CSC165 Mathematical Expression and Reasoning for Computer Science

Lisa Yan

Department of Computer Science
University of Toronto

January 28, 2015
Announcements

- **TERM TEST 1:**
  - Time: Tuesday *Feb 03*, 2:10-3:30 Location: MP203
  - Time: Thursday *Feb 05*, 2:10-3:30 Location: MP103
  - **CONTENT:** Chapter 2

- **TA OFFICE HOURS:**
  - Mon., Feb 02, 1-3pm, 4:30-6:30pm in BA3201
  - Wed., Feb 04, 12-2pm, 3:30-5:30pm in BA3201

- **ASSIGNMENT 1:**
  - Due on 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
Topics: How to Prove?

- **Direct Proof**
  - Direct Proof of Universally Quantified Implication
  - Direct Proof of the Existential

- **Indirect Proof**
  - Indirect Proof of Universally Quantified Implication
  - Proof by Contradiction

- Multiple Quantifiers, Implications, and Conjunctions

- Example of Proving a Statement about a Sequence

- Example of Disproving a Statement about a Sequence
Proof

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

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**
Proof Structure

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.

Prove $P \Rightarrow Q$

- Given $P$, prove $Q$:
  - Assume $P$. # Given assumption
  - Then $R_1$. # by $P$ or another known fact
  - Then $R_2$. # by $R_1$ or another known fact
  - $\vdots$
  - Then $R_n$. # by $R_{n-1}$ or another known fact
  - Then $Q$. # by $R_n$ or another known fact
How to prove?

**DIRECT PROOF**
- **DIRECT PROOF OF UNIVERSALLY QUANTIFIED IMPLICATION**

**INDIRECT PROOF**
- **INDIRECT PROOF OF UNIVERSALLY QUANTIFIED IMPLICATION**
Universally Quantified Implications

Reminder

- \( C_1 : \forall x \in D, p(x) \Rightarrow q(x) \).
- \( p(x) \) is the ANTECEDENT.
- \( q(x) \) is the CONSEQUENCE.
- \( C_1 \) 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)
Direct Proof Structure for Universally Quantified Implications

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

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 $C_1.0$

Then $r_2(x)$. # by $C_1.1$

...$

Then q(x). # by $C_1.n$

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.
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 \( \forall x \in D, p(x) \Rightarrow q(x) \)
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 $\neg q(x) \Rightarrow \neg p(x)$. # assuming $\neg q(x)$ leads to $\neg p(x)$

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

Then $\forall x \in D, p(x) \Rightarrow q(x)$. # $x$ was a typical element of $D$
How to prove?

- **DIRECT PROOF**
  - DIRECT PROOF OF UNIVERSALLY QUANTIFIED IMPLICATION

- **INDIRECT PROOF**
  - INDIRECT PROOF OF UNIVERSALLY QUANTIFIED IMPLICATION
  - PROOF BY CONTRADICTION
To prove $P \Rightarrow Q$, follow this format:

Assume $\neg Q$. # in order to derive a contradiction

\[ \vdots \] # some steps leading to a contradiction, say $\neg P$

Then $\neg P$. # contradiction, since $P$ is known to be true

Then $Q$. # since assuming $\neg Q$ leads to contradiction
Proof by Contradiction: Example

Prove: there are infinitely many prime numbers.

Restate the problem: naming sets/predicates for this proof

- $P = \{p \in \mathbb{N} : p \text{ has exactly two factors}\}$
- $SP: \forall n \in \mathbb{N}, |P| > n$
Proof by Contradiction: Example

Proof by Contradiction: $\neg SP$:

Assume $\neg SP$: $\exists n \in \mathbb{N}, |P| \leq n$. # to derive a contradiction

Then there is a finite list, $p_1, \ldots, p_k$ of elements of $P$.
# at most $n$ elements in the list

Then I can take the product $p' = p_1 \times \cdots \times p_k$.
# finite products are well-defined

Then $p'$ is the product of some natural numbers 2 and greater.
# 0, 1 aren’t primes, 2, 3 are

Then $p' > 1$. # $p'$ is at least 6

Then $p' + 1 > 2$. # add 1 to both sides

Then $\exists p \in P, p$ divides $p' + 1$.
# every integer $> 2$ (such as $p' + 1$) has a prime divisor

Let $p_0 \in P$ be such that $p_0$ divides $p' + 1$.
# instantiate existential

Then $p_0$ is one of $p_1, \ldots, p_k$. # by assumption, the only primes

Then $p_0$ divides $p' + 1 - p' = 1$. # a divisor of each term divides difference

Then $1 \in P$. Contradiction! # 1 is not prime

Then $SP$. # “assume $\neg SP$” leads to a contradiction
How to prove?

