STARKWARE STARK 101

Stark 101: Part 4

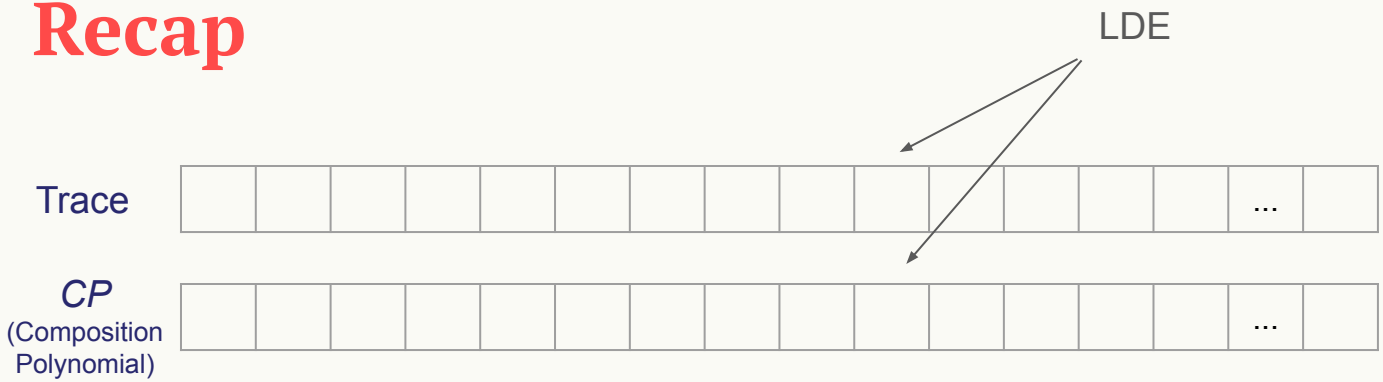
The Proof

Recap

Commitment

Trace Root

Recap



Commitment

Trace Root

CP Root

Recap

Commitment

Trace Root

CP Root

CP_1 Root

CP_2 Root

:

CP_{10} Root

The Entire Proof

Commitment

- Decommitment (Convincing)

How Can the Prover Convince the Verifier?

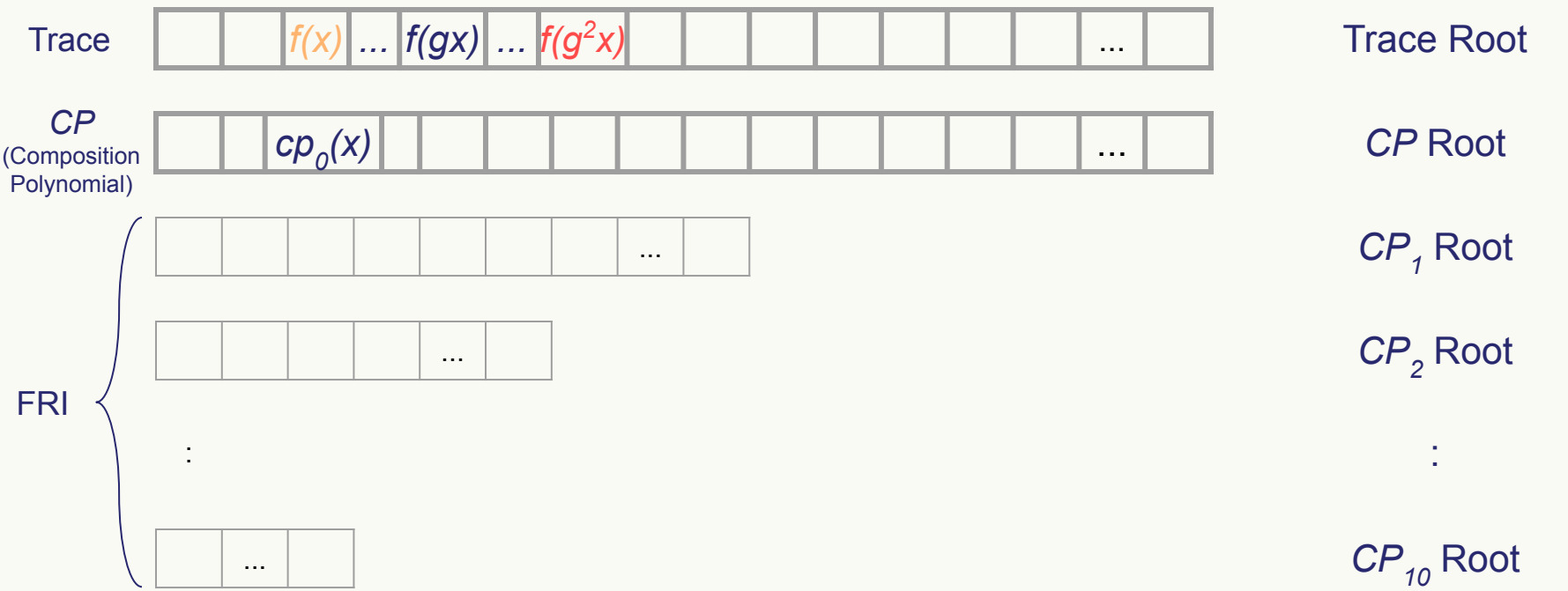
How Can the Prover Convince the Verifier?

