Interactive proof

Schwartz–Zippel lemma

Expand $f(x)$ for me

Polynomial expansion

$g(x) = 6x^3+49x^2+128x+105$

$f(x) = (x+3)(3x+5)(2x+7)$

Verification: pick a random value r
test $f(r) - g(r) = 0$

If $f(x) - g(x) \neq 0$, but $f(r) - g(r) = 0$,

$\rightarrow r$ is a root of $f(x) - g(x)$,

$\rightarrow \Pr[r \text{ is a root}] = \frac{3}{|\text{random space}|}$

Sumcheck protocol

$$H = \sum_{b_1,\ldots,b_k \in \{0,1\}} f(b_1, \ldots, b_k)$$

- Multivariate polynomial $f(x_1, \ldots, x_k)$

Number of evaluations in the sum: 2^k

Time to compute each evaluation: $\mathrm{T} = (d+1)^k \cdot k$

Total time to compute the sum: $2^k \cdot T$

Sumcheck protocol

$f(x_1, \dots, x_k)$

$$H = \sum_{b_1,\dots,b_k \in \{0,1\}} f(b_1, \dots, b_k)$$

$$f_1(x_1) = \sum_{b_2,\dots,b_k \in \{0,1\}} f(x_1, b_2 \dots, b_k)$$

r_1

$$f_2(x_2) = \sum_{b_3,\dots,b_k \in \{0,1\}} f(r_1, x_2, b_3 \dots, b_k)$$

....

r_i

$$f_{i+1}(x_{i+1}) = \sum_{b_{i+2},\dots,b_k \in \{0,1\}} f(r_1, \dots, r_i, x_{i+1}, b_{i+2} \dots, b_k)$$

....

r_{k-1}

$$f_k(x_k) = f(r_1, \dots, r_{k-1}, x_k)$$

Check:

$$H = f_1(0) + f_1(1)$$

$$f_1(r_1) = f_2(0) + f_2(1)$$

....

$$f_i(r_i) = f_{i+1}(0) + f_{i+1}(1)$$

....

$$f_{k-1}(r_{k-1}) = f_k(0) + f_k(1)$$

$$f_k(r_k) = f(r_1, \dots r_k)$$

Complexity

- Correctness: 1
- Soundness: $\frac{d(k+1)}{|\mathbb{F}|}$

- Prover time: $O\left(2^k\right)$ if d=1
- Proof size: $O(dk)$
- Verification time: $O(dk) + T$

Total time to compute the sum: $2^k \cdot T$

GKR protocol

Verifiable Computation (VC)

