DEPARTMENT OF MATHEMATICS

Math2033 TA note 2

Yang Yunfei, Chen Yipei, Liu Ping

February 19, 2019

1 LOGIC

Direct proof: Assume p and show q.
Proof by contrapositive: Assume $\sim q$ and show $\sim p$.
(This corresponds to the equivalence $p \Rightarrow q \equiv \sim q \Rightarrow \sim p$)
Proof by contradiction: First assuming that the opposite proposition is true, and then shows that such an assumption leads to a contradiction. For a conditional statement, assume p and $\sim q$ and derive a contradiction.
(This corresponds to the equivalences

$$p \Rightarrow q \equiv \sim\sim (p \Rightarrow q) \equiv \sim (p \Rightarrow q) \Rightarrow \bot \equiv (p \ and \sim q) \Rightarrow \bot,$$

where $\bot$ is the logical contradiction, or *false* value.).

Example 1. *Suppose $a \in \mathbb{Z}$. If a^2 is even, then a is even.*

Proof. For the sake of contradiction, suppose a^2 is even *and* a is not even. Then a^2 is even, and a is odd.
Since a is odd, there is an integer c for which $a = 2c + 1$. Then

$$a^2 = (2c+1)^2 = 4c^2 + 4c + 1 = 2(2c^2 + 2c) + 1,$$

so a^2 is odd.
Thus a^2 is even and a^2 is not even, a contradiction.
(And since we have arrived at a contradiction, our original supposition that a^2 is even and a is odd could not be true.) $\square$

Reference material could be find in http://cgm.cs.mcgill.ca/ godfried/teaching/dm-reading-assignments/Contradiction-Proofs.pdf

2 BASICS OF SET THEORY

Definition 2. *For sets $A_1, A_2, \ldots, A_n$,*
(i) their union *is*

$$\bigcup_{k=1}^{n} A_k = A_1 \cup A_2 \cup \cdots \cup A_n = \{x : x \in A_1 \ or \ x \in A_2 \ or \ \cdots \ or \ x \in A_n\},$$

(ii) their intersection *is*

$$\bigcap_{k=1}^{n} A_k = A_1 \cap A_2 \cap \cdots \cap A_n = \{x : x \in A_1 \ and \ x \in A_2 \ and \ \cdots \ and \ x \in A_n\},$$

(iii) their Cartesian product *is*

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) : x \in A_1 \ and \ x \in A_2 \ and \ \cdots \ and \ x \in A_n\},$$

(iv) the complement *of A_2 in A_1 is*

$$A_1 \setminus A_2 = \{x : x \in A_1 \ and \ x \notin A_2\}$$

.

Notation: The notation $A_1 \cup A_2 \cup A_3 \cup \cdots$ may be abbreviated as $\bigcup\limits_{k=1}^{\infty} A_k$ or $\bigcup\limits_{k\in\mathbb{N}} A_k$. If for every $x \in S$, there is a set A_x, then the union of all the sets A_x's for all $x \in S$ is denoted by $\bigcup\limits_{x\in S} A_x$. Similar abbreviations exit for intersection and Cartesian product.

Example 3. $\bigcap\limits_{n\in\mathbb{N}} [0, 1 + \frac{1}{n}) = [0, 2) \cap [0, \frac{3}{2}) \cap [0, \frac{4}{3}) \cap [0, \frac{5}{4}) \cap \cdots = [0, 1]$.

Proof. Denoted $A_n = [0, 1 + \frac{1}{n}), A = \bigcap\limits_{n\in\mathbb{N}} A_n, B = [0, 1]$.
To show $A = B$, we need to show $A \subseteq B$ and $A \supseteq B$.
Step 1, to show $A \subseteq B$, by definition of subset, we only need to show if $x \in A$, then $x \in B$.
Further, we only need to show its contrapositive statement, if $x \notin B$, then $x \notin A$.
For $x < 0$, it is clear that $x \notin A_n$ and hence $x \notin A$.
For $x > 1$, there $\exists n \in \mathbb{N}$ such that $1 + \frac{1}{n} < x$ and hence $x \notin A_n \Rightarrow x \notin A = \bigcap\limits_{n\in\mathbb{N}} A_n$.
Step 2, it is simpler to show $A \supseteq B$.
Since $A_n \supseteq B$ and $A = \bigcap\limits_{n\in\mathbb{N}} A_n$, we can conclude that $A \supseteq B$.
Therefore, we show that $\bigcap\limits_{n\in\mathbb{N}} [0, 1 + \frac{1}{n}) = A = B = [0, 1]$. □

Example 4. *For all sets A, B, C, it is always true that $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$?*

Proof. LHS $= A \setminus (B \cup C) = \{x : x \in A \ and \ x \notin (B \cup C)\}$ (Definition of complement)
Since $x \in A \ and \ x \notin (B \cup C)$
$\Leftrightarrow x \in A \ and \ \sim (x \in (B \cup C))$ (Negation of statement)
$\Leftrightarrow x \in A \ and \ \sim (x \in B \ or \ x \in C))$ (Definition of union)
$\Leftrightarrow x \in A \ and(\ x \notin B \ and \ x \notin C))$ (Negation of statement)
$\Leftrightarrow (x \in A \ and \ x \notin B) \ and \ (x \in A \ and \ x \notin C))$
$\Leftrightarrow x \in (A \setminus B) \ and \ x \in (A \setminus C)$ (Definition of complement)
$\Leftrightarrow x \in (A \setminus B) \cap (A \setminus C)$ (Definition of intersection)
Therefore, LHS= $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ =RHS □

3 Function

3.1 Function composition

Given two functions $f : A \to B$, $g : B \to C$, the composition of g by f is

$$g \circ f : A \to C \qquad g \circ f(x) = g(f(x)) \text{ for any } x \in A.$$

Note that for any $x \in A$, we have $f(x) \in B$, therefore $g(f(x)) \in C$ and $g \circ f$ is well-defined.

