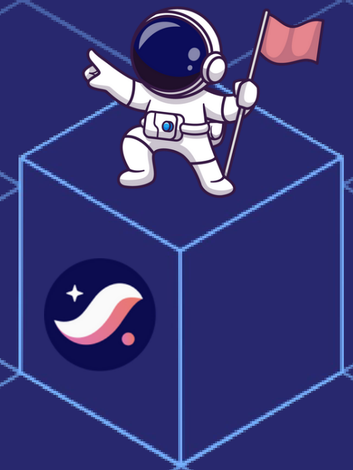
STARKWARE

Nadai Carlos

Sesión 3: Las matemáticas detrás de las STARKs

- 4 de Mayo del 2023

Stark 101: Parte 1



@Nadai02010

https://github.com/Nadai2010

@0xhasher_

https://github.com/cliraa

CuadFibonacci

(Cuadrados de Fibonacci)

CuadFibonacci (Cuadrados de Fibonacci)

CuadFibonacci: $a_{n+2} = a_{n+1}^2 + a_n^2$

- Representada como: $a_0, a_1, a_2, a_3, \ldots$
- Determinada por los primeros dos elementos
- Ejemplo:
  - 1, 3, 10, 109, 11981, 143556242,...

Pequeño problema

$$a_{10} = 1058538448149133154544343598019533016808522710856082409891927825821583978969754411443713008055652428916885458657978238751812992228283226160560814552379774771482746584257000514878526588336710877240208661850336931934256166336593387070293738452872952783090264176685$$

CuadFibonacci Mod Primo

CuadFibonacci mod primo: $a_{n+2} = a_{n+1}^2 + a_n^2 \bmod primo$

Ejemplo:

- 1, 3, 10, 109, 11981, 143556242,...

mod 7:

- 1, 3, 3, 4, 4, 4, ...

CuadFibonacci Mod Primo

CuadFibonacci mod primo: $a_{n+2} = a_{n+1}^2 + a_n^2 \bmod primo$

- Ejemplo - mod 7:
  - 1, 3, 3, 4, 4, 4, ...

Usaremos el *primo* = $3 \cdot 2^{30} + 1 = 3221225473$

Finite field *F*

Declaración

Declaración a probar

Existe un número x tal que:

Para CuadFibonacci mod 3221225473 con

- $a_0 = 1$
- $a_1 = x$

Tenemos que $a_{1022} = 2338775057$

X = 3141592

Protocolo STARK

Protocolo STARK - Parte I

- LDE - Low Degree Extension (Extensión de Bajo Grado)
- Commitment (Compromiso)

Low Degree Extension (LDE)

