Lecture 07-08: More Proofs

Jingjin Yu | Computer Science @ Rutgers

September 25, 2020

Outline

- Lecture 06 review
- Exhaustive proofs
  - Exclusive enumeration
  - Non-exclusive cases
- Existence proofs
  - Providing an example
  - Proving existence without an example
- Uniqueness proof
- Strategies
  - Reasoning backwards
  - Adapting existing proofs
  - Finding counterexamples
- Tiling dominos

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

L06: Introduction to Proofs: Basics

negate of if statement

$\neg(A \to B) \equiv A \wedge \neg B$

- Proofs, formal v.s. informal proofs
- Theorems, lemmas, propositions, corollaries, conjectures
- General methods:
  - Direct proof

    $p_1, \ldots, p_n, q = p_{n+1}$

    directly establish a relationship

    $(p_1 \wedge \ldots \wedge p_n) \to q$

  - Proving the contrapositive

    $p \to q \equiv \neg p \to \neg q$

  - Proof via contradiction

    q assume $\neg q \to p'$

    $\to \neg p'$ $\Rightarrow$ q must be true

L06: An Example: $3n + 2$ odd $\rightarrow n$ odd

Direct Proof:

$3n + 2 = 2k - 1$

$k = 3L$

(1) $k = 3L$, $3n = 6L - 1$ can't happen

$n = 2L - \frac{1}{3}$

(2) $k = 3L + 1$ $3n = 6n + 1$, $n = 2n + \frac{1}{3}$ can't happen

(3) $k = 3L + 2$, $3n = 3n \, 6L \, 3$, $n = 2L+1$ odd

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

Proving the contrapositive

n even $\rightarrow 3n + 2$ even

$n = 2k \Rightarrow \underline{3n + 2 = 6k + 2 = 2(3k+1)}$

even

proof via contradiction

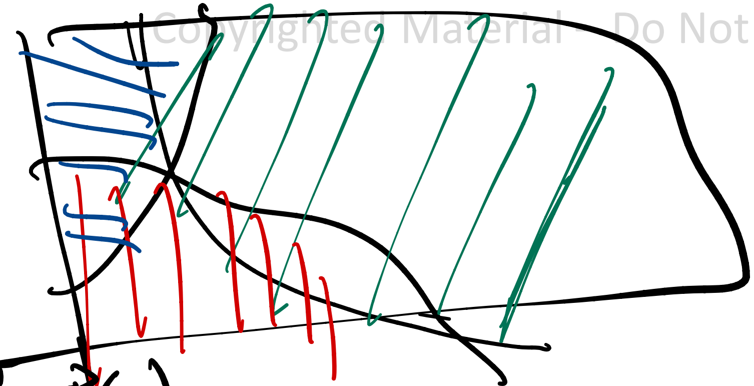
$3n + 2$ odd $\rightarrow n$ odd

$3n + 2$ is odd $\cap$ n is even

$n = 2k \Rightarrow 3n + 2 = 6k + 2 = 2(3k+1)$ which is even

a contradiction

Exhaustive Proof: The Principle



$$p \to q$$

$$(p_1 \to q) \wedge (p_2 \to q) \wedge (p_3 \to q)$$

$$\Leftrightarrow (p_1 \vee p_2 \vee p_3) \to q$$

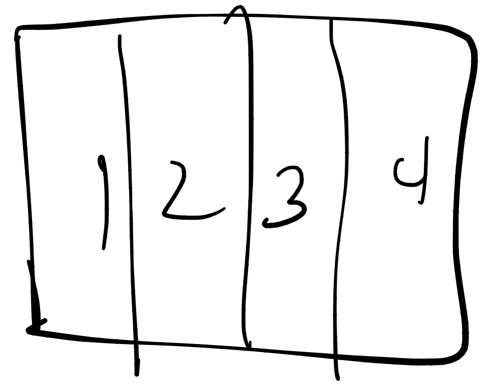
$$(p_1 \vee \dots \vee p_n) \to q \Leftrightarrow (p_1 \to q) \wedge \dots \wedge (p_n \to q)$$

Exhaustive Proof: Example 1 (Exclusive Or)

of cases

- **Ex**: You have a drawer filled with red or blue socks. Show that if you pick three socks, you will have a pair of socks of the same color.

