STARKWARE STARK 101

Stark 101: Part 1

Statement, LDE and Commitment

Statement

FibonacciSq (Fibonacci Square)

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

- Represented as: $a_0, a_1, a_2, a_3, \ldots$
- Determined by first two elements
- Example:
  - 1, 3, 10, 109, 11981, 143556242,...

Tiny Problem

$a_6 =$

$$810574682645736646170815895946896861049268181$$

$$679227161342419752207920339408210879818119924$$

$$662826503344193502128621935238534388755008182$$

$$003074570944767205108835898326040168629340775$$

$$573476061591508763885136668 5$$

FibonacciSq Mod Prime

FibonacciSq mod prime: $a_{n+2} = a_{n+1}^2 + a_n^2 \mod prime$

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

We use $prime = 3 \cdot 2^{30} + 1 = 322122547$

Finite field F

Statement to Prove

There is a number x such that:

For the FibonacciSq mod 3221225473 with

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

we have $a_{1022} = 2338775057$

STARK Protocol

STARK Protocol - Part I

- LDE - Low Degree Extension
- Commitment

Low Degree Extension (LDE)

LDE 3 Steps

1. Generate input
2. Interpolate
3. Extend

LDE Step 1 - Generate Input

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

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

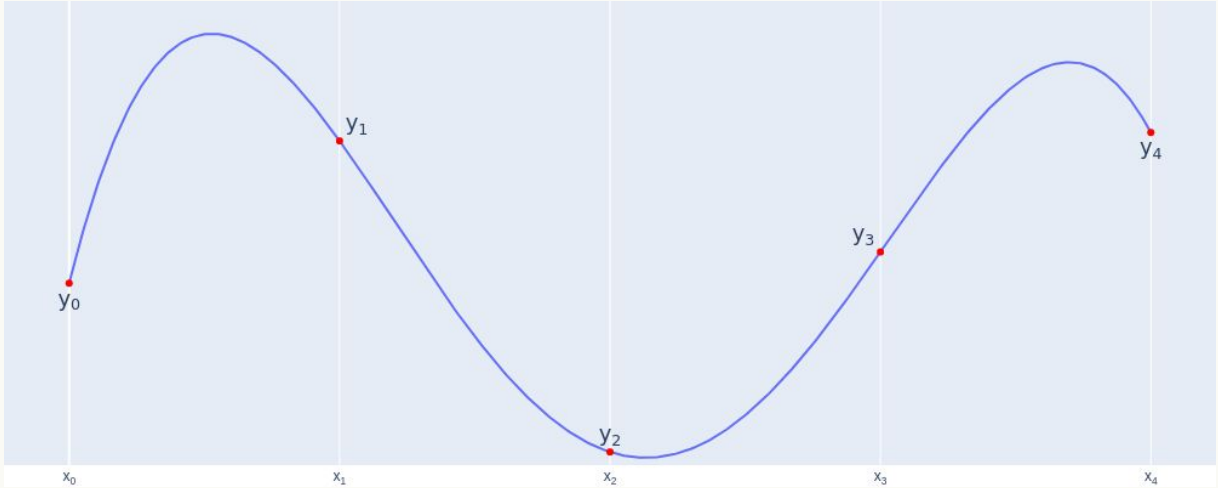
x	*y*
x_0	y_0
x_1	y_1
x_2	y_2
x_3	y_3
x_4	y_4

LDE Step 2 - Interpolate Poly

Interpolate a polynomial *f*:

For each i : $f(x_i)=y_i$

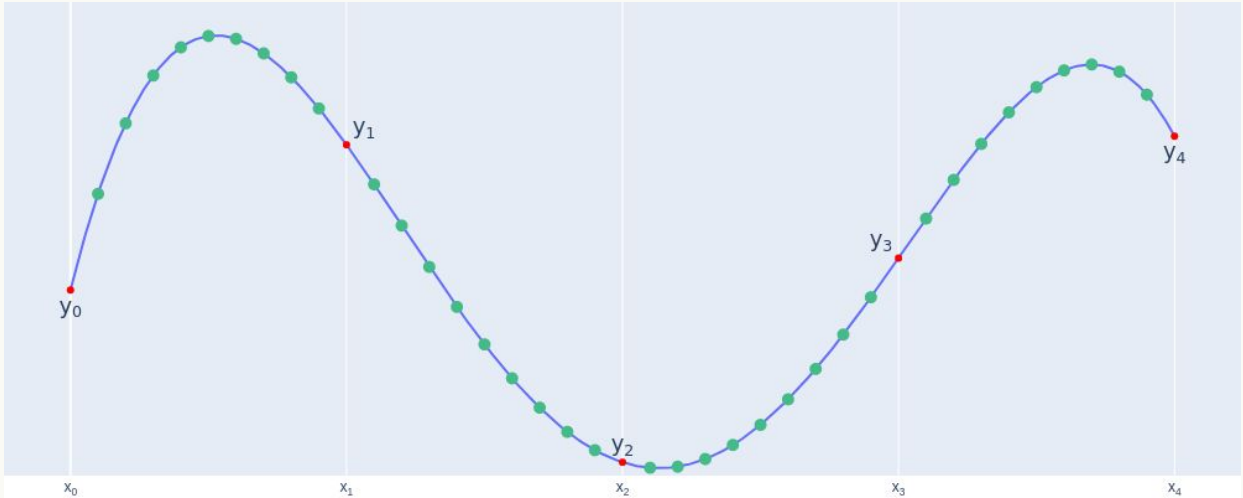
x	*f(x)*
x_0	y_0
x_1	y_1
x_2	y_2
x_3	y_3
x_4	y_4



LDE Step 3 - Extend

- Pick a larger evaluation domain $\{x_j`\}$
- 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 in STARK

