ZERO-KNOWLEDGE (INTRO)

ALON ROSEN

IDC HERZLIYA

IDC HERZLIYA

fact FOUNDATIONS & APPLICATIONS of CRYPTOGRAPHIC THEORY

Zero-knowledge proofs

Prover P **Verifier V**

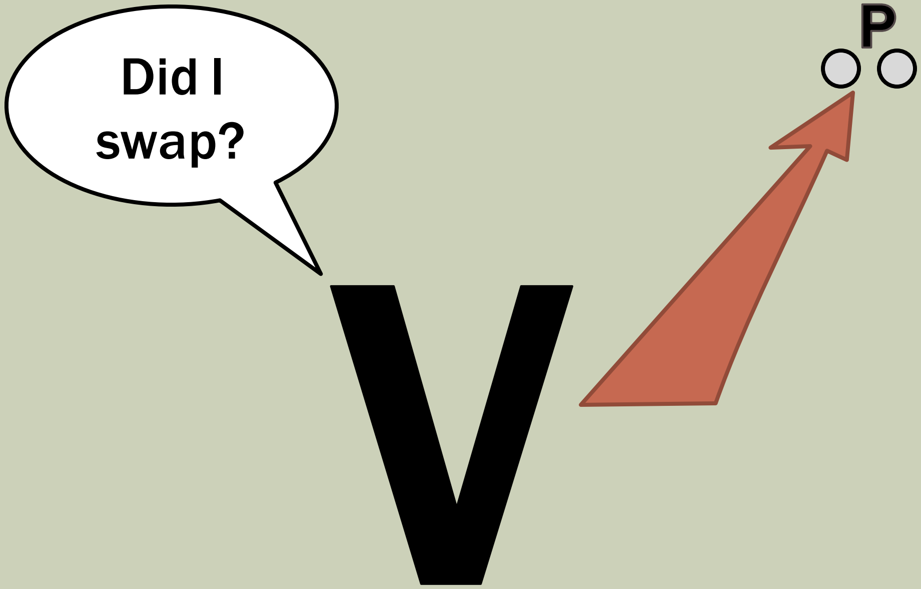
P interacts with V convincing him that a proposition is true

Interaction reveals nothing beyond validity of the proposition

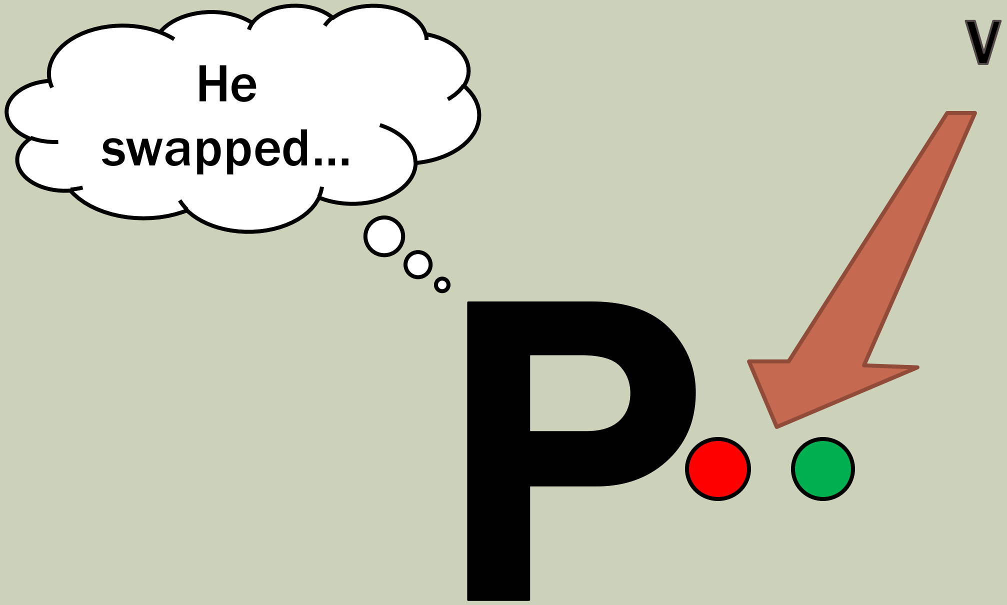
If proposition is true, *any* V^* might as well have generated (simulated) the interaction on his own

Avoids the question "what is knowledge?" altogether!

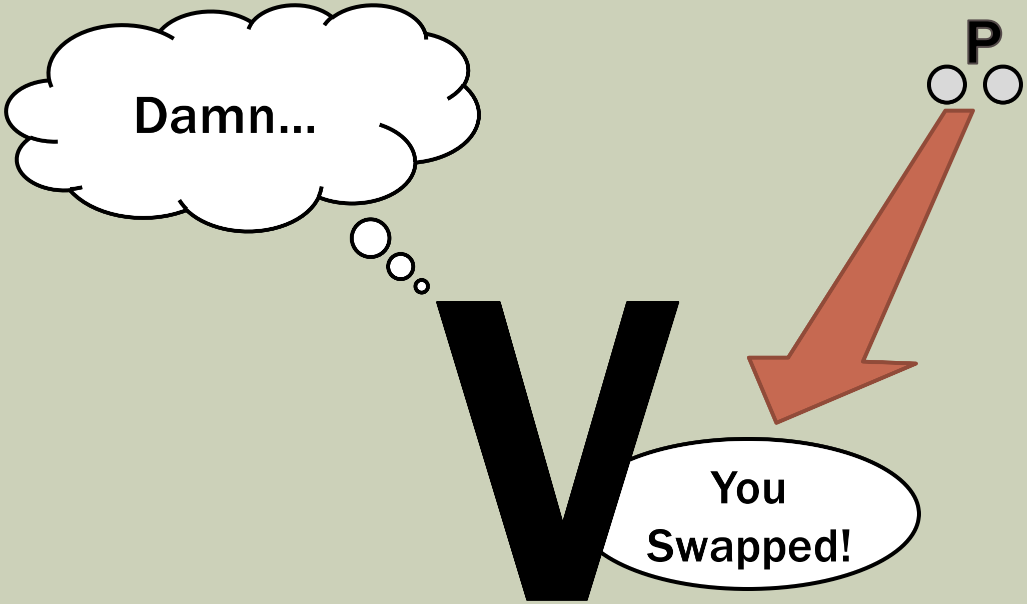
Example: color non-blindness



Example: color non-blindness



Example: color non-blindness



- V's "view": *a random bit that equals his "swap or not" bit*
- V could simulate view by picking random bit on his own!

What is zero-knowledge good for?

Can prove that I know a secret without having to reveal it

Identification:

1. **Alice publishes** $y = f(x)$
2. **Alice proves to Bob in ZK that she knows** $x' \in f^{-1}(y)$

Protocol design:

1. **Design against parties that follow instructions**
2. **Use ZK proof to force honest behavior**

"trusted party" → protocol

Why zero-knowledge?

