Introduction to Sets and Logic (MATH 1190)

Instructor: Lili Shen
Email: shenlili@yorku.ca

Department of Mathematics and Statistics
York University

Nov 27, 2014

Outline

Well-ordering property

Well-ordering property of nonnegative integers

Every nonempty set of nonnegative integers has a least element.

Examples of using well-ordering property

Example (The division algorithm)

Show that if a is an integer and d is a positive integer, then there are unique integers q and r with $0 \leq r < d$, such that $a = dq + r$.

Examples of using well-ordering property

Proof.

Let S be the set of nonnegative integers of the form $a - dq$, where q is an integer. The set is nonempty since $-dq$ can be made as large as needed.

By the well-ordering property, S has a least element $r = a - dq_0$. The integer r is nonnegative. It also must satisfy $r < d$; otherwise, there would be a smaller nonnegative element in S, namely,

$$a - d(q_0 + 1) = a - dq_0 - d = r - d > 0.$$

Therefore, there are integers q and r with $0 \leq r < d$.

Examples of using well-ordering property

For the uniqueness of q and r, suppose there are two such pairs (q, r) and (q', r'), so that $a = dq + r = dq' + r'$ with $0 \leq r, r' < d$. Then

$$d(q - q') = r' - r,$$

and consequently $d \mid (r' - r)$. But $|r' - r| < d$ (since both r' and r are nonnegative integers less than d), we must have $r' - r = 0$, i.e., $r = r'$. Finally,

$$q = \frac{a - r}{d} = \frac{a - r'}{d} = q'.$$

$\square$

Generalized well-ordering property

The well-ordering property plays an important role in modern set theory.

Definition

A set is well-ordered if every non-empty subset has a least element.

Generalized well-ordering property

Example

- $\mathbf{N}$ and $\mathbf{Z}^+$ are both well-ordered under $\leq$.
- $\mathbf{Z}$, $\mathbf{Q}$ or $\mathbf{R}$ are not well-ordered under $\leq$.
- The set of all English words is well-ordered under lexicographic ordering.

Well-ordering theorem

Theorem (Well-ordering theorem)

For any set S, there exists a well-order on S.

In other words, every set can be organized as a well-ordered set.

This theorem is counterintuitive. As a special case, there "should be" a "well-order" on $\mathbf{R}$, but no one knows what it is (the ordinary "$\leq$" is not a "well-order" for $\mathbf{R}$)!

Axiom of choice

Theorem (Axiom of choice)

Let I be a nonempty set. If for each $i \in I$, A_i is a nonempty set, then there exists a choice function

$$f : I \longrightarrow \bigcup_{i \in I} A_i$$

such that $f(i) \in A_i$ for all $i \in I$.

This axiom is intuitive: if we have a family of nonempty sets, then we can "pick out" an element from each set.

Axiom of choice and well-ordering theorem

However, it is surprisingly that the axiom of Choice and well-ordering theorem are equivalent:

$$\text{Well-ordering theorem} \longleftrightarrow \text{Axiom of Choice.}$$

So, what is the problem of Axiom of Choice?

Axiom of choice and well-ordering theorem

If we have an infinite family of nonempty sets, how can we exactly describe the process of "picking out" an element from each set?

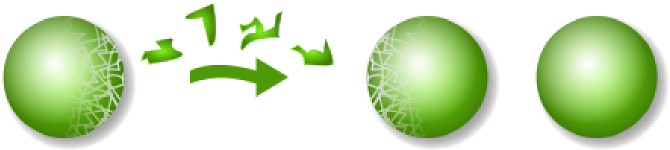
- For infinitely many pairs of shoes, we may pick out the left shoe from each pair.
- For infinitely many pairs of socks (i.e., assumed to have no distinguishing features inside each pair), such a selection can be obtained only by invoking the axiom of choice.

Since the "Axiom of Choice" is so intuitive, many important conclusions in modern mathematics cannot be established without it. However, once we admit the axiom of choice, we also need to accept well-ordering theorem, and some more strange conclusions.

Banach-Tarski paradox

Banach-Tarski paradox

Assume the axiom of choice. Then a ball be decomposed into a finite number of pieces, and reassembled into two balls identical to the original only by rotating and translating the pieces.



Indeed, the proof of this statement tells us that, decomposing a ball into 5 pieces is enough to reassemble them into two balls that are identical to the original one!

Outline

Climbing an infinite ladder

Suppose we have an infinite ladder:

(1) We can reach the first rung of the ladder.
(2) If we can reach a particular rung of the ladder, then we can reach the next rung.

From (1), we can reach the first rung. Then by applying (2), we can reach the second rung. Applying (2) again, the third rung. And so on. We can apply (2) any number of times to reach any particular rung, no matter how high up.

