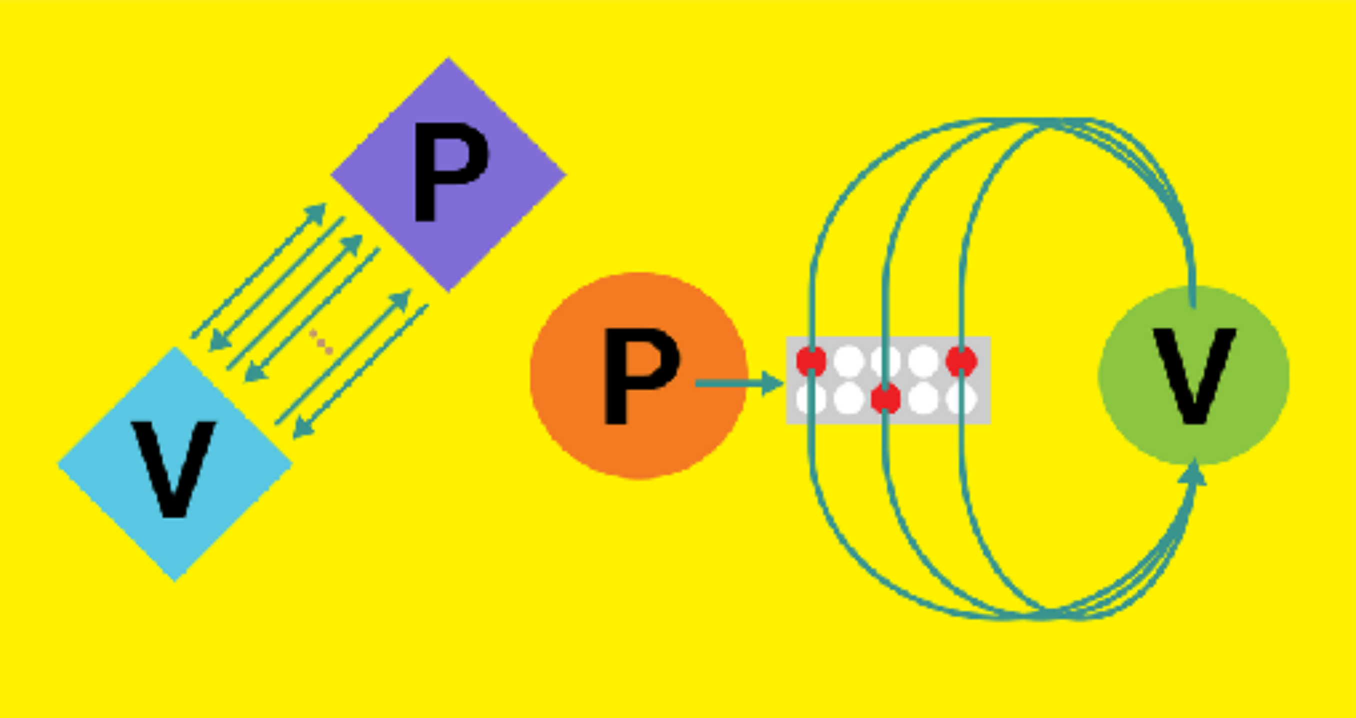
Foundations & Frontiers of Probabilistic Proofs



Summer 2021

MSRI Mathematical Sciences Research Institute

ethereum foundation

Course Staff

Instructors

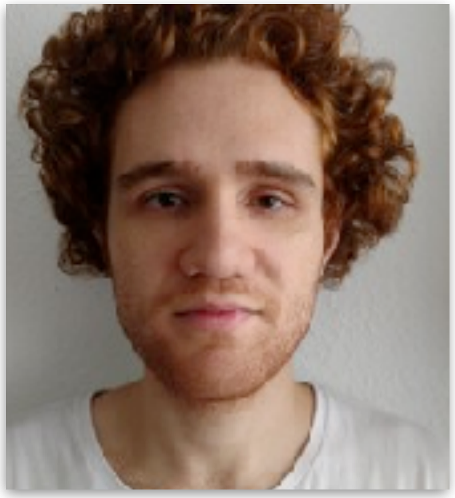
Alessandro Chiesa

Tom Gur

Teaching Assistants

Gal Arnon

Inbal Livni Navon



Marcel Dall'Agnol

Nick Spooner

Organization

This school consists of 10 days over two weeks (twice Monday to Friday).