Remarkable definitional framework:

- At the heart of protocol design and analysis
- Brings to light key concepts and issues

Right level of abstraction:

- Simple enough to be studied/realized
- Feasibility/limitations delineate what is attainable

ZK is just a means to an end

- Weaker definitions are also useful (WI/WH/NIZK)
- Tension between modularity and efficiency

Proof Systems

What is a proof?

A method for establishing truth:

1. legal
2. authoritative
3. scientific
4. philosophical
5. mathematical

$$\underline{\text{Axioms}} \quad \to \to \overset{\pi}{\cdots} \quad \to \quad \underline{\text{Propositions}}$$

6. probabilistic, interactive

Proof Systems

Want to prove: $x \in L$ for some language $L \subseteq \Sigma^*$

$$L = \{x \mid \exists \pi, V(x, \pi) = \text{ACCEPT}\}$$

Definition: A proof system for membership in L is an algorithm V such that $\forall x$:

Completeness: If $x \in L$, then $\exists \pi$, V(x, π) = ACCEPT

Soundness: If $x \notin L$, then $\forall \pi$, V(x, π) = REJECT

NP Proof Systems

efficient verification $\Leftrightarrow$ poly-time verification

Definition: An NP proof system for membership in L is an algorithm V such that $\forall x$:

Completeness: If $x \in L$, then $\exists \pi$, V(x, π) = ACCEPT

Soundness: If $x \notin L$, then $\forall \pi$, V(x, π) = REJECT

Efficiency: V(x, π) halts after at most $poly(|x|)$ steps

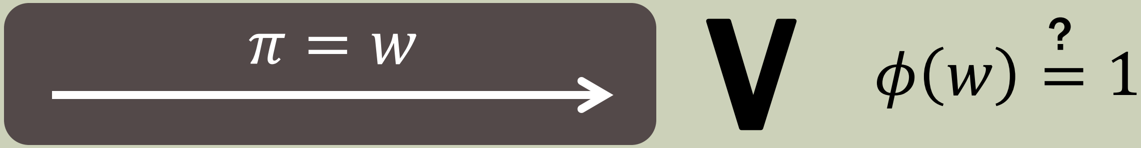
- V's running time is measured in terms of $|x|$, the length of x
- $\mathrm{poly}(|x|) = |x|^c$ for some constant c
- Necessarily, $|\pi| = poly(|x|)$

Example I: Boolean Satisfiability

$$SAT = \{\phi | \phi \textit{ is a satisfiable Boolean formula}\}$$

$$SAT = \{\phi(w_1, \dots, w_n) \mid \exists w \in \{0,1\}^n, \phi(w) = 1\}$$

$\phi \in SAT$:



$\xrightarrow{\pi = w}$ **V** $\phi(w) \overset{?}{=} 1$

Complete: every $L \in NP$ reduces to SAT

Unstructured: $exp(O(n))$ time (*worst case*).

Example II: Linear Equations

$$LIN = \{(A, b) | Aw = b \text{ } has \text{ } a \text{ } solution \text{ } over \text{ } \mathbb{F}\}$$

$(A, b) \in LIN$: $\xrightarrow{\pi = w}$ **V** $Aw \overset{?}{=} b$

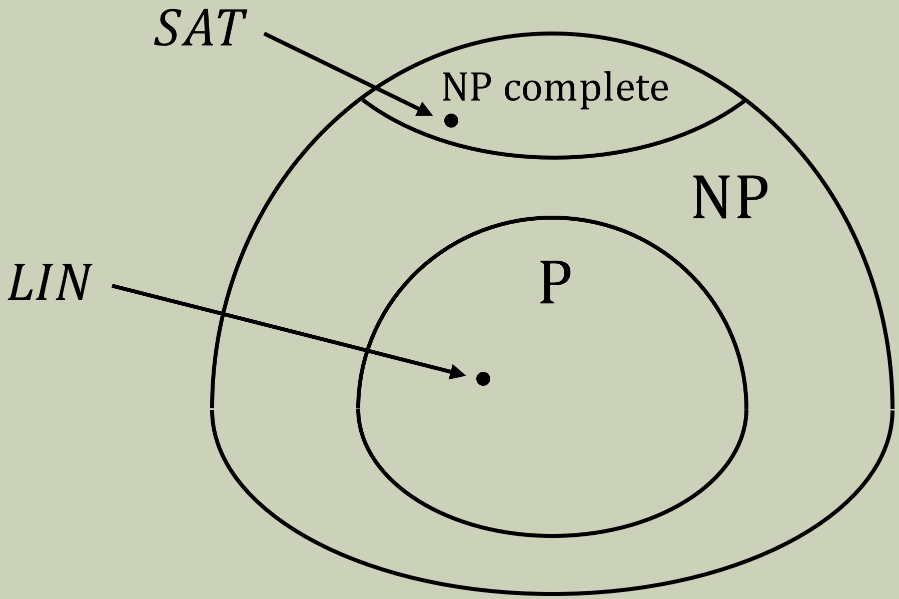
$exp(n)$ **many** w**'s**

<u>Structured</u>: decidable in time $O(n^{2.373}) = poly(n)$

The class P

poly-time ⟺ efficient

Definition: $L \in \mathrm{P}$ if there is a poly-time algorithm A such that $L = \{x \mid A(x)$ = ACCEPT$\}$



BPP: A is probabilistic poly-time (PPT) and errs w.p. $\leq 1/3$

Example III: Quadratic Residuosity

$$QR_N = \{x \mid x \; is \; a \; quadratic \; residue \; mod \; N\}$$

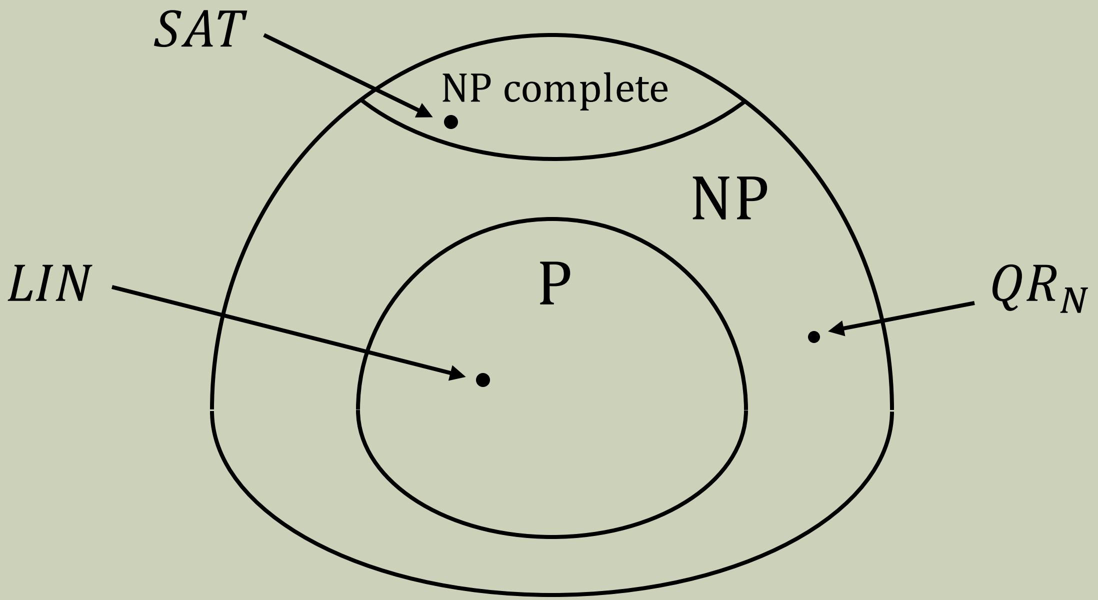
$$x \in QR_N: \quad \xrightarrow{\pi = w} \quad \mathbf{V} \quad x \overset{?}{\equiv} w^2 \; mod \; N$$

