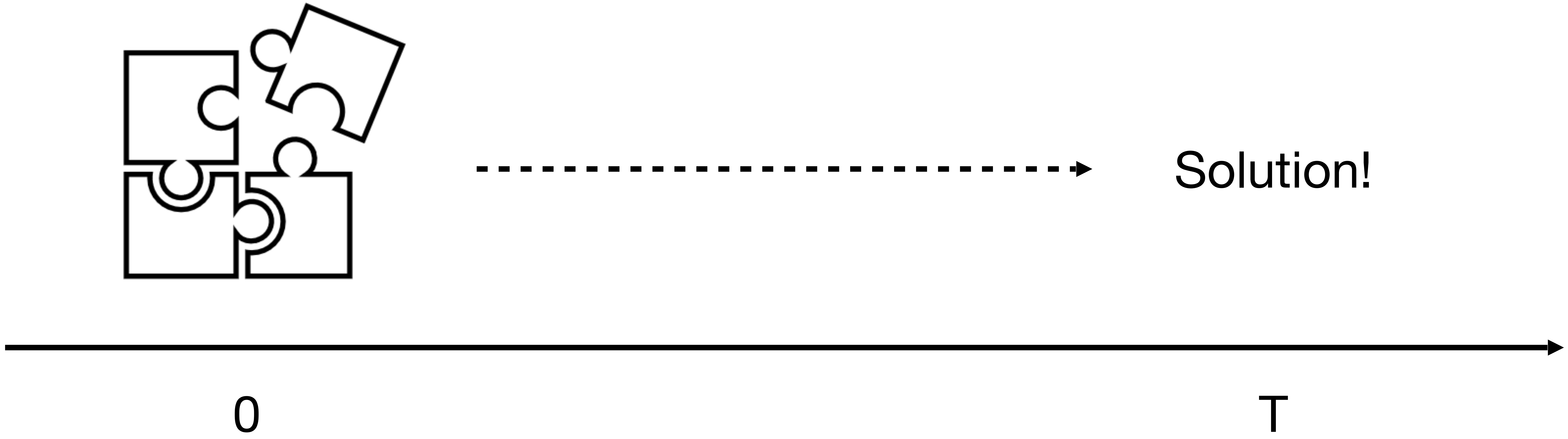
Lattice-Based Timed Cryptography

Giulio Malavolta
(Max Planck Institute —> Bocconi University)

