STARKWARE STARK 101

Stark 101: Part 3

FRI Commitment

Recap

Goal : prove a statement on FibonacciSq

- Trace in 1023 points
- Create *Trace* polynomial (Lagrange interpolation)
- Evaluate and commit on a larger domain

Recap

- 3 constraints on *f(x)*:

$$f(x) - 1 = 0 \quad \text{, for } x = 1$$

...

- 3 rational functions from the constraints:

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

...

Recap

- **C**omposition **P**olynomial:

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

- Prover commits on CP
- Goal - show that CP is a **polynomial**
- CP is a **polynomial** $\longrightarrow$ All constraints satisfied

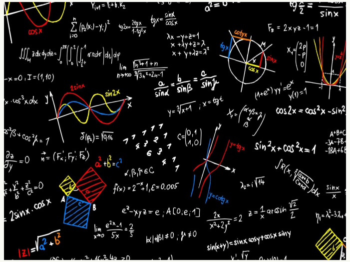
What Will We Do?

Goal:

Prove that CP is a **polynomial**

Instead:

Prove that CP is **close** to a **polynomial** of **low degree**



What is close?

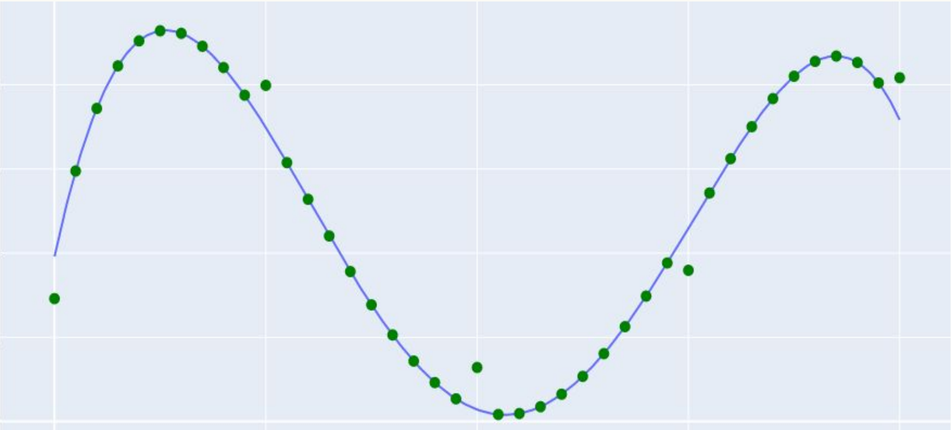
What is low degree?

Proximity to Polynomials

Distance (def):

Distance between a function $\boldsymbol{f}: D \to F$ *to a polynomial* $\boldsymbol{p}$:

$D(f,p)$:= # points $x \in D$ such that $f(x) \neq p(x)$



$D(\boldsymbol{f}, \boldsymbol{p}) = 5$

Proximity to Polynomials

Distance (def):

Distance between a function ***f****: D → F to a polynomial* ***p****:*

$D(f,p)$:= # points $x \in D$ such that $f(x) \neq p(x)$

Proximity

A function $f: D \rightarrow F$ is ***close*** *to a* polynomial p if: $D(f,p)$ is **small**

FRI

Fast Reed-Solomon Interactive Oracle Proofs of Proximity

By Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M.

https://eccc.weizmann.ac.il/report/2017/134/

FRI

Prover convinces verifier:

> **“The commitment is close to a low degree polynomial“**

Without Using FRI

FRI Operator - The Reduction

FRI Operator

Goal:

Prove that a function is close to a polynomial of a bounded degree ***D***

Applying the FRI operator

New Goal:

Prove that a **new** function is close to a **new** polynomial

Half of the domain size

Degree bound ***D/2***

FRI Operator - Example

Before applying FRI operator

- Prove:

A function is close to a polynomial of a bounded degree **1024**

where domain size = **8192**

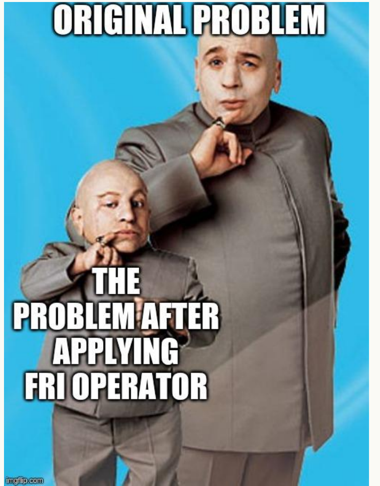
FRI Operator - Example

~~Before~~ After applying FRI operator

- Prove:

A function is close to a polynomial of a bounded degree ~~1024~~ **512**

where domain size = ~~8192~~ **4096**



FRI Overview

FRI - The Protocol

- Receives random β
- Computes the next polynomial
- Commit
- Lastly the prover sends the constant

Do it repeatedly until:

***deg(poly)* < 1**

where

domain size is 8

FRI - Illustration

Showing that *deg(CP)<1024, |D|=8192*

CP(x)

CP Commitment

β_0

$deg(CP_1)<512$, $|D_1| = 4096$

β_1

$deg(CP_2)<256$, $|D_2| = 2048$

⋮

β_9

$\boldsymbol{deg(CP_{10})<1,\ |D_{10}| = 8}$

Deep Into FRI

STARKWARE

FRI Operator - How Does it Work?

- Split to even and odd powers

$$P_0(x) = g(x^2) + xh(x^2)$$

- Get a random β

- Consider the new function:

$$P_1(y) = g(y) + \beta h(y)$$

- Example:

$$P_0(x) = 5x^5+3x^4+7x^3+2x^2+x+3$$

$g(x^2)$ $3x^4$ $2x^2$ 3

$xh(x^2)$ $5x^5$ $7x^3$ x

FRI Operator - How Does it Work?

- Split to even and odd powers

$$P_0(x) = g(x^2) + xh(x^2)$$

- Get a random β

- Consider the new function:

$$P_1(y) = g(y) + \beta h(y)$$

- Example:

$$P_0(x) = 5x^5+3x^4+7x^3+2x^2+x+3$$

$g(y)$ $3y^2$ $2y$ 3

$h(y)$ $5y^2$ $7y$ 1

- $P_1(y) = 3y^2 +2y+3+\beta(5y^2+7y +1)$

$$= (3+5\beta)y^2+(2+7\beta)y+3+\beta$$

FRI - The Protocol - Reminder

- Receives random β
- Computes the next polynomial
- Commit
- Lastly the prover sends the constant

Do it repeatedly until:

***deg(poly)* < 1**

where

domain size is 8

FRI - The Protocol - A Single Step

$$P_0(x) = 5x^{5}+3x^4+7x^3+2x^2+x+3$$

Degree bound = 6

$$\boldsymbol{deg(P_1) \le deg(P_0)/2}$$

Degree bound = 3

- Receives random β
- Computes the next polynomial
- Commit

$$P_1(y) = (3+5\beta)y^{2}+(2+7\beta)y+3+\beta$$

Thank you