We teach 2 courses: **A** and **B** (course plan in a few slides).

Every day consists of:
- 1.5h lecture + 1h recitation for **Course A**
- 1.5h lecture + 1h recitation for **Course B**

Lectures: live on Zoom and then available as recording

Recitations: live on Zoom but not recorded

You have been assigned to a recitation group (one of G, I, M, N).
You must attend the assigned recitations for that grou[.

Office hours: 2x per day to serve different time zones

come to mingle in today's (first) office hour!

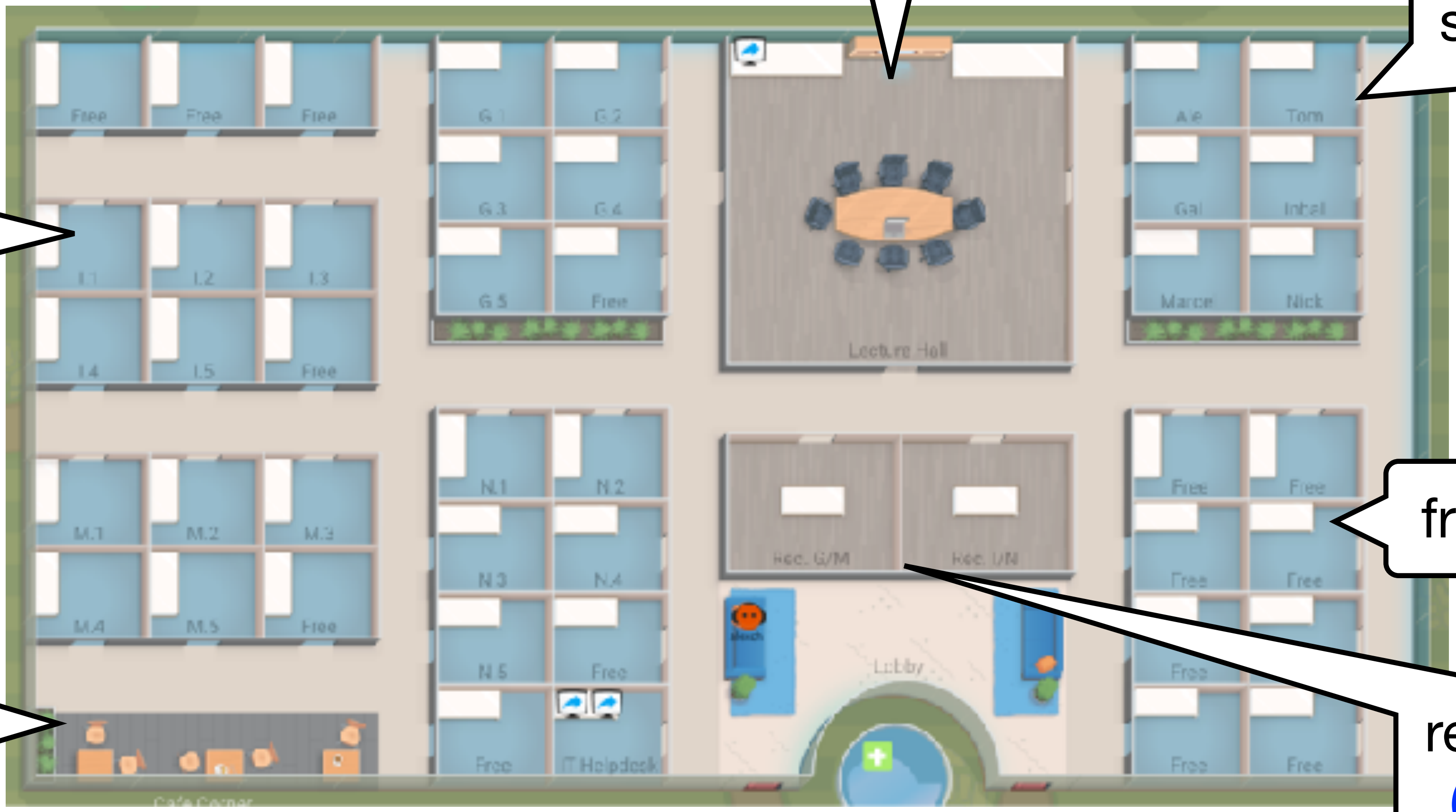
Working groups: collaboration on worksheet during recitation (and offline)

You have been assigned to a working group of 3-4 people.
You must collaborate within this group during recitations.