Verifier: Sends q random elements

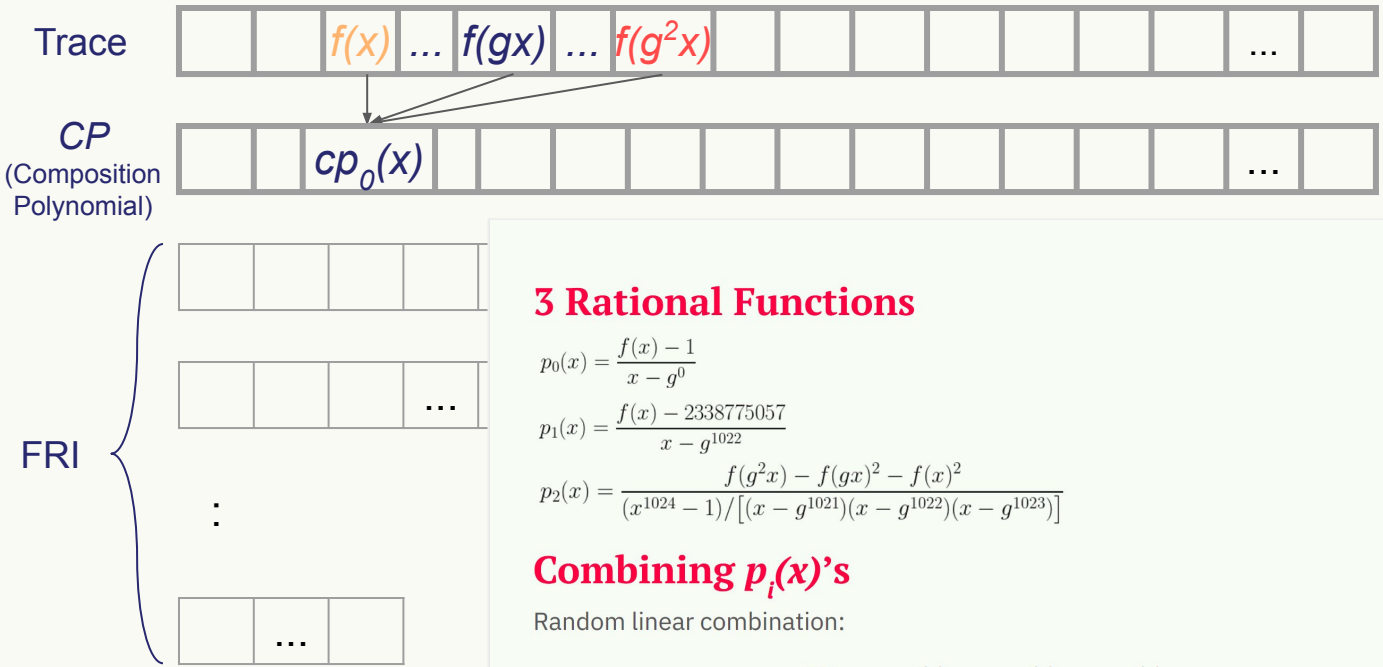
Prover: Provides a validation data for each

What is a validation data?

