Model Answer

AS - 2221

M.A./M.Sc. (First Semester) Examination - 2013

Mathematics

Discrete Mathematical Structures-I

Sol^n. 1 (a). All the declarative sentences to which it is possible to assign one and only one of the two possible truth values, are called statements.

(b). **Absorption laws.** For any two statement variables P and Q,

$$P \vee (P \wedge Q) \equiv P$$

$$P \wedge (P \vee Q) \equiv P$$

(c). **NAND.** For any two statement variables P and Q, NAND of P and Q is defined by

$$P \uparrow Q \equiv \sim (P \wedge Q)$$

NOR. NOR of P and Q is defined by

$$P \downarrow Q \equiv \sim (P \vee Q)$$

(d). **CP rule.** If we can derive S ~~or~~ from R and a set of premises, then we can derive $R \to S$ from the set of premises alone.

(e). **Quantifier.** Quantifier modifies the predicate by determine whether all or some values of domain satisfy the predicate.

There are two types of quantifiers

(i) Universal quantifier

(ii) Existential quantifier

(f). A lattice is a partially ordered set $(L, \leq)$ in which every pair of elements $a, b \in L$ has a greatest lower bound a least upper bound.

eg. Let S be a set and $P(S)$ be its power set. The partially ordered set $(P(S), \subseteq)$ is a lattice.

(g). Modular inequality. Let $(L, \leq)$ be a lattice. For any $a, b, c \in L$, the following holds:

$$a \leq c \iff a \oplus (b * c) \leq (a \oplus b) * c.$$

(h). Distributive lattice. A lattice $(L, *, \oplus)$ is called a distributive lattice if for any $a, b, c \in L$,

$$a * (b \oplus c) = (a * b) \oplus (a * c)$$

and

$$a \oplus (b * c) = (a \oplus b) * (a \oplus c).$$

eg. every chain is a distributive lattice.

(i). Stone's representation theorem. Any Boolean algebra is isomorphic to a power set algebra $(P(S), \cap, \cup, ', \phi, S)$. for some set S.

(j). A regular grammar contains only productions of the form $\alpha \to \beta$ where $|\alpha| \leq |\beta|$, $\alpha \in V_N$ and β has the form 'aB' or 'a' where $a \in V_T$ and $B \in V_N$.

2(a). Since

$$P \wedge Q \equiv \neg(\neg P \vee \neg Q)$$

$$P \to Q \equiv \neg P \vee Q$$

$$\begin{aligned} P \leftrightarrow Q &\equiv (P \to Q) \wedge (Q \to P) \\ &\equiv \neg(\neg(P \to Q) \vee \neg(Q \to P)) \\ &\equiv \neg(\neg(\neg P \vee Q) \vee \neg(\neg Q \vee P)) \end{aligned}$$

therefore every formula can be expressed in terms of an equivalent formula containing the connectives $\{\neg, \vee\}$. Hence $\{\neg, \vee\}$ is a functionally complete set of connectives.

Again since

$$P \vee Q \equiv \neg(\neg P \wedge \neg Q)$$

$$P \rightarrow Q \equiv \neg P \vee Q$$

$$\equiv \neg(P \wedge \neg Q)$$

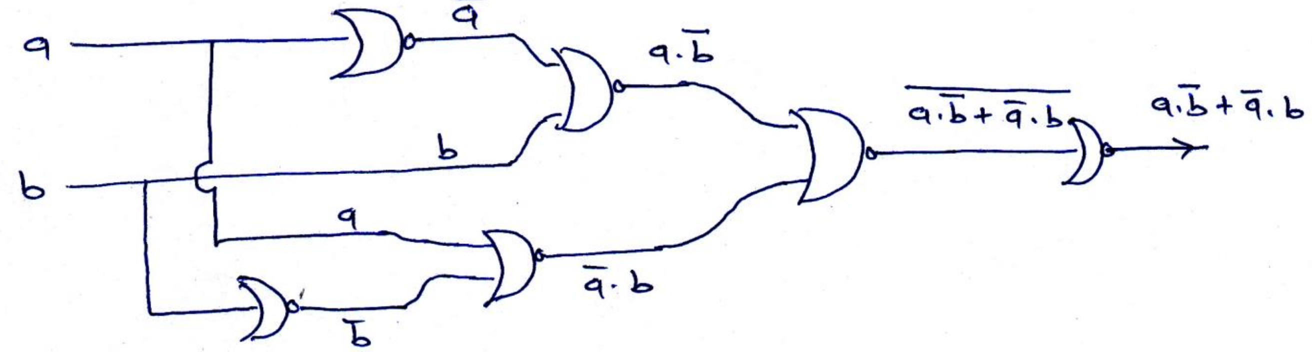
and

$$P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$$

$$\equiv \neg(P \wedge \neg Q) \wedge \neg(Q \wedge \neg P)$$

Hence $\{\neg, \wedge\}$ is a functionally complete set of connectives.

