Discrete Mathematics Recitation Class

Tianyu Qiu

University of Michigan - Shanghai Jiaotong University

Joint Institute

Summer Term 2019

Contents

Relations

Definitions (P70)

1. *relation*: set that only contains ordered pairs
2. *domain*
3. *range*
4. *field*: $ranR \cup domR$
5. *a relation on set M*

e.g. (P71)

- $R = \emptyset$ is a relation with $domR = \emptyset$ and $ranR = \emptyset$.
- If A, B are sets, then $R = A \times B$ is a relation with $domR = A$ and $ranR = B$.
- $R = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a, b$ are both even or both odd$\}$ is a relation with $domR = ranR = \mathbb{N}$. This relation is equivalence $(\bmod 2)$.

Properties of Relations (P72)

Definitions(easy but also easy to be mistaken)

1. *reflexive*
2. *symmetric*
3. *antisymmetric*
4. *asymmetric*
5. *transitive*

The antecedents for these properties are usually strict, so it is not difficult for a relation to obtain these properties (recall the truth table of implication).

Properties for Relations (P73)

e.g.

- $R = \emptyset$ on $\emptyset$ is reflexive, symmetric, antisymmetric, asymmetric and transitive. If $M \neq \emptyset$, then R is symmetric, antisymmetric, asymmetric and transitive.
- $R = \{(1,2),(3,4)\}$ is antisymmetric, asymmetric and transitive.

Equivalence Relations (P74)

Definitions

1. *equivalence relation*: a relation R on M that is reflexive, symmetric and transitive.
2. *equivalence class of* $a \in M$: $[a]_R = \{b \in M | (a, b) \in R\}$

If R is a relation on a set M, then for all $a, b \in M$,

$$\text{either } [a]_R \cap [b]_R = \emptyset \text{ or } [a]_R = [b]_R$$

i.e. equivalence classes partition the set M.

Equivalence Relations (P75-P76)

e.g.

- $R = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a, b$ are both even or both odd$\}$ is an equivalence relation on $\mathbb{N}$ and the equivalence classes partition $\mathbb{N}$ into two sets:

$$[0]_R = \{n \in \mathbb{N} \mid n \text{ is even}\}\text{and } [1]_R = \{n \in \mathbb{N} \mid n \text{ is odd}\}$$

- For $n \in \mathbb{N}, I(n) :=$ sum of all digits of n.

$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N} | I(a) = I(b)\}$$

is an equivalence relation on $\mathbb{N}$ and the equivalence classes partition $\mathbb{N}$ into infinitely many sets:

$$[1]_R = \{n \in \mathbb{N} | I(n) = 1\}$$
$$[11]_R = \{n \in \mathbb{N} | I(n) = 2\}$$
$$[111]_R = \{n \in \mathbb{N} | I(n) = 3\}$$
$$\vdots$$

Orders

Definitions

For relation R on set M

1. *partial order*: reflexive, antisymmetric and transitive (P77)
2. *strict partial order*: asymmetric and transitive (P77)
3. *(strict) linear/total order*: a (strict) partial order satisfying that $\forall x, y \in M,\ (x, y) \in R$ or $(y, x) \in R$ (P78)
4. *(strict) well-order*: a (strict) linear order satisfying that for all non-empty $A \subseteq M,\ \exists x \forall y \in A$, if$(y, x) \in R$ then $y = x$.
   i.e. There exists an element that can only appear as the first element in all ordered pairs (except that it is related to itself) (P79)
5. *maximal/greatest element & minimal/least element* (P80)

A linear order on a finite set is a well-order.

Least elements and greatest elements of a partial order are unique.

Lattices

Definitions

1. *upper/lower bound* (P82)
2. *least upper bound(l.u.b.) & greatest lower bound(g.l.b.)* (P82)
3. *lattice*: any two-element subset has its g.l.b. and l.u.b. (P83)

e.g. (P83-P84)

- The poset $(\mathbb{N} \setminus \{0\}, |)$ is a lattice. If $x, y \in \mathbb{N} \setminus \{0\}$ then $x \vee y$ is $lcm(x, y)$ and $x \wedge y$ is $gcd(x, y)$.
- If $A = \{1, 2, 3, 4\}$ and $R = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,4), (3,4), (1,4)\}$, then (A, R) is not a lattice because $\{2, 3\}$ has no lower bound.
- If A is a set, then $(\mathcal{P}(A), \subseteq)$ is a poset. Moreover, $(\mathcal{P}(A), \subseteq)$ is a lattice. If $x, y \in \mathcal{P}(A)$, then

$$x \vee y = x \cup y, \ x \wedge y = x \cap y$$

Complete Lattices (P85)

Definition

complete lattice: any subset has its g.l.b. and l.u.b.

