1 Introduction

About this lecture

- Proof strategies
- Proofs involving negations and conditionals.
- Proofs involving quantifiers
- Proofs involving conjunctions and biconditionals (up to here in this lecture.)
- Proofs involving disjunctions
- Existence and uniqueness proof
- More examples of proofs..
- 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.
- A mathematical introduction to logic, H. Enderton, Academic Press.
- `http://plato.stanford.edu/contents.html` has much resource.
- Introduction to set theory, Hrbacek and Jech, CRC Press.
- Thinking about Mathematics: The Philosophy of Mathematics, S. Shapiro, Oxford. 2000.

Some helpful references

- `http://en.wikipedia.org/wiki/Truth_table`,
- `http://logik.phl.univie.ac.at/~chris/gateway/formular-uk-zentral.html`, complete (i.e. has all the steps)
- `http://svn.oriontransfer.org/TruthTable/index.rhtml`, has xor, complete.

2 Proof strategies

Proof strategies

- A mathematician and/or logicians use many methods to obtain results: These includes guessing, finding examples and counter-examples, experimenting with computations, analogies, physical experiments, and thought experiments (like pictures).
- Sometimes proofs involve constructions, i.e., the proof of polynomial root existences by Gauss.
- However, the only results that the mathematicians accept are given by logical deductions from the set theoretical foundations. (This includes finding counter-examples by guessing)
- There are some controversies as to whether the ZFC is the only foundation.
- Other fields such as numerical mathematics, physics, and so on have different standards.
- Because of these differences of standards, it is often very hard to communicate with other fields.

- Finding proofs are hard: example: Fermat's conjecture...
- Finding a proof is an art. However, there are hints.
- Most proofs that you have to do have no more than 5-6 steps.
- In this book, the proof strategies are divided into
- for a given of form: $\neg P, P \wedge Q.P \vee Q.P \rightarrow Q, P \leftrightarrow Q, \forall x P(x), \exists x P(x), \exists! x P(x)$.
- for a goal of form: $\neg P, P \wedge Q, P \vee Q, P \rightarrow Q, P \leftrightarrow Q, \forall x P(x), \forall n \in \mathbb{N} P(n), \exists x P(x), \exists! x P(x)$.

- We use a "structural method" in this book. The method is that of divide and conquer or "Top down" approach.
- This means breaking down the proof into smaller and smaller pieces which are easier to prove or already proven by someone else.
- Never assert anything until you can justify it fully using hypothesis or the conclusions reached earlier.
- The basic assumption we will have in mathematics is the ZFC.
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are the important sets.

3 Proofs involving negations and conditionals.

To prove the form $P \to Q$

- First method: Assume P and prove Q. Or add P to the list of hypothesis and prove Q.
Given	Goal
$----$	$P \to Q$
$----$	
- Change to

Given	Goal
$----$	Q
$----$	
P	
- Example $0 < a < b \to a^2 < b^2$.
Given	Goal
$---$	$0 < a < b \to a^2 < b^2$
$----$	
- Change to

Given	Goal
$----$	$a^2 < b^2$
$----$	
$0 < a < b$	
Given	Goal
$0 < a < b$	$a^2 < b^2$
$0 < a^2 < ab$	
$0 < ab < b^2$	

To prove $P \to Q$

- $P \to Q \leftrightarrow \neg Q \to \neg P$.
- Second method: Assume $\neg Q$ and prove $\neg P$.
Given	Goal
$----$	$P \to Q$
$----$	

- Change to

$$\begin{array}{cc} \text{Given} & \text{Goal} \\ ---- & \neg P \\ ---- & \\ \neg Q & \end{array}$$

- Example: Let $a > b$. Then if $ac \leq bc$, then $c \leq 0$.

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ a, b, c \text{ are real numbers} & (ac \leq bc) \to (c \leq 0) \\ a > b & \end{array}$$

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ a, b, c \text{ are real numbers} & ac > bc \\ a > b & \\ c > 0 & \end{array}$$

Write this in English

- Theorem: Let $a > b$. Then if $ac \leq bc$, then $c \leq 0$.

- Proof: We will prove this by contrapositives. To prove $ac \leq bc \to c \leq 0$. It is sufficient to prove $c > 0 \to ac > bc$. Suppose $c > 0$. Then $ac > bc$ by $a > b$. $\square$

To prove a goal of the form $\neg P$.

- First method: Try to re-express $\neg P$ in some other form. (in a positive form)

- Example: Suppose that $A \cap C \subset B$ and $a \in C$. Prove $a \notin A - B$.

