# Logic and the set theory

## Lecture 18: Mathematical Inductions in How to Prove It.

S. Choi

Department of Mathematical Science
KAIST, Daejeon, South Korea

Fall semester, 2012

# About this lecture

- Proof by mathematical inductions

# About this lecture

- Proof by mathematical inductions
- More examples

# About this lecture

- Proof by mathematical inductions
- More examples
- Recursion

# About this lecture

- Proof by mathematical inductions
- More examples
- Recursion
- Strong induction

# About this lecture

- Proof by mathematical inductions
- More examples
- Recursion
- Strong induction
- Closures again

# About this lecture

- Proof by mathematical inductions
- More examples
- Recursion
- Strong induction
- Closures again
- Course homepages: `http://mathsci.kaist.ac.kr/~schoi/logic.html` and the moodle page `http://moodle.kaist.ac.kr`

## About this lecture

- Proof by mathematical inductions
- More examples
- Recursion
- Strong induction
- Closures again
- Course homepages: `http://mathsci.kaist.ac.kr/~schoi/logic.html` and the moodle page `http://moodle.kaist.ac.kr`
- Grading and so on in the moodle. Ask questions in moodle.

# Some helpful references

- Sets, Logic and Categories, Peter J. Cameron, Springer. Read Chapters 3,4,5.

# Some helpful references

- Sets, Logic and Categories, Peter J. Cameron, Springer. Read Chapters 3,4,5.
- `http://plato.stanford.edu/contents.html` has much resource.

# Some helpful references

- Sets, Logic and Categories, Peter J. Cameron, Springer. Read Chapters 3,4,5.
- `http://plato.stanford.edu/contents.html` has much resource.
- Introduction to set theory, Hrbacek and Jech, CRC Press. (Chapter 3 (3.2, 3.3))

# Some helpful references

- Sets, Logic and Categories, Peter J. Cameron, Springer. Read Chapters 3,4,5.
- `http://plato.stanford.edu/contents.html` has much resource.
- Introduction to set theory, Hrbacek and Jech, CRC Press. (Chapter 3 (3.2, 3.3))
- Mathematical logic, J. Shoenfield, Assoc. for Symbolic logic.

# Proof by mathematical inductions

## Definition

(The induction principle) Let $P(x)$ be a property. Assume that

- $P(1)$ holds
- For all $n \in \mathbb{N}$, $P(n)$ implies $P(n+1)$.

Then $P$ holds for all natural numbers.

# Proof by mathematical inductions

## Definition

(The induction principle) Let $P(x)$ be a property. Assume that

- $P(1)$ holds
- For all $n \in \mathbb{N}$, $P(n)$ implies $P(n+1)$.

Then $P$ holds for all natural numbers.

## Definition

(The induction principle: strong version) Let $P(x)$ be a property. Assume that for all $n \in \mathbb{N}$,

$$(\forall k < n, P(k)) \to P(n).$$

Then $P$ holds for all natural numbers.

# Proof by mathematical inductions

## Lemma

- $1 \leq n$ *for all* $n \in \mathbb{N}$.
- *For all* $k, n \in \mathbb{N}$, $k < n + 1$ *if and only if* $k < n$ *or* $k = n$.

# Proof by mathematical inductions

## Lemma

- $1 \leq n$ *for all* $n \in \mathbb{N}$*.*
- *For all* $k, n \in \mathbb{N}$, $k < n + 1$ *if and only if* $k < n$ *or* $k = n$*.*

## Theorem

$\mathbb{N}$ *is a linearly ordered set.*

# Examples

- For all $n \in \mathbb{N}$, $(3|n^3 - n)$.

## Examples

- For all $n \in \mathbb{N}$, $(3|n^3 - n)$.
- $n = 1$, $1^3 - 1 = 0$ and $3|0$.