Extensión de Bajo Grado

LDE en 3 Pasos

1. Generar input
2. Interpolar
3. Extender

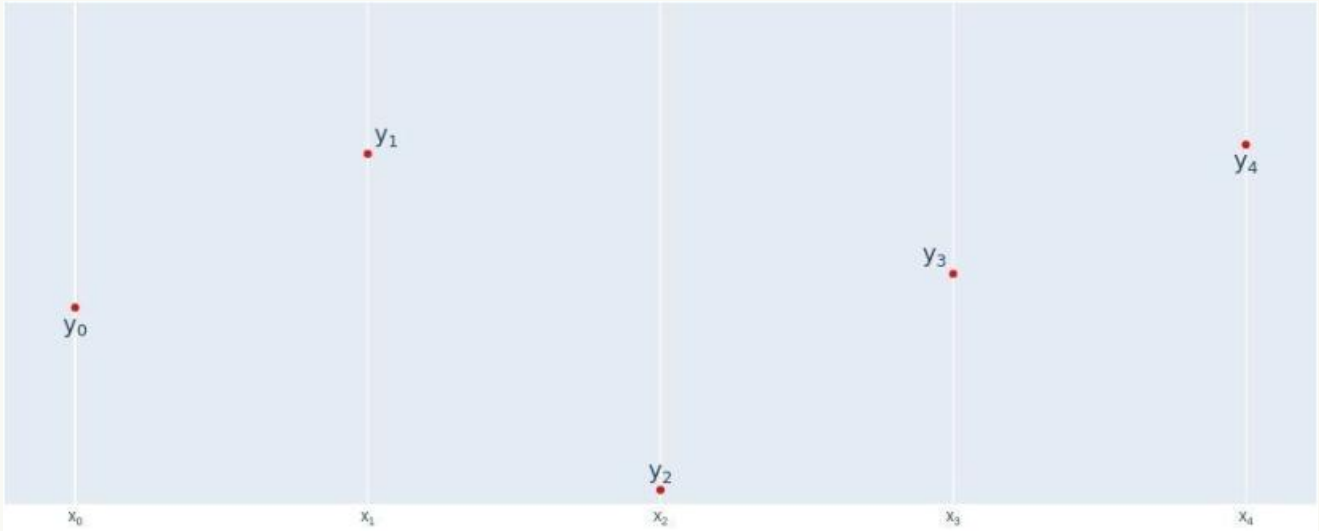
LDE - General

LDE Paso 1 - Generar Input

Input: $y_0, y_1, y_2, y_3, y_4, \ldots$

Escoger: $x_0, x_1, x_2, x_3, x_4, \ldots$

x	*y*
x_0	y_0
x_1	y_1
x_2	y_2
x_3	y_3
x_4	y_4

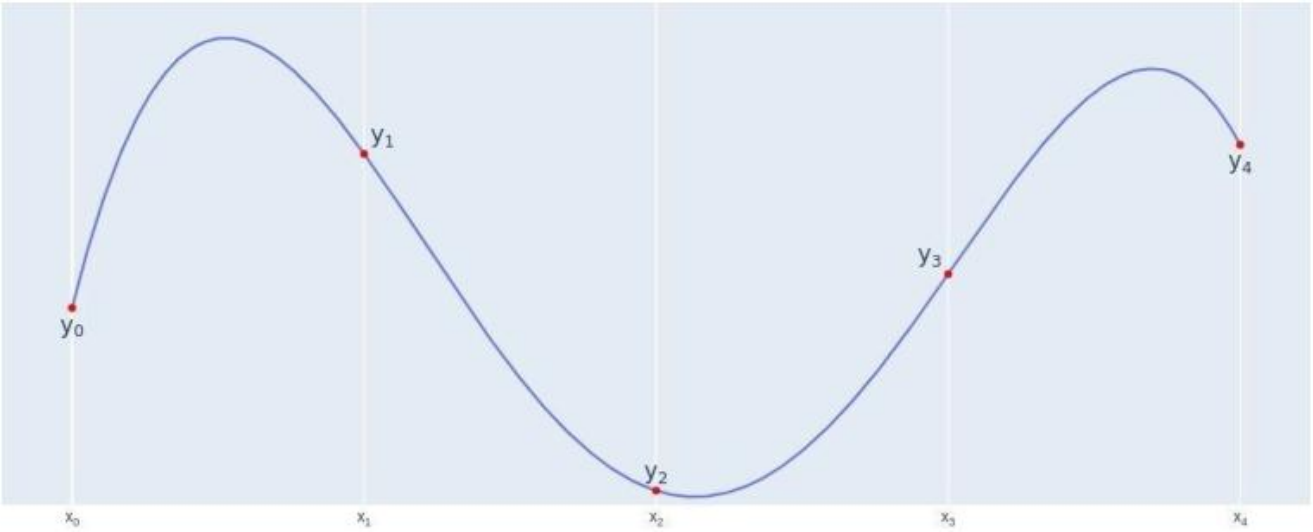


LDE Paso 2 - Interpolación Polinómica

Interpolar un polinomio *f*:

Para cada i : $f(x_i)=y_i$

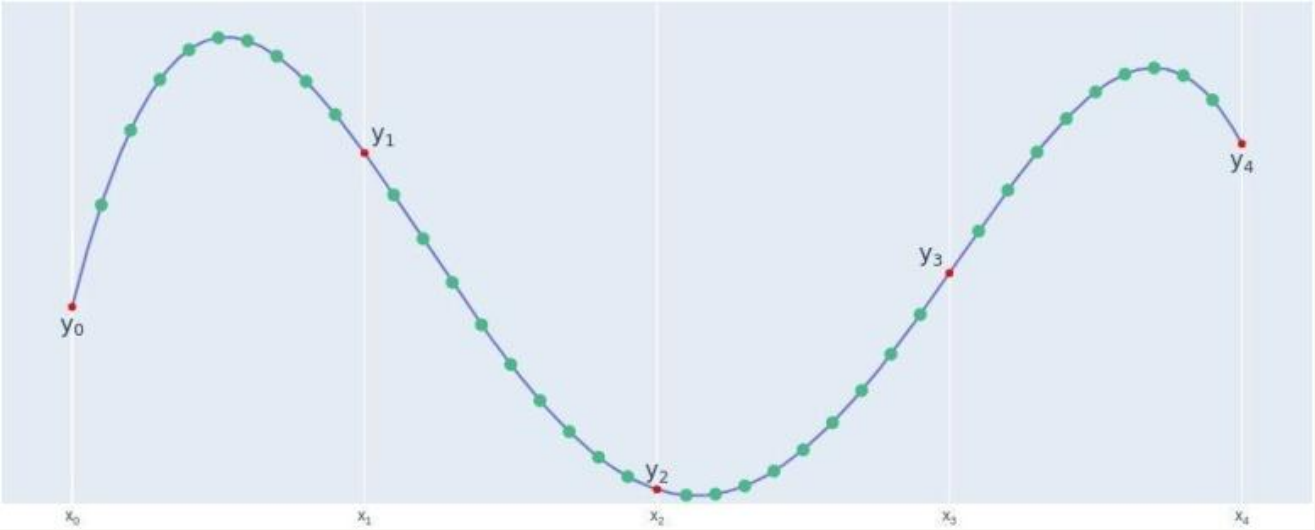
x	*f(x)*
x_0	y_0
x_1	y_1
x_2	y_2
x_3	y_3
x_4	y_4



LDE Paso 3 - Extender

- Elegir un dominio de evaluación más grande $\{x`_j\}$
- Output: $\{f(x`_j)\}$

$x`$	$f(x`)$
$x`_0$	$f(x`_0)$
$x`_1$	$f(x`_1)$
$x`_2$	$f(x`_2)$
$x`_3$	$f(x`_3)$
...	...



LDE en STARK

LDE para STARK Paso 1 - Generar Input

Input: $a_0, a_1, a_2, \ldots, a_{1022}$

La **Traza**

Escogemos: $1, g, g^2, g^3, \ldots, g^{1022}$

g - elemento de F

LDE para STARK Paso 1 - Generar Input

Input: $a_0, a_1, a_2, \ldots, a_{1022}$

Escogemos: $1, g, g^2, g^3, \ldots, g^{1022}$

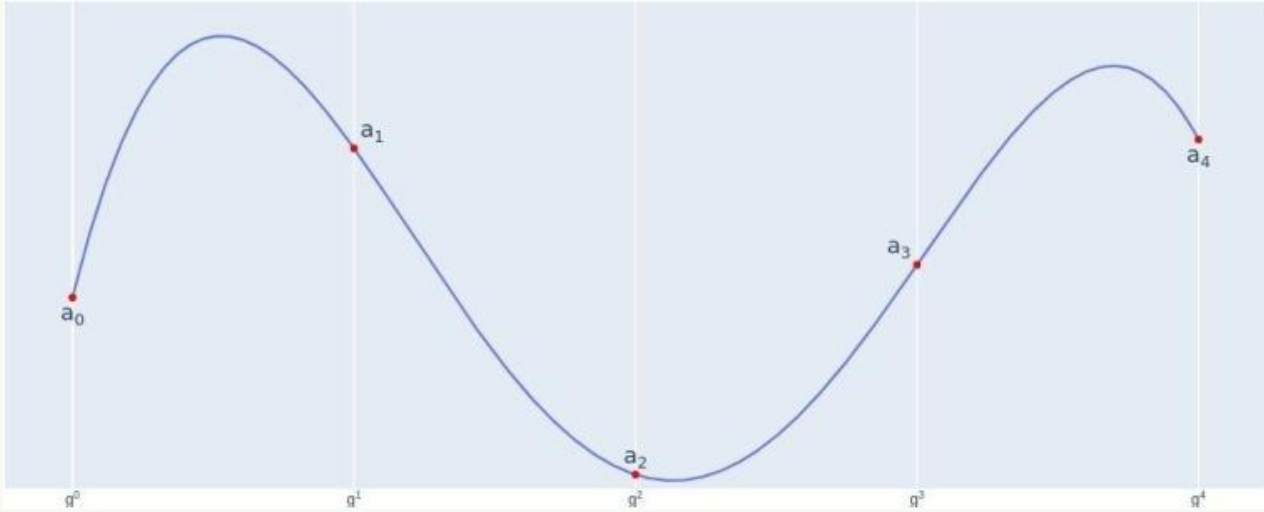
x	$f(x)$
g^0	a_0
g^1	a_1
g^2	a_2
...	...
g^{1022}	a_{1022}