LDE for STARK Step 1 - Generate Input

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

The **Trace**

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

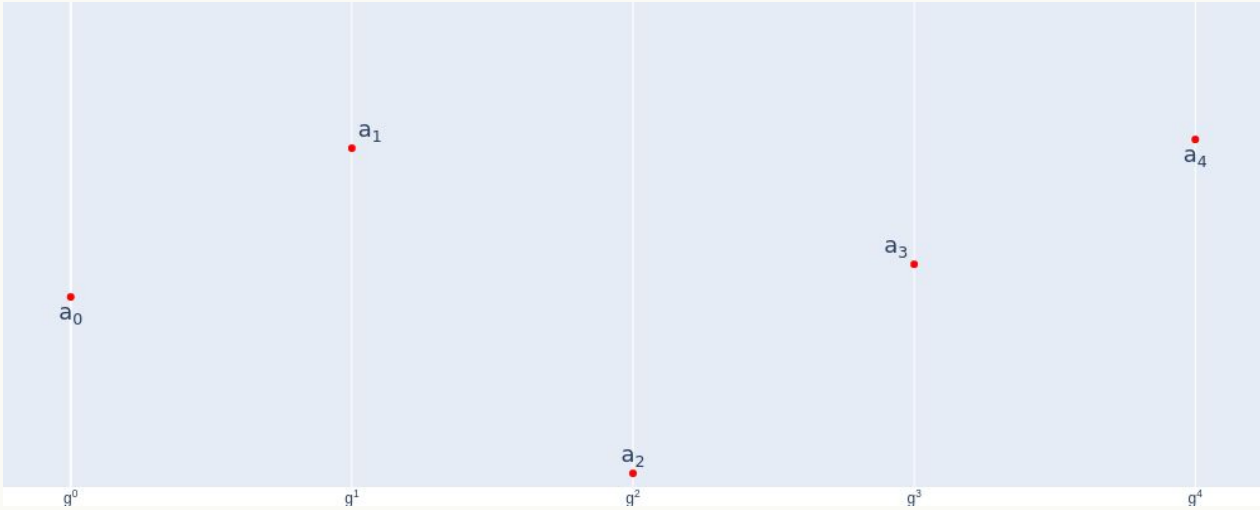
g - element from F

LDE for STARK Step 1 - Generate Input

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

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

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

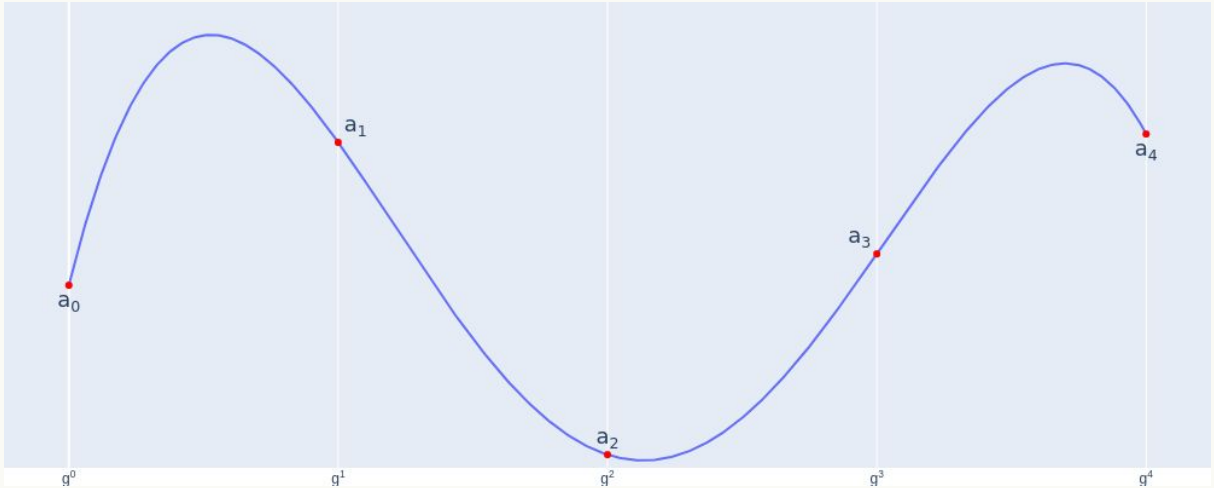


LDE for STARK Step 2 - Interpolate Poly

Interpolate a polynomial f:

$$for\ each\ i : f(g^i)=a_i$$

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



LDE for STARK Step 3 - Extend

- Pick a larger evaluation domain (8k)
- $\{x_i`\} = w, w \cdot h, w \cdot h^2, \ldots, w \cdot h^{8191}$

LDE for STARK Step 3 - Extend

- Pick a larger evaluation domain (8k)
- $\{x_i`\} = w, w \cdot h, w \cdot h^2, \ldots, w \cdot h^{8191}$