Joint work with Russell Lai

Timed Cryptography



Timed Cryptography

- Time-Lock Puzzles

Timed Cryptography

- Time-Lock Puzzles
- Proofs of Sequential Work

Timed Cryptography

- Time-Lock Puzzles
- Proofs of Sequential Work
- Verifiable Delay Functions

Applications

Seal-Bid Auctions

E-Voting

Randomness Generation

Contract Signing

More Applications

Hardness vs Fine-Grained Hardness

Hardness vs Fine-Grained Hardness

<u>One-Way Problems</u>

poly-size

P $\neq$ NP

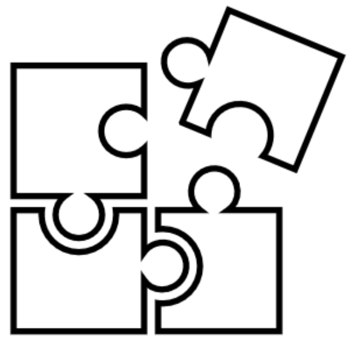
Hardness vs Fine-Grained Hardness

One-Way Problems

} poly-size

$P \neq NP$

Sequential Problems

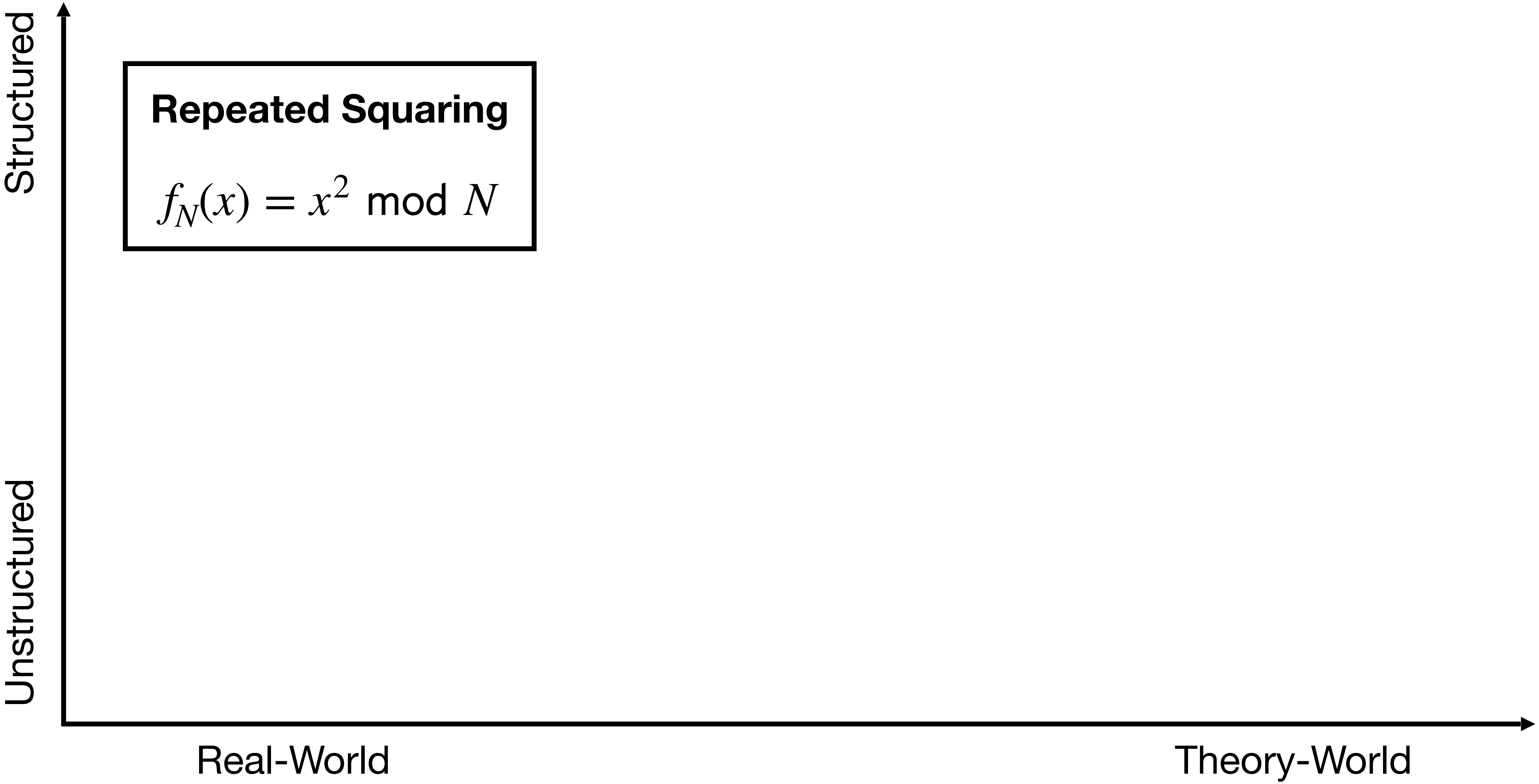


} T-depth

$NC \neq P$

Landscape of Sequential Problems

Landscape of Sequential Problems



Landscape of Sequential Problems

Structured

Repeated Squaring

$f_N(x) = x^2 \text{ mod } N$

Unstructured

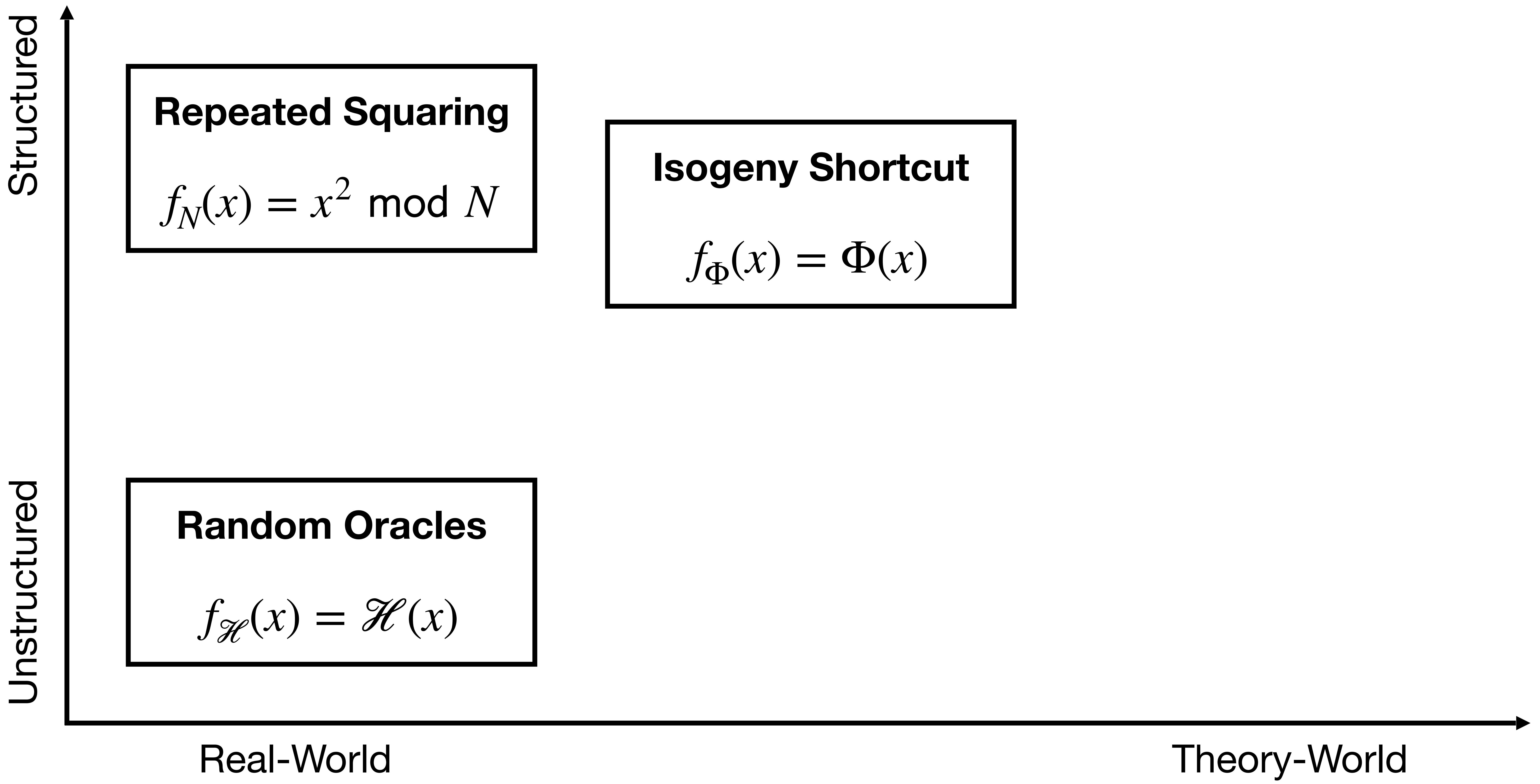
Random Oracles

$f_{\mathscr{H}}(x) = \mathscr{H}(x)$

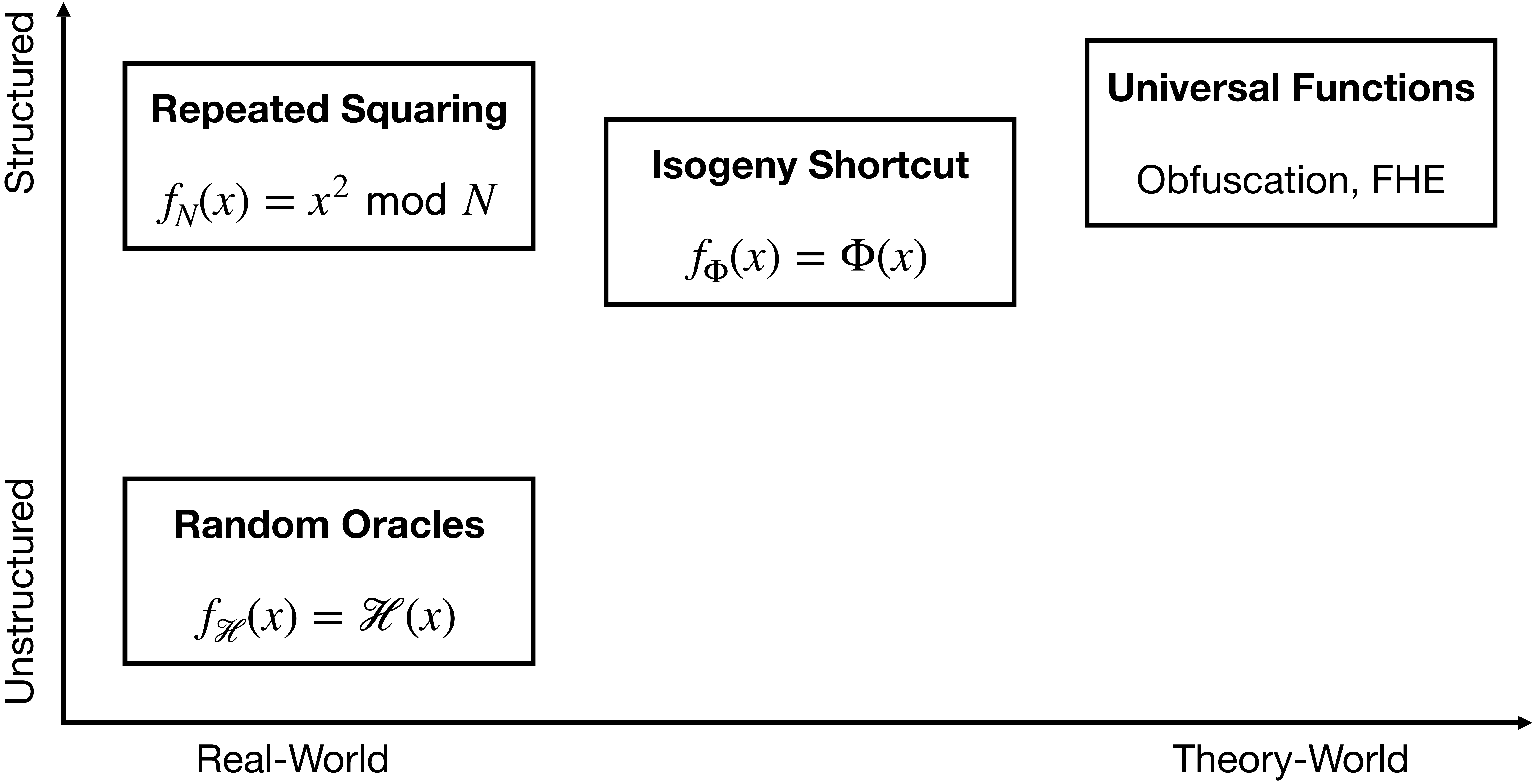
Real-World

Theory-World

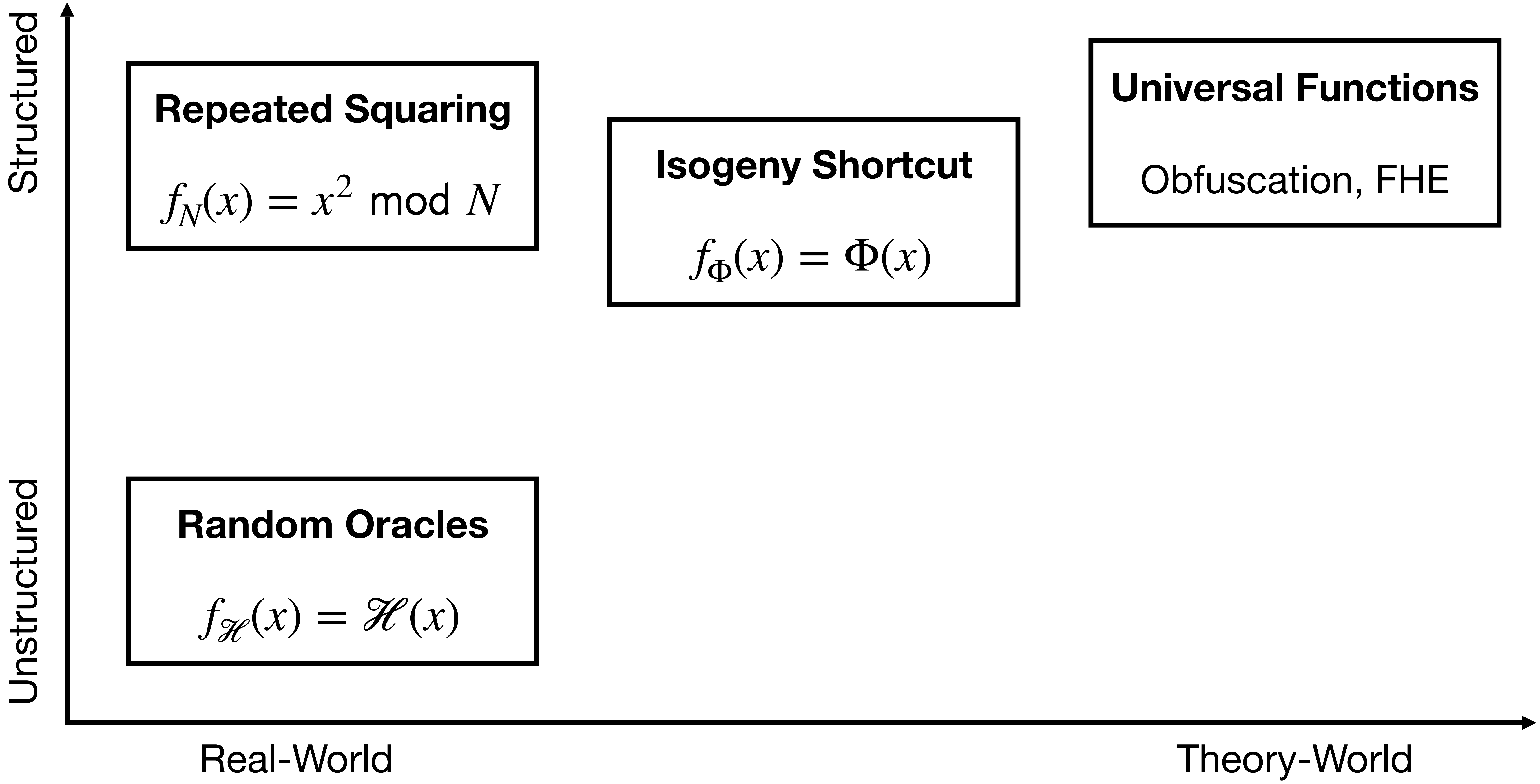
Landscape of Sequential Problems



Landscape of Sequential Problems



Enter Quantum Computing



Enter Quantum Computing

Structured

Unstructured

Repeated Squaring

$f_N(x) = x^2 \bmod N$

Isogeny Shortcut

$f_\Phi(x) = \Phi(x)$

Universal Functions

Obfuscation, FHE

Random Oracles

$f_{\mathscr{H}}(x) = \mathscr{H}(x)$

Real-World

Theory-World

Enter Quantum Computing

Structured

Unstructured

Universal Functions

Obfuscation, FHE

Isogeny Shortcut

$$f_{\Phi}(x) = \Phi(x)$$

Random Oracles

$$f_{\mathscr{H}}(x) = \mathscr{H}(x)$$

Real-World

Theory-World

Enter Quantum Computing

Structured

Unstructured

Universal Functions

Obfuscation, FHE

Random Oracles

$f_{\mathscr{H}}(x) = \mathscr{H}(x)$

Isogeny Shortcut

$f_{\Phi}(x) = \Phi(x)$

Real-World

Theory-World

Can we construct efficient *post-quantum* timed cryptography?

Our Results

Our Results

- A new candidate “lattice-based” sequential function

Our Results

- A new candidate “lattice-based” sequential function
    - Evidence of sequentiality

Our Results