Example: If $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = 2x + 4$ and $g : \mathbb{R} \to \mathbb{R}$ is given by $g(x) = x^2$. Then

$$g \circ f(x) = g(f(x)) = g(2x+4) = (2x+4)^2,$$

$$f \circ g(x) = f(g(x)) = f(x^2) = 2x^2 + 4.$$

3.2 Bijection:

Let $f : A \to B$ be a function,

(1) f is surjective iff $f(A) = B$.

(2) f is injective iff $f(x) = f(y)$ implies $x = y$.

(3) f is bijective iff f is injective and surjective.

(4) If f is injective, define $f^{-1} : f(A) \to A$ by $f^{-1}(f(x)) = x$. f^{-1} is called the inverse of f. f^{-1} is well-defined because for any $y \in f(A)$ there exists only one $x \in A$ such that $f(x) = y$, and for such x we have $f^{-1}(y) = f^{-1}(f(x)) = x$.

Theorem 5. *$f : A \to B$ is bijective iff $\exists\, g : B \to A$ such that $g \circ f = I_A$ and $f \circ g = I_B$.*

Proof. $\Leftarrow$: Let $x, y \in A$ and $f(x) = f(y)$, then

$$x = I_A(x) = g \circ f(x) = g(f(x)) = g(f(y)) = g \circ f(y) = I_A(y) = y.$$

Therefore, f is injective.

By the definition of f, $f(A) \subseteq B$. We are going to prove $B \subseteq f(A)$. Let $y \in B$, then $g(y) \in A$ and

$$y = I_B(y) = f \circ g(y) = f(g(y)) \in f(A).$$

Thus, $B \subseteq f(A)$. Consequently, $B = f(A)$. So f is surjective.

$\Rightarrow$: Since f is injective, $f^{-1} : f(A) \to A$ is well-defined. Since f is surjective, $f(A) = B$. Let $g = f^{-1} : B \to A$. Then, by the definition of f^{-1}, for any $x \in A$,

$$g(f(x)) = f^{-1}(f(x)) = x = I_A(x),$$

which means $g \circ f = I_A$.

For any $y \in B = f(A)$, there exists $x \in A$ such that $f(x) = y$. Thus,

$$f(g(y)) = f(g(f(x))) = f(f^{-1}(f(x))) = f(x) = y = I_B(y),$$

which means $f \circ g = I_B$. $\square$

4 Equivalence relation

Definition: A relation on set S is any subset of $S \times S$. A relation on a set S is an equivalence relation iff

1. $\forall x \in S, (x, x) \in R$ (Reflexive)
2. $(x, y) \in R \implies (y, x) \in R$ (Symmetry)
3. $(x, y) \in R, (y, z) \in R \implies (x, z) \in R$ (Transitive)

Remark: To avoid some paradox in some example, we do not specify the set S. We write $x \sim y$ when x, y are equivalent, then the equivalent class satisfies that

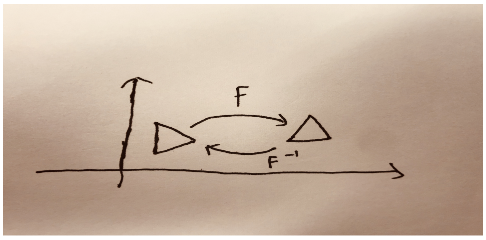
1. $x \sim x$
2. $x \sim y \implies y \sim x$
3. $x \sim y, y \sim z \implies x \sim z$

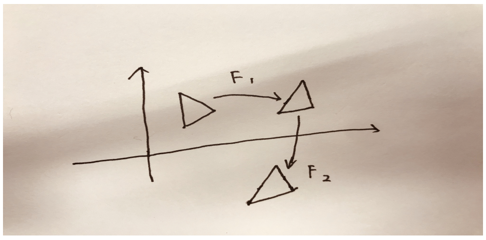
Example: $S =$ the set of all triangles in the plane $\mathbb{R}^2$. Define a relation R on S by

$$\begin{aligned} R = \{&(T_1, T_2), T_1 \text{ and } T_2 \text{ are congruent, that is} \\ &\text{(after some rigid transform (reflection,translation,rotation)}, T_1 \text{ can be } T_2)\} \end{aligned} \tag{4.1}$$

We check that R is an equivalence relation.

1. For x in S, choosing identity transform (translate 0, rotation 0), we have x can be x. That is $(x, x) \in R$.
2. For $(x, y) \in R$, by definition we have some rigid transform F such that $Fx = y$. Then we choose the inverse transform of F as F^{-1}, it is still a rigid transform. So we get $x = F^{-1}y$ and we have $(y, x) \in R$.





3. For $(x, y) \in R, (y, z) \in R$, by definition we have some rigid transform F_1, F_2 such that $F_1 x = y, F_2 y = z$. So we have $F_2 \circ F_1 x = z$ and $F_2 \circ F_1$ is still a rigid transform. So we have $(x, z) \in R$.