Trace -> *CP*


Commitment
Trace
f(x)
...
f(gx)
...
f(g^2x)
...
Trace Root
CP
(Composition
Polynomial)
cp_0(x)
...
CP Root
FRI
...
CP_1 Root
...
CP_2 Root
:
:
...
CP_10 Root

Trace -> *CP*



3 Rational Functions

$$p_0(x) = \frac{f(x) - 1}{x - g^0}$$

$$p_1(x) = \frac{f(x) - 2338775057}{x - g^{1022}}$$

$$p_2(x) = \frac{f(g^2x) - f(gx)^2 - f(x)^2}{(x^{1024} - 1)/\left[(x - g^{1021})(x - g^{1022})(x - g^{1023})\right]}$$

Combining $p_i(x)$'s

Random linear combination:

$$CP = \alpha_0 \cdot p_0(x) + \alpha_1 \cdot p_1(x) + \alpha_2 \cdot p_2(x)$$

STARKWARE STARK 101

Commitment

Trace Root

CP Root

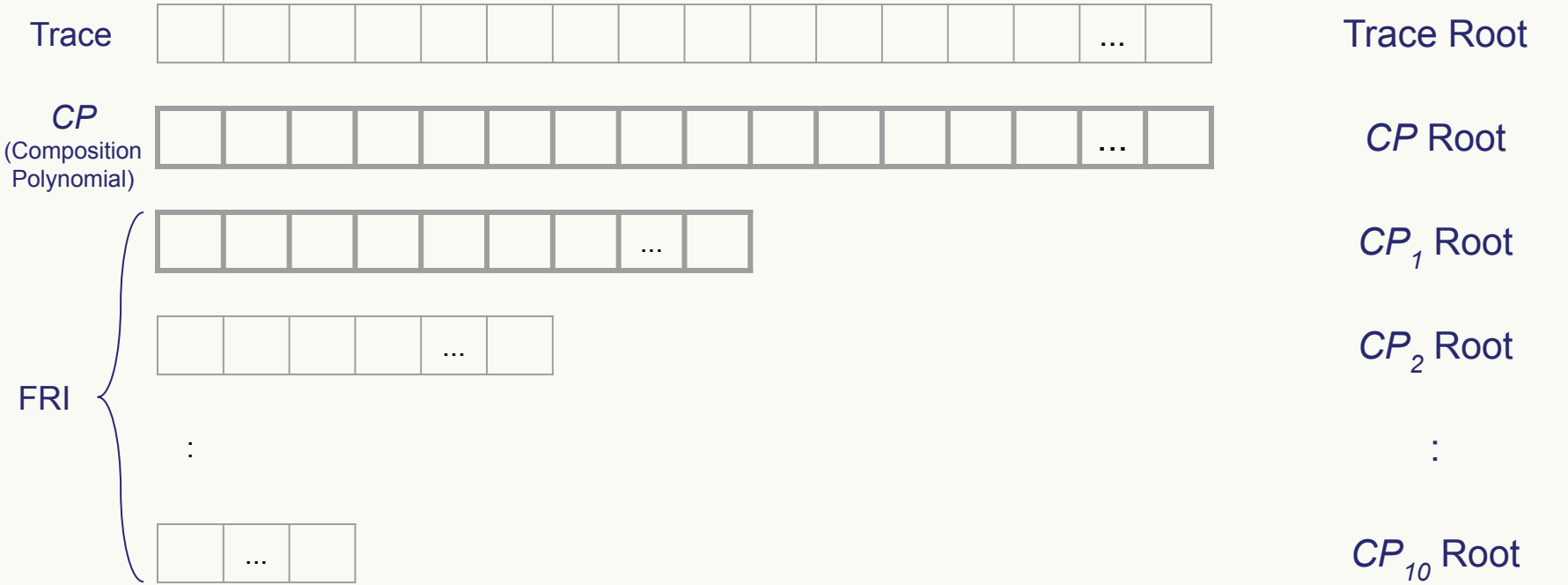
CP_1 Root

CP_2 Root

:

CP_{10} Root

FRI Step


Commitment
Trace
Trace Root
CP
(Composition
Polynomial)
CP Root
FRI
CP1 Root
CP2 Root
CP10 Root