<u>Structured</u>: QR_N is a subgroup of $\mathbb{Z}_N^*$

$N = PQ \; (|P| = |Q| = n)$: $exp\left(\tilde{O}\left(n^{1/3}\right)\right)$ time (avg. case)

Summary so far

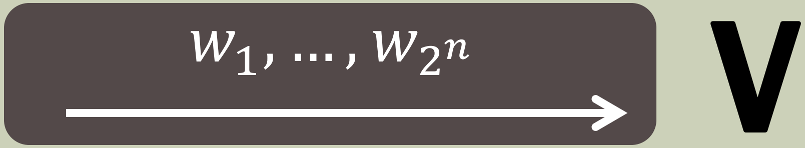
efficient verification $\Leftrightarrow$ poly-time verification



Proving non-membership?

$(A, b) \notin LIN?$

$\phi \notin SAT$:

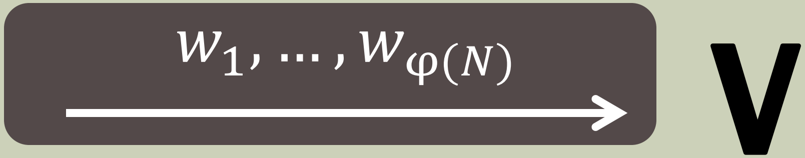


$w_1, \dots, w_{2^n}$

V

$\forall i, \phi(w_i) \overset{?}{=} 0$

$x \notin QR_N$:



$w_1, \dots, w_{\varphi(N)}$

V

$\forall i, x \overset{?}{\not\equiv} w_i^2 \bmod N$

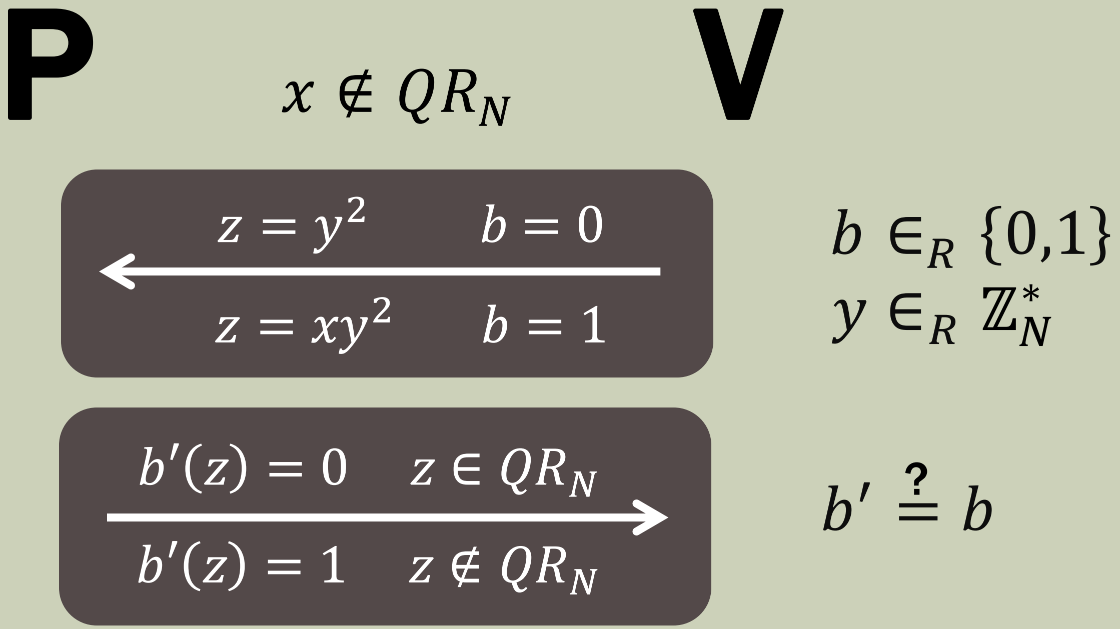
Naïve proof is exponentially large

[GMR'85]: allow proof to use

- **Randomness (tolerate "error")**
- **Interaction (add a "prover")**

Interactive Proofs

Interactive proof for $\overline{QR_N}$ [GMR'85]



