Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Optimal Proof Systems for Complex Sets are Hard to Find

Fabian Egidy, Christian Glaßer

STACS 2025 Workshop, Jena, 03. March 2025

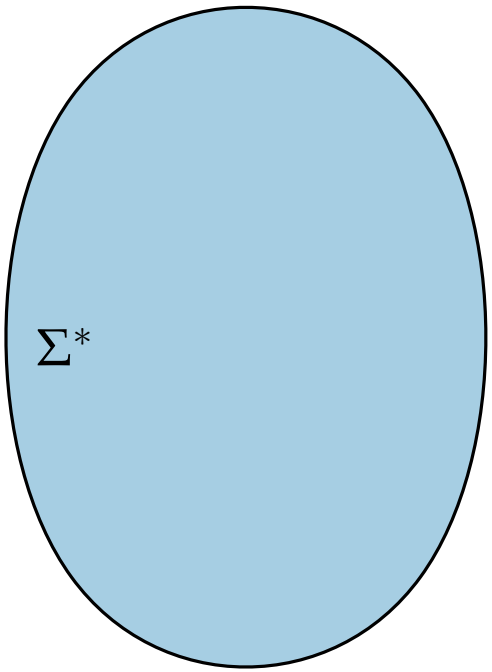
Proof Systems (Cook and Reckhow, 1979)

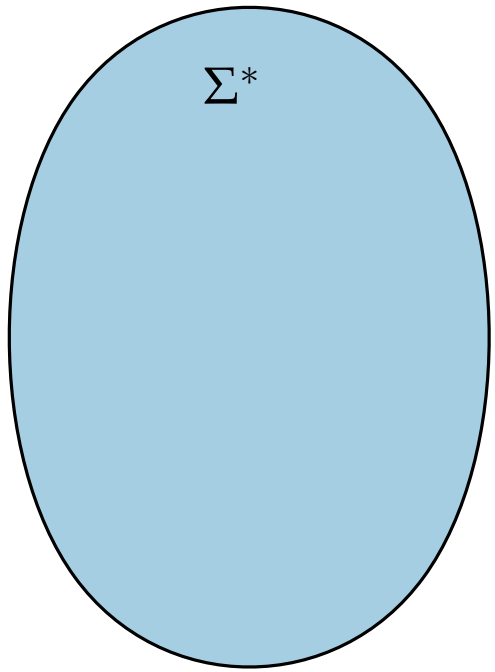
Proof Systems (Cook and Reckhow, 1979)

A function $f \in \mathrm{FP}$ is called a **proof system** for ran_f

Proof Systems (Cook and Reckhow, 1979)

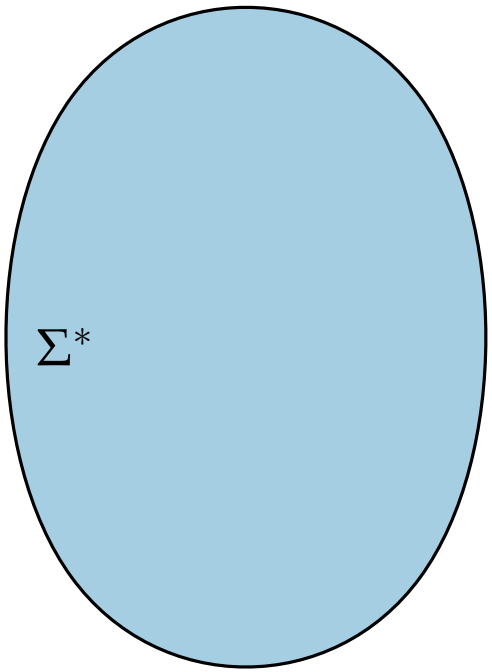
A function $f \in \mathrm{FP}$ is called a **proof system** for ran_f

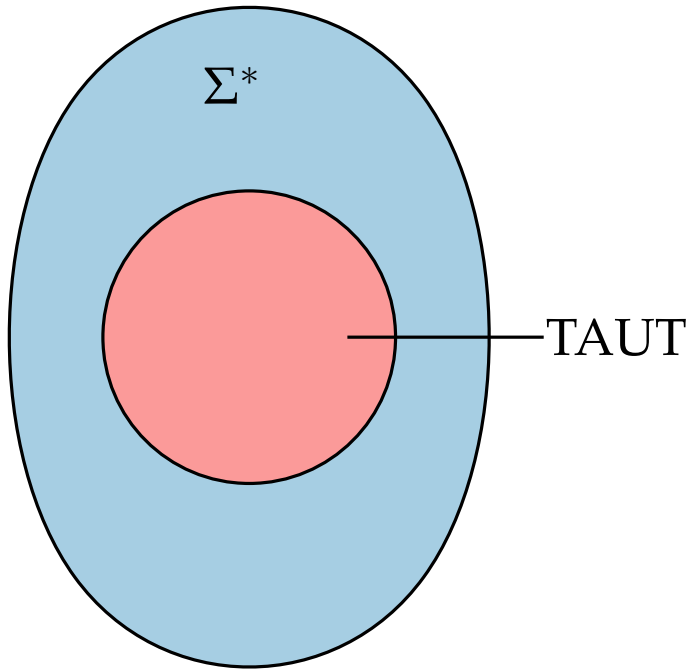




Proof Systems (Cook and Reckhow, 1979)

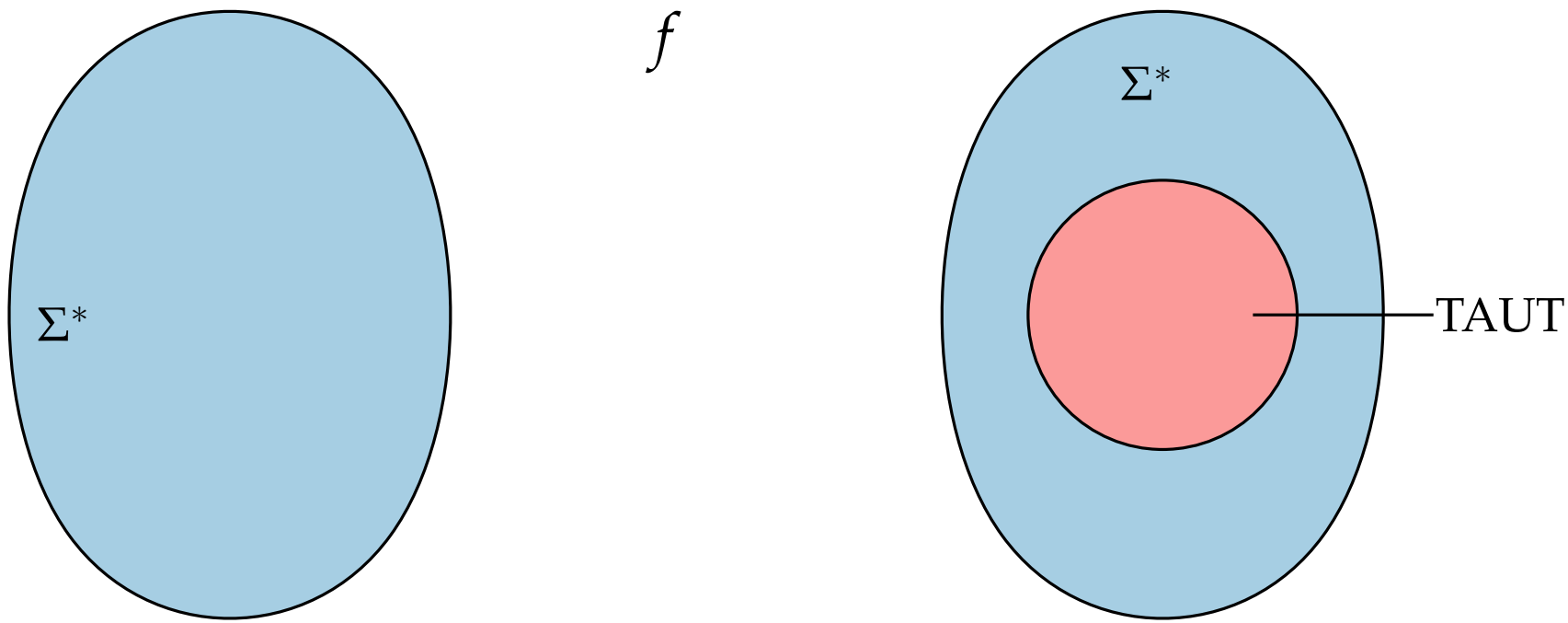
A function $f \in \mathrm{FP}$ is called a **proof system** for ran_f