- **Direct Proof**
  - Direct Proof of Universally Quantified Implication
  - Direct Proof of the Existential

- **Indirect Proof**
  - Indirect Proof of Universally Quantified Implication
  - Proof by Contradiction
Direct proof structure of the existential

The general form for a direct proof of $\exists x \in D, p(x)$ is:

Let $x = \ldots$ # choose a particular element of the domain
Then $x \in D$. # this may be obvious, otherwise prove it

\[ \vdash \# \text{ prove } p(x) \]

Then $p(x)$. # you’ve shown that $x$ satisfies $p$
$\exists x \in D, p(x)$. # introduce existential
How to prove?

- **DIRECT PROOF**
  - **DIRECT PROOF OF UNIVERSALLY QUANTIFIED IMPLICATION**
  - **DIRECT PROOF OF THE EXISTENTIAL**

- **INDIRECT PROOF**
  - **INDIRECT PROOF OF UNIVERSALLY QUANTIFIED IMPLICATION**
  - **PROOF BY CONTRADICTION**

- **MULTIPLE QUANTIFIERS, IMPLICATIONS, AND CONJUNCTIONS**
Proof Structure for Multiple quantifiers, implications, and conjunctions:

Consider $\forall x \in D, \exists y \in D, p(x, y)$. The corresponding proof structure is:

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

Let $y_x = \ldots$  # choose an element that works

\[ \vdots \]

Then $y_x \in D$.  # verify that $y \in D$

\[ \vdots \]

Then $p(x, y_x)$.  # $y$ satisfies $p(x, y)$

Then $\exists y, p(x, y)$.  # introduce existential

Then $\forall x \in D, \exists y \in D, p(x, y)$.  # introduce universal
Example: suppose a function $f$, constants $a$ and $l$, and the following statement

$$\forall e \in \mathbb{R}, e > 0 \Rightarrow (\exists d \in \mathbb{R}, d > 0 \land (\forall x \in \mathbb{R}, 0 < |x - a| < d \Rightarrow |f(x) - l| < e))$$

Direct proof: structure of the proof to prove this TRUE

Assume $e \in \mathbb{R}$. # typical element of $\mathbb{R}$
Assume $e > 0$. # antecedent
Let $d_e = \ldots$ # something helpful, probably depending on $e$
Then $d_e \in \mathbb{R}$. # verify $d_e$ is in the domain
Then $d_e > 0$. # show $d_e$ is positive
Assume $x \in \mathbb{R}$. # typical element of $\mathbb{R}$
Assume $0 < |x - a| < d_e$. # antecedent

\[\vdots\]
Then $|f(x) - l| < e$. # inner consequent
Then $0 < |x - a| < d_e \Rightarrow (|f(x) - l| < e)$. # introduce implication
Then $\forall x \in \mathbb{R}, 0 < |x - a| < d_e \Rightarrow (|f(x) - l| < e)$. # introduce universal
Then $\exists d \in \mathbb{R}, d > 0 \land (\forall x \in \mathbb{R}, 0 < |x - a| < d \Rightarrow (|f(x) - l| < e))$. # introduce existential
Then, $e > 0 \Rightarrow (\exists d \in \mathbb{R}, d > 0 \land (\forall x \in \mathbb{R}, 0 < |x - a| < d \Rightarrow (|f(x) - l| < e)))$. Then $\forall e \in \mathbb{R}, e > 0 \Rightarrow (\exists d \in \mathbb{R}, d > 0 \land (\forall x \in \mathbb{R}, 0 < |x - a| < d \Rightarrow (|f(x) - l| < e))).$
Multiple quantifiers, implications, and conjunctions: Example

Example: suppose a function $f$, constants $a$ and $l$, and the following statement

$$\forall e \in \mathbb{R}, \, e > 0 \Rightarrow (\exists d \in \mathbb{R}, \, d > 0 \land (\forall x \in \mathbb{R}, \, 0 < |x - a| < d \Rightarrow |f(x) - l| < e))$$

Prove by contradiction: negate the statement

$$\neg((\forall e \in \mathbb{R}, \, e \leq 0 \lor (\exists d \in \mathbb{R}, \, d > 0 \land (\forall x \in \mathbb{R}, \, \neg(0 < |x - a| < d) \lor |f(x) - l| < e))))$$

$$\exists e \in \mathbb{R}, \, e > 0 \land (\forall d \in \mathbb{R}, \, d > 0 \Rightarrow (\exists x \in \mathbb{R}, \, 0 < |x - a| < d \land |f(x) - l| \geq e))$$
How to prove?