This example motivates the idea of proof by mathematical induction.

Principle of mathematical induction

Principle of mathematical induction

Let $P(n)$ be a propositional function with the set $\mathbf{Z}^+$ of positive integers as the domain. To prove that $P(n)$ is true for all positive integers n, we complete these steps:

- Basis step: Show that $P(1)$ is true.
- Inductive step: Show that $P(k) \to P(k+1)$ is true for all positive integers k.

To complete the inductive step, assuming the inductive hypothesis that $P(k)$ holds for an arbitrary integer k, show that $P(k+1)$ must be true.

Using mathematical induction

Remark

- Mathematical induction can be expressed as the rule of inference

$$(P(1) \wedge \forall k (P(k) \to P(k+1))) \to \forall n\, P(n),$$

where the domain is the set $\mathbf{Z}^+$ of positive integers.

- In a proof by mathematical induction, we do not assume that $P(k)$ is true for all positive integers k! We just show that if we assume that $P(k)$ is true, then $P(k+1)$ must also be true.
- Proofs by mathematical induction do not always start at the integer 1. In such a case, the basis step begins at a starting point $b \in \mathbf{Z}$. We will see examples of this soon.

Validity of mathematical induction

We present here a proof (by contradiction) of the validity of mathematical induction using the well-ordering property.

Theorem

$(P(1) \wedge \forall k (P(k) \rightarrow P(k+1))) \rightarrow \forall n\, P(n).$

That is, suppose that $P(1)$ holds and $P(k) \rightarrow P(k+1)$ is true for all positive integers k, we need to show $\forall n\, P(n)$.

Validity of mathematical induction

Proof.

Assume there is at least one positive integer n for which $P(n)$ is false. Then:

- The set S of positive integers for which $P(n)$ is false is nonempty.
- By the well-ordering property, S has a least element, say m. We know that m can not be 1 since $P(1)$ holds.
- Since m is positive and greater than 1, $m - 1$ must be a positive integer. Since $m - 1 < m$, it is not in S, so $P(m - 1)$ must be true.
- But then, since the conditional $P(k) \to P(k + 1)$ for every positive integer k holds, $P(m)$ must also be true. This contradicts $P(m)$ being false.

Hence, $P(n)$ must be true for every positive integer n. $\square$

How mathematical induction works

Consider an infinite sequence of dominoes, labeled $1, 2, 3, \ldots,$ where each domino is standing. Let $P(n)$ be the proposition that the nth domino is knocked over.

- We know that the first domino is knocked down, i.e., $P(1)$ is true .
- We also know that if whenever the kth domino is knocked over, it knocks over the $(k+1)$st domino, i.e, $P(k) \to P(k+1)$ is true for all positive integers k.
- Hence, all dominos are knocked over, i.e., $P(n)$ is true for all positive integers n.

Examples of proofs by mathematical induction

Example (Sum of arithmetic progression)

Let n be a positive integer. Show that

$$\sum_{i=1}^{n} i = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Examples of proofs by mathematical induction

Proof.

Let $P(n)$ denote "$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$."

For $n = 1$, $P(1)$ is true since

$$\frac{1(1+1)}{2} = 1.$$

Assume the $P(k)$ is true, i.e., $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$.

We need to show that $P(k+1)$ is true, i.e.,

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}.$$

Indeed,

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \Big(\sum_{i=1}^{k} i\Big) + (k+1)\\ &= \frac{k(k+1)}{2} + k + 1\\ &= \frac{k(k+1) + 2(k+1)}{2}\\ &= \frac{(k+1)(k+2)}{2};\end{aligned}$$

the conclusion thus follows. $\square$

Examples of proofs by mathematical induction

Example (Sum of geometric progression)

Let n be a nonnegative integer and $r \neq 1$. Show that

$$\sum_{j=0}^{n} ar^j = a + ar + ar^2 + \cdots + ar^n = \frac{ar^{n+1} - a}{r - 1}.$$

Examples of proofs by mathematical induction

Proof.

Let $P(n)$ denote "$\sum_{j=0}^{n} ar^j = \frac{ar^{n+1} - a}{r - 1}$."

For $n = 0$, $P(0)$ is true since

$$\frac{ar^{0+1} - a}{r - 1} = \frac{ar - a}{r - 1} = a.$$

Assume $P(k)$ is true, i.e., $\sum_{j=0}^{k} ar^j = \frac{ar^{k+1} - a}{r - 1}$.

