Chapter 3

Formal Proofs

Bahar Aameri
Department of Computer Science
University of Toronto

Feb 06, 2015
Today’s Topics

- Last Lecture: Exercise on Proof by Cases
- Non-Boolean Functions in Logical Statements
- Substituting Known Results
- Inference Rules: Building/Breaking Formulas
Chapter 3

Formal Proofs

Exercise on Proof by Cases
Proof by Cases

Exercise

Prove that the square of a natural is a multiple of 3 or a multiple of 3 plus 1.

Solution

- **Step 1:** Translate the claim to logical notation.
  - $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n^2 = 3k) \lor (\exists k \in \mathbb{N}, n^2 = 3k + 1)$.

- **Step 2:** Find a plan for the proof:
  - Consider three cases: $n = 3k$ or $n = 3k + 1$ or $n = 3k + 2$.

- **Step 3:** Translate the assumptions/facts to logical notation
  - $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n = 3k \lor n = 3k + 1 \lor n = 3k + 2)$.

- **Step 4:** Choose an appropriate proof structure. Use the assumptions/facts to prove the claim.
Proof by Cases

Structure

- **Disjunction in the assumptions** $\rightarrow$ proof by cases
- **Disjunction in the claim** $\rightarrow$ proof structure for disjunction

Assumption: $P \lor Q$.

Claim: $S \lor R$.

Assume $P \lor Q$

Case 1: Assume $P$.

\[ \therefore \text{prove } R \]

Then $R$.

Case 2: Assume $Q$.

\[ \therefore \text{prove } S \]

Then $S$.

Thus $R \lor S$. $\#$ introduce disjunction
Proof by Cases

Solution

Assume \( n \in \mathbb{N} \). \# \( n \) is a typical element of \( \mathbb{N} \)
Then \( \exists k \in \mathbb{N}, n = 3k \lor n = 3k + 1 \lor n = 3k + 2 \). \# properties of \( \mathbb{N} \)

\[
\vdash
\]

Then \( (\exists k \in \mathbb{N}, n^2 = 3k) \lor (\exists k \in \mathbb{N}, n^2 = 3k + 1) \). \# true in all possible cases
Then \( \forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n^2 = 3k) \lor (\exists k \in \mathbb{N}, n^2 = 3k + 1) \). \# introduction of \( \forall \)
Proof by Cases

Solution

Assume $n \in \mathbb{N}$. # $n$ is a typical element of $\mathbb{N}$

Then $\exists k \in \mathbb{N}, n = 3k \lor n = 3k + 1 \lor n = 3k + 2$. # properties of $\mathbb{N}$

Let $k_0 \in \mathbb{N}$ be such that $n = 3k_0 \lor n = 3k_0 + 1 \lor n = 3k_0 + 2$. # instantiate $\exists$

Then $(\exists k \in \mathbb{N}, n^2 = 3k) \lor (\exists k \in \mathbb{N}, n^2 = 3k + 1)$. # true in all possible cases

Then $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n^2 = 3k) \lor (\exists k \in \mathbb{N}, n^2 = 3k + 1)$. # introduction of $\forall$
Proof by Cases

Solution

Assume $n \in \mathbb{N}$. $\#$ $n$ is a typical element of $\mathbb{N}$

Then $\exists k \in \mathbb{N}, n = 3k \lor n = 3k + 1 \lor n = 3k + 2$. $\#$ properties of $\mathbb{N}$

Let $k_0 \in \mathbb{N}$ be such that $n = 3k_0 \lor n = 3k_0 + 1 \lor n = 3k_0 + 2$. $\#$ instantiate $\exists$

Case 1: Assume $n = 3k_0$.

Then $n^2 = 9k_0^2 = 3(3k_0^2)$. $\#$ algebra

Then $\exists k \in \mathbb{N}, n^2 = 3k$. $\# k = 3k_0^2, k \in \mathbb{N}$

\[ \vdots \]

Then $(\exists k \in \mathbb{N}, n^2 = 3k) \lor (\exists k \in \mathbb{N}, n^2 = 3k + 1)$. $\#$ true in all possible cases

Then $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n^2 = 3k) \lor (\exists k \in \mathbb{N}, n^2 = 3k + 1)$. $\#$ introduction of $\forall$
Proof by Cases

Solution

Assume $n \in \mathbb{N}$. # $n$ is a typical element of $\mathbb{N}$

Then $\exists k \in \mathbb{N}, n = 3k \lor n = 3k + 1 \lor n = 3k + 2$. # properties of $\mathbb{N}$

Let $k_0 \in \mathbb{N}$ be such that $n = 3k_0 \lor n = 3k_0 + 1 \lor n = 3k_0 + 2$. # instantiate $\exists$

Case 1: Assume $n = 3k_0$.

Then $n^2 = 9k_0^2 = 3(3k_0^2)$. # algebra

Then $\exists k \in \mathbb{N}, n^2 = 3k$. # $k = 3k_0^2, k \in \mathbb{N}$

Case 2: Assume $n = 3k_0 + 1$.

