Lecture 06: Introduction to Proofs

Jingjin Yu |Computer Science @ Rutgers

RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

September 22, 2020

Algorithmic Robotics & Control Lab

Outline

- Lecture 05 review
- Introduction
  - From “formal” to “informal” proofs
  - Terminology
- Methods for proving theorems
  - Direct proofs
  - Proof the contrapositive
  - Proof via contradiction

- A repeating note: **make sure you read the textbook**

L05: Proof under a Logical System

Logical system

Assumptions (premises) $\mathcal{A} = \{A_1, \dots, A_n\}$

Conclusion P

Proof:

$$\mathcal{A} \xRightarrow{rules\ of\ inference} C_1 \text{ (new conclusion)}$$

$$\mathcal{A} \cup \{C_1\} \xRightarrow{rules\ of\ inference} C_2$$

...

$$\mathcal{A} \cup \{C_1, C_2, \dots\} \xRightarrow{rules\ of\ inference} P$$

L05: Making Valid Argument

- We have a set of premises, $p_1, \ldots, p_n$
- We want to draw the conclusion $q = p_{n+1}$
- To do this, we need to show $p_1 \wedge \cdots \wedge p_n \rightarrow q$
- This can be shown by showing that if $p_1 \wedge \cdots \wedge p_n$ is true, then q is true
- This shows $p_1 \wedge \cdots \wedge p_n \rightarrow q$ is a tautology

$p_1 \wedge \cdots \wedge p_n$	q	$(p_1 \wedge \cdots \wedge p_n) \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

L05: Two Basic "Rules"

- **Ex**: modus ponens
  - S_1: If it snows today, then we go skiing
  - S_2: It is snowing today
  - S_3: We go skiing

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline q \end{array}$$

- **Ex**: modus tollens
  - S_1: If it snows today, then we go skiing
  - S_2: We do not go skiing
  - S_3: It is not snowing today

$$\begin{array}{l} p \rightarrow q \\ \neg q \\ \hline \neg p \end{array}$$

L05: A Useful Set of Rules

Rule	Tautology	Name
$p \to q$ $q \to r$ --- $p \to r$	$((p \to q) \land (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \lor q$ $\neg p$ --- q	$((p \lor q) \land \neg p) \to q$	Disjunctive syllogism
p --- $p \lor q$	$p \to (p \lor q)$	Addition
$p \land q$ --- p .	$(p \land q) \to p$	Simplification
p q --- $p \land q$	$((p) \land (q)) \to (p \land q)$	Conjunction
$p \lor q$ $\neg p \lor r$ --- $q \lor r$	$((p \lor q) \land (\neg p \lor r)) \to (q \lor r)$	Resolution

Formal v.s. Informal Proofs

- **Ex:** Proving $\sqrt{2}$ is irrational

easy to read

Formal proof by contradiction:

```
theorem sqrt-prime-irrational:
  assumes prime (p::nat)
  shows sqrt p ∉ ℚ
proof
  from ⟨prime p⟩ have p: 1 < p by (simp add: prime-nat-iff)
  assume sqrt p ∈ ℚ
  then obtain m n :: nat where
      n: n ≠ 0 and sqrt-rat: |sqrt p| = m / n
    and coprime m n by (rule Rats-abs-nat-div-natE)
  have eq: m^2 = p * n^2
  proof −
    from n and sqrt-rat have m = |sqrt p| * n by simp
    then have m^2 = (sqrt p)^2 * n^2
      by (auto simp add: power2-eq-square)
    also have (sqrt p)^2 = p by simp
    also have ... * n^2 = p * n^2 by simp
    finally show ?thesis using of-nat-eq-iff by blast
  qed
  have p dvd m ∧ p dvd n
  proof
    from eq have p dvd m^2 ..
    with ⟨prime p⟩ show p dvd m by (rule prime-dvd-power-nat)
    then obtain k where m = p * k ..
    with eq have p * n^2 = p^2 * k^2 by (auto simp add: power2-eq-square ac-simps)
    with p have n^2 = p * k^2 by (simp add: power2-eq-square)
    then have p dvd n^2 ..
    with ⟨prime p⟩ show p dvd n by (rule prime-dvd-power-nat)
  qed
  then have p dvd gcd m n by simp
  with ⟨coprime m n⟩ have p = 1 by simp
  with p show False by simp
qed

corollary sqrt-2-not-rat: sqrt 2 ∉ ℚ
  using sqrt-prime-irrational[of 2] by simp
```

long and difficult

Source: https://ts.data61.csiro.au/projects/TS/l4.verified/sqrt-2-proof.pdf

Informal proof by contradiction:

