PETS 25: SNARKs

Florian Tramèr

SNARGS

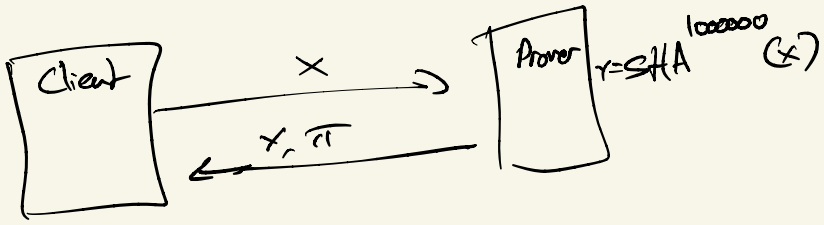
"succinct" "non interactive" "arguments"

(of "knowledge")

↳ SNARK

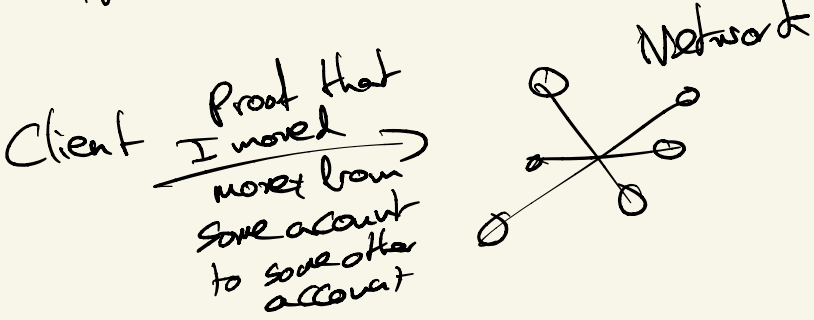
proof with comp. soundness

Ex:



Trivial solution: $\pi = x$

Ex: Cryptocurrencies like ZCash



→ avoid the client having to interact with the entire network

→ proofs that are as short and quick to verify as possible

What we want:

- non-interactive proofs (NIZKs)
- Short proofs: $|\pi|$ is $O(\lambda, \text{poly}\log(|x|, |w|))$
- Efficient verifier: runtime of V is

$$O(\lambda, |x|, \text{poly}\log(|w|))$$

- (ZK)

Non trivial even without ZK.

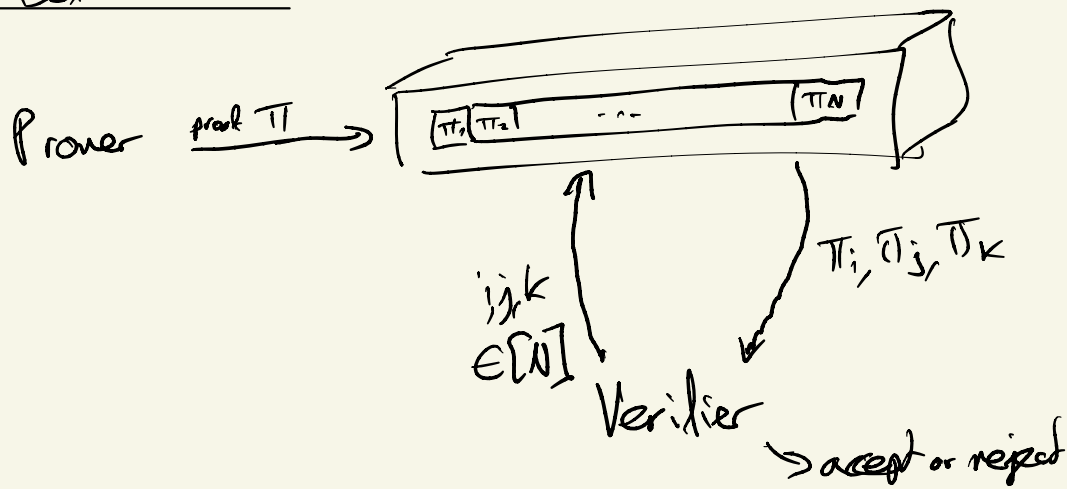
A typical "NP proof" $P \xrightarrow{w} V$ is not succinct.

