11)$$
$$m = m1 \times m2 \times m3 \times m4 = 2 * 3 * 5 * 11 = 330$$
$$M_1 = \frac{m}{m_1} = \frac{330}{2} = 165 \quad M_2 = \frac{m}{m_2} = \frac{330}{3} = 110 \quad M_3 = \frac{m}{m_3} = \frac{330}{5} = 66 \quad M_4 = \frac{330}{11} = 30$$

Inverse of 165 mod 2	Inverse of 110 mod 3	Inverse of 66 mod 5	Inverse of 30 mod 11
$165 = 82 \times 2 + 1$ $1 = 165 - 82 \times 2$ The inverse is 1	$110 = 36 \times 3 + 2$ $3 = 1 \times 2 + 1$ $1 = 3 - 1 \times 2$ $1 = 3 - 1(110 - 36 \times 3)$ $1 = -1 \times 110 + 37 \times 3$ The inverse is -1 mod 3 or 2	$66 = 13 \times 5 + 1$ $1 = 66 - 13 \times 5$ The inverse is 1	$30 = 2 \times 11 + 8$ $11 = 1 \times 8 + 3$ $8 = 2 \times 3 + 2$ $3 = 1 \times 2 + 1$ $1 = 3 - 1 \times 2$ $1 = 3 - 1 \times (8 - 2 \times 3)$ $1 = -1 \times 8 + 3 \times 3$ $1 = -18 + 3 \times (11 - 1 \times 8)$ $1 = 3 \times 11 - 4 \times 8$ $1 = 3 \times 11 - 4 \times (30 - 2 \times 11)$ $1 = -4 \times 30 + 11 \times 11$ The inverse is -4 mod 11 or 7

$$x = 1 \times 1 \times 165 + 2 \times 2 \times 110 + 1 \times 3 \times 66 + 7 \times 4 \times 30$$
$$x \equiv 1643 \ (mod\ 330)$$
$$x \equiv 323 \ (mod\ 330)$$

Question 6: The following message was encrypted using RSA algorithm with key(n=119,e=77) **20 points**

9172585856

1- Determine the block size.

$25 < 119 < 2525$ the block size is 2

2- Find the primes factorization

$119 = 7 \times 17 \quad p = 7 \quad q = 17$

3- Find the decryption key

The decryption key is inverse of $e\, mod\, (p-1)(q-1)$=inverse of $77 mod\, 96$

$96 = 1 \times 77 + 19$ $77 = 4 \times 19 + 1$ $1 = 77 - 4 \times 19$ $1 = 77 - 4 \times (96 - 1 \times 77)$ $1 = -4 \times 96 + 5 \times 77$	The inverse of $77\, mod\, 96$ is 5 The decryption key $d = 5$

4- Restore the original message.

$$P = C^d mod\, n$$

$P_1 = 91^5 mod\, 119 \quad p_1 = 7$	$p_2 = 72^5 mod\, 119 \quad P_2 = 4$
$P_3 = 58^5\, mod\, 119 \quad P_3 = 11$	$P_4 = 58^5\, mod\, 119 \quad P_4 = 11$
$P_5 = 56^5 mod\, 119 \quad P_5 = 14$	

The original message is **HELLO**

Question 7: **10 points**

A). Use mathematical induction to prove the followings

1. $3^n < n! \quad for\, n > 6$

Basic step: at n=7

$$3^7 = 2187 < 7! = 5040$$

Inductive step: Assume the relation is true at n=k

Then $3^k < k!$ Prove that $3^{k+1} < (k+1)!$

$$3^k < k! \quad then \quad 3 \times 3^k < 3 \times k!$$

$$3^{k+1} < 3 \times k! < (k+1) \times k! \quad since\, 3 < (k+1) \quad then \quad 3^{k+1} < (k+1)!$$

2. $1 \times 1! + 2 \times 2! + 3 \times 3! + \cdots + n \times n! = (n+1)! - 1$

Basic step at n=1

$$1 \times 1! = 2! - 1 \qquad 1 = 1$$

Inductive step: Assume the relation is true at n=k

Then $1 \times 1! + 2 \times 2! + 3 \times 3! + \cdots + k \times k! = (k+1)! - 1$

Prove that $1 \times 1! + 2 \times 2! + 3 \times 3! + \cdots + (k+1) \times (k+1)! = (k+2)! - 1$

$$1 \times 1! + 2 \times 2! + 3 \times 3! + \cdots + k \times k! + (k+1) \times (k+1)! = (k+1)! - 1 + (k+1) \times (k+1)!$$
$$= (k+1)!\left((k+1)+1\right) - 1 = (k+1)! \times (k+2) - 1 = (k+2)! - 1$$

B). Give a recursive definition for $a_n = n^2$ then design a recursive algorithm to find n^2

$$a_0 = 0 \quad a_1 = 1 \quad a_2 = 4 \quad a_3 = 9 \quad a_4 = 16 \qquad a_n = a_{n-1} + (2n-1)$$

```
Fun(n: n is a positive integer)
     If n=0 then return 0
     Else  return Fun(n-1)+2n-1
end
```

Question 8: R1 and R2 are relations defined on set $A = \{1,2,3,4\}$ where

$$R1 = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(3,3),(4,2),(4,3),(4,4)\}$$
$$R2 = \{(1,1),(1,3),(1,4),(2,3),(2,4),(3,3),(3,4),(4,1),(4,2),(4,3)\}$$

10 points

A). Represent these relations using Zero-One Matrix then determine wither these relations are reflexive , symmetric and /or antisymmetric.

