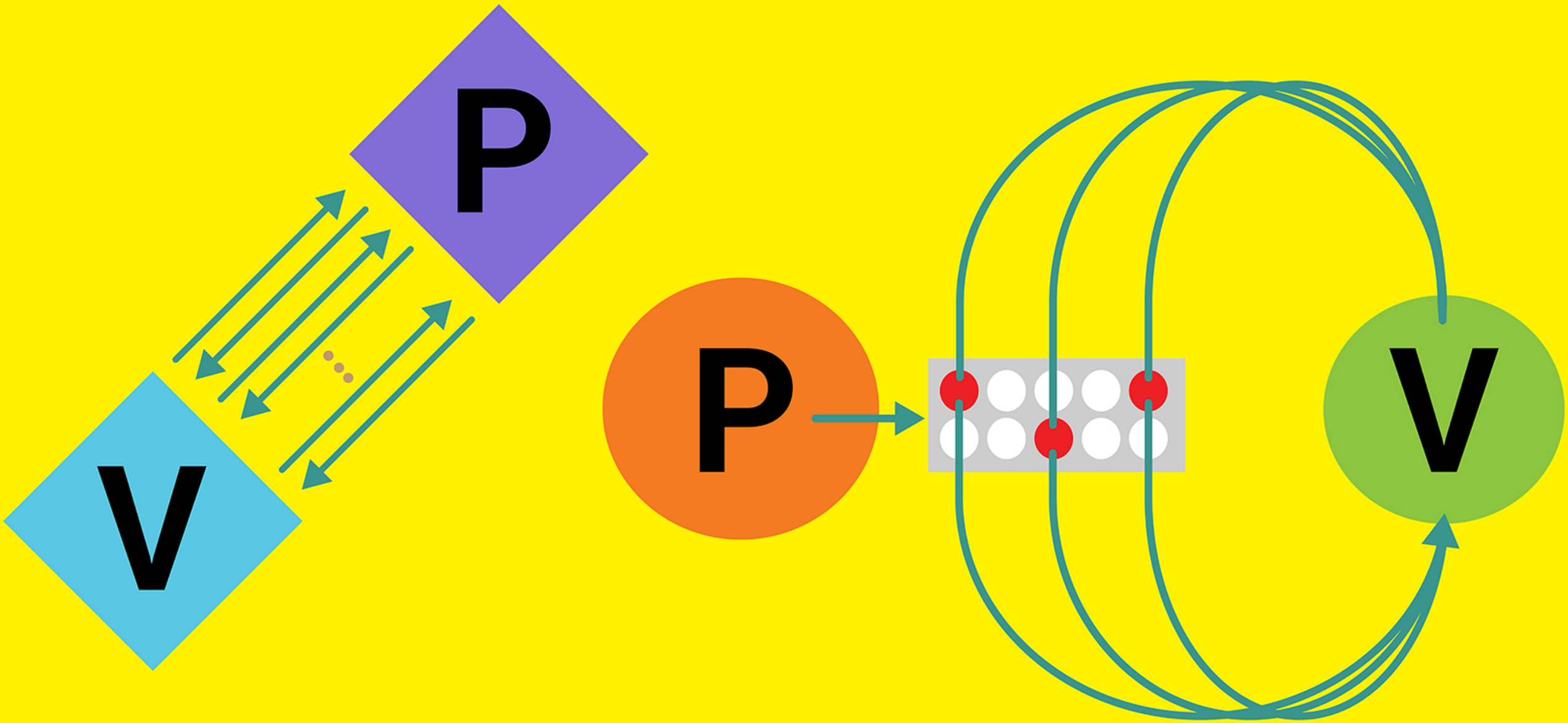
Foundations of Probabilistic Proofs

A course by **Alessandro Chiesa**



Organization

Instructor: Alessandro Chiesa
Teaching Assistants: Burcu Yıldız, Guy Weissenberg

Lectures:
Tuesdays and Wednesdays 13:15-15:00.
In person attendance/interaction.
No recordings or live streaming.