(b).



3(a). Instead of deriving $P \rightarrow S$, we shall include P as an additional premise and show S first:

$\{1\}$	(1)	$\neg P \vee Q$	Rule P
$\{2\}$	(2)	P	Rule P (assumed premise)
$\{1,2\}$	(3)	Q	Rule T, (1), (2), $(A, \neg A \vee B \Rightarrow B)$
$\{3\}$	(4)	$\neg Q \vee R$	Rule P
$\{1,2,3\}$	(5)	R	Rule T, (3), (4), $(A, \neg A \vee B \Rightarrow B)$
$\{4\}$	(6)	$R \rightarrow S$	Rule P
$\{1,2,3,4\}$	(7)	S	Rule T, (5), (6), $(A, A \rightarrow B \Rightarrow B)$
$\{1,3,4\}$	(8)	$P \rightarrow S$	Rule CP

(b).

$\{1\}$	(1)	$P \rightarrow M$	Rule P
$\{2\}$	(2)	$\neg M$	Rule P
$\{1,2\}$	(3)	$\neg P$	Rule T, (1), (2), $(\neg A, B \rightarrow A \Rightarrow \neg B)$
$\{3\}$	(4)	$P \vee Q$	Rule P
$\{1,2,3\}$	(5)	Q	Rule T, (3), (4), $(\neg A, A \vee B \Rightarrow B)$

$\{4\}$	(6)	$Q \to R$	Rule P
$\{1,2,3,4\}$	(7)	R	Rule T, (5), (6), $(A, A \to B \Rightarrow B)$
$\{1,2,3,4\}$	(8)	$R \wedge (P \vee Q)$	Rule T, (4), (7), $(A, B \Rightarrow A \wedge B)$

4(a). Let $(S, *)$ be a finite semigroup and $a \in S$. Consider integer powers of x. Since S is finite, we have

$$a^r = a^s \quad \text{for some } r > s$$

$$a^{s+k} = a^s \quad \text{--- (1)} \quad \text{for } r = s+k, \quad k \in Z^+$$

Now $a^{2s+k} = a^s \cdot a^{s+k}$

$= a^s \cdot a^s = a^{2s}$ using (1)

Similarly $a^{ms+k} = a^{ms}$ --- (2) for every $m \in Z^+$

Again $a^{ms+2k} = a^{ms+k} \cdot a^k$

$= a^{ms} \cdot a^k$ using (2)

$= a^{ms+k}$

$= a^{ms}$ --- (3) using (2)

and $a^{ms+3k} = a^{ms+2k} \cdot a^k$

$= a^{ms} \cdot a^k$ using (3)

$= a^{ms+k}$

$= a^{ms}$ using (2)

Similarly $a^{ms+nk} = a^{ms}$ --- (4) for every $n \in Z^+$

Put $m = k$ and $n = s$ in (4), we get

$$a^{ks+ks} = a^{ks}$$

ie $(a^{ks})^2 = a^{ks}$

Put $x = a^{ks}$ then

$$x^2 = x$$

Hence $x = a^{ks}$ is an idempotent element in finite semigroup $(S, *)$.

(b). Semigroup homomorphism. Let $(S,*)$ and (T,Δ) be any two semigroup. A mapping $g: S \to T$ such that

$$g(a*b) = g(a) \Delta g(b) \qquad \forall a,b \in S,$$

is called a semigroup homomorphism.

Consider $(\mathbb{N}^+, +)$ be the semigroup of natural numbers with zero, and $(S,*)$ be the semigroup on $S = \{e, 0, 1\}$ with the operation $*$ given by

*	e	0	1
e	e	0	1
0	0	0	0
1	1	0	1

A mapping $g: \mathbb{N}^+ \to S$ given by $g(0) = 1$ and $g(j) = 0$ for $j \neq 0$ is a semigroup homomorphism. Although both $(\mathbb{N}^+, +)$ and $(S,*)$ are monoids with identities 0 and e respectively. Since $g(0) \neq e$ therefore g is not a monoid homomorphism.