A blueprint for a SNARG

A special model: interactive oracle proofs

1) Show an information theoretic proof system in some "weird" model
2) Instantiate this "weird" model with Cryptography

A Box Game



Q: Say L is an NP language.
Can we build a complete/sound proof system in this box game?

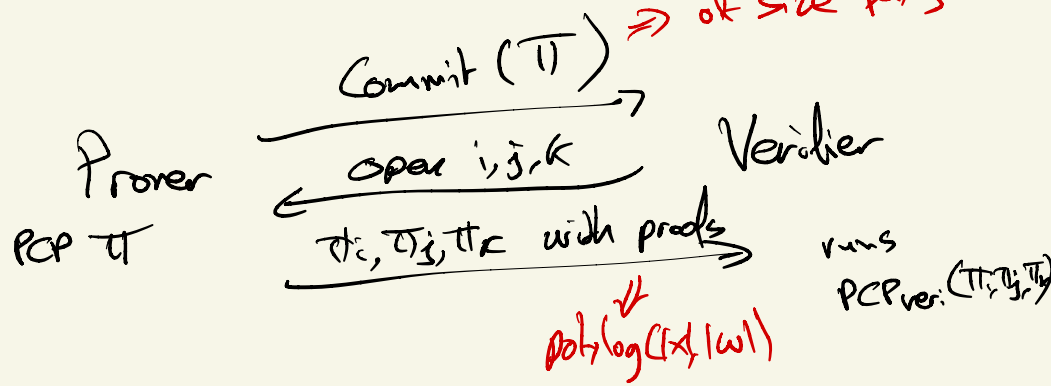
Answer: YES

Why: PCP theorem

if L is an NP language, there exists a proof Π of size polynomial in the instance $x \in L$ s.t. you can verify the proof by reading 3 random bits with completeness 100%
soundness error 1/2

How do we turn the PCP theorem into a SNARG?

We want a succinct "Vector commitment scheme"



⇒ See homework (3)

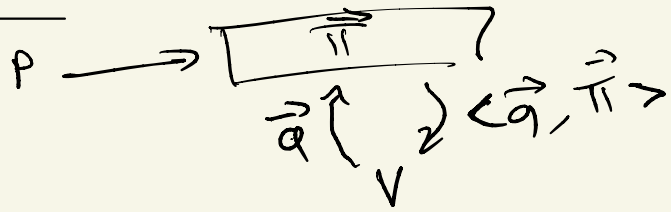
If I asked you to implement this and run it (before end of semester) you would fail

- in the PCP: the proof Π is size poly (|x|, |w|)

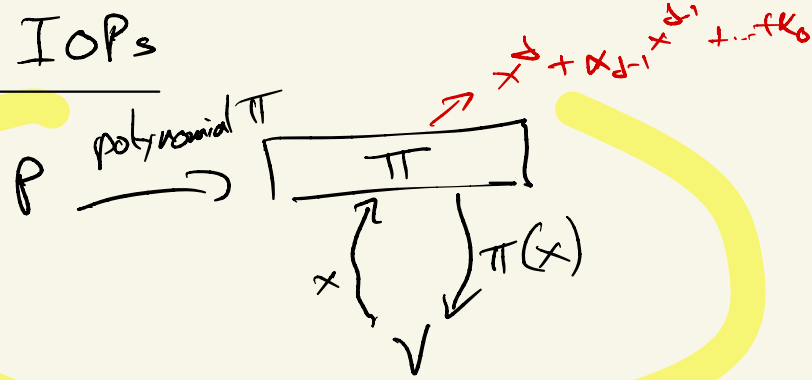
there is a BIG constant and poly terms

In practice: use a different type of box

- linear IOPs → interactive oracle proof



- Polynomial IOPs



SNARG

Example (due to Vitalik Buterin)

