The Power of Interactive Proofs

$NP \subseteq IP \subseteq PSPACE$

$GNI \in IP$

$PSPACE \subseteq IP$

Sumcheck

[LFKN '92]

$\mathbb{F}$ finite field $g : \mathbb{F}^n \to \mathbb{F}$ $\deg(g) \le d$ in each var.

$$\underbrace{\sum_{x_1, x_2, \dots, x_n \in \{0,1\}} g(x_1, \dots, x_n)}_{\sigma} = z \qquad z \in \mathbb{F}$$

Evaluate the sum: 2^n evals of g :(

<u>Fact 1:</u> f, g polys. $\mathbb{F} \to \mathbb{F}$ $\deg(f), \deg(g) \le d$

$|\{\# x \in \mathbb{F} : f(x) = g(x)\}| \le d$ if $f \ne g$

$$g_1(x) = \sum_{x_2, \dots x_n \in \{0,1\}} g(x, x_2, \dots, x_n)$$

- $\deg(g_1) \le d$
- If g_1 is known, $\sigma = g_1(0) + g_1(1)$

$$g(x_1, x_2) = x_1^2 + x_1 x_2$$

$$\sum_{x_1, x_2 \in [0,1]} g(x_1, x_2) = g(0,0) + g(1,0) + g(0,1) + g(1,1)$$

$$g_1(x) = g(x,0) + g(x,1)$$

$$= x^2 + x^2 + x$$

$P \quad g, z \qquad V$

$\xrightarrow{g_1}$

$\xleftarrow{y_1}$

$O(d)$

1. P sends g_1', which should be g_1
2. V checks $g_1'(0) + g_1'(1) = z$
3. V checks $g_1' \equiv g_1$
   - Sample $y_1 \leftarrow F$
   - Check $g_1'(y_1) = g_1(y_1)$

0. If $n = 1$,
   compute $g(0) + g(1)$ of g — 2 evals.
   check $= z$?

$$g_1'(y_1) = \sum_{x_2, \dots x_n \in \{0,1\}} \underbrace{g(y_1, x_2, \dots, x_n)}$$

4. Define $g_{y_1}(x_2, \ldots, x_n) \triangleq g(y_1, x_2, \ldots, x_n)$

5. Repeat protocol with $(g_{y_1}, g_1'(y_1))$

$$\sum_{x_1, \ldots, x_n \in \{0,1\}} g(x_1, \ldots, x_n) = z$$

$\Big\downarrow$ after 1 round

$$\sum_{x_2, \ldots, x_n \in \{0,1\}} g_{y_1}(x_2, \ldots, x_n) = g_1'(y_1) :$$

$$\underbrace{\sum g_{y_1,y_2}(x_3,\ldots,x_n)}_{g(y_1,y_2,x_3\ldots x_n)} = g_2'(y_1,y_2)$$

$$g(y_1,\ldots,y_{n-1},x_n)$$

Efficiency of V: $O(nd)$ field ops. $+ O(1)$ evals. of g

P: $O(nd\,2^n)$ evals. of g

Completeness: (If $\sigma = 2$, V must accept)

Induction on n.

If $n=1$: Perfect $\because$ V does challenge itself

Suppose Sumcheck with $(n-1)$ vars. is perf. complete

Soundness: (If $\sigma \neq 2$, V should not accept)

If $n=1$: $Pr[V \text{ accepts}] = 0$

For n, $Pr[V \text{ accepts}] : \epsilon_n$

- $Pr[V \text{ picks bad } y_1] \leq \frac{d}{|F|}$

- $Pr[V \text{ accepts} \mid y_1 \text{ good}] = \epsilon_{n-1}$

ϵ_n :

