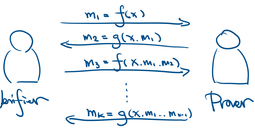
Interactive proofs

3/1/21 10:53 AM

Administrivia.

- Midterm 2 tomorrow, same format as midterm 1.
- Homework 7 out. due next Monday 3/8.
- solutions to Homework 6 not done yet; join OH

Interactive Proofs.



L has k-round (deterministic) interactive proof if $\exists$ verifier V (poly-time) s.t. $x \in L \Leftrightarrow \exists$ prover P convinces V. (all-powerful).

Lemma. $\mathrm{IP} = \mathrm{NP}$.

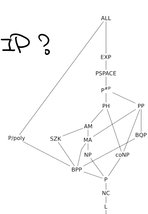
pf. (sketch) P proves to V by showing all their future conversation before V asks questions.

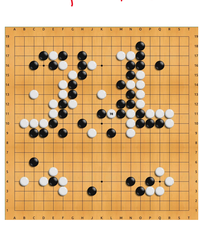
L has interactive proof ($L \in \mathrm{IP}$).
if $\exists$ verifier V BPP. verifier has private coin.
s.t. $x \in L$: $\exists$ prover P convinces V. w.p. $\geq 2/3$.
$x \notin L$: $\forall$ prover P convinces V w.p. $\leq 1/3$.

Q. How strong is IP?

- NP $\subseteq$ IP.
- BPP $\subseteq$ IP.
- IP $\subseteq$ PSPACE.

How to even prove coNP $\subseteq$ IP?



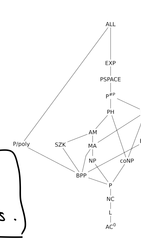


[LFKN '90. S '90]

Thm. IP = PSPACE

Lemma. #SAT is in IP.

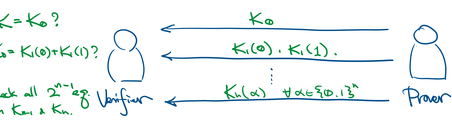
#SAT
- input: CNF ϕ and integer K.
- output: ϕ has exactly K sat. assignments.



Goal. Prover try to convince verifier ϕ has K sat. assignments.

$K_i(a_1, \dots, a_i) :=$ # sat. x of ϕ with $x_j = a_j \ \forall j \in [i]$.

$K_i(a_1, \dots, a_i) = K_{i+1}(a_1, \dots, a_i, 0) + K_{i+1}(a_1, \dots, a_i, 1)$



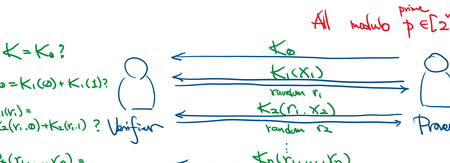
Q. Too many objects to check. What to do?

Key idea. Encode formulas as polynomials. (arithmetization)

3CNF $\phi = \bigwedge C_j$ $\longleftrightarrow$ polynomial $P_\phi = \prod P_j(X)$.

$C_j = (x_i \vee \bar{x}_j \vee x_k)$ $\longleftrightarrow$ $P_j = 1 - (1-x_i)x_j(1-x_k)$

$$K_i(a_1, \dots, a_i) = \sum_{a_{i+1}, \dots, a_n \in \{0,1\}} P_\phi(a_1, \dots, a_n). \quad \deg \leq 3n$$



Analysis. For Prover to fool Verifier,
sent fake $\tilde{K}_0, \dots, \tilde{K}_n(r_1, \dots, r_i)$.

Lemma. $\Pr\left[\tilde{K}_i(r_1, \dots, r_i) = K_i(r_1, \dots, r_i)\right] < 1/n^2$.
if r_i chosen from $[1 \dots p]$ unif. random.

pf. Schwartz-Zippel. $\deg(\tilde{K}_i - K_i)/2^n$. ☐

Probability Verifier caught Prover cheated: $(1 - 1/n^2)^n > 1 - \frac{1}{n}$

☐.

Conclusion. interaction + randomness is powerful!