Proof: We enumerate possible rates of sock distribution in 3 socks



Case 1: 0 red + 3 blue socks

Case 2: 1 red + 2 blue, a blue pair

case 3: 2 red + 1 blue, a pair

case 4: 3 red + 0 blue, a red pair

For all cases, there is a pair of socks of the same color

Exhaustive Proof: Example 2 (Exclusive Or)

- **Ex**: Prove that $(n+1)^3 \geq 3^n$ if $n \leq 4$ is a positive integer.

Proof. There are four possible cases, $n = 1, 2, 3, 4$

1. $n = 1$, $(1+1)^3 = 8 \geq 3$ ✓
2. $n = 2$, $(2+1)^3 = 27 \geq 9 = 3^2$
3. $n = 3$, $(3+1)^3 = 64 \geq 3^3$
4. $n = 4$, $(4+1)^3 = 128 \geq 81 = 3^4$ ✓

All cases hold

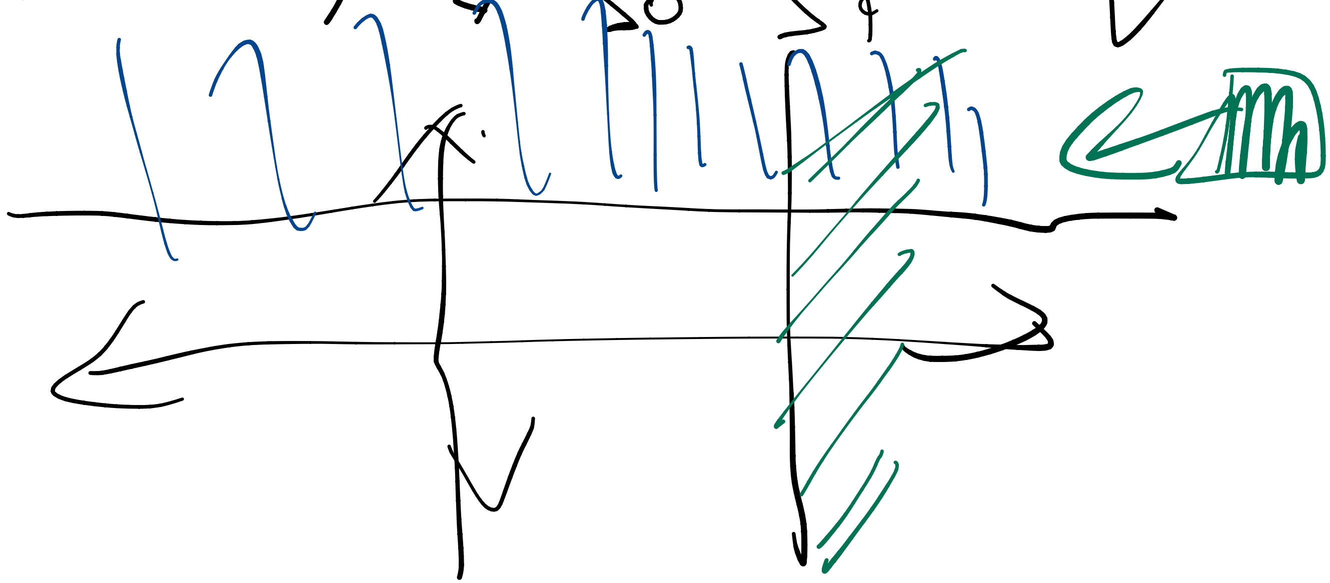
Exhaustive Proof: Example 3 (non-Exclusive Or)

- **Ex**: Show that $((x > 4) \vee (y > 2)) \rightarrow (|x| + y^2 > 4)$.

Proof:

Case 1: Let $x > 4$, $\underbrace{|x|}_{>4} + \underbrace{y^2}_{\geq 0} > 4$

Case 2: Let $y > 2$, $\underbrace{|x|}_{\geq 0} + \underbrace{y^2}_{> 4} > 4$



Exhaustive Proof: Example 4 (non-Exclusive Or)

- **Def^n**: $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$.
- **Ex**: Show that $|xy| = |x||y|$ for real numbers x and y.

