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
  - four those taking course for credit:
    - occasional homeworks ] submit on Gradescope ] anyone else also welcome to do any of these
    - research project
    - working on course notes
    - participation (live or on Piazza)

- this online course is an experiment: feedback on format is welcome!
Course Plan

Unit 1: Interactive Proofs
- arithmetization, sumcheck,
- low-degree extension, GKR,
- IP=PSACE, limitations, 2K

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, Rat's theorem,
- sliding scale conjecture
Background

- finite fields ($\text{GF}(q)$ for prime power $q$)
- basics of linear codes (rate, distance, ...)
- polynomials $\text{IF}[x]$, $\text{IF}[x_1,...,x_n]$
- 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 & 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”)

Let’s get started!