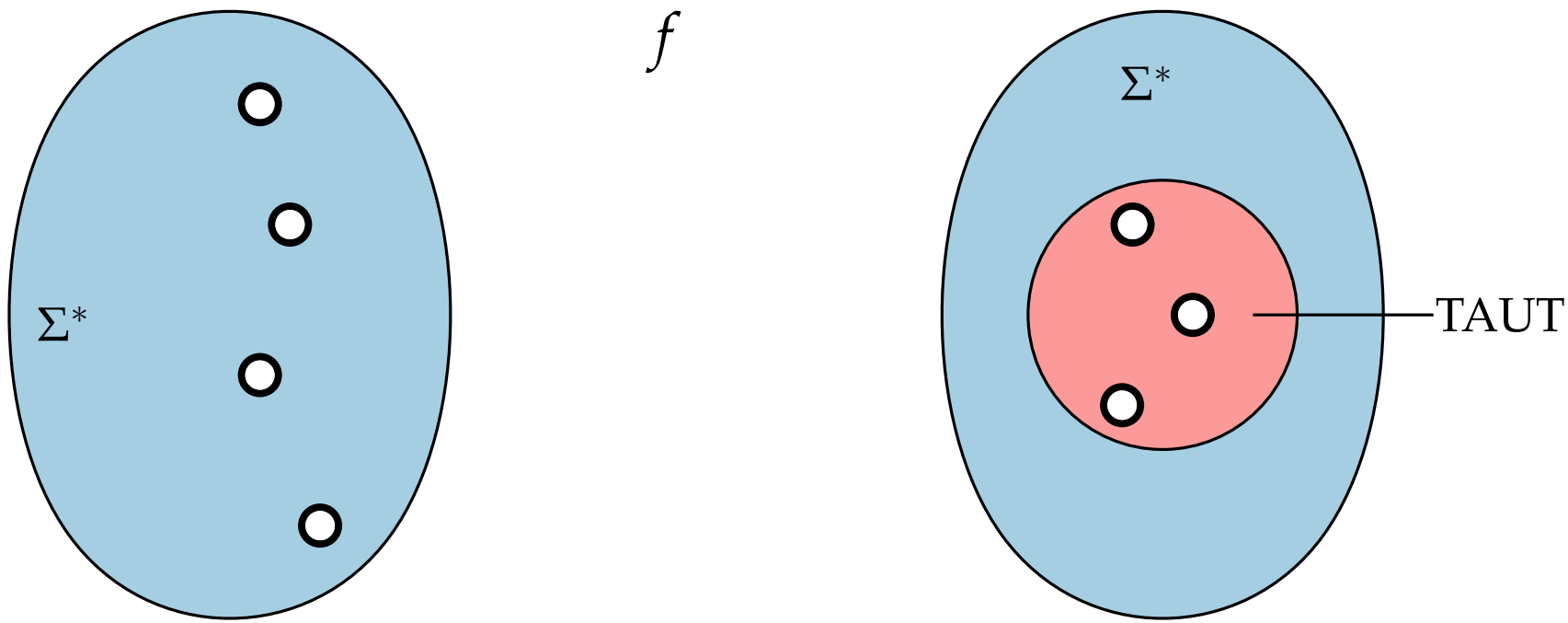
Proof Systems (Cook and Reckhow, 1979)

A function $f \in \mathrm{FP}$ is called a **proof system** for ran_f



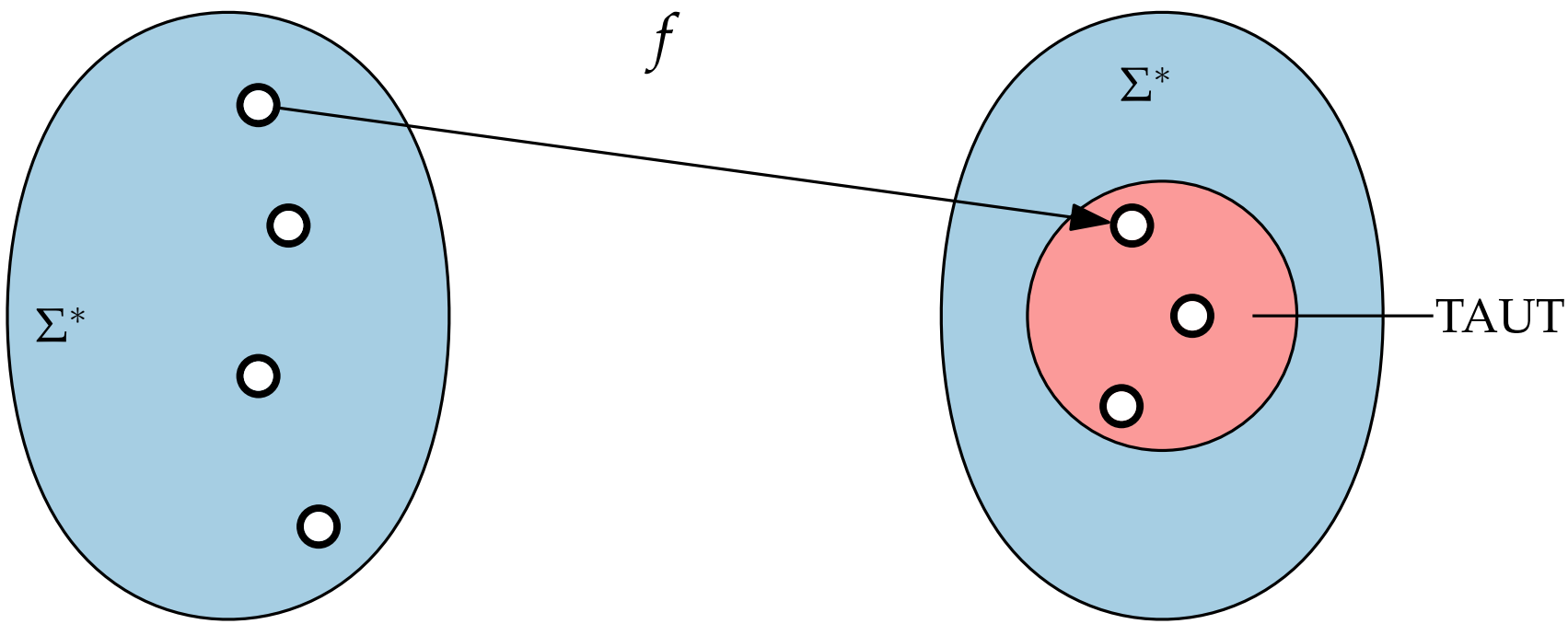
Proof Systems (Cook and Reckhow, 1979)