LDE para STARK Paso 2 - Interpolar

Interpolar un polinomio *f*:

$$para\ cada\ i : f(g^i) = a_i$$

x	*f(x)*
g^0	a_0
g^1	a_1
g^2	a_2
...	...
g^{1022}	a_{1022}



LDE para STARK Paso 3 - Extender

- Elegir un dominio de evaluación más grande (8k)
- $\{ x_i` \} = w, w \cdot h, w \cdot h^2, \ldots, w \cdot h^{8191}$

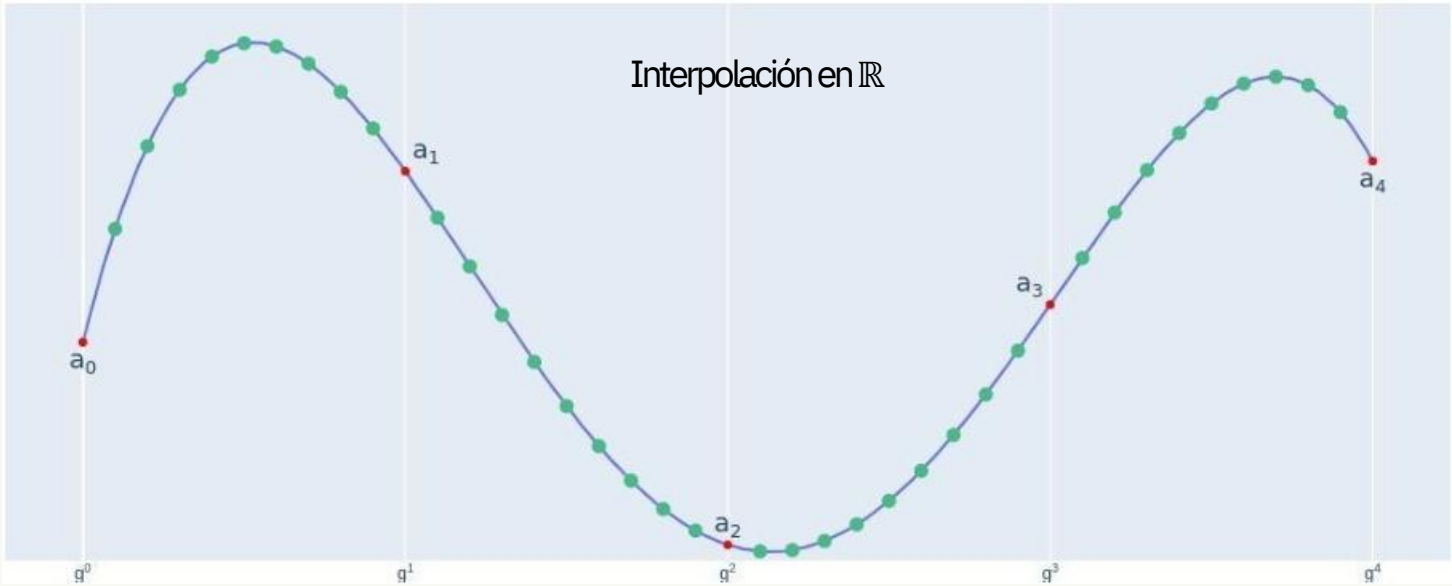
w, h - elementos de F

- Resultado: $f(w), f(w \cdot h), f(w \cdot h^2), \ldots$

Reed-Solomon codeword

LDE para STARK Paso 3 - Extender

x	$f(x)$
$w \cdot h^0$	$f(w \cdot h^0)$
$w \cdot h^1$	$f(w \cdot h^1)$
$w \cdot h^2$	$f(w \cdot h^2)$
...	...
$w \cdot h^{8191}$	$f(w \cdot h^{8191})$