- A non-empty finite lattice is a complete lattice.
- Complete lattice $(L, \preceq)$ has a maximal element $\bigvee L$ and a minimal element $\bigwedge L$.

e.g.

- If A is any set, then $(\mathcal{P}(A), \subseteq)$ is a complete lattice. If $X \subseteq P(A)$, then

$$\bigvee X = \bigcup X, \; \bigwedge X = \bigcap X$$

- Lattice $(\mathbb{Q}, \leqslant)$ is not complete since $\{x \in \mathbb{Q} | x^2 \leqslant 2\}$ has no l.u.b.
- Is the lattice $(\mathbb{R}, \leqslant)$ complete? No.

Chain Complete Posets (P87)

Definitions

1. *chain*: A subset of a partial order that is a linear order.
2. *chain complete*: A partial order any of whose subsets that is a chain has l.u.b.

Key Points

- Chain points to the subset while chain complete points to the universal set.
- The definition of chain complete ensures the existence of a unique least element.
- Subsets of a linear order are linear orders (i.e. chains).
- Every complete lattice is a chain complete poset.

Functions

Definitions

1. *function* (P89)
   - relation
   - uniqueness
2. $f''C = \{y | \exists x (x \in C \wedge (x, y) \in f)\} \subseteq ran f \subseteq B$ (P90)
3. $f \upharpoonright C = \{(x, y) | \exists x (x \in C \wedge (x, y) \in f)\} \subseteq f$ (P90)
4. *injective functions* (P90)
5. *composing functions* (P91)
6. *inverses* (P93)
7. *identity function* (P94)
8. *surjective functions* (P95)
9. *bijection*: both injective and surjective (P95)

Inverse Functions & Identity Functions (P94)

Lemma

Let $f : A \to B$ be a function. The relation f^{-1} is a function with $\mathrm{dom} f^{-1} = \mathrm{ran} f$ and $\mathrm{ran} f^{-1} = A$ if and only if f is injective. Moreover, f^{-1} is injective and $f \circ f^{-1} = f^{-1} \circ f = id_A$

Proof.

Suppose $f : A \to B,\ w, x \in A;\ y, z \in B$

1. Given that f^{-1} is a function, then (according to the definition of function) for all $y \in B$ and for all $w, x \in A$ if $(y, x) \in f^{-1}$ and $(y, w) \in f^{-1}$, then $w = x$. This is also the definition of injection for f.
2. Given that f is injective, conversely we can have f^{-1} is a function as well as f^{-1} is injective.
3. For all $a \in A,\ b \in B$, if $(a, b) \in f$, then $(b, a) \in f^{-1}$, $f^{-1}(f(a)) = f^{-1}(b) = a,\ f(f^{-1}(b)) = f^{-1}(a) = b$

Problems in Assignment 1

Q4. Suppose that a truth table in n propositional variables is specified. Show that a compound proposition with this truth table can be formed by taking the disjunction of conjunctions of the variables or their negations, with one conjunction for each combination of values for which the compound proposition is true. The resulting compound proposition is said to be in *disjunctive normal form*.

Problems in Assignment 1

Corresponding Knowledge

- *simple disjunctive/conjunctive form*
- *disjunctive/conjunctive normal form*
- *major disjunctive/conjunctive normal form*

Theorem

Any compound proposition that is not a contradiction can be expressed by a unique major disjunctive normal form.

Proof.

- Existence
- Uniqueness (proof by contradiction)

□

What about a compound proposition that is contradiction?

