Philadelphia University Faculty of Engineering Department of Computer Engineering		First Semester 2015/2016 Date:- 02/02/2016 Allowed time:- 2 Hours

Discrete Mathematics (630260) Final Exam

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

Question 1:-Show that the following two statements are logically equivalent 2 points

$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$

Left side		*Right side*
$(\neg p \vee q) \wedge (\neg p \vee r)$ $\neg p \vee (q \wedge r)$ $p \rightarrow (q \wedge r)$	*OR*	$\neg p \vee (q \wedge r)$ $(\neg p \vee q) \wedge (\neg p \vee r)$ $(p \rightarrow q) \wedge (p \rightarrow r)$

Question 2:- Use rules of inference to show that if 4 points

$\forall x(P(x) \vee Q(x))$ and $\forall x(\neg Q(x) \vee S(x))$ and $\forall x(R(x) \rightarrow \neg S(x))$ and $\exists x \neg P(x)$ then $\exists x \neg R(x)$	*Answer* $\forall x(P(x) \vee Q(x)) \equiv \forall x(\neg P(x) \rightarrow Q(x))$ $\forall x(\neg P(x) \rightarrow Q(x))$ $\neg P(a)$ *Existential Instantiation* ——— $Q(a)$ *Modus ponens* $\forall x(\neg Q(x) \vee S(x)) \equiv \forall x(Q(x) \rightarrow S(x))$ $\forall x(Q(x) \rightarrow S(x))$ $Q(a)$ ——— $S(a)$ *Modus ponens* $\forall x(R(x) \rightarrow \neg S(x))$ $S(a)$ ——— $\neg R(a)$ *Modus Tollens* *then* $\exists x \neg R(x)$ *Existential Generralization*

Question 3:- Let $Ai = \{. . . ,-2,-1, 0, 1, . . . , i\}$. Find 2 points

a) $\bigcup_{i=1}^{n} Ai$	**b)** $\bigcap_{i=1}^{n} Ai$
$\bigcup_{i=1}^{n} Ai$ $A1 = \{\dots,-2,-1,0,1\}$ $A2 = \{\dots,-2,-1,0,1,2\}$ $A3 = \{\dots,-2,-1,0,1,2,3\}$ . . . $An = \{\dots,-2,-1,0,1,2,3,\dots,n\}$ $\bigcup_{i=1}^{n} Ai = \{\dots,-2,-1,0,1,2,3,\dots,n\} = An$	$\bigcap_{i=1}^{n} Ai$ $A1 = \{\dots,-2,-1,0,1\}$ $A2 = \{\dots,-2,-1,0,1,2\}$ $A3 = \{\dots,-2,-1,0,1,2,3\}$ . . . $An = \{\dots,-2,-1,0,1,2,3,\dots,n\}$ $\bigcap_{i=1}^{n} Ai = \{\dots,-2,-1,0,1\} = A1$

Question 4:- Let A is a zero-one matrix where 3 points

$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$.

Find

a) $\boldsymbol{A^2}$ **b)** $\boldsymbol{A^3}$ **c)** $\boldsymbol{A \vee A^2 \vee A^3}$

$$\boldsymbol{A^2 = A \odot A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \odot \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}}$$

$$\boldsymbol{A^3 = A^2 \odot A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \odot \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}}$$

$$\boldsymbol{A \vee A^2 \vee A^3 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \vee \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \vee \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}}$$

Question 5:- Prove that if *a* and *b* are positive integers, then *ab* =gcd*(a, b)* . lcm*(a, b).* 3 points

Any integer number can be represented in term of its prime factors

$$a = p1^{n1}p2^{n2}p3^{n3} \ldots..$$
$$b = p1^{m1}p2^{m2}p3^{m3} \ldots..$$
$$ab = p1^{n1+m1}p2^{n2+m3}p3^{n3+m3} \ldots..$$
$$\gcd(a,b) = p1^{\min(n1,m1)}p2^{\min(n2,m2)}p3^{\min(n3,m3)} \ldots..$$
$$\text{lcm}(a,b) = p1^{\max(n1,m1)}p2^{\max(n2,m2)}p3^{\max(n3,m3)} \ldots..$$
$$\gcd(a,b)\,.\,lcm(a,b) = p1^{\min(n1,m1)+\max(n1,m1)}p2^{\min(n2,m2)+\max(n2,m2)}p3^{\min(n3,m3)+\max(n2,m3)} \ldots..$$