Then $n^2 = 9k_0^2 + 6k + 1 = 3(3k_0^2 + 2k_0) + 1$. # algebra

Then $\exists k \in \mathbb{N}, n^2 = 3k + 1$. # $k = 3k_0^2 + 2k_0, k \in \mathbb{N}$

Then $(\exists k \in \mathbb{N}, n^2 = 3k) \lor (\exists k \in \mathbb{N}, n^2 = 3k + 1)$. # true in all possible cases

Then $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n^2 = 3k) \lor (\exists k \in \mathbb{N}, n^2 = 3k + 1)$. # introduction of $\forall$
Proof by Cases

Solution

Assume $n \in \mathbb{N}$. # $n$ is a typical element of $\mathbb{N}$

Then $\exists k \in \mathbb{N}, n = 3k \lor n = 3k + 1 \lor n = 3k + 2$. # properties of $\mathbb{N}$

Let $k_0 \in \mathbb{N}$ be such that $n = 3k_0 \lor n = 3k_0 + 1 \lor n = 3k_0 + 2$. # instantiate $\exists$

Case 1: Assume $n = 3k_0$.

Then $n^2 = 9k_0^2 = 3(3k_0^2)$. # algebra

Then $\exists k \in \mathbb{N}, n^2 = 3k$. # $k = 3k_0^2, k \in \mathbb{N}$

Case 2: Assume $n = 3k_0 + 1$.

Then $n^2 = 9k_0^2 + 6k + 1 = 3(3k_0^2 + 2k_0) + 1$. # algebra

Then $\exists k \in \mathbb{N}, n^2 = 3k + 1$. # $k = 3k_0^2 + 2k_0, k \in \mathbb{N}$

Case 3: Assume $n = 3k_0 + 2$.

Then $n^2 = 9k_0^2 + 12k + 4 = 3(3k_0^2 + 4k_0 + 1) + 1$. # algebra

Then $\exists k \in \mathbb{N}, n^2 = 3k + 1$. # $k = 3k_0^2 + 4k_0 + 1, k \in \mathbb{N}$

Then $(\exists k \in \mathbb{N}, n^2 = 3k) \lor (\exists k \in \mathbb{N}, n^2 = 3k + 1)$. # true in all possible cases

Then $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n^2 = 3k) \lor (\exists k \in \mathbb{N}, n^2 = 3k + 1)$. # introduction of $\forall$
Chapter 3

Formal Proofs

Non-Boolean Functions in Logical Statements
Non-Boolean Functions in Logical Statements

- Suppose we want to use properties of a non-boolean function: 
  \( \lfloor x \rfloor \) denotes floor of \( x \):
  - \( \lfloor x \rfloor : \mathbb{R} \to \mathbb{Z} \).
  - \( \lfloor x \rfloor \): the largest integer \( \leq x \).

- Non-boolean functions cannot take the place of predicates.

- How can we use them?
  - Use predicates to make and/or verify claims about non-boolean functions.
  - \( \forall x \in \mathbb{R}, \lfloor x \rfloor < x + 1 \).

- non-boolean functions are not:
  - Variables:
    \( \forall \lfloor x \rfloor \in \mathbb{R}, P \) \( \rightarrow \) incorrect
  - Predicates:
    \( \forall x \in \mathbb{R}, \lfloor x \rfloor \lor \lfloor x + 1 \rfloor \) \( \rightarrow \) incorrect
Exercise

Prove $\forall x \in \mathbb{R}, \lfloor x \rfloor < x + 1$.

Assume $x \in \mathbb{R}$. # $x$ is a typical element of $\mathbb{R}$
Then $\lfloor x \rfloor \leq x$. # by definition of floor
Then $\lfloor x \rfloor < x + 1$. # $x < x + 1$ and transitivity of $<$
Then $\forall x \in \mathbb{R}, \lfloor x \rfloor < x + 1$. # introduce $\forall$
Chapter 3

Formal Proofs

Substituting Known Results
Substituting Known Results

- To make proofs shorter and modular, some of the required results might be proved separately, and then be referred to.
- Existing theorems/lemmas can also be reused.

\[ C_1 : \forall y \in \mathbb{R}, y \neq 0 \Rightarrow 1/(y^2 + 2) < 3. \]

**Theorem 1:** \( \forall x \in \mathbb{R}, x > 0 \Rightarrow 1/(x + 2) < 3. \)
Exercise

- Use Theorem 1 to prove $C_1$
- $C_1: \forall y \in \mathbb{R}, y \neq 0 \Rightarrow 1/(y^2 + 2) < 3.$

Theorem 1: $\forall x \in \mathbb{R}, x > 0 \Rightarrow 1/(x + 2) < 3.$

Proof:

Assume $y \in \mathbb{R}$. # $y$ is a typical element of $\mathbb{R}$

Then $\forall y \in \mathbb{R}, y \neq 0 \Rightarrow 1/(y^2 + 2) < 3.$
Substituting Known Results

Use Theorem 1 to prove $C_1$

$C_1 : \forall y \in \mathbb{R}, y \neq 0 \Rightarrow 1/(y^2 + 2) < 3.$

Theorem 1: $\forall x \in \mathbb{R}, x > 0 \Rightarrow 1/(x + 2) < 3.$

Proof:

Assume $y \in \mathbb{R}$. # $y$ is a typical element of $\mathbb{R}$

Assume $y \neq 0$. # antecedent

Then $y^2 \neq 0$. # $y \neq 0$

Then $y^2 \in \mathbb{R}$ and $y^2 \geq 0$. # $\mathbb{R}$ closed under $\times$, squares are $\geq 0$

Then $y^2 > 0$. # $y^2 \geq 0$ and $y^2 \neq 0$.

