



Stark 101: Part 2

Polynomial Constraints

What Do We Want to Prove?

There is a number x such that:

$$a_0 = 1$$

$$a_1 = x$$

$$a_{1022} = 2338775057$$

For $\{a_n\}$ FibonacciSq: $a_{n+2} = a_{n+1}^2 + a_n^2$, for any n

We will use part I:

Trace - α

Generator of G - g

Trace Polynomial - $f(x)$

Constraints on $\{a_n\}$

We need:

$$a_0 = 1$$

$$a_{1022} = 2338775057$$

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

Where are We Heading?

Constraints on $\{a_n\}$:

$$a_0 = 1$$

$$a_{1022} = 2338775057$$

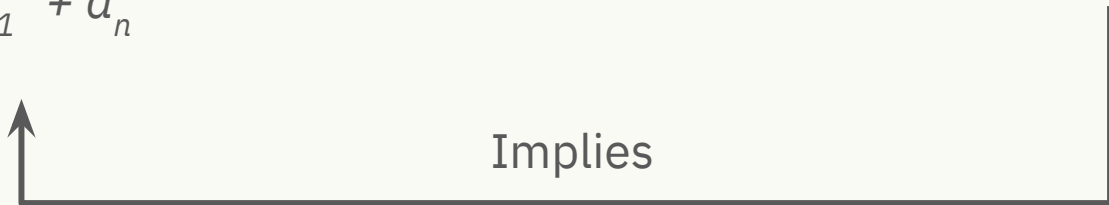
$$a_{n+2} = a_{n+1}^2 + a_n^2$$

Reductions



Another statement

Implies



Where are We Heading?

Constraints on $\{a_n\}$:

$$a_0 = 1$$

$$a_{1022} = 2338775057$$

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

Reductions



Exists a polynomial $f(x)$

such that:

3 rational functions

$p_0(x)$, $p_1(x)$, $p_2(x)$ are **polynomials**

Where are We Heading?

Constraints on $\{a_n\}$:

$$a_0 = 1$$

$$a_{1022} = 2338775057$$

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

Reductions



Exists a polynomial $f(x)$

such that:

3 **rational functions**

$p_0(x), p_1(x), p_2(x)$ are **polynomials**

$$\frac{a(x)}{b(x)}$$

Trace
polynomial

Step I - From $\{a_n\}$ to $f(x)$

Trace
polynomial

3 constraints on $\{a_n\}$ — — — — — \blacktriangleright 3 constraints on $f(x)$

$$a_0 = 1 \quad \text{--- -- -- -- --} \blacktriangleright \quad f(x) = 1, \text{ for } x = g^0$$

$$a_{1022} = 2338775057 \quad \text{--- -- -- -- --} \blacktriangleright \quad f(x) = 2338775057, \text{ for } x = g^{1022}$$

$$a_{n+2} = a_{n+1}^2 + a_n^2 \quad \text{--- -- -- -- --} \blacktriangleright \quad f(g^2x) = f(gx)^2 + f(x)^2,$$

for $x = g^i, 0 \leq i \leq 1020$

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

Third $f(x)$ Constraint

$$a_{n+2} = a_{n+1}^2 + a_n^2 \quad \text{--- -- -- --} \blacktriangleright \quad f(g^2x) = f(gx)^2 + f(x)^2,$$

for $x = g^i$, $0 \leq i \leq 1020$

Example: for $x = g^5$:

$$\underbrace{f(g^2 \cdot g^5)}_{g^7} = \underbrace{f(g \cdot g^5)^2}_{g^6} + \underbrace{f(g^5)^2}_{g^5}$$

x	$f(x)$
g^0	a_0
g^1	a_1
g^2	a_2
...	...
g^5	a_5
g^6	a_6
g^7	a_7
...	...
g^{1022}	a_{1022}