Recitations: Wednesdays 15:15-16:00

Office hours:
- Alessandro → by appointment
- Burcu, Guy → Wednesdays 16:15-17:00 in BC242

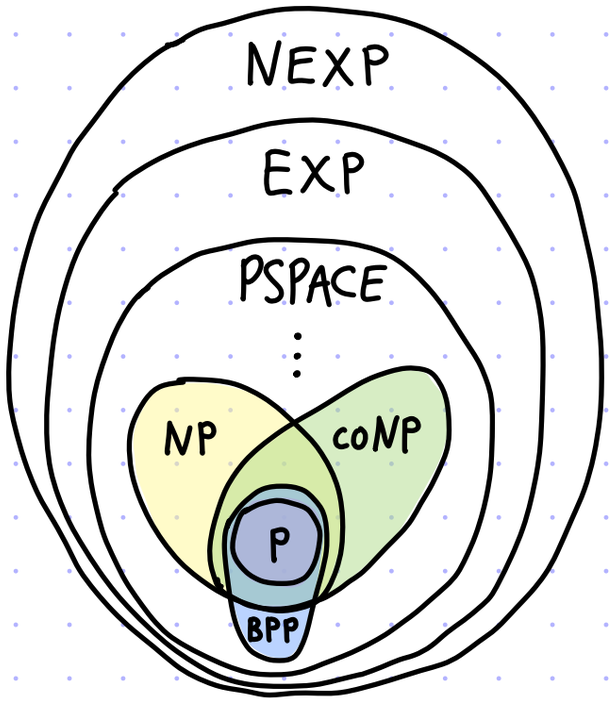
Materials: `probabilistic-proofs-course.org`

Assignments: weekly homework + end-of-semester project

Grading: 60% homework + 30% project presentation + 10% project report

Background

- finite fields ($\mathbb{F}_q$ for prime q)
- basics of linear codes (rate, distance, ...)
- univariate polynomials ($\mathbb{F}[X]$) and multivariate polynomials ($\mathbb{F}[X_1,\dots,X_n]$)
- basic complexity theory:
  - machines, circuits, reductions
  - Cook-Levin theorem
  - basic complexity classes



Goals

- understand different MODELS
  - interactive proofs (IPs)
  - probabilistically checkable proofs (PCPs)
  - interactive oracle proofs (IOPs)
- understand their POWER
  - check "hard" problems beyond BPP
  - exponential savings in communication or time
  - zero knowledge
- design & analyze

Course Plan

Unit 1: Interactive Proofs
- arithmetization
- sumcheck protocol
- IP=PSPACE
- low-degree extensions
- GKR protocol
- zero-knowledge IPs

Unit 2: Probabilistically Checkable Proofs
- linearity testing
- exponential-size PCPs
- low-degree testing
- polynomial-size PCPs
- sublinear verification

Unit 3: Interactive Oracle Proofs
- linear-size IOPs
- univariate sumcheck
- FRI protocol

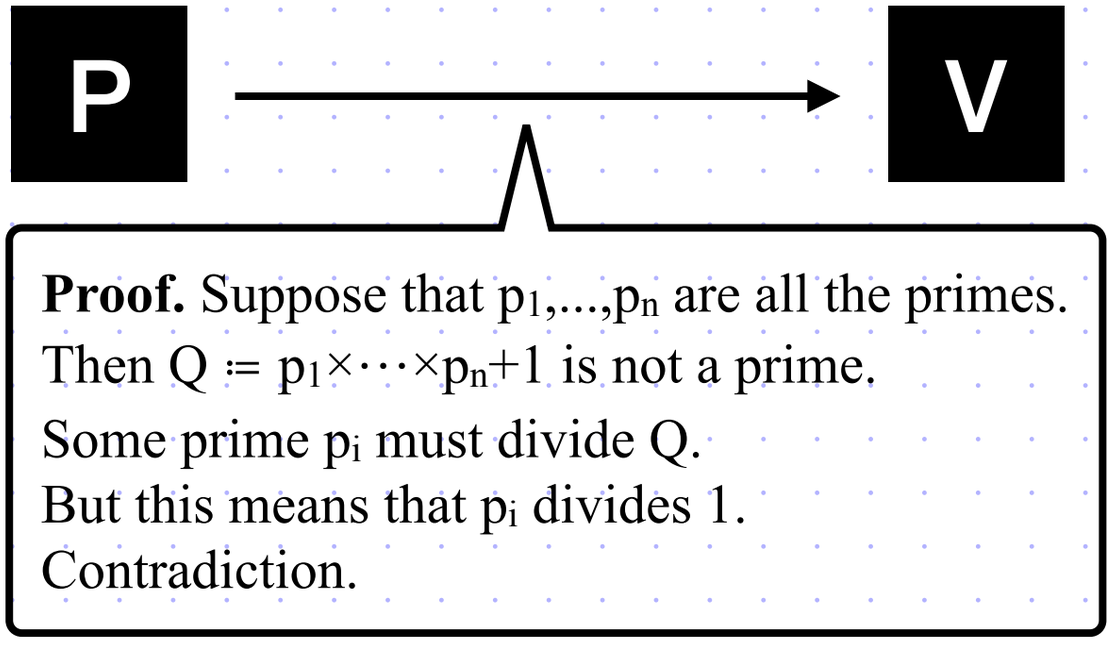
Unit 4: Additional Topics
- holographic proofs
- proof composition
- PCP Theorem
- public vs. private coins
- limitations of probabilistic proofs
- parallel repetition
- hardness of approximation

