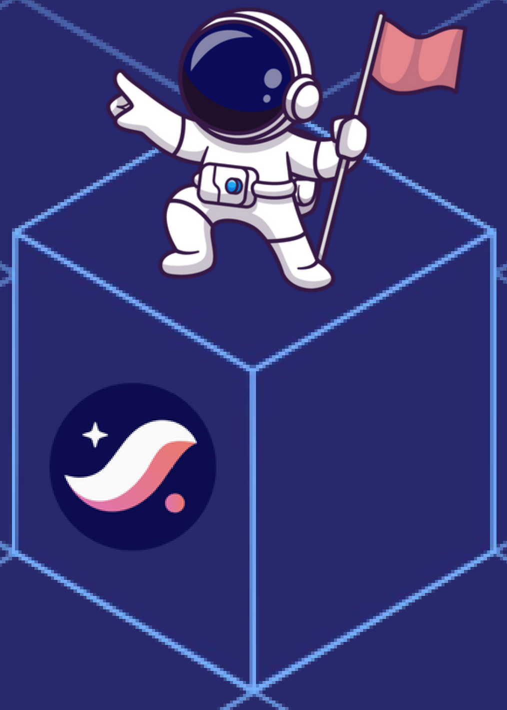
Nadai

Carlos

Sesión 3: Las matemáticas detrás de las STARKs

- 4 de Mayo del 2023

Stark 101: Parte 3



@Nadai02010

https://github.com/Nadai2010

@0xhasher_

https://github.com/cliraa

Recapitulemos

Objetivo: probar una declaración sobre CuadFibonacci

- Traza en 1023 puntos
- Crear polinomio de Traza (Interpolación de Lagrange)
- Evaluar y comprometerse en un dominio más grande

Recapitulemos

- 3 restricciones en *f(x)*:

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

$$\ldots$$

- 3 funciones racionales a partir de las restricciones:

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

$$\ldots$$

Recapitulemos

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

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

- El probador se compromete en CP
- Objetivo - demostrar que CP es un **polinomio**
- CP es un **Polinomio** $\longrightarrow$ Todas las restricciones están satisfechas

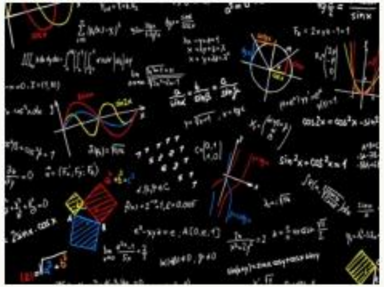
¿Qué haremos?

Objetivo:

Probar que CP es un **polinomio**

En su lugar:

Probar que CP es **cercano** a un **polinomio** de **bajo grado**



¿Qué es cercano?

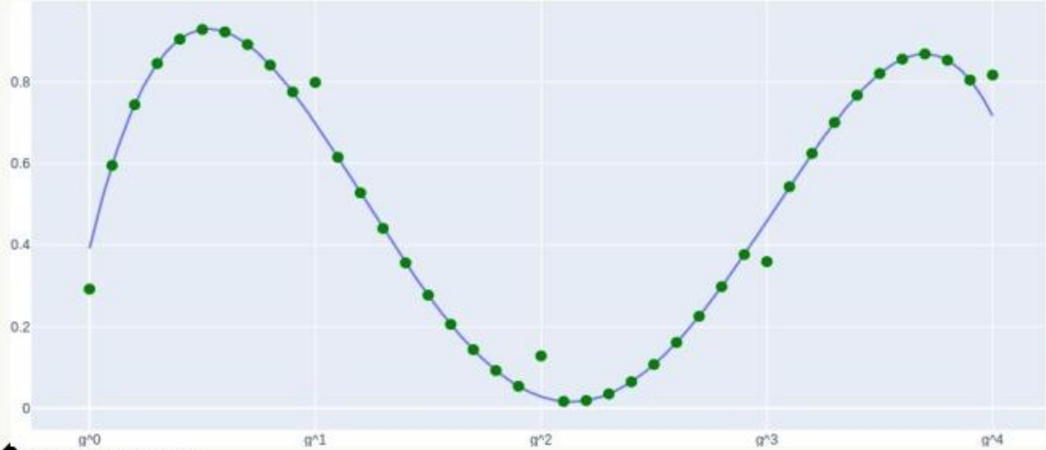
¿Qué es bajo grado?

