CS 331, Fall 2026 Today: Proofs

Mini-lecture 1 (8/24)

Proofs

We want proofs to be $\boxed{\text{Correct}}$ and $\boxed{\text{Well-written}}$

Correct: Every statement is logically true

All edge cases matter! All primes are odd X

Typical structure: True statement 1

True statement 2 builds on

True statement 3

Well-written: reader can follow flow of argument

This is an art! Best way: practice lots, discuss

Helpful tips: "Declare gameplan"

Organize into self-contained claims

Implication

$A \Rightarrow B$ "if A is true, so is B"

Simple structure: Prove D

A, $A \Rightarrow B$, $B \Rightarrow C$, $C \Rightarrow D$

obvious
true statement

Theorem: For all $x, y \geq 0$, $\underbrace{\sqrt{xy} \leq \frac{x+y}{2}}_{\star}$

Proof:

① $0 \leq a \leq b \iff 0 \leq \sqrt{a} \leq \sqrt{b}$

② $xy \leq \frac{x^2 + 2xy + y^2}{4} \iff \star$

③ $\ldots \iff 0 \leq x^2 - 2xy + y^2$

④ $\ldots \iff 0 \leq (x-y)^2$

$\blacksquare$

Proof, but better:

(1) $0 \leq (x-y)^2$ obvious

(2) $0 \leq x^2 - 2xy + y^2$

(3) $xy \leq \frac{x^2 + 2xy + y^2}{4}$

(4) $\sqrt{xy} \leq \frac{x+y}{2}$

each follows from previous by implication

$\blacksquare$

Theorem: Let $x, y \in \mathbb{R}^d$, then, ← dimension

$$\left(\sum_{i \in [d]} x_i y_i\right)^2 \leq \left(\sum_{i \in [d]} x_i^2\right)\left(\sum_{i \in [d]} y_i^2\right)$$

$[d] = \{1, 2, 3, \ldots, d\}$

e.g.

$x = \begin{pmatrix} 1 \\ 4 \\ 2 \end{pmatrix}$ $y = \begin{pmatrix} -3 \\ -2 \\ 4 \end{pmatrix}$ $(-3)^2 \leq (21) \cdot (29)$

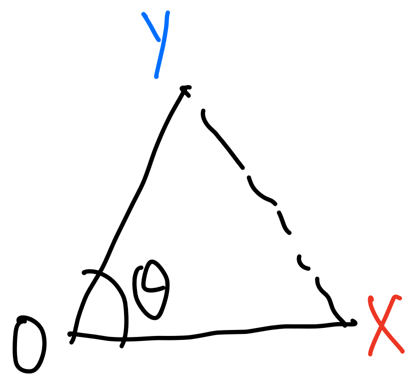
"Proof": $\|x\|_2 =$ "Length" of vector x

