CS789: Introduction to Probabilistic Proof Systems Spring 2025

Lecture 3.14

15/Aug/1947

Instructor: Chethan Kamath Scribe: Your name (Roll no)

1 Motivation

In this course we will study probabilistic proofs.

2 Notation

Let's try to use the following notation for the objects we will use in our course.

- Sets: $\mathcal{M} \cup \mathcal{K}$
- Complexity classes: **NP**, **coNP**
- Problems: GNI, GI
- Matrices and vectors: $\bar{A}$, $\bar{x}$
- Algorithms: P, V
- Algebraic objects: $\mathbb{G}$, $\mathbb{N}$ (natural numbers), $\mathbb{Z}$ (integers), $\mathbb{F}$ (finite fields)

3 Environments: Definitions, Lemmata, Proofs etc

Definition 1 (Interactive Protocol)**.** Write your definition of interactive protocols here.

Definition 2 (Interactive Proofs)**.** Write your definition of interactive proofs here.

Lemma 1 (Chernoff Bound)**.** *Chernoff bound states that...*

Proof. Prove using Markov's inequality... □

Open Problem 1. Is $\mathbf{P} = \mathbf{NP}$?

Homework 1. Prove that any two unequal degree-d univariate polynomials over a finite field $\mathbb{F}_q$ agree on at most d points.

You can use `\cref` to refer to the above (do give meaningful label names). You can use `\href` to refer to articles or papers online (e.g., StackExchange or Wikipedia)

- The class **IP** doesn't change when we alter Definitions 1 and 2 to allow for randomised provers.
- Cramér's theorem is quite similar to Lemma 1.
- Open Problem 1 is one of the Millenium Prize problems.
- Homework 1 is *not* one of the Millenium Prize problems.

4 Misc.

Do feel free to use the other macros defined, such as $|-1|$, $[1, n]$, $\{1, 2, 3\}$, $\{1, \ldots, 3\}$, $\langle \mathsf{P}, \mathsf{V} \rangle(x)$, $k \leftarrow \mathcal{K}$ etc