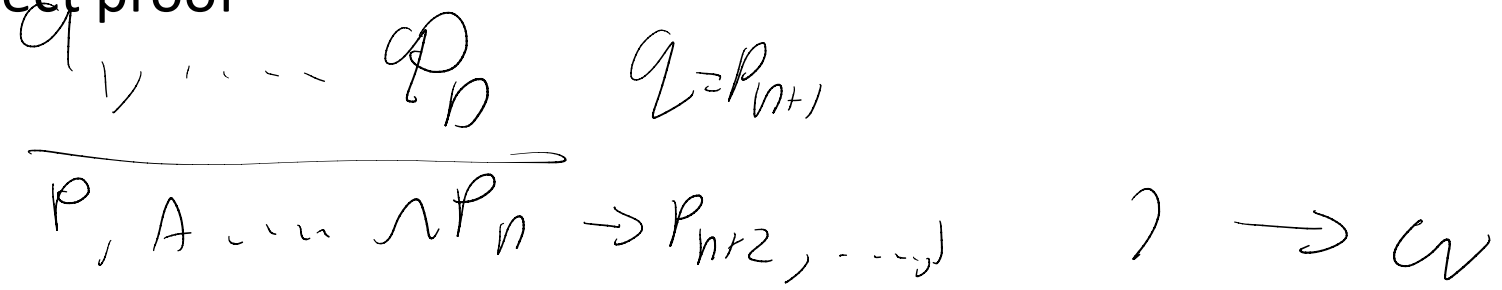
- Let $\sqrt{2} = \frac{n}{m}$ where n, m are co-prime
- Then $2 = \frac{n^2}{m^2}$
- But n^2 and m^2 are co-prime because n and m are
- Contradiction

Terminologies

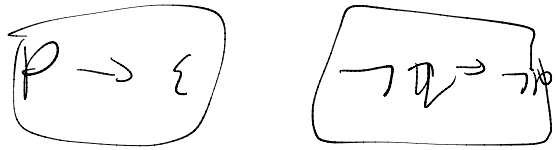
- Definition: a statement describing certain (mathematical, logical, and so on) objects
- Axiom: a propositional statement that is assumed as true
- Theorem: a propositional statement that is relatively important and must be proven to be true.
- Proposition: a less important theorem
- Lemma: a less important theorem that is used to prove a theorem
- Corollary: a useful proposition that readily follows another theorem/corollary/proposition
- Proof: arguments showing that a theorem is true

Methods for Proving Theorems

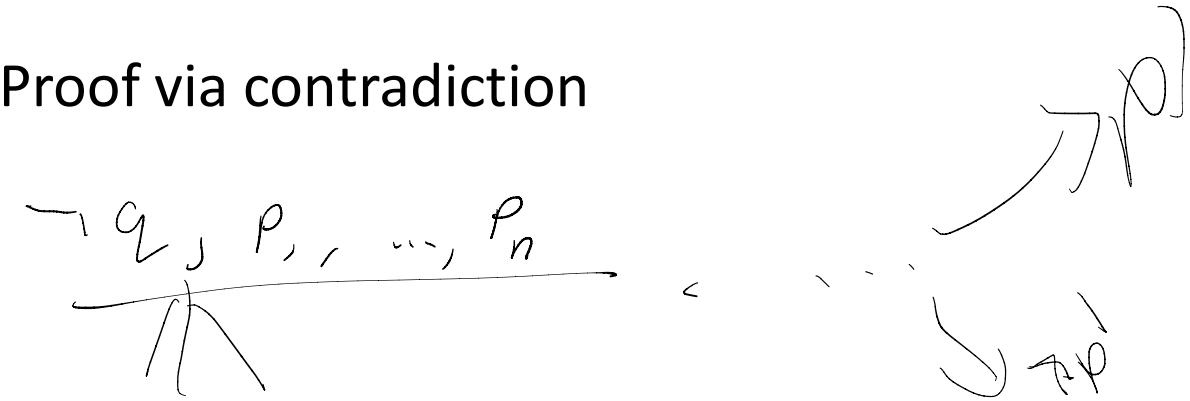
- General methods:
  - Direct proof



  - Proving the contrapositive



  - Proof via contradiction



Proving Theorems: Basics

- Some basic techniques
  - For proving $\forall x(P(x) \rightarrow Q(x))$
    - Generally, we show $P(c) \rightarrow Q(c)$ for an arbitrary c
  - For proving $p \rightarrow q$
    - We only need to show if p is true then q is true

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Direct Proof: Example 1

- **Def**^{n}: An integer n is **odd** if $n = 2k + 1$ for some integer k.
- **Ex**: A direct proof of "If n is odd, then n^2 is odd."