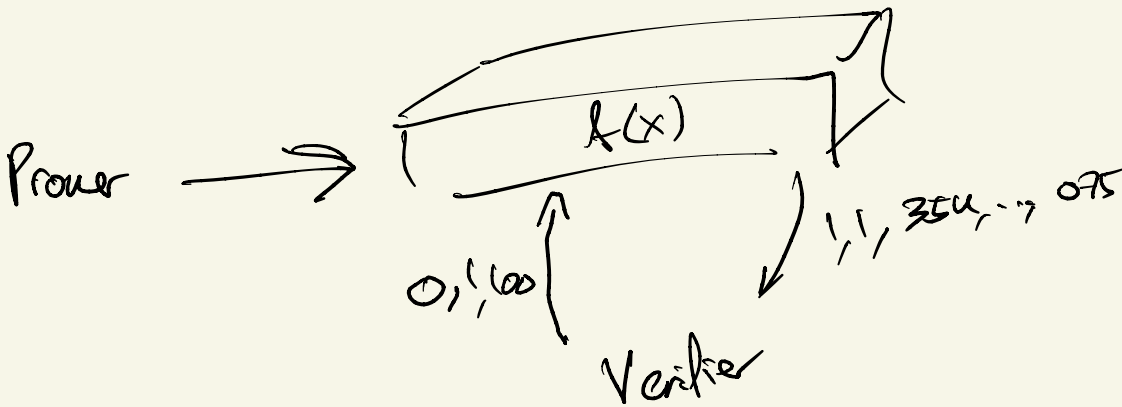
Proving Fibonacci

Claim: the 100th Fibonacci number is

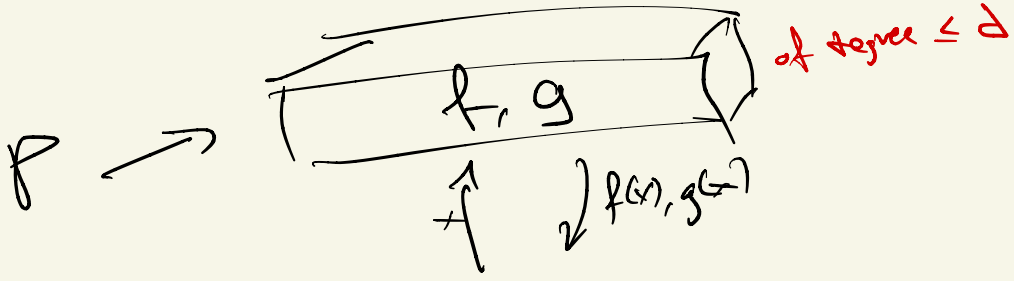
$$354,\ldots,075 \quad (21 \text{ digits})$$

Proof: I build a polynomial $f(x)$ over some large field $\mathbb{F}_p$ and claim:

1. $f(0) = f(1) = 1$ ✓
2. $f(100) = 354,\ldots,075$ ✓
3. $\forall x \in \{0,\ldots,98\}\ f(x+2) = f(x) + f(x+1)$?



An IOP for equality tests of polynomials:



Idea 1: query $f(x), g(x)$ at $d+1$ points and check equality

- This works because $d+1$ points define a unique polynomial of degree d

Idea 2: query $f(r), g(r)$ at one random point $r \in \mathbb{F}$ and check if equal.

Completeness ✓

Soundness: soundness error is $\frac{d}{|\mathbb{F}|}$

Proof of Soundness

Thm (Fundamental Thm of algebra):

A non-zero polynomial of degree d over $\mathbb{F}$ has at most d roots over $\mathbb{F}$

Consider the polynomial $(f-g)(x)$.

It has degree at most d.

It has at most d roots over $\mathbb{F}$.

$$\Rightarrow \Pr_{r \xleftarrow{\$} \mathbb{F}}[f(r) = g(r) \mid f \neq g] \leq \frac{d}{|\mathbb{F}|}$$

Extension to multivariate polynomials $(x^2 + 2xy + y^2 + z^3)$

Schwartz-Zippel Lemma:

if $f(x_1, \ldots, x_n)$ is a non-zero poly of total degree d. Let $r_1, \ldots, r_n \xleftarrow{\$} \Omega \subseteq \mathbb{F}$

(total degree: max degree of a monomial)

Then $\Pr[f(r_1, \ldots, r_n) = 0] \leq \frac{d}{|\Omega|}$

Zero Test

We want to show $f(x+2) = f(x) + f(x+1) \quad \forall x \in \{0, \ldots, 98\}$

$\iff f(x+2) - f(x+1) - f(x) = 0 \quad \forall x \in \{0, \ldots, 98\}$

More generally: Prove that $f \in \mathbb{F}[X]^{\leq d}$ is zero on a set $\Omega \subseteq \mathbb{F}$ of size $|\Omega| = k \leq d$