# Examples

- For all $n \in \mathbb{N}$, $(3|n^3 - n)$.
- $n = 1$, $1^3 - 1 = 0$ and $3|0$.
- $n > 1$

| Given | Goal |
|---|---|
| $n \in \mathbb{N}$ | $\exists j \in \mathbb{Z}(3j = (n+1)^3 - (n+1))$ |
| $\exists k \in \mathbb{Z}(3k = n^3 - n)$ | |

# Examples

- For all $n \in \mathbb{N}$, $(3|n^3 - n)$.
- $n = 1$, $1^3 - 1 = 0$ and $3|0$.
- $n > 1$

| Given | Goal |
|---|---|
| $n \in \mathbb{N}$ | $\exists j \in \mathbb{Z}(3j = (n+1)^3 - (n+1))$ |
| $\exists k \in \mathbb{Z}(3k = n^3 - n)$ | |

- Guess $j$.

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

- Let $R$ be a partial order on $A$. Prove that each finite nonempty subset $B$ has an $R$-minimal element

$$\forall n \geq 1, \forall B \subset A(B \text{ has finitely many elements }) \rightarrow \\ B \text{ has an } R\text{-minimal element}$$

- Let $R$ be a partial order on $A$. Prove that each finite nonempty subset $B$ has an $R$-minimal element

$$\forall n \geq 1, \forall B \subset A(B \text{ has finitely many elements }) \rightarrow \\ B \text{ has an } R\text{-minimal element}$$

- For $n = 1$, this is true.

- Let $R$ be a partial order on $A$. Prove that each finite nonempty subset $B$ has an $R$-minimal element

$$\forall n \geq 1, \forall B \subset A(B \text{ has finitely many elements }) \rightarrow \\ B \text{ has an } R\text{-minimal element}$$

- For $n = 1$, this is true.
- Given $n \geq 1$,

$$\forall B \subset A(B \text{ has } n \text{ elements }) \rightarrow B \text{ has an } R\text{-minimal element}$$

- Let $R$ be a partial order on $A$. Prove that each finite nonempty subset $B$ has an $R$-minimal element

$$\forall n \geq 1, \forall B \subset A(B \text{ has finitely many elements }) \rightarrow \\ B \text{ has an } R\text{-minimal element}$$

- For $n = 1$, this is true.
- Given $n \geq 1$,

$$\forall B \subset A(B \text{ has } n \text{ elements }) \rightarrow B \text{ has an } R\text{-minimal element}$$

- Goal:

$$\forall B \subset A(B \text{ has } n+1 \text{ elements }) \rightarrow B \text{ has an } R\text{-minimal element}$$

- Let $R$ be a partial order on $A$. Prove that each finite nonempty subset $B$ has an $R$-minimal element

$$\forall n \geq 1, \forall B \subset A(B \text{ has finitely many elements }) \rightarrow \\ B \text{ has an } R\text{-minimal element}$$

- For $n = 1$, this is true.
- Given $n \geq 1$,

$$\forall B \subset A(B \text{ has } n \text{ elements }) \rightarrow B \text{ has an } R\text{-minimal element}$$

- Goal:

$$\forall B \subset A(B \text{ has } n+1 \text{ elements }) \rightarrow B \text{ has an } R\text{-minimal element}$$

- Let $B' = B - b$ for an element of $B$. $B'$ has a minimal element $c$. $c \neq b$.

- Let $R$ be a partial order on $A$. Prove that each finite nonempty subset $B$ has an $R$-minimal element

$$\forall n \geq 1, \forall B \subset A(B \text{ has finitely many elements }) \rightarrow \\ B \text{ has an } R\text{-minimal element}$$

- For $n = 1$, this is true.
- Given $n \geq 1$,

$$\forall B \subset A(B \text{ has } n \text{ elements }) \rightarrow B \text{ has an } R\text{-minimal element}$$

- Goal:

$$\forall B \subset A(B \text{ has } n+1 \text{ elements }) \rightarrow B \text{ has an } R\text{-minimal element}$$

- Let $B' = B - b$ for an element of $B$. $B'$ has a minimal element $c$. $c \neq b$.
- Either we have $bRc$ or $\neg bRc$.