Step I - From $\{a_n\}$ to $f(x)$

3 constraints on $\{a_n\}$ — — — — — \blacktriangleright 3 constraints on $f(x)$

$$a_0 = 1 \quad \text{--- -- -- -- --} \blacktriangleright f(x) = 1, \text{ for } x = g^0$$

$$a_{1022} = 2338775057 \quad \text{--- -- -- -- --} \blacktriangleright f(x) = 2338775057, \text{ for } x = g^{1022}$$

$$a_{n+2} = a_{n+1}^2 + a_n^2 \quad \text{--- -- -- -- --} \blacktriangleright f(g^2x) = f(gx)^2 + f(x)^2,$$

for $x = g^i, 0 \leq i \leq 1020$

Step I - From $\{a_n\}$ to $f(x)$

3 constraints on $\{a_n\}$ $--- \blacktriangleright$ 3 constraints on $f(x)$

$a_0 = 1$ $--- \blacktriangleright$ $f(x) = 1$, for $x = g^0$

$a_{1022} = 2338775057$ $--- \blacktriangleright$ $f(x) = 2338775057$, for $x = g^{1022}$

$a_{n+2} = a_{n+1}^2 + a_n^2$ $--- \blacktriangleright$ $f(g^2x) = f(gx)^2 + f(x)^2$,

for $x = g^i$, $0 \leq i \leq 1020$

If $f(x)$ satisfies constraints \longrightarrow Original statement is true

Step II - From Constraints to Roots

$$f(x) - 1 = 0, \text{ for } x = g^0 \text{ --- } \blacktriangleright \text{ root: } g^0$$

$$f(x) - 2338775057 = 0, \text{ for } x = g^{1022} \text{ --- } \blacktriangleright \text{ root: } g^{1022}$$

$$f(g^2x) - f(gx)^2 - f(x)^2 = 0, \text{ for } x = g^i, 0 \leq i \leq 1020 \text{ --- } \blacktriangleright \text{ roots: } \{g^i \mid 0 \leq i \leq 1020\}$$

Step II - From Constraints to Roots

$f(x) - 1 = 0$, for $x = g^0$ — — — — \blacktriangleright root: g^0

$f(x) - 2338775057 = 0$, for $x = g^{1022}$ — — — — \blacktriangleright root: g^{1022}

$f(g^2x) - f(gx)^2 - f(x)^2 = 0$, for $x = g^i$, $0 \leq i \leq 1020$ — — — — \blacktriangleright roots: $\{g^i \mid 0 \leq i \leq 1020\}$

g^0 is a root of $f(x) - 1$

g^{1022} is a root of $f(x) - 2338775057$

$\{g^i \mid 0 \leq i \leq 1020\}$ are roots of $f(g^2x) - f(gx)^2 - f(x)^2$

Original
statement is
true

Step III - From Roots to Rational Functions

Thm: z is a root of $p(x) \Leftrightarrow (x - z)$ divides $p(x)$

Def: $(x - z)$ divides $p(x)$ if $p(x) / (x - z)$ is a polynomial

Polynomial

$$\frac{x^2 - 3x + 2}{x - 2} = \frac{(x - 2)(x - 1)}{x - 2} = x - 1$$

2 is a root

Not polynomial

$$\frac{x^2 - 7x + 6}{x - 2} = \frac{(x - 1)(x - 6)}{x - 2}$$

2 is NOT a root

Step III - From Roots to Rational Functions

Thm: z is a root of $p(x) \Leftrightarrow (x - z)$ divides $p(x)$

Def: $(x - z)$ divides $p(x)$ if $p(x) / (x - z)$ is a polynomial

g^0 is a root of $f(x) - 1 \dashrightarrow \frac{f(x) - 1}{x - g^0}$ is a polynomial

g^{1022} is a root of $f(x) - 2338775057 \dashrightarrow \frac{f(x) - 2338775057}{x - g^{1022}}$
is a polynomial

Step III - From Roots to Rational Functions

$\{g^i \mid 0 \leq i \leq 1020\}$ are roots of $f(g^2x) - f(gx)^2 - f(x)^2$ --- ►

$$\frac{f(g^2x) - f(gx)^2 - f(x)^2}{\prod_{i=0}^{1020} (x - g^i)}$$

is a polynomial

Not Efficient

Step III - From Roots to Rational Functions

$\{g^i \mid 0 \leq i \leq 1020\}$ are roots of $f(g^2x) - f(gx)^2 - f(x)^2$ --- ►

$$\frac{f(g^2x) - f(gx)^2 - f(x)^2}{\prod_{i=0}^{1020} (x - g^i)}$$

is a polynomial

$$\prod_{i=0}^{1023} (x - g^i) = x^{1024} - 1 \quad \text{fix:}$$

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

3 Rational Functions

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

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

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

3 Rational Functions

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

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

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

If $p_0(x)$, $p_1(x)$, $p_2(x)$ are polynomials \longrightarrow Original statement is true!