A function $f \in \mathrm{FP}$ is called a **proof system** for ran_f



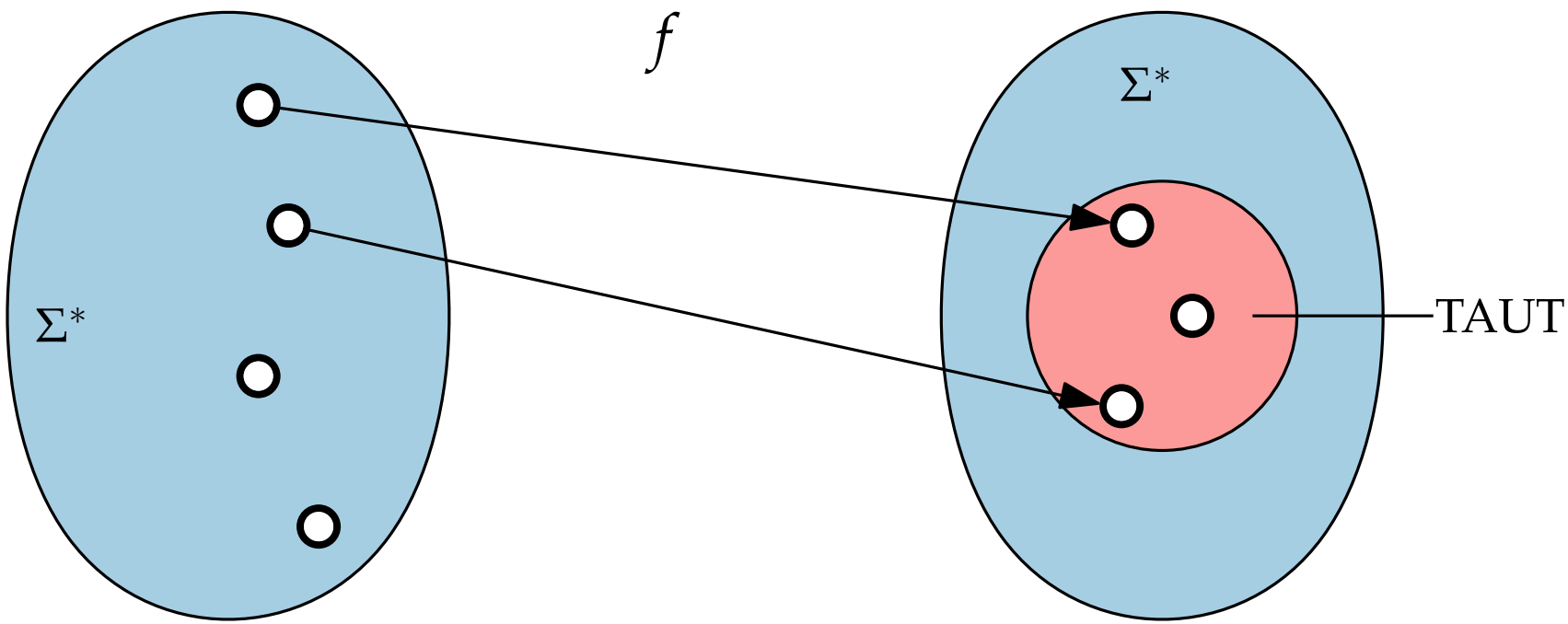
Proof Systems (Cook and Reckhow, 1979)

A function $f \in \mathrm{FP}$ is called a **proof system** for ran_f



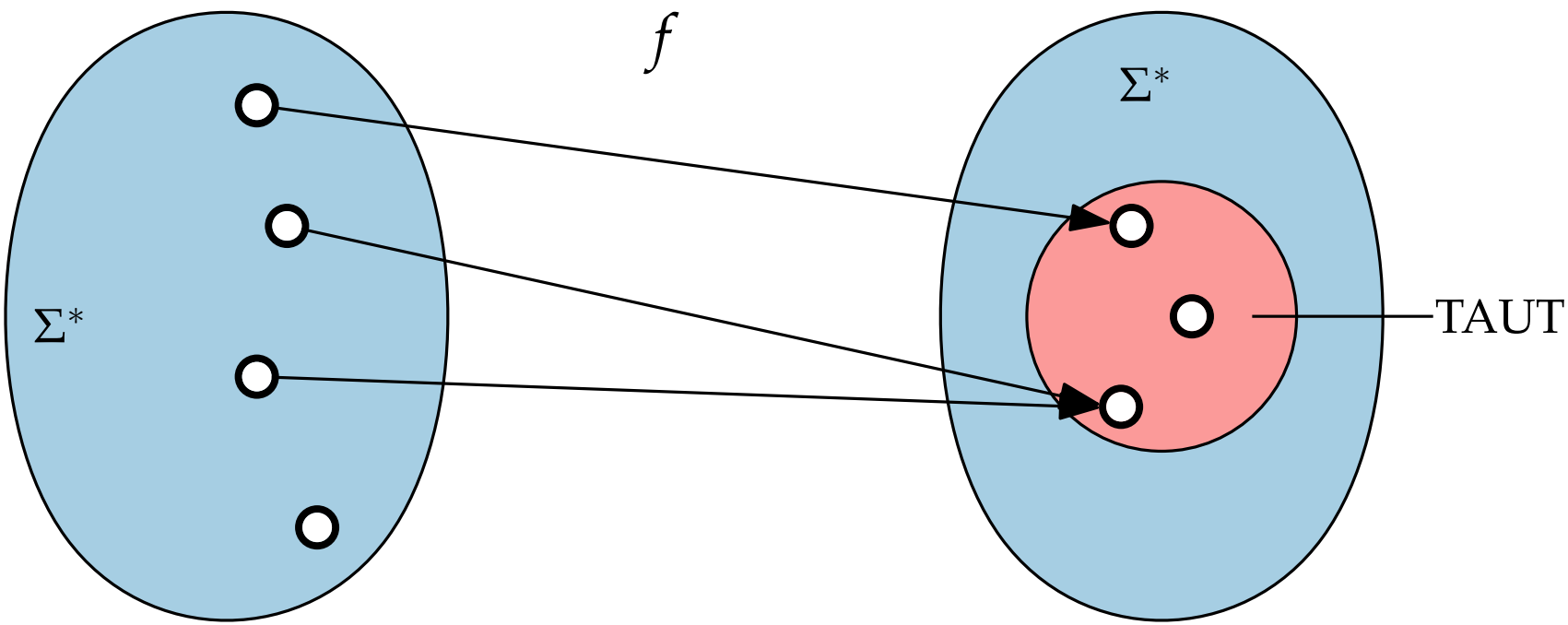
Proof Systems (Cook and Reckhow, 1979)

