Foundations of Probabilistic Proofs (Fall 2022)
Note 8: Exponential-Size PCP
Date: 2022.10.12

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 LPCP for NP by QESAT

In the lecture, we describe an LPCP for NP by constructing an LPCP over $\mathbb{F}$ for the language QESAT($\mathbb{F}$). The lecture gives a proof outline via reduction from CSAT (boolean circuit satisfiability) to QESAT. In this section, we give an introduction to CSAT, revisit the definition of QESAT and then give a complete proof.

To start with, we give formal definitions of SAT and CSAT:

Definition 1 (SAT)**.** *The language* SAT *is the set of all Boolean formulas having a satisfying assignment.*

Definition 2 (CSAT)**.** *The language* CSAT *is the set of all Boolean circuits having a satisfying assignment (input).*

If we give a satisfying assignment as the witness, verifying the correctness of the Boolean circuit will be in polynomial time. Therefore, CSAT $\in \mathsf{NP}$. To show that CSAT is NP-complete, it suffices to show that SAT $\leq_m^P$ CSAT, because we know that SAT is NP-complete from the Cook-Levin theorem. We briefly explain the intuition of the reduction from SAT to CSAT: Given a CNF φ, we can transform it to a Boolean circuit size poly(n, k) such that it has an input corresponding to every variable and a gate corresponding to every operator.

Moreover, it can be shown that that the NAND gate is a universal gate, that is, a gate which can implement any Boolean function without needing to use any other type of gates. Thus we can consruct a Boolean circuit using only NAND with polynomial overhead from the Boolean circuit above using AND, OR, NOT.

Exercise 1. *Show that any Boolean function can be implemented by* NAND *gates.*

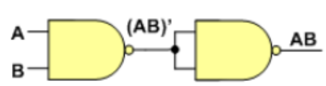

Figure 1: Implementing AND Using only NAND

Solution. It suffices to show AND, OR, NOT operations can be performed using only NAND. For example, Figure 1 shows how to implement an AND gate using two NAND gates. ■

Now we are ready to show that QESAT is NP-complete. We first revisit the definition of the language QESAT:

Definition 3 (QESAT)**.** *A system of m quadratic equations in n variables over a finite field $\mathbb{F}$ is a list of polynomials $p_1, \ldots, p_m \in \mathbb{F}[X_1, \ldots, X_n]$ where each p_i has total degree at most 2. The language* QESAT($\mathbb{F}$) *is the set of all such systems having an assignment $a \in \mathbb{F}^n$ such that $p_i(a) = 0$ for all $1 \leq i \leq m$.*

Theorem 1. QESAT($\mathbb{F}$) *is* NP*-complete for every finite field $\mathbb{F}$.*

Proof. We follow the standard paradigm by showing QESAT($\mathbb{F}$) $\in$ NP and QESAT($\mathbb{F}$) is NP-hard for every finite field $\mathbb{F}$.

- If we give a satisfying assignment as the witness, verifying $p_i(a) = 0$ for all $1 \leq i \leq m$ will be in polynomial time. Therefore, QESAT($\mathbb{F}$) $\in$ NP.
- The goal is to find a polynomial-time function f such that for any Boolean circuit C, $C \in$ CSAT iff $f(C) \in$ QESAT($\mathbb{F}$).
- Let $C\colon \{0,1\}^k \to \{0,1\}$ be a Boolean circuit only with NAND gates, consider the transformation from C to a quadratic equation system over $\mathbb{F}$ with $m = k + |C| + 1$ equations and $n = k + |C|$ variables in the following sense:
  - The first k variables $X_1, \ldots, X_k$ represent C's input and the remaining $|C|$ variables $X_{k+1}, \ldots, X_{k+|C|}$ represent outputs of all NAND gate. $X_{k+|C|}$ represents C's output.
  - We use quadratic equations $X_i(X_i - 1) = 0$ for $1 \leq i \leq k$ to represent the input being boolean constraints.
  - For every NAND in C with inputs X_{i_1}, X_{i_2} and output X_{i_3}, we use a quadratic equation $(1 - X_{i_1}X_{i_2}) - X_{i_3} = 0$.
  - We use $X_{k+|C|} = 1$ for the satisfiability constraint.
- We define f such that given the circuit C, f runs the transformation and outputs the quadratic equation system.
- $C \in$ CSAT iff $f(C)$ has a solution over $\mathbb{F}$.

$\square$