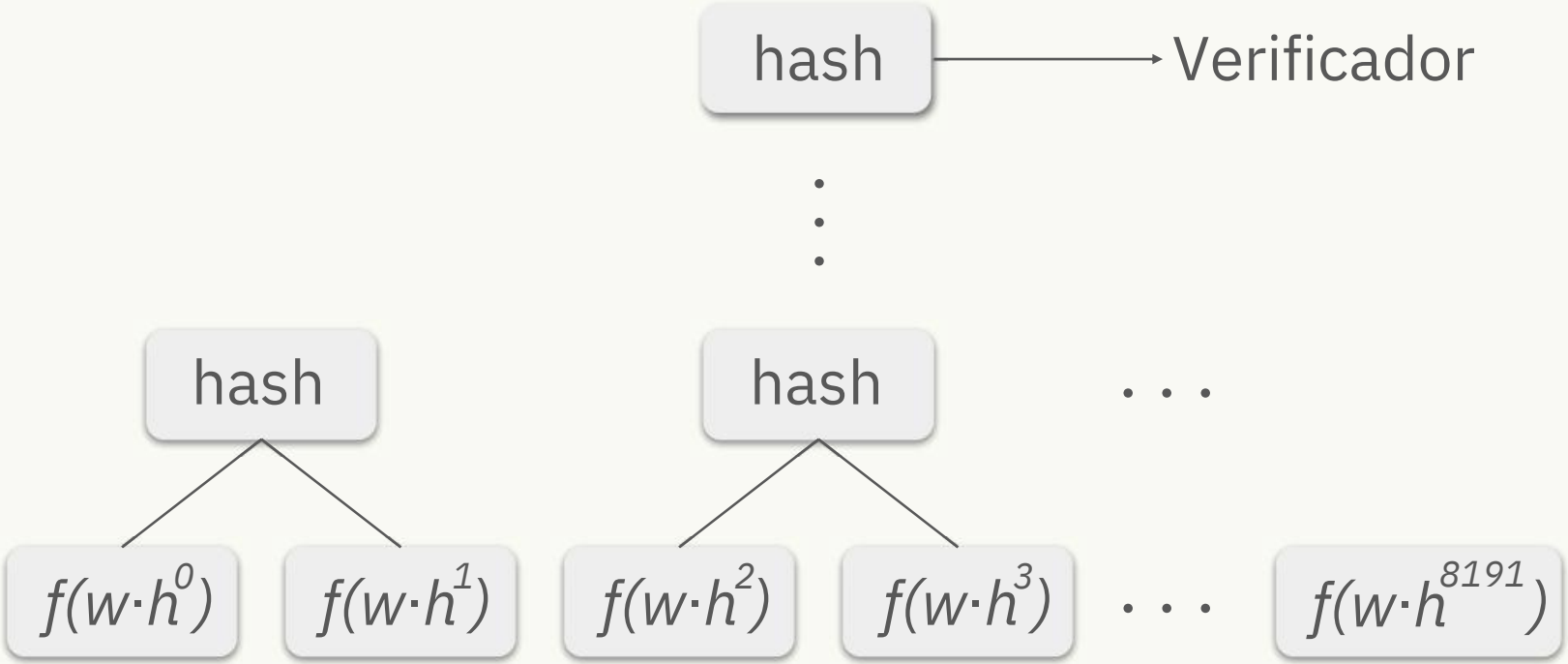


Commitment

(Compromiso)

Compromiso sobre LDE

Árbol de Merkle



Resumen

- Declaración
  - Existe un número x tal que si iniciamos una secuencia CuadFibonacci mod 3221225473, el elemento a_{1022}= 2338775057
- Protocolo STARK - parte I:
  - LDE - Low Degree Extension (Extensión de Bajo Grado)
  - Commitment (Compromiso) - Árbol de Merkle

¿Qué sigue?

Parte 2 - restricciones polinómicas

Pero primero - el código...

1) Trace, LDE

2) Commit LDE trace

Gracias