## Case 1 $bRc$

- | Given | Goal |
  |---|---|
  | $bRc$ | $b$ is the $R$-minimal element of $B$ |

# Case 1 $bRc$

- | Given | Goal |
  |---|---|
  | $bRc$ | $b$ is the $R$-minimal element of $B$ |

- | Given | Goal |
  |---|---|
  | $bRc$ | contradiction |
  | $b$ is not the $R$-minimal element of $B$ | |
  | $xRb, x \neq b$ | |

# Case 1 $bRc$

- | Given | Goal |
  |---|---|
  | $bRc$ | $b$ is the $R$-minimal element of $B$ |

- | Given | Goal |
  |---|---|
  | $bRc$ | contradiction |
  | $b$ is not the $R$-minimal element of $B$ | |
  | $xRb, x \neq b$ | |

- Then $x \in B'$. Since $xRb$ and $bRc$, we obtain $xRc$.

# Case 1 $bRc$

- | Given | Goal |
  |---|---|
  | $bRc$ | $b$ is the $R$-minimal element of $B$ |

- | Given | Goal |
  |---|---|
  | $bRc$ | contradiction |
  | $b$ is not the $R$-minimal element of $B$ | |
  | $xRb, x \neq b$ | |

- Then $x \in B'$. Since $xRb$ and $bRc$, we obtain $xRc$.
- Since $c$ is $R$-minimal in $B'$, $x = c$.

# Case 1 $bRc$

- 

| Given | Goal |
|---|---|
| $bRc$ | $b$ is the $R$-minimal element of $B$ |

- 

| Given | Goal |
|---|---|
| $bRc$ | contradiction |
| $b$ is not the $R$-minimal element of $B$ | |
| $xRb, x \neq b$ | |

- Then $x \in B'$. Since $xRb$ and $bRc$, we obtain $xRc$.
- Since $c$ is $R$-minimal in $B'$, $x = c$.
- Hence $cRb$ by $xRb$. We also have $bRc$, we have $c = b$ contradiction.

# Case 2 $\neg bRc$

- | Given | Goal |
  |---|---|
  | $\neg bRc$ | $c$ is the $R$-minimal element of $B$ |

# Case 2 $\neg bRc$

- | Given | Goal |
  | --- | --- |
  | $\neg bRc$ | $c$ is the $R$-minimal element of $B$ |

- | Given | Goal |
  | --- | --- |
  | $\neg bRc$ | contradiction |
  | $c$ is not the $R$-minimal element of $B$ | |

# Case 2 $\neg bRc$

- | Given | Goal |
  | --- | --- |
  | $\neg bRc$ | $c$ is the $R$-minimal element of $B$ |

- | Given | Goal |
  | --- | --- |
  | $\neg bRc$ | contradiction |
  | $c$ is not the $R$-minimal element of $B$ | |

- $\exists x \in B(xRc \wedge x \neq c)$.

## Case 2 $\neg bRc$

- | Given | Goal |
  |---|---|
  | $\neg bRc$ | $c$ is the $R$-minimal element of $B$ |

- | Given | Goal |
  |---|---|
  | $\neg bRc$ | contradiction |
  | $c$ is not the $R$-minimal element of $B$ | |

- $\exists x \in B(xRc \wedge x \neq c)$.
- $x \notin B'$ since $c$ is the minimal of $B'$.

# Case 2 $\neg bRc$

- | Given | Goal |
  | --- | --- |
  | $\neg bRc$ | $c$ is the $R$-minimal element of $B$ |

- | Given | Goal |
  | --- | --- |
  | $\neg bRc$ | contradiction |
  | $c$ is not the $R$-minimal element of $B$ | |

- $\exists x \in B(xRc \wedge x \neq c)$.
- $x \notin B'$ since $c$ is the minimal of $B'$.
- Thus, $x = b$. $\neg bRc$. A contradiction.

# Recursions

## Theorem

*(Recursion Theorem) Given a function* $g : A \times \mathbb{N} \to A$*,* $a \in A$*, There exists a unique function* $f : \mathbb{N} \to A$ *such that*

- $f(1) = a$.
- $f(n+1) = g(f(n), n)$ *for all* $n \in N$.

