Prologue and Notation

Xiaofeng Gao

Department of Computer Science and Engineering
Shanghai Jiao Tong University, P.R.China

February 23, 2016

Outline

Definition

- A set is an unordered collection of elements. $\rightarrow$ No duplications.
- Examples and notations:
  - $\{a, b, c\}$
  - $\{x \mid x \text{ is an even integer}\} \rightarrow \{0, 2, 4, 6, \cdots\}$
  - ϕ: empty set
  - $\mathbb{N} = \{0, 1, 2, \ldots\}$: natural numbers (nonnegative integers)
  - $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$: integers
  - $\mathbb{R}$: real numbers
  - $\mathbb{E}$: even numbers
  - $\mathbb{O}$: odd numbers

Definition (2)

- Cardinality of a set: $|S| \rightarrow$ number of distinct elements
- Set Equality: $S = T \rightarrow x \in S$ iff $x \in T$
- Subset: A set S is a subset of T, $S \subseteq T$, if every element of S is an element of T
- Proper subset: a subset of T is a subset other than the empty set $\emptyset$ or T itself (Use of word proper, proper subsequence or proper substring)
- Strict Subset: S is a strict subset, $S \subset T$, if not equal to T

$\cup$, $\cap$, $\rightarrow$, $\overline{S}$

- Union: $S \cup T \rightarrow$ the set of elements that are either in S or in T.
  - $S \cup T = \{s \mid s \in S \text{ or } s \in T\}$
  - $\{a,b,c\} \cup \{c,d,e\} = \{a,b,c,d,e\}$
  - $|S \cup T| \leq |S| + |T|$
- Intersection: $S \cap T$
  - $S \cap T = \{s \mid s \in S \text{ and } s \in T\}$
  - $\{a,b,c\} \cap \{c,d,e\} = \{c\}$
- Difference: $S - T \rightarrow$ set of all elements in S not in T
  - $S - T = \{s \mid s \in S \text{ but not in } T\} = S \cap \overline{T}$
  - $\{1,2,3\} - \{1,4,5\} = \{2,3\}$
- Complement:
  - Need universal set U
  - $\overline{S} = \{s \mid s \in U \text{ but not in } S\}$

$\times$, 2^S

- Cartesian Product
  - $S \times T = \{(s,t) \mid s \in S, t \in T\}$
  - In a graph $G = (V,E)$, the edge set E is the subset of Cartesian product of vertex set V. $E \subseteq V \times V$.
- Power Set
  - 2^S set of all subsets of S
  - Note: notation $|2^S| = 2^{|S|}$, meaning 2^S is a good representation for power set.
  - $S = \{a,b,c\}$, then $2^S = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$
  - Indicator Vector: Use a zero/one vector to represent the elements in power set.

	a	b	c
$\emptyset$	0	0	0
$\{a\}$	1	0	0
$\{b\}$	0	1	0
$\{a,b,c\}$	1	1	1

Ordered Pair

- (x,y): ordered pair of elements x and y; $(x,y) \neq (y,x)$.
- $(x_1, \cdots, x_n)$: ordered n-tuple $\rightarrow$ boldfaced $\mathbf{x}$.
- $A_1 \times A_2 \times \cdots \times A_n = \{(x_1, \cdots, x_n) \mid x_1 \in A_1, \cdots, x_n \in A_n\}$.
- $A \times A \times \cdots \times A = A^n$.
- $A^1 = A$.

Definition

- f is a set of ordered pairs s.t. if $(x,y) \in f$ and $(x,z) \in f$, then $y = z$, and $f(x) = y$.
- $Dom(f)$: Domain of f, $\{x : f(x) \text{ is defined}\}$.
- $f(x)$ is undefined if $x \notin Dom(f)$.
- $Ran(f)$: Range of f, $\{f(x) : x \in Dom(f)\}$.
- f is a function from A to B: $Dom(f) \subseteq A$ and $Ran(f) \subseteq B$.
- $f : A \rightarrow B$: f is a function from A to B with $Dom(f) = A$.

Mapping

- Injective: if $x, y \in Dom(f)$, $x \neq y$, then $f(x) \neq f(y)$.
- Inverse f^{-1}: the unique function g s.t. $Dom(g) = Ran(f)$, and $g(f(x)) = x$.
- Surjective: if $Ran(f) = B$.
- Bijective: both injective and surjective.