Proof $|x| = -x$ if $x < 0$, $|x| = x$ if $x \geq 0$

Case 1: $x \geq 0$, $y \geq 0$ $\quad xy \geq 0 \Rightarrow |xy|$

$|x| = x$, $|y| = y \Rightarrow |x||y| = xy$

Case 2: $x \geq 0$, $y \leq 0$, $\quad xy < 0 \Rightarrow |xy| = -xy$

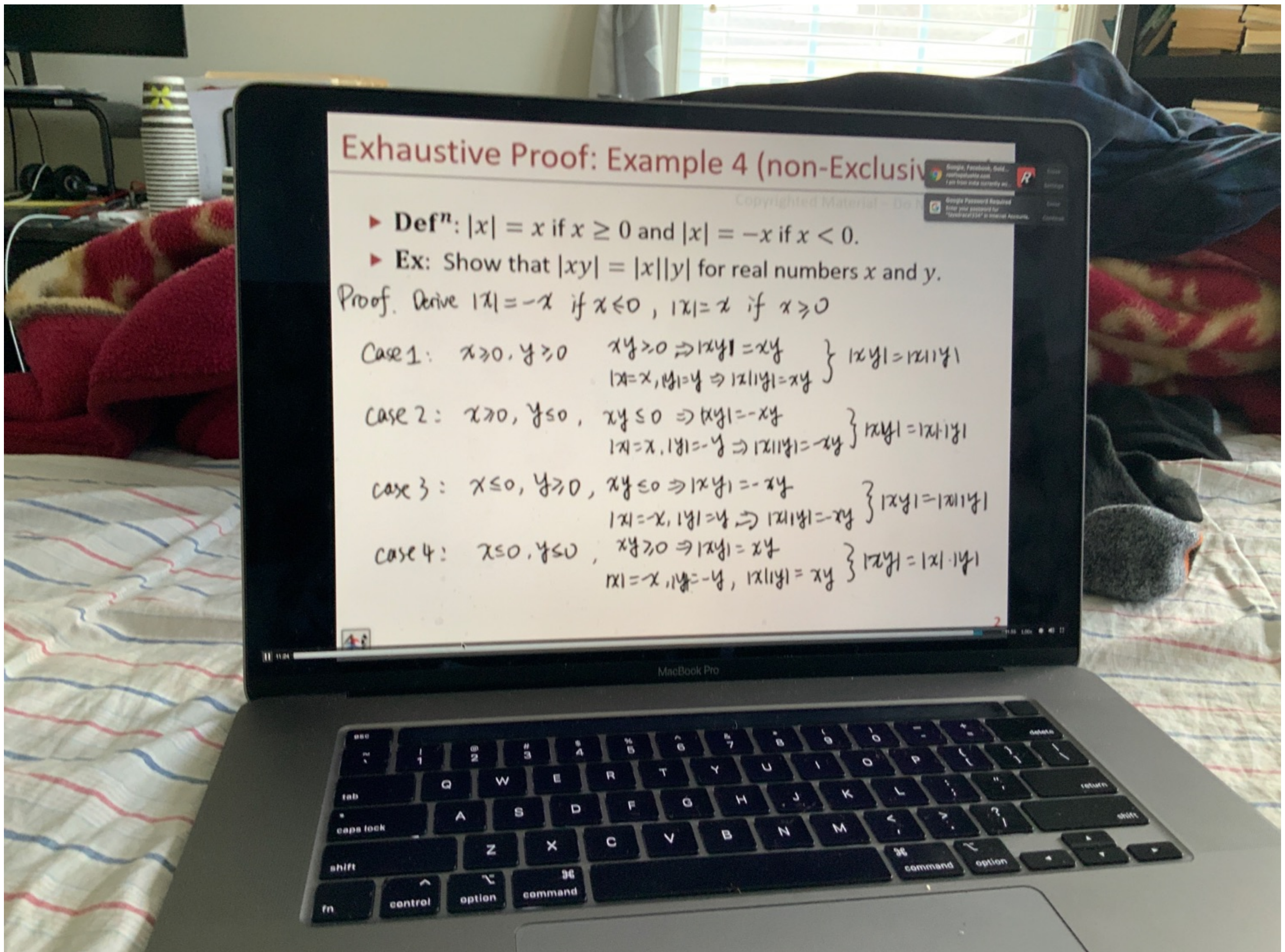
$|x| = x$, $|y| = -y \Rightarrow$

$|x||y| = -xy$

$|xy| = |x||y|$

Exhaustive Proof: Example 4 (non-Exclusive Or)

- **Def^{n}**: $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$.
- **Ex**: Show that $|xy| = |x||y|$ for real numbers x and y.



