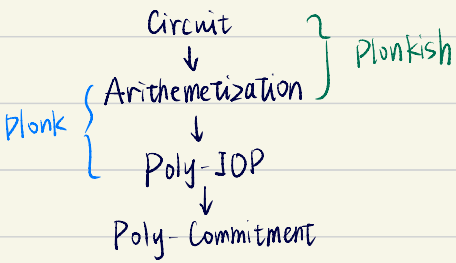
PLONK

properties:
1. universal setup
2. Prover time $O(n \log n)$
   Verifier time $O(\log n)$
   Proof size $O(1)$

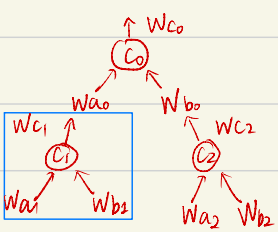


Aim: prove $C(x)=y$

"C" is large so that the verifier is "lazy" to read it.

Step I: arithemetization Step II: prove

↳ w_a w_b w_c / q_L q_R q_m q_c q_o — gate constraints



$$q_L \circ w_a + q_R \circ w_b + q_M \circ (w_a \cdot w_b) + q_c - q_o \circ w_c = 0$$

Not enough!

copy constraints: $w_{a_0} = w_{c_1}$, $w_{b_0} = w_{c_2}$

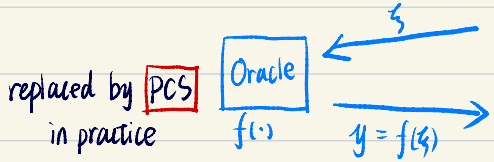
Lesson 2

Step 4. prove 1. gate constraints method: PIOP

2. copy constraints

What's PIOP Polynomial IOP (IP)

Prover Verifier



What's PCS Lesson6

[f] := com(f) — binding, hiding

support linear combination

[f] + [g] = com(f+g)

1. go back to the gate constraints Lesson3

(1) write $\vec{w}_a$, $\vec{w}_b$, $\vec{w}_c$ in polynomials → Lagrange

commit to $w_a(X)$, $w_b(X)$, $w_c(X)$

as well as q_L, q_R, q_M, q_C, q_O

(2) prove $q_L(X)\,w_a(X) + q_R(X)\,w_b(X) + q_M(X)\,w_a(X)\,w_b(X) + q_C(X) - q_O(X)\,w_c(X) = 0$

$\|$ F(X)

(PIOP: V chooses query ξ and checks if F(ξ) = 0)

2. copy constraints

prove $w_{a_0} = w_{c_1}$, $w_{b_0} = w_{c_2}$ $\Rightarrow$ $(w_{a_0}, id_{a_0}) = (\sigma(w_{c_1}), \sigma(id_{c_1}))$, $(w_{b_0}, id_{b_0}) = (\sigma(w_{c_2}), \sigma(id_{c_2}))$ apply permutation

$\{w_{a_0}, w_{b_0}\} = \{w_{c_1}, w_{c_2}\} \Rightarrow \{(w_{a_0}, id_{a_0}), (w_{b_0}, id_{b_0})\} = \{(w_{c_1}, id_{c_1}), (w_{c_2}, id_{c_2})\}$

$\{(w_{a_0} + \beta id_{a_0}), (w_{b_0} + \beta id_{b_0})\} = \{(w_{c_1} + \beta id_{c_1}), (w_{c_2} + \beta id_{c_2})\}$ ← fold

↳ $p = q_0 \cdots q_{n-1}$ aux $\vec{r}$

Lesson4

denote by Z(X)

commit to $a(X)$, $b(X)$, $c(X)$, $z(X)$, apply PIOP

3. putting all together

fold 1 & 2 $\quad F(X) + \alpha Z(X) = q(X)\, z_H(X)$

other optimizations: public inputs, id and coset

Lesson 5