$p \rightarrow q$ p: "n is odd", q: "n is odd"

Assume $n = 2k+1$ for some integer k

$$n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$$

Let $k' = 2k^2+2k$, then $n^2 = 2k'+1$

by definition n^2 is odd

We have shown, "n is odd", "n^2 is odd"

Direct Proof: Example 2

- **Def**^{n}: An integer n is a **perfect square** if $n = k^2$ for some integer k.
- **Ex**: A direct proof of if m and n are both perfect squares, so is mn.

Need: m, n are perfect squares $\rightarrow mn$ is a perfect square

proof: assume m, n are perfect squares then we have $m = k^2$ and $n = l^2$ for integers k and l

Therefore, $mn = k^2 l^2 = (kl)^2$

Vacuous and Trivial Proofs

- **Def^n**: A proof is **vacuous** if we have p is always false in the statement $p \rightarrow q$, which is to be proven.
  - **Ex**: Show that for integer n, $n^2 < 0 \rightarrow n = 2n$.

- **Def^n**: A proof of $p \rightarrow q$ is **trivial** if q is always true.
  - **Ex**: Show that if $2 > 3$, then $3 > 2$.

Proving Contraposition: Example 1

- **Def^n**: An integer n is **even** if $n = 2k$ for some integer k
- **Ex**: Show that an integer n is odd if $3n + 2$ is odd.

show "$3n+2$ is odd" $\rightarrow$ "n is odd"

$= 2k+1$

Proof (Direct)

assuming $3n+2$ is odd, $3n+2 = 2k+1 \Rightarrow 3n = 2k+1$

$$\begin{cases} k = 3l & 3n = 6l - 1 \Rightarrow n = 2l - \frac{1}{3} \\ k = 3l+1 & 3n = 6l+2-1 = 6l+1 \Rightarrow n = 2l + \frac{1}{3} \\ k = 3l+2 & 3n = 6l+4-1 = 6l+3 \Rightarrow n = 2l+1 \end{cases}$$

n is odd

Proving Contraposition: Example 1

- **Def^n**: An integer n is **even** if $n = 2k$ for some integer k
- **Ex**: Show that an integer n is odd if $3n + 2$ is odd.

Proof (via contrapositive)

need to show n is even $\rightarrow$ 3n+2 is even

assume "n is even", n = 2k for some integer k then 3n+2 =

$3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2k$

3n+2 must be even

Proving Contraposition: Example 2

- **Ex**: Prove that if $n = ab$ for positive integers a and b, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. $\neg(a \leq \sqrt{n} \vee b \leq \sqrt{n})$

$\equiv \neg(a \leq \sqrt{n}) \wedge \neg(b \leq \sqrt{n})$

Proof

Contrapositive! $(a > \sqrt{n} \wedge b > \sqrt{n})$

$\rightarrow (n \neq ab)$

Assume $a > \sqrt{n}$, $b > \sqrt{n}$, then

$a \cdot b > \sqrt{n} \cdot \sqrt{n} = n \Rightarrow n < a \cdot b \Rightarrow n \neq ab$

- Read examples 7 and 8 carefully to learn more.

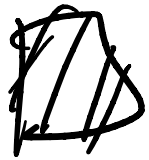
Proving via Contradiction: Example 1

- **Ex:** Show that at least four of any 22 days must fall on the same day of the week.

proof. 1 2 3 4 5 6 7

$\neg p$ $3+3+3+3+3+3+3 = 21$

Contradition. $\neg p$ Cannot be true



Proving via Contradiction: Example 2

- **Ex:** Prove $\sqrt{2}$ is irrational.

Proof (via contradiction): Assume $\sqrt{2}$ is rational, $\sqrt{2} = \frac{n}{m}$. We may assume n, m are co-prime.

We have $2 = \frac{n^2}{m^2} \Rightarrow n^2 = 2m^2 \Rightarrow n^2$ is an even integer $n^2 = 2k$

(n^2 is even $\Rightarrow n$ is even) $\int$ n is even

$n = 2l$

$n^2 = 2m^2$ $\Big\}$ $\Rightarrow 4l^2 = 2m^2 \Rightarrow m^2 = 2l^2$

$\Rightarrow m$ is even

Proving via Contradiction: Example 3

- **Ex:** Show if $3n + 2$ is odd, then n is odd.

Proof (via contradiction):

"$3n+2$ is odd" → "n is odd" = p

Assume $\neg p$ is true = ($3n+2$ is odd) (Mistake)

Let $n = 2k$ for some k, then $3n+2 = 3(2k)+2$

$= 3n+2 = 6k+2$ is even

Contradiction.

- Read examples 12, 13, and 14, as well as the part "Mistakes in proofs", which is an easy read.