A function $f \in \mathrm{FP}$ is called a **proof system** for ran_f



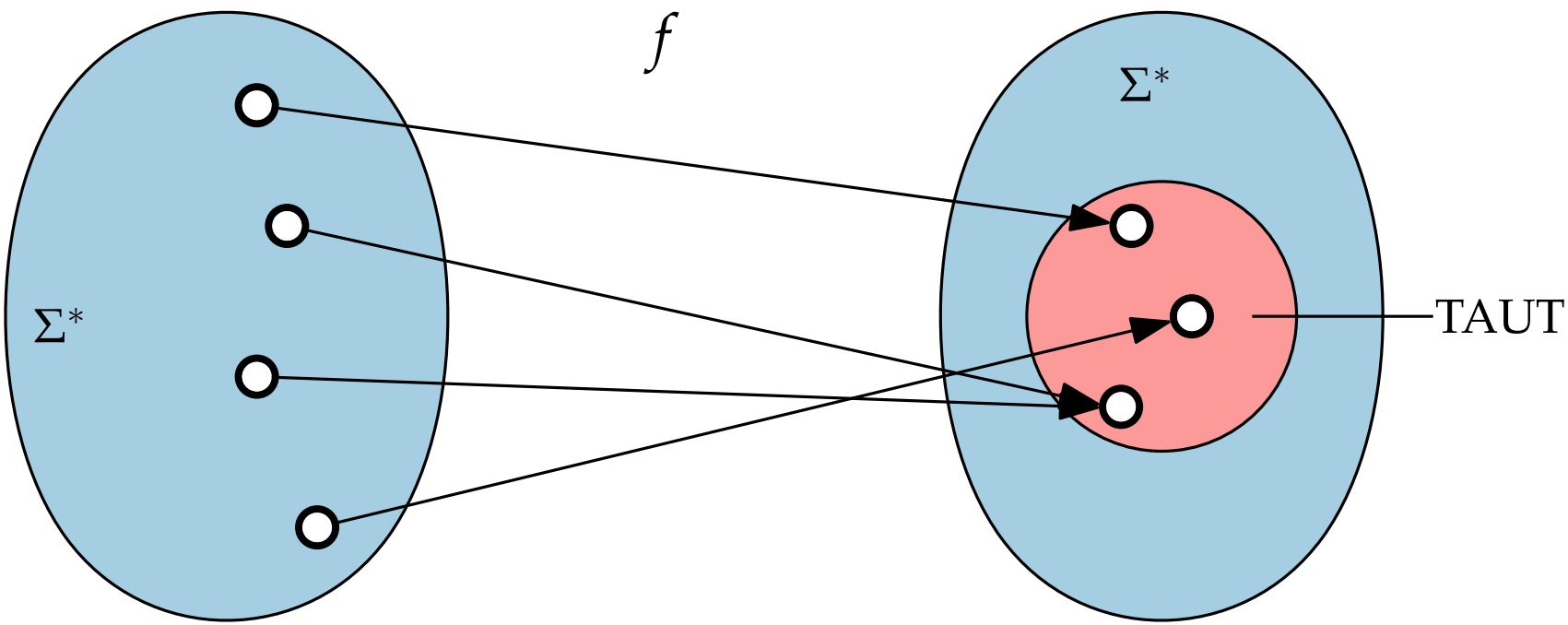
Proof Systems (Cook and Reckhow, 1979)

A function $f \in \mathrm{FP}$ is called a **proof system** for ran_f



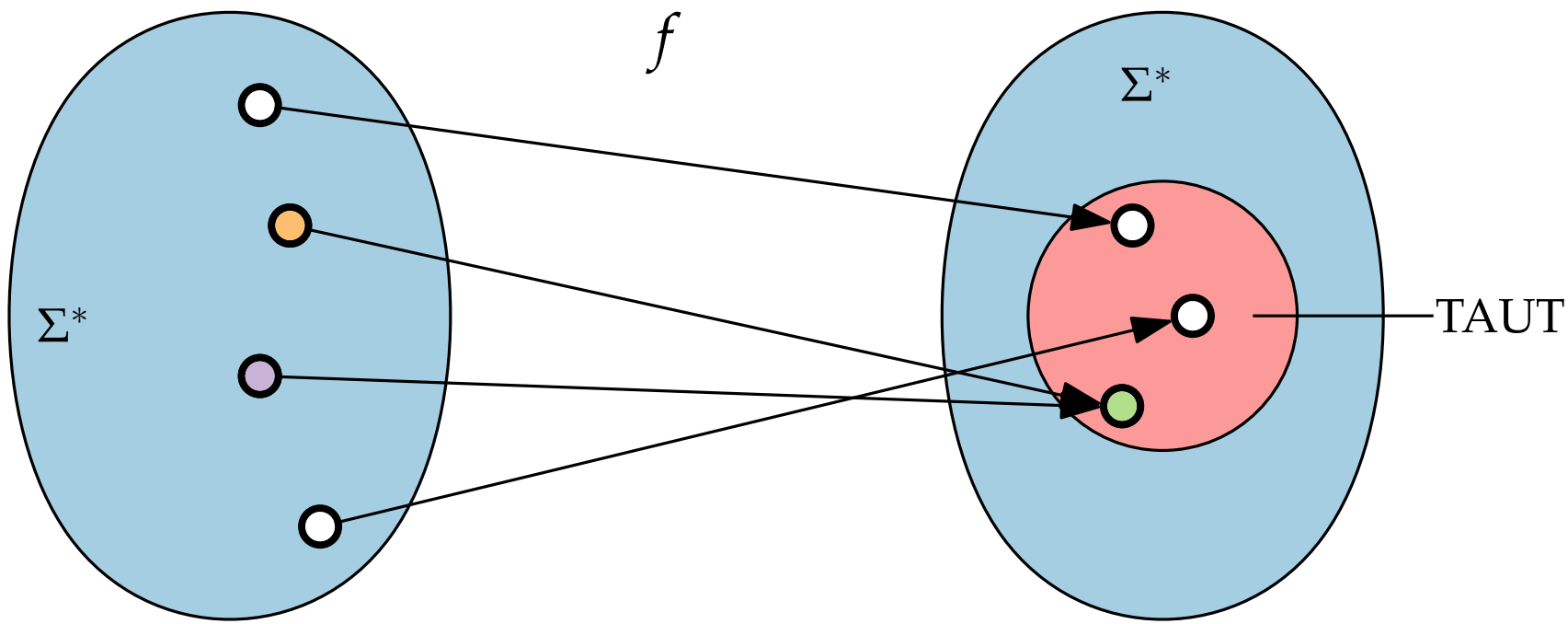
Proof Systems (Cook and Reckhow, 1979)

A function $f \in \mathrm{FP}$ is called a **proof system** for ran_f



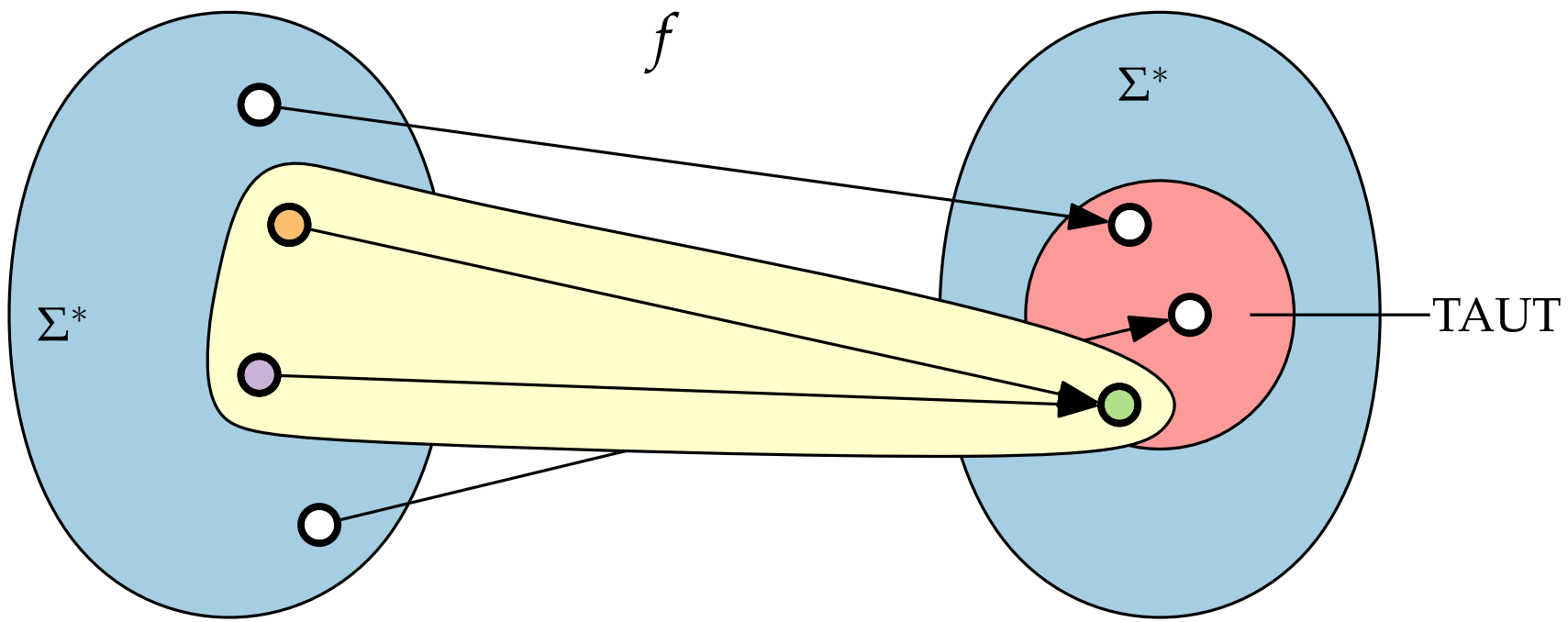
Proof Systems (Cook and Reckhow, 1979)

