6.842 Randomness and Computation April 27, 2022

Lectures on Probabilistically Checkable Proofs

Lecturer: Ronitt Rubinfield *Scribe: Yuchong Pan*

The probablistically checkable proof (PCP) model consists of a polynomial time verifier, which is given an input x, a random string \$, and a proof π (i.e., a fixed function).

Definition 1. We say that a language $L \in \mathsf{PCP}(r, q)$ if there exists a polynomial time verifier V such that

(i) for all $x \in L$, there exists a proof π such that $\mathbb{P}_{\$}[V, \pi \text{ accepts}] = 1$;

(ii) for all $x \notin L$, for any proof π', $\mathbb{P}_{\$}[V, \pi' \text{ accepts}] < 1/4$.

Moreover, V uses at ist $r(n)$ random bits and makes $q(n)$ queries to π (each using 1 bit).

It is easy to see that $\mathsf{SAT} \in \mathsf{PCP}(0, n)$. Recall that the $\mathsf{3SAT}$ problem asks for the satisfiability of a Boolean function F of the form $F = \bigwedge_i C_i$, where each clause C_i is of the form $C_i = y_{i_1} \vee y_{i_2} \vee y_{i_3}$ and each literal $y_{i_j} \in \{x_1, \ldots, x_n, \overline{x_1}, \ldots, \overline{x_n}\}$. We shall show the following theorem:

Theorem 2. $\mathsf{3SAT} \in \mathsf{PCP}(O(n^3), O(1))$.

Corollary 3. $\mathsf{NP} \subseteq \mathsf{PCP}(O(n^3), O(1))$.

Indeed, the following theorem holds:

Theorem 4. $\mathsf{NP} \subseteq \mathsf{PCP}(O(\log n), O(1))$.

The first attempt of proving Theorem 2 is defining the proof π to be the settings of an assignment a, e.g., $a_1 = \mathsf{T}, a_2 = \mathsf{F}, \ldots$, and defining the verifier to pick a random clause C_i and check if a satisfies C_i. This is good because if a satisfies F, then $\mathbb{P}[V \text{ succeeds}] = 1$. However, this is bad because if a does not satisfy F, then there exists a clause i such that a does not satisfy C_i, so $\mathbb{P}_{\$}[V \text{ finds an unsatisfied } C_i] \geq 1/m$, where m is the number of clauses in F.

Recall Freivald's test:

Theorem 5 (Freivald's test)**.** *If $a, b \in \mathbb{Z}_2^n$ are such that $a \neq b$, then $\mathbb{P}_{r \in \mathbb{Z}_2^n}[a \cdot r \neq b \cdot r] \geq 1/2$. If A, B, C are $\{0,1\}$-valued $n \times n$ matrices such that $A \cdot B \neq C$, then $\mathbb{P}_{r \in \mathbb{Z}_2^n}[A \cdot B \cdot r \neq C \cdot r] \geq 1/2$. This also holds for equality modulo 2.*

Proof. See Homework 1 and the orthogonality of the Fourier basis. □

Proof of Theorem 2. We introduce an arithmetrization $A(F)$ of a Boolean formula F over $\mathbb{Z}_2$ in Table 1. Then a Boolean formula F is satisfied by an assignment a if and only if $A(F)(a) = 1$. For a Boolean formula F consisting of clauses with 3 literals, $\deg A(F) \leq 3$.

We arithmetrize the complement of each clause separately (using ˆ for complements), i.e., let

$$\mathcal{C}(x) = \left(\widehat{C_1}(x), \widehat{C_2}(x), \ldots\right).$$

Then $\widehat{C_i}(x) = 0$ if x satisfies C_i, so $\mathcal{C}(x) = (0, 0, \ldots)$ if F is satisfied by x. Recall that each C_i is a polynomial of degree at most 3, and the verifier V knows the coefficients.

Boolean formula F	$A(F)$ over $\mathbb{Z}_2$
T	1
F	0
x_i	x_i
$\overline{x_i}$	$1 - x_i$
$\alpha \wedge \beta$	$\alpha \cdot \beta$
$\alpha \vee \beta = \overline{\bar{\alpha} \wedge \bar{\beta}}$	$1 - (1-\alpha)(1-\beta)$
$\alpha \vee \beta \vee \gamma$	$1 - (1-\alpha)(1-\beta)(1-\gamma)$

Table 1: An arithmetization $A(F)$ of a Boolean formula F.

We apply Freivald's test to $\mathcal{C}(a)$. Fix an assignment a. For all $r \in \mathbb{Z}_2^m$,

$$\left(\widehat{C_1}(a), \ldots, \widehat{C_m}(a)\right) \cdot (r_1, \ldots, r_m) \equiv \sum_{i=1}^{m} r_i \widehat{C_i}(a) \pmod 2,$$

so by Freivald's test,

$$\mathbb{P}_{r \in \mathbb{Z}_2^m}\left[\sum_{i=1}^{m} r_i \widehat{C_i}(a) \equiv 0 \pmod 2\right] = \begin{cases} 1, & \text{if } \widehat{C_i}(a) = 0 \text{ (i.e., } F \text{ is satisfied by } a\text{) for all } i \in [m], \\ \frac{1}{2}, & \text{otherwise.} \end{cases}$$

$\square$

TODO.