5(a). Isotonicity property. Let $(L, \leq)$ be a lattice. For any $a,b,c \in L$, the following property is called isotonicity property:

$$b \leq c \implies \begin{cases} a*b \leq a*c \\ a \oplus b \leq a \oplus c \end{cases}$$

Proof. Let $b \leq c$ then $b*c = b$. ---(1)

To show $a*b \leq a*c$, we will show that

$$(a*b)*(a*c) = (a*b).$$

Now, $(a*b)*(a*c) = (a*a)*(b*c)$ by associativity & Commutation

$= a*(b*c)$ idempotent law

$= a*b$ by (1)

Hence $a*b \leq a*c$

Similarly,

Let $b \leq c$ then $b \oplus c = c$ --- (2)

Now $(a \oplus b) \oplus (a \oplus c) = (a \oplus a) \oplus (b \oplus c)$ by associativity & Commutativity

$= a \oplus (b \oplus c)$ idempotent law

$= a \oplus c$ by (2)

Hence $a \oplus b \leq a \oplus c$.

(b). Let $(L, \leq)$ be a chain and $a, b, c \in L$. Consider the following possible cases:

Case 1. $a \leq b$ or $a \leq c$

Case 2. $a \geq b$ and $a \geq c$.

For the case 1,

$$a * (b \oplus c) = a$$

and $(a * b) \oplus (a * c) = a \oplus a = a$

Hence $a * (b \oplus c) = (a * b) \oplus (a * c)$

For the case 2.

$$a * (b \oplus c) = b \oplus c$$

and $(a * b) \oplus (a * c) = b \oplus c$

Hence $a * (b \oplus c) = (a * b) \oplus (a * c)$

Therefore in both cases, the distributive property holds. Hence every chain is a distributive lattice.

6(a). $(a * b) \oplus (b * c) \oplus (c * a) \leq (a \oplus b) * (b \oplus c) * (c \oplus a)$

$$LHS = (a*b) \oplus (b*c) \oplus (c*a)$$

$$= ((a*b) \oplus (b*c)) \oplus (c*a)$$ by associativity

$$\leq \left((a*b) \oplus (b*c) \oplus c\right) * \left((a*b) \oplus (b*c) \oplus a\right)$$ distributive inequality

$$= ((a*b) \oplus c) * (a \oplus (b*c))$$ idempotent law

$$\leq ((a \oplus c) * (b \oplus c)) * ((a \oplus b) * (a \oplus c))$$ distributive inequality

$$= (a \oplus b) * (b \oplus c) * (c*a)$$ idempotent law

$$= RHS$$

Hence $(a*b) \oplus (b*c) \oplus (c*a) \leq (a \oplus b) * (b \oplus c) * (c*a)$

(b). $(a*b) \oplus (c*d) \leq (a \oplus c) * (b \oplus d)$

since $a*b \leq a \leq a \oplus c$ --- (1)

and $a*b \leq b \leq b \oplus d$ --- (2)

From (1) & (2)

$a*b \leq (a \oplus c) * (b \oplus d)$ --- (3)

Again $c*d \leq c \leq a \oplus c$ --- (4)

and $c*d \leq d \leq b \oplus d$ --- (5)

From (4) & (5)

$c*d \leq (a \oplus c) * (b \oplus d)$ --- (6)

From (3) & (6), we get

$(a*b) \oplus (c*d) \leq (a \oplus c) * (b \oplus d)$

7(a). $x_1 \oplus (x_2 \oplus x_3')$

$$= (x_1 * 1) \oplus (x_2 * 1) \oplus (x_3' * 1)$$ as $a*1 = a$

$$= (x_1 * (x_2 \oplus x_2')) \oplus (x_2 * (x_1 \oplus x_1')) \oplus (x_3' * (x_1 \oplus x_1'))$$ as $a \oplus a' = 1$

$$= x_1 x_2 + x_1 x_2' + x_2 x_1 + x_2 x_1' + x_3' x_1 + x_3' x_1'$$

$$= x_1 x_2 + x_1 x_2' + x_1' x_2 + x_1 x_3' + x_1' x_3'$$ as $a + a = a$

$$= x_1 x_2 (x_3 + x_3') + x_1 x_2' (x_3 + x_3') + x_1' x_2 (x_3 + x_3') + x_1 x_3' (x_2 + x_2') + x_1' x_3' (x_2 + x_2')$$