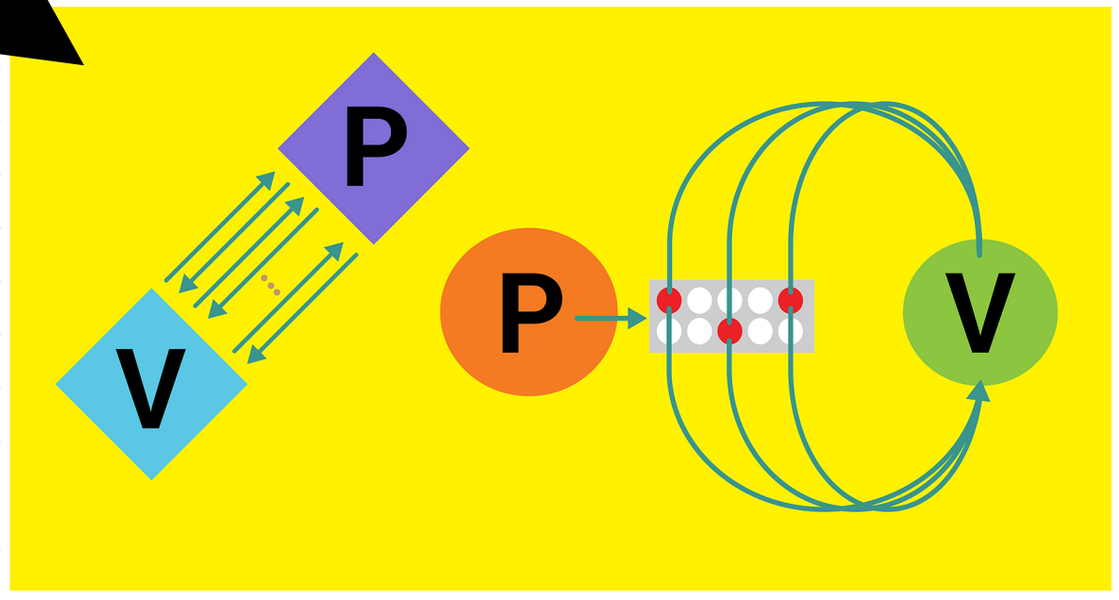
Why Care? [1/3]

Philosophy

Probabilistic proofs are meaningful re-envisionings
of the classical notion of a mathematical proof
(which did not change much for 2000+ years).

Theorem.
There are infinitely many primes.





Why Care? [2/3]

Theory

Probabilistic proofs are an invaluable perspective and set of tools to solve problems in the theory of computation (and beyond!).

privacy & scalability in cryptography

COMPUTATIONALLY SOUND PROOFS*

SILVIO MICALI†

Abstract. This paper puts forward a new notion of a proof based on computational complexity and explores its implications for computation at large.

hardness of approximation (PCP Theorem & co.)

Interactive Proofs and the Hardness of Approximating Cliques

Uriel Feige * Shafi Goldwasser † Laszlo Lovasz ‡
Shmuel Safra § Mario Szegedy ¶

power of entanglement

MIP* = RE

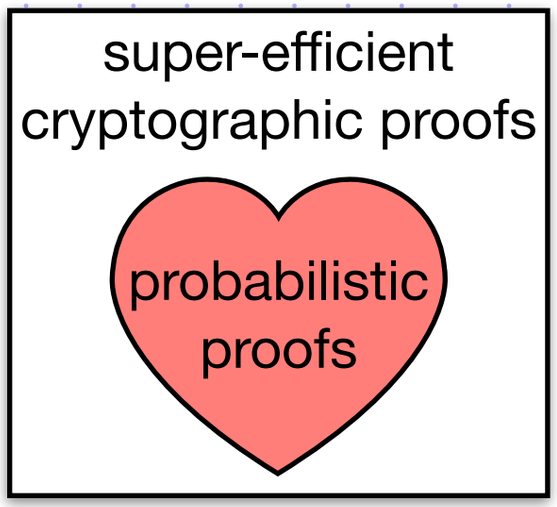
Zhengfeng Ji*[1], Anand Natarajan†[2,3], Thomas Vidick‡[3], John Wright§[2,3,4], and Henry Yuen¶[5]

Why Care? [3/3]

Security

Probabilistic proofs are the algorithmic heart of super-efficient cryptographic proofs.

Such cryptographic proofs are a powerful tool in secure distributed systems and more.