Operation

1. $f|X$: Restriction of f to X.
   Domain $X \cap Dom(f)$. Write $f(X)$ for $Ran(f|X)$.
2. $f^{-1}(Y) = \{x : f(x) \in Y\}$: inverse image of Y under f.
3. $f \subseteq g$: g extends f, $f = g|Dom(f)$.
   $Dom(f) \subseteq Dom(g)$ and $\forall x \in Dom(f), f(x) = g(x)$.
4. $f \circ g$: composition of f and g. Domain $\{x : x \in Dom(g) \text{ and } g(x) \in Dom(f)\}$, value $f(g(x))$.
5. $f_\emptyset$: function defined nowhere. $Dom(f_\emptyset) = Ran(f_\emptyset) = \emptyset$.
   $f_\emptyset = g|\emptyset$ for any function g.

$\simeq$: similar-or-equal-to

Suppose $\alpha(\mathbf{x})$ and $\beta(\mathbf{x})$ are expressions involving $\mathbf{x} = (x_1, \cdots, x_n)$, then $\alpha(\mathbf{x}) \simeq \beta(\mathbf{x})$ means $\forall \mathbf{x}$, $\alpha(\mathbf{x})$ and $\beta(\mathbf{x})$ are either bother defined, or both undefined, and if defined they are equal.

- $f(x) \simeq g(x)$ means $f = g$.
- $f(x) \simeq y$ means $f(x)$ is defined and $f(x) = y$.

Partial and Total Function

- n-ary function: $f(\mathbf{x}), f(x_1, \cdots, x_n), f : \mathbb{N}^n \to \mathbb{N}$.
- Partial function: $Dom(f)$ is not necessarily the whole $\mathbb{N}^n$. (In our class function means partial function)
- Total function: $Dom(f) = \mathbb{N}^n$.
- Zero function: $\mathbf{0}$ from $\mathbb{N}$ to $\mathbb{N}$.
- Symbol function: $\mathbf{m}$ from $\mathbb{N}$ to $\mathbb{N}$.

Relation

If A is a set, a property $M(x_1, \cdots, x_n)$ that holds for some n-tuple from A^n and does not hold for all other n-tuples from A^n is called an n-ary relation or predicate on A.

- Property $x < y$. $2 < 5$, $6 < 4$.
- f from $\mathbb{N}^n$ to $\mathbb{N}$ gives rise to predicate $M(\mathbf{x}, y)$ by: $M(x_1, \cdots, x_n, y)$ iff $f(x_1, \cdots, x_n) \simeq y$.

Equivalence Relation

- A binary relation R on A is called equivalence relation if

$$\left.\begin{array}{lll} \text{reflexivity} & \forall x \text{ in } A & R(x,x) \\ \text{symmetry} & R(x,y) \Rightarrow R(y,x) & \\ \text{transitivity} & R(x,y), R(y,z) \Rightarrow R(x,z) & \end{array}\right\} \text{equivalence}$$

- A binary relation R on A is called a partial order if

$$\left.\begin{array}{ll} \text{irreflexivity} & \text{not } R(x,x) \\ \text{transitivity} & R(x,y), R(y,z) \Rightarrow R(x,z) \end{array}\right\} \text{partial order}$$

Example

	reflexive	symmetric	transitive
$<$	No	No	Yes
$\leq$	Yes	No	Yes
Parent of	No	No	No
$=$	Yes	Yes	Yes

Hand Writing

- Small letters for elements and functions.
  - a, b, c for elements,
  - f, g for functions,
  - i, j, k for integer indices,
  - x, y, z for variables,
- Capital letters for sets. A, B, S. $A = \{a_1, \cdots, a_n\}$
- Bold small letters for vectors. $\mathbf{x}$, $\mathbf{y}$. $\mathbf{v} = \{v_1, \cdots, v_m\}$
- Bold capital letters for collections. $\mathbf{A}$, $\mathbf{B}$. $\mathbf{S} = \{S_1, \cdots, S_n\}$
- Blackboard bold capitals for domains (standard symbols). $\mathbb{N}$, $\mathbb{R}$.
- German script for collection of functions. $\mathscr{C}$, $\mathscr{S}$, $\mathscr{T}$.
- Greek letters for parameters or coefficients. α, β, γ.
- Double strike handwriting for bold letters.

