Discrete Mathematics Recitation Class

Tianyu Qiu

University of Michigan - Shanghai Jiaotong University

Joint Institute

Summer Term 2020

Contents

The Natural Numbers

Induction
- Mathematical Induction
- Strong Induction
- Recursive Definitions & Structural Induction

Exercises

Questions in Assignment 1

Peano Axioms (P78)

Definition

1. $\mathbb{N}$ contains at least one object, called zero.
2. $\mathbb{N}$ is closed under the successor function, i.e., if n is in $\mathbb{N}$, the successor of n is in $\mathbb{N}$.
3. Zero is not the successor of a number.
4. Two numbers of which the successors are equal are themselves equal.
5. (Induction Axiom) If a set $S \subset \mathbb{N}$ contains zero and also the successor of every number in S, then $S = \mathbb{N}$.

Any set with a successor relation satisfying these axioms is called a realization of the natural numbers.

The von Neumann Realization(P79)

$$
\begin{aligned}
0 &:= \emptyset \\
1 &:= \{0\} = \{\emptyset\} \\
2 &:= \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\
3 &:= \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
&\vdots
\end{aligned}
$$

Operations on $\mathbb{N}$

Definitions

1. Addition(P81)
   - $+ := \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \qquad (a, b) \mapsto a + b$
   - Neutral element: 0
   - Associativity/Communitativity
2. Multiplication(P82)
   - $\cdot := \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \qquad (a, b) \mapsto a \cdot b$
   - Neutral element: 1
   - Associativity/Communitativity
   - Distributivity

Mathematical Induction

Mathematical induction works by establishing two statements (P84):

1. $A(n_0)$ is true.
2. $A(n+1)$ is true whenever $A(n)$ is true for $n \geq n_0$,i.e.

$$\forall_{\substack{n \in \mathbb{N} \\ n \geq n_0}} (A(n) \Rightarrow A(n+1))$$

Induction axiom ensures that the principle of Mathematical Induction is valid:(P87)

Suppose $S := \{n \in \mathbb{N} | A(n)\}$. We show $A(0)$ is true, so $0 \in S$. Next we show that $A(n) \Rightarrow A(n+1)$ for all $n \in \mathbb{N}$. This means that if $n \in S$, then $n+1 \in S$. By Induction axiom, this means that $S = \mathbb{N}$, which means that $A(n)$ is true for all $n \in \mathbb{N}$

Well-Ordering Principle (P87-P88)

Definition

Every non-empty set $S \subset \mathbb{N}$ has a least element. Let S_m be

the set containing m as well as the successor of any element of S_m, then

$$m < n :\Leftrightarrow (n \in S_m) \wedge (n \neq m)$$

We now take a "least element of M" to be an element $m_0 \in M$ such that $M \in S_{m_0}$, then the Well-Order Principle can then be written as

$$\underset{M \subset \mathbb{N}}{\forall} \quad \underset{m \in M}{\exists} \quad M \subset S_m$$

The Well-Ordering Principle $\equiv$ the Induction Axiom

1. Well-Ordering Principle $\Rightarrow$ Induction Axiom (P90)

Proof.

Suppose that there exists an $n_0 \in \mathbb{N}$ such that $n_0 \notin S$. Then the set $M = \mathbb{N} - S$ is non-empty. By the well-ordering principle, M must have a least element m_0. Since $0 \in S, m_0 \neq 0$, there exists $m_0 - 1$ preceding m_0. Therefore $m_0 - 1 \in S$. However, m_0, the successor of $m_0 - 1 \notin S$, which leads to a contradiction. □

2. Induction Axiom $\Rightarrow$ Well-Ordering Principle (P91)

Proof.