We need to show that $P(k + 1)$ is true, i.e.,

$$\sum_{j=0}^{k+1} ar^j = \frac{ar^{k+2} - a}{r - 1}.$$

Examples of proofs by mathematical induction

Indeed,

$$\begin{aligned}\sum_{j=0}^{k+1} ar^j &= \Big(\sum_{j=0}^{k} ar^j\Big) + ar^{k+1} \\ &= \frac{ar^{k+1} - a}{r-1} + ar^{k+1} \\ &= \frac{ar^{k+1} - a + ar^{k+2} - ar^{k+1}}{r-1} \\ &= \frac{ar^{k+2} - a}{r-1},\end{aligned}$$

as desired. $\square$

Examples of proofs by mathematical induction

Example (Table 2 on P166, Exercise 3 on P329)

Let n be a positive integer. Show that

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Examples of proofs by mathematical induction

Proof.

Let $P(n)$ denote "$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$."

For $n = 1$, $P(1)$ is true since

$$\frac{1(1+1)(2\cdot 1+1)}{6} = 1 = 1^2.$$

Assume the $P(k)$ is true, i.e., $\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}$.

We need to show that $P(k+1)$ is true, i.e.,

$$\sum_{i=1}^{k+1} i^2 = \frac{(k+1)(k+2)(2k+3)}{6}.$$

In fact,

$$\begin{aligned}\sum_{i=1}^{k+1} i^2 &= \Big(\sum_{i=1}^{k} i^2\Big) + (k+1)^2 \\ &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\ &= \frac{(k+1)(2k^2+7k+6)}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6},\end{aligned}$$

completing the proof. $\square$

Examples of proofs by mathematical induction

Example (Table 2 on P166, Exercise 4 on P329)

Let n be a positive integer. Show that

$$\sum_{i=1}^{n} i^3 = 1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

Examples of proofs by mathematical induction

Proof.

Let $P(n)$ denote "$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$."

For $n = 1$, $P(1)$ is true since

$$\frac{1^2(1+1)^2}{4} = 1 = 1^3.$$

Assume the $P(k)$ is true, i.e., $\sum_{i=1}^{k} i^3 = \frac{k^2(k+1)^2}{4}$.

We need to show that $P(k+1)$ is true, i.e.,

$$\sum_{i=1}^{k+1} i^3 = \frac{(k+1)^2(k+2)^2}{4}.$$

Examples of proofs by mathematical induction

Indeed,

$$\begin{aligned}\sum_{i=1}^{k+1} i^3 &= \Big(\sum_{i=1}^{k} i^3\Big) + (k+1)^3 \\ &= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\ &= \frac{k^2(k+1)^2 + 4(k+1)^3}{4} \\ &= \frac{(k+1)^2(k^2+4k+4)}{4} \\ &= \frac{(k+1)^2(k+2)^2}{4}.\end{aligned}$$

Thus $P(k+1)$ is true, as desired. $\square$

Examples of proofs by mathematical induction

Example (Exercise 14 on P330)

Let n be a positive integer. Show that

$$\sum_{k=1}^{n} k2^k = 1\cdot 2^1 + 2\cdot 2^2 + \cdots + k2^k = (n-1)2^{n+1} + 2.$$

Examples of proofs by mathematical induction

Proof.

Let $P(n)$ denote "$\sum_{k=1}^{n} k2^k = (n-1)2^{n+1} + 2$.

For $n = 1$, $P(1)$ is true since

$$(1-1)2^{1+1} + 2 = 2 = 1 \cdot 2^1.$$

Assume the $P(m)$ is true, i.e., $\sum_{k=1}^{m} k2^k = (m-1)2^{m+1} + 2$.

We need to show that $P(m+1)$ is true, i.e.,

$$\sum_{k=1}^{m+1} k2^k = m2^{m+2} + 2.$$

Examples of proofs by mathematical induction

Indeed,

$$\begin{aligned}
\sum_{k=1}^{m+1} k2^k &= \Big(\sum_{k=1}^{m} k2^k\Big) + (m+1)2^{m+1} \\
&= (m-1)2^{m+1} + 2 + (m+1)2^{m+1} \\
&= (m-1+m+1)2^{m+1} + 2 \\
&= 2m \cdot 2^{m+1} + 2 \\
&= m2^{m+2} + 2.
\end{aligned}$$

Thus $P(m+1)$ is true, and consequently $P(n)$ is true for all integers n. □

Outline

Strong induction

Strong induction

Let $P(n)$ be a propositional function with the set $\mathbf{Z}^+$ of positive integers as the domain. To prove that $P(n)$ is true for all positive integers n, we complete these steps:

- Basis step: Show that $P(1)$ is true.
- Inductive step: Show that

$$(P(1) \wedge P(2) \wedge \cdots \wedge P(k)) \rightarrow P(k+1)$$

  is true for all positive integers k.

To complete the inductive step, assuming the inductive hypothesis that each P_j $(1 \leq j \leq k)$ holds for an arbitrary integer k, show that $P(k+1)$ must be true.