$Pr[V \text{ accepts}]$

$\leq \frac{d}{|F|} + \epsilon_{n-1}$

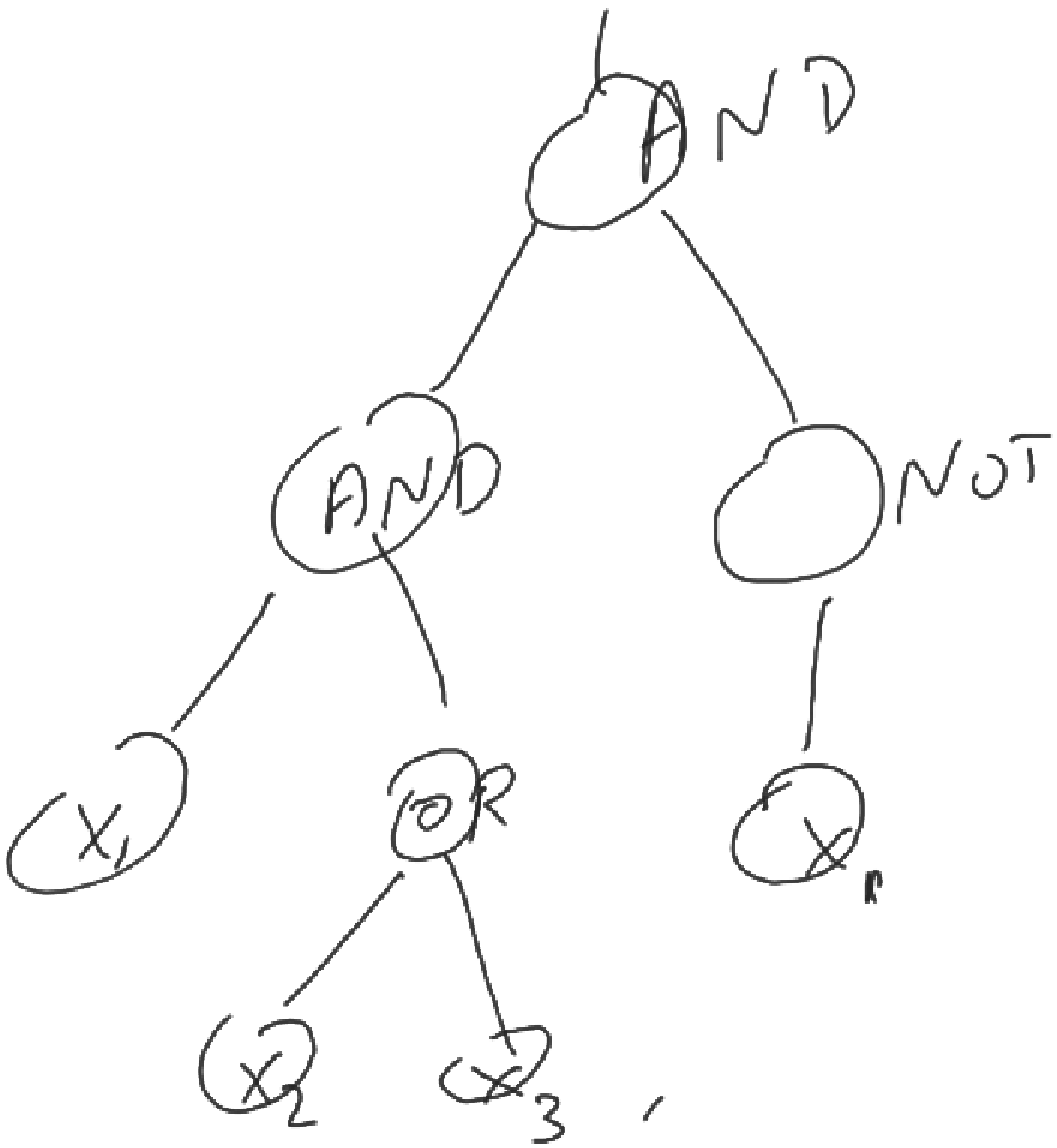
$$\boxed{\epsilon_n \leq (n-1)\frac{d}{|F|}}$$

