

# CMPT 710 - Complexity Theory: Lecture 21

Valentine Kabanets

November 20, 2007

## 1 Interactive Protocols for #SAT

In the last lecture, I mentioned the theorem of Shamir that  $\text{IP} = \text{PSPACE}$ , i.e., that any language in  $\text{PSPACE}$  can be decided by an interactive protocol between an all-powerful but not trusted Prover and a probabilistic polytime Verifier. Instead of proving this result, we'll show an earlier result upon which Shamir's proof is based.

Define #3SAT to be a function that maps a 3-CNF  $\phi(x_1, \dots, x_n)$  into a number  $s$  that is equal to the number of satisfying assignments of  $\phi$ . We'll show the following

**Theorem 1** (Lund, Fortnow, Karloff, Nisan). *#3SAT is in IP.*

**Remark** Here, by IP we mean  $\text{IP}[\text{poly}]$ , i.e., an interactive protocol with a polynomial number of rounds.

The key ingredient in the proof of both results mentioned above is *arithmetization* of propositional formulas. Namely, the conversion of a given 3-CNF  $\phi(x_1, \dots, x_n)$  into an arithmetic formula computing a multivariate polynomial  $f(x_1, \dots, x_n)$  satisfying the following property. For any truth assignment  $a = (a_1, \dots, a_n)$  (which we view as a 0-1 vector), if  $\phi(a)$  is True, then  $f(a) = 1$ ; and if  $\phi(a)$  is False, then  $f(a) = 0$ .

Such an arithmetization of a formula  $\phi$  is carried out inductively. A variable  $x$  becomes the function  $x$ , and the literal  $\bar{x}$  becomes the function  $1 - x$ . A formula  $\phi_1 \wedge \phi_2$  becomes the function  $f_1 * f_2$ , where  $f_i$  is an arithmetization of  $\phi_i$ ,  $i = 1, 2$ . Finally, a formula  $\phi_1 \vee \phi_2$  becomes the function  $1 - (1 - f_1)(1 - f_2)$ , where  $f_i$  is the arithmetization of  $\phi_i$ ,  $i = 1, 2$ . (To make sense of the last rule, recall that by de Morgan's rule,  $\phi \vee \psi \equiv \neg(\neg\phi \wedge \neg\psi)$ .)

**Example:** Let  $\phi(x_1, x_2, x_3, x_4) = (x_1 \vee x_2 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee \bar{x}_3 \vee x_4)$ . Then the corresponding arithmetic formula will be  $f(x_1, x_2, x_3, x_4) = [1 - (1 - x_1)(1 - x_2)x_3][1 - x_1x_3(1 - x_4)]$ , which is a polynomial of degree 6.

Note that the degree of the constructed polynomial is 3 times the number of clauses in  $\phi$ . This is not a coincidence. It is easy to see that any 3-CNF  $\phi$  with  $m$  clauses is transformed by the arithmetization procedure described above into a polynomial of total degree at most  $3m$ .

**Lemma 2.** *Let  $\phi(x_1, \dots, x_n)$  be a 3-CNF with  $m$  clauses, and let  $f(x_1, \dots, x_n)$  is the arithmetic formula obtained by arithmetizing  $\phi$ . Then (1) the total degree of  $f$  is at most  $3m$ , (2) on any 0-1 vector  $a$ ,  $f(a) \in \{0, 1\}$ , and (3) on any 0-1 vector  $a$ ,  $f(a) = 1$  iff  $\phi(a)$  is True.*

*Proof.* Exercise. (Hint: use induction.) □

For a 3-CNF  $\phi$  and the corresponding arithmetization  $f$ , let's define  $\#\phi$  (# satisfying assignments of  $\phi$ ), and  $\#f = \sum_{x_1=0}^1 \sum_{x_2=0}^1 \cdots \sum_{x_n=0}^1 f(x_1, x_2, \dots, x_n)$ . Then, by the lemma above, we get that  $\#\phi = \#f$ . So, proving that  $\#\phi = s$  is equivalent to proving that  $\#f = s$ . The latter is what our IP protocol is going to do.

The details will be given next time.