server

client

data

function f

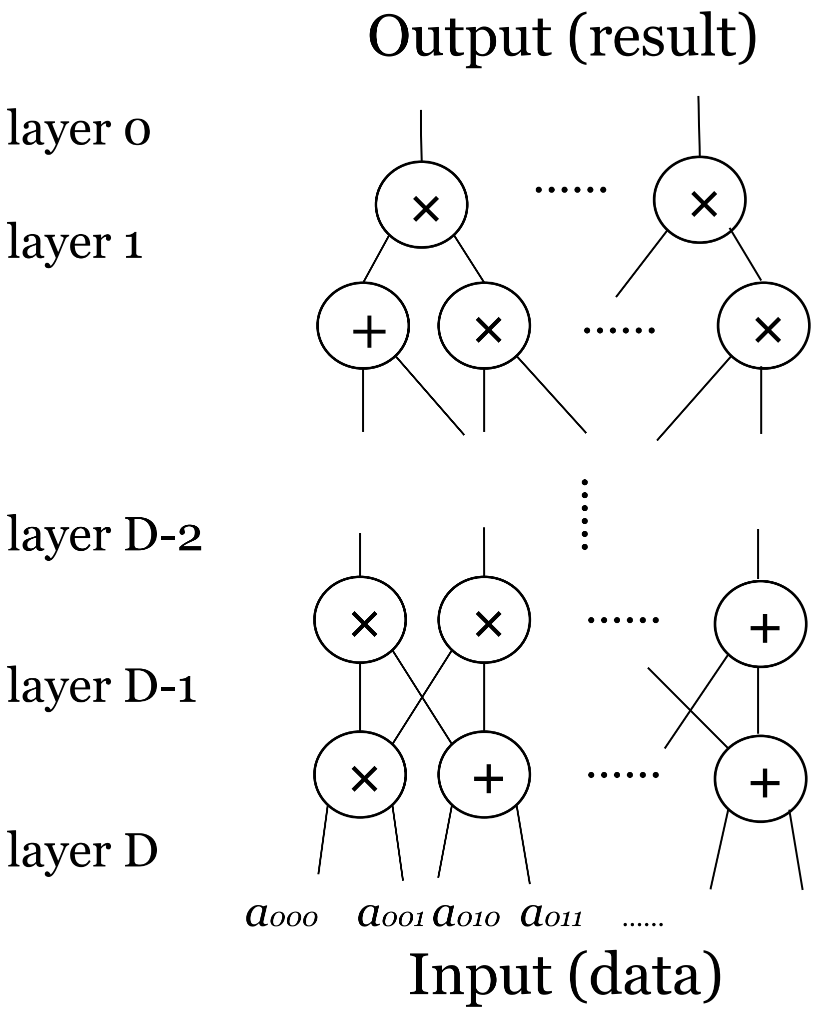
result = f(data) + 

Verification: ✔ **or** ☐

Correctness/completeness: Pr[result = f(data) and proof is honest and verification is ✓] = 1

Soundness/security: Pr [result ≠ f (data) and verification is ✓] ≤ $\frac{1}{2^{100}}$