Then $1/(y^2 + 2) < 3$. # by Theorem 1

Then $y \neq 0 \Rightarrow 1/(y^2 + 2) < 3$. # introduction of $\Rightarrow$

Then $\forall y \in \mathbb{R}, y \neq 0 \Rightarrow 1/(y^2 + 2) < 3$. # introduction of $\forall$
Chapter 3

Formal Proofs

Inference Rules: Building/Breaking Formulas
Most of the times, claims are not just predicates.

We need to be able to reduce claims to simpler statement, or combine simpler statements to build more complex ones.

**Inference Rules:**

- **Introduction Rules:** rules that allow making up more complex logical sentences from simpler ones.

- **Elimination Rules:** rules that allow reducing a logical sentence to simpler sentences.
## Inference Rules: Building/Breaking Formulas

### Introduction Rules

For each rule, if **everything** that is **above** the line is already known/shown, **anything** that is **below** the line can be conclude.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| $\Rightarrow I$ (implication introduction) | (direct) Assume $A$ ... $B$  

$A \Rightarrow B$  

(indirect) Assume $\neg B$ ... $\neg A$  

$A \Rightarrow B$ | $A \Rightarrow B$ | $A \Rightarrow B$ |
| $\iff I$ (bi-implication introduction) | $A \Rightarrow B$  

$B \Rightarrow A$  

$A \iff B$ | $P(a)$  

$a \in D$  

$\exists x \in D, P(x)$ | $P(a)$  

$a \in D$  

$\exists x \in D, P(x)$ |
| $\forall I$ (universal introduction) | Assume $a \in D$  

$\vdots$  

$P(a)$  

$\forall x \in D, P(x)$ | $P(a)$  

$a \in D$  

$\exists x \in D, P(x)$ |
Inference Rules: Building/Breaking Formulas

**Introduction Rules**

- For each rule, if **everything** that is **above** the line is already known/shown, **anything** that is **below** the line can be conclude.

\[-I\] negation introduction:

Assume \( A \)

\[ \begin{array}{c}
\vdash \\
\text{contradiction} \\
\hline
\neg A \\
\end{array} \]

\[\neg I\]

\[\land I\] conjunction introduction:

\[ \begin{array}{c}
A \\
B \\
\hline
A \land B \\
\end{array} \]

\[\lor I\] disjunction introduction:

\[ \begin{array}{c}
A \\
B \\
\hline
A \lor B \\
\end{array} \]

\[A \lor \neg A\]
Inference Rules: Building/Breaking Formulas

Elimination Rules

- For each rule, if **everything** that is **above** the line is already known/shown, **anything** that is **below** the line can be conclude.

\[ \Rightarrow E \] implication elimination:

\[
\begin{array}{c}
(\text{Modus Ponens}) \\
A \Rightarrow B \\
A \\
\hline
B
\end{array}
\]

\[
\begin{array}{c}
(\text{Modus Tollens}) \\
A \Rightarrow B \\
\neg B \\
\hline
\neg A
\end{array}
\]

\[ \Leftarrow E \] bi-implication elimination:

\[
\begin{array}{c}
A \iff B \\
A \Rightarrow B \\
B \Rightarrow A
\end{array}
\]

\[ \forall E \] universal elimination:

\[
\begin{array}{c}
\forall x \in D, P(x) \\
a \in D \\
\hline
P(a)
\end{array}
\]

\[ \exists E \] existential elimination:

\[
\begin{array}{c}
\exists x \in D, P(x) \\
\text{Let } a \in D \text{ such that } P(a) \\
\text{...}
\end{array}
\]
Inference Rules: Building/Breaking Formulas

**Elimination Rules**

- For each rule, if *everything* that is *above* the line is already known/shown, *anything* that is *below* the line can be conclude.

- **[¬E]** negation elimination:

  \[
  \frac{\neg
\neg A}{\neg A \quad A}
  \]

  \[
  \frac{\neg A}{\text{contradiction}}
  \]

- **[∧E]** conjunction elimination:

  \[
  \frac{A \land B}{A \quad B}
  \]

  \[
  \frac{A \land B}{A \quad B}
  \]

- **[∨E]** disjunction elimination:

  \[
  \frac{A \lor B}{\neg A \quad A \lor B}
  \]

  \[
  \frac{\neg A \quad A \lor B}{\neg B \quad A}
  \]