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ A \cap C \subset B & a \notin A - B \\ a \in C & \end{array}$$

- We change $a \notin A - B$.

- $a \notin A - B \leftrightarrow \neg(a \in A \wedge b \notin B). \leftrightarrow (a \notin A \vee a \in B). \leftrightarrow (a \in A \to a \in B)$.

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ A \cap C \subset B & a \in A \to a \in B \\ a \in C & \end{array}$$

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ A \cap C \subset B & a \in B \\ a \in C & \\ a \in A & \end{array}$$

- Theorem: Suppose that $A \cap C \subset B$ and $a \in C$. Prove $a \notin A - B$.

- Proof: To show $a \notin A - B$, it is equivalent to show $a \in A \to a \in B$. (See above). Assume $a \in A$. Since $A \cap C \subset B$ and $a \in C$, it follows that $a \in B$. $\square$

To prove a goal of the form $\neg P$.

- Second method: Assume P and find a contradiction:

- As above: Show $A \cap C \subset B$, $a \in C$. Prove $a \notin A - B$.

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ A \cap C \subset B & a \notin A - B \\ a \in C & \end{array}$$

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ A \cap C \subset B & \text{contradiction} \\ a \in C & \\ a \in A - B & \end{array}$$

To prove a goal of the form $\neg P$.

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ A \cap C \subset B & \text{contradiction} \\ a \in C & \\ a \in A - B & \\ a \in (A \cap C) - B & \\ a \in \emptyset & \end{array}$$

To use a given of the form $\neg P$.

- First method: If we are doing a proof by contradiction, then use P as the goal.

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ \neg P & contradiction \\ ---- & \end{array}$$

- Change to

Given	Goal
$\neg P$	P
$----$	

- Second method: re-express in some other form (positive form)

To use the given of the form $P \to Q$

- Use modus ponens $P, P \to Q \vdash Q$.
- Use modus tollens $P \to Q, \neg Q \vdash \neg P$.
- Example: Suppose $A \subset B, a \in A$, and a and b are not both elements of B. Prove $b \notin B$.
-

Given	Goal
$A \subset B$	$b \notin B$
$a \in A$	
$\neg(a \in B \wedge b \in B)$	

-

Given	Goal
$A \subset B$	$b \notin B$
$a \in A$	
$(a \in B \to b \notin B)$	

-

Given	Goal
$A \subset B$	$b \notin B$
$a \in A$	
$(a \in B \to b \notin B)$	
$a \in B$	

- Theorem: Suppose $A \subset B, a \in A$, and a and b are not both elements of B. Then $b \notin B$.
- Proof: Since a and b are not both elements of B, it follows that if a is an element of B, then b is not an element of B. Since $a \in A$, we have $a \in B$. Thus b is not an element of B. $\square$

4 Proofs involving quantifiers

To show a goal of the form $\forall x P(x)$

- We introduce some arbitrary variable x in the assumption and prove $P(x)$.
-
Given	Goal
$----$	$\forall x P(x)$
$----$	

-
Given	Goal
$----$	$P(x)$
$----$	
x is an arbitrary variable.	

Examples

- A, B, C are sets. $A - B \subset C$. Prove $A - C \subset B$.
-
Given	Goal
$A - B \subset C$	$A - C \subset B$

-
Given	Goal
$\forall x(x \in A - B \to x \in C)$	$\forall x(x \in A - C \to x \in B)$

-
Given	Goal
$\forall x(x \in A - B \to x \in C)$	$x \in A - C \to x \in B$
x arbitrary	

Examples

-
Given	Goal
$\forall x(x \in A - B \to x \in C)$	$x \in B$
x arbitrary	
$x \in A - C$	

-
Given	Goal
$\forall x(x \in A - B \to x \in C)$	contradiction
$x \in A$	
$x \notin C$	
$x \notin B$	

Given	Goal
$\forall x(x \in A - B \to x \in C)$	$x \in C$
$x \in A$	
$x \notin C$	
$x \notin B$	

- Read the English proof also.

