Computational Efficiency and Delegation of Computation

Doubly Efficient IPs

DE-IP

Given input of size n

P runs in $\text{poly}(n)$

V runs in $\underbrace{O(n\,\text{polylog}(n))}_{\tilde{O}(n)}$

$\text{DE-IP} \subseteq \text{BPP}$

$\subseteq \text{SPACE}[\tilde{O}(n)]$

$BPP \cap SPACE[\tilde{O}(n)] \subseteq DE\text{-}IP$?

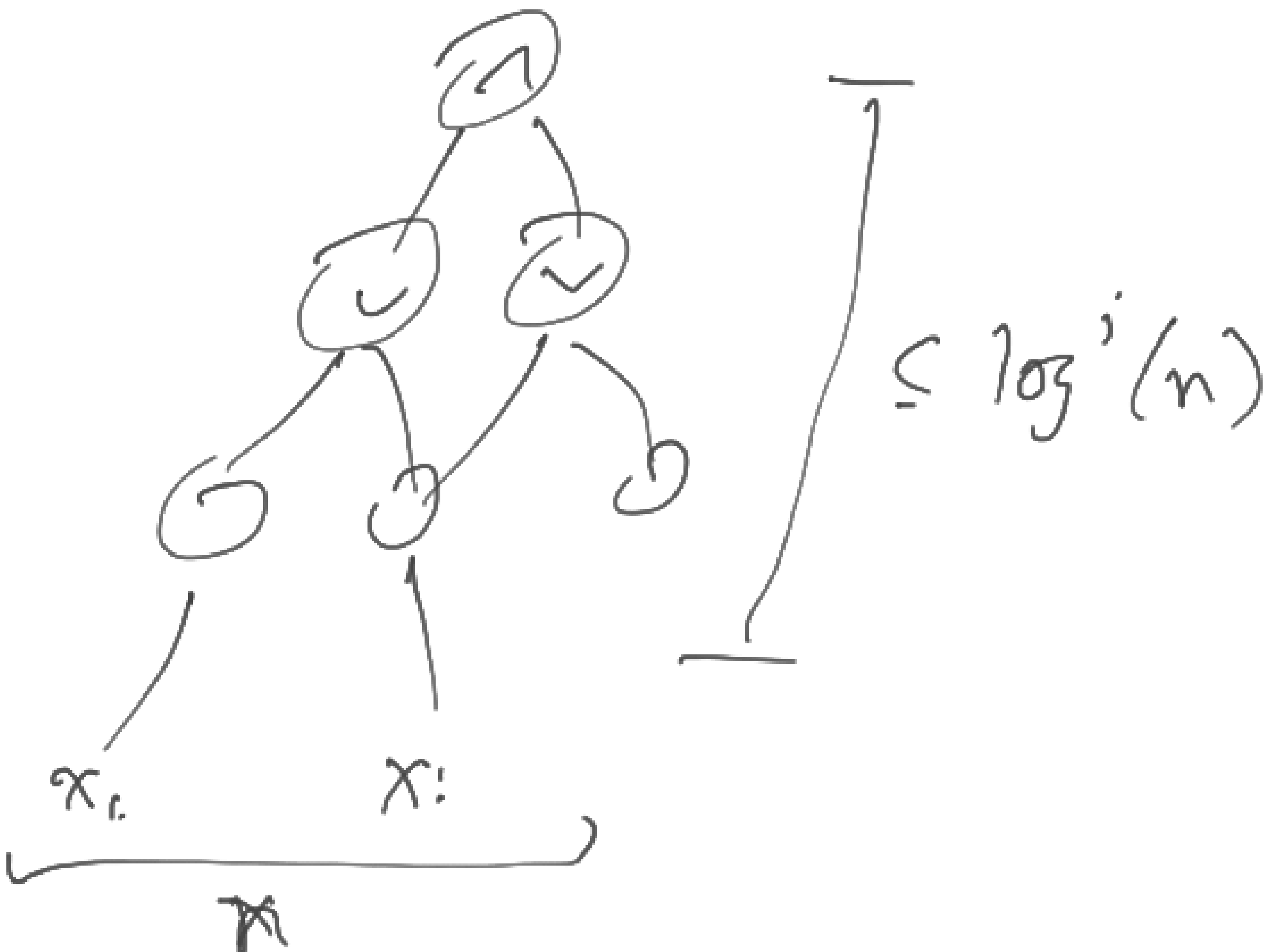
Ans: Don't know

$P \cap SPACE[\tilde{O}(n^{0.49})] \subseteq DE\text{-}IP$ [RRR16]

