Chapter 3

Formal Proofs

Bahar Aameri
Department of Computer Science
University of Toronto

Jan 23, 2015

Announcements

- **Assignment 1** is due next Friday Jan 30, before midnight.
- **TA office Hours** for Assignment 1:
  - Tuesday, Jan 27, 5-7pm in **BA3201**
  - Thursday, Jan 29, 3:30-5:30pm in **BA3201**
- **Monday**: Review session for Chapter 2.
  - Vote on the discussion board for topics that would like us to spend more time on.
- Next week tutorial **exercises** and **quiz** will only cover Chapter 2

Today's Topics

- **What is a Proof?**
- **Direct Proof of Universally Quantified Implication**
- **Indirect Proof of Universally Quantified Implication**

Motivation

Reminder from Chapter 1: Two Objectives of the Course

- Communicate precisely and concisely. $\rightarrow$ **Chapter 2**
- Make convincing arguments, aka Proofs. $\rightarrow$ **Chapter 3**

Chapter 3

Formal Proofs

What is a Proof?

What is a Proof?

Proof

- A **proof** is an **argument** that is **precise** and **logically correct**.

General Structure of a Typical Proof

- Given a set of **assumptions**, prove a **claim**.
  - Start from the assumptions.
  - Derive a logical consequence, based on the assumptions.
  - Add the new consequence to the original set of assumptions.
  - Continue until the claim can be derived from the assumptions.

What is a Proof?

Proof Structure

- Given P, prove Q:

Assume $\mathbf{P}$. # Given assumption
    Then $\mathbf{R_1}$. # by P or another known fact
    Then $\mathbf{R_2}$. # by R_1 or another known fact
    $\vdots$
    Then $\mathbf{R_n}$. # by R_{n-1} or another known fact
Then $\mathbf{Q}$. # by R_n or another known fact

It is not that easy!!

How to find a proof?

Creating a Proof

- **Finding a Proof**: Understanding why something is true.
- **Writing up the Proof**: Writing up your understanding

How to find a proof?

Creating a Proof

- **Finding a Proof**: It is like solving a problem
  - Understand the problem:
    - Know what is **required**
    - Know what is **given**
    - **Re-state** the problem in your own words;
    - Might help to draw some **diagrams**.
  - Plan solution(s):
    - Use **similar** results.
    - Work **backwards**:
    - Solving **simpler versions** of the problem.
  - Carry out your plan
    - If needed, **repeat** (parts of) the earlier steps.
    - If you are still stuck, identify *exactly* what information/assumptions you require that are missing and find a way to achieve them.
  - Review and verify your solution

How to find a proof?

Creating a Proof

- **Finding a Proof**: Understanding why something is true.
- **Writing up the Proof**:
  - Every statement in the proof should be true in the context it's written.
  - Might be helpful to use symbolic form to ensure the proof is precise.
  - Often errors will be detected while the proof is being written,
  - It is common to go back to step 1 to refine the proof.

What is a Proof?

Taxonomies of Claims

- **Axiom**: something we assert to be true, without justification.
- **Theorem**: a main result that we care about (at the moment).
- **Lemma**: a small result needed to prove a theorem.
- **Corollary**: an easy consequence of a theorem or a lemma.
- **Conjecture**: something suspected to be true, but not yet proven.

Chapter 3

Formal Proofs

Direct Proof of Universally Quantified Implication

Universally Quantified Implications

Reminder

- $\mathbf{C_1}$: $\forall x \in D, p(x) \Rightarrow q(x)$.
- $p(x)$ is the **antecedent**.
- $q(x)$ is the **consequence**.
- $\mathbf{C_1}$ is **True** iff for **all** elements in D, whenever $p(x)$ is **True**, $q(x)$ is also **True**.

How to prove $\forall x \in D, p(x) \Rightarrow q(x)$?

- Assume x is a generic member of D and $p(x)$ is **True**. (**Assumptions**) Show that $q(x)$ is **True**. (**Claim**)

- Prove $\forall x \in \mathbb{R}, (x > 0) \Rightarrow (1/(x+2) < 3)$.
  - **Assumptions**: x is a real number and $x > 0$.
  - **Claim**: $(1/(x+2)) < 3$.

Proving Universally Quantified Implications

- Most of the times, the given assumptions are **not enough** for proving the claim.
  - $(1/(x+2) < 3)$ **cannot** be derived directly from $(x > 0)$.
- Must use **previously proven statements** and **axioms** that link the assumptions to the claim:

$$\mathbf{C_2.0}: \ \forall x \in D, p(x) \Rightarrow r_1(x)$$

$$\mathbf{C_2.1}: \ \forall x \in D, r_1(x) \Rightarrow r_2(x)$$

$$\vdots$$

$$\mathbf{C_2.n}: \ \forall x \in D, r_n(x) \Rightarrow q(x)$$

Proof Structure for Universally Quantified Implications

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

  Assume $p(x)$. # x has property p, the antecedent

    Then $r_1(x)$. # by $\mathbf{C_1.0}$

    Then $r_2(x)$. # by $\mathbf{C_1.1}$

    $\vdots$

    Then $q(x)$. # by $\mathbf{C_1.n}$

  Then $p(x) \Rightarrow q(x)$. # assuming antecedent leads to consequent

Then $\forall x \in D, p(x) \Rightarrow q(x)$. # we only assumed x is a generic D

- The **explanation** after # is justification for each step.
- The **indentation** shows the scope of the assumptions.