Exhaustive Proof: Example 5

- **Ex**: Formulate a conjecture about the last decimal digit of x^2 for an integer x. Prove your conjecture.

Exhaustive Proof: Example 6

- **Ex**: If x and y are integers and both xy and $x + y$ are even, then x and y are both even.

Proof. $(xy \text{ even} \wedge x+y \text{ even}) \Rightarrow x \text{ even} \wedge y \text{ even}$

$\equiv \neg(x \text{ even} \wedge y \text{ even}) \Rightarrow \neg(xy \text{ even} \wedge (x+y) \text{ even})$

$\equiv (x \text{ odd} \vee y \text{ odd}) \Rightarrow (xy \text{ odd} \vee (x+y) \text{ odd})$

Case 1: x odd
- y odd $\Rightarrow xy$ odd
- y even $\Rightarrow x+y$ odd

Case 2: y odd
- x odd $\Rightarrow xy$ odd
- x even $\Rightarrow x+y$ odd

Existence Proof: Basics and Approaches

- Existence proofs: $\exists x\ P(x)$

- General approaches
  - Constructive: build a positive example
  - Non-constructive: show there must somehow exist such an object, without actually providing an example

Existence Proof: Examples 1-2 (Constructive)

- **Ex:** Show that there are positive integers that can be written as the sum of cubes of integers in two different ways.

$x = a_1^3 + b_1^3 = a_2^3 + b_2^3$

$1729 = 12^3 + 1^3 = 10^3 + 9^3$

$1728 = 12^3$

1728 can ...

(x, y) $x_1, x_2, \ldots, x_k$ $x_1 + \cdots + x_k = y$

$y_1, y_2, \ldots, y_n$ $y_1 + \cdots + y_n = x$

- **Def^n:** Two different numbers are **amicable** if the sum of the proper divisors of each is equal to the other number.
- **Ex:** Show that there exists a pair of amicable numbers.

1, 2, 4, 110, 4, 35, 5, 44, 10, 22, 11, 20 284, 220

1, 2, 142, 71

Existence Proof: Example 3 (Non-Constructive)

- **Ex:** Prove the existence of irrational numbers x and y such that x^y is rational.

$x = \sqrt{2}$ $y = \sqrt{2}$

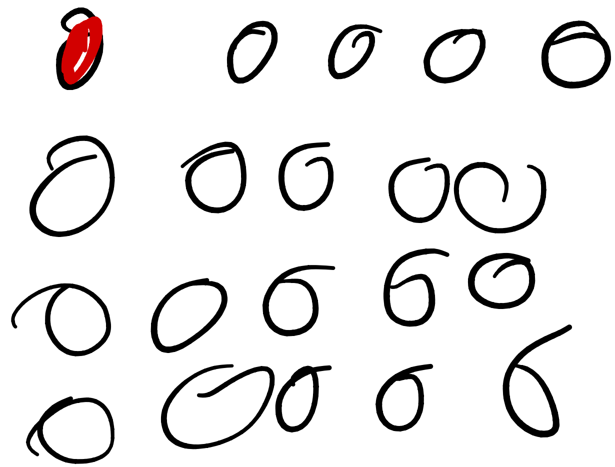
$x^y = \sqrt{2}^{\sqrt{2}}$

$x' = \sqrt{2}^{\sqrt{2}}$, $y' = \sqrt{2}$, $x'^{y'} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$

$(\sqrt{2}, \sqrt{2})$ or $(\sqrt{2}^{\sqrt{2}}, \sqrt{2})$ is whatever

Existence Proof: Example 4 (Non-Constructive)