$$RHS = \|x\|_2^2 \; \|y\|_2^2$$

$$\| \quad \left(x_1^2 + x_2^2 \cdots + x_d^2\right)$$

$$LHS = \left(x \cdot y \text{ "dot product"}\right)^2$$

$$= \|x\|_2^2 \; \|y\|_2^2 \cos^2\theta$$

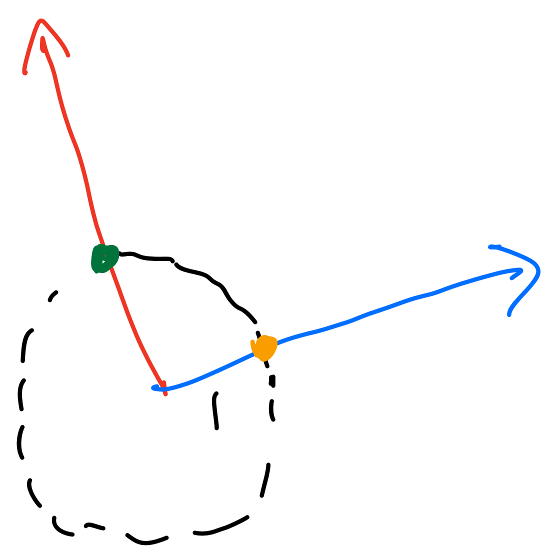


So, $LHS \leq RHS \iff \cos^2\theta \leq 1$

Idea: we may as well consider <u>unit vectors</u>

Proof: Let

$$u = \frac{x}{\|x\|_2} \qquad v = \frac{y}{\|y\|_2}$$



Claim 1: $\sum_{i\in[d]} u_i^2 = 1, \quad \sum_{i\in[d]} v_i^2 = 1$

Because $\sum_{i\in[d]} u_i^2 = \frac{1}{\|x\|_2^2} \sum_{i\in[d]} x_i^2 = 1$

Claim 2: $(\star) \iff \left(\sum_{i\in[d]} u_i v_i\right)^2 \leq 1$

Because multiply both sides by $\|x\|_2^2 \|y\|_2^2$

Claim 3: $\left(\sum_{i\in[d]} u_i v_i\right)^2 \leq 1$

$$\sum_{i\in[d]} u_i v_i \leq \sum_{i\in[d]} \frac{u_i^2 + v_i^2}{2} = \frac{1}{2} + \frac{1}{2} = 1$$

(old theorem) (Claim 1)

$$-\sum_{i\in[d]} u_i v_i \leq \sum_{i\in[d]} \frac{u_i^2 + v_i^2}{2} = \frac{1}{2} + \frac{1}{2} = 1 \quad \blacksquare$$

Contrapositive

What does $A \Rightarrow B$ mean?

Not "A is true". Rather, "if A is true, so is B"

		B: True	B: False
A	True		X
	False		

Rules out 1/4 of possible worlds

Equivalent statement: "if B is false, so is A"

Shorthand: $\neg B \Rightarrow \neg A$

Example

"if you go to lecture, these notes will make sense"

Warning: debatable

"if these notes don't make sense you did not go to lecture"

Theorem: If $p = 2^n - 1$, $n \in \mathbb{N}$

p is prime implies n is prime.

Proof: Contrapositive. n composite $\Rightarrow$ p composite

$$n = ab$$

$$p = 2^n - 1 = m^b - 1, \quad m = 2^a$$

$$p = (m-1)(1 + m + m^2 + \dots + m^{b-1}) \quad \blacksquare$$

composite

Contradiction

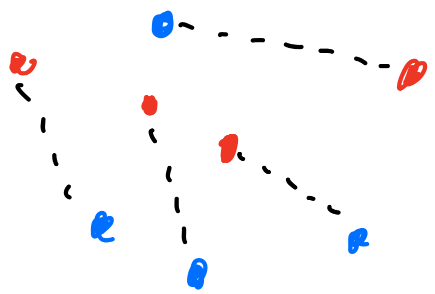
You're asked: prove <statement>

① Assume "for the sake of contradiction" $\neg$ statement

② Show $\neg$ statement $\Rightarrow \dots \Rightarrow \dots \Rightarrow$ obviously false

③ $\neg$ statement must also be false. $\blacksquare$

Theorem: Let $n \in \mathbb{N}$. Suppose R = n red points, B = n blue points in the plane. There's a way to pair up R & B s.t. no crossing lines.

Ex. 

Proof: Pick pairings w. minimal total length

$$|r_1 b_1| + |r_2 b_2| + \dots + |r_n b_n|$$

Claim: has no crossings.

Suppose for contradiction otherwise. Consider "uncrossings"

Shorter!

So, it wasn't the minimal total length $\Rightarrow$ Contradiction $\blacksquare$

Induction

Covered in class.