coNP $\subseteq$ IP

TRUE := 1 FALSE := 0

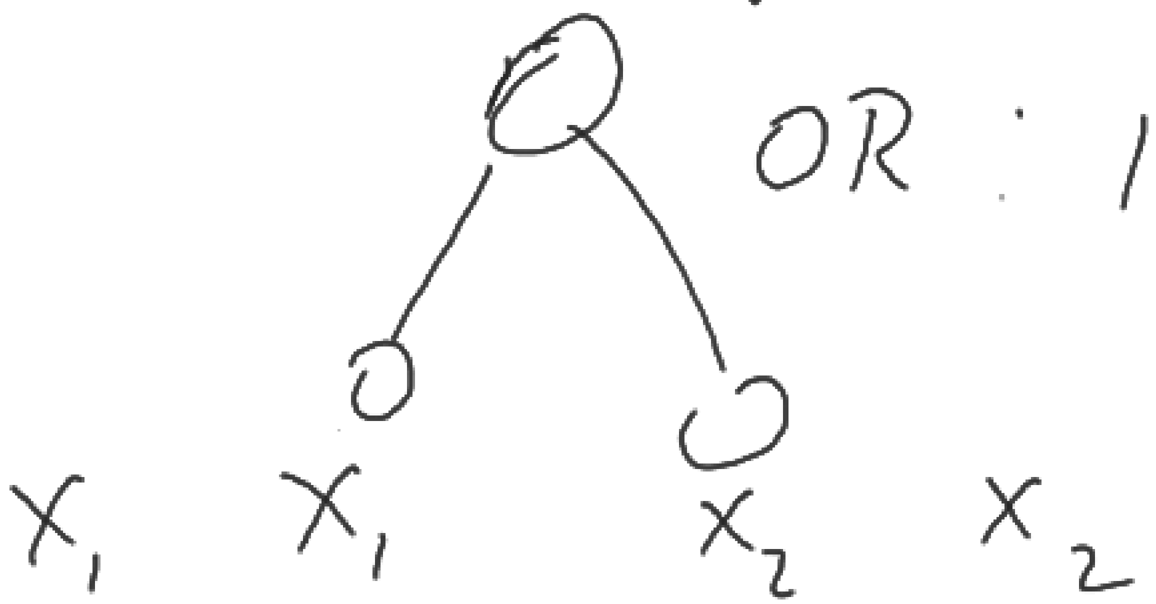
$$\text{UNSAT} = \{ \text{Boolean formulas } \phi \text{ s.t. } \forall x : \phi(x) = 0 \}$$

$$[x_1 \wedge (x_2 \vee x_3) \wedge (\neg x_1)]$$



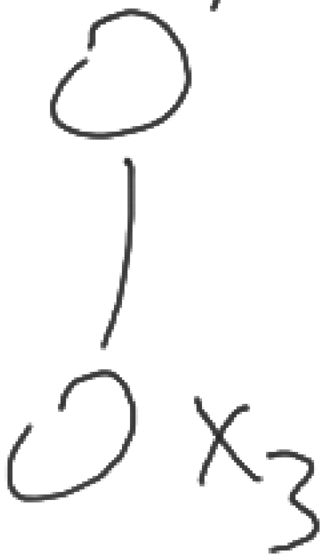
$\phi \to g_\phi$ - poly over F

$$\boxed{\begin{aligned}&\deg(g_\phi) \le \text{size}(\phi)\\ &\forall x_1 \dots x_n \in \{0,1\}: \phi(\bar{x}) = g_\phi(\bar{x})\end{aligned}}$$