- A new candidate “lattice-based” sequential function
  - Evidence of sequentiality
  - Cryptanalysis

Our Results

- A new candidate “lattice-based” sequential function
  - Evidence of sequentiality
  - Cryptanalysis
- Application: Simple proof of sequential work

Our Results

- A new candidate “lattice-based” sequential function
  - Evidence of sequentiality
  - Cryptanalysis
- Application: Simple proof of sequential work
  - Protocol & soundness analysis

Our Results

- A new candidate “lattice-based” sequential function
  - Evidence of sequentiality
  - Cryptanalysis
- Application: Simple proof of sequential work
  - Protocol & soundness analysis
- Open problems

A New Sequential Function

A New Sequential Function

$m \approx n \cdot \log q$

- Input: a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{x} \in \mathbb{Z}_q^n$

A New Sequential Function

$m \approx n \cdot \log q$

- Input: a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{x} \in \mathbb{Z}_q^n$
- Compute:

A New Sequential Function

$m \approx n \cdot \log q$

- Input: a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{x} \in \mathbb{Z}_q^n$
- Compute:
  - The binary decomposition $\mathbf{u} = \mathbf{G}^{-1}(\mathbf{x})$

A New Sequential Function

$m \approx n \cdot \log q$

- Input: a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{x} \in \mathbb{Z}_q^n$
- Compute:
  - The binary decomposition $\mathbf{u} = \mathbf{G}^{-1}(\mathbf{x})$
  - Return $\mathbf{A} \cdot \mathbf{u} \bmod q$

A New Sequential Function

$m \approx n \cdot \log q$

- Input: a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{x} \in \mathbb{Z}_q^n$
- Compute:
  - The binary decomposition $\mathbf{u} = \mathbf{G}^{-1}(\mathbf{x})$
  - Return $\mathbf{A} \cdot \mathbf{u} \mod q$
- Feed the output of the function as an input T times

A New Sequential Function

$m \approx n \cdot \log q$

- Input: a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{x} \in \mathbb{Z}_q^n$
- Compute:
  - The binary decomposition $\mathbf{u} = \mathbf{G}^{-1}(\mathbf{x})$
  - Return $\mathbf{A} \cdot \mathbf{u}$ mod q
- Feed the output of the function as an input T times