This summer school is in its first edition --- feedback is welcome!

Software

(1) Sococo: virtual space for us



lecture room (& Zoom link)

staff offices

working group rooms

free offices

hangout area

recitation rooms (& Zoom links)

(2) Slack: all course communication

#ffpp-2021-general → main channel (daily schedule, roster, materials are pinned there)

#ffpp-2021-background → background material (references are pinned there)

#ffpp-2021-lecture → lecture discussion/questions

#ffpp-2021-recitation-{g,i,m,n} → recitation discussion/questions split by group

#ffpp-2021-social → social channel

Private questions: DM on Slack your TA or the instructors

Working groups: please create your own private Slack channels to collaborate

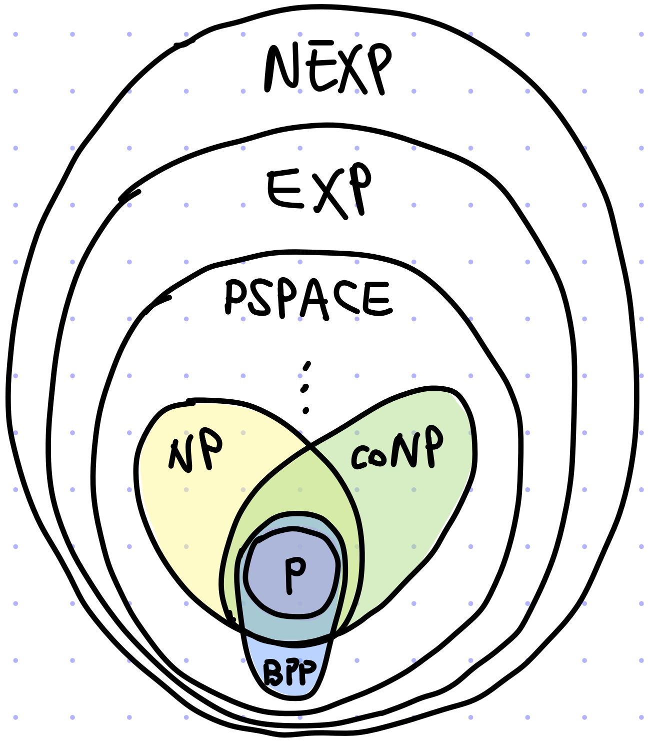
Course Plan

Day	Course A (Ale)	Course B (Tom)
01	Introduction to IPs	Introduction to PCPs
02	Sumcheck Protocol	Linearity Testing
03	IP for PSPACE	Low-Degree Testing
04	Doubly-Efficient IPs	FRI Protocol (1/2)
05	Zero-Knowledge IPs	FRI Protocol (2/2)
06	Limitations of IPs	Exp-Size PCPs
07	Intro to IOPs	Poly-Size PCPs
08	Linear-Size IOPs for Circuits	PCPs with Sublinear Verification
09	Linear-Size IOPs for Machines	Proof Composition
10	Limitations of IOPs	Applications of PCPs

🟥	IPs	🟧	Property Testing
🟩	IOPs	🟦	PCPs

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 of probabilistic proofs (interactive proofs, probabilistically checkable proofs, interactive oracle proofs)
- understand their power
  - check "hard" problems beyond BPP
  - exponential savings in communication or time
  - zero knowledge
- design & analyze probabilistic proofs

Why Care?