$R1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$ R1 is reflexive R1 is not symmetric R1 is not antisymmetric	$R2 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$ R2 is not reflexive R2 is not symmetric R2 is not antisymmetric

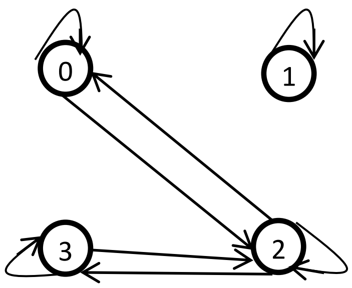
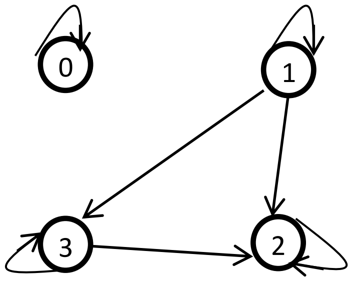
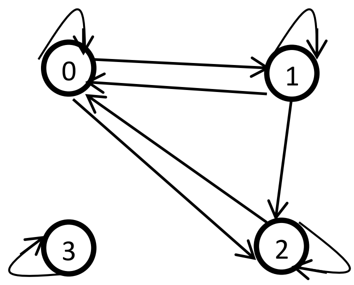
B). Find $1 \cup R2$, $R1 \cap R2$ and $R1 \circ R2$ using Zero-One Matrices.

$R1 \cup R2 = M_{R_1} \vee M_{R_2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$
$R1 \cap R2 = M_{R_1} \wedge M_{R_2} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$
$R1 \circ R2 = M_{R_2} \odot M_{R_1} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$

Question 9: R3,R4 and R5 are relations defined on set $A = \{0,1,2,3\}$ where

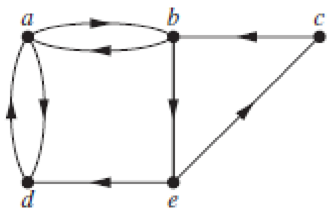
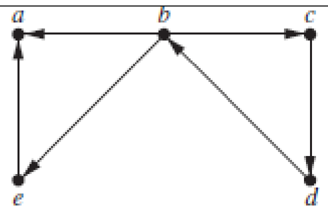
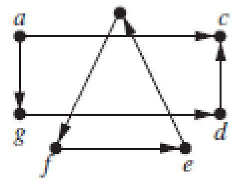
$$R3 = \{(0,0),(0,2),(1,1),(2,0),(2,2),(2,3),(3,2),(3,3)\}$$
$$R4 = \{(0,0),(1,1),(2,2),(3,3),(1,2),(1,3),(3,2)\}$$
$$R5 = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,2),(3,3)\}$$

Represent the relations above using directed graphs, then determine wither the relation are equivalence or partially ordered. **10 points**

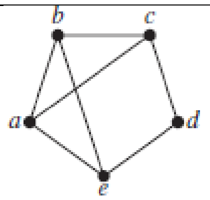
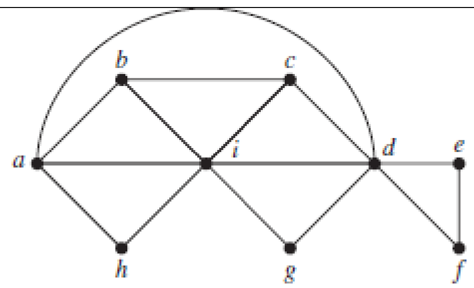
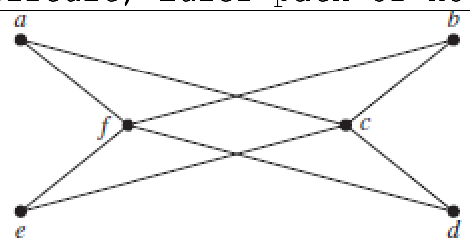
R3	*R4*	*R5*
		
Reflexive Symmetric Transitive Not antisymmetric Then R3 Equivalence	Reflexive Not Symmetric Transitive antisymmetric Then R4 Partialy ordered	Reflexive Not Symmetric Not Transitive Not antisymmetric Then R5 neither equivalence nor partially ordered

Question 10: **9 points**

A). Determine whether each of these graphs is strongly connected and if not, whether it is weakly connected.

		
G1	G2	G3
Strongly Connected	Weakly Connected	Not Connected

B). Determine wither each of the following graphs is bipartite or not then determine wither each one have an Euler circuit, Euler path or not

		
G4	G5	G6
Not Bipartite Have neither Euler path nor Euler circuit	Not Bipartite Have Euler path Don't have Euler circuit	Bipartite Don't have Euler path Have Euler circuit