What is proof?

A proof of a statement is essentially a convincing argument that the statement is true. A typical step in a proof is to derive statements from

- assumptions or hypotheses.
- statements that have already been derived.
- other generally accepted facts, using general principles of logical reasoning.

Types of Proof

- Proof by Construction
- Proof by Contrapositive
  - Proof by Contradiction
  - Proof by Counterexample
- Proof by Cases
- Proof by Mathematical Induction
  - The Principle of Mathematical Induction
  - Minimal Counterexample Principle
  - The Strong Principle of Mathematical Induction

Proof by Construction ($\forall x, P(x)$ holds)

Example: For any integers a and b, if a and b are odd, then ab is odd.

Proof: Since a and b are odd, there exist integers x and y such that $a = 2x + 1$, $b = 2y + 1$. We wish to show that there is an integer z so that $ab = 2z + 1$. Let us therefore consider ab.

$$\begin{aligned} ab &= (2x+1)(2y+1) \\ &= 4xy + 2x + 2y + 1 \\ &= 2(2xy + x + y) + 1 \end{aligned}$$

Thus if we let $z = 2xy + x + y$, then $ab = 2z + 1$, which implies that ab is odd. □

Proof by Contrapositive ($p \to q \Leftrightarrow \neg q \to \neg p$)

Example: $\forall i, j, n \in \mathbb{N}$, if $i \times j = n$, then either $i \leq \sqrt{n}$ or $j \leq \sqrt{n}$.

Proof: We change this statement by its logically equivalence:
$\forall i, j, n \in \mathbb{N}$, if it is not the case that $i \leq \sqrt{n}$ or $j \leq \sqrt{n}$, then $i \times j \neq n$.

If it is not true that $i \leq \sqrt{n}$ or $j \leq \sqrt{n}$, then $i > \sqrt{n}$ and $j > \sqrt{n}$.

Since $j > 0$, $\sqrt{n} \geq 0$, we have

$$i > \sqrt{n} \Rightarrow i \times j > \sqrt{n} \times j \geq \sqrt{n} \times \sqrt{n} = n.$$

It follows that $i \times j \neq n$. The original statement is true. □

Proof by Contradiction (p is true $\Leftrightarrow \neg p \rightarrow \mathit{false}$ is true)

Example: For any sets A, B, and C, if $A \cap B = \emptyset$ and $C \subseteq B$, then $A \cap C = \emptyset$.

Proof: Assume $A \cap B = \emptyset$, $C \subseteq B$, and $A \cap C \neq \emptyset$.

Then there exists x with $x \in A \cap C$, so that $x \in A$ and $x \in C$.

Since $C \subseteq B$ and $x \in C$, it follows that $x \in B$.

Therefore $x \in A \cap B$, which contradicts the assumption that $A \cap B = \emptyset$. □

Proof by Contradiction (2)

Example: $\sqrt{2}$ is irrational. (A real number x is *rational* if there are two integers m and n so that $x = m/n$.)

Proof: Suppose on the contrary $\sqrt{2}$ is rational.

Then there are integers m' and n' with $\sqrt{2} = \frac{m'}{n'}$.

By dividing both m' and n' by all the factors that are common to both, we obtain $\sqrt{2} = \frac{m}{n}$, for some integers m and n having no common factors.

Since $\frac{m}{n} = \sqrt{2}$, we can have $m^2 = 2n^2$, therefore m^2 is even, and m is also even.

Proof by Contradiction (Cont.)

Let $m = 2k$. Therefore, $(2k)^2 = 2n^2$.

Simplifying this we obtain $2k^2 = n^2$, which means n is also a even number.

We have shown that m and n are both even numbers and divisible by 2. This contradicts the previous statement m and n have no common factors. Therefore, $\sqrt{2}$ is irrational. □

Proof by Cases (Divide domain into distinct subsets)

Example: Prove that if $n \in \mathbb{N}$, then $3n^2 + n + 14$ is even.