- **Direct Proof**
  - Direct Proof of Universally Quantified Implication
  - Direct Proof of the Existential

- **Indirect Proof**
  - Indirect Proof of Universally Quantified Implication
  - Proof by Contradiction

- **Multiple quantifiers, implications, and conjunctions**

- **Example of proving a statement about a sequence**
Consider the statement to prove it:

\[ \exists i \in \mathbb{N}, \forall j \in \mathbb{N}, a_j \leq i \Rightarrow j < i \] and the sequence: (A1) 0, 1, 4, 9, 16, 25, …

Going back to our proof structure, we have:

Let \( i = \_ \). Then \( i \in \mathbb{N} \).

Assume \( j \in \mathbb{N} \). # typical element of \( \mathbb{N} \)
   Assume \( a_j \leq i \).

\[
\vdots
\]

Then \( j < i \).
Example of proving a statement about a sequence

Consider the statement to prove it:

\[ \exists i \in \mathbb{N}, \forall j \in \mathbb{N}, a_j \leq i \Rightarrow j < i \] and the sequence: (A1) 0, 1, 4, 9, 16, 25, …

Thoughts:

we decide that setting \( i = 2 \) is a good idea, since then \( a_j \leq i \) is only true for \( j = 0 \) and \( j = 1 \), and these are smaller than 2.

Also, here, the contrapositive, \( \neg(j < i) \Rightarrow \neg(a_j \leq a_i) \) is easier to work with.

Let \( i = 2 \). Then \( i \in \mathbb{N} \). # 2 \( \in \mathbb{N} \)

Assume \( j \in \mathbb{N} \). # typical element of \( \mathbb{N} \)

Assume \( \neg(j < i) \). # antecedent for contrapositive

Then \( j \geq 2 \). # negation of \( j < i \) when \( i = 2 \)

Then \( a_j = j^2 \geq 2^2 = 4 \). # since \( a_j = j^2 \), and \( j \geq 2 \)

Then \( a_j > 2 \). # since \( 4 > 2 \)

Then \( \neg(j < i) \Rightarrow \neg(a_j \leq a_i) \). # assuming antecedent leads to consequent

Then \( a_j \leq 2 \Rightarrow j < i \). # implication equivalent to contrapositive

Then \( \forall j \in \mathbb{N}, a_j \leq i \Rightarrow j < i \). # introduce universal

Then \( \exists i \in \mathbb{N}, \forall j \in \mathbb{N}, a_j \leq i \Rightarrow j < i \). # introduce existential
Topics: How to Prove?

- Direct Proof
  - Direct Proof of Universally Quantified Implication
  - Direct proof of the existential

- Indirect Proof
  - Indirect Proof of Universally Quantified Implication
  - Proof by Contradiction

- Multiple quantifiers, implications, and conjunctions

- Example of proving a statement about a sequence

- Example of disproving a statement about a sequence
Example of disproving a statement about a sequence

Consider the statement to disprove it:

$$\exists i \in \mathbb{N}, \forall j \in \mathbb{N}, j > i \Rightarrow a_j = a_i$$

and the sequence: (A2) 0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, …

Disprove it: simply prove the negation:

$$\forall i \in \mathbb{N}, \exists j \in \mathbb{N}, j > i \land a_j \neq a_i$$

Sketch in the outline of the proof:

Assume $i \in \mathbb{N}$.

Let $j = i + 2$. Then $j \in \mathbb{N}$.

Then $j > i \land a_j \neq a_i$.

Then $\exists j \in \mathbb{N}, j > i \land a_j \neq a_i$.

Then $\forall i \in \mathbb{N}, \exists j \in \mathbb{N}, j > i \land a_j \neq a_i$.

# introduction of existential

# introduction of universal