A function $f \in \mathrm{FP}$ is called a **proof system** for ran_f



Proof Systems (Cook and Reckhow, 1979)

A function $f \in \mathrm{FP}$ is called a **proof system** for ran_f



● and ● are proofs of the tautology ●

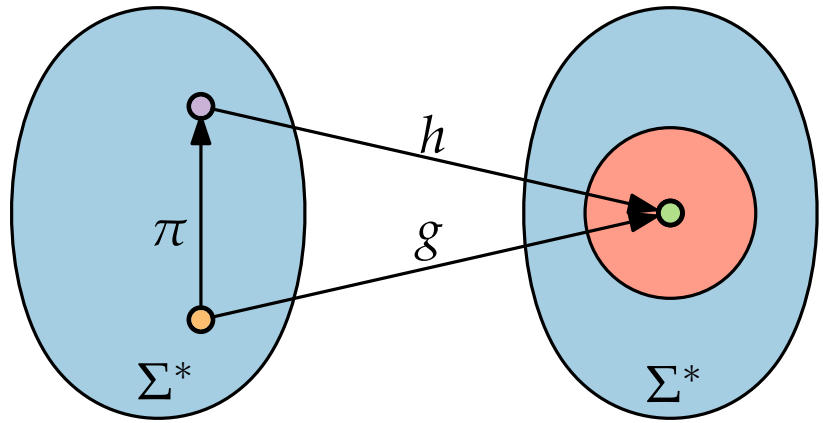
Simulation and Optimality

Simulation and Optimality

simulation:

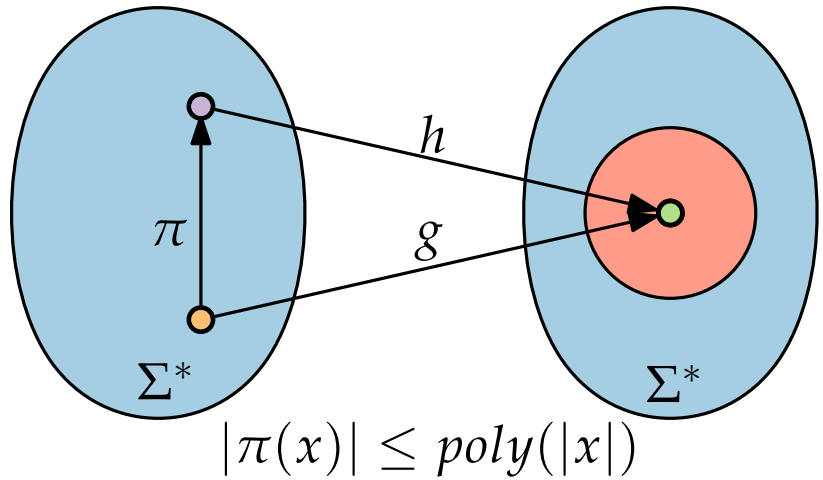
Simulation and Optimality

simulation:



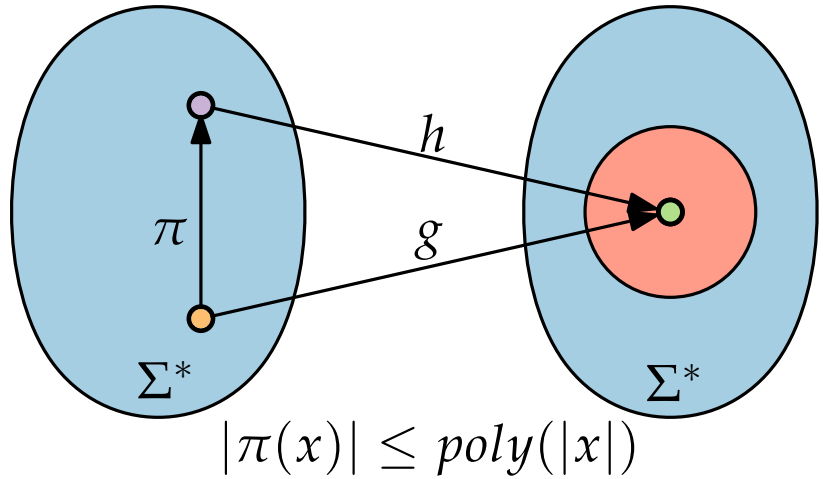
Simulation and Optimality

simulation:



Simulation and Optimality

simulation:



Def. A proof system for L that simulates all proof systems for L is an optimal proof system for L.

Existence of Optimal Proof Systems

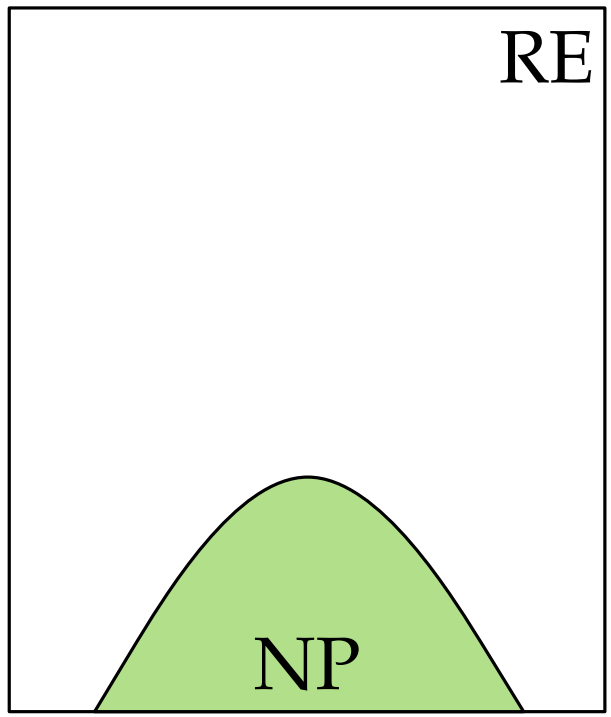
Existence of Optimal Proof Systems

Are there sets with optimal proof systems?

Existence of Optimal Proof Systems

Are there sets with optimal proof systems?

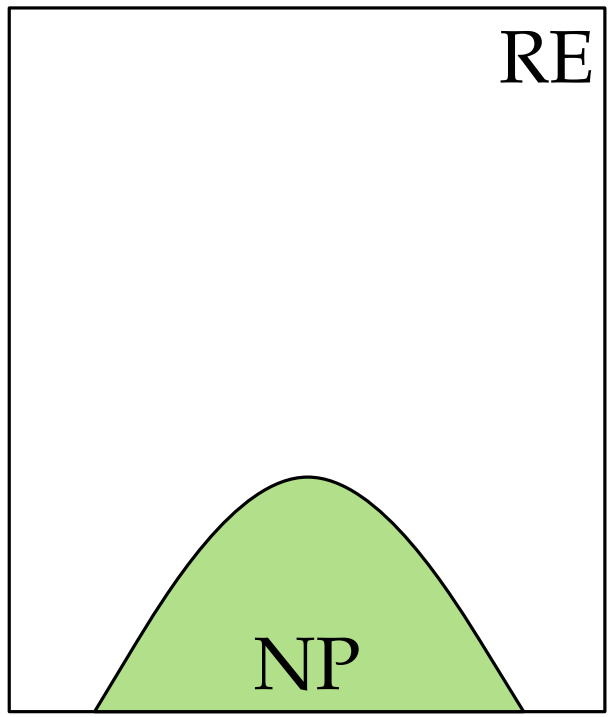
Thm. All sets in NP have optimal proof systems.



