Chapter 3

Formal Proofs

Bahar Aameri
Department of Computer Science
University of Toronto

Feb 04, 2015

Today's Topics

- **Review: Proof Structures for Quantifiers, Implications and Conjunctions**
- **Proof Structure for Disjunction**
- **Proof by Cases**

Chapter 3

Formal Proofs

Review: Proof Structures for Quantifiers, Implications and Conjunctions

Proof of Multiple Quantifiers

Structure

- Prove $\forall x \in D, \exists y \in E, P(x, y)$

Assume $x \in D$. # x is a typical element of D

    Let $y = \_\_\_\_$. # choose a particular element of the domain

    Then $y \in E$. # this may be obvious, otherwise prove it

    $\vdots$ # prove $P(x, y)$

    Then $P(x, y)$.

    Then $\exists y \in E, P(x, y)$. # introduce existential

Then $\forall x \in D, \exists y \in E, P(x, y)$. # introduce universal

Proof of Multiple Quantifiers

Structure

- Prove $\exists x \in D, \forall y \in E, P(x, y)$

Let $x =$ ____. # choose a particular element of the domain
Then $x \in D$. # this may be obvious, otherwise prove it
Assume $y \in E$. # y is a typical element of E

$\vdots$ # prove $P(x, y)$

Then $P(x, y)$.

Then $\forall x \in D, P(x, y)$. # introduce universal
Then $\exists y \in E, \forall x \in D, P(x, y)$. # introduce existential

Proof of Conjunction

Structure

- Prove $\forall x \in D, P(x) \wedge Q(x)$

  Assume $x \in D$. # x is a typical element of D

  $\vdots$ # prove $P(x)$

  Then $P(x)$.

  $\vdots$ # prove $Q(x)$

  Then $Q(x)$.

  Then $P(x) \wedge Q(x)$. # introduce conjunction

  Then $\forall x \in D, P(x) \wedge Q(x)$. # introduce universal

Chapter 3

Formal Proofs

Proof Structure for Disjunction

Proof of Disjunction

Structure

- Prove $\forall x \in D, P(x) \vee Q(x)$
- Assume $x \in D$. # x is a typical element of D

  $\vdots$ # prove $P(x)$

  Then $P(x)$.

  Then $P(x) \vee Q(x)$. # introduce disjunction

  Then $\forall x \in D, P(x) \vee Q(x)$. # introduce universal
- Assume $x \in D$. # x is a typical element of D

  $\vdots$ # prove $Q(x)$

  Then $Q(x)$.

  Then $P(x) \vee Q(x)$. # introduce disjunction

  Then $\forall x \in D, P(x) \vee Q(x)$. # introduce universal

Chapter 3

Formal Proofs

Proof by Cases

Proof by Cases

Implications with Disjunctive Antecedents

- Consider an **implication** which has a **disjunction** as the **antecedent**:
  - $\mathbf{S_1}$: $(A_1 \vee A_2) \Rightarrow C$.
- How can we prove $\mathbf{S_1}$?
  - $(A_1 \vee A_2) \Rightarrow C$ is equivalent with $(A_1 \Rightarrow C) \wedge (A_2 \Rightarrow C)$.

General Structure

Assume $A_1 \vee A_2$.
Case 1: Assume A_1.
⋮ # prove C
Then C.
Then $A_1 \Rightarrow C$. # assuming A_1 leads to C
Case 2: Assume A_2.
⋮ # prove C
Then C.
Then $A_2 \Rightarrow C$. # assuming A_2 leads to C
Then $(A_1 \Rightarrow C) \wedge (A_2 \Rightarrow C)$. # introduce conjunction
Then $(A_1 \vee A_2) \Rightarrow C$. # logically equiv. the previous statement

Proof by Cases

General Case

- $\mathbf{S_2}$: $(A_1 \vee \ldots \vee A_n) \Rightarrow C$.
- $\mathbf{S_2}$ is equivalent with $(A_1 \Rightarrow C) \wedge \ldots \wedge (A_n \Rightarrow C)$.

General Structure

Assume $A_1 \vee \ldots \vee A_n$.
Case 1: Assume A_1.

$\vdots$ # prove C

Then C.
Then $A_1 \Rightarrow C$. # assuming A_1 leads to C

$\vdots$

Case n: Assume A_n.

$\vdots$ # prove C

Then C.
Then $A_n \Rightarrow C$. # assuming A_n leads to C
Then $(A_1 \Rightarrow C) \wedge \ldots \wedge (A_n \Rightarrow C)$. # introduce conjunction
Then $(A_1 \vee \ldots \vee A_n) \Rightarrow C$. # logically equiv. the previous statement

Proof by Cases

General Case

- **Assumption:** $(A_1 \lor \ldots \lor A_n)$.
- **Claim:** C.