P

$x \notin QR_N$

V

$z = y^2 \quad b = 0$

$z = xy^2 \quad b = 1$

$b \in_R \{0,1\}$

$y \in_R \mathbb{Z}_N^*$

$b'(z) = 0 \quad z \in QR_N$

$b'(z) = 1 \quad z \notin QR_N$

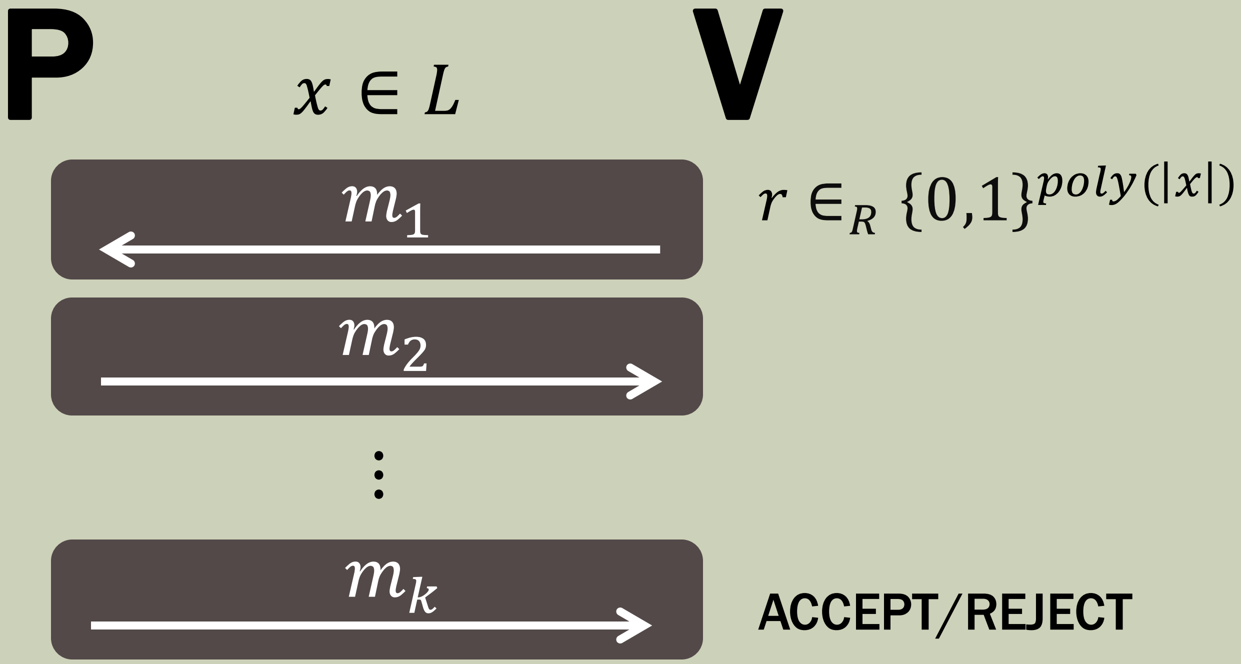
$b' \overset{?}{=} b$

<ins>**Completeness:**</ins> $x \notin QR_N \rightarrow y^2 \in QR_N$ <ins>**and**</ins> $xy^2 \notin QR_N$

<ins>**Soundness:**</ins> $x \in QR_N \rightarrow y^2 \in QR_N$ <ins>**and**</ins> $xy^2 \in QR_N$

$$\forall P^*, Pr_b[P^*(z) = b] = 1/2$$

Interactive Proof



P

$x \in L$

V

$r \in_R \{0,1\}^{poly(|x|)}$

m_1

m_2

$\vdots$

m_k

ACCEPT/REJECT

V **is probabilistic polynomial time (**PPT**)**

For any <u>common input</u> x**, let:**

$$Pr[(P,V) \text{ accepts } x] \triangleq Pr_r[(P,V)(x,r) = \text{ ACCEPT}]$$

Interactive Proof Systems

Definition [GMR'85]: An interactive proof system for L is a PPT algorithm V and a function P such that $\forall x$:

Completeness: If $x \in L$, then $Pr[(P,V) \text{ accepts } x] \geq 2/3$

Soundness: If $x \notin L$, then $\forall P^*, Pr[(P^*,V) \text{ accepts } x] \leq 1/3$

- Completeness and soundness can be bounded by any $c: \mathbb{N} \rightarrow [0,1]$ and $s: \mathbb{N} \rightarrow [0,1]$ as long as
  - $c(|x|) \geq 1/2 + 1/poly(|x|)$
  - $s(|x|) \leq 1/2 - 1/poly(|x|)$
- $poly(|x|)$ independent repetitions → $c(|x|) - s(|x|) \geq 1 - 2^{-poly(|x|)}$
- NP is a special case ($c(|x|) = 1$ and $s(|x|) = 0$)
- BPP is a special case (no interaction)

The Power of IP

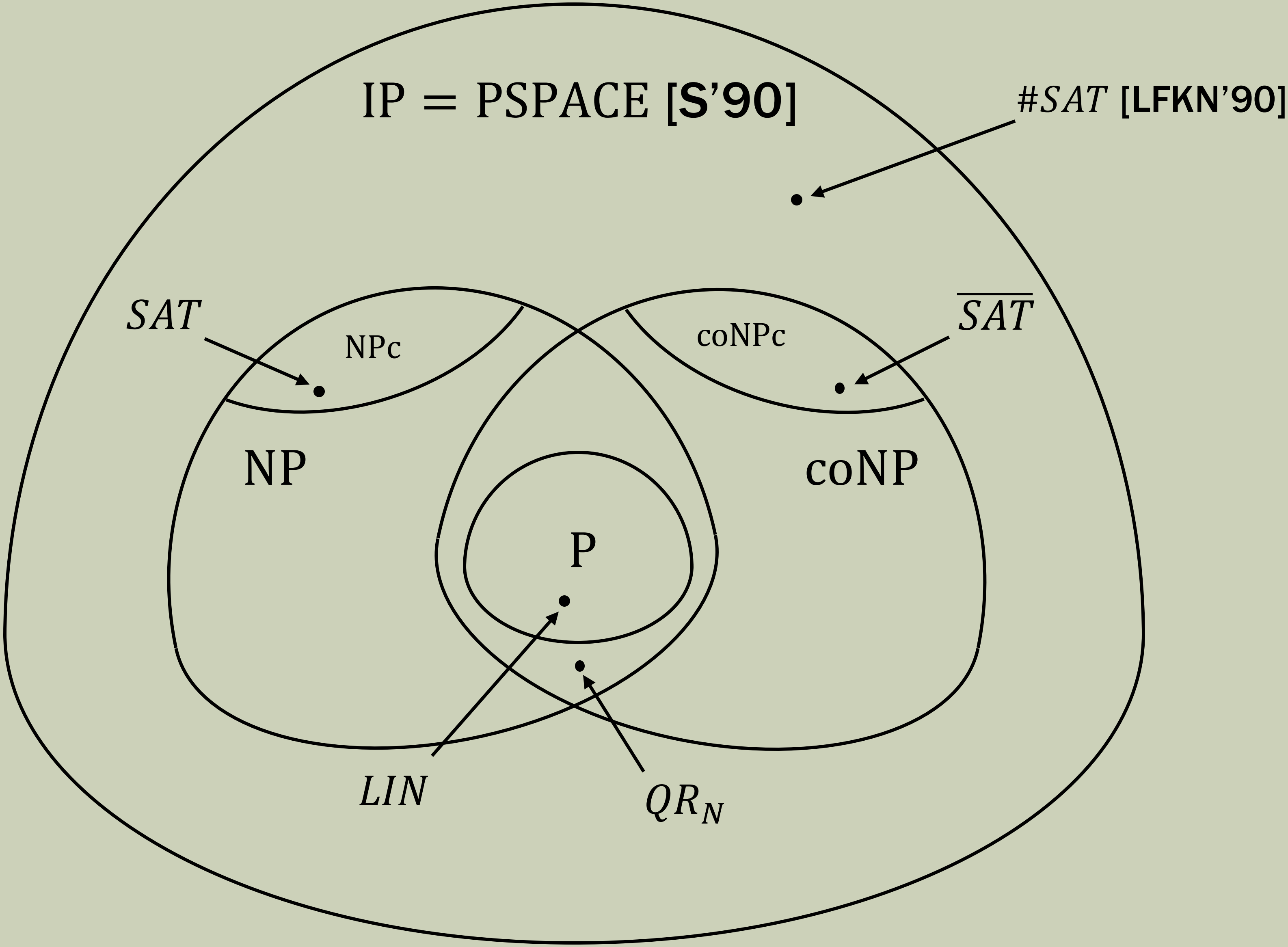
Proposition: $\overline{QR_N} \in \mathrm{IP}$