Existence of Optimal Proof Systems

Are there sets outside NP with optimal proof systems?

Thm. All sets in NP have optimal proof systems.

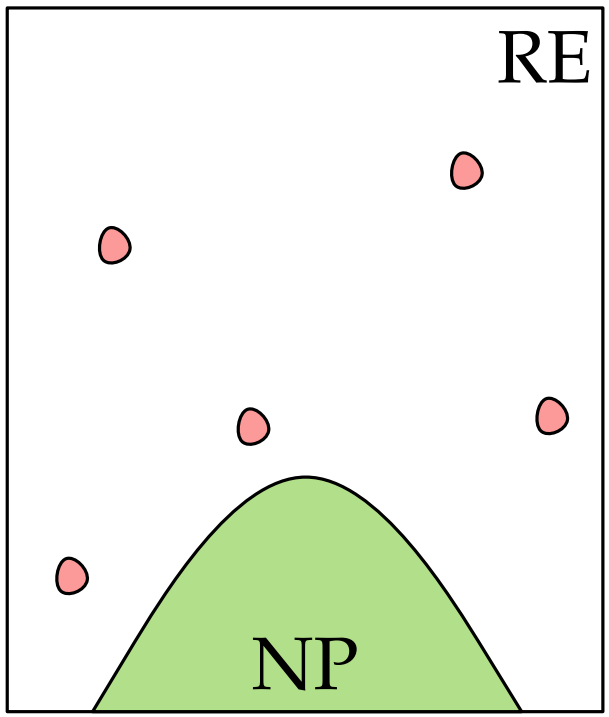


Existence of Optimal Proof Systems

Are there sets outside NP with optimal proof systems?

Thm. All sets in NP have optimal proof systems.

Thm. [Mes00]
coNE contains sets without optimal proof systems.

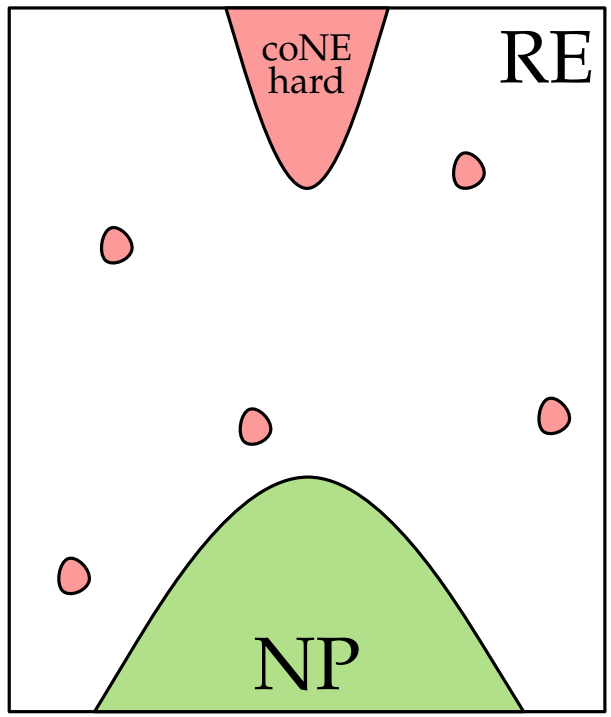


Existence of Optimal Proof Systems

Are there sets outside NP with optimal proof systems?

Thm. All sets in NP have optimal proof systems.

Thm. [Mes00]
coNE contains sets without optimal proof systems.

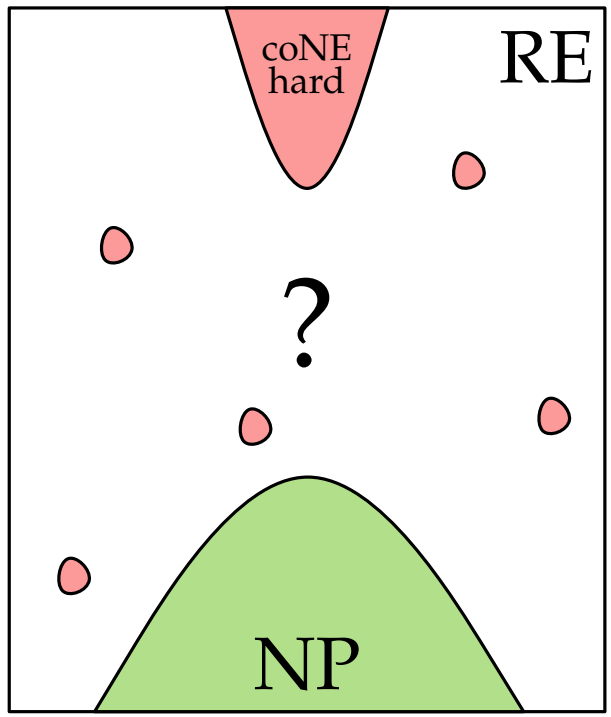


Existence of Optimal Proof Systems

Are there sets outside NP with optimal proof systems?

Thm. All sets in NP have optimal proof systems.

Thm. [Mes00]
coNE contains sets without optimal proof systems.



Is This Question Hard?

Are there sets outside NP with optimal proof systems?

Is This Question Hard?

Are there sets outside NP with optimal proof systems?

Negative Answer

Is This Question Hard?

Are there sets outside NP with optimal proof systems?

Negative Answer

- implies NP $\neq$ coNP

Is This Question Hard?

Are there sets outside NP with optimal proof systems?

Negative Answer

- implies NP $\neq$ coNP
- relativization barrier for plausible assumptions

Is This Question Hard?

Are there sets outside NP with optimal proof systems?

Negative Answer

- implies NP $\neq$ coNP
- relativization barrier for plausible assumptions

$\Downarrow$

Provably difficult!

Is This Question Hard?

Are there sets outside NP with optimal proof systems?

Negative Answer

- implies NP $\neq$ coNP
- relativization barrier for plausible assumptions

$\Downarrow$

Provably difficult!

Positive Answer

Is This Question Hard?

Are there sets outside NP with optimal proof systems?

Negative Answer

- implies NP $\neq$ coNP
- relativization barrier for plausible assumptions

$\Downarrow$

Provably difficult!

Positive Answer

—

Is This Question Hard?

Are there sets outside NP with optimal proof systems?

Negative Answer

- implies NP $\neq$ coNP
- relativization barrier for plausible assumptions

$\Downarrow$

Provably difficult!

Positive Answer

—

$\Downarrow$

Feasible?

Is This Question Hard?

Are there sets outside NP with optimal proof systems?

Negative Answer

- implies NP $\neq$ coNP
- relativization barrier for plausible assumptions

$\Downarrow$

Provably difficult!

Positive Answer

—

$\Downarrow$

Feasible?

Both answers aren't known to have unlikely consequences!

Is This Question Hard?

Are there sets outside NP with optimal proof systems?

Negative Answer

- implies NP $\neq$ coNP
- relativization barrier for plausible assumptions

$\Downarrow$

Provably difficult!

Positive Answer

Relativization barrier!

