Foundations of Probabilistic Proofs (Fall 2022)
Note 2: Sumcheck Protocol
Date: 2022.09.21

This note contains definitions, theorems, facts, *etc.* that are not fully explained in lectures due to limited time. If you think there are anything missing or any mistakes, please contact ziyi.guan@epfl.ch.

1 Complexity classes

We introduce more complexity classes.

Definition 1 (#P)**.** *The class of counting problems associated with decision problems in* NP*.*

- *Problems in* #P *are formally described as to compute* $f(x)$*, where* f *is the number of accepting paths of a polynomial-time non-deterministic Turing machine that always halts.*
- $\#\text{SAT} \in \#\mathsf{P}$*: a canonical complete problem in* #P*.*

Definition 2 ($\mathsf{P}^{\#\mathsf{P}}$)**.** P *with* #P *oracle.*

- *It is standard for* A^B *to describe the set of languages solvable in* A *with oracle access to languages in* B*.*
- *Formally, we define oracle Turing machines* M^O*: a Turing machine* M *with a blackbox that is able to solve* O *with one operation.*
- $\mathsf{P}^{\#\mathsf{P}}$ *is the set of languages solvable by polynomial-time oracle Turing machines, which has oracle access to a language in* #P*:*

$$\mathsf{P}^{\#\mathsf{P}} = \bigcup_{\mathcal{L} \in \#\mathsf{P}} \mathsf{P}^{\mathcal{L}}.$$

2 Schwartz-Zippel lemma (Polynomial identity lemma)

In the soundness proof of the sumcheck protocol, we use the Schwartz-Zippel lemma. It is very important to understand the theorem because it will frequently show up in the future.

Theorem 1 (Schwartz, Zippel)**.** *Let* $p(x_1, \ldots, x_n)$ *be a non-zero polynomial of total degree* $d \geq 0$ *over a field* $\mathbb{F}$*. Let* S *be a finite subset of* $\mathbb{F}$ *and let* $r_1, r_2, \ldots, r_n$ *be selected at random independently and uniformly from* S*. Then*

$$\Pr\left[p(r_1, r_2, \ldots, r_n) = 0\right] \leq \frac{d}{|S|}.$$

Equivalently, we could say that for any finite subset S *of* $\mathbb{F}$*, if* $Z(p) = \{x \in \mathbb{F}^n \colon p(x) = 0\}$*, then*

$$|Z(p) \cap S^n| \leq d \cdot |S|^{n-1}.$$

Remark 1. *Before getting into the proof of this theorem, it is important to know how to use it. A straight-forward example would be polynomial identity testing. Given two polynomials, we want to know if they are equal. The protocol is simply to compute the values of the polynomials at random points. The soundness is guaranteed by Schwartz-Zippel lemma for polynomials with large enough degree. This is significant not only because of its simplicity but also since there are lots of algorithmic problems (some of them will show up later in this course) that reduce to polynomial identity testing.*

Proof. We prove by induction on the number of variables n.

- Base case $n = 1$: In this case, p can have at most d roots.
- Inductive step: We assume that the theorem is true for polynomials with at most $n-1$ variables. Then, write $p(x_1, \ldots, x_n)$ using polynomials with $n-1$ variables. In particular, we have that $p(x_1, \ldots, x_n) = \sum_{i=0}^{d} x_1^i p_i(x_2, \ldots, x_n)$. Since p is non-zero, there is some i such that p_i is non-zero. Take the largest such i, we know that $\mathsf{deg}(p_i) \leq d - i$. Now, by the inductive hypothesis, we have that $\Pr[p_i(r_2, \ldots, r_n) = 0] \leq \frac{d-i}{|S|}$. Moreover, if $p_i(r_2, \ldots, r_n) \neq 0$, then $p(x_1, r_2, \ldots, r_n)$ is non-zero and has degree at most i. Thus, $\Pr[p(r_1, r_2, \ldots, r_n) = 0 | p_i(r_2, \ldots, r_n) \neq 0] \leq \frac{i}{|S|}$.

  Let A be the event $p(r_1, r_2, \ldots, r_n) = 0$, B be the event $p_i(r_2, \ldots, r_n) = 0$. We have

$$\begin{aligned}
\Pr[A] &= \Pr[A \cap B] + \Pr[A \cap B^c] \\
&= \Pr[B] \Pr[A|B] + \Pr[B^c] \Pr[A|B^c] \\
&\leq \Pr[B] + \Pr[A|B^c] \\
&\leq \frac{d-i}{|S|} + \frac{i}{|S|} \\
&= \frac{d}{|S|}.
\end{aligned}$$

□