Math 261C: Randomized Algorithms

Lecture topic: \( \#SAT \in IP \)

Lecturer: Sam Buss
Scribe notes by: James Aisenberg
Date: May 28, 2014

1

**Theorem 1.** \( \#SAT \in IP \)

To prove the theorem, we start by encoding a CNF, \( \phi \), with a polynomial, \( \phi^*(x_1, \ldots, x_n) \) over \( \mathbb{N} \). The number 1 encodes \( \top \), the number 0 encodes \( \bot \). The formula \( \phi^* \) is defined inductively. For the base cases, \( x_i^* = x_i \), and \( \bar{x}_i^* = 1 - x_i \). Inductively, we have \( (a \land b \land c)^* = a^* \cdot b^* \cdot c^* \), and \( (a \lor b \lor c)^* = 1 - (1 - a^*) \cdot (1 - b^*) \cdot (1 - c^*) \). It suffices to consider 3-SAT, but it is easy to generalize these notions. Observe that \( \deg(\phi) \leq |\phi| \).

Next, notice that

\[
\#SAT(\phi) = \sum_{a_1, \ldots, a_n \in \{0,1\}} \phi(a_1, \ldots, a_n) =: S.
\]

Observe that \( S \leq 2^n \), so it suffices to verify the value of \( S \mod p \) for \( p > 2^n \). The prover will supply \( p > 2^n \) along with a Pratt certificate for \( p \). We think of \( S \) as being part of the input. If we are being careful, we remark that the thing we are actually proving is that the graph of \( \#SAT \) is in IP. However, it is not a big deal either way, because the (all powerful) prover could simply pass along the value of \( S \), but it is customary to define IP as a decision procedure, and not a function class.

**Definition 2.**

\[
f_i(x_1, \ldots, x_i) := \sum_{a_{i+1} \in \{0,1\}} \cdots \sum_{a_n \in \{0,1\}} \phi^*(x_1, \ldots, x_i, a_{i+1}, \ldots, a_n)
\]

In the following protocol, we will fix values \( a_1, \ldots, a_{i-1} \), and then define

\[
g_i(x_i) := f_i(a_1, \ldots, a_{i-1}, x_i)
\]

a univariate polynomial of degree less than or equal to \( |\phi| \). The polynomial \( g_i \) is specified indirectly as a polynomial size. Let \( h_i(x_i) \) be an explicit representation of \( g_i \), in other words, its coefficients are given explicitly.
1.1. Protocol. The IP protocol for \#SAT is as follows:

Input: \( \phi, S \).
Output:
- Accept if \( \# \text{SAT}(\phi) = S \) (with probability 1 for the honest prover).
- Reject if \( \# \text{SAT}(\phi) \neq S \) (with probability close to 1 for all provers).

Round 1: Prover supplies \( p > 2^n \) and a Pratt certificate for \( p \), and an explicit description of \( h_1(x_1) \).

Verifier rejects if Pratt certificate is invalid, or if \( S \neq h_1(0) + h_1(1) \).

Subsequent rounds check that \( h_i(x) \) is correct.

Round \( i \): The verifier picks \( a_i \in \mathbb{Z}_p \) at random and sends \( a_i \) to the prover. Notice that this is an IP protocol, so in principle we could use private coins, but that we only need public coins.

Prover sends \( h_{i+1}(a_{i+1}) \) to verifier (as an explicitly specified polynomial.)

Verifier checks that \( h_i(a_i) = h_{i+1}(0) + h_{i+1}(1) \), and rejects if not.

At round \( n + 1 \): Verifier checks that \( h_{n+1} \) is the constant polynomial.

\( \phi^*(a_1, \ldots, a_n) \).

\( V \) accepts if so, and rejects if not.

1.2. Analysis. If \( S = \# \text{SAT}(\phi) \) then the honest prover causes the verifier to accept with probability 1.

Now suppose \( S \neq \# \text{SAT}(\phi) \). Fix a prover \( P \), possibly malicious.

Claim I: \( \text{Prob}[V \text{ accepts}] \leq \frac{|\phi|}{2^n} \cdot n \leq \frac{|\phi|}{2^n} \cdot O(1) \)

Claim II: \( \text{Prob}[V \text{ accepts}|h_i(x_i) \text{ is incorrect}] \leq \frac{|\phi|}{2^n} \cdot (n - i + 1) \).

Recall that \( |\phi| \) bounds the degrees of the \( h_i \)'s. Observe that Claim II implies Claim I.

\textit{Proof of Claim II}. Induct on \( i = n + 1, \ldots, 1 \). For the base case, \( i = n + 1 \), we have \( \text{Prob}[V \text{ accepts}] = 0 \).

For the induction step, \( \text{Prob}[V \text{ accepts}|h_i \text{ is incorrect}] \) is less than or equal to

\[ \text{Prob}[V \text{ accepts}|h_i \text{ is incorrect and } h_{i+1} \text{ is correct}] + \text{Prob}[V \text{ accepts}|h_{i+1} \text{ is incorrect}] \]

This is less than or equal to

\[ \frac{|\phi|}{p} \cdot \frac{|\phi|}{p} (n - (i + 1) - 1) \leq \frac{|\phi|}{p} (n - i + 1) \]

by the Schwartz-Zippel Lemma and the induction hypothesis, respectively. \( \square \)
References