FRI Step

$$\begin{cases} CP_i(x) = g(x^2) + xh(x^2) \\ CP_i(-x) = g(x^2) - xh(x^2) \end{cases} \longrightarrow \begin{cases} g(x^2) = \dfrac{CP_i(x) - CP_i(-x)}{2} \\ h(x^2) = \dfrac{CP_i(x) - CP_i(-x)}{2x} \end{cases}$$

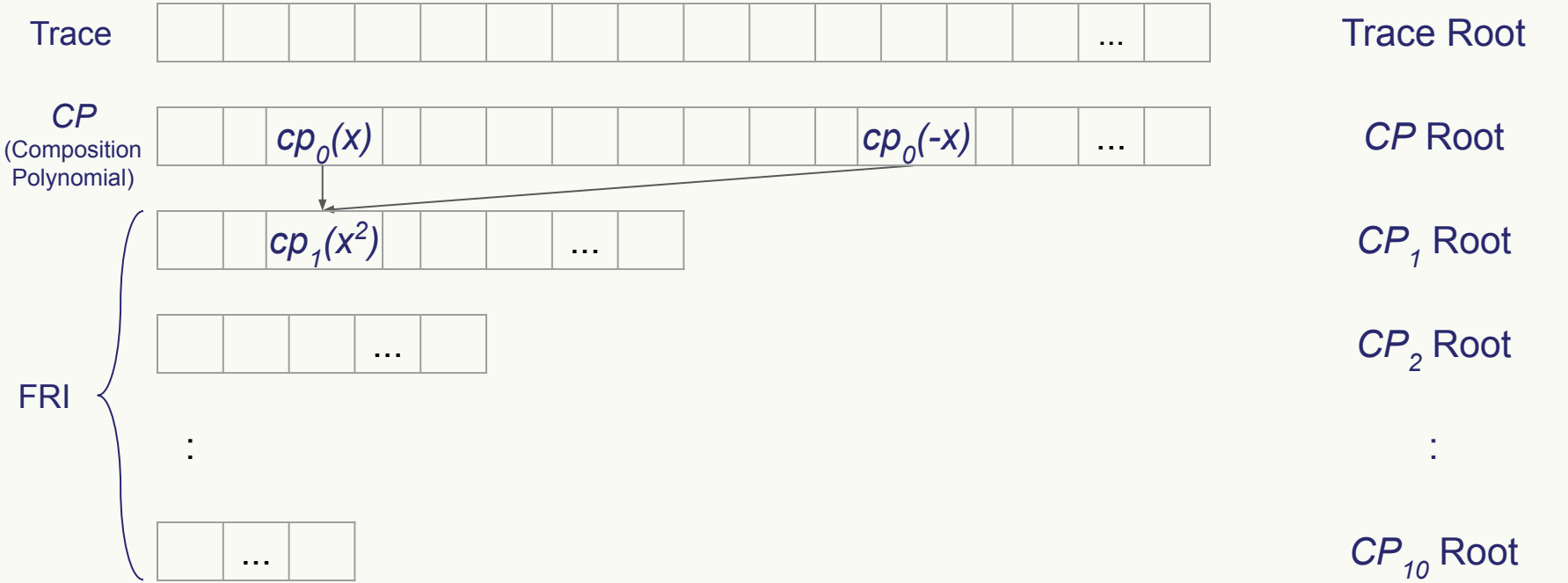
Reminder:

$$CP_{i+1}(x^2) = g(x^2) + \beta h(x^2)$$

Bottom line:

