Thursday, May 24, 2018 3:01 PM

For $L = \{(\phi, k) \mid \phi$ has exactly k satisfying assignments$\}$

Showed $L \in IP$ L is co-NP hard, so co-NP $\subseteq$ IP.

Theorem (Shamir): $IP = PSPACE$.

$IP \subseteq PSPACE$ is easy: enumerate all possible interactions, explicitly calculate success probability.

Interaction is very powerful!

Can interact w/ master player of generalized geography and determine if she can win, even if you can not compute optimal moves.)

Need to show $PSPACE \subseteq IP$ (i.e. $QSAT \in IP$).

Same basic idea as co-NP proof (plus a few additional ingredients).

(*) First assume that no occurrence of x_i separated by more than one $\forall$ from the point of quantification:

$\forall x \quad \exists \quad \forall \quad \exists \quad \forall$

occurrences of x | no occurrences of x.

This helps ensure that the degree of a single variable is $O(|\phi|)$

Friday, May 25, 2018 8:02 AM

$\forall x\ \phi_1(x) \wedge \exists y\ \phi_2(x,y) \vee \forall z\ \phi_3(x,y,z) \vee \exists \ldots$

$\forall x\ \phi_1(x) \wedge \exists y\ \phi_2(x,y) \vee \forall x'\ (x = x') \rightarrow \forall z\ \phi_3(x',y,z) \vee \exists \ldots$

replace x w/ x'.

Arithmetization:

$$\exists x_i\ \phi \longrightarrow \sum_{x_i = 0,1} P_\phi(x_i, \ldots)$$

$$\forall x_i\ \phi \longrightarrow \prod_{x_i = 0,1} P_\phi(x_i, \ldots).$$

this can double the degree and square the size of P_ϕ.

Degree of a single variable x is bounded by poly$(|\phi|)$.

Thursday, May 24, 2018 3:01 PM

Arithmetization:

$\exists x_i \phi \longrightarrow \sum_{x_i = 0,1} P_\phi(x_i, \ldots)$

$\forall x_i \phi \longrightarrow \prod_{x_i = 0,1} P_\phi(x_i, \ldots)$.

← this can double the degree and square the size of P_ϕ.

$\Rightarrow$ Quantified Boolean expression ϕ is true iff $P_\phi > 0$

Problem: the $\forall$ (Π) terms may cause $P_\phi > 2^{2^{|\phi|}}$ (too large to compute).