Proof: Let $n \in \mathbb{N}$. We can consider two cases: n is even and n is odd.

Case 1. n is even. Let $n = 2k$, where $k \in \mathbb{N}$. Then

$$\begin{aligned} 3n^2 + n + 14 &= 3(2k)^2 + 2k + 14 \\ &= 12k^2 + 2k + 14 \\ &= 2(6k^2 + k + 7) \end{aligned}$$

Since $6k^2 + k + 7$ is an integer, $3n^2 + n + 14$ is even if n is even.

Proof by Cases (Cont.)

Case 2. n is odd. Let $n = 2k + 1$, where $k \in \mathbb{N}$. Then

$$\begin{aligned} 3n^2 + n + 14 &= 3(2k+1)^2 + (2k+1) + 14 \\ &= 3(4k^2 + 4k + 1) + (2k+1) + 14 \\ &= 12k^2 + 12k + 3 + 2k + 1 + 14 \\ &= 12k^2 + 14k + 18 = 2(6k^2 + 7k + 9) \end{aligned}$$

Since $6k^2 + 7k + 9$ is an integer, $3n^2 + n + 14$ is even if n is odd.

Since in both cases $3n^2 + n + 14$ is even, it follows that if $n \in \mathbb{N}$, then $3n^2 + n + 14$ is even.

The Principle of Mathematical Induction

Suppose $P(n)$ is a statement involving an integer n. Then to prove that $P(n)$ is true for every $n \geq n_0$, it is sufficient to show these two things:

- $P(n_0)$ is true.
- For any $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is true.

An Example for Mathematical Induction

Example: Let $P(n)$ be the statement $\sum_{i=0}^{n} i = n(n+1)/2$. Prove that $P(n)$ is true for every $n \geq 0$.

Proof: We prove $P(n)$ is true for $n \geq 0$ by induction.

Basis step. $P(0)$ is $0 = 0(0+1)/2$, and it is obviously true.

Induction Hypothesis. Assume $P(k)$ is true for some $k \geq 0$. Then $0 + 1 + 2 + \cdots + k = k(k+1)/2$.

Proof of Induction Step. Now let us prove that $P(k+1)$ is true.

$$\begin{aligned} 0 + 1 + 2 + \cdots + k + (k+1) &= k(k+1)/2 + (k+1) \\ &= (k+1)(k/2 + 1) \\ &= (k+1)(k+2)/2 \end{aligned} \qquad \square$$

An Example for Mathematical Induction (2)

Example: For any $x \in \{0,1\}^*$, if x begins with 0 and ends with 1 (i.e., $x = 0y1$ for some string y), then x must contain the substring 01. (Note that * is the *Kleene star*. $\{0,1\}^*$ means "every possible string consisted of 0 and 1, including the empty string".)

Proof: Consider the statement $P(n)$: If $|x| = n$ and $x = 0y1$ for some string $y \in \{0,1\}^*$, then x contains the substring 01. If we can prove that $P(n)$ is true for every $n \geq 2$, it will follow that the original statement is true. We prove it by induction.

Basis step. $P(2)$ is true.

Induction hypothesis. $P(k)$ for $k \geq 2$.

An Example for Mathematical Induction (2)

Proof of induction step. Let's prove $P(k+1)$.

Since $|x| = k+1$ and $x = 0y1$, $|y1| = k$.

If y begins with 1 then x begins with the substring 01. If y begins with 0, then $y1$ begins with 0 and ends with 1;

by the induction hypothesis, y contains the substring 01, therefore x does else. □

The Minimal Counterexample Principle

Example: Prove $\forall n \in \mathbb{N}$, $5^n - 2^n$ is divisible by 3.

Proof: If $P(n) = 5^n - 2^n$ is not true for every $n \geq 0$, then there are values of n for which $P(n)$ is false, and there must be a smallest such value, say $n = k$.

Since $P(0) = 5^0 - 2^0 = 0$, which is divisible by 3, we have $k \geq 1$, and $k - 1 \geq 0$.

Since k is the smallest value for which $P(k)$ false, $P(k-1)$ is true. Thus $5^{k-1} - 2^{k-1}$ is a multiple of 3, say $3j$.