General Structure

Assume $A_1 \lor \ldots \lor A_n$.
Case 1: Assume A_1.
$\quad\vdots$ # prove C
Then C.
$\vdots$
Case n: Assume A_n.
$\quad\vdots$ # prove C
Then C.
Then C. # assuming $A_1 \lor \ldots \lor A_n$ leads to C

Proof by Cases

Exercise

- Prove that if n is an integer number, then $n^2 + n$ is **even**.

Solution

- **Step 1:** Translate the claim to logical notation.
  - For all integers n, $n^2 + n$ is even.
    $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.
- **Step 2:** Find a plan for the proof :
  - Consider two cases: n is odd or n is even.
- **Step 3:** Translate the assumptions/facts to logical notation
  - $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
- **Step 4:** Choose an appropriate proof structure. Use the assumptions/facts to prove the claim.

Proof by Cases

Exercise

- **Assumption**: $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
- **Claim**: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

Solution

Assume $n \in \mathbb{Z}$. # n is a typical integer number

$\vdots$

Then $\forall n \in \mathbb{Z}, \exists k \in, n^2 + n = 2k$. # introduction of universal

Proof by Cases

Exercise

- **Assumption**: $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
- **Claim**: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

Solution

Assume $n \in \mathbb{Z}$. # n is a typical integer number

$\vdots$

Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$.

Then $\forall n \in \mathbb{Z}, \exists k \in, n^2 + n = 2k$. # introduction of universal

Proof by Cases

Exercise

- **Assumption**: $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
- **Claim**: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

Solution

Assume $n \in \mathbb{Z}$. # n is a typical integer number

Then $(\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$. # by Assumption, $n \in \mathbb{Z}$

$\vdots$

Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$.

Then $\forall n \in \mathbb{Z}, \exists k \in, n^2 + n = 2k$. # introduction of universal

Proof by Cases

Exercise

- **Assumption**: $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
- **Claim**: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

Solution

Assume $n \in \mathbb{Z}$. # n is a typical integer number
  Then $(\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$. # by Assumption, $n \in \mathbb{Z}$
  Case 1: Assume $\exists k \in \mathbb{Z}, n = 2k + 1$.

  ⋮

  Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # true in all (both) possible cases
Then $\forall n \in \mathbb{Z}, \exists k \in, n^2 + n = 2k$. # introduction of universal

Proof by Cases

Exercise

- **Assumption**: $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
- **Claim**: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

Solution

Assume $n \in \mathbb{Z}$. # n is a typical integer number

Then $(\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$. # by Assumption, $n \in \mathbb{Z}$

Case 1: Assume $\exists k \in \mathbb{Z}, n = 2k + 1$.

Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0 + 1$. # instantiate existential

$\vdots$

$\vdots$

Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # true in all (both) possible cases

Then $\forall n \in \mathbb{Z}, \exists k \in, n^2 + n = 2k$. # introduction of universal

Proof by Cases

Exercise

- **Assumption**: $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
- **Claim**: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

Solution

Assume $n \in \mathbb{Z}$. # n is a typical integer number
    Then $(\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$. # by Assumption, $n \in \mathbb{Z}$
    Case 1: Assume $\exists k \in \mathbb{Z}, n = 2k + 1$.
        Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0 + 1$. # instantiate existential
        Then $n^2 + n = n(n+1) = (2k_0 + 1)(2k_0 + 2) = 2(2k_0 + 1)(k_0 + 1)$. # some algebra

            ⋮

    ⋮

    Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # true in all (both) possible cases
Then $\forall n \in \mathbb{Z}, \exists k \in, n^2 + n = 2k$. # introduction of universal

Proof by Cases

Exercise

- **Assumption**: $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k+1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
- **Claim**: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

Solution

Assume $n \in \mathbb{Z}$. # n is a typical integer number
  Then $(\exists k \in \mathbb{Z}, n = 2k+1) \vee (\exists k \in \mathbb{Z}, n = 2k)$. # by Assumption, $n \in \mathbb{Z}$
  Case 1: Assume $\exists k \in \mathbb{Z}, n = 2k+1$.
    Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0 + 1$. # instantiate existential
    Then $n^2 + n = n(n+1) = (2k_0+1)(2k_0+2) = 2(2k_0+1)(k_0+1)$. # some algebra
    Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # $k = (2k_0+1)(k_0+1) \in \mathbb{Z}$