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{y} = \mathbf{A} \cdot \mathbf{G}^{-1}(\mathbf{x})$$

A New Sequential Function

$m \approx n \cdot \log q$

- Input: a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{x} \in \mathbb{Z}_q^n$
- Compute:
  - The binary decomposition $\mathbf{u} = \mathbf{G}^{-1}(\mathbf{x})$
  - Return $\mathbf{A} \cdot \mathbf{u}$ mod q
- Feed the output of the function as an input T times

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{y} = \mathbf{A} \cdot \mathbf{G}^{-1}(\mathbf{x}) \iff \begin{bmatrix} \mathbf{G} \\ \mathbf{A} \end{bmatrix} \cdot \mathbf{u} = \begin{bmatrix} \mathbf{x} \\ \mathbf{y} \end{bmatrix}$$

$$\mathbf{u} \in \{0,1\}^m$$

The Sequentiality Assumption

The Sequentiality Assumption

- For uniform $\mathbf{A}$ and $\mathbf{x}$, the T-fold recursive application of $f_{\mathbf{A}}$ is sequential

The Sequentiality Assumption

- For uniform $\mathbf{A}$ and $\mathbf{x}$, the T-fold recursive application of $f_{\mathbf{A}}$ is sequential
- In other words, it takes parallel time T to find $\mathbf{u}$ such that

The Sequentiality Assumption

- For uniform $\mathbf{A}$ and $\mathbf{x}$, the T-fold recursive application of $f_{\mathbf{A}}$ is sequential
- In other words, it takes parallel time T to find $\mathbf{u}$ such that

$$\begin{bmatrix} -\mathbf{G} & & & \\ \mathbf{A} & -\mathbf{G} & & \\ & \mathbf{A} & & \\ & & \ddots & \\ & & & -\mathbf{G} \\ & & & \mathbf{A} \end{bmatrix} \cdot \mathbf{u} = \begin{bmatrix} -\mathbf{x} \\ 0 \\ \vdots \\ 0 \\ \mathbf{y} \end{bmatrix} \qquad \mathbf{u} \in \{0,1\}^m$$

The Strong Sequentiality Assumption

- For uniform $\mathbf{A}$ and $\mathbf{x}$, the T-fold recursive application of $f_{\mathbf{A}}$ is sequential
- In other words, it takes parallel time T to find $\mathbf{u}$ such that

$$\begin{bmatrix} -\mathbf{G} & & & \\ \mathbf{A} & -\mathbf{G} & & \\ & \mathbf{A} & & \\ & & \ddots & \\ & & & -\mathbf{G} \\ & & & \mathbf{A} \end{bmatrix} \cdot \mathbf{u} = \begin{bmatrix} -\mathbf{x} \\ 0 \\ \vdots \\ 0 \\ \mathbf{y} \end{bmatrix} \qquad \mathbf{u} \approx \text{small}$$

Evidence of Sequentiality

Evidence of Sequentiality

- The function $f_{\mathbf{A}}$ is collision-resistant

Evidence of Sequentiality

- The function $f_{\mathbf{A}}$ is collision-resistant
  - Simple reduction to the SIS problem w.r.t. $\mathbf{A}$

Evidence of Sequentiality

- The function $f_{\mathbf{A}}$ is collision-resistant
  - Simple reduction to the SIS problem w.r.t. $\mathbf{A}$

- The function $f_{\mathbf{A}}$ is uniformity-preserving (assuming LWE)

Evidence of Sequentiality

- The function $f_{\mathbf{A}}$ is collision-resistant
  - Simple reduction to the SIS problem w.r.t. $\mathbf{A}$

- The function $f_{\mathbf{A}}$ is uniformity-preserving (assuming LWE)
  - $\{\mathbf{y} : \mathbf{y} \leftarrow \mathbb{Z}_q^n\} \approx \{\mathbf{A}(\mathbf{x}) : \mathbf{x} \leftarrow \mathbb{Z}_q^n\}$

Evidence of Sequentiality

- The function $f_{\mathbf{A}}$ is collision-resistant
  - Simple reduction to the SIS problem w.r.t. $\mathbf{A}$
- The function $f_{\mathbf{A}}$ is uniformity-preserving (assuming LWE)
  - $\{\mathbf{y} : \mathbf{y} \leftarrow \mathbb{Z}_q^n\} \approx \{\mathbf{A}(\mathbf{x}) : \mathbf{x} \leftarrow \mathbb{Z}_q^n\}$
  - Consequently, so is it's T-fold repetition

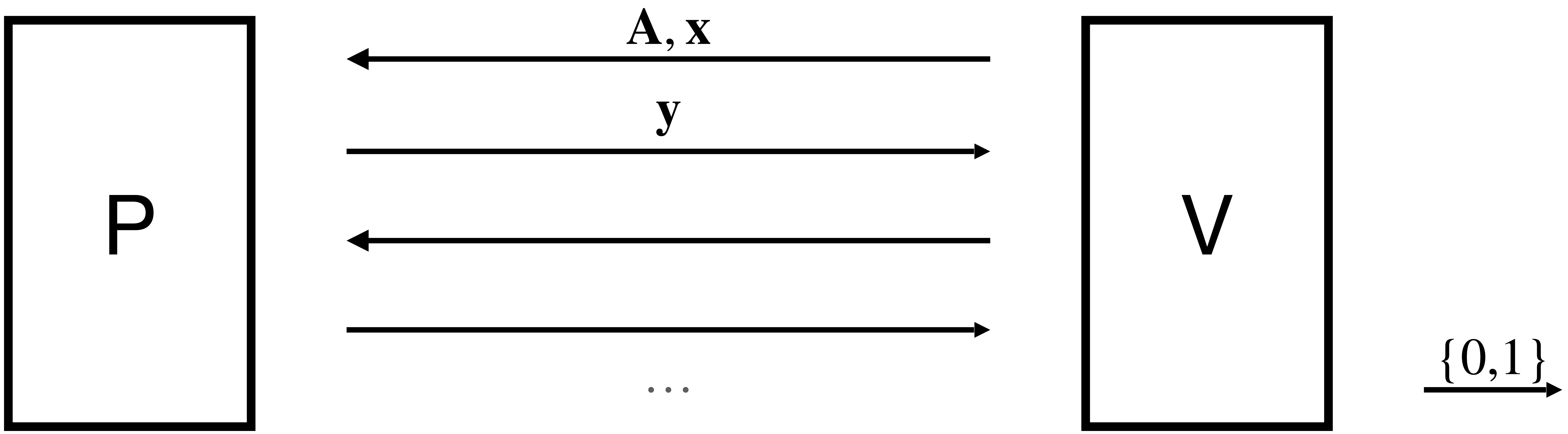
Evidence of Sequentiality

- The function $f_{\mathbf{A}}$ is collision-resistant
  - Simple reduction to the SIS problem w.r.t. $\mathbf{A}$