- NP **proof for** $\overline{QR_N}$ **not self-evident**
- **This suggests that maybe** $\mathrm{NP} \subset \mathrm{IP}$
- **Turns out that** $\overline{SAT} \in \mathrm{IP}$ **(in fact** $\#SAT$**)**

Theorem [LFKN'90]: $P^{\#\mathrm{P}} \subseteq \mathrm{IP}$

Theorem [Shamir'90]: $\mathrm{IP} = \mathrm{PSPACE}$

The power of IP



Zero-Knowledge

A Proof that (presumably) Does Leak Info

$$QR_N = \{x \mid x \text{ is a quadratic residue mod } N\}$$

$x \in QR_N$: $\xrightarrow{\pi = w}$ **V** $x \overset{?}{\equiv} w^2 \bmod N$

- **Generating** π **-** $exp(\tilde{O}\left(n^{1/3}\right)$ **time**
- **Verifying -** $O(n^2)$ **time**

V "got something for free" from seeing π

V may have not been able to find w on his own!

Defining that "no knowledge leaked"

Some attempts:

- V **didn't learn** w **(sometimes good enough!)**
- V **didn't learn any symbol of** w
- V **didn't learn any information about** w
- V **didn't learn *any information at all* (beyond** $x \in L$**)**

When would we say that V ***did* learn something?**

If following the interaction V **could compute something he could have not computed without it!**

Zero-knowledge: whatever is computed following interaction could have been computed without it

Zero-Knowledge (at last)

V's view = V's random coins and messages it receives

$\forall x \in L, V$'s view can be efficiently "simulated"

What does this mean?

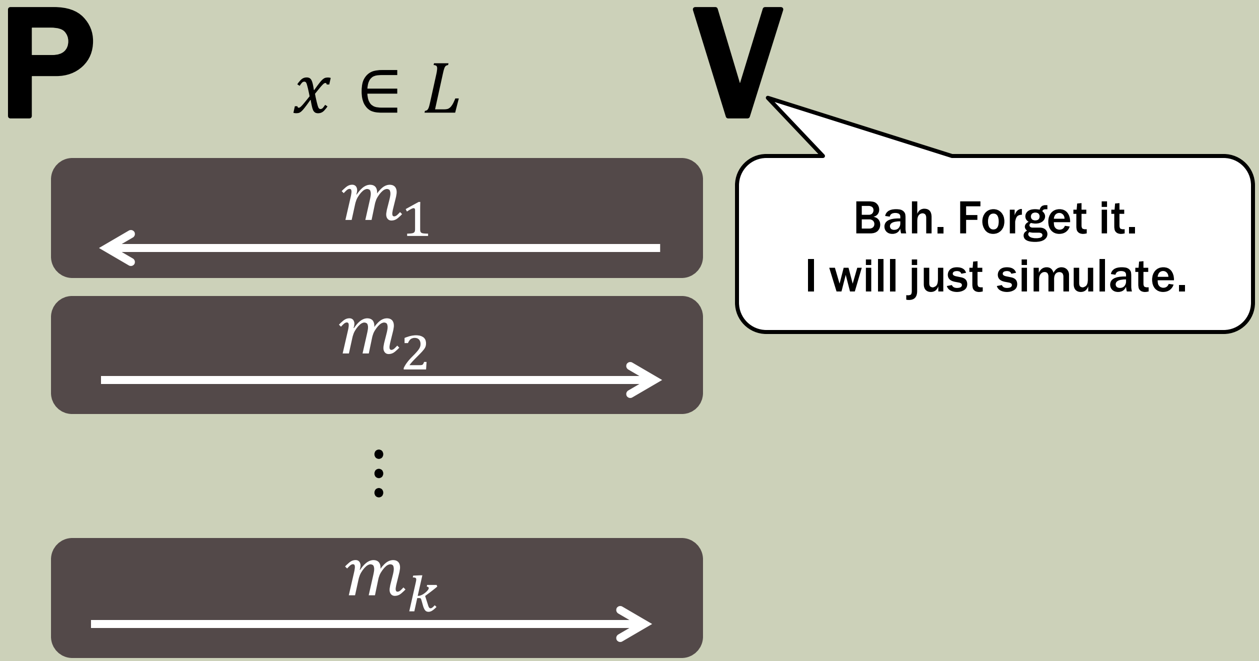
Philosophically: V is given the information that $x \in L$

Modulo this, V might as well have talked to himself

Technically: $V(\text{view}) \cong V(\text{simulation})$

Whatever V could compute following the interaction,
he could have computed even without talking to P,
by running the simulator on his own

V might as well talk to himself



P

$x \in L$

V

m_1

m_2

$\vdots$

m_k

Bah. Forget it.
I will just simulate.

$$V(x, r, m_1, \ldots, m_k)$$
$$\downarrow$$
$$V(\mathrm{sim}(x))$$

Honest Verifier Zero-Knowledge

V's view distribution can be simulated in poly-time

- We will allow simulator S to be probabilistic (PPT)
- Efficient ⟺ Probabilistic poly-time (BPP instead of P)

Definition [GMR'85]: An interactive proof (P, V) for L is (honest-verifier) zero-knowledge if $\exists PPT\ S\ \forall x \in L$

$$S(x) \cong (P, V)(x)$$

- We use $(P, V)(x)$ to denote V's view
- Usually $(P, V)(x) = V(\text{view})$ denotes V's output
- Simulator for V's view implies simulator for V's output