Problems in Assignment 1

Q6. Let M be a set and let $X, Y, Z \subseteq M$. We define the *symmetric difference*:

$$X \triangle Y := (X \cup Y) \setminus (X \cap Y)$$

(iii) Show that the *symmetric difference* is associative, i.e.

$$(X \triangle Y) \triangle Z = X \triangle (Y \triangle Z)$$

(iv) Prove that $X \cap (Y \triangle Z) = (X \cap Y) \triangle (X \cap Z)$.

Problems in Assignment 1

Solution.

$\triangle$ is commutative. (why?) Thus the problem turns out to prove

$$Z\triangle(X\triangle Y)=X\triangle(Y\triangle Z)$$

$$\begin{aligned}
&Z\triangle(X\triangle Y)=[Z\cup(X\triangle Y)]\cap[Z\cap(X\triangle Y)]^c\\
&=[Z\cup(X\triangle Y)]\cap[Z^c\cup(X\triangle Y)^c]=[Z\cap(X\triangle Y)^c]\cup[Z^c\cap(X\triangle Y)]\\
&=\{Z\cap[(X\cup Y)\cap(X\cap Y)^c]^c\}\cup[Z^c\cap(X\cup Y)\cap(X\cap Y)^c]\\
&=\{Z\cap[(X\cup Y)^c\cup(X^c\cup Y^c)^c]\}\cup[Z^c\cap(X\cup Y)\cap(X^c\cup Y^c)]\\
&=\{Z\cap(X^c\cap Y^c)\cup(X\cap Y)\}\cup\{Z^c\cap[(X\cap Y^c)\cup(X^c\cap Y)]\}\\
&=(X\cap Y\cap Z)\cup(X^c\cap Y\cap Z)\cup(X\cap Y^c\cap Z)\cup(X\cap Y\cap Z^c)
\end{aligned}$$

Since the form is symmetric, we immediately obtain

$$(X\triangle Y)\triangle Z=Z\triangle(X\triangle Y)=X\triangle(Y\triangle Z)$$

Problems in Assignment 1

Solution(continued).

$$
\begin{aligned}
& (X \cap Y) \triangle (X \cap Z) \\
= & [(X \cap Y) \setminus (X \cap Z)] \cup [(X \cap Z) \setminus (X \cap Y)] \\
= & [(X \cap Y) \cap (X \cap Z)^c] \cup [(X \cap Z) \cap (X \cap Y)^c] \\
= & [(X \cap Y) \cap (X^c \cup Z^c)] \cup [(X \cap Z) \cap (X^c \cup Y^c)] \\
= & (X \cap Y \cap Z^c) \cup (X \cap Z \cap Y^c) \\
= & X \cap (Y \setminus Z) \cup X \cap (Z \setminus Y) \\
= & X \cap (Y \setminus Z \cup Z \setminus Y) = X \cap (Y \triangle Z)
\end{aligned}
$$

Useful Equivalence

$$(X \cup Y) \cap (X^c \cup Y^c) \equiv (X \cap Y^c) \cup (X^c \cap Y)$$

Problems in Assignment 1

Q8. Show that

$$(\exists x P(x) \Rightarrow Q(x)) \Longleftrightarrow ((\forall x P(x)) \Rightarrow (\exists x Q(x)))$$

is a tautology.

Problems in Assignment 1

Solution.

Recall the following tautology of contraposition:

Suppose A, B are propositions, then $(A \Leftrightarrow B) \equiv (\neg A \Leftrightarrow \neg B)$.

Thus we are going to prove

$$\neg(\exists x P(x) \Rightarrow Q(x)) \equiv \neg((\forall x P(x)) \Rightarrow (\exists x Q(x)))$$

$$\begin{aligned}
LHS &\equiv \forall x(\neg(P(x) \Rightarrow Q(x))) \\
&\equiv \forall x(\neg(\neg P(x) \vee Q(x))) \\
&\equiv \forall x(P(x) \wedge \neg Q(x)) \\
RHS &\equiv \neg(\neg(\forall x P(x))) \vee (\exists x Q(x)) \\
&\equiv (\forall x P(x)) \wedge (\forall x(\neg Q(x))) \\
&\equiv \forall x(P(x) \wedge \neg Q(x)) \\
&\equiv LHS
\end{aligned}$$

Problems in Assignment 1

Q10. In computer design, the logical operations NAND and NOR play an important role. In logic, NAND is represented by the *Scheffer stroke* $|$ while NOR is represented by the *Peirce arrow* $\downarrow$. They are defined as

$$A \mid B :\equiv \neg(A \wedge B) \text{ and } A \downarrow B :\equiv \neg(A \vee B)$$

(ii) Show that every connective of propositional logic can be defined using only the connective $|$.
(iii) Show that every connective of propositional logic can be defined using only the connective $\downarrow$.