Solution: evaluate mod q $\quad 2^n < q < 2^{3n}$

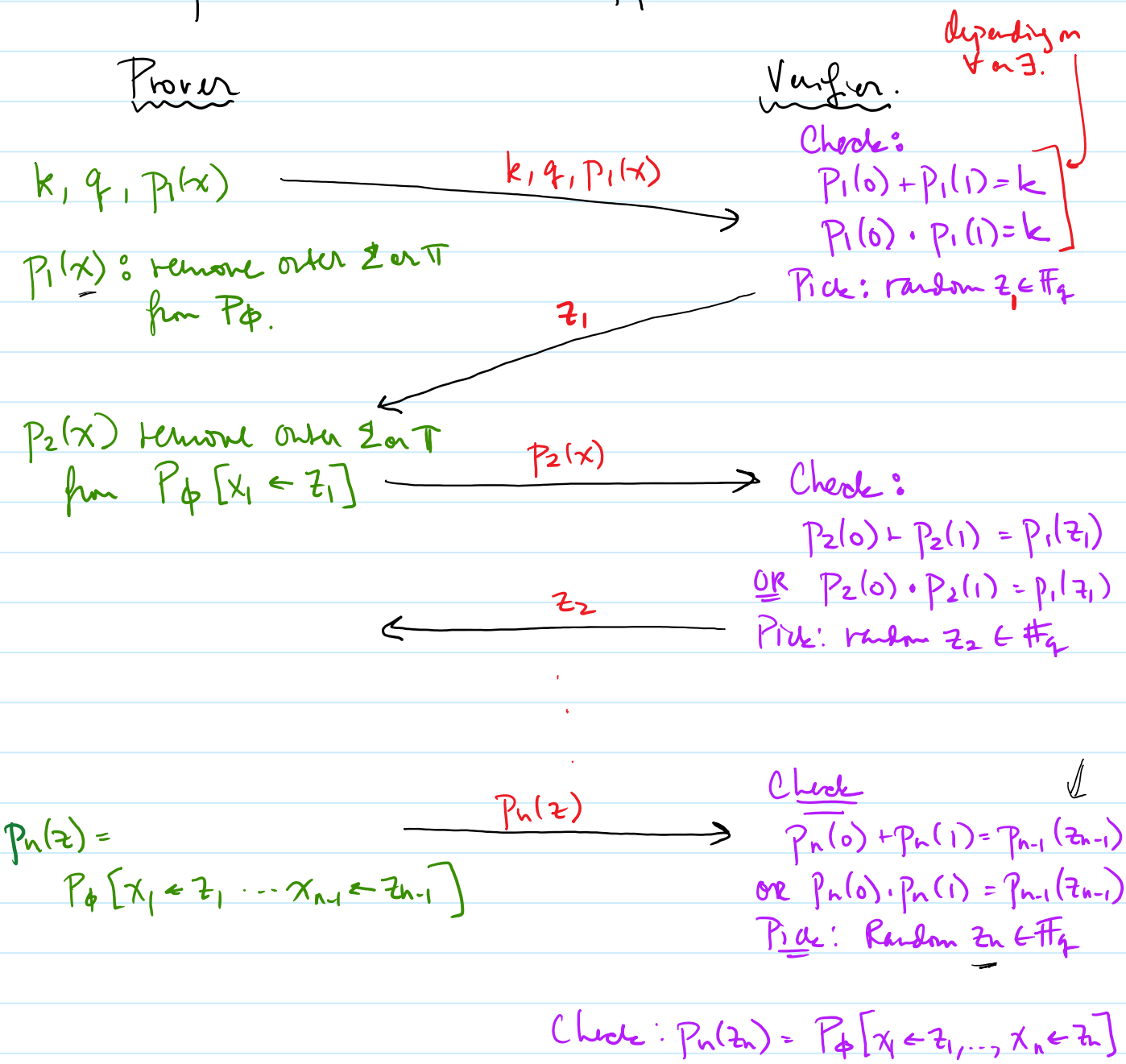
Prover sends a "good" q to V in the first round.
a "good" q is one such that $P_\phi \bmod q > 0$.

Claim: A good q exists because the # primes in the range $> 2^n$
↳ the product of all these primes $> P_\phi$,
So it can't be that $P_\phi \bmod q \equiv 0$ for all q in the range.

Since prover is trying to get V to accept, he is motivated to send a good q.

Thursday, May 24, 2018 3:01 PM

QSAT protocol: Prover claims: $P_\phi = k > 0$.



Note: Each $P_i(x)$ is bounded in size because of (*)
So it can be sent to V.

Also: $P_\phi[x_1 \leftarrow z_1, \ldots, x_n \leftarrow z_n]$ has no quantifiers
Can be computed in polynomial time.

Thursday, May 24, 2018 3:01 PM

Example:

$\phi = \forall x \exists y (x \vee y) \wedge \forall z ((x \wedge z) \vee (y \wedge \neg z)) \vee \exists w (z \vee (y \wedge \neg w))$

x ← 0
y ← 3
z ← 4
z ← 2.

$P_\phi = \prod_{x=0,1} \sum_{y=0,1} [(x+y) * \prod_{z=0,1} [(xz + y(1-z)) + \sum_{w=0,1} (z + y(1-w))]]$

$\prod_{X=0,1} \sum_{y=0,1} [(x+y) * \prod_{z=0,1} [(xz + y(1-z)) + 2z + y]]$

$\prod_{X=0,1} \sum_{y=0,1} [(x+y) \cdot (2y)(x+2+y)]$

$\prod_{X=0,1} (X+1) \cdot 2 \cdot (x+3) = (1 \cdot 2 \cdot 3)(2 \cdot 2 \cdot 4) = 96 = P_\phi$

Prover claims $P_\phi > 0$.

Prover sends $q = 13$ claim: $P_\phi \bmod q = 96 \bmod 13 = 5 > 0$.
sends $k = 5$.

Removes outer $\prod_{x=0,1}$ and sends: $(x+1) \cdot 2 \cdot (x+3) =$
$2x^2 + 8x + 6 = p_1(x)$

Verifier checks $p_1(0) \cdot p_1(1) \bmod q = 5$. $p_1(a)$
Verifier picks random $z_1 = 9$.

