CS 579: Computational Complexity. Lecture 9

IP=PSPACE, Part 1

Alexandra Kolla

Today

- Proof: UNSAT ⊆ IP
- Proof: #3SAT ⊆ IP
- PH⊆ IP
- Start discussing PSPACE ⊆ IP

Representing boolean formulas with polynomials

- Formula ϕ with m clauses on variables $x_1, \dots, x_n$.
- $\mathrm{N} \geq 2^n \cdot 3^m$ prime number.
- Translate ϕ to a polynomial p over the field (mod N) as follows:
- $x_i \rightarrow x_i, \quad \overline{x_i} \rightarrow (1 - x_i)$
- Clause is translated to the sum of the (at most 3) expressions corresponding to the literals in the clause.
- p is the product of all the m expressions corresponding to the m clauses.

Representing boolean formulas with polynomials

- Each literal has degree 1, so p has degree at most m.
- For a zero-one assignment, p evaluates to zero if this assignment does not satisfy ϕ, and to a non-zero number otherwise.
- This number can be at most 3^m.
- ϕ is unsatisfiable if and only if

$$\sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} p(x_1, \dots, x_n) \equiv 0 \ (mod N)$$

IP for UNSAT

$\phi \to$ P | $\phi \to$ V

P → V: N, a proof that N is prime — V: check primality proof

P → V: $q_1(x) = \sum_{x_2,\ldots,x_n \in \{0,1\}} p(x, x_2, \ldots, x_n)$ — V: check $q_1(0) + q_1(1) = 0$

V → P: r_1 — V: pick random $r_1 \in \{0, \ldots, N-1\}$

P → V: $q_2(x) = \sum_{x_3,\ldots,x_n \in \{0,1\}} p(r_1, x, x_3, \ldots, x_n)$ — V: check $q_2(0) + q_2(1) = q_1(r_1)$

V → P: r_2 — V: pick random $r_2 \in \{0, \ldots, N-1\}$

⋮

P → V: $q_i(x) = \sum_{x_{i+1},\ldots,x_n \in \{0,1\}} p(r_1, \ldots, r_{i-1}, x, x_{i+1}, \ldots, x_n)$ — V: check $q_i(0) + q_i(1) = q_{i-1}(r_{i-1})$

V → P: r_i — V: pick random $r_i \in \{0, \ldots, N-1\}$

⋮

P → V: $q_n(x) = p(r_1, \ldots, r_{n-1}, x)$ — V: check $q_n(0) + q_n(1) = q_{n-1}(r_{n-1})$

pick random $r_n \in \{0, \ldots, N-1\}$

check $q_n(r_n) = p(r_1, \ldots, r_n)$

A proof system for #SAT

- Formula ϕ with m clauses on variables $x_1, \dots, x_n$, suppose it has k satisfying assignments.
- We want an IP s.t. if P gives k as an answer then V will accept w.p. 1, otherwise V will reject w.h.p.
- Change the way to translate ϕ to a polynomial p over the field (mod N) as follows:
- $z_1 \vee z_2 \vee z_3 \rightarrow 1-(1-z_1)(1-z_2)(1-z_3)$
- p is the product of all the m expressions corresponding to the m clauses.

A proof system for #SAT

- For a zero-one assignment the clause evaluates to 1 if the assignment satisfies that clause and 0 if not.
- So zero-one assignments that satisfy formula will make p=1 and the rest p=0.
- Degree of p is now 3m, instead of m, but now

$\sum_{x_1\in\{0,1\}} \dots \sum_{x_n\in\{0,1\}} p(x_1, \dots, x_n)$= # sat. assignments.

- Enough to take $N > 2^n$.

A proof system for #SAT

- First round prover sends k.
- Then follows the previous protocol.
- After first message, verifier checks if $q_1(0) + q_1(1) = k$.
- Rest is the same as before.