> Thm: f is zero on Ω iff and only if $f(X)$ is divisible by $Z_\Omega(X) := \prod_{a \in \Omega}(X - a)$

$f(x) = Z_\Omega(x) \cdot q(x)$ iff f is zero on Ω

Our IOP:

compute $q(X) = \frac{f(X)}{Z_\Omega(X)}$ → $f(X), q(X)$

Prover ↑ poly of degree $\leq d - |\Omega|$

$r \xleftarrow{\$} \mathbb{F}$ ↑ $f(r), q(r)$

Verifier check that $f(r) = q(r) \cdot Z_\Omega(r)$

$Z_\Omega(r)$ can be computed in $O(\log|\Omega|)$ time

- Completeness: ✓ $f(x) = z_{S2}(x) \cdot q(x)$
  and so $f(r) = z_{S2}(r) \cdot q(r)$

- Soundness: Assume f is not zero on Ω
  $\Rightarrow$ f cannot be written as $z_\Omega(x) \cdot q(x)$
  $\Leftrightarrow$ $\frac{f(x)}{z_\Omega(x)}$ is not a polynomial over $\mathbb{F}$

So the prover has to commit to some $q(x)$
but $f(x) \neq z_\Omega(x) \cdot q(x)$

And so, by Schwartz-Zippel

$$\Pr\left[f(r) - z_\Omega(r) \cdot q(r) = 0 \right] \leq \frac{2d}{|\mathbb{F}|}$$

deg d | deg $|\Omega| \leq d$ | deg $\leq d$

Putting it all together

Prover $f, q(x) = \frac{f(x+2) - f(x) - f(x+1)}{\prod_{a \in \Omega}^{\Omega} (x-a)}$ ($\prod_{a \in \Omega}^{\Omega} (x-a) = z_\Omega(x)$)

$f(x)$, $q(x)$

0, 1, 100 ↓ $f(0), f(1), f(100)$ ↑ $f(r), f(r+1), f(r+2), q(r)$

Verifier $f(r+2) - f(r) - f(r+1) = q(r) \cdot z_{S2}(r)$

Ex: $f(x) = x^3 - 7x + 6$ and $\Omega = \{1, 2, 3\}$

$$f(x) = \underbrace{(x-1)(x-2)}_{Z_\Omega(x)} \underbrace{(x+3)}_{q(x)}$$

This holds over the entire field!

ex: $f(100) = 99 \cdot 98 \cdot 103$

Polynomial Commitment Schemes

SNARG : Poly IOP(s) + PCS

Poly IOP(s): info theoretic; PCS: crypto

Def: A PCS over a field $\mathbb{F}$ has 4 algs:

- $\text{Setup}(d, \lambda) \to pp$ (public parameters)
- $\text{Commit}(pp, f) \to c$ commit to $f \in \mathbb{F}[X]^{\leq d}$
- $\text{Open}(pp, f, x) \to (\pi, y)$ proof that $f(x) = y$
- $\text{Verify}(pp, c, x, y, \pi) \to \{0,1\}$ check proof that committed polynomial satisfies $f(x) = y$

Properties

- Correctness: $\forall d \in \mathbb{N}, \forall f \in \mathbb{F}[X]^{\leq d}, \forall x \in \mathbb{F}$

$$\Pr\left[\text{Verify}(pp, c, x, f(x), \pi) = 1 \;\middle|\; \begin{array}{l} pp \leftarrow \text{Setup}(d, \lambda) \\ c \leftarrow \text{Commit}(pp, f) \\ \pi \leftarrow \text{Open}(pp, f, x) \end{array}\right] = 1$$