(1) $S(1)$ is true

(2) $S(n) \Rightarrow S(n+1) \;\forall n$

$\Big\}$ all $S(n)$ is true

We proved $x^n - 1 = (x-1)(1+x+x^2+\dots+x^{n-1})$

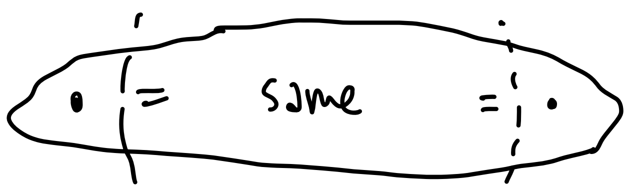
Key idea: $\underbrace{x^{n+1}-1}_{S(n+1)} = \underbrace{(x^{n+1}-x^n)}_{(x-1)\cdot x^n} + \underbrace{(x^n-1)}_{S(n)}$

Warning Check (2) holds for all $n \geq 1$!

Example: All horses are same color.

"Proof": $S(n)$ = All n horses are same color.

Spot the bug: $S(1)$ ✓ $\quad S(n) \Rightarrow S(n+1)$?



$n+1$

May as well do strong induction (used in recursive algos!)

$$\underbrace{S(1), S(2), \ldots S(n)}_{\text{all true already}} \implies S(n+1)$$

$\boxed{\text{Puzzle}}$ There's 1000 dragons on an island.

All can see all other dragons' eyes, but not their own.

All eyes are red. Dragons can't communicate.

If you know your eyes are red you turn into sparrow @ midnight when you find out.

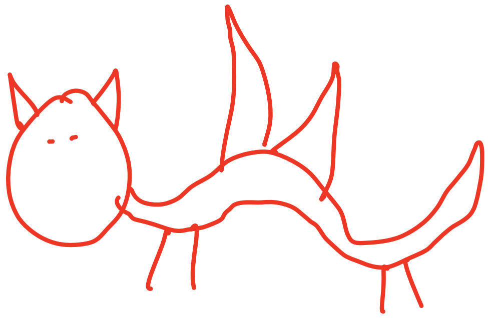
One day evil wizard  arrives & says

"At least one of you has red eyes"

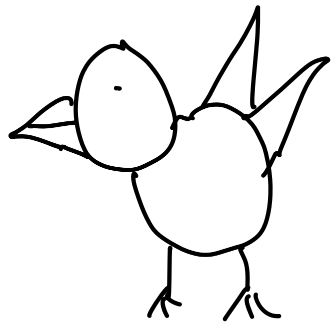
Which night do dragons turn into sparrows?

Q: What is "S(n)"? n=1000...

If n=1:

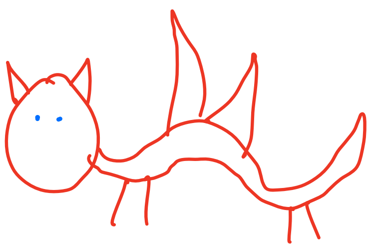


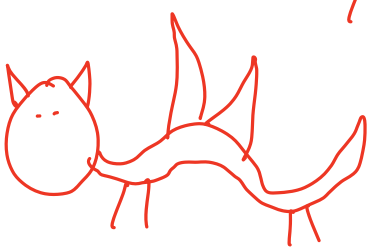
day 1 $\Longrightarrow$



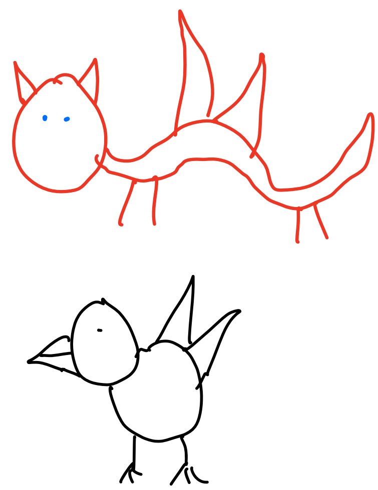
If n=2: me

Case 1:





day 1 $\Longrightarrow$



Case 2: I have red eyes...

S(n): n dragons turn to sparrows after day n

Why is S(n) => S(n+1)? (Casework again...)