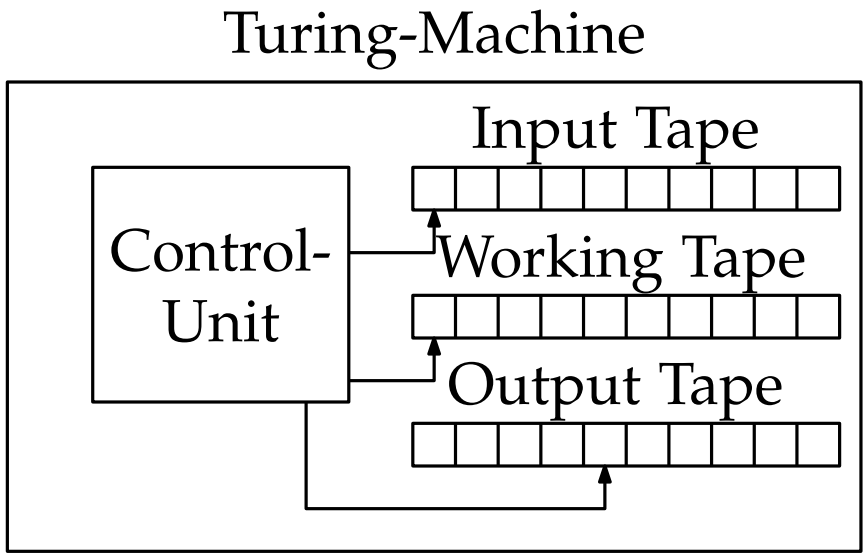
$\Downarrow$

Feasible?

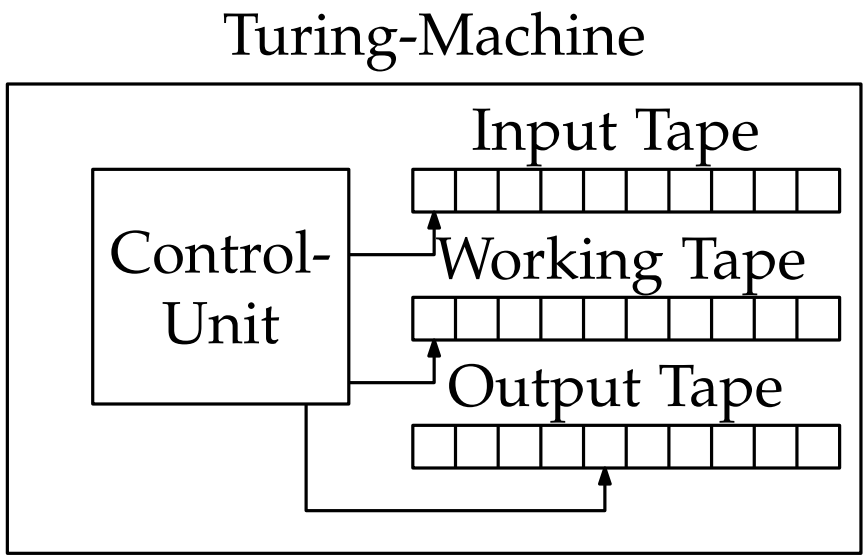
Both answers aren't known to have unlikely consequences!