Gate label and multi-linear extension



S: number of gates in each layer
D: depth of the circuit

What's the # of variables in V_D ?
s = log S

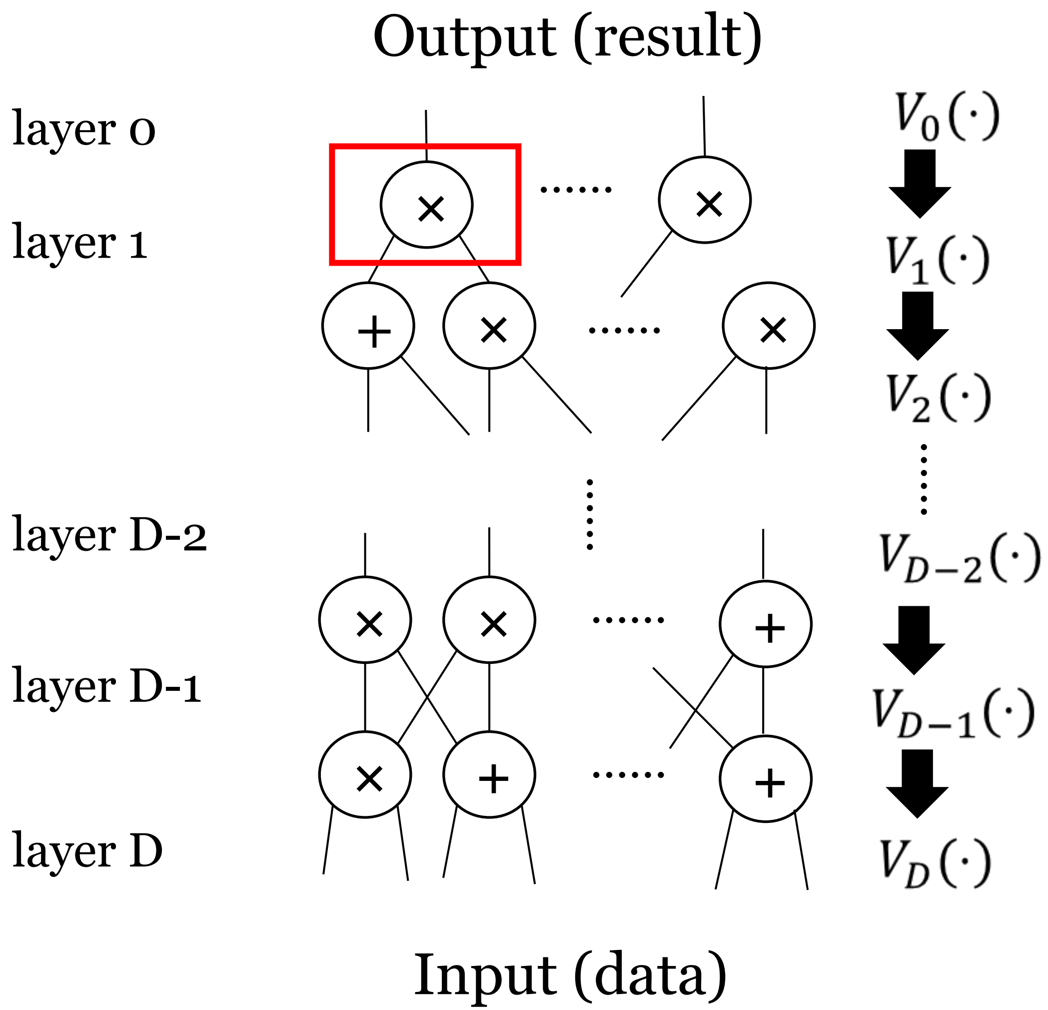
If V_D is multilinear, how many coefficients?
2^s=S