# Recursions

## Theorem

*(Recursion Theorem) Given a function $g : A \times \mathbb{N} \to A$, $a \in A$, There exists a unique function $f : \mathbb{N} \to A$ such that*

- $f(1) = a$.
- $f(n+1) = g(f(n), n)$ *for all* $n \in N$.

## Definition

$f$ is said to be *recursively defined function*. In general recursive functions are more general than this. (See Shoenfield Ch. 6).

# Recursions

## Theorem

*(Recursion Theorem) Given a function* $g : A \times \mathbb{N} \to A$*,* $a \in A$*, There exists a unique function* $f : \mathbb{N} \to A$ *such that*

- $f(1) = a$*.*
- $f(n+1) = g(f(n), n)$ *for all* $n \in N$*.*

## Definition

$f$ is said to be *recursively defined function*. In general recursive functions are more general than this. (See Shoenfield Ch. 6).

## Example

The definition of $f(n) = n!$.

- $f(1) = 1$.
- For all $n$, $f(n+1) = (n+1)f(n)$.

# Example

- Define $a^1 = a$ and $a^{n+1} = a^n a$ inductively.

# Example

- Define $a^1 = a$ and $a^{n+1} = a^n a$ inductively.
- $a \in \mathbb{R}$. $n, m \in \mathbb{N}$, Prove $a^{m+n} = a^m a^n$.

# Example

- Define $a^1 = a$ and $a^{n+1} = a^n a$ inductively.
- $a \in \mathbb{R}$. $n, m \in \mathbb{N}$, Prove $a^{m+n} = a^m a^n$.
- $\forall a \in \mathbb{R} \forall m \in \mathbb{N} \forall n \in \mathbb{N} (a^{m+n} = a^m a^n)$.

# Example

- Define $a^1 = a$ and $a^{n+1} = a^n a$ inductively.
- $a \in \mathbb{R}$. $n, m \in \mathbb{N}$, Prove $a^{m+n} = a^m a^n$.
- $\forall a \in \mathbb{R} \forall m \in \mathbb{N} \forall n \in \mathbb{N}(a^{m+n} = a^m a^n)$.
-

| Given | Goal |
|---|---|
| $a, m, n$ | $a^{m+n} = a^m a^n$ |

# Example

- Define $a^1 = a$ and $a^{n+1} = a^n a$ inductively.
- $a \in \mathbb{R}$. $n, m \in \mathbb{N}$, Prove $a^{m+n} = a^m a^n$.
- $\forall a \in \mathbb{R} \forall m \in \mathbb{N} \forall n \in \mathbb{N} (a^{m+n} = a^m a^n)$.
- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ a, m, n & a^{m+n} = a^m a^n \end{array}$$
- For $n = 1$, true by definition:

$$\begin{array}{cc} \text{Given} & \text{Goal} \\ a, m, n = 1 & a^{m+1} = a^m a \end{array}$$

## Example

- For $n > 1$

| Given | Goal |
|---|---|
| $a, m$ | $\forall n \in \mathbb{N}(a^{m+n} = a^m a^n) \to (a^{m+n+1} = a^m a^{n+1})$ |

## Example

- For $n > 1$

$$\begin{array}{cc} \text{Given} & \text{Goal} \\ a, m & \forall n \in \mathbb{N}(a^{m+n} = a^m a^n) \rightarrow (a^{m+n+1} = a^m a^{n+1}) \end{array}$$

- 

$$\begin{array}{cc} \text{Given} & \text{Goal} \\ a, m & a^{m+n+1} = a^m a^{n+1} \\ n \in N, (a^{m+n} = a^m a^n) & \end{array}$$

# Example

- For $n > 1$

$$\begin{array}{cc} \text{Given} & \text{Goal} \\ a, m & \forall n \in \mathbb{N}(a^{m+n} = a^m a^n) \to (a^{m+n+1} = a^m a^{n+1}) \end{array}$$

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ a, m & a^{m+n+1} = a^m a^{n+1} \\ n \in N, (a^{m+n} = a^m a^n) & \end{array}$$

- $a^{m+n+1} = a^{m+n} a = a^m a^n a = a^m a^{n+1}$.