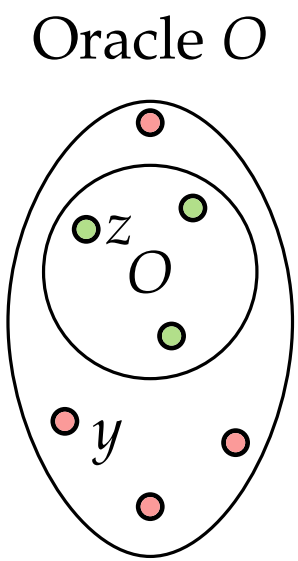
Oracles

Oracles

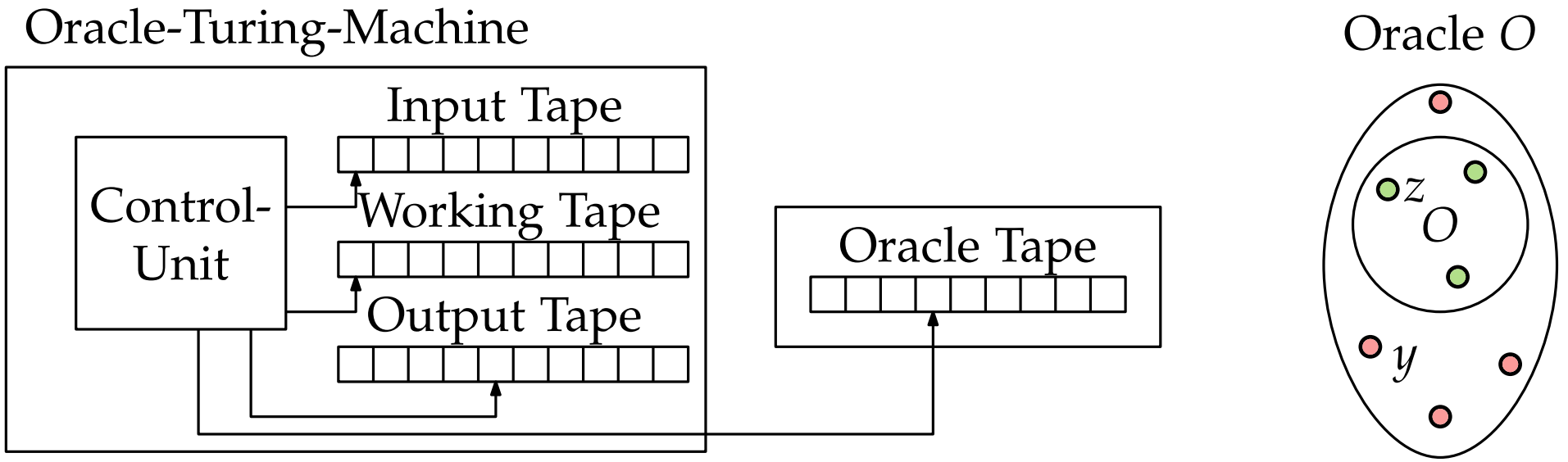

Turing-Machine
Input Tape
Control-
Unit
Working Tape
Output Tape

Oracles

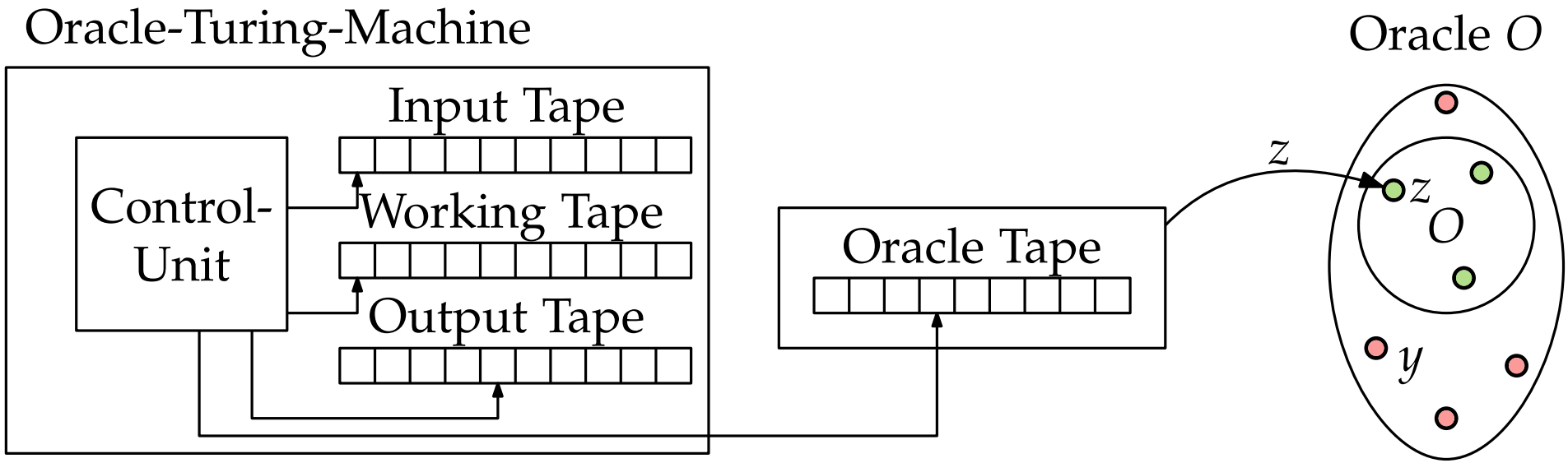

Turing-Machine
Input Tape
Control-
Unit
Working Tape
Output Tape


Oracle O
z
O
y

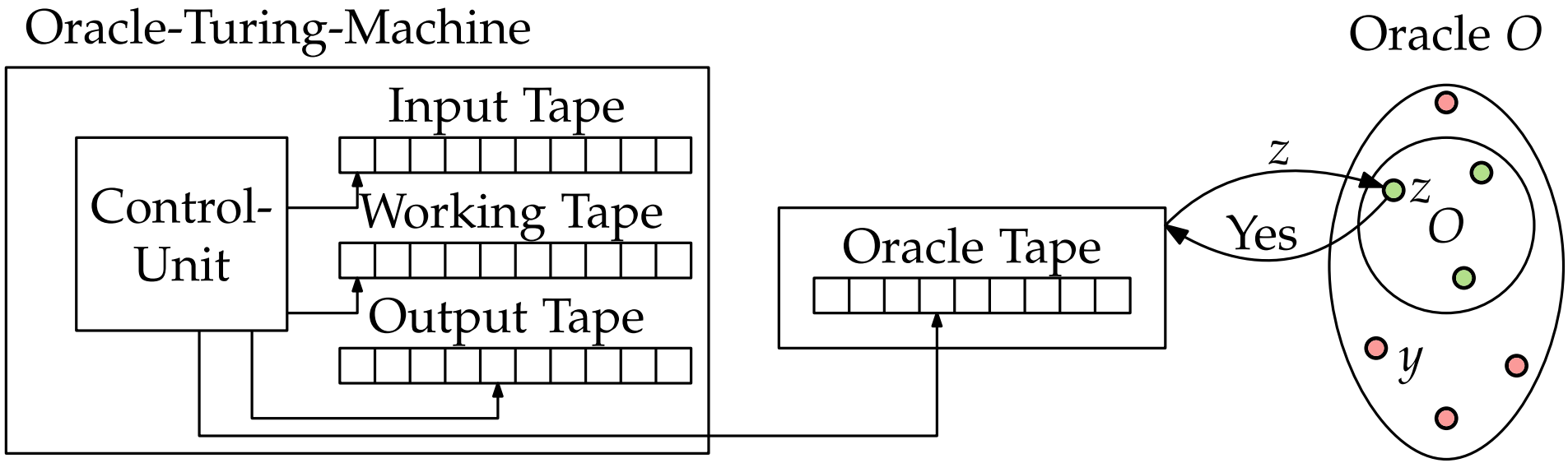
Oracles


Oracle-Turing-Machine
Input Tape
Control-
Unit
Working Tape
Output Tape
Oracle Tape
Oracle O
z
O
y

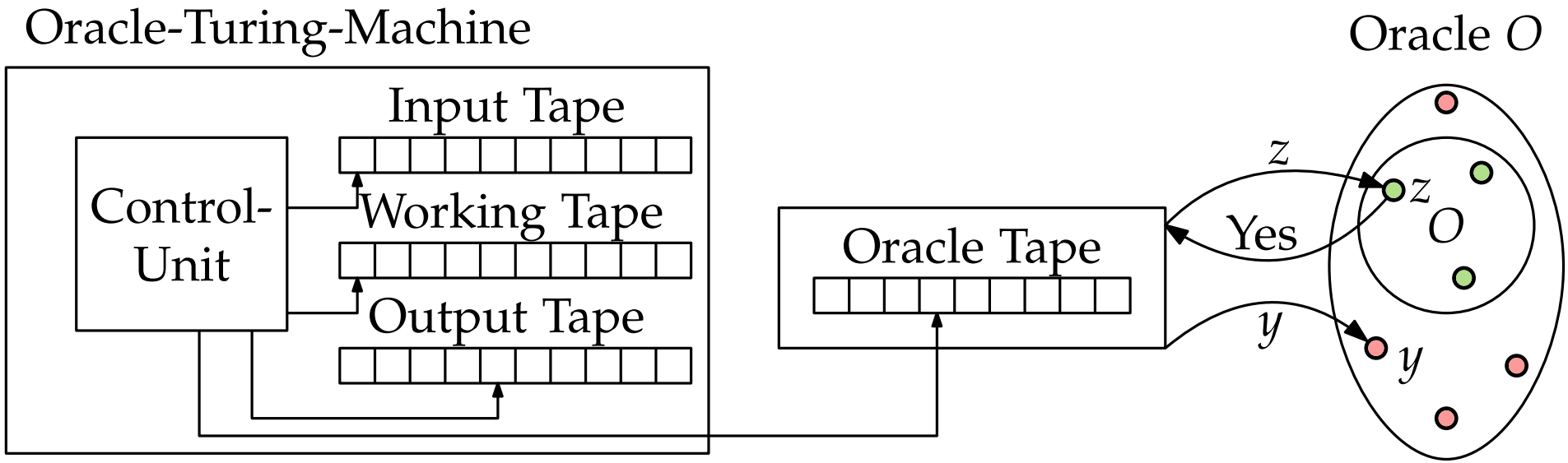
Oracles


Oracle-Turing-Machine
Input Tape
Control-
Unit
Working Tape
Output Tape
Oracle Tape
Oracle O
z
z
O
y

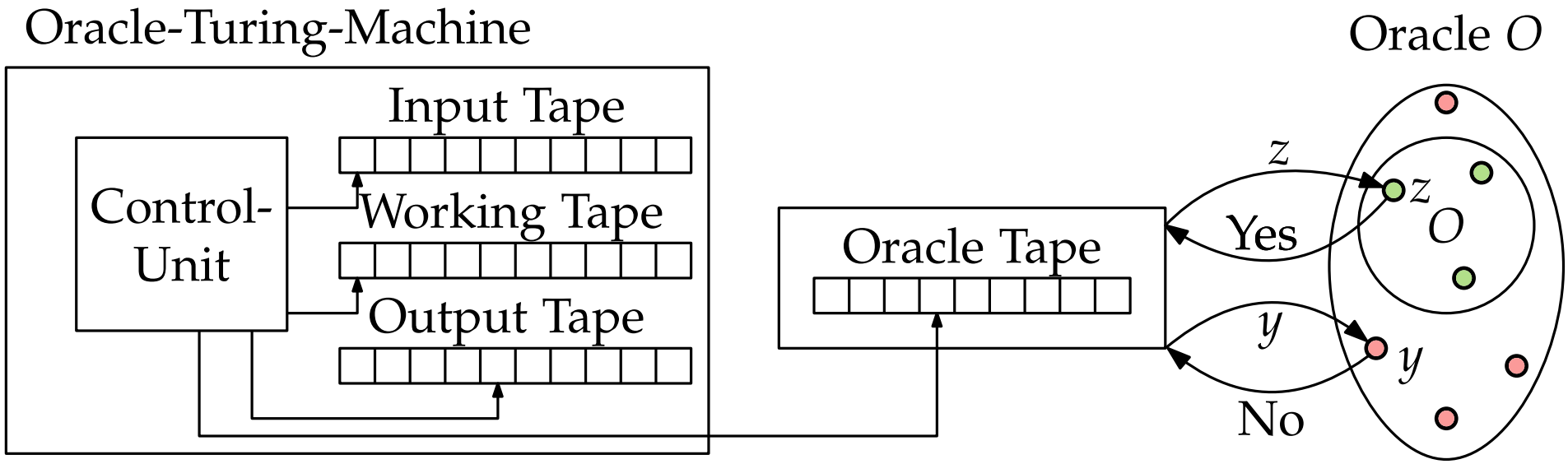
Oracles


Oracle-Turing-Machine
Input Tape
Control-