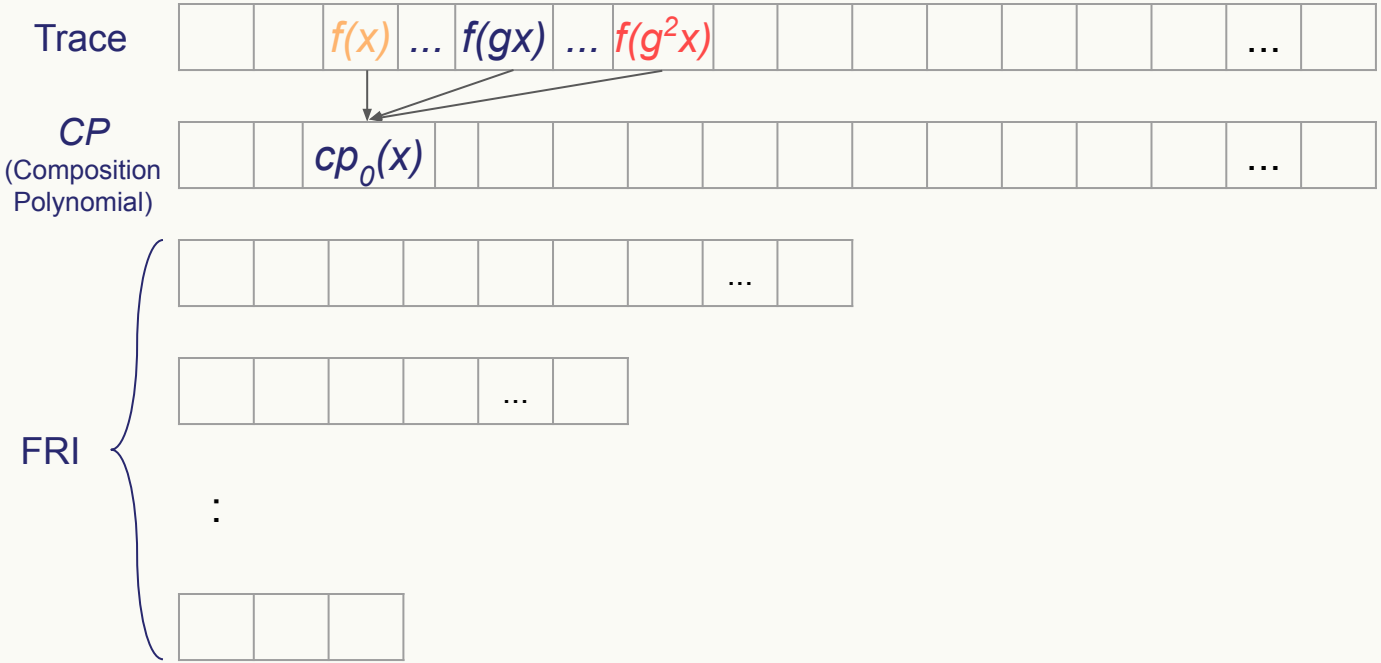
To compute $CP_{i+1}(x^2)$ *we only need* $CP_i(x)$ *and* $CP_i(-x)$

FRI Step


Commitment
Trace
Trace Root
CP
(Composition
Polynomial)
$cp_0(x)$
$cp_0(-x)$
CP Root
$cp_1(x^2)$
CP_1 Root
FRI
CP_2 Root
:
:
CP_{10} Root

Decommitment Phase (for query x)

Decommitment Phase (for query x)



Decommitment

$f(x)$	+ path
$f(gx)$	+ path
$f(g^2x)$	+ path
$cp_0(x)$	+ path

Decommitment Phase (for query x)