- **Ex:** Game of Chomp



① At least one cookie is removed each round

② There are a finite # of cookies

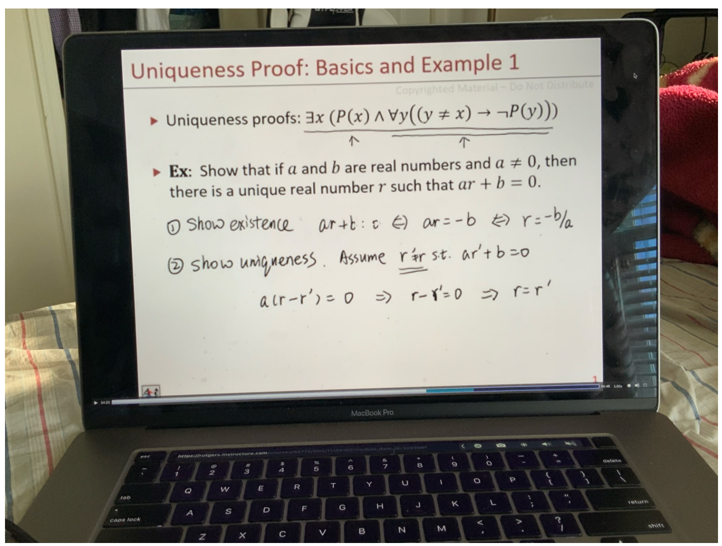
Player 1 < Take the lower right cookie
do something else

player 2 plays the winning strategy

Uniqueness Proof: Basics and Example 1

- Uniqueness proofs: $\exists x\,(P(x) \wedge \forall y((y \neq x) \rightarrow \neg P(y)))$

- **Ex:** Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.



Uniqueness Proof: Example 2

- **Ex:** Show $f(x) = x^2 + 4x + 9$ has a unique minimum.

Set $f'(x) = 2x + 4 = 0 \Rightarrow x = -2$

$f''(x) \Rightarrow 2 > 0$

shows that $x = -2$ is the unique min of $f(x)$

Strategy: Reasoning Backwards, Example 1

- **Ex:** Show for positive real numbers x and y, $\frac{x+y}{2} \geq \sqrt{xy}$.

$$\frac{x+y}{2} \geq \sqrt{xy} \Longleftrightarrow x+y \geq \sqrt{xy} \Longleftrightarrow$$

$$(x+y)^2 \geq 4xy \Longleftrightarrow$$

$$x^2+2xy+y^2 \geq 4xy \Longleftrightarrow$$

$$x^2-2xy+y^2 \geq 0$$

$$\Longleftrightarrow (x-y)^2 \geq 0$$

Strategy: Reasoning Backwards, Example 2

- **Ex:** Stone removal. Suppose two players taking turns to remove stones from a pile of 15 stones. Each player must remove 1-3 stones during a turn. The last player who removes the last stone wins. Show that the first player can always win.

Strategy: Reasoning Backwards, Example 3

- **Ex:** 99 wolves and a magic sheep.

1 wolf 1 sheep => wolf eats sheep

2 wolves 1 sheep => sheep is safe

3 wolves 1 sheep => sheep gets eaten

4 wolves 1 sheep → sheep is safe

- **Ex:** 100 wolves and a magic sheep.

Strategy: Adapting Existing Proofs, Example

- **Ex:** Show that $\sqrt{3}$ is irrational.
- (Generalization) If p is prime, then $\sqrt{p}$ is irrational.
- (Further generalization) If n is not a perfect square, then $\sqrt{n}$ is irrational.

since they are irrational

$\sqrt{3} = \frac{m}{n}$, m, n, are co-prime $3n^2 = m^2$

$\Rightarrow 3n^2 = 9k^2 \Rightarrow n^2 = 3k^2 \Rightarrow n = 3k$

$\sqrt{p} = \frac{m}{n}$

$n = m^2$ $\times$ $p_1 \ldots p_k$ $\sqrt{p_1 \ldots p_{1}}$

Strategy: Looking for Counter Examples

- **Ex:** Every positive integer is the sum of two squares
- **Ex:** Every positive integer is the sum of three squares

$1 = 1^2 + 0^2, \quad 2 = 1^2 + 1^2, \quad 3 = 1^2 + 1^2 + 1^2$

$1 = 1^2 + 0^2 + 0^2, \quad 2 = 1^2 + 1^2 + 0, \quad 3 = 1^2 + 1^2 + 1^2$

$4 = 2^2 + 0^2 + 0^2, \quad 5 = 2^2 + 1^2 + 0^2, \quad 6 = 2^2 + 1^2 + 1^2, \quad 7 = 2^2 + 1^2 + 1^2 + 1^2$

Put it Together: Domino Tiling

- **Ex:** Can a checkerboard be covered by 32 dominos?
- **Ex:** Can a checkerboard, with two opposite corners removed, be covered by 31 dominos?