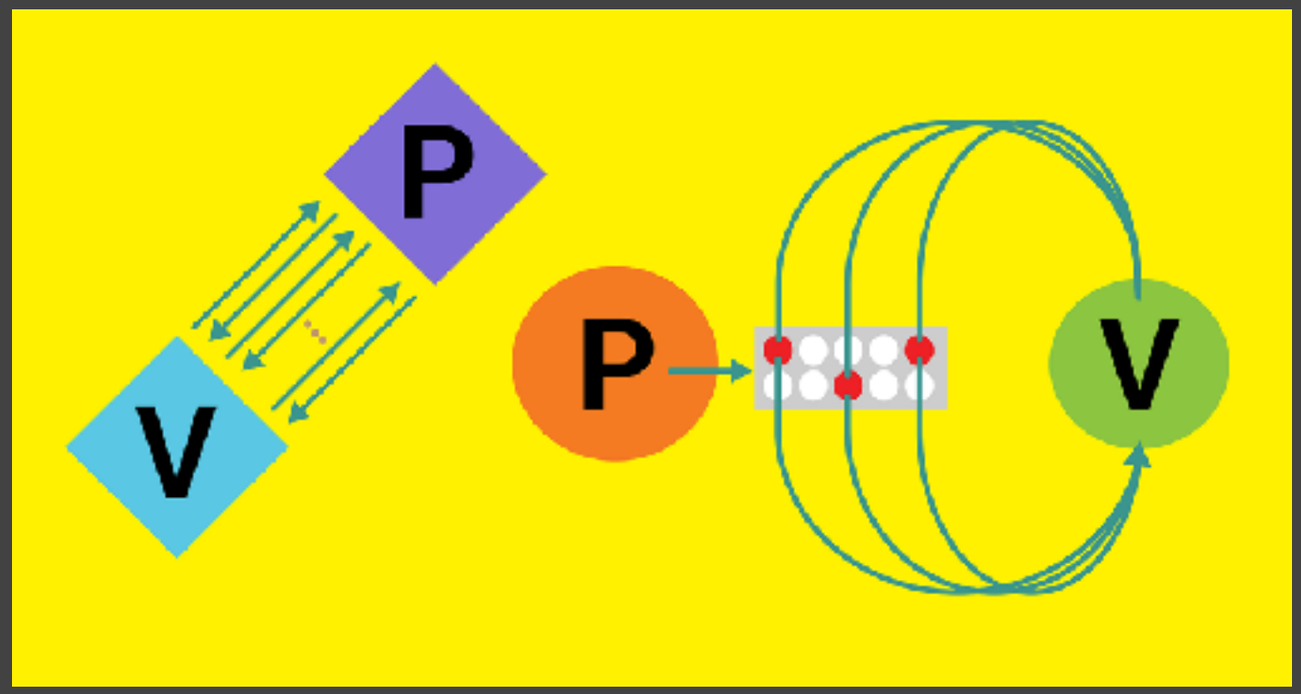
Foundations of Probabilistic Proofs



Fall 2020

Alessandro Chiesa

Foundations of Probabilistic Proofs

Administrivia

- Tuesdays and Thursdays at 11:00 - 12:30 (CA time)
- ongoing syllabus on course website
- all course communication on Piazza (access code is fopp-2020)

  ↑ me to you & you to me
- for those taking course for credit:
  - occasional homeworks] submit on Gradescope
  - research project]
  - working on course notes
  - participation (live or on Piazza)

  } anyone else also welcome to do any of these
- this online course is an experiment: feedback on format is welcome!