Problems in Assignment 1

Solution.

The tricky point is to apply de Morgan Rules.

$$
\begin{aligned}
\neg A &\equiv \neg(A \wedge A) \equiv A|A \\
A \wedge B &\equiv \neg(A|B) \equiv (A|B)|(A|B) \\
A \vee B &\equiv \neg(\neg A \wedge \neg B) \equiv (\neg A)|(\neg B) \equiv (A|A)|(B|B) \\
A \Rightarrow B &\equiv \neg A \vee B \equiv \neg(A \wedge \neg B) \equiv A|(B|B) \\
A \Leftrightarrow B &\equiv (A \vee \neg B) \wedge (B \vee \neg A) \equiv (A \wedge B) \vee (\neg A \wedge \neg B) \\
&\equiv \neg(\neg(A \wedge B) \wedge \neg(\neg A \wedge \neg B)) \\
&\equiv \neg(\neg(A \wedge B) \wedge (A \vee B)) \\
&\equiv (A|B)|((A|A)|(B|B))
\end{aligned}
$$

Think a little bit further

- $|$ is commutative but not associative. (why?)
- $(A|A)|(A|A) \equiv A$ and $A|A|A|A \equiv \neg A$. (why?)

Problems in Assignment 1

Solution(continued).

$$
\begin{aligned}
\neg A &\equiv \neg(A \vee A) \equiv A \downarrow A \\
A \vee B &\equiv \neg(A \downarrow B) \equiv (A \downarrow B) \downarrow (A \downarrow B) \\
A \wedge B &\equiv \neg(\neg A \vee \neg B) \equiv \neg A \downarrow \neg B \equiv (A \downarrow A) \downarrow (B \downarrow B) \\
A \Rightarrow B &\equiv \neg A \vee B \equiv ((A \downarrow A) \downarrow B) \downarrow ((A \downarrow A) \downarrow B) \\
A \Leftrightarrow B &\equiv (A \vee \neg B) \wedge (B \vee \neg A) \equiv \neg(\neg(A \vee \neg B) \vee \neg(B \vee \neg A)) \\
&\equiv (\neg(B \vee \neg A)) \downarrow (\neg(A \vee \neg B)) \equiv (B \downarrow (\neg A)) \downarrow (A \downarrow \neg B) \\
&\equiv (B \downarrow (A \downarrow A)) \downarrow (A \downarrow (B \downarrow B))
\end{aligned}
$$

Think a little bit further

- $\downarrow$ is commutative but not associative. (why?)
- $(A \downarrow A) \downarrow (A \downarrow A) \equiv A$ and $A \downarrow A \downarrow A \downarrow A \equiv \neg A$. (why?)

Problems in Assignment 1

Relationship between Sets & Predicates

Suppose $A(x), B(x)$ are predicates, $A = \{x|A(x) \text{ (is true)}\}$, $B = \{x|B(x) \text{ (is true)}\}$ are sets. $A, B \subseteq M$, which is the domain of discourse. Then we have the following relationships:

- $A \cap B$: a set in which all elements makes both $A(x)$ and $B(x)$ true: $A(x) \wedge B(x)$.
- $A \cup B$: a set in which all elements makes either $A(x)$ or $B(x)$ true: $A(x) \wedge B(x)$.
- $A \setminus B (A \cap B^c)$: a set in which all elements makes $A(x)$ true and makes $B(x)$ false: $A(x) \wedge \neg B(x)$
- $A \subseteq B$: Any element in A (that makes $A(x)$ true) is in B (makes $B(x)$ true): $A(x) \Rightarrow B(x)$.
- $A = B$: Any element in A is in B, any element not in A is not in B: $A(x) \Leftrightarrow B(x)$.