L-uniform $NC \subseteq DE\text{-}IP$

$NC^i = \{ L \mid L$ can be decided by poly-size Boolean circuits of depth $\log^i(n)$ of fan-in 2 $\}$

$NC = \bigcup_i NC^i$



$\{C_n\}_{n \in \mathbb{N}}$

s.t. $\forall x \in \{0,1\}^n$

$C_n(x) = 1(x \in L)$

$\{C_n\}$ is uniform if $\exists$ alg. A s.t.
$\forall n \in \mathbb{N}$, $A(n)$ outputs description of C_n

$\{C_n\}$ is P-uniform if A is poly-time
$\{C_n\}$ is L-uniform if A is logspace

L-uniform $NC \subseteq P$

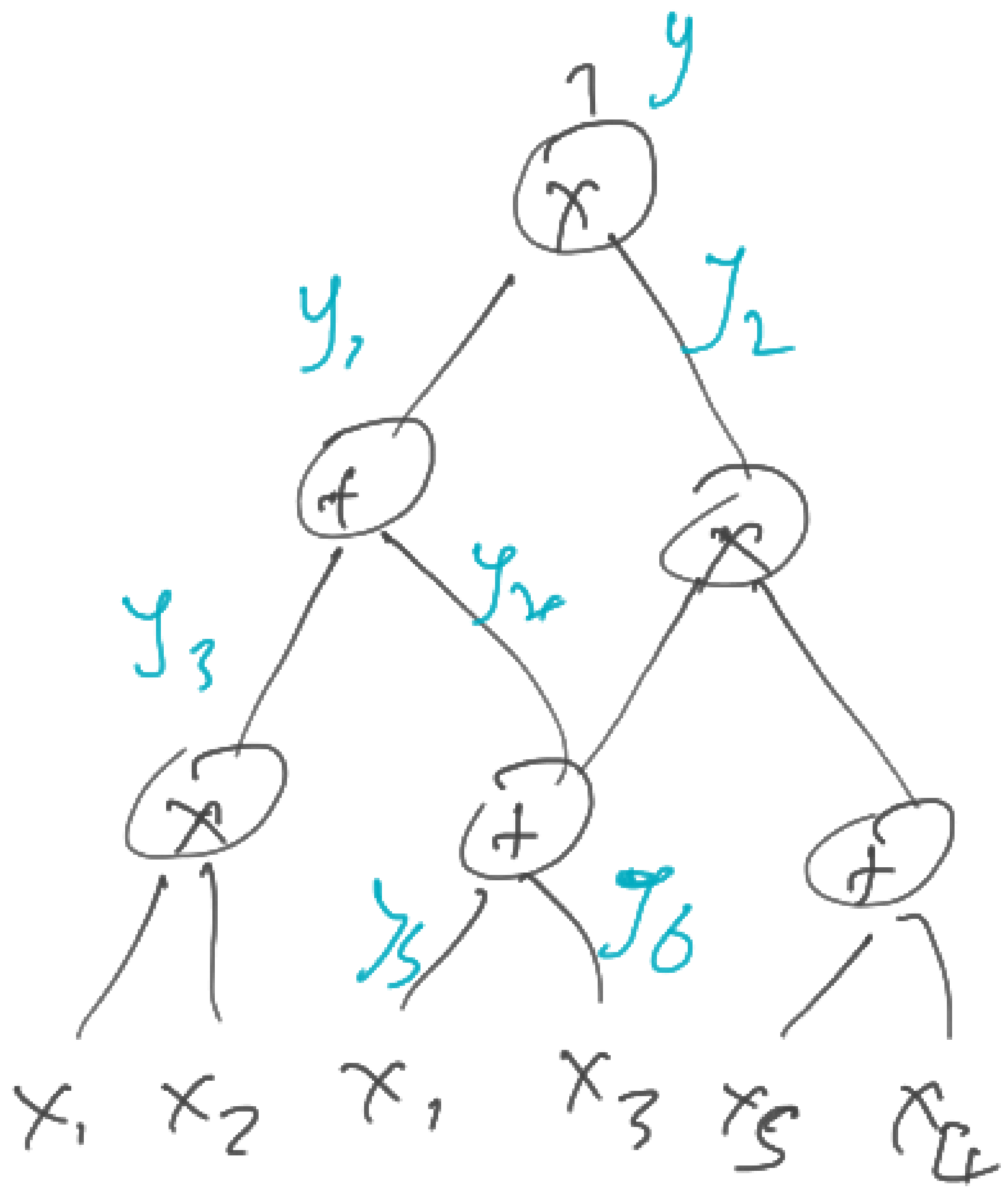
Evaluating Arithmetic Circuits

Fix field $\mathbb{F}$, $C : \mathbb{F}^n \to \mathbb{F}$

(L-uniform)

$x_1, \dots, x_n, y \in \mathbb{F}$

$C(x_1, \dots, x_n) = y$

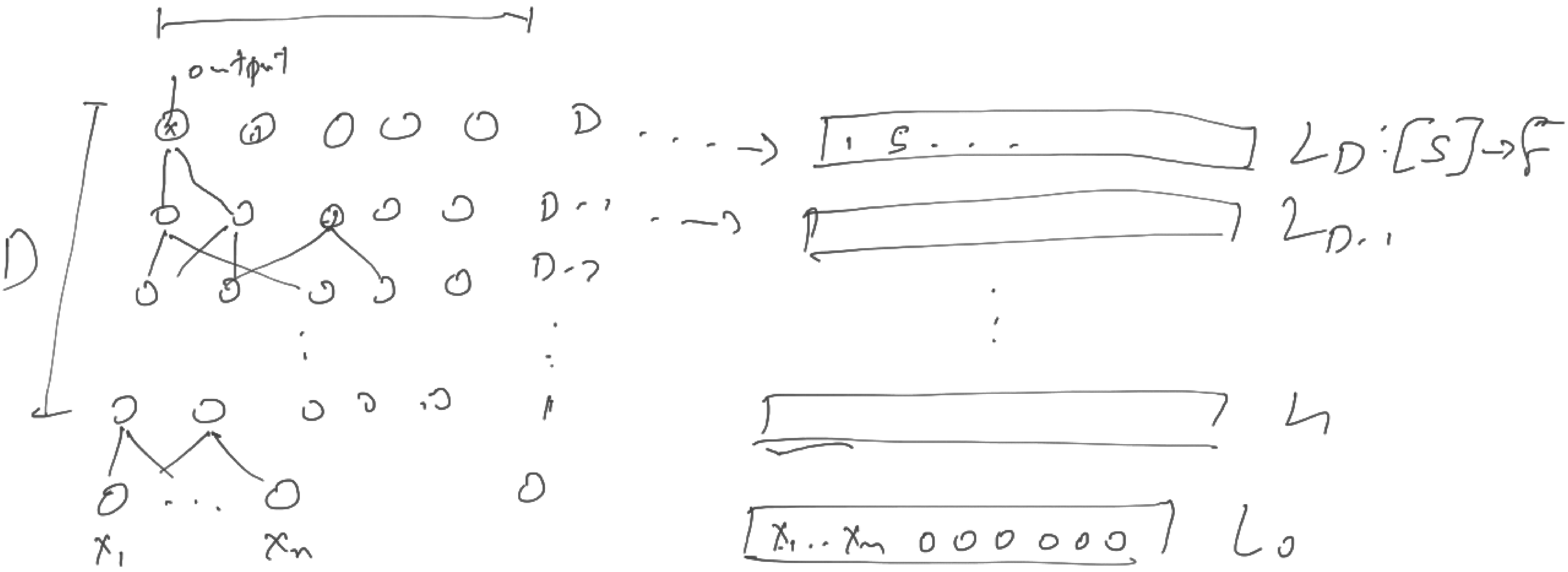


P   V

Soundress error $\geq 1 - \frac{1}{2^d}$

$\exists P^*$ s.t. $\Pr[\langle P^*, V \rangle \text{ accepts}] \geq 1 - \frac{1}{2^d}$