Proximidad

Distancia (def):

Distancia entre una función $\boldsymbol{f}: D \to F$ a un polinomio $\boldsymbol{p}$:

$D(f,p) :=$ # puntos $x \in D$ tal que $f(x) \neq p(x)$



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

Proximidad

Distancia (def):

Distancia entre una función ***f**: D → F a un polinomio **p**:*

$D(f,p)$:= # puntos $x \in D$ tal que $f(x) \neq p(x)$

Proximidad

Una función $f: D \rightarrow F$ es ***cercana*** a un polinomio p si: $D(f,p)$ es **pequeña**

¿Qué vamos a hacer? - Recordatorio

Objetivo:

Probar que CP es **cercano** a un **polinomio** de **bajo grado**

¿Cómo?

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 - Objetivo:

Permitir que el probador convenza al verificador:

> **“El compromiso es cercano a un polinomio de bajo grado"**

FRI - El Protocolo

- Recibir el número β random
- Aplicar el operador FRI
- Comprometerse
- Por último, el probador envía el resultado

Hacerlo repetidamente

FRI

- Operador FRI - motivación
- Visión General de los pasos de FRI
- Profundizar en el operador FRI

Operador FRI

Operador FRI

Objetivo:

Probar que una función es cercana a un polinomio de un grado < **D**

Aplicando el operador FRI

Nuevo Objetivo:

Probar que una **nueva** función es cercana a un **nuevo** polinomio

La mitad del tamaño del dominio

Grado < **D/2**

Operador FRI - Ejemplo
Antes de aplicar el Operador FRI

- Probar:

Una función es cercana a un polinomio de grado < **1024**

donde el tamaño del dominio = **8192**

Operador FRI - Ejemplo
~~Antes~~ Después de aplicar el Operador FRI

- Probar:

  Una función es cercana a un polinomio de grado < ~~**1024**~~ **512**

  donde el tamaño del dominio = ~~**8192**~~ **4096**

Visión general de los pasos de FRI

Visión general de los pasos de FRI

Demostrando que $gra(CP)<1024,\ |D|=8192$

$CP(x)$ **CP Commitment**

β_0

$gra(CP_1)<512,\ |D_1|= 4096$

β_1

$gra(CP_2)<256,\ |D_2|= 2048$

. . .

β_9

Constante

$\mathbf{gra(CP_{10})<1, |D_{10}|= 8}$

Profundizando en el Operador FRI

STARKWARE

Operador FRI - ¿Cómo funciona?

- Dividir entre pares e impares

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

- Obtener un número β random

- Considera la nueva función:

$$\boldsymbol{P_1(y) = g(y) + \beta h(y)}$$

- Ejemplo:

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

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

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

Operador FRI - ¿Cómo funciona?

- Dividir entre pares e impares

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

- Obtener un número β random

- Considera la nueva función:

$$P_1(y) = \mathbf{g(y)} + \beta h(y)$$

- Ejemplo:

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

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

$g(\mathbf{y})$ $3\mathbf{y}^2$ $2\mathbf{y}$ 3

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

Operador FRI - ¿Cómo funciona?

- Dividir entre pares e impares

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

- Obtener un número β random

- Considera la nueva función:

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

- Ejemplo:

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

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

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

Operador FRI - ¿Cómo funciona?

- Dividir entre pares e impares

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

- Obtener un número β random

- Considera la nueva función:

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

- Ejemplo:

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

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

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

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

Operador FRI - ¿Cómo funciona?

- Dividir entre pares e impares

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

- Obtener un número β random

- Considera la nueva función:

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

- Ejemplo:

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

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

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

Operador FRI - ¿Cómo funciona?

- Dividir entre pares e impares

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

- Obtener un número β random

- Considera la nueva función:

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

- Ejemplo:

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

$g(y)$: $3y^2$ $2y$ 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 - El Protocolo - Recordatorio

- Recibir el número β random
- Aplicar el operador FRI
- Comprometerse
- Por último, el probador envía el resultado

Hacerlo repetidamente

gra(poli) < 1

donde el tamaño del dominio es 8

constante

FRI - El Protocolo - Un solo paso

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

Grado límite = 6

$$\boldsymbol{gra(P_1) \leq gra(P_0)/2}$$

Grado límite = 3

- Recibir el número β
- Aplicar operador FRI
- Comprometerse

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

Gracias