Theorem 18.1 Shamir's Theorem: IP = PSPACE

Proof: IP $\subseteq$ PSPACE: Evaluate the game tree.

For **M**'s moves choose the maximum value over its possible messages: $m_0 = 0^{p(n)}, \ldots, c_{2^{p(n)}-1} = 1^{p(n)}$

For **A**'s moves choose the average value over its possible coin tosses: $c_0 = 0^{r(n)}, \ldots, c_{2^{r(n)}-1} = 1^{r(n)}$.

There are polynomially many moves and each move has a polynomial-length label, so polynomial space suffices for the stack.

Show QSAT $\in$ IP

$$\varphi \;\equiv\; \forall x \exists y (x \vee y) \wedge \forall z ((x \wedge z) \vee (y \wedge \bar{z})) \vee \exists w (z \vee (y \wedge \bar{w}))$$

Formula φ is *simple* iff no occurrence of a variable is separated by more than one universal quantifier from its point of quantification.

Lemma 18.2 *Any quantified boolean formula can be transformed in logspace to an equivalent, simple formula.*

Proof: Suppose that x is quantified before $\forall y$ and used after $\forall y$

$$\varphi \quad = \quad \cdots Qx \cdots \forall y \psi(x)$$

Right after the $\forall y$, rename x,

$$\varphi' \quad = \quad \cdots Qx \cdots \forall y \exists x' ((x \wedge x') \vee (\bar{x} \wedge \overline{x'})) \wedge \psi(x')$$

This needs to be done fewer than $|\varphi|^2$ times. $\square$

From now on we may **assume that φ is simple** and **all $\neg$'s are pushed all the way inside.**

Arithmetization of formulas

Define f : boolean formulas $\rightarrow$ polynomials.

$x = 1$ means x is true; $x = 0$ means x is false.

$$\begin{aligned}
f(\bar{x}) &= 1 - x \\
f(\alpha \wedge \beta) &= f(\alpha) \cdot f(\beta) \\
f(\alpha \vee \beta) &= f(\alpha) + f(\beta) \\
f(\forall x(\alpha(x))) &= \prod_{i=0}^{1} f(\alpha(i)) \\
f(\exists x(\alpha(x))) &= \sum_{i=0}^{1} f(\alpha(i))
\end{aligned}$$

Lemma 18.3 *Let φ be a closed, quantified boolean formula with all "$\neg$"s pushed to variables. Then,*

$$\varphi \in \mathrm{QSAT} \quad \Leftrightarrow \quad f(\varphi) > 0$$

M must prove to A that $f(\varphi) > 0$

Lemma 18.4 *Let $n = |\varphi|$ If $f(\varphi) \neq 0$, then there is a prime p, $2^n < p < 2^{3n}$ s.t.*

$$f(\varphi) \quad \not\equiv \quad 0 \quad (\mod p)$$

M must prove to A that $f(\varphi) \not\equiv 0$ (mod p)

Example:

$$\begin{aligned}
\varphi &\equiv \forall x \exists y (x \vee y) \wedge \forall z ((x \wedge z) \vee (y \wedge \bar{z})) \\
&\qquad \vee \quad \exists w (z \vee (y \wedge \bar{w})) \\
f(\varphi) &= \prod_x \sum_y ((x + y) \cdot \prod_z ((x \cdot z) + (y \cdot (1 - z)) \\
&\qquad + \quad \sum_w (z + (y \cdot (1 - w)) \\
f_1(x) &= \sum_y ((x + y) \cdot \prod_z ((x \cdot z) + (y \cdot (1 - z)) \\
&\qquad + \quad \sum_w (z + (y \cdot (1 - w)) \\
&= 2x^2 + 8x + 6
\end{aligned}$$

Note, $f_1 \in \mathbf{Z}[x]$ has degree $\leq 2n$ because φ is simple. There is at most one "$\prod$" affecting x.

$$\begin{array}{ccccc}
f(\varphi) & = & f_1(0) & \cdot & f_1(1) \\
96 & = & 6 & \cdot & 16
\end{array}$$

$$\begin{aligned}
\varphi &= (\forall x)(\exists y)\psi \\
f(\varphi) &= \prod_{x=0}^{1} f_1(x)
\end{aligned}$$

1. M sends to A:

- p
- v_0 where $v_0 \equiv f(\varphi) \pmod{p}$
- coefficients of g_1, where $g_1 \equiv f_1 \pmod{p}$

2. **A**

- checks that p is prime
- checks that $g_1(0) \cdot g_1(1) \equiv v_0 \pmod{p}$
- chooses random $r_1 \in \mathbf{Z}_p$
- computes $v_1 \equiv g_1(r_1) \pmod{p}$
- sends r_1 to $\mathbf{M}$

M must prove to A that $f_1(r_1) \equiv v_1 \pmod{p}$

Lemma 18.5 *If* $g_1 \not\equiv f_1 \pmod{p}$*, then*

$$\text{Prob}[g_1(r_1) \equiv f_1(r_1) \pmod{p}] \ \leq \ \frac{2n}{p} \ < \ \frac{2n}{2^n}$$

Proof: Since g_1 and f_1 each have degree $2n$, so does $g_1 - f_1$. But a degree d polynomial has at most d zeros. Thus, with r chosen at random, $\text{Prob}[(g_1 - f_1)(r) \equiv 0 \pmod{p}] \ \leq \ \frac{2n}{p}$ $\square$

Thus, in one double round, we have removed one quantifier from φ.

Key idea: replace the universal boolean quantifier:

$$\forall x (f_1(x) = g_1(x))$$

with a random quantifier

$$(\text{for most } r)(f_1(r) = g_1(r))$$

M must prove to A that $f_1(r_1) \equiv v_1 \pmod{p}$

$$\begin{aligned} \varphi &= (\forall x)(\exists y)\psi \\ f(\varphi) &= \prod_{x=0}^{1} f_1(x) \\ f_1(r_1) &= \sum_{y=0}^{1} f_2(r_1, y) \end{aligned}$$

3. **M** sends to **A**:

- coefficients of $g_2(y)$, where $g_2(y) \equiv f_2(r_1, y) \pmod p$

4. **A**

   - checks that $g_2(0) + g_2(1) \equiv v_1 \pmod p$
   - chooses random $r_2 \in \mathbf{Z}_p$
   - computes $v_2 \equiv g_2(r_2) \pmod p$
   - sends r_2 to $\mathbf{M}$

$\mathbf{M}$ must prove to $\mathbf{A}$ that $f_2(r_2) \equiv v_2 \pmod p$

After n steps, all the variables are eliminated and $\mathbf{A}$ should accept iff $f_n(r_n) = v_n$.

The probability of $\mathbf{M}$ getting away with a lie is at most $n\left(\frac{2n}{2^n}\right)$.

Shamir's Theorem is proved. $\square$