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.
  - $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n^2 = 3k) \vee (\exists k \in \mathbb{N}, n^2 = 3k + 1)$.
- **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
  - $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n = 3k \vee n = 3k + 1 \vee n = 3k + 2)$.
- **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:** $P \vee Q$.
- **Claim:** $S \vee R$.

Assume $P \vee Q$
Case 1: Assume P.
$\vdots$ # prove R
Then R.
Case 2: Assume Q.
$\vdots$ # prove S
Then S.
Thus $R \vee S$.# introduce disjunction

Proof by Cases

Solution

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

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

$\vdots$

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

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

Proof by Cases

Solution

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

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

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

$\vdots$

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

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

Proof by Cases

Solution

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

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

Let $k_0 \in \mathbb{N}$ be such that $n = 3k_0 \vee n = 3k_0 + 1 \vee n = 3k_0 + 2$.# 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 $(\exists k \in \mathbb{N}, n^2 = 3k) \vee (\exists k \in \mathbb{N}, n^2 = 3k + 1)$. # true in all possible cases

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

Proof by Cases

Solution

Assume $n \in \mathbb{N}$. # n is a typical element of $\mathbb{N}$
Then $\exists k \in \mathbb{N}, n = 3k \vee n = 3k+1 \vee n = 3k+2$. # properties of $\mathbb{N}$
Let $k_0 \in \mathbb{N}$ be such that $n = 3k_0 \vee n = 3k_0+1 \vee n = 3k_0+2$. # 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 $\exists k \in \mathbb{N}, n^2 = 3k + 1$. # $k = 3k_0^2 + 2k_0, k \in \mathbb{N}$

$\vdots$

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

Proof by Cases

Solution

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

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

Let $k_0 \in \mathbb{N}$ be such that $n = 3k_0 \vee n = 3k_0 + 1 \vee n = 3k_0 + 2$.# 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 $(\exists k \in \mathbb{N}, n^2 = 3k) \vee (\exists k \in \mathbb{N}, n^2 = 3k+1)$. # true in all possible cases

Then $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n^2 = 3k) \vee (\exists k \in \mathbb{N}, n^2 = 3k+1)$. # 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.
  - $\forall \mathbf{x} \in \mathbb{R}, \lfloor \mathbf{x} \rfloor < \mathbf{x} + \mathbf{1}$.

- non-boolean functions are **not**:
  - **Variables**:
    $\forall \lfloor x \rfloor \in \mathbb{R}, P \quad \to$ **incorrect**
  - **Predicates**:
    $\forall x \in \mathbb{R}, \lfloor x \rfloor \vee \lfloor x + 1 \rfloor \quad \to$ **incorrect**

Non-Boolean Functions in Logical Statements

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

Substituting Known Results

Exercise

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

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 $\mathbb{R}$

$\vdots$

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

Substituting Known Results

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

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 ≥ 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

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.

[$\Rightarrow$I] implication introduction:

(*direct*)

$$\frac{\begin{array}{l}\text{Assume } A\\ \quad\vdots\\ \quad B\end{array}}{A \Rightarrow B}$$

(*indirect*)

$$\frac{\begin{array}{l}\text{Assume } \neg B\\ \quad\vdots\\ \quad \neg A\end{array}}{A \Rightarrow B}$$

[$\forall$I] universal introduction:

$$\frac{\begin{array}{l}\text{Assume } a \in D\\ \quad\vdots\\ \quad P(a)\end{array}}{\forall x \in D, P(x)}$$

[$\Leftrightarrow$I] bi-implication introduction:

$$\frac{\begin{array}{l}A \Rightarrow B\\ B \Rightarrow A\end{array}}{A \Leftrightarrow B}$$

[$\exists$I] existential introduction:

$$\frac{\begin{array}{l}P(a)\\ a \in D\end{array}}{\exists x \in D, P(x)}$$

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:

$$\frac{\begin{array}{l}\text{Assume } A\\ \quad\vdots\\ \quad\text{contradiction}\end{array}}{\neg A}$$

[∨I] disjunction introduction:

$$\frac{A}{\begin{array}{l}A \vee B\\ B \vee A\end{array}} \qquad \frac{}{A \vee \neg A}$$

[∧I] conjunction introduction:

$$\frac{\begin{array}{l}A\\ B\end{array}}{A \wedge B}$$

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:

(*Modus Ponens*)

$$\frac{A \Rightarrow B \qquad A}{B}$$

(*Modus Tollens*)

$$\frac{A \Rightarrow B \qquad \neg B}{\neg A}$$

[$\forall$E] universal elimination:

$$\frac{\forall x \in D, P(x) \qquad a \in D}{P(a)}$$

[$\Leftrightarrow$E] bi-implication elimination:

$$\frac{A \Leftrightarrow B}{A \Rightarrow B \qquad B \Rightarrow A}$$

[$\exists$E] existential elimination:

$$\frac{\exists x \in D, P(x)}{\text{Let } a \in D \text{ such that } P(a)}$$

$\vdots$

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:

$$\frac{\neg\neg A}{A} \qquad \frac{\begin{array}{l} A \\ \neg A \end{array}}{\text{contradiction}}$$

[∨E] disjunction elimination:

$$\frac{\begin{array}{l} A \vee B \\ \neg A \end{array}}{B} \qquad \frac{\begin{array}{l} A \vee B \\ \neg B \end{array}}{A}$$

[∧E] conjunction elimination:

$$\frac{A \wedge B}{\begin{array}{l} A \\ B \end{array}}$$