If *n1* is the min then *m1* is the max and vice versa so *min(n1,m1)+max(n1,m1)=n1+m1* and the same for *n2,m2* and *n3,m3* and so on then

$$p1^{\min(n1,m1)+\max(n1,m1)}p2^{\min(n2,m2)+\max(n2,m2)}p3^{\min(n3,m3)+\max(n2,m3)} \ldots = p1^{n1+m1}p2^{n2+m3}p3^{n3+m3} \ldots$$

Then *ab* =gcd*(a, b)* . lcm*(a, b)*

Question 6:- Solve each of these congruences 6 points

a) $5x \equiv 43 \ (mod\ 53)$	b) $17x \equiv 10 \ (mod\ 11)$
Find the inverse of *5(mod 53)*	Find the inverse of *17 (mod 11)*
53=10.5+3	*17=1.11+6*
5=1.3+2	*11=1.6+5*
3=1.2+1	*6=1.5+1*
1=3-1.2	*1=6-1.5*
1=3-1.(5-1.3)	*1=6-1(11-1.6)*
1=-1.5+2.3	*1=-1.11+2.6*
1=-1.5+2(53-10.5)	*1=-1.11+2(17-1.11)*
1=2.53-21.5	*1=2.17-3.11*
The inverse is *-21≡32 (mod 53)*	The inverse is *2*
32.5x≡32.43 (mod 53)	*2.17x≡2.10 (mod 11)*
x≡1376 (mod 53)	*x≡20 (mod 11)*
x≡51 (mod 53)	*x≡9 (mod 11)*

Question 7:- Use mathematical induction to prove the followings: 2 points

$3+3.5+3.5^2+\cdots+3.5^n=3\frac{5^{n+1}-1}{4}$ whenever *n* is a positive integer.

Basic step at n=0 $3=3\frac{5^1-1}{4}=3\frac{4}{4}=3$ is true

the formula at *n=k* is $3+3.5+3.5^2+\cdots+3.5^k=3\frac{5^{k+1}-1}{4}$

the formula at *n=k+1* is $3+3.5+3.5^2+\cdots+3.5^{k+1}=3\frac{5^{k+2}-1}{4}$

assume the formula at *n=k* is true then use it to prove the formula at *n=k+1*

$$3+3.5+3.5^2+\cdots+3.5^k+3.5^{k+1}=3\frac{5^{k+1}-1}{4}+3.5^{k+1}$$

$$3+3.5+3.5^2+\cdots+3.5^k+3.5^{k+1}=3(\frac{5^{k+1}-1}{4}+5^{k+1})$$

$$3+3.5+3.5^2+\cdots+3.5^k+3.5^{k+1}=3(\frac{5^{k+1}-1+4.5^{k+1}}{4})$$

$$3+3.5+3.5^2+\cdots+3.5^k+3.5^{k+1}=3(\frac{5^{k+1}-1+(5-1).5^{k+1}}{4})$$

$$3+3.5+3.5^2+\cdots+3.5^k+3.5^{k+1}=3(\frac{5^{k+1}-1+5.5^{k+1}-5^{k+1}}{4})$$

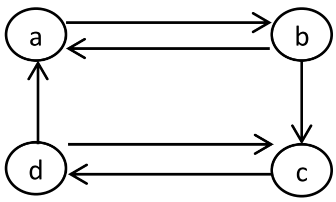
$$3+3.5+3.5^2+\cdots+3.5^k+3.5^{k+1}=3(\frac{5^{k+1}-1+5^{k+2}-5^{k+1}}{4})$$

Then $3+3.5+3.5^2+\cdots+3.5^k+3.5^{k+1}=3(\frac{5^{k+2}-1}{4})$

Question 8:- given the following relation *R* on set *A= {a, b, c, d}*

R={*(b, c), (b, a), (c, d), (d, a), (a, b), (d, c)*} answer the following questions.