Proof by contradiction □

Strong Induction (P97-P98)

Strong induction works by establishing two statements:

1. $A(n_0)$ is true.
2. $A(n+1)$ is true whenever all the statement $A(n_0+1), A(n_0+2), \cdots, A(n)$ is true for $n \geq n_0$,i.e.

$$\forall_{\substack{n\in\mathbb{N} \\ n\geq n_0}} ((A(n_0) \wedge A(n_0+1) \wedge \cdots \wedge A(n)) \Rightarrow A(n+1))$$

Mathematical Induction is a special case of Strong Induction Since

$$((A(n_0) \wedge \cdots \wedge A(n)) \Rightarrow A(n+1)) \Rightarrow (A(n)) \Rightarrow A(n+1))$$

What's more, the Mathematical Induction, Strong Induction and Well-Ordering Principle are mutually equivalent.

Example for Strong Induction (P97)

e.g.

Prove that every natural number $n \geq 2$ is a prime number or the product of primes.

Proof.

The statement is true for $n = 2$. For $n > 2$, assume that this statement is true for $2,3,\cdots,n$. Then $n+1$ is either prime or not prime. If $n+1$ is prime, we are finished. If $n+1$ is not prime, but the definition of prime number, there exists natural number(s) $k, m, (1 < k, m < n+1)$ satisfying that $k \cdot m = n+1$. Since k, m are either prime numbers or the products of primes, we are able to prove that $n+1$ is alao product of primes. $\square$

Recursive Definitions (existence and uniqueness)

- Recursively defined functions (P100)
  e.g. Factorial function: $(\cdot)! : \mathbb{N} \to \mathbb{N}$ with properties that

$$0! = 1,\ n! = n \cdot (n-1)!, n \in \mathbb{N} \setminus \{0\}$$

  We alternatively have the following expression: $n! := \prod_{k=1}^{n} k$

- Recursively defined sequences (P102)
  e.g. The Fibonacci sequence is defined through

$$a_0 := 1, a_1 := 1, a_n = a_{n-1} + a_{n-2}$$

- Recursively defined sets (P103)
  e.g. A set $S \subset \mathbb{N}$ is defined by the following properties: 1) $3 \in S$, 2) $\forall x, y \in S, x + y \in S$, then

$$S = \{n \in \mathbb{N} |\ 3|n, n \in \mathbb{N} \setminus \{0\}\}$$

Structural Induction (P108)

A useful variant of induction that allows us to prove properties for recursively defined objects.

1. Show that the result holds for all elements specified in the basis step of the recursive definition to be in the set.
2. Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

Examples for Structural Induction

- The length of string xy, $l(xy)$ can be calculated by $l(xy) = l(x) + l(y)$. (P109-P110)
  e.g. maths=math+s=mat+h+s=ma+t+h+s=m+a+t+h+s
- Given recursively defined set S: 1) $3 \in S$, 2) $\forall x, y \in S, x + y \in S$, and set $T := \{n \in \mathbb{N} |\ 3|n, n \in \mathbb{N} \setminus \{0\}\}$, show that $S = T$. (P111-P112)

Proof.

1. Show that $S \subset T$(Structural Induction). First, $3 \in S, 3 \in T$, then assume that $x, y \in S$ is also elements in T, i.e. $x, y \in T$, then $3|x+y$ is satisfied, which means $x + y \in T$. Thus $S \subset T$.
2. Show that $T \subset S$(Mathematical Induction). First, $3 \in T, 3 \in S$, then assume that $n = 3k \in S$, then $n' = 3(k+1) \in T$, is also an element in S, so that $T \subset S$.
3. Having $T \subset S$ and $S \subset T$, we have $S = T$.

□

Examples for Structural Induction

Theorem

Let $B = \{A_1, A_2, \cdots\}$ be a set of atomic propositions. Every well-formed compound propositional expression formed from atomic propositions in B is logically equivalent to a compound expression that only involves atomic propositions from B and the connectives $\vee$ and $\neg$.

Examples for Structural Induction

Proof.

