Probabilistic Proof Systems May 23, 2021

IP#1 - Graph Non-Isomorphism & PSPACE Upper Bound

Instructor: Alessandro Chiesa *Scribe: Shuangjun Zhang*

1 The class $\mathcal{NP}$

The class $\mathcal{NP}$ can be regarded as traditional mathematical proof systems. Let's recall the definition of $\mathcal{NP}$:

Definition 1 *A language $L \in \mathcal{NP}$ if and only if there exists a polynomial time decider $\mathcal{D}$ such that*

(1) $\forall x \in \mathcal{L}$, $\exists$ witness w, such that $\mathcal{D}(x, w) = 1$.

(2) $\forall x \notin \mathcal{L}$, $\forall$ witness w, $\mathcal{D}(x, w) = 0$.

For example, consider the boolean satisfiable problem $\mathcal{SAT}$, x is a boolean formula $\phi(x_1, x_2, ..., x_n)$, w is an assignment $(a_1, a_2, ..., a_n) \in \{0, 1\}^n$ and $\mathcal{D}$ checks that $\phi(a_1, a_2, ..., a_n)$ is true.

$\mathcal{NP}$ captures classical mathematical proofs.

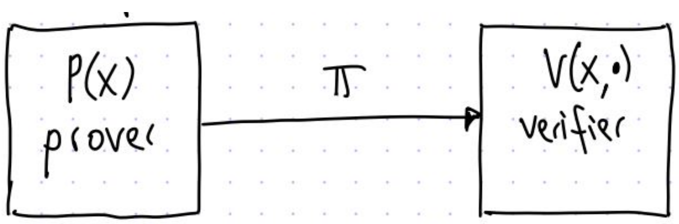

Figure 1: $\mathcal{NP}$ Proof Systems

2 Interactive Proofs

Here is a demonstration of the theorem environments.

Theorem 2 *This is a theorem.*

Definition 3 *This is a definition.*

Remark 4 *This is a remark.*

Lemma 5 *This is a lemma.*

Corollary 6 *This is a corollary.*

Proposition 7 *This is a proposition.*

Claim 8 *This is a claim.*

Observation 9 *This is an observation.*

Fact 10 *This is a fact.*

Assumption 11 *This is an assumption.*

2.1 Proof Environments

Here is a demonstration of the proof environments.

Theorem 12 *This is a theorem with a proof.*

Proof: This is the theorem's proof. $\square$

Theorem 13 *This is a theorem with a proof claim.*

This is the theorem's proof claim. $\diamond$

Proof of Theorem 12: This is another proof of Theorem 12. $\square$