Climbing an infinite ladder

Strong induction is also called the second principle of mathematical induction, or complete induction.

Strong induction tells us that we can reach all rungs of an infinite ladder if:

(1) We can reach the first rung of the ladder.

(2) For every integer k, if we can reach the first k rungs, then we can reach the $(k+1)$st rung.

Climbing an infinite ladder

Example

Suppose we can reach the first and second rungs of an infinite ladder, and we know that if we can reach a rung, then we can reach two rungs higher. Prove that we can reach every rung.

Climbing an infinite ladder

Proof.

- Basis step: We can reach the first step.
- Inductive step: The inductive hypothesis is that we can reach the first k rungs, for any $k \geq 2$. We can reach the $(k+1)$st rung since we can reach the $(k-1)$st rung by the inductive hypothesis.

Hence, we can reach all rungs of the ladder. $\square$

Which form of induction should be used?

Remark

- We can always use strong induction instead of mathematical induction. But there is no reason to use it if it is simpler to use mathematical induction.
- In fact, the principles of mathematical induction, strong induction, and the well-ordering property are all equivalent. (Exercises 41-43)
- Sometimes it is clear how to proceed using one of the three methods, but not the other two.

Examples of proofs by strong induction

Example (The fundamental theorem of arithmetic)

Show that if n is an integer greater than 1, then n can be written as the product of primes.

Examples of proofs by strong induction

Proof.

Let $P(n)$ denote "n can be written as a product of primes."

For $n = 2$, $P(2)$ is true since 2 is itself a prime.

Assume $P(j)$ is true for all integers j with $2 \leq j \leq k$, we need to show that $P(k+1)$ is true.

- If $k+1$ is a prime number, then $P(k+1)$ is true.

Examples of proofs by strong induction

- Otherwise, $k + 1$ is a composite number and can be written as the product of two positive integers a and b with
$$2 \leq a \leq b < k + 1.$$
By the inductive hypothesis a and b can be written as the product of primes and therefore $k + 1$ can also be written as the product of those primes.

Hence, $P(n)$ is true for all integers $n \geq 2$. □

Examples of proofs by strong induction

Example (Exercise 3 on P341)

Show that every amount of postage of 8 cents or more can be formed using just 3-cent and 5-cent stamps.

Examples of proofs by strong induction

Proof.

Let $P(n)$ denote "a postage of n cents can be formed using just 3-cent and 5-cent stamps."

For $n = 8$, $P(8)$ is true since $8 = 3 + 5$;
For $n = 9$, $P(9)$ is true since $9 = 3 + 3 + 3$;
For $n = 10$, $P(10)$ is true since $10 = 5 + 5$.

Assume $P(j)$ is true for all integers j with $8 \leq j \leq k$, where we assume $k \geq 10$, we need to show that $P(k+1)$ is true.

Examples of proofs by strong induction

In order to form $k+1$ cents of postage, note that $P(k-2)$ is true (since $k \geq 10$) by our inductive hypothesis.
Put one more 3-cent stamp on the evelope with $k-2$ cents of postage, and we have formed $k+1$ cents of postage, as desired.

Hence, $P(n)$ is true for all integers $n \geq 8$. $\square$

Examples of proofs by strong induction

Example (Exercise 9 on P342)

Show that $\sqrt{2}$ is irrational.

Examples of proofs by strong induction

Proof.

Let $P(n)$ denote "$\sqrt{2} \neq \dfrac{n}{b}$ for any positive integer b."

For $n = 1$, $P(1)$ is true since $\dfrac{1}{b} \leq 1 < \sqrt{2}$ for any positive integer b.

Assume $P(j)$ is true for all integers j with $1 \leq j \leq k$, we need to show that $P(k+1)$ is true. To this end, we prove by contradiction.

Suppose $\sqrt{2} = \dfrac{k+1}{b}$ for some positive integer b. Squaring on both sides one obtains

$$2b^2 = (k+1)^2.$$

This means $(k+1)^2$ is even, thus $k+1$ is even (see Page 42-49 in the lecture note of Oct 2). Therefore $k+1 = 2t$ for some positive integer t, and consequently

$$2b^2 = 4t^2 \longrightarrow b^2 = 2t^2.$$

Thus b^2 is also even, which means b is even, i.e., $b = 2s$ for some positive integer s. Therefore

$$\sqrt{2} = \frac{k+1}{b} = \frac{2t}{2s} = \frac{t}{s}.$$

But $t \leq k$, so this contradicts to our inductive hypothesis, and it follows that $P(k+1)$ is true.

Hence, $P(n)$ is true for all integers $n \geq 1$. $\square$

Recommended exercises

Section 5.1: 3, 4, 14.

Section 5.2: 3, 9, 37.