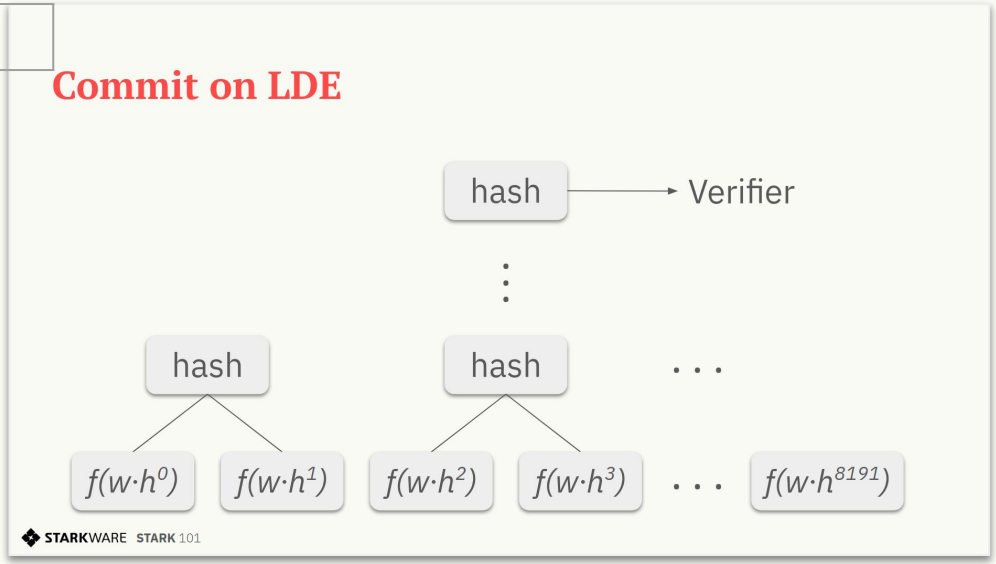
Decommitment

$f(x)$ + path
$f(gx)$ + path
$f(g^2x)$ + path
$cp_0(x)$ + path

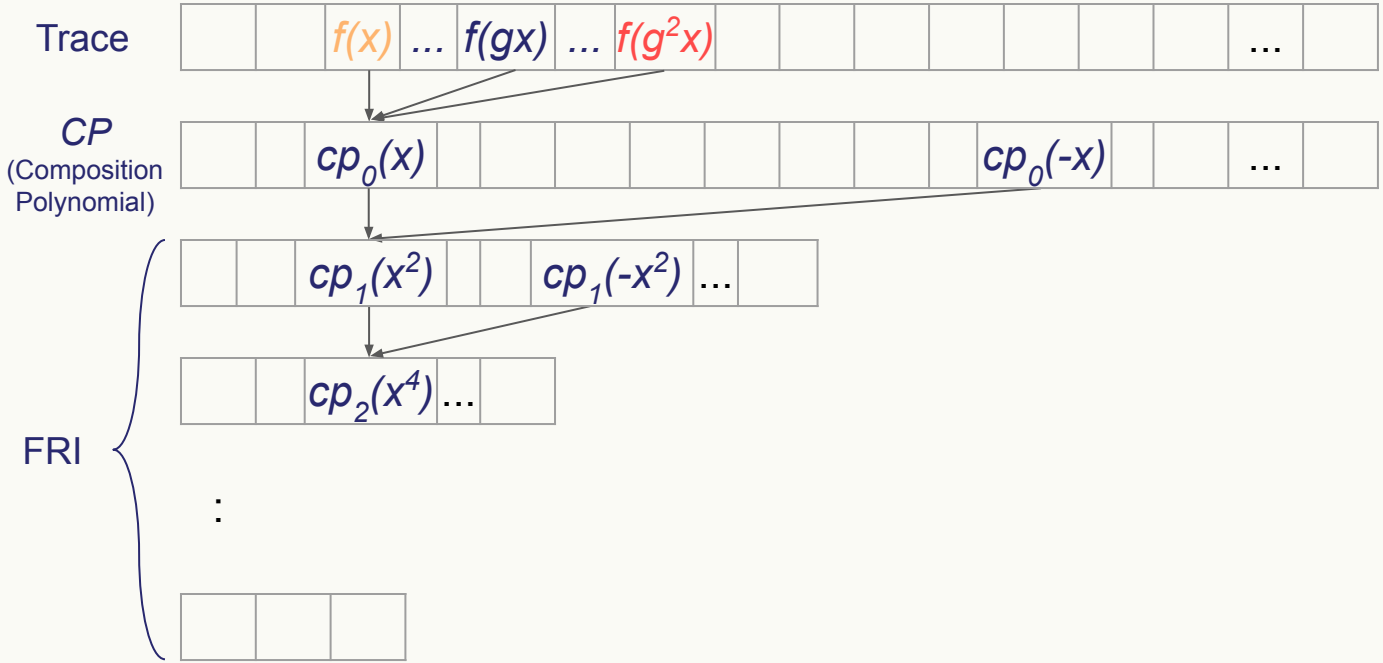
Trace

CP (Composition Polynomial)

FRI



Decommitment Phase (for query x)



Decommitment

$f(x)$ + path
$f(gx)$ + path
$f(g^2x)$ + path
$cp_0(x)$ + path
$cp_0(-x)$ + path

$cp_1(x^2)$ + path
$cp_1(-x^2)$ + path

$cp_2(x^4)$ + path
$cp_2(-x^4)$ + path

:

$cp_{10}(x^{1024})$ + path

The Entire Proof

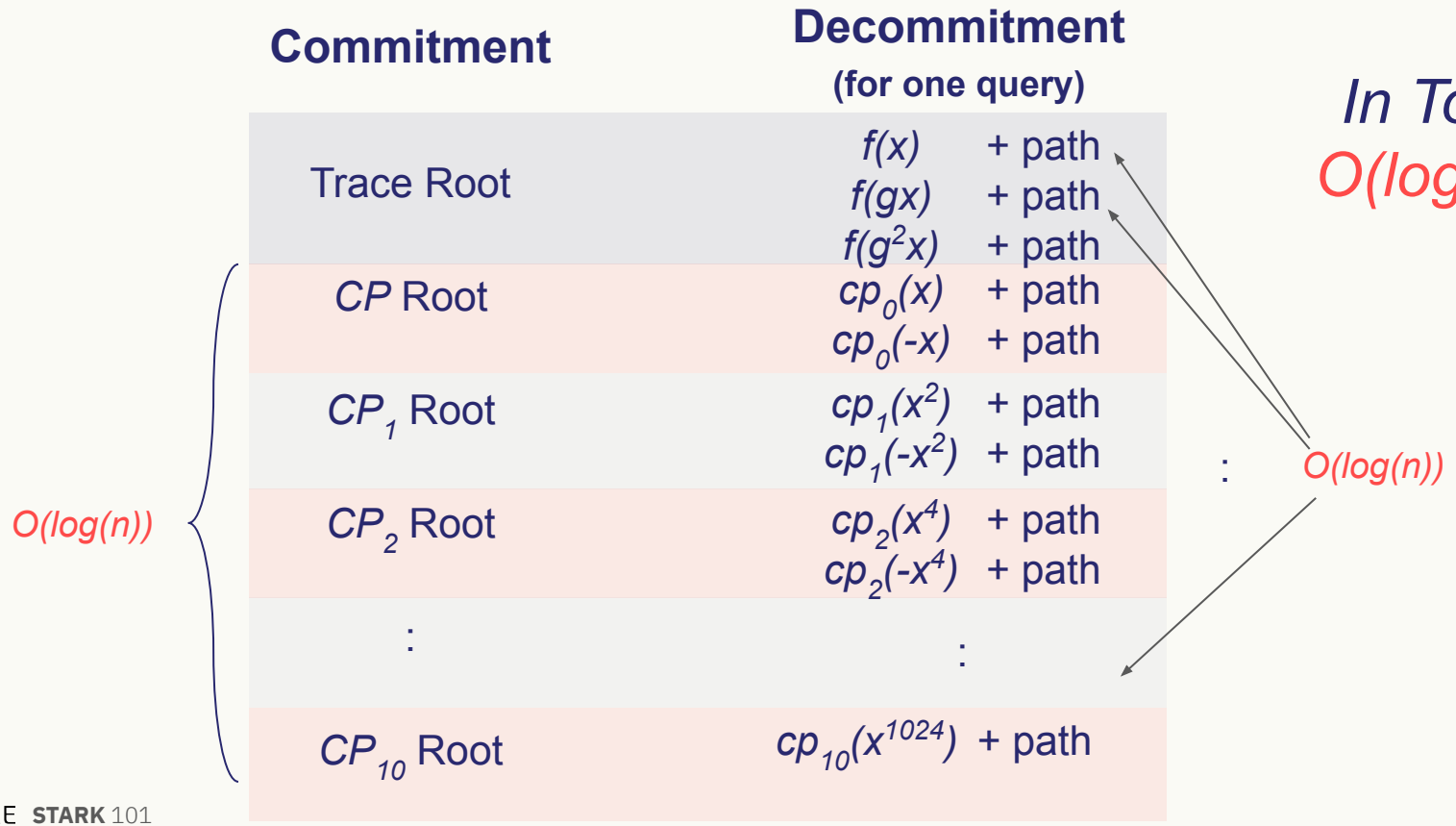
- Commitment
- Decommitment
  - Get q random elements
  - Provide a validation data for each

Proof Length

	Commitment	Decommitment (for one query)
	Trace Root	$f(x)$ + path $f(gx)$ + path $f(g^2x)$ + path
	CP Root	$cp_0(x)$ + path $cp_0(-x)$ + path
	CP_1 Root	$cp_1(x^2)$ + path $cp_1(-x^2)$ + path
$O(log(n))$	CP_2 Root	$cp_2(x^4)$ + path $cp_2(-x^4)$ + path
	:	:
	CP_{10} Root	$cp_{10}(x^{1024})$ + path