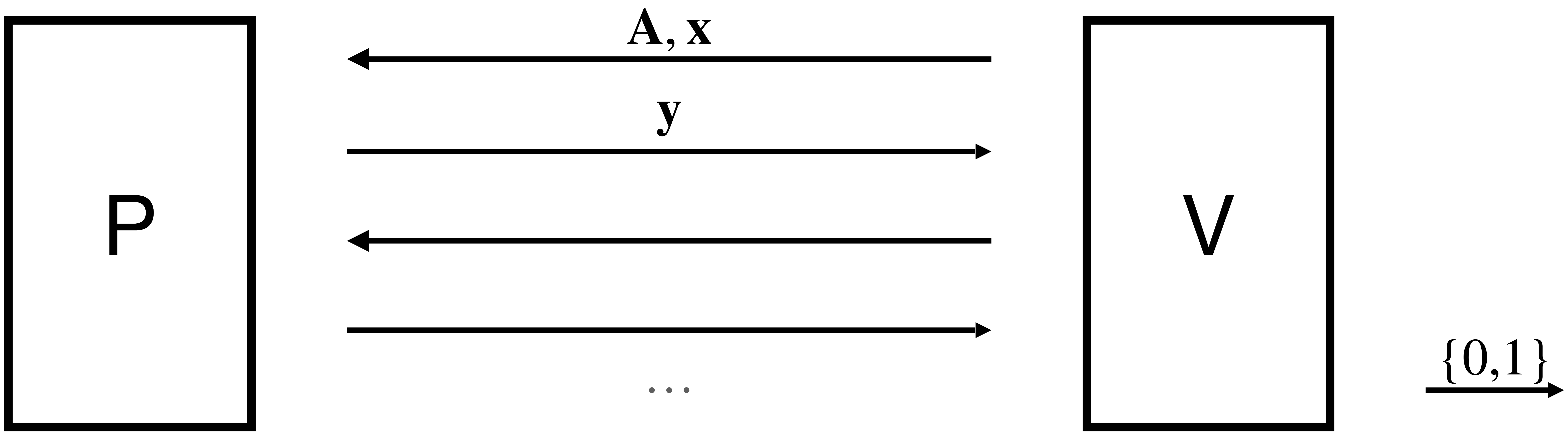
- The function $f_{\mathbf{A}}$ is uniformity-preserving (assuming LWE)
  - $\{\mathbf{y} : \mathbf{y} \leftarrow \mathbb{Z}_q^n\} \approx \{\mathbf{A}(\mathbf{x}) : \mathbf{x} \leftarrow \mathbb{Z}_q^n\}$
  - Consequently, so is it's T-fold repetition

- More heuristic evidence & cryptanalysis (see paper)

Proofs of Sequential Work

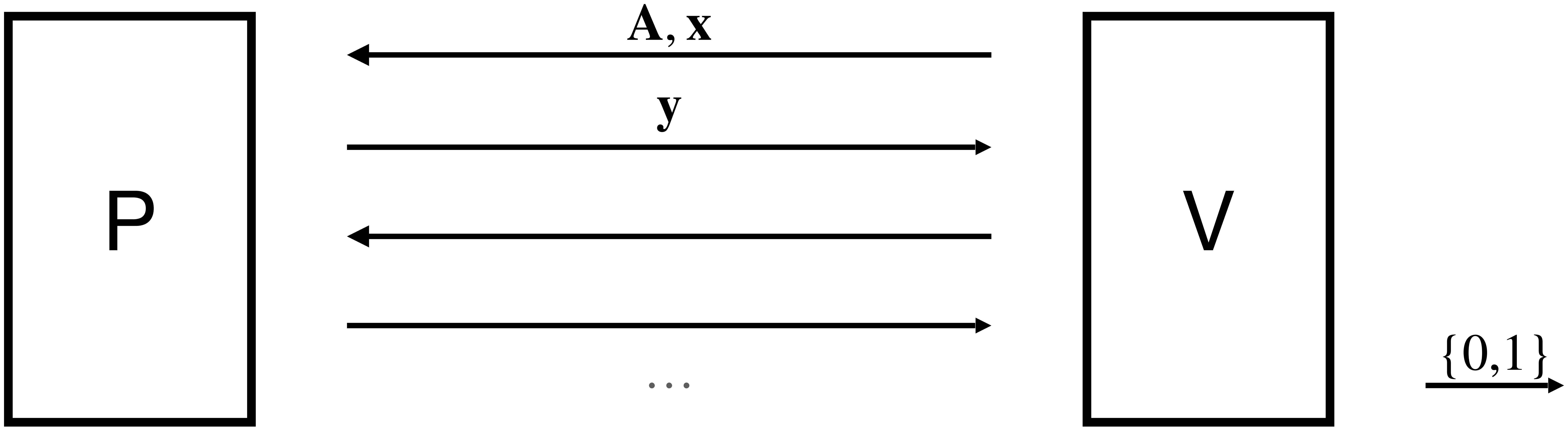


Proofs of Sequential Work



- Succinctness: V’s work is ~logT

Proofs of Sequential Work



- Succinctness: V's work is ~logT
- Soundness: No prover of depth << T can pass the verification

Self-Symmetry

Self-Symmetry

$$\mathbf{A}_T = \begin{bmatrix} -\mathbf{G} & & & & \\ \mathbf{A} & -\mathbf{G} & & & \\ & \mathbf{A} & & & \\ & & \ddots & & \\ & & & & -\mathbf{G} \\ & & & & \mathbf{A} \end{bmatrix}$$

Self-Symmetry

$$\mathbf{A}_T = \begin{bmatrix} -\mathbf{G} & & & \\ \mathbf{A} & -\mathbf{G} & & \\ & \mathbf{A} & & \\ & & \ddots & \\ & & & -\mathbf{G} \\ & & & \mathbf{A} \end{bmatrix} = \begin{bmatrix} \mathbf{A}_t & & \\ & -\mathbf{G} & \\ & \mathbf{A} & \\ & & \mathbf{A}_t \end{bmatrix}$$

$$T = 2t + 1$$

The Protocol (Step 1)

The Protocol (Step 1)

- P sends the intermediate value $\mathbf{u}_t$ to V

The Protocol (Step 1)

- P sends the intermediate value $\mathbf{u}_t$ to V
- V checks that $\mathbf{u}_t$ is small

The Protocol (Step 1)

- P sends the intermediate value $\mathbf{u}_t$ to V
- V checks that $\mathbf{u}_t$ is small
- The new relation is:

The Protocol (Step 1)

- P sends the intermediate value $\mathbf{u}_t$ to V
- V checks that $\mathbf{u}_t$ is small
- The new relation is:

$$\mathbf{A}_t \cdot \begin{bmatrix} \mathbf{u}_0 & \mathbf{u}_{t+1} \\ \vdots & \vdots \\ \mathbf{u}_{t-1} & \mathbf{u}_{T-1} \end{bmatrix} = \begin{bmatrix} -\mathbf{x}_0 & -\mathbf{A} \cdot \mathbf{u}_t \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \\ -\mathbf{G} \cdot \mathbf{u}_t & \mathbf{x}_T \end{bmatrix}$$

The Protocol (Step 2)

The Protocol (Step 2)

- V sends a small r to P

The Protocol (Step 2)

- V sends a small r to P
- The new relation is:

The Protocol (Step 2)

- V sends a small r to P
- The new relation is:

$$\mathbf{A}_t \cdot \begin{bmatrix} \mathbf{u}_0 + \mathbf{u}_{t+1} \cdot r \\ \vdots \\ \mathbf{u}_{t-1} + \mathbf{u}_{T-1} \cdot r \end{bmatrix} = \begin{bmatrix} -\mathbf{x}_0 - \mathbf{A} \cdot \mathbf{u}_t \cdot r \\ 0 \\ \vdots \\ 0 \\ -\mathbf{G} \cdot \mathbf{u}_t + \mathbf{x}_T \cdot r \end{bmatrix}$$

The Protocol (Step 2)

- V sends a small r to P
- The new relation is:

$$\mathbf{A}_t \cdot \begin{bmatrix} \mathbf{u}_0 + \mathbf{u}_{t+1} \cdot r \\ \vdots \\ \mathbf{u}_{t-1} + \mathbf{u}_{T-1} \cdot r \end{bmatrix} = \begin{bmatrix} -\mathbf{x}_0 - \mathbf{A} \cdot \mathbf{u}_t \cdot r \\ 0 \\ \vdots \\ 0 \\ -\mathbf{G} \cdot \mathbf{u}_t + \mathbf{x}_T \cdot r \end{bmatrix}$$

- Dimension halved, recurse!