- Evaluation Binding: $\forall d \in \mathbb{N}$, poly time adversaries A

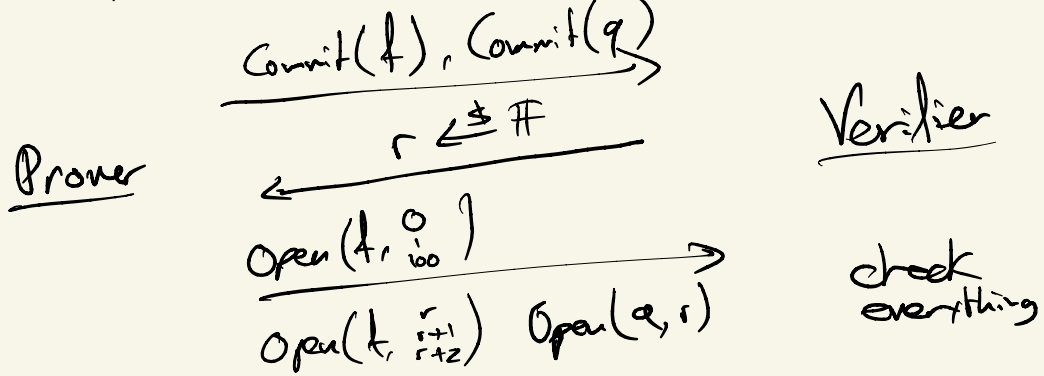
$$\Pr\left[\begin{array}{l} \text{Verify}(pp, c, x, y, \pi) = 1 \\ \text{Verify}(pp, c, x, y', \pi') = 1 \\ y \neq y' \end{array} \;\middle|\; \begin{array}{r} pp \leftarrow \text{Setup}(d, \lambda) \\ (c, x, y, \pi, y', \pi') \leftarrow A(pp) \end{array}\right] \leq \text{negl}(\lambda)$$

Intuition for KZG scheme:

$pp = \{ g^{r^i} : 0 \le i \le d \}$ for $r \xleftarrow{\$} \mathbb{F}$

$\Rightarrow$ lets you compute $g^{f(r)}$ for $f \in \mathbb{F}^{\le d}$

Back to Fibonacci:

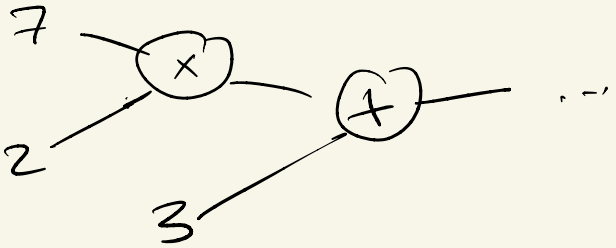


PLONK

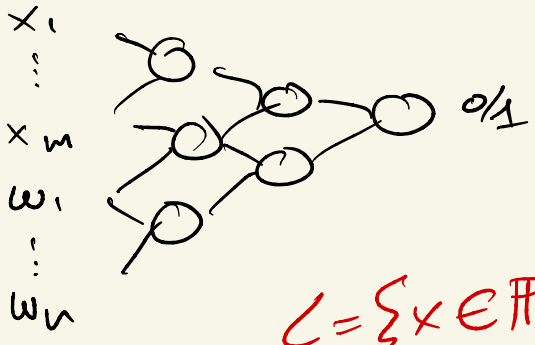
A Poly IOP for NP

Def: Arithmetic Circuits

An arithmetic circuit $C : \mathbb{F}^{\ell} \to \mathbb{F}$ is a circuit with $\times, +$ over $\mathbb{F}$



Our arithmetic circuits have a "public" input x and a "private" witness w



$$\mathcal{L} = \{ x \in \mathbb{F}^m \mid \exists\, w \in \mathbb{F}^n : C(x,w) = 0 \}$$

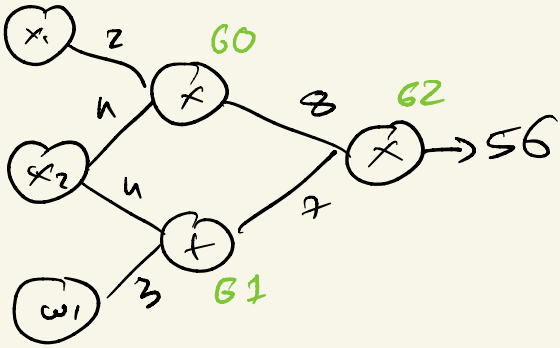
We want a SNARG with

$$|\pi| = O(\lambda, \text{polylog}(|C|))$$

($|C|$ = # of gates)