V_D is unique, multi-linear extension

$V_D(\cdot)$

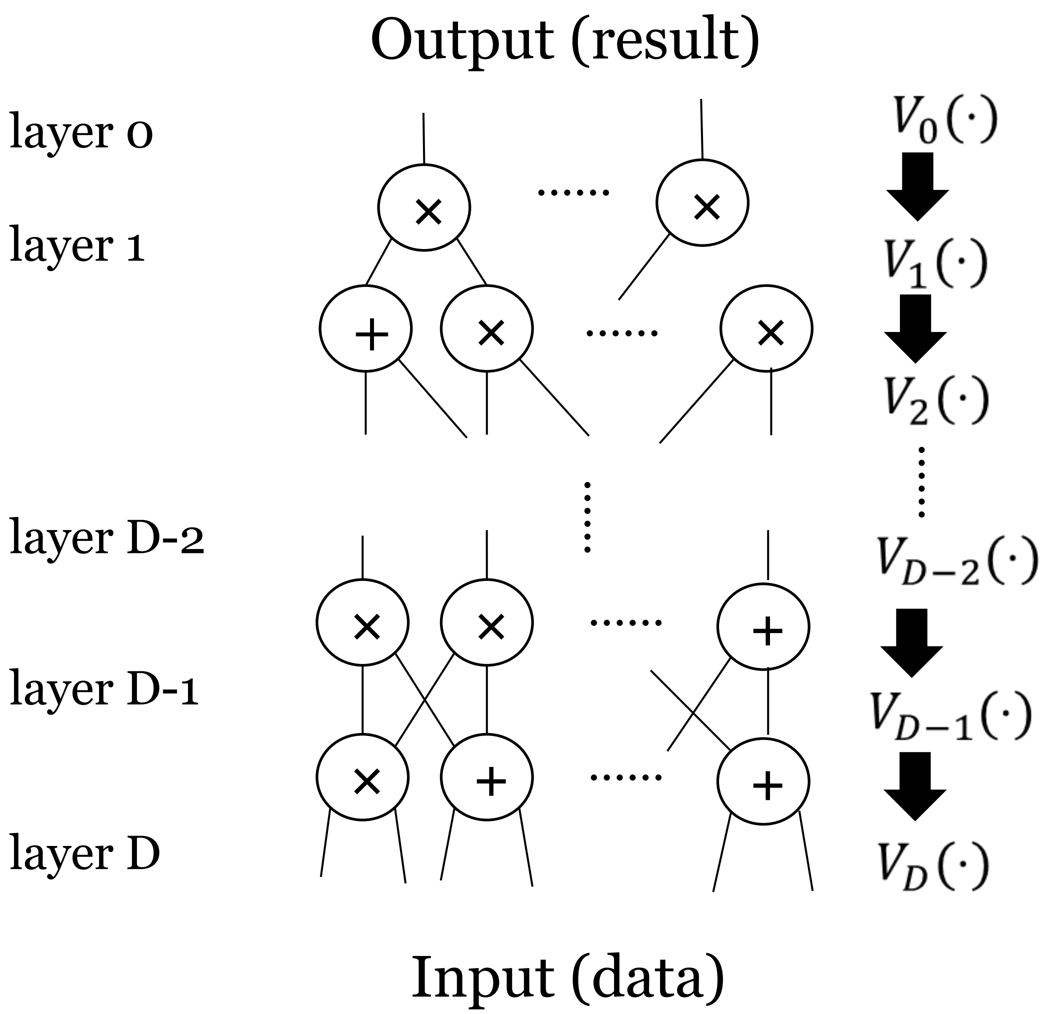
$V_D(0,0,0) = a_0$
$V_D(0,0,1) = a_1$
$V_D(0,1,0) = a_2$
…