The result clearly holds for every atomic proposition in B. Suppose that the result holds for the compound expressions P and Q. Let P' and Q' be expressions involving only atomic propositions in B and the connectives $\vee$ and $\neg$ such that $P \equiv P'$ and $Q \equiv Q'$. Now

$$\neg P \equiv \neg P'$$

$$P \vee Q \equiv P' \vee Q'$$

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

$$P \Rightarrow Q \equiv \neg P' \vee Q'$$

$$P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P) \equiv \neg(\neg(\neg P' \vee Q') \vee \neg(\neg Q' \vee P'))$$

Thus if the theorem holds for the compound expressions P and Q, then the theorem also holds for $\neg P, P \vee Q, P \wedge Q, P \Rightarrow Q, P \Leftrightarrow Q$. Therefore the result follows by structural induction. □

Exercises (DMA P343)

Show that if the statement $P(n)$ is true for infinitely many positive integers n and $P(n+1) \rightarrow P(n)$ is true for all positive integers n, the $P(n)$ is true for all positive integers n.

Solution

Proof.

We can show this result by proof by contradiction. Suppose there exists $n_0 \in \mathbb{N} \setminus \{0\}$ such that $P(n_0)$ is false. Then we immediately get $P(n_0 + 1)$ is false (this is due to contraposition of implication), then $P(n_0 + 2), P(n_0 + 3), \cdots$ is also false in the same way. In the end, we can only have no more than $n_0 - 1$ positive integers that may make $P(n)$ ture, which contradicts the condition that $P(n)$ is true for infinitely many positive integers. $\square$

Exercise 1.4

In every-day language, the phrase "A or B" is generally taken to mean A or B, but not both A and B." The corresponding binary operation is called the *exclusive or*, written as in logic or XOR in logic gate design. It is defined by the truth table

A	B	$A \oplus B$
T	T	F
T	F	T
F	T	T
F	F	F

i) Express $\oplus$ by logical conjunction, disjunction and negation, i.e. through the operations $\{\wedge, \vee, \neg\}$.
ii) Write $\vee$ using $\{\wedge, \oplus, \neg\}$.
iii) Explain why ii) proves that $\{\wedge, \oplus, \neg\}$ is functionally complete.

Solutions

i)

$$A \oplus B \equiv \neg(A \Leftrightarrow B) \equiv \neg((\neg A \vee B) \wedge (\neg B \vee A)) \equiv (A \wedge \neg B) \vee (B \wedge \neg A)$$

ii) Comparing the truth table of $A \oplus B$, $A \vee B$ and $A \wedge B$

A	B	$A \oplus B$	$A \wedge B$	$A \vee B$
T	T	F	T	T
T	F	T	F	T
F	T	T	F	T
F	F	F	F	F

$$A \vee B \equiv (A \wedge B) \oplus (A \oplus B)$$

iii) Since we can express $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$ merely by $\{\wedge, \oplus, \neg\}$, thus it is functionally complete.

Exercise 1.5

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

$$A|B :\equiv \neg(A \wedge B),\ A \downarrow B :\equiv \neg(A \vee B)$$

- Deduce that $\{|\}$ is a functionally complete collection of logical operators.
- Deduce that $\{\downarrow\}$ is a functionally complete collection of logical operators.
- Express $\oplus$ solely through $\downarrow$.

Solutions

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

Solutions

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

Solutions

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

More Thoughts on $\oplus, \downarrow$, and $|$

$$A \oplus B \equiv \neg(A \Leftrightarrow B),\ A|B \equiv \neg(A \wedge B),\ A \downarrow B \equiv \neg(A \vee B)$$

Some basic facts:

- 1. $\oplus$ is communitative as well as associative.
  2. $\downarrow$ is communitative but not associative.
  3. $|$ is communitative but not associative.
- 1. $A \oplus A \equiv F,\ A \oplus \neg A \equiv T,\ A \oplus T \equiv \neg A,\ A \oplus F \equiv A$
  2. $A|A \equiv \neg A,\ A|\neg A \equiv T,\ A|T \equiv \neg A, A|F \equiv T$
  3. $A \downarrow A \equiv \neg A,\ A \downarrow \neg A \equiv F,\ A \downarrow T \equiv F, A \downarrow F \equiv \neg A$
- $A \oplus \neg B \equiv \neg A \oplus B \equiv \neg(A \oplus B)$
- $(A|A)|(A|A) \equiv A,\ (A \downarrow A) \downarrow (A \downarrow A) \equiv A$