Sanity check

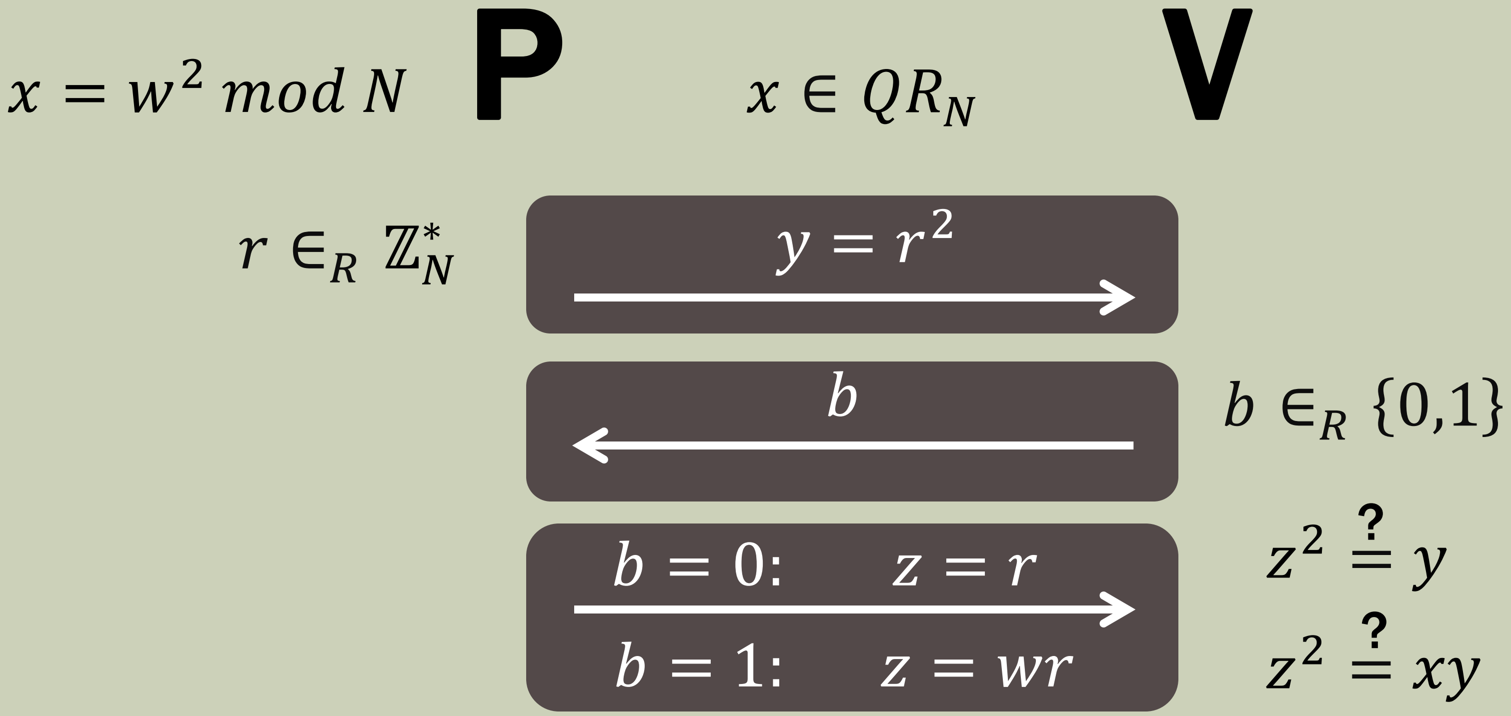
$x \in QR_N$: $\xrightarrow{\pi = w}$ **V** $x \overset{?}{\equiv} w^2 \, mod \, N$

- $\forall x \in QR_N, S(x)^2 \equiv x \, mod \, N$
- $\forall x \notin QR_N, \; S(x)^2 \not\equiv x \, mod \, N$
- $QR_N \notin BPP \rightarrow \; S(x)^2 \not\equiv x \, mod \, N$ **<u>for some</u>** $x \in QR_N$

(P, V) for L is <u>not</u> (honest-verifier) zero-knowledge if $\forall \; PPT \; S \; \exists x \in L$ so that

$$S(x) \not\equiv (P, V)(x)$$

A Zero-Knowledge proof for QR_N



$x = w^2 \bmod N$ **P**

$x \in QR_N$

V

$r \in_R \mathbb{Z}_N^*$

$\xrightarrow{y = r^2}$

$\xleftarrow{b}$

$b \in_R \{0,1\}$

$b = 0$: $z = r$

$\longrightarrow$

$b = 1$: $z = wr$

$z^2 \overset{?}{=} y$

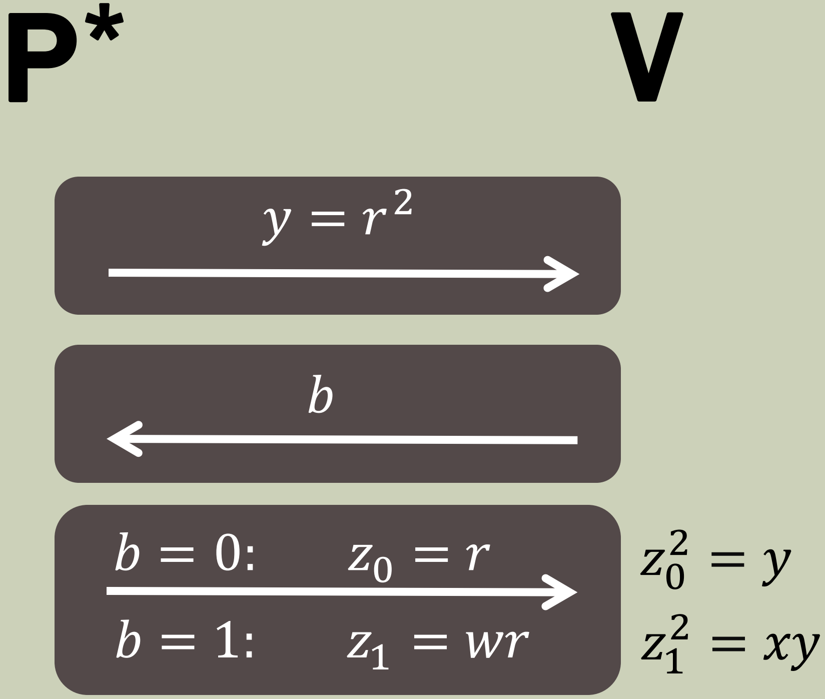
$z^2 \overset{?}{=} xy$

- P is randomized and has auxiliary input w
- Distribution of V's "view" $(P(w), V)(x)$:

  uniformly random (y, b, z) such that $z^2 = x^b y$

A Zero-Knowledge proof for QR_N

<u>Claim:</u> (P, V) **is an interactive proof for** QR_N



P*

V

$y = r^2$ →

b ←

$b = 0$: $z_0 = r$ →

$b = 1$: $z_1 = wr$

$z_0^2 = y$

$z_1^2 = xy$

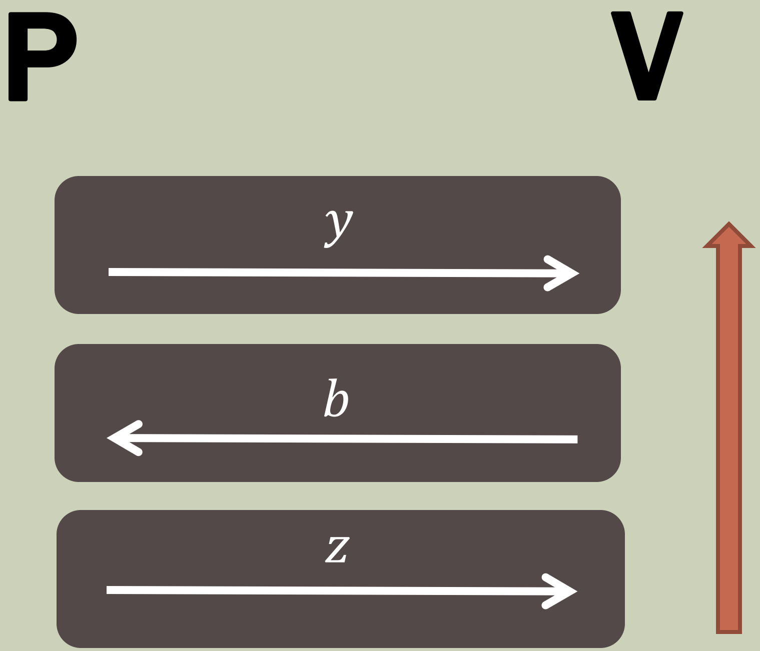
<u>Soundness</u>:

$$x \in QR_N$$
$$\updownarrow$$
$$\exists y, y \in QR_N \text{ \underline{and} } xy \in QR_N$$