Relation of consecutive layers



$$V_0(0) = V_1(0,0) \times V_1(0,1)$$

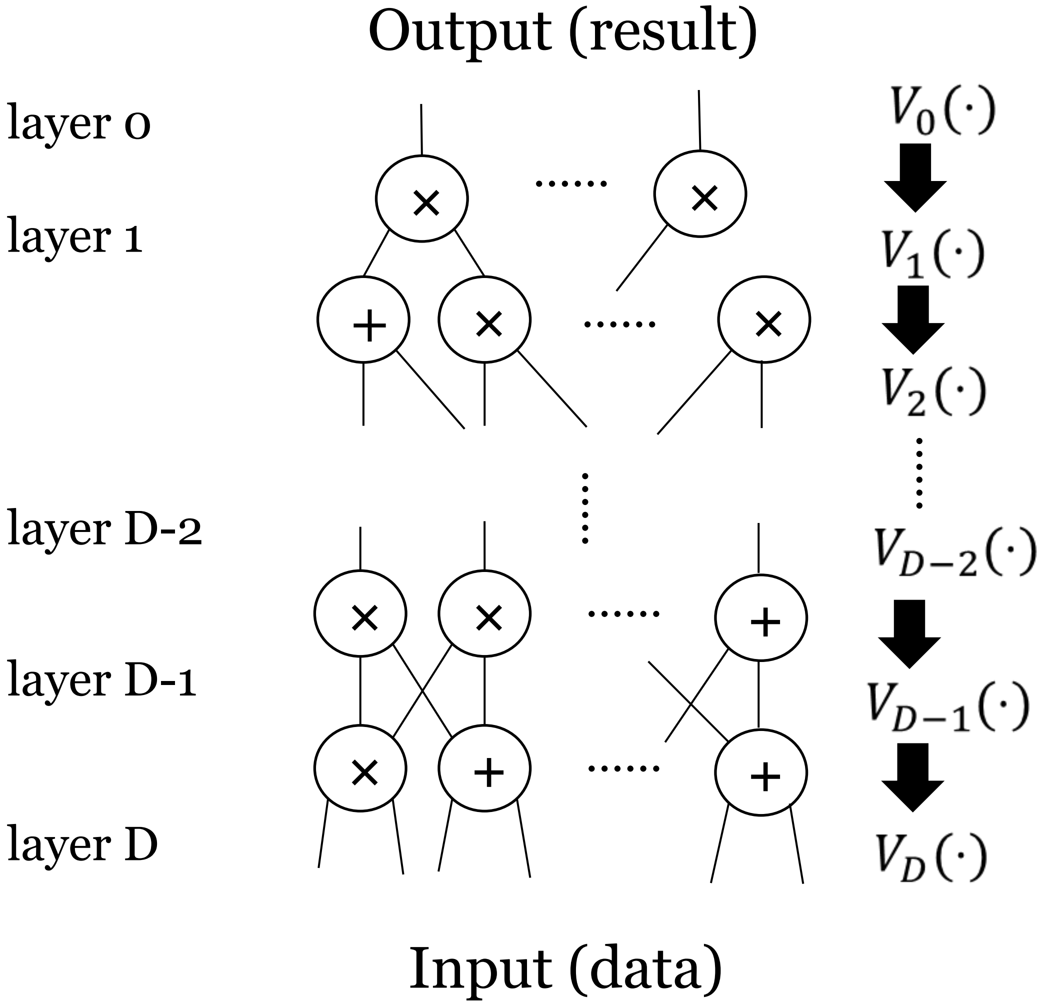
Checking relation efficiently



$$V_i(\vec{g}) = \sum_{\vec{u},\vec{v}\in\{0,1\}^s} \left(add_i\,(\vec{g},\vec{u},\vec{v})(V_{i+1}(\vec{u}) + V_{i+1}(\vec{v})) + mult_i(\vec{g},\vec{u},\vec{v})V_{i+1}(\vec{u})V_{i+1}(\vec{v})\right)$$

Wiring predicate:
$add_i(\vec{g},\vec{u},\vec{v}) = 1$iff $(\vec{g},\vec{u},\vec{v})$ connects to an add gate
$mult_i(\vec{g},\vec{u},\vec{v}) = 1$iff $(\vec{g},\vec{u},\vec{v})$ connects to a mult gate

Sumcheck



$$V_i(\vec{g}) = \sum_{\vec{u},\vec{v}\in\{0,1\}^s} f_{i,\vec{g}}(\vec{u},\vec{v})$$

$$= \sum_{\vec{u},\vec{v}\in\{0,1\}^s} \left(add_i(\vec{g},\vec{u},\vec{v})(V_{i+1}(\vec{u}) + V_{i+1}(\vec{v})) + mult_i(\vec{g},\vec{u},\vec{v})V_{i+1}(\vec{u})V_{i+1}(\vec{v})\right)$$

Sumcheck protocol

$f(x_1, \dots, x_k)$

$$H = \sum_{b_1,\dots,b_k \in \{0,1\}} f(b_1, \dots, b_k)$$

$$f_1(x_1) = \sum_{b_2,\dots,b_k \in \{0,1\}} f(x_1, b_2 \dots, b_k)$$

r_1

$$f_2(x_2) = \sum_{b_3,\dots,b_k \in \{0,1\}} f(r_1, x_2, b_3 \dots, b_k)$$

....

r_i

$$f_{i+1}(x_{i+1}) = \sum_{b_{i+2},\dots,b_k \in \{0,1\}} f(r_1, \dots, r_i, x_{i+1}, b_{i+2} \dots, b_k)$$

....

r_{k-1}

$$f_k(x_k) = f(r_1, \dots, r_{k-1}, x_k)$$

Check:

$$H = f_1(0) + f_1(1)$$

$$f_1(r_1) = f_2(0) + f_2(1)$$

....

$$f_i(r_i) = f_{i+1}(0) + f_{i+1}(1)$$

....