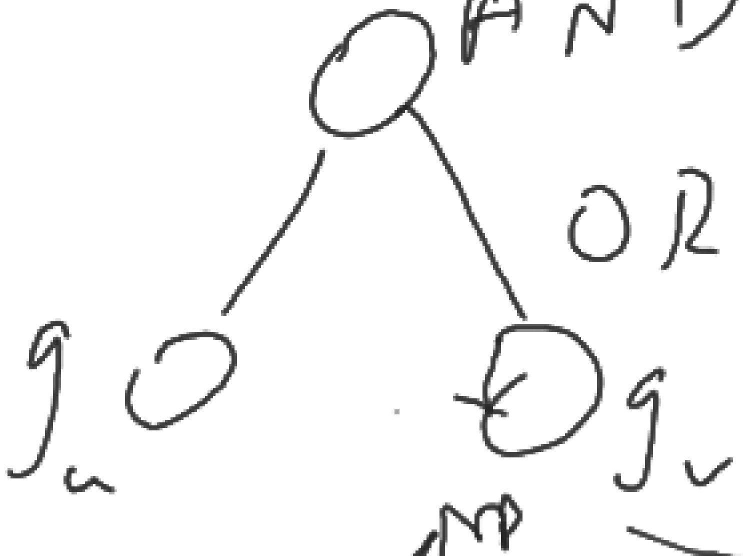


AND: $x_1 \cdot x_2$

OR: $1-(1-x_1)(1-x_2)$



NOT: $1-x_3$



AND: $g_u \cdot g_v$

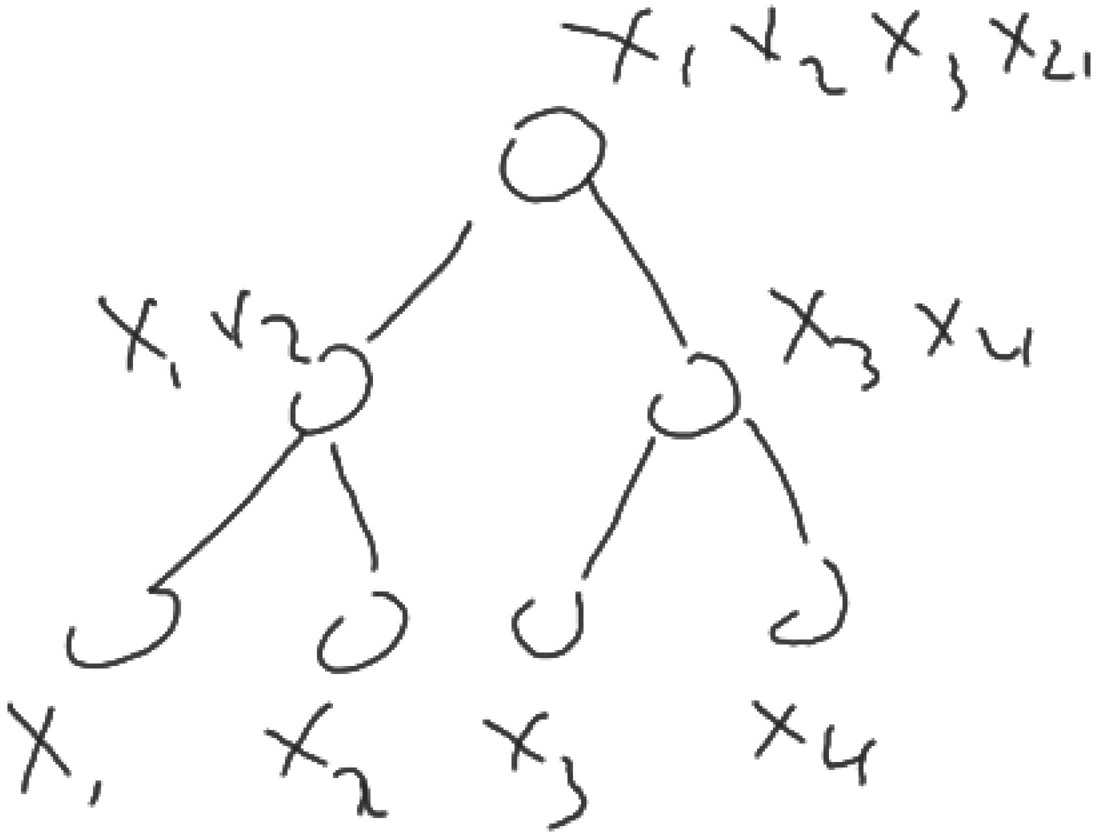
OR: $1-(1-g_u)(1-g_v)$ -

Low-degree extension

$f : \{0,1\}^n \longrightarrow \{0,1\}$ (or $\mathbb{F}$)

$g : \mathbb{F}^n \longrightarrow \mathbb{F}$

- $\forall \bar{x} \in \{0,1\}^n : g(\bar{x}) = f(x)$
- g has relatively low degree


x1 x2 x3 x4
x1 x2
x3 x4
x1
x2
x3
x4

Wanted: IP for UNSAT

$\Leftrightarrow$ IP to prove: ϕ has no satisfying assignments

$$\Leftrightarrow \forall \bar{x} \in \{0,1\}^n : \phi(x) = 0$$

$$\Leftrightarrow \forall \bar{x} \in \{0,1\}^n \quad g_\phi(x) = 0$$

$$\Leftrightarrow \sum_{\bar{x} \in \{0,1\}^n} g_\phi(\bar{x}) = 0$$

Use sumcheck with $|F| >> \deg(g_\phi) \cdot n$

Protocol for #SAT

Toda's Theorem: $PH \subseteq \underline{P^{\#SAT}}$

$\Rightarrow PH \subseteq IP$

L - Deterministic poly time V

$NP: x \in L \iff \exists y : V(x,y) = 1$

$coNP: x \in L \iff \forall y : V(x,y) = 1$

$\Sigma^2 : x \in L \iff \exists y \forall z : V(x,y,z) = 1$

$\Pi^2 : x \in L \iff \forall y \exists z : V(x,y,z) = 1$