If $Pr_b[(P^*, V)$ **accepts** $x]$ **> 1/2**

then both $z_0^2 = y$ **<u>and</u>** $z_1^2 = xy$

Simulating V's view



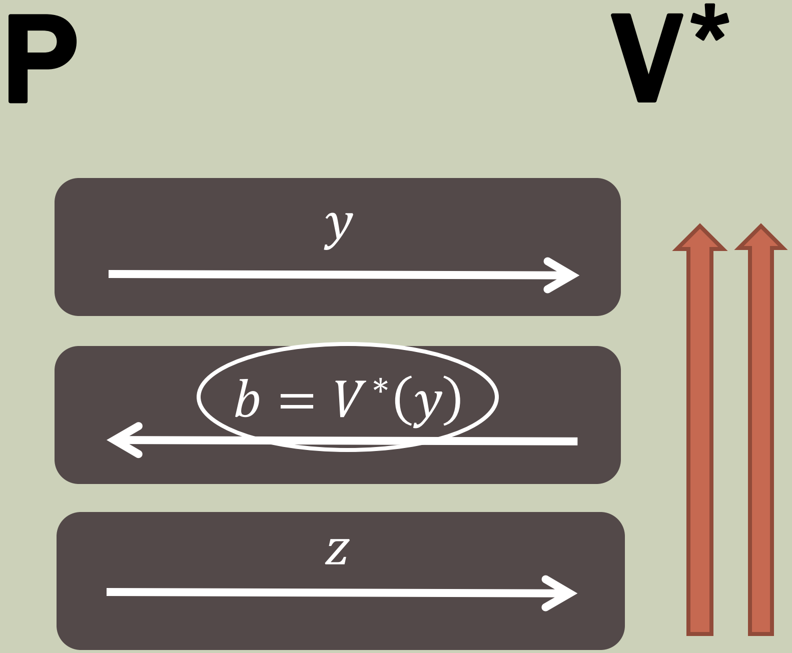
<u>**Simulator $S(x)$**</u>

1. **Sample** $z \in_R \mathbb{Z}_N^*$
2. **Sample** $b \in_R \{0,1\}$
3. **Set** $y = z^2/x^b$
4. **Output** (y, b, z)

random (y, b, z) **such that** $z^2 = x^b y$ $\cong$ **random** (y, b, z) **such that** $z^2 = x^b y$

<u>**Proposition**</u>**:** $QR_N \in \mathrm{HVZK}$

Simulating malicious V^*'s view



P

V*

y

$b = V^*(y)$

z

<u>Simulator $S(x)$</u>

1. Sample $z \in_R \mathbb{Z}_N^*$
2. Sample $b \in_R \mathbb{Z}_N^*$
3. Set $y = z^2/x^b$
4. If $V^*(y) = b$ output (y, b, z)
5. Otherwise <u>repeat</u>

$$x \in QR_N$$
$$\downarrow$$
$$\mathbb{E}[\#\text{repetitions}] = 2$$

random (y, b, z) such that $z^2 = x^b y$ <u>and</u> $b = V^*(y)$

$\cong$

random (y, b, z) such that $z^2 = x^b y$ <u>and</u> $b = V^*(y)$

Perfect Zero-Knowledge

Definition: An interactive proof system (P, V) for L is perfect zero-knowledge if $\forall PPT\ V^* \ \exists PPT\ S\ \forall x \in L$

$$S(x) \cong (P, V^*)(x)$$

Proposition: $QR_N \in \mathrm{PZK}$

- Actually showed "black-box" ZK: $\exists PPT\ S\ \forall PPT\ V^*\ \forall x \in L$

$$S^{V^*}(x) \cong (P, V^*)(x)$$

- We allowed S to run in expected polynomial time
- Can we build S with strict polynomial running time?

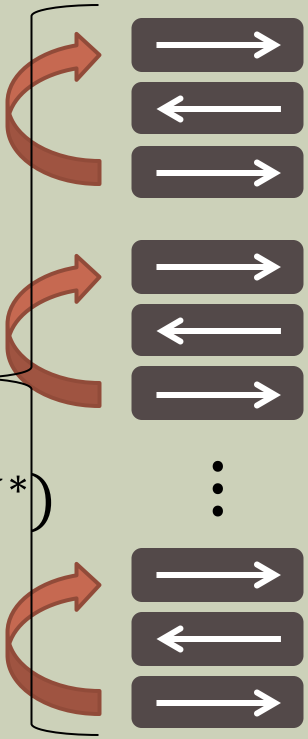
Amplifying soundness

P **V***

$S^{V^*}(x)$ **keeps state of partial view**

Repeat sequentially $k = poly(|x|)$ **times**

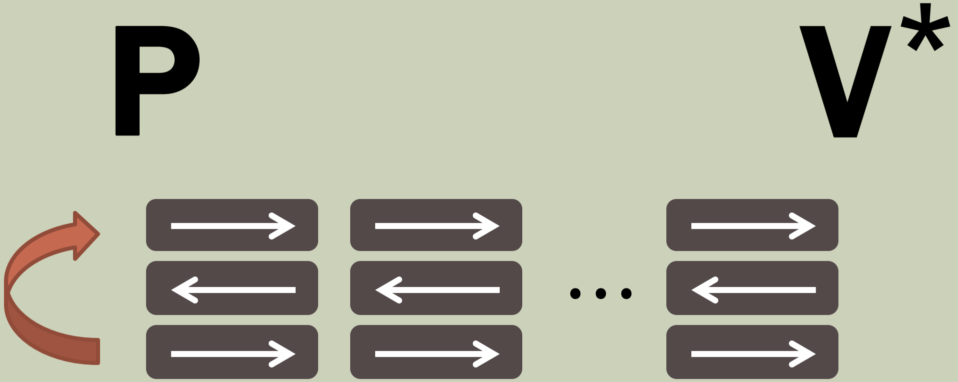
$\mathbb{E}[\text{time}(S)] = 2\ \text{time}(V^*)$