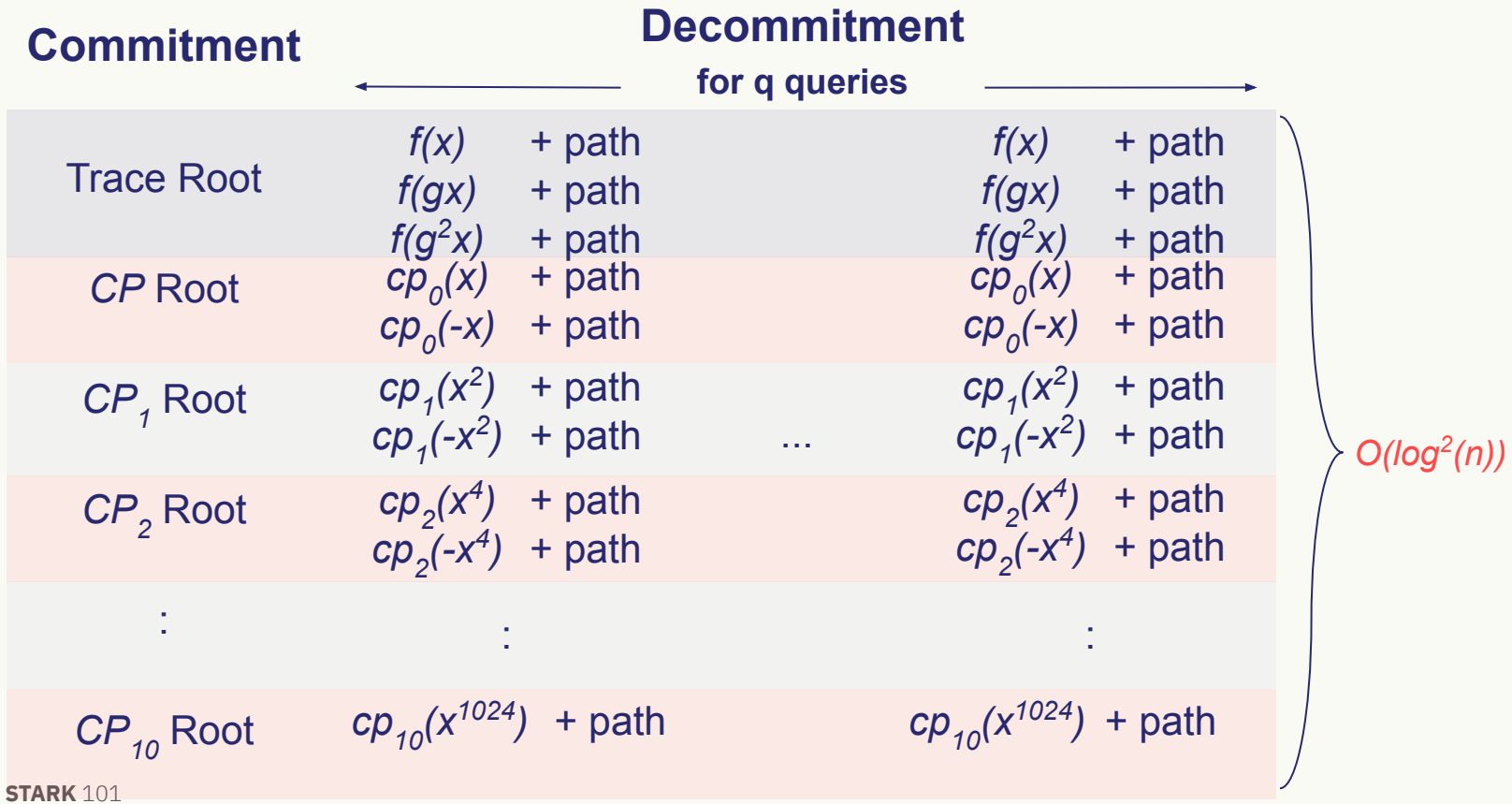
n = trace length (1023)

Proof Length



In Total:
$O(\log^2(n))$

Proof Length



And now - coding (final)

After that -
You will become a STARK expert

Thanks!