Course Plan

Unit 1: Interactive Proofs

arithmetization, sumcheck, low-degree extension, GKR, IP=PSPACE, limitations, zk

Unit 2: Probabilistically Checkable Proofs

Hadamard PCP, BFLS PCP, linearity testing, low-degree testing, zero testing

Unit 3: Interactive Oracle Proofs

linear-size proofs, univariate sumcheck, FRI protocol

Unit 4: Proof Composition

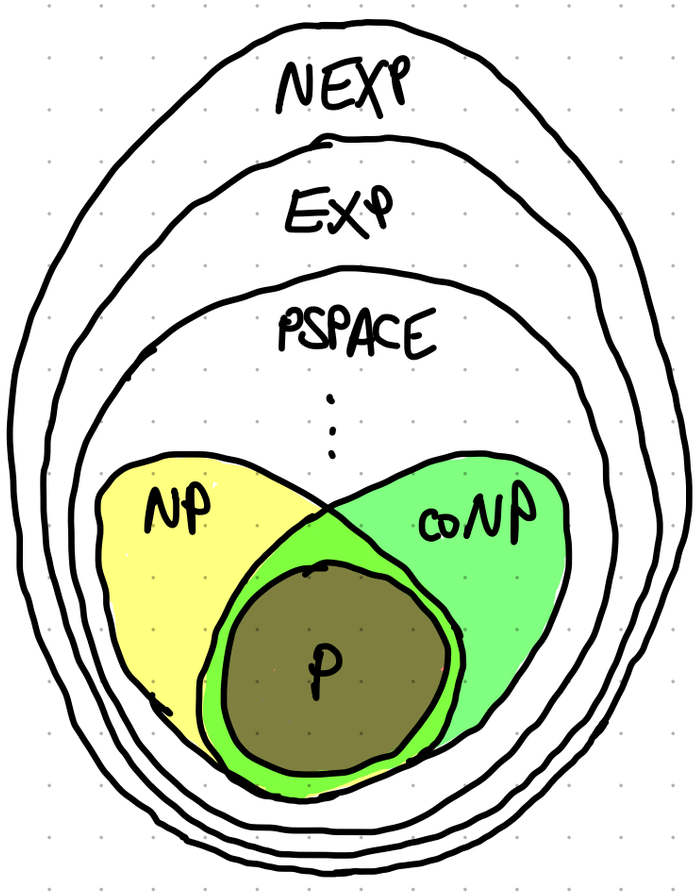
robust proofs, proximity proofs, composition, PCP theorem

Unit 5: parallel repetition

Verbitsky's theorem, Raz's theorem, sliding scale conjecture

Background

- finite fields ($\mathbb{F}_q$ for prime power q)
- basics of linear codes (rate, distance, ...)
- polynomials $\mathbb{F}[x]$, $\mathbb{F}[x_1, \ldots, x_n]$
- basic complexity theory
  - machines, circuits, reductions
  - Cook-Levin Theorem
  - basic complexity classes



Goals

- understand different models of probabilistic proofs (IP, PCP, IOP)
- understand their power:
  - check "hard" problems beyond BPP
  - exponential savings in communication or verification
  - zero knowledge
- design & analyze probabilistic proofs

Why care?

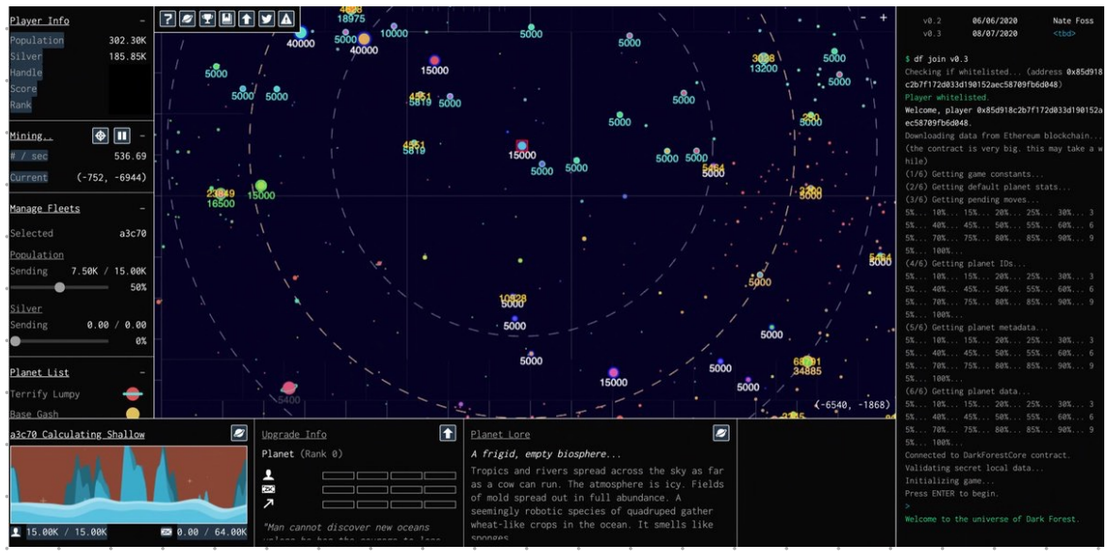
- philosophy ➡ meaningful re-envisioning of the classical notion of a mathematical proof (which has not changed for 2k+ years)
- theory ➡ invaluable perspective and set of tools to solve problems
  - hardness of approximation (PCP Theorem & co.)
  - power of entanglement ($MIP^* = RE$)
  - applications to privacy & scalability in cryptography
- security ➡ super-efficient cryptographic proofs

  probabilistic proofs

powerful tool in distributed systems:

① privacy-preserving digital currencies

② scalability tool in blockchains ("roll ups")



③ fun P2P games!

Let's get started!