C is "layered". $\quad \mathrm{size}(C) = S, \quad \mathrm{depth}(C) = D$
$= 2^S$



$\boxed{L_i(u) = \text{output of } u^{\text{th}} \text{ gate in layer } i}$

Multilinear Extension (MLE)

Given fns. $f : \{0,1\}^s \to \mathbb{F}$, $g : \mathbb{F}^s \to \mathbb{F}$, where:

- g is a multilinear polynomial
- $\forall x \in \{0,1\}^s : g(x) = f(x)$

Then, g is an MLE of f.

Every f has a unique MLE, given as follows:

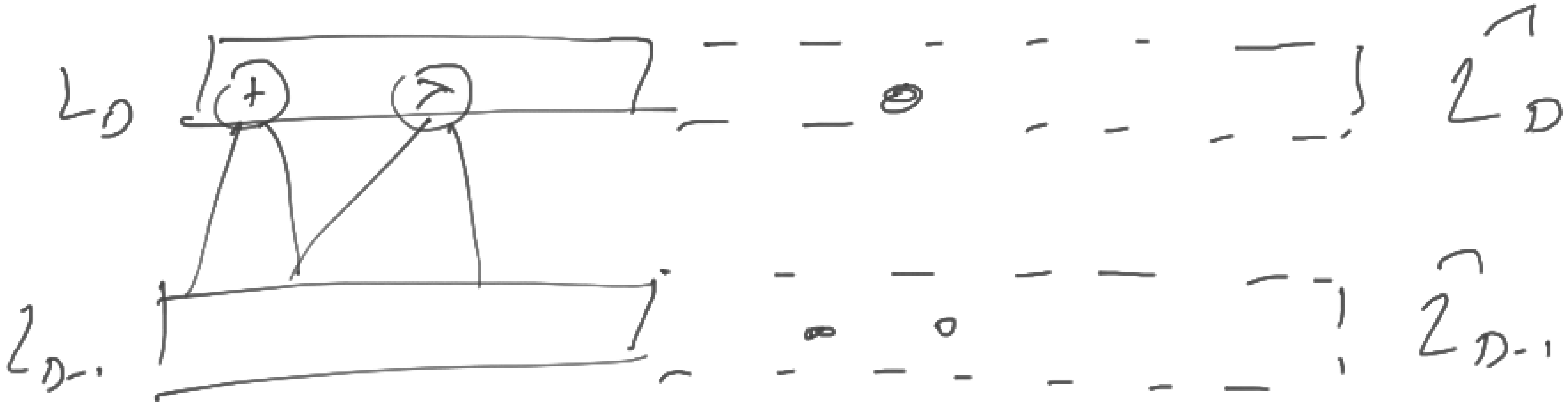
$$g(x) = \sum_{z \in \{0,1\}^s} f(z) \cdot \prod_{i \in [s]} \left(x_i z_i + (1-x_i)(1-z_i) \right)$$

GKR protocol:

$L_D : [S] \to F$

$L_D : \{0,1\}^s \to F$

$\hat{L}_D : F^s \to F$



$add_i : (\{0,1\}^s)^3 \to F$: $add_i(u,v,w) = 1$ if u^{th} gate at layer i is an add gate with input v^{th} and w^{th} gates of layer $(i-1)$

$= 0$ else

$mult_i : (\{0,1\}^s)^3 \to F$

$\widehat{add}_i : F^{3s} \to F$

$\widehat{mult}_i : F^{3s} \to F$

Assume: V has oracle access to $\widehat{add}_i$'s and $\widehat{mult}_i$'s.

