CS 538
Jorge Padilla

In this lecture, we continue the proof of $PSPACE = IP$. Ending proof of $PSPACE \subseteq IP$.

It will suffice to have an IP protocol to TQBF. We will do this by arithmetizing QBF as follows:

$\neg x \rightarrow (1 - x)$
$\alpha \wedge \beta \rightarrow \alpha.\beta$
$\alpha \vee \beta \rightarrow \alpha + \beta - \alpha.\beta$
Any $x\alpha(x) \rightarrow Ax\alpha(x)$
Exists $x\alpha(x) \rightarrow Ex\alpha(x)$
$Rx\alpha(x) \rightarrow \alpha(x) mod(x^2 - x)$

(Here, $Ex\alpha(x)$ is a short way of expressing $\alpha(0) + \alpha(1)$, and $Ax\alpha(x)$ is a short way of expressing $\alpha(0) \cdot \alpha(1)$.)

Given QBF $\phi = \forall x1 \exists x2 ... \forall xk \;\; \alpha(x1, ..., xk)$.

1) Consider the expression:
$\psi = Ax1Rx1Ex2Rx1Rx2Rx3Ax3...AxkRx1Rx2...Rxk \;\; \alpha(x1, ..., xK)$.

2) ψ and ϕ agree on Boolean inputs.

3) Prover wants to prove that $\psi = 1$ (evaluated over GF(p) fro some prime p with n^k bits).

4) At each stage, the prover is trying to prove that some expression α evaluates to c in GF(p).

If α has NO A, E or R then the verifier can do this directly.

If $\alpha = Ax\beta(x)$, then the prover send the coefficients of $\beta(x) = \sum \beta_i x^i$. Verifier checks that $\beta(0) \cdot \beta(1) = c$. Verifier picks at random $r \in GF(p)$., and ask the prover to show that $\beta(r) = \sum \beta_i r^i$.

If $\alpha = Ex\beta(x)$. Then same as above. But, Verifier checks $\beta(0) + \beta(1) - \beta(0).\beta(1) = c$.

If $\alpha = Rx\beta(x)$. Verifier checks $\beta(0) + (\beta(1) - \beta(0)) \cdot r = c$.