# Strong induction

## Definition

$$\forall n \in \mathbb{N} P(n)$$

can be shown by

$$\forall n((\forall k < n P(k)) \to P(n))$$

# Strong induction

## Definition

$$\forall n \in \mathbb{N} P(n)$$

can be shown by

$$\forall n((\forall k < n P(k)) \rightarrow P(n))$$

## Theorem

*(The well-ordering principle) Every nonempty set of $\mathbb{N}$ has a smallest element.*

# Strong induction

## Definition

$$\forall n \in \mathbb{N} P(n)$$

can be shown by

$$\forall n((\forall k < n P(k)) \rightarrow P(n))$$

## Theorem

*(The well-ordering principle) Every nonempty set of $\mathbb{N}$ has a smallest element.*

$$\forall S \subset \mathbb{N}((S \neq \emptyset) \rightarrow S \text{ has a smallest element. })$$

# Strong induction

## Definition

$$\forall n \in \mathbb{N} P(n)$$

can be shown by

$$\forall n((\forall k < n P(k)) \to P(n))$$

## Theorem

*(The well-ordering principle) Every nonempty set of $\mathbb{N}$ has a smallest element.*

$$\forall S \subset \mathbb{N}((S \neq \emptyset) \to S \text{ has a smallest element. })$$

We prove

$$\forall S \subset \mathbb{N}(S \text{ has no smallest element} \to S = \emptyset)$$

## Proof.

- Goal: $\forall n \in \mathbb{N}, n \notin S$.

$\square$

Proof.

- Goal: $\forall n \in \mathbb{N}, n \notin S$.
- $n = 1$. Then $S = \{1, ...\}$. True.

$\square$

## Proof.

- Goal: $\forall n \in \mathbb{N}, n \notin S$.
- $n = 1$. Then $S = \{1, ...\}$. True.
- We show $\forall n((\forall k < n(k \notin S)) \rightarrow (n \notin S))$.

$\square$

## Proof.

- Goal: $\forall n \in \mathbb{N}, n \notin S$.
- $n = 1$. Then $S = \{1, ...\}$. True.
- We show $\forall n((\forall k < n(k \notin S)) \rightarrow (n \notin S))$.
- 

| Given | Goal |
|---|---|
| $\forall S \subset \mathbb{N}$ | $n \notin S$ |
| $S$ has no smallest element | |
| $\forall k < n(k \notin S)$ | |

$\square$

## Proof.

- Goal: $\forall n \in \mathbb{N}, n \notin S$.
- $n = 1$. Then $S = \{1, ...\}$. True.
- We show $\forall n((\forall k < n(k \notin S)) \rightarrow (n \notin S))$.
- | Given | Goal |
  | --- | --- |
  | $\forall S \subset \mathbb{N}$ | $n \notin S$ |
  | $S$ has no smallest element | |
  | $\forall k < n(k \notin S)$ | |
- | Given | Goal |
  | --- | --- |
  | $\forall S \subset \mathbb{N}$ | contradiction |
  | $S$ has no smallest element | |
  | $\forall k < n(k \notin S), n \in S$ | |

$\square$

## Proof.

- Goal: $\forall n \in \mathbb{N}, n \notin S$.
- $n = 1$. Then $S = \{1, ...\}$. True.
- We show $\forall n((\forall k < n(k \notin S)) \rightarrow (n \notin S))$.
- | Given | Goal |
  |---|---|
  | $\forall S \subset \mathbb{N}$ | $n \notin S$ |
  | $S$ has no smallest element | |
  | $\forall k < n(k \notin S)$ | |
- | Given | Goal |
  |---|---|
  | $\forall S \subset \mathbb{N}$ | contradiction |
  | $S$ has no smallest element | |
  | $\forall k < n(k \notin S), n \in S$ | |
- $n$ is a minimal element of $S$. $S$ is totally ordered. $n$ is a smallest element. Thus contradiction arises.