Where are We Heading?

Constraints on $\{a_n\}$:

$$a_0 = 1$$

$$a_{1022} = 2338775057$$

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

Reductions



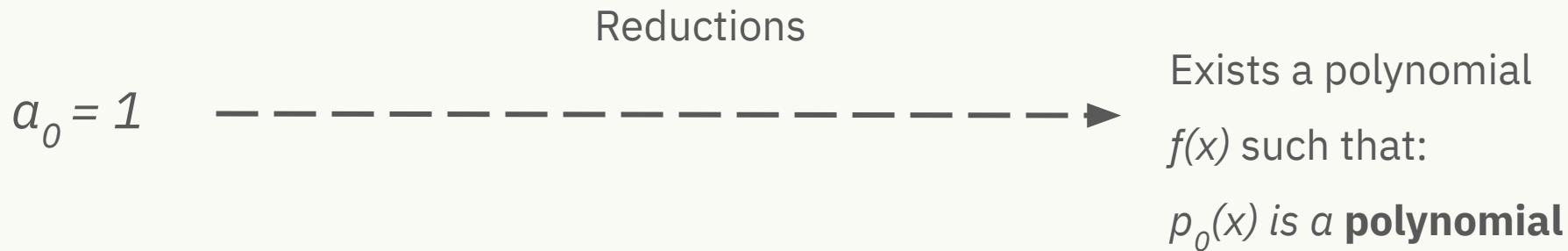
Exists a polynomial $f(x)$

such that:

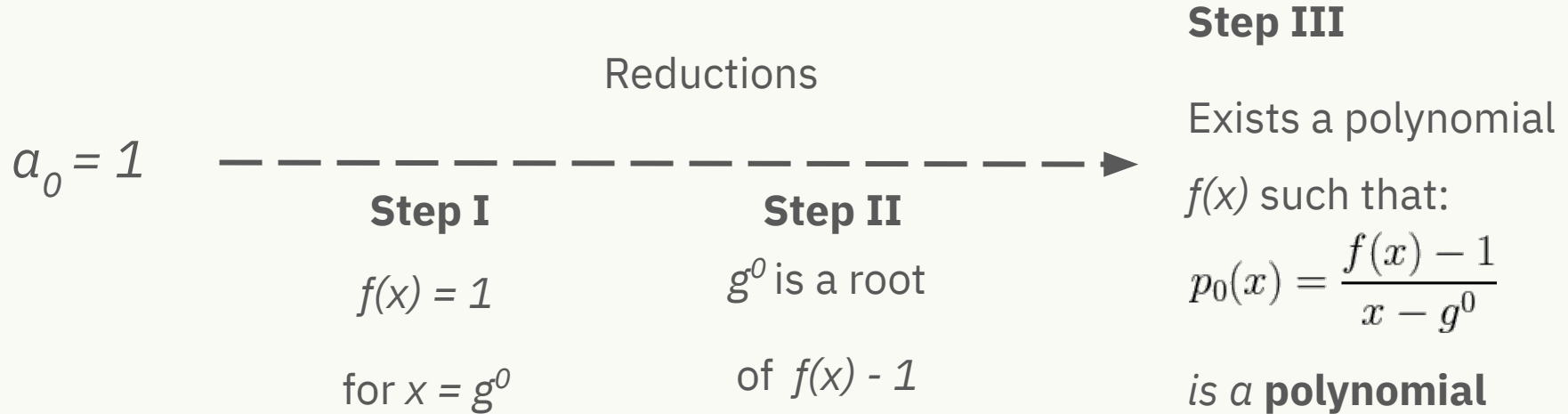
3 rational functions

$p_0(x)$, $p_1(x)$, $p_2(x)$ are **polynomials**

Reduction Overview - First Constraint



Reduction Overview - First Constraint



3 Rational Functions

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

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

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

If $p_0(x)$, $p_1(x)$, $p_2(x)$ are polynomials \longrightarrow Original statement is true!

Combining $p_i(x)$'s

Random linear combination:

Composition
Polynomial

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

With high probability:

CP is a polynomial \Leftrightarrow all p_i 's are polynomials

Committing on CP with Merkle Tree

What's Next?

Part 3 - how to prove that CP is a polynomial?

But first - coding.....

1) $p_0(x), p_1(x), p_2(x)$

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

3) Commit on CP

Thank you