Thursday, May 24, 2018 3:01 PM

$y : 3$

$$P_\phi[x \leftarrow 9] = \sum_{y=0,1} \left[(9+y) \times \prod_{z=0,1} \left[(9z + y(1-z)) + \sum_{w=0,1} (z + y(1-w)) \right] \right]$$

$P_1(9) =$

$$P_2(y) = (9+y) * \prod_{z=0,1} \left[(9z + y(1-z)) + 2z + y \right]$$

$$= (9+y)(2y)(11+y) = 2y^3 + 18y^2 + 22y^2 + 198y \bmod 13$$
$$= 2y^3 + y^2 + 3y$$

Prover sends : $P_2(y) = 2y^3 + y^2 + 3y$.

Verifier checks $P_2(0) + P_2(1) \equiv P_1(9) \bmod 13$

$6 \equiv 6$

Verifier picks random : $y = 3$ $P_2(3) = 7 \bmod 13$.

$$P_\phi[x \leftarrow 9 \; y \leftarrow 3] = \left[(9+3) * \prod_{z=0,1} (9z + 3(1-z)) + \sum_{w=0,1} (z + 3(1-w)) \right]$$

$\Rightarrow P_3(z) = 6z + 3 + 2z + 3$
$= 8z + 6.$

$\leftarrow (z+3) + z = 2z + 3$

Prover sends $P_3(z)$. Verifier checks $12 \cdot P_3(0) \cdot P_3(1) \equiv P_2(3)$

$12 \cdot 6 \cdot 14 \equiv 7 \bmod 13.$

Verifier selects random $z \leftarrow 7$

Friday, May 25, 2018 8:02 AM

$P_\phi[x \leftarrow 9, y \leftarrow 3, z \leftarrow 7] = 12 * [(9 \cdot 7) + 3(1-7) + \sum_{w=0,1} (7 + 3(1-w))]$

(6 mod 13; $P_4(w)$)

$= 12\, p_3(7) = 12 * 10 \bmod 13 = 3.$

$12 * [6 + p_4(w)] = 12 * [6 + (10 - 3w)]$

$p_4(w) = 10w + 10.$

Prover sends $p_4(w)$.

Verifier checks: $12 * [6 + p_4(0) + p_4(1)] = 12 \cdot 10 \bmod 13$ ($p_3(7)$)

Verifier selects: $w = 2$.

Final check: $12[6 + p_4(2)] =$

$P_\phi[x \leftarrow 9\ y \leftarrow 3\ z \leftarrow 7\ w \leftarrow 2]:$

$12[(9 \times 7) + 3(1-7) + (7 + 3(1-2))] = 12[6 + p_3(9)]$

Friday, May 25, 2018 8:02 AM

Completeness: if $\phi \in$ QSAT then an honest prover (who also sends good q) will cause V to accept.

Soundness: Let $p_i(x)$ be correct polynomial
Let $p_i^*(x)$ be poly sent by prover.

if $\phi \notin$ QSAT then $p_1(0) +/* p_1(1) = 0 \neq k$.

If $p_1^*(0) +/* p_1^*(1) \neq k$ then V will reject.

If this doesn't happen then $p_1 \neq p_1^*$.

$$\text{Prob}_{z_1}[p_1^*(z_1) = p_1(z_1)] \leq \frac{\text{poly}(|\phi|)}{2^n}$$

Because of degree bound on any single variable.

By induction assume: $p_i^*(z_i) \neq p_i(z_i) = p_{i+1}(0) +/* p_{i+1}(1)$

If $p_{i+1}^*(0) +/* p_{i+1}^*(1) \neq p_i^*(z)$ then V rejects.

Otherwise $p_{i+1}^* \neq p_{i+1}$

$$\Rightarrow \text{Prob}_{z_{i+1}}[p_{i+1}(z_{i+1}) = p_{i+1}^*(z_{i+1})] \leq \frac{\text{poly}(|\phi|)}{2^n}.$$

$x_1 \leftarrow z_1, \quad x_2 \leftarrow z_2$

$\cdots \quad x_n \leftarrow z_n$

Tuesday, May 29, 2018 3:47 PM

At the end, we have $p_n(z_n) \neq p_n^*(z_n)$

$\phi[x_1 \leftarrow z_1 \cdots x_n \leftarrow z_n]$

Can calculate this from the original ϕ and $z_1 \cdots z_n$.

V will detect that they are unequal.

V will reject as long as $p_i(z_i) \neq p_i^*(z_i) \quad \forall i$

For each i, the probability $p_i(z_i) = p_i^*(z_i) \leq \text{poly}(|\phi|)$

Prob that for any i, $p_i(z_i) = p_i^*(z_i) \leq \frac{n \cdot \text{poly}(|\phi|)}{2^n} \ll \frac{1}{3}$

$=$