$= x_1 x_2 x_3 + x_1 x_2 x_3' + x_1 x_2' x_3 + x_1 x_2' x_3' + x_1' x_2 x_3 + x_1' x_2 x_3'$

$+ x_1 x_3' x_2 + x_1 x_3' x_2' + x_1' x_3' x_2 + x_1' x_3' x_2'$ (distributive law)

$= x_1 x_2 x_3 + x_1 x_2 x_3' + x_1 x_2' x_3 + x_1 x_2' x_3' + x_1' x_2 x_3 + x_1' x_2 x_3' + x_1' x_2' x_3'$

(idempotent law)

$= \oplus\ m_0, m_2, m_3, m_4, m_5, m_6, m_7$

This is sum of product canonical form.

Also $x_1 \oplus (x_2 \oplus x_3')$

$= (x_1 \oplus x_2 \oplus x_3')$

$= *\ M_1$

This is product of sum canonical form,

(b). $(x_1 \oplus x_2)' \oplus (x_1' \oplus x_3)$

as $(a \oplus b)' = a' * b'$

$= (x_1' * x_2') \oplus (x_1' \oplus x_3)$

$= x_1' x_2' + x_1' + x_3$

$= x_1' x_2' (x_3 + x_3') + x_1' (x_2 + x_2')(x_3 + x_3') + x_3 (x_1 + x_1')(x_2 + x_2')$

$= x_1' x_2' x_3 + x_1' x_2' x_3' + x_1' x_2 x_3 + x_1' x_2 x_3' + x_1' x_2' x_3 + x_1' x_2' x_3'$

$+ x_1 x_2 x_3 + x_1 x_2' x_3 + x_1' x_2 x_3 + x_1' x_2' x_3$ (distributive law)

$= x_1' x_2' x_3 + x_1' x_2' x_3' + x_1' x_2 x_3 + x_1' x_2 x_3' + x_1 x_2 x_3 + x_1 x_2' x_3$

$= \oplus\ m_0, m_1, m_2, m_3, m_5, m_7$

This is sum of product canonical form.

Also $(x_1 \oplus x_2)' \oplus (x_1' \oplus x_3)$

$= (x_1' * x_2') \oplus (x_1' \oplus x_3)$ as $(a \oplus b)' = a' * b'$

$= (x_1' \oplus x_1' \oplus x_3) * (x_2' \oplus x_1' \oplus x_3)$ distributive law

$= (x_1' \oplus x_3) * (x_1' \oplus x_2' \oplus x_3)$ idempotent law

$= (x_1' \oplus x_2 x_2' \oplus x_3) * (x_1' \oplus x_2' \oplus x_3)$ as $aa' = 0$ & $a \oplus 0 = a$

$= ((x_1' \oplus x_3) \oplus (x_2 * x_2')) * (x_1' \oplus x_2' \oplus x_3)$ associative law

$= (x_1' \oplus x_3' \oplus x_2) * (x_1' \oplus x_3' \oplus x_2') * (x_1' \oplus x_2' \oplus x_3)$ distributive law

$= (x_1' \oplus x_2 \oplus x_3) * (x_1' \oplus x_2' \oplus x_3)$ idempotent law

$= * \ M_4, M_6$

This is product of sum canonical form.

Q. Let $G = \{V_N, V_T, S, \Phi\}$ be a grammar for the language $L = \{a^x b^y \mid x > y > 0\}$ where

$V_N = \{S, A\}$ is the set of non-terminals

$V_T = \{a, b\}$ is the set of terminals

S is the starting element

and Φ is the set of production consists of

$S \to aS$, $S \to aA$, $A \to aAb$, $A \to ab$

Since $a^x b^y = a^{x-y} a^y b^y$, we can use the productions $A \to aAb$ and $A \to ab$ to generate $a^y b^y$. And we use the productions $S \to aS$ and $S \to aA$ to generate a^{x-y}.

Now, $S \Rightarrow a^{x-y-1} S$ using $S \to aS$, $x-y-1$ times

$\Rightarrow a^{x-y-1} aA$ using $S \to aA$ once

$\Rightarrow a^{x-y} . a^{y-1} A b^{y-1}$ using $A \to aAb$, $y-1$ times

$\Rightarrow a^{x-y} a^{y-1} . a b . b^{y-1}$ using $A \to ab$ once

Hence $L(G) = \{a^x b^y \mid x > y > 0\}$.

R. Gupta