The Protocol (Step 2)

- V sends a small r to P
- The new relation is:

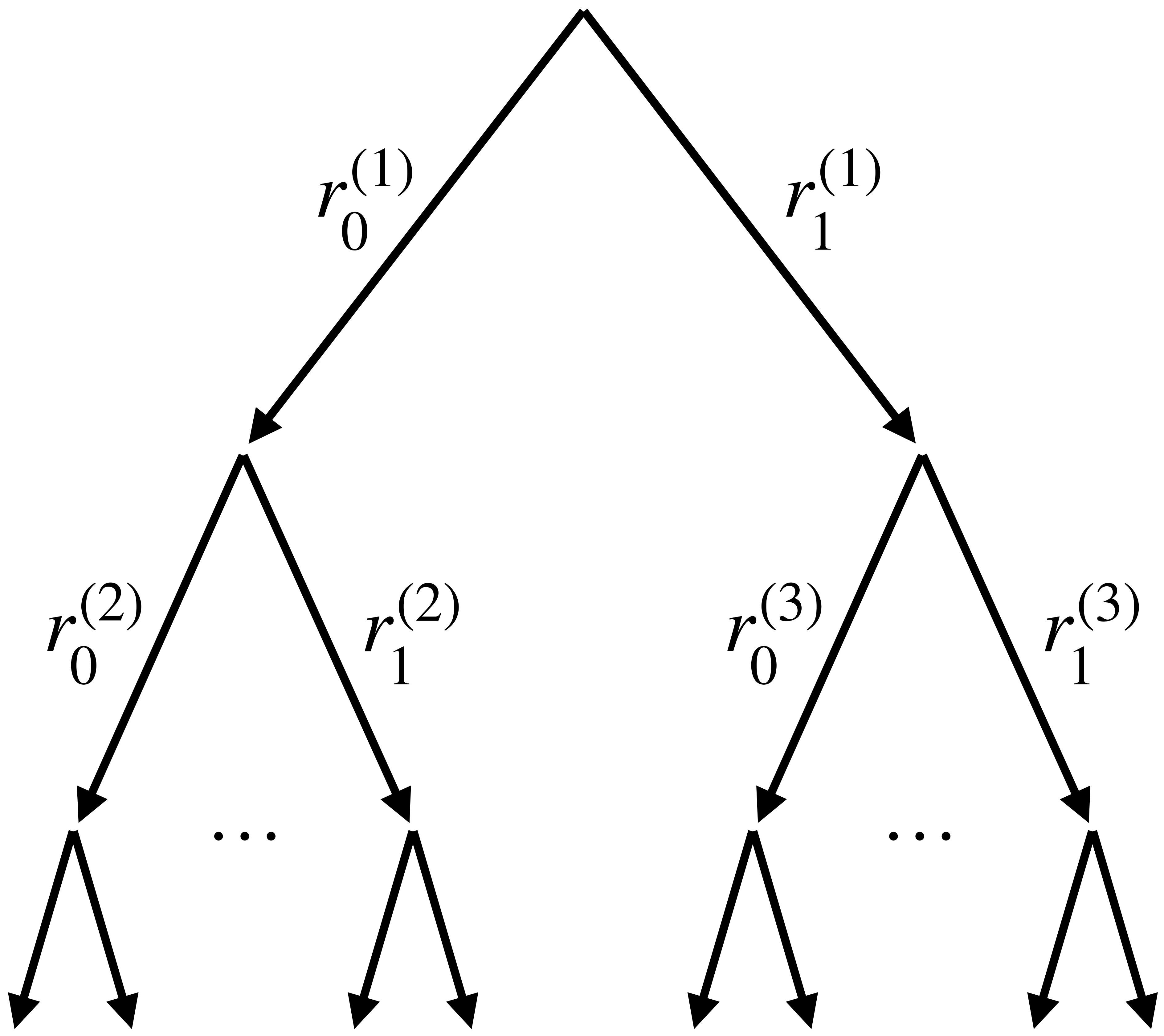
$$\mathbf{A}_t \cdot \begin{bmatrix} \mathbf{u}_0 + \mathbf{u}_{t+1} \cdot r \\ \vdots \\ \mathbf{u}_{t-1} + \mathbf{u}_{T-1} \cdot r \end{bmatrix} = \begin{bmatrix} -\mathbf{x}_0 - \mathbf{A} \cdot \mathbf{u}_t \cdot r \\ 0 \\ \vdots \\ 0 \\ -\mathbf{G} \cdot \mathbf{u}_t + \mathbf{x}_T \cdot r \end{bmatrix}$$

- Dimension halved, recurse!
- Verifier's runtime ~log(T)