The Minimal Counterexample Principle (Cont.)

However, we have

$$\begin{aligned} 5^k - 2^k &= 5 \times 5^{k-1} - 2 \times 2^{k-1} \\ &= 5 \times (5^{k-1} - 2^{k-1}) + 3 \times 2^{k-1} \\ &= 5 \times 3j + 3 \times 2^{k-1} \end{aligned}$$

This expression is divisible by 3. We have derived a contradiction, which allows us to conclude that our original assumption is false.

An Example for the Weakness of Mathematical Induction

Example: Prove that $\forall n \in \mathbb{N}$ with $n \geq 2$, it has prime factorizations.

Proof: Define $P(n)$ be the statement that "n is either prime or the product of two or more primes". We will try to prove that $P(n)$ is true for every $n \geq 2$.

Basis step. $P(2)$ is true, since 2 is a prime. ✓

Induction hypothesis. $P(k)$ for $k \geq 2$. (as usual process)

Proof of induction step. Let's prove $P(k+1)$.

If $P(k+1)$ is prime, ✓
If $P(k+1)$ is not a prime, then we should prove that $k+1 = r \times s$, where r and s are positive integers greater than 1 and less than $k+1$.

However, from $P(k)$ we know nothing about r and s $\longrightarrow$???

The Strong Principle of Mathematical Induction

Suppose $P(n)$ is a statement involving an integer n. Then to prove that $P(n)$ is true for every $n \geq n_0$, it is sufficient to show these two things:

- $P(n_0)$ is true.
- For any $k \geq n_0$, if $P(n)$ is true for every n satisfying $n_0 \leq n \leq k$, then $P(k+1)$ is true.

Also called the principle of complete induction, or course-of-values induction.

To Complete the Example

Example: Prove that $\forall n \in \mathbb{N}$ with $n \geq 2$, it has prime factorizations.

Continue the Proof:
Induction hypothesis. For $k \geq 2$ and $2 \leq n \leq k$, $P(n)$ is true. (Strong Principle)

Proof of induction step. Let's prove $P(k+1)$.

If $P(k+1)$ is prime, ✓
If $P(k+1)$ is not a prime, by definition of a prime, $k+1 = r \times s$, where r and s are positive integers greater than 1 and less than $k+1$.

It follows that $2 \leq r \leq k$ and $2 \leq s \leq k$. Thus by induction hypothesis, both r and s are either prime or the product of two or more primes. Then their product $k+1$ is the product of two or more primes. $P(k+1)$ is true.

Giuseppe Peano (1858-1932)

- In 1889, Peano published the first set of axioms.
- Build a rigorous system of arithmetic, number theory, and algebra.
- A simple but solid foundation to construct the edifice of modern mathematics.
- The fifth axiom deserves special comment. It is the first formal statement of what we now call the “induction axiom" or “the principle of mathematical induction".

Peano Five Axioms

- Axiom 1. 0 is a number.
- Axiom 2. The successor of any number is a number.
- Axiom 3. If a and b are numbers and if their successors are equal, then a and b are equal.
- Axiom 4. 0 is not the successor of any number.
- Axiom 5. If S is a set of numbers containing 0 and if the successor of any number in S is also in S, then S contains all the numbers.

Peano Axioms vs Theorem of Mathematical Induction

Let $S(n)$ be a statement about $n \in \mathbb{N}$. Suppose

1. $S(1)$ is true, and
2. $S(t+1)$ is true whenever $S(t)$ is true for $t \geq 1$.

Then $S(n)$ is true for all $n \in \mathbb{N}$.

Proof

Let $A = \{n \in \mathbb{N} \mid S(n) \text{ is false}\}$. It suffices to show that $A = \emptyset$.

If $A \neq \emptyset$, A would contain a smallest positive integer, say $n_0 \in \mathbb{N}$, s.t.$n_0 \leq n, n \in A$.

Thus, the statement $S(n_0)$ is false and because of hypothesis (1), $n_0 > 1$.

Since n_0 is the smallest element of A, the statement $S(n_0 - 1)$ is true. Thus, by hypothesis (2), $S(n_0 - 1)$ is true which implies that $S(n_0)$ is true, a contradiction which implies that $A = \emptyset$. $\square$