verifier runs in time $O(\lambda, |x|, \text{polylog}(|C|))$

From Circuits to Polynomials



	x		w
inputs:	2	4	3
Gate 0:	2	4	8
Gate 1:	4	3	7
Gate 2:	8	7	56
	L	R	O

let $|C|$ be the # of gates

let $|I| = |I_x| + |I_w|$ be the # of inputs

let $d = 3|C| + |I|$

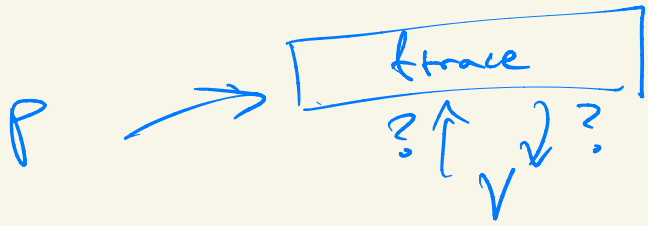
let $\Omega = \{1, \omega, \omega^2, \ldots, \omega^{d-1}\}$ where ω is a "root of unity" such that: $\omega^d = 1$

We build $f_{trace} \in \mathbb{F}[X]^{\leq d}$

1. encode inputs: $f(\omega^{-j}) =$ input #j for $j = 1 \ldots |I|$
2. encode wires: $\begin{cases} f(\omega^{3\ell}) = \text{left input of gate \#}\ell \\ f(\omega^{3\ell+1}) = \text{right} \quad " \\ f(\omega^{3\ell+2}) = \text{output of} \quad " \end{cases}$ $\forall\ \ell = 0$ to $|C|-1$

Verify the circuit trace:

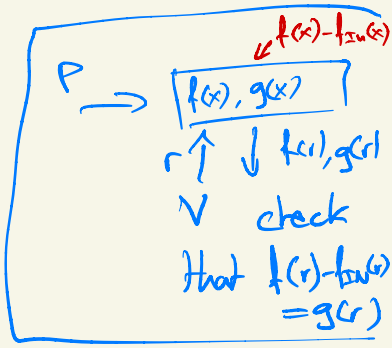
1. The output of the last gate is 0
2. The poly f_{trace} encodes the statement x
3. Each gate is evaluated correctly
4. The wiring is consistent
   ↳ (zero test)



1: $f_{trace}(\omega^{3|C|-1}) = 0$ ✓ 1 opening

2: checking the inputs

$f(\omega^{-1}) = x_1$
$f(\omega^{-2}) = x_2$
$\vdots$
$f(\omega^{-|I_x|}) = x_m$



verifier builds $f_{in}(x)$ s.t $f_{in}(\omega^{-i}) = x_i$

Prove that $f_{trace}(x) - f_{in}(x) = 0 \quad \forall x \in \Omega_I$

$= \{\omega^{-1}, \ldots, \omega^{-|I_x|}\}$

$\Rightarrow$ Zero Test

3. we want

$$f(\omega^2) = f(\omega^0) \cdot f(\omega^1)$$

$$f(\omega^5) = f(\omega^3) + f(\omega^4)$$

...

	x		ω
inputs:	2	4	3
Gate 0:	2	4	8
Gate 1:	4	3	7
Gate 2:	8	7	56
	L	R	O

Def: $f_{sel}(x) \in \mathbb{F}[x]^{\leq d}$ encodes gate types

$$f_{sel}(\omega^{3\ell}) = \begin{cases} 0 & \text{if gate } \ell \text{ is "}\times\text{"} \\ 1 & \text{" "+"} \end{cases}$$

$$f_{gates}(x) = f_{SEL}(x)\left[f(x) + f(\omega x)\right] + (1 - f_{SEL}(x))\left[f(x) \cdot f(\omega x)\right] = f(\omega^2 x)$$

(left input; right input; output)

check that $f_{gates}(x) = 0$

$\forall x \in \{\omega^0, \omega^3, \omega^6, \ldots, \omega^{3(d-1)}\}$

$\Rightarrow$ Zero Test