Soundness

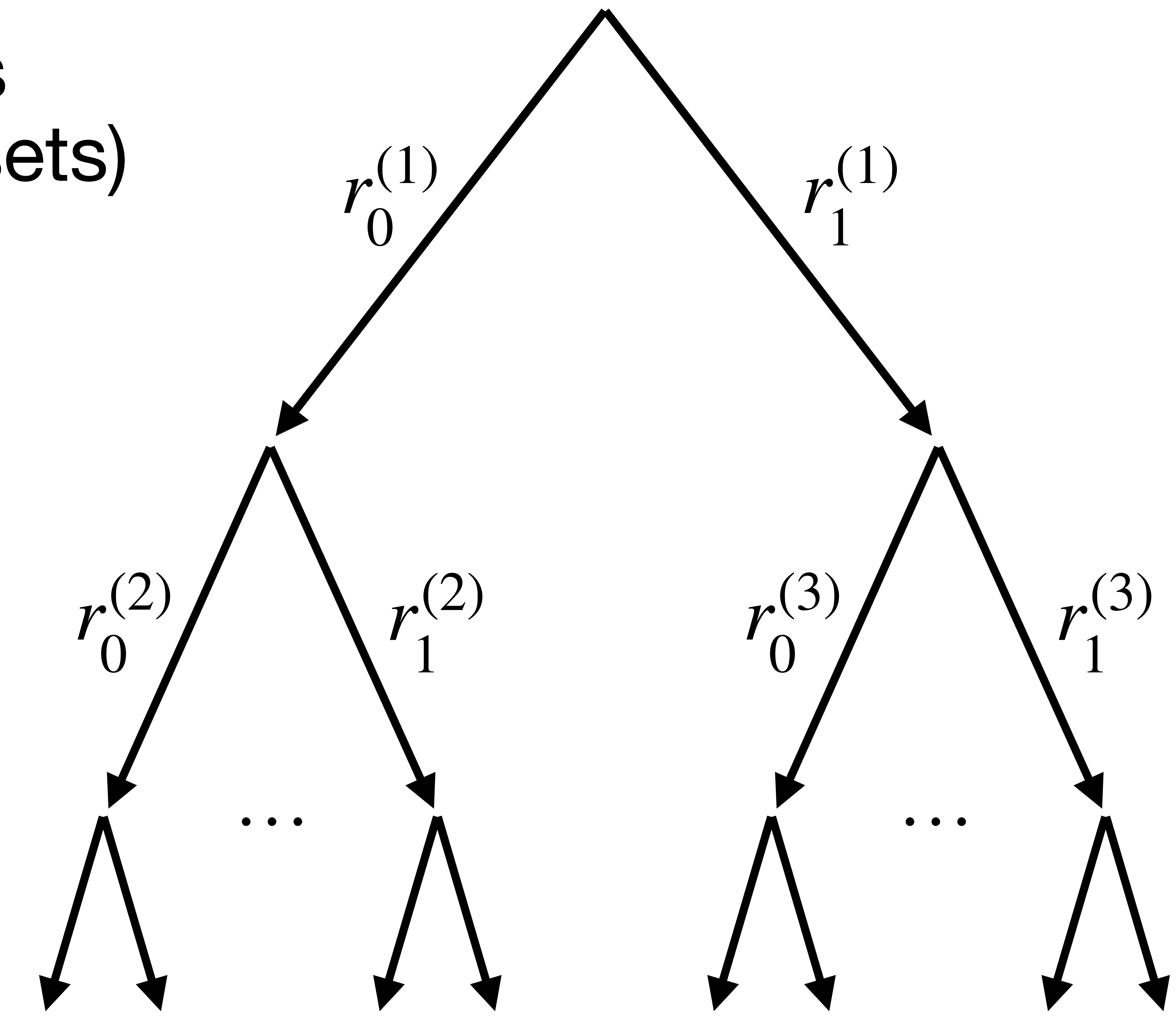
Soundness

- (2, …, 2)-special soundness: Given a binary tree of accepting transcripts, one can recover a valid witness



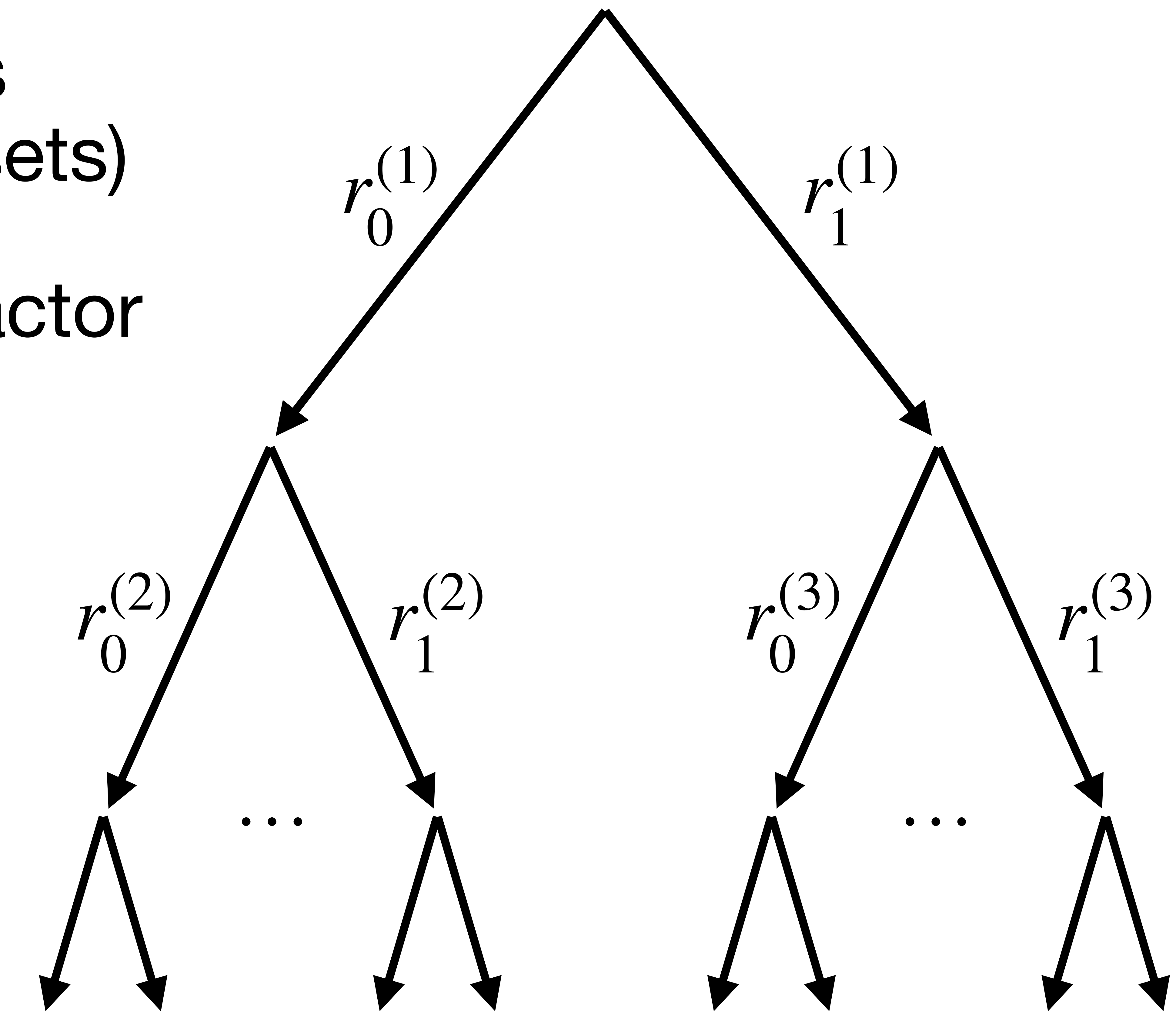
Soundness

- (2, …, 2)-special soundness: Given a binary tree of accepting transcripts, one can recover a valid witness
  - Can be shown if we sample the challenges from the appropriate domain (subtractive sets)