ACCEPT iff all repetitions are accepting

Proposition: $QR_N \in \text{PZK}$ **w/ soundness error** $2^{-poly(|x|)}$

Parallel repetition



P

V^*

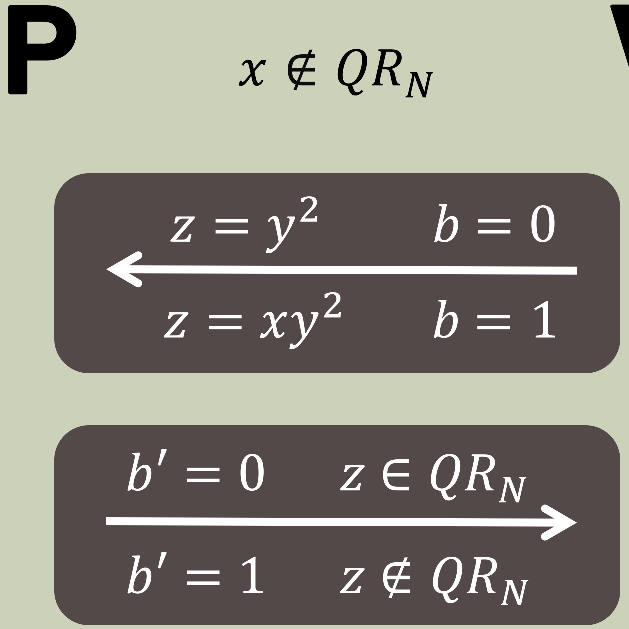
$$\mathbb{E}\left[\mathrm{time}\left(S^{V^*}\right)\right] = 2^k\,\mathrm{time}(V^*)$$

Later:

- **Black-box impossibility**
- V^* **whose view cannot be efficiently simulated**

Auxiliary input and Composition

IP for $\overline{QR_N}$ is not ZK



P $x \notin QR_N$ **V**

$z = y^2$ $b = 0$

$\xleftarrow{\hspace{3cm}}$

$z = xy^2$ $b = 1$

$b' = 0$ $z \in QR_N$

$\xrightarrow{\hspace{3cm}}$

$b' = 1$ $z \notin QR_N$

<u>Not ZK wrt “auxiliary input”</u>

$V^*(z)$: use P to decide if $z \in QR_N$

z is V^*‘s auxiliary input

<u>Proposition:</u> $\overline{QR_N} \in \mathrm{HVZK}$

<u>Claim:</u> (P, V) is <u>not</u> ZK (wrt auxiliary input)

ZK wrt auxiliary input

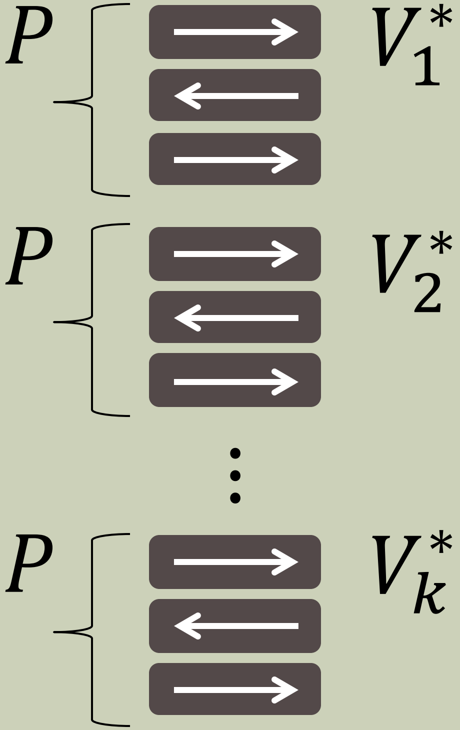
Definition: An interactive proof (P,V) for L is (perfect) ZK wrt auxiliary input if $\forall PPT\ V^* \ \exists PPT\ S\ \forall x \in L\ \forall z$

$$S(x,z) \cong \big(P,V^*(z)\big)(x)$$

- z captures "context" in which protocol is executed
  - Other protocol executions ("environment")
  - A-priori information (in particular about w)
- Simulator is also given the auxiliary input z
- Simulator runs in time $poly(|x|)$
- Auxiliary input z is essential for composition

Sequential composition of ZK

P **V***



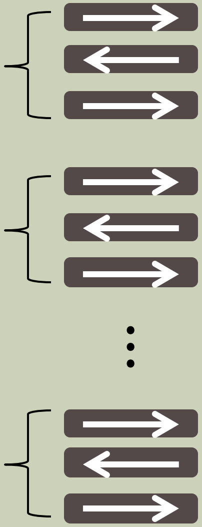
Compose sequentially
$k = poly(|x|)$ **times**

simulating view of each of V_i's → simulating view of V^*

Sequential composition of ZK

Theorem: ZK is closed under sequential composition

P $\quad\quad$ $\mathbf{V}^*_{(x,z)}$



$V_1^*(x,z)$

$S^{V_1^*}(x,z) = \boldsymbol{z_1}$

$V_2^*(x,z,\boldsymbol{z_1})$

$S^{V_2^*}(x,z,\boldsymbol{z_1}) = \boldsymbol{z_2}$

$\vdots$

$V_k^*(x,z,\boldsymbol{z_1},\dots,\boldsymbol{z_{k-1}})$

$S^{V_k^*}(x,z,\boldsymbol{z_1},\dots,\boldsymbol{z_{k-1}}) = \boldsymbol{z_k}$

$S^{V^*}(x,z) = \boldsymbol{z_1},\dots,\boldsymbol{z_k}$

$$\forall i, \boldsymbol{z_i} \cong \left(P, V_i^*(z,\boldsymbol{z_1},\dots,\boldsymbol{z_{i-1}})\right)(x)$$

Summary

Defined:

- $\text{NP}, \text{P}, \text{BPP}, \text{IP}\ (= \text{PSPACE})$
- PZK, HVZK

Saw:

- $LIN, QR_N, SAT \in \text{NP}$
- $QR_N \in \text{HVZK}$
- $QR_N \in \text{PZK}$
- $\overline{QR_N} \in \text{HVZK}$
- **auxiliary input for** ZK **protocols**
- **sequential composition of** ZK **protocols**

Food for Thought

What if P=NP?

- If $\mathrm{P} = \mathrm{NP}$ then all $L \in \mathrm{NP}$ can be proved in PZK
- P sends nothing to V, who decides $x \in L$ on his own
- But what about ZK within P?
- For instance against quadratic time verifiers?

<u>Exercise</u>: Suppose $\omega > 2$. Construct an interactive proof for LIN that is PZK for quadratic time verifiers

- <u>An issue</u>: composition. What about say n executions?
- In contrast, $poly(n)$ is closed under composition

History

Shafi Goldwasser

Silvio Micali

Charlie Rackoff

The End

Definition: An interactive proof system for L is a PPT algorithm V and a function P such that $\forall x$:

Completeness: If $x \in L$, then $Pr[(P,V)$ accepts $x] \geq 2/3$

Soundness: If $x \notin L$, then $\forall P^*, Pr[(P^*,V)$ accepts $x] \leq 1/3$

Definition: (P,V) for L is (perfect) ZK wrt auxiliary input if $\forall PPT\ V^*\ \exists PPT\ S\ \forall x \in L\ \forall z$

$$S(x,z) \cong \big(P(w), V^*(z)\big)(x)$$