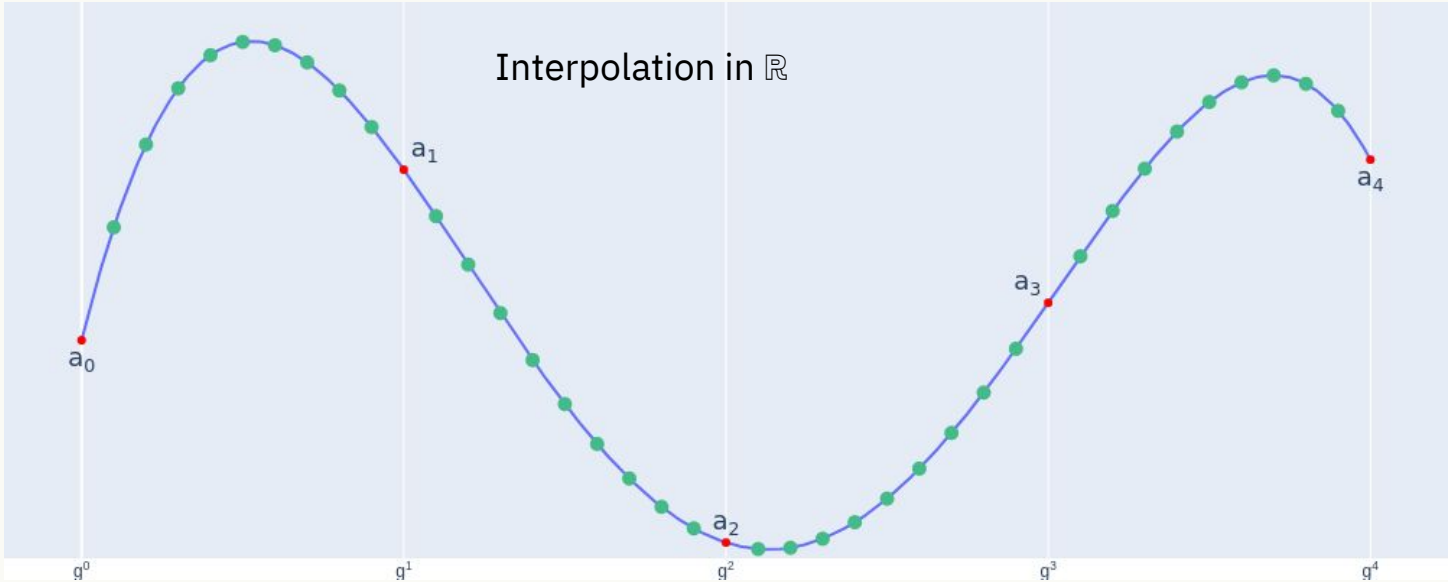
w, h - elements from *F*

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

Reed-Solomon codeword

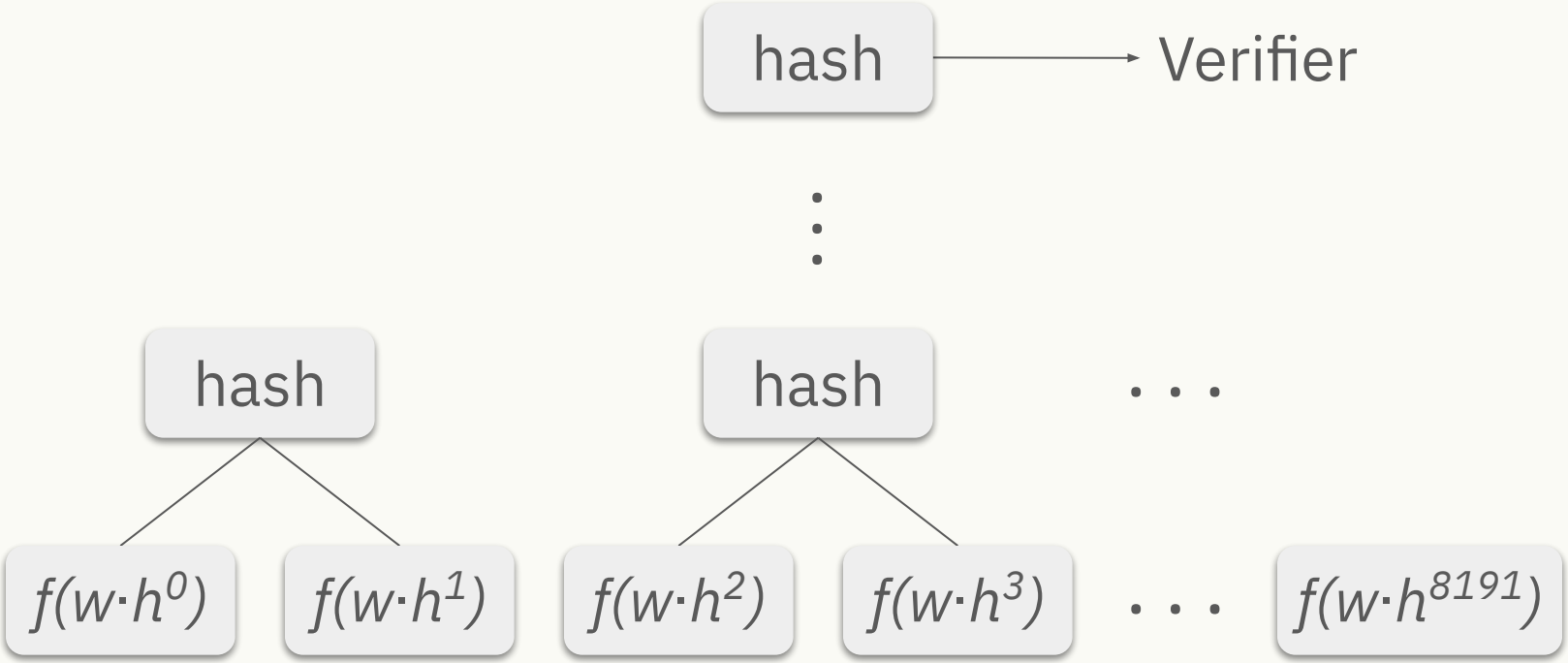
LDE for STARK Step 3 - Extend

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

Commit on LDE



Summary

- Statement
  - We know x s.t. a_{1022}= ... in FibonacciSq mod prime
- STARK protocol - part I:
  - LDE - Low Degree Extension
  - Commitment - Merkle Tree
- Hands on: http://rebrand.ly/STARK101

Thank you