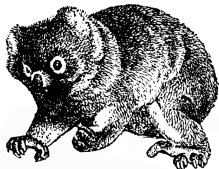


# A Soft Introduction to zkML

Lucas A. Vittor

lucasvittor.com, @lvvittor

August 26, 2023



## Warm Up

1. Who works in Web3 as a developer/researcher?
2. Who works in a data-first company?
3. Who works with Machine Learning (ML)?
4. Who knows what Zero Knowledge Proofs (ZKPs) are?
5. What is the name of the set of problems that can be solved in the  $\mathcal{O}(n^k)$  time complexity type?

# What are Proofs?

## Def. Mathematical Proof

*A deductive argument for a proposition, showing that the stated assumptions logically guarantee the conclusion.*

Common methods of proof:

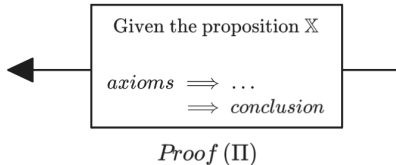
1. Direct
2. Contradiction
3. Contraposition
4. Induction

# Proofs as Static Objects

Verifier



Prover



## Example of a Proof

$\sqrt{2}$  is irrational

Assume  $\sqrt{2}$  is rational, so  $\sqrt{2} = \frac{a}{b}$  in simplest form.

Squaring both sides yields  $2 = \frac{a^2}{b^2}$ , implying  $a^2 = 2b^2$ .

Since  $a^2$  is even,  $a$  must be even (odd<sup>2</sup> is odd).

Let  $a = 2k$ , then  $4k^2 = 2b^2$ , giving  $2k^2 = b^2$ .

Now, both  $a$  and  $b$  are even, contradicting their coprimality.

Thus, our assumption is false, and  $\sqrt{2}$  is irrational. ■

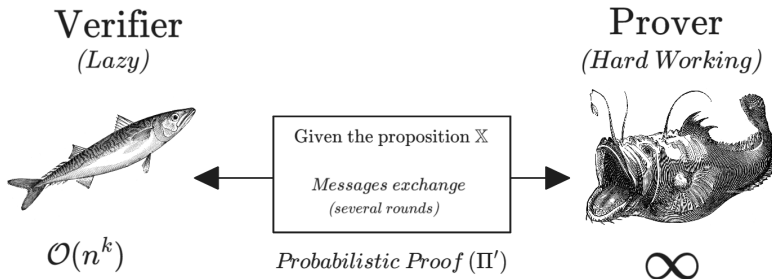
## How about efficiency?

Given a valid proof  $\Pi$  about a proposition  $\mathbb{X}$ ,  
how "*easy*" is to convince me it's true?

# An Intuition About Interactive Proofs (IPs)

1. ***True** propositions are **Provable***
2. ***False** propositions **NOT***

# Visualizing IPs





# Defining Knowledge

Q: *How much knowledge to verify a proof?*

Q: *What is knowledge?*

# Zero Knowledge Proofs (ZKPs)

*“Nothing but the truth”*

# Formal Definition of ZKPs

## Def. Zero Knowledge Proof

Suppose  $\mathcal{L}$  is a language. A zero-knowledge protocol is an interaction between two algorithms  $P$  and a probabilistic polynomial time (PPT) algorithm  $V$  with  $P$  trying to convince  $V$  that  $x \in \mathcal{L}$  and the satisfying properties:

- (i) *Completeness*
- (ii) *Soundness*
- (iii) *Zero-knowledge*

## ZK Properties Definition

### Completeness

If the proposition  $\mathbb{X}$  is **true** and  $V, P$  are honest  $\Rightarrow V$  will be convinced.

### Soundness

If the proposition  $\mathbb{X}$  is **false**  $\Rightarrow \nexists$  cheating  $P$  who can convince an honest  $V$  that  $\mathbb{X}$  is true (except with some small probability).

### Zero Knowledge

$\forall x \in \mathcal{L}, z \in \{0, 1\}^*, \text{View}_V[P(x) \longleftrightarrow V(x, z)] = S(x, z)$

# The Two Balls Problem

Proposition  $\mathbb{X}$ :

*I have two balls of different colors.*

# Soundness Score

$k$	$1/2^k$
1	0.5
2	0.25
3	0.125
4	0.0625
5	0.03125
6	0.015625
$\vdots$	$\vdots$

# Where We Can Use ZKPs?

*One proposition?*

*Some propositions?*

*Special propositions?*

# Tip of the Iceberg

*Everything provable **is provable**  
in Zero-Knowledge.*



# Machine Learning (ML)

*Which option is correct?*

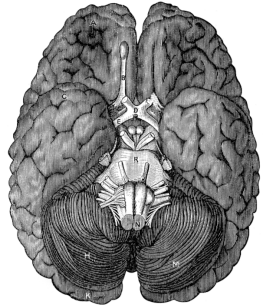
1)  $\text{AI} = \text{ML}$

2)  $\text{AI} \neq \text{ML}$

# What is AI?

AI

$\geq$

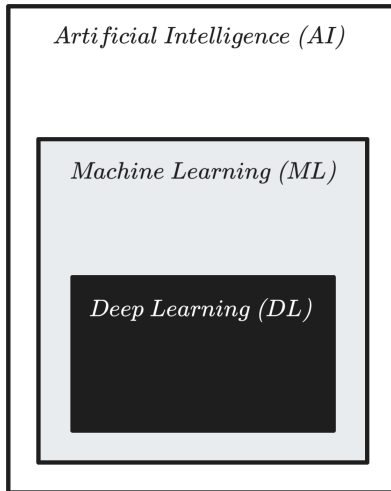


# What is ML?

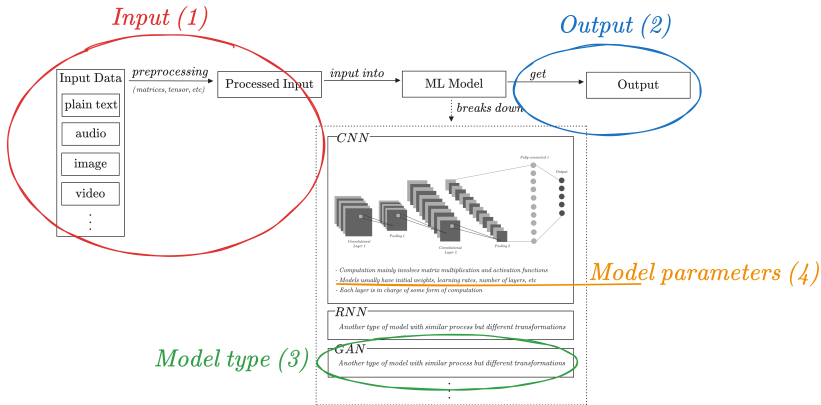
*A computer program is said to learn from experience  $E$  with respect to some task  $T$  and some performance measure  $P$ , if its performance on  $T$ , as measured by  $P$ , improves with experience  $E$ . — Tom Mitchell, 1997*

*It is the adaptation of the free parameters of a system in order to satisfy an object function. — J. M. Santos*

# Venn Diagram



# ELI5 ML



# Issues with State Of the Art ML

1. *Black-box nature of NNs*

2. *Privacy*

Warm Up  
○

Zero Knowledge Proofs (ZKPs)  
○○○  
○  
○  
○  
○○○○○  
○○

Machine Learning (ML)  
○○○○○

zkML  
●

Web3 Tales  
○

$$zk + ML = \heartsuit$$

# Web3 Tales

*Making web3 uncool again @ web3tales.com*