Proving Universally Quantified Implications

Example

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

Assume $x \in \mathbb{R}$. # x is a typical real number
    Assume $x > 0$. # antecedent
        $\vdots$ # prove $1/(x+2) < 3$
        Then $1/(x+2) < 3$. # get here somehow
    Then $x > 0 \Rightarrow 1/(x+2) < 3$. # antecedent implies consequent
Then $\forall x \in \mathbb{R}, x > 0 \Rightarrow 1/(x+2) < 3$. # x is a typical element of $\mathbb{R}$

Proving Universally Quantified Implications

Example

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

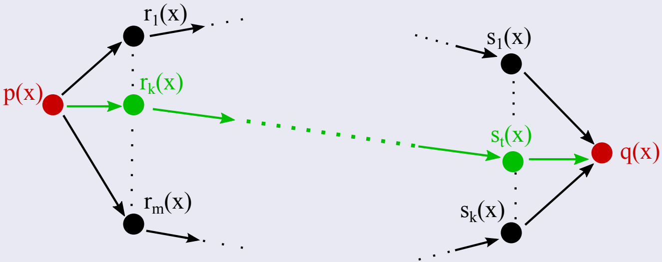
Assume $x \in \mathbb{R}$. # x is a typical real number
  Assume $x > 0$. # antecedent
    Then $x + 2 > 2$. # $x > 0$, add 2 to both sides
    Then $1/(x+2) < 1/2$. # reciprocals reverse inequality, and are defined for numbers > 2
    Then $1/(x+2) < 3$. # since $1/(x+2) < 1/2$ and $1/2 < 3$
  Then $x > 0 \Rightarrow 1/(x+2) < 3$. # antecedent implies consequent
Then $\forall x \in \mathbb{R}, x > 0 \Rightarrow 1/(x+2) < 3$. # x is a typical element of $\mathbb{R}$

Hunting the Elusive Direct Proof

- In practice, it is **not easy** to find a chain between the assumptions and the claim:
  - There are **many, many, many true** but irrelevant facts!

$$\forall x \in D, p(x) \Rightarrow (r_1(x) \wedge r_2(x) \wedge \cdots \wedge r_m(x)).$$

$$\forall x \in D, (s_k(x) \vee \cdots \vee s_1(x)) \Rightarrow q(x).$$



Universally Quantified Implications

Exercise

- Prove: $\forall n \in \mathbb{N}, n \text{ is odd} \Rightarrow n^2 \text{ is odd}.$

Assume $n \in \mathbb{N}$. # n is a generic natural number
    Assume n is odd. # n a typical odd natural number
        Then, $\exists j \in \mathbb{N}, n = 2j + 1$. # by definition of n odd
        Then $n^2 = (2j+1)^2 = 4j^2 + 4j + 1$. # some algebra
        Then $n^2 = 2(2j^2 + 2j) + 1$. # some algebra
        Then $\exists k \in \mathbb{N}, n^2 = 2k + 1$. # $k = 2j^2 + 2j \in \mathbb{N}$
        Then n^2 is odd. # by definition of n^2 odd
    Then n is odd $\Rightarrow n^2$ is odd. # assume n is odd, derived n^2 is odd
Then $\forall n \in \mathbb{N}, n$ is odd $\Rightarrow n^2$ is odd. # n is a generic natural number

Chapter 3

Formal Proofs

Indirect Proof of Universally Quantified Implication

Indirect Proof of Universally Quantified Implication

Reminder: Contrapositive

- **Contrapositive** of $P \Rightarrow Q$: $\neg Q \Rightarrow \neg P$.
- Contrapositive of an implication is equivalent with the implication.

Indirect Proof of $\forall x \in D, p(x) \Rightarrow q(x)$

- $p(x) \Rightarrow q(x)$ is equivalent with $\neg q(x) \Rightarrow \neg p(x)$.
- Proving $\forall x \in D, \neg q(x) \Rightarrow \neg p(x)$, proves $\forall x \in D, p(x) \Rightarrow q(x)$

Indirect Proof of Universally Quantified Implication

Structure of an Indirect Proof

- Prove $\forall x \in D, p(x) \Rightarrow q(x)$

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

Assume $\neg q(x)$. # negation of the **consequent**!

$\vdots$

Then $\neg p(x)$. # negation of the **antecedent**!

Then $\neg q(x) \implies \neg p(x)$. # assuming $\neg q(x)$ leads to $\neg p(x)$

Then $p(x) \Rightarrow q(x)$. # implication is equivalent to contrapositive

Then $\forall x \in D, p(x) \implies q(x)$. # x was a typical element of D

Indirect Proof of Universally Quantified Implication

Exercise

- Prove $\forall n \in \mathbb{N}, n^2$ is odd $\Rightarrow n$ is odd.

Assume $n \in \mathbb{N}$. # n is a generic natural number
    Assume n is **not** odd. # negation of the consequent
        Then, $\exists j \in \mathbb{N}, n = 2j$. # by definition of n even
        Then $n^2 = (2j)^2 = 4j^2$. # some algebra
        Then $n^2 = 2(2j^2)$. # some algebra
        Then $\exists k \in \mathbb{N}, n^2 = 2k$. # $k = 2j^2 \in \mathbb{N}$
        Then n^2 is even. # by definition of n^2 even
        Then n^2 is **not** odd. # negation of the antecedent
    Then n is **not** odd $\Rightarrow n^2$ is **not** odd.# assume $\neg q(x)$ leads to $\neg p(x)$
    Then n^2 is odd $\Rightarrow n$ is odd. # impl. is equivalent to contrapos.
Then $\forall n \in \mathbb{N}, n^2$ is odd $\Rightarrow n$ is odd. # n is a generic natural number