To prove a goal of form $\exists x P(x)$

- We guess x and show $P(x)$.
Given	Goal
$----$	$\exists x P(x)$
$----$	

Given	Goal
$----$	$P(x)$
$----$	
x the value you decided	

- $\exists x, |x^2 - 1| < 1/2$.
Given	Goal
$x \in \mathbb{R}$	$\exists x, |x^2 - 1| < 1/2$

Given	Goal
$x \in \mathbb{R}$	$\exists x, |x^2 - 1| < 1/2$
$x = 1.1$	$(x^2 = 1.21, |x^2 - 1| = 0.21 < 1/2)$

To use a given of form $\exists x P(x)$ or $\forall x P(x)$

- $\exists x P(x)$: Introduce new variable x_0. $P(x_0)$ is true (existential instantiation)
- $\forall x P(x)$: wait until a particular value a for x to pop-up and use $P(a)$.
- Example: $\mathcal{F}, \mathcal{G}$ families of sets. Suppose that $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Then $\bigcap \mathcal{F} \subset \bigcup \mathcal{G}$.
Given	Goal
$\mathcal{F} \cap \mathcal{G} \neq \emptyset$	$\forall x(x \in \bigcap \mathcal{F} \to x \in \bigcup \mathcal{G})$

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ \mathcal{F} \cap \mathcal{G} \neq \emptyset & x \in \bigcup \mathcal{G} \\ x \in \bigcap \mathcal{F} & \end{array}$$

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ \exists A(A \in \mathcal{F} \cap \mathcal{G}) & \exists A \in \mathcal{G}(x \in A) \\ \forall A \in \bigcap \mathcal{F}(x \in A) & \end{array}$$

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ A_0 \in \mathcal{F} & \exists A \in \mathcal{G}(x \in A) \\ A_0 \in \mathcal{G} & \\ \forall A \in \bigcap \mathcal{F}(x \in A) & \\ x \in A_0 & \end{array}$$

- $$\begin{array}{cc} \text{Given} & \text{Goal} \\ A_0 \in \mathcal{F} & \exists A \in \mathcal{G}(x \in A) \\ A_0 \in \mathcal{G} & \\ \forall A \in \bigcap \mathcal{F}(x \in A) & \\ x \in A_0 & (\text{ Use } A = A_0) \end{array}$$

- Theorem: Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets. $\mathcal{F} \cap \mathcal{G} = \emptyset$. Then $\bigcap \mathcal{F} \subset \bigcup \mathcal{G}$.

- Proof: Suppose $x \in \bigcap \mathcal{F}$. Since $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Let A_0 be the common element. Then $A_0 \in \mathcal{F}$. Thus, $x \in A_0$ as $A_0 \in \mathcal{F}$. Since $A_0 \in \mathcal{G}$, then $x \in \bigcup G$. $\square$

Proofs involving conjunctions and biconditionals

- To prove a goal of the form $P \wedge Q$: Prove P and Q separately.
- To use $P \wedge Q$: Regard as P and Q.
- To prove a goal $P \leftrightarrow Q$: Prove $P \rightarrow Q$ and $Q \rightarrow P$.
- To use $P \leftrightarrow Q$: Treat as two givens $P \rightarrow Q$ and $Q \rightarrow P$.

Example

- Prove $\forall x \neg P(x) \leftrightarrow \neg \exists x P(x)$.
- Prove $\rightarrow$: $\forall x \neg P(x) \rightarrow \neg \exists x P(x)$

-

Given	Goal
$\forall x \neg P(x)$	contradiction
$\exists x P(x)$	

-

Given	Goal
$\forall x \neg P(x)$	contradiction
$P(x_0)$	

-

Given	Goal
$\forall \neg P(x)$	contradiction
$P(x_0)$	
$\neg P(x_0)$	

Example

- Prove $\forall x \neg P(x) \leftrightarrow \neg \exists x P(x)$.
- Prove $\leftarrow$: $\neg \exists x P(x) \rightarrow \forall x \neg P(x)$
-

Given	Goal
$\neg \exists x P(x)$	$\forall x \neg P(x)$

-

Given	Goal
$\neg \exists x P(x)$	$\neg P(x)$
x arbitrary	

-

Given	Goal
$\neg \exists x P(x)$	contradiction
x arbitrary	
$P(x)$	

-

Given	Goal
$\neg \exists x P(x)$	$\exists x P(x)$
x arbitrary	
$P(x)$	

- Theorem: $\forall x \neg P(x) \leftrightarrow \neg \exists x P(x)$.
- Proof: $(\rightarrow)$ Suppose $\forall x \neg P(x)$ and suppose $\exists x P(x)$. We choose x_0 such that $P(x_0)$ is true. Since $\forall x \neg P(x)$, we know $\neg P(x_0)$. This is a contradiction. Thus, $\forall x \neg P(x) \rightarrow \neg \exists x P(x)$.

- Proof: ($\leftarrow$) Suppose $\neg\exists x P(x)$. Let x be arbitrary. Suppose that $P(x)$. Then $\exists x P(x)$. This is a contradiction. Thus $\neg P(x)$ is true. Since x was arbitrary, we have $\forall x \neg P(x)$. $\square$