  ⋮

  Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # true in all (both) possible cases
Then $\forall n \in \mathbb{Z}, \exists k \in, n^2 + n = 2k$. # introduction of universal

Proof by Cases

Exercise

- **Assumption**: $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k+1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
- **Claim**: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

Solution

Assume $n \in \mathbb{Z}$. # n is a typical integer number
    Then $(\exists k \in \mathbb{Z}, n = 2k+1) \vee (\exists k \in \mathbb{Z}, n = 2k)$. # by Assumption, $n \in \mathbb{Z}$
    Case 1: Assume $\exists k \in \mathbb{Z}, n = 2k+1$.
        Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0 + 1$. # instantiate existential
        Then $n^2 + n = n(n+1) = (2k_0+1)(2k_0+2) = 2(2k_0+1)(k_0+1)$. # some algebra
        Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # $k = (2k_0+1)(k_0+1) \in \mathbb{Z}$
    Case 2: Assume $\exists k \in \mathbb{Z}, n = 2k$.

    ⋮

    Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # true in all (both) possible cases
Then $\forall n \in \mathbb{Z}, \exists k \in, n^2 + n = 2k$. # introduction of universal

Proof by Cases

Exercise

- **Assumption**: $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k+1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
- **Claim**: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

Solution

Assume $n \in \mathbb{Z}$. # n is a typical integer number
Then $(\exists k \in \mathbb{Z}, n = 2k+1) \vee (\exists k \in \mathbb{Z}, n = 2k)$. # by Assumption, $n \in \mathbb{Z}$
Case 1: Assume $\exists k \in \mathbb{Z}, n = 2k+1$.
Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0 + 1$. # instantiate existential
Then $n^2 + n = n(n+1) = (2k_0+1)(2k_0+2) = 2(2k_0+1)(k_0+1)$. # some algebra
Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # $k = (2k_0+1)(k_0+1) \in \mathbb{Z}$
Case 2: Assume $\exists k \in \mathbb{Z}, n = 2k$.
Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0$. # instantiate existential
⋮
Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # true in all (both) possible cases
Then $\forall n \in \mathbb{Z}, \exists k \in, n^2 + n = 2k$. # introduction of universal

Proof by Cases

Exercise

- **Assumption**: $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k+1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
- **Claim**: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

Solution

Assume $n \in \mathbb{Z}$. # n is a typical integer number
Then $(\exists k \in \mathbb{Z}, n = 2k+1) \vee (\exists k \in \mathbb{Z}, n = 2k)$. # by Assumption, $n \in \mathbb{Z}$
Case 1: Assume $\exists k \in \mathbb{Z}, n = 2k+1$.
Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0 + 1$. # instantiate existential
Then $n^2 + n = n(n+1) = (2k_0+1)(2k_0+2) = 2(2k_0+1)(k_0+1)$. # some algebra
Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # $k = (2k_0+1)(k_0+1) \in \mathbb{Z}$
Case 2: Assume $\exists k \in \mathbb{Z}, n = 2k$.
Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0$. # instantiate existential
Then $n^2 + n = n(n+1) = 2k_0(2k_0+1) = 2[k_0(2k_0+1)]$.

⋮

Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # true in all (both) possible cases
Then $\forall n \in \mathbb{Z}, \exists k \in, n^2 + n = 2k$. # introduction of universal

Proof by Cases

Exercise

- **Assumption**: $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k+1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
- **Claim**: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

Solution

Assume $n \in \mathbb{Z}$. # n is a typical integer number
    Then $(\exists k \in \mathbb{Z}, n = 2k+1) \vee (\exists k \in \mathbb{Z}, n = 2k)$. # by Assumption, $n \in \mathbb{Z}$
    Case 1: Assume $\exists k \in \mathbb{Z}, n = 2k+1$.
        Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0 + 1$. # instantiate existential
        Then $n^2 + n = n(n+1) = (2k_0+1)(2k_0+2) = 2(2k_0+1)(k_0+1)$. # some algebra
        Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # $k = (2k_0+1)(k_0+1) \in \mathbb{Z}$
    Case 2: Assume $\exists k \in \mathbb{Z}, n = 2k$.
        Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0$. # instantiate existential
        Then $n^2 + n = n(n+1) = 2k_0(2k_0+1) = 2[k_0(2k_0+1)]$.
        Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # $k = k_0(2k_0+1) \in \mathbb{Z}$
    Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # true in all (both) possible cases
Then $\forall n \in \mathbb{Z}, \exists k \in, n^2 + n = 2k$. # introduction of universal

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** $\to$ proof by cases
- Disjunction in the **claim** $\to$ 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

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