1. privacy-preserving digital currencies

Zcash MONERO Aleo

2. scalability in blockchains ("roll-ups")
   (see www.l2beat.com)

STARKWARE Aztec polygon
zkSync LOOPRING Succinct

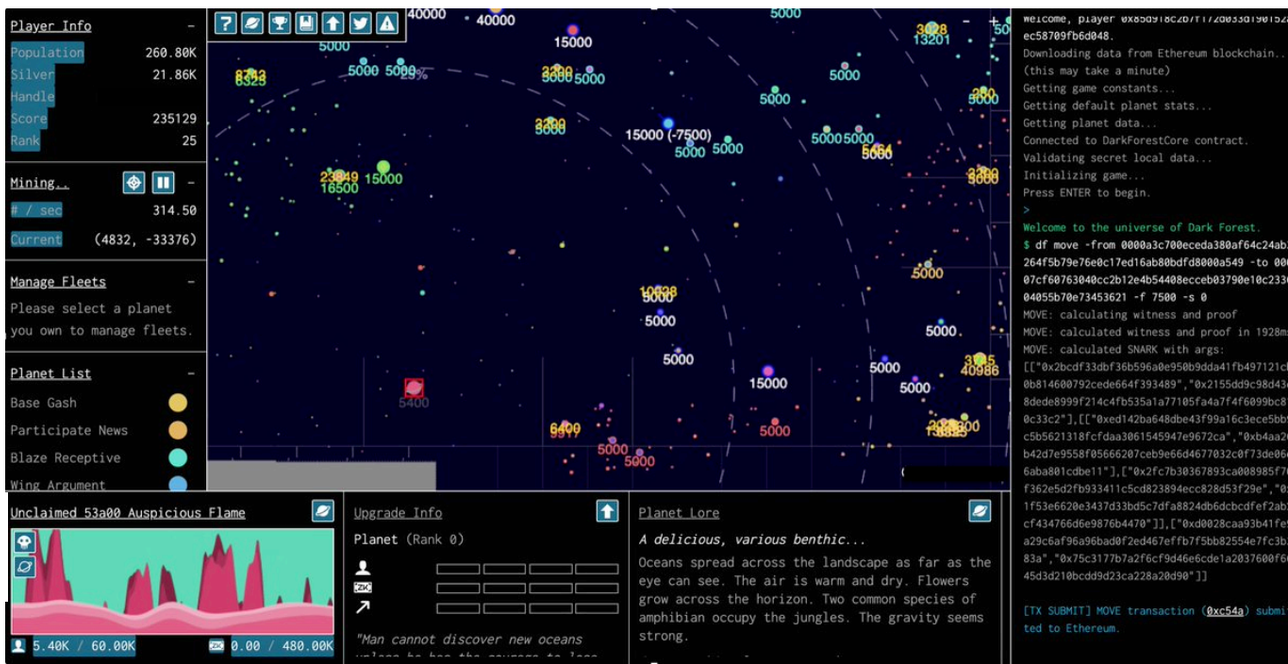
3. disclose software vulnerabilities in zero knowledge

4. digital identities with privacy

5. image authentication with privacy

⋮

N. P2P games!



Dark Forest
zkSNARK space warfare

Let's get started!

Bibliography

Background

Fundamentals of computational complexity:
Computational Complexity: A Modern Approach by Sanjeev Arora and Boaz Barak.
- Turing machines, complexity classes, and reductions (1.2-1.5, 2.2).
- The Cook–Levin theorem (2.3).
- P, NP, PSPACE, NEXP, and their complete languages (1.6, 2.1, 2.6, 4.1, 4.2).
- The computation model of Boolean circuits, circuit satisfiability, and exponential size circuits (6.1-6.4, 6.8).
- Probabilistic computation and BPP (7.1-7.4).

(▸Theory of computation course) by Michael Sipser.

Finite fields and their properties:
- Forney's Introduction to finite fields (chapter 7).
- Sutherland's notes on finite fields and integer arithmetic.
- Guruswami's cheat sheet on finite fields.

Theory

- [Micali 2000]: Computationally sound proofs, by Silvio Micali.
- [FGLSS 1996]: Interactive proofs and the hardness of approximating cliques, by Uriel Feige, Shafi Goldwasser, Laszlo Lovasz, Shumel Safra, Mario Szegedy.
- [JNVWY 2020]: MIP* = RE. Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, Henry Yuen. (CACM article)

Practice

- **Privacy-preserving digital currencies**: Zcash, Monero, Aleo.
- **Roll-ups** (see l2beat.com): Starkware, Aztec, Polygon, zkSync, Loopring, ...
- **zkVMs**: RISC0, Succinct, Jolt.
- **Digital identities:** zkLogin, Google ZK.
- **Image authentication:** PhotoProof, ZK-IMG, VerITAS.
- Software vulnerabilities, P2P games, ...