$$L_D(u) = \sum_{v,w \in \{0,1\}^s} \Big[add_D(u,v,w)\,(L_{D-1}(v) + L_{D-1}(w)) + mult_D(u,v,w)\,(L_{D-1}(v) \cdot L_{D-1}(w)) \Big]$$

$$\widehat{L}_D(u) = \sum_{v,w \in \{0,1\}^s} \underbrace{\Big[\widehat{add}_D(u,v,w)\,(\widehat{L}_{D-1}(v) + \widehat{L}_{D-1}(w)) + \widehat{mult}_D(u,v,w)\,(\widehat{L}_{D-1}(v) \cdot \widehat{L}_{D-1}(w)) \Big]}_{g_{D,u}(v,w)}$$

$$\widehat{L}_D(u) = \sum_{v,w \in \{0,1\}^s} g_{D,u}(v,w)$$

- P claims $C(x_1, \ldots, x_n) = y \equiv L_D(0^s) = y$

$\equiv \hat{L}_D(0^s) = y$

$\Downarrow$

$$\sum_{\substack{v_1, \ldots, v_s \in \{0,1\} \\ w_1, \ldots, w_s}} g_{D,u}(v, w) = y$$

$\deg(g_{D,u}) \leq 2$ in each variable

$\tilde{L}_D(0) = y$

- P, V run sumcheck to prove $\sum_{v,w \in \{0,1\}^s} g_{D,u}(v,w) = y$

- V needs to evaluate $g_{D,u}(v,w)$ at a random point
  - have oracle access to $\widetilde{add}_D(u,v,w)$, $\widetilde{mult}_D(u,v,w)$
  - need $\hat{L}_{D-1}(v)$, $\hat{L}_{D-1}(w)$

- Ask prover for y_1, y_2, s.t. $\hat{L}_{D-1}(v) = y_1$, $\hat{L}_{D-1}(w) = y_2$

- Do two sumchecks to verify

→ reduce this to one eval. of $\hat{L}_{D-1}$

want to reduce checking $\hat{L}_{D-1}(v) = y_1$, $\hat{L}_{D-1}(w) = y_2$

$v, w \in F^S$

- Define $\ell : F \to F^S$: $\ell(z) = (1-z) \cdot v + z \cdot w$

$\ell(0) = v$, $\ell(1) = w$

- Define $q(z) = \hat{L}_{D-1}(\ell(z))$

$\deg.(q) \leq S$

$q(0) = \hat{L}_{D-1}(\ell(0)) = \hat{L}_{D-1}(v)$

$q(1) = \hat{L}_{D-1}(w)$

$\hat{L}_{D-1}(v)$

$= v_1 v_2 + v_3 v_5 \dots v_5$

$\underline{\ell_1(z)} \cdot \underline{\ell_2(z)} + \ell_3(z) \dots$

- P sends co-effs. of q
- Uses $q(0)$ and $q(1)$ as values for $\hat{L}_{D-1}(v)$ and $\hat{L}_{D-1}(w)$ in the sumcheck
- Pick random $r \in \mathbb{F}$, check that $\hat{L}_{D-1}(l(r)) = q(r)$
  - Can eval. $q(r)$ on its own
  - Recurse with claim $\hat{L}_{D-1}(l(r)) = q(r)$

Soundness

Suppose $\hat{L}_D(0) \neq y$

$$\Pr[V \text{ accepts}] \le \underbrace{\Pr[V \text{ acc.} \wedge \hat{L}_{D-1}(\ell(r)) = q(r)]}_{\le O\left(\frac{s}{|F|}\right)}$$

$$+ \underbrace{\Pr[V \text{ acc} \mid \hat{L}_{D-1}(\ell(r)) \neq q(r)]}_{\text{Soundness error for depth } D-1}$$

$\le O\left(\frac{d \cdot s}{|F|}\right)$

$$\le \Pr[V \text{acc} \wedge \underbrace{(\hat{L}_{D-1}(v) = q(0) \wedge \hat{L}_{D-1}(w) = q(1))}_{2}]$$

$$+ \Pr[V \text{acc} \wedge \hat{L}_{D-1}(\ell(r)) = q(r) \mid \text{this didn't happen}]$$

Sumcheck error $\le O\left(\frac{s}{|F|}\right)$

$\le s/|F|$