$$f_{k-1}(r_{k-1}) = f_k(0) + f_k(1)$$

$$f_k(r_k) = f(r_1, \dots r_k)$$

Reduction

- Receive output $V_0(0)$

- Run sumcheck: last round, need to check $f(r_1, \dots r_{2s})$

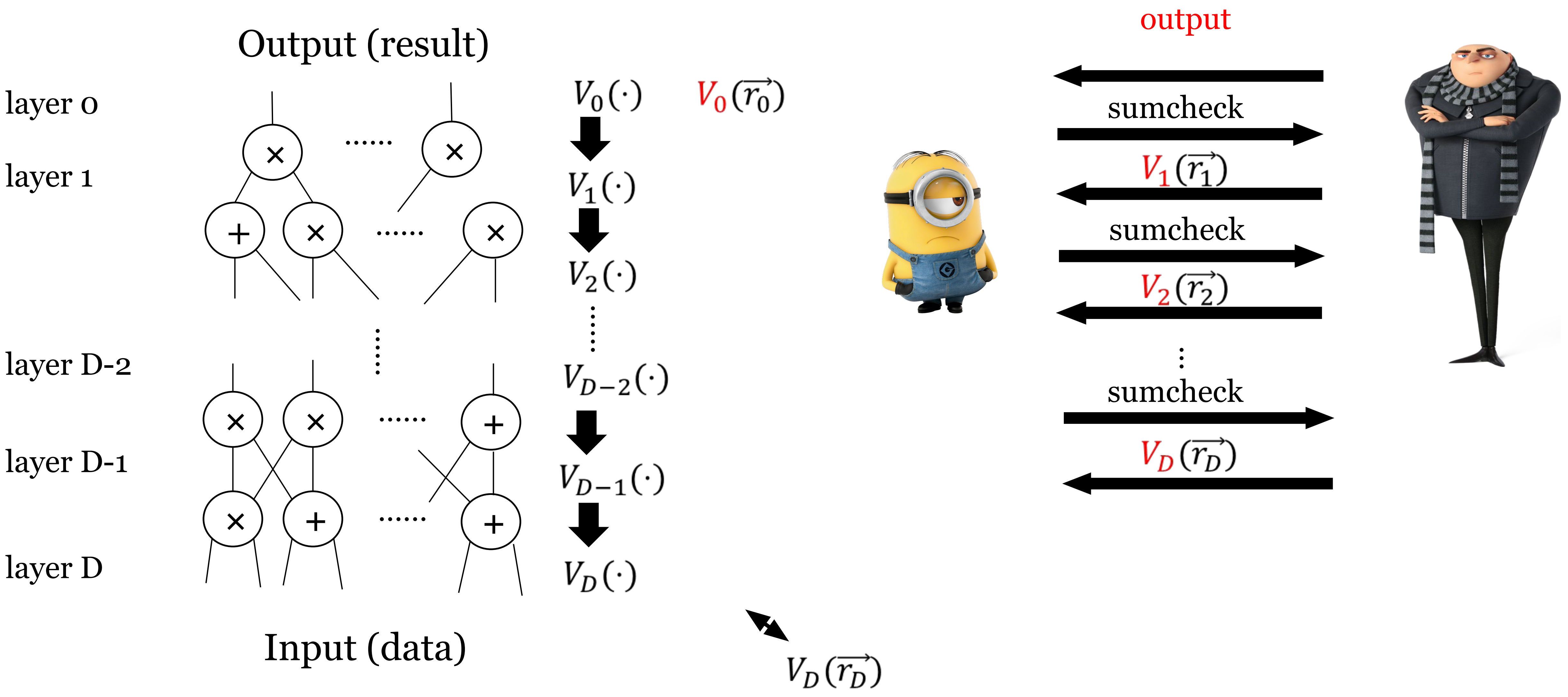
- $f(r_1, \dots r_{2s}) = add_i\ (0, r_1, \dots r_{2s})\big(V_{i+1}(r_1, \dots r_s) + V_{i+1}(r_{s+1}, \dots r_{2s})\big) +$
$mult_i\ (0, r_1, \dots r_{2s})\big(V_{i+1}(r_1, \dots r_s) \times V_{i+1}(r_{s+1}, \dots r_{2s})\big)$

- Compute $add_i\ (0, r_1, \dots r_{2s})$, $mult_i\ (0, r_1, \dots r_{2s})$ locally, receive $V_{i+1}(r_1, \dots r_s), V_{i+1}(r_{s+1}, \dots r_{2s})$ from the prover and check the equality

- Combine $V_{i+1}(r_1, \dots r_s), V_{i+1}(r_{s+1}, \dots r_{2s})$ into $V_{i+1}(\vec{r})$

- Recurse to next layer

GKR protocol



Correctness and soundness

- Correctness: 1
- Soundness: $O(\frac{D \log C}{|\mathbb{F}|})$

Complexity

- Proof size: $O(D \log C)$

- Verification time: $O(D \log C + n)$ + time to compute add and $mult$
    - Worst case: O(C)
    - Structured circuits: $O(D \log C + n)$
      e.g., matrix multiplication, data parallel circuits

- Prover time: O(C), [XZZPS, crypto 2019]

- No setup, no cryptographic assumption

Applications

- Verifiable computation
- Complexity theory
- Zero knowledge proof