□

# Closures

## Definition

Let $R$ be a relation on $A$. Define recursively $R^1 = R$. $R^{n+1} = R^n \circ R$.

# Closures

## Definition

Let $R$ be a relation on $A$. Define recursively $R^1 = R$. $R^{n+1} = R^n \circ R$.

## Lemma

$R^{m+n} = R^m \circ R^n$.

# Closures

## Definition

Let $R$ be a relation on $A$. Define recursively $R^1 = R$. $R^{n+1} = R^n \circ R$.

## Lemma

$R^{m+n} = R^m \circ R^n$.

## Theorem

*The transitive closure of R is* $\bigcup_{n\in\mathbb{N}} R^n$.

**Proof.**

- Let $S = \bigcup_{n \in \mathbb{N}} R^n$.

$\square$

**Proof.**

- Let $S = \bigcup_{n \in \mathbb{N}} R^n$.
- Transitive: $(x, y) \in S, (y, z) \in S$. Then $(x, y) \in R^m, (y, z) \in R^n$. Thus $(x, z) \in R^m \circ R^n = R^{m+n} \subset S$.

$\square$

**Proof.**

- Let $S = \bigcup_{n \in \mathbb{N}} R^n$.
- Transitive: $(x, y) \in S, (y, z) \in S$. Then $(x, y) \in R^m, (y, z) \in R^n$. Thus $(x, z) \in R^m \circ R^n = R^{m+n} \subset S$.
- Closure: Let $T$ be a transtive relation $\supset R$. We show $S \subset T$.

$\square$

## Proof.

- Let $S = \bigcup_{n\in\mathbb{N}} R^n$.
- Transitive: $(x, y) \in S, (y, z) \in S$. Then $(x, y) \in R^m, (y, z) \in R^n$. Thus $(x, z) \in R^m \circ R^n = R^{m+n} \subset S$.
- Closure: Let $T$ be a transtive relation $\supset R$. We show $S \subset T$.
- We show for all $n \in \mathbb{N}(R^n \subset T)$.

$\square$

## Proof.

- Let $S = \bigcup_{n \in \mathbb{N}} R^n$.
- Transitive: $(x, y) \in S, (y, z) \in S$. Then $(x, y) \in R^m, (y, z) \in R^n$. Thus $(x, z) \in R^m \circ R^n = R^{m+n} \subset S$.
- Closure: Let $T$ be a transtive relation $\supset R$. We show $S \subset T$.
- We show for all $n \in \mathbb{N}(R^n \subset T)$.
- for $n = 1$. True,

$\square$

## Proof.

- Let $S = \bigcup_{n \in \mathbb{N}} R^n$.
- Transitive: $(x, y) \in S, (y, z) \in S$. Then $(x, y) \in R^m, (y, z) \in R^n$. Thus $(x, z) \in R^m \circ R^n = R^{m+n} \subset S$.
- Closure: Let $T$ be a transtive relation $\supset R$. We show $S \subset T$.
- We show for all $n \in \mathbb{N}(R^n \subset T)$.
- for $n = 1$. True,
- $\forall n \in \mathbb{N}(R^n \subset T \rightarrow R^{n+1} \subset T)$.

$\square$

## Proof.

- Let $S = \bigcup_{n\in\mathbb{N}} R^n$.
- Transitive: $(x, y) \in S, (y, z) \in S$. Then $(x, y) \in R^m, (y, z) \in R^n$. Thus $(x, z) \in R^m \circ R^n = R^{m+n} \subset S$.
- Closure: Let $T$ be a transtive relation $\supset R$. We show $S \subset T$.
- We show for all $n \in \mathbb{N}(R^n \subset T)$.
- for $n = 1$. True,
- $\forall n \in \mathbb{N}(R^n \subset T \to R^{n+1} \subset T)$.
- Omit

$\square$