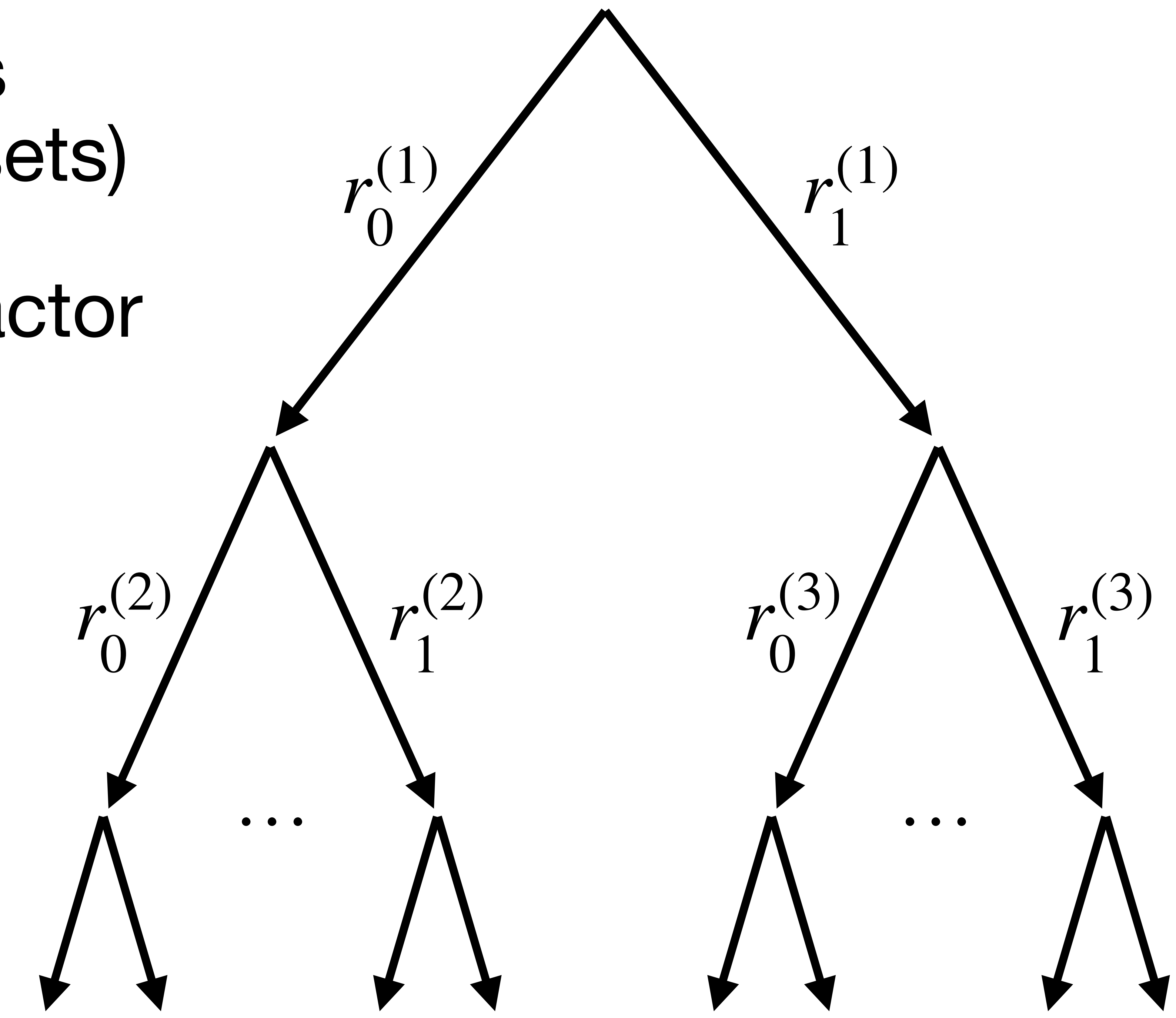
Soundness

- (2, …, 2)-special soundness: Given a binary tree of accepting transcripts, one can recover a valid witness
    - Can be shown if we sample the challenges from the appropriate domain (subtractive sets)
- [AF'22] There exists a depth-preserving extractor for the parallel-repeated protocol



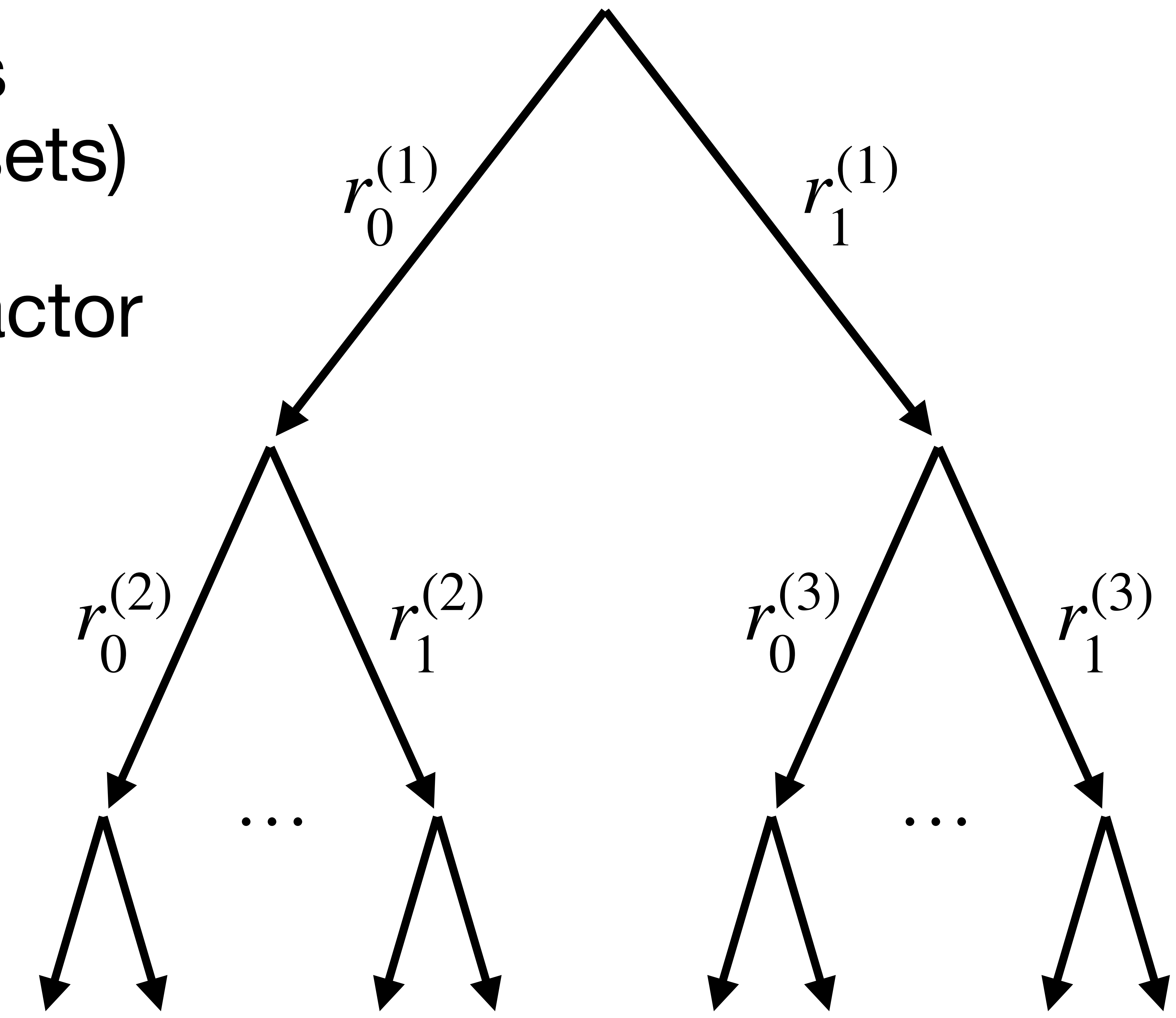
Soundness

- (2, …, 2)-special soundness: Given a binary tree of accepting transcripts, one can recover a valid witness
    - Can be shown if we sample the challenges from the appropriate domain (subtractive sets)
- [AF'22] There exists a depth-preserving extractor for the parallel-repeated protocol
- Can extract a valid transcript in time o(T)



Soundness

- (2, …, 2)-special soundness: Given a binary tree of accepting transcripts, one can recover a valid witness
    - Can be shown if we sample the challenges from the appropriate domain (subtractive sets)
- [AF'22] There exists a depth-preserving extractor for the parallel-repeated protocol
- Can extract a valid transcript in time o(T)
    - Contradiction!



Open Problems

Open Problems

- Efficient “lattice-based” VDF?

Open Problems

- Efficient “lattice-based” VDF?
  - Candidate construction: Valerio’s talk!

Open Problems

- Efficient “lattice-based” VDF?
  - Candidate construction: Valerio’s talk!

- More evidence of sequentiality?

Open Problems

- Efficient “lattice-based” VDF?
  - Candidate construction: Valerio’s talk!
- More evidence of sequentiality?
- More applications?

Open Problems

- Efficient “lattice-based” VDF?
  - Candidate construction: Valerio’s talk!
- More evidence of sequentiality?
- More applications?
- Post-quantum security?

Open Problems

- Efficient “lattice-based” VDF?
  - Candidate construction: Valerio’s talk!
- More evidence of sequentiality?
- More applications?
- Post-quantum security?

Thank you!