- **philosophy** meaningful re-envisioning(s) of the classical notion of a mathematical proof (which did not change for 2000 years)

- **theory** invaluable perspective and set of tools to solve problems

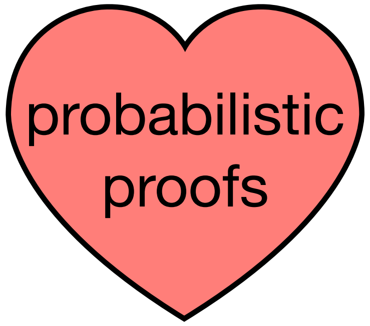
privacy & scalability in cryptography

hardness of approximation (PCP Theorem & co.)

power of entanglement (MIP*=RE)

- **security** powerful tool in distributed systems

super-efficient cryptographic proofs

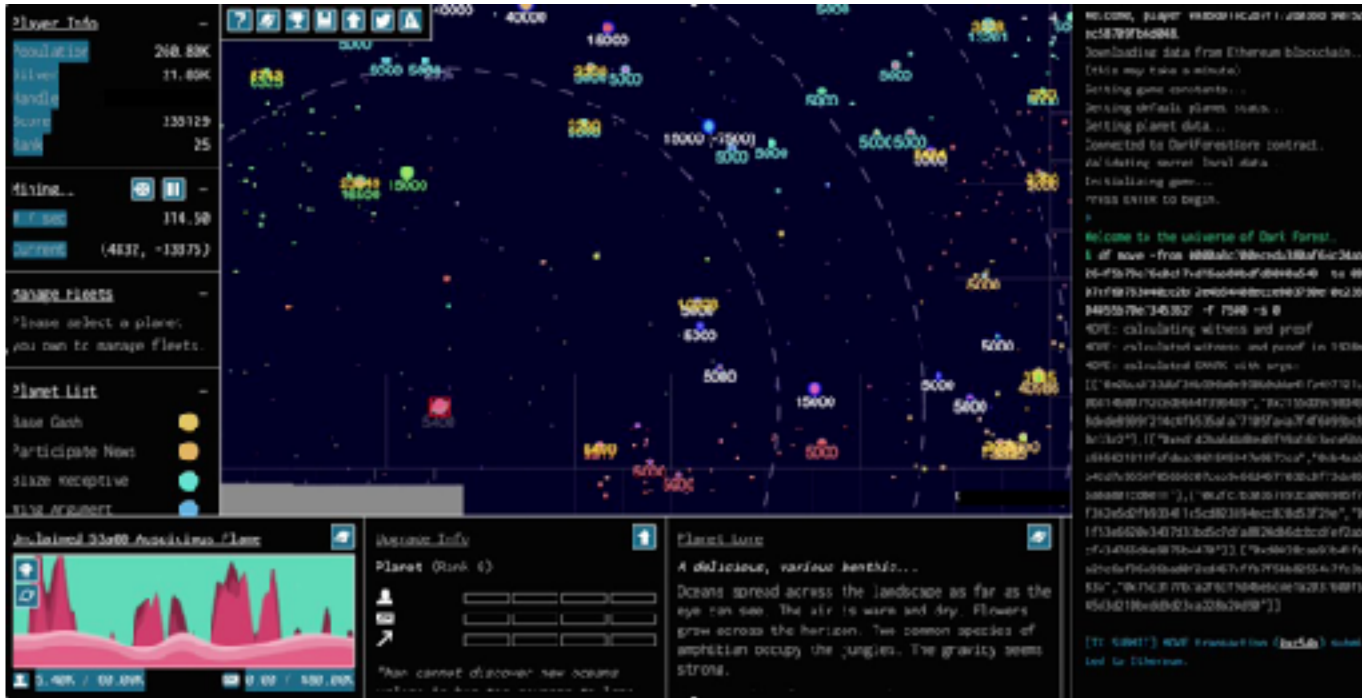


probabilistic proofs

1. privacy-preserving digital currencies
2. scalability tool in blockchains ("roll-ups")

⋮

N. P2P games!



```
Downloading data from Ethereum blockchain...
(this may take a minute)
Getting game constants...
Getting planet data...
Connected to DarkForestCore contract.
Initializing game...
Press ENTER to begin.
Welcome to the universe of Dark Forest.
calculating witness and proof
```

A delicious, various benthic...

Oceans spread across the landscape as far as the eye can see. The air is warm and dry. Flowers grow across the horizon. Two common species of amphibian occupy the jungles. The gravity seems strong.

Let's get started!