a) Represent the relation using directed graph 1 point



b) Represent the relation using Zero-One matrix 1 point

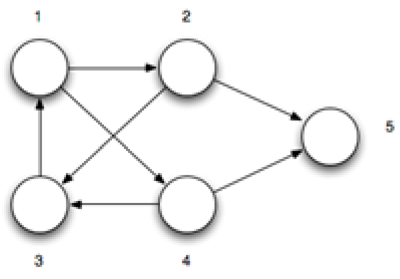
$$\begin{bmatrix}0&1&0&0\\1&0&1&0\\0&0&0&1\\1&0&1&0\end{bmatrix}$$

c) Determine wither the relation *R* is Equivalence, Partial ordering or not. 2 points

Ans: the relation is not reflexive, not symmetric not transitive nor anti-symmetric so the relation is not Equivalence and it is not Partial ordering

---

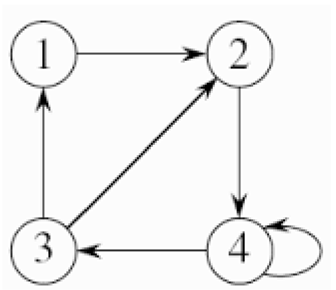
Question 9:- Determine whether each of these graphs is strongly connected and if not, whether it is weakly connected. 3 points



G1

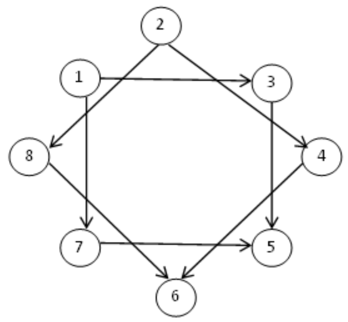
Not strongly connected

It is weakly connected



G2

It is strongly connected

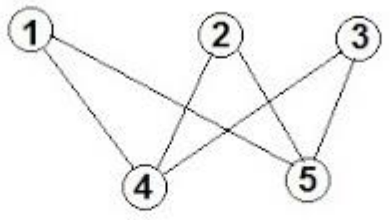


G3

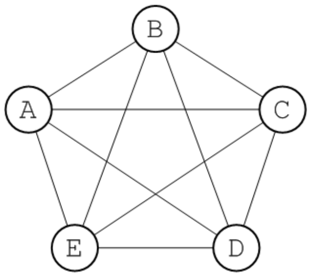
It is not strongly connected

It is not weakly connected

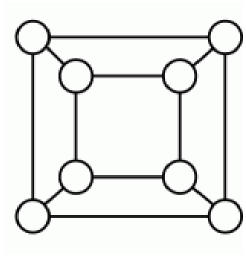
Question 10:- Determine wither each of the following graphs is bipartite or not then determine wither each one have an Euler circuit, Euler path or not. 6 points



G4
It is bipartite graph
It does not have euler circuit
It has euler path



G5
It is not bipartite graph
It has euler circuit



G6
It is bipartite graph
It does not have euler cicuit
It does not have euler path

Question 11: The following cipher text was encrypted using RSA algorithm with public key KEY(e=23,n=55) , break the cipher and restore the original message. 5 points

39182514

n is the product of two primes *p* and *q* which is in this case *p=11* and *q=5 (55=11×5)*
the block size is *2* because *25<55<2525*
the decryption key *d* is the inverse of *e (mod(p-1)(q-1)* (inverse of *23mod(40)*)

40=1.23+17
23=1.17+6
17=2.6+5
6=1.5+1
1=6-1.5
1=6-1(17-2.6)
1=-1.17+3.6
1=-1.17+3(23-1.17)
1=3.23-4.17
1=3.23-4(40-1.23)
1=-4.40+7.23
The inverse is *7 (mod 40)*

The decryption formula is $c^d (mod\ n)$

$$39^7 (mod\ 55) = 19$$
$$18^7 (mod\ 55) = 17$$
$$25^7 (mod\ 55) = 20$$
$$14^7 (mod\ 55) = 4$$

The plain text is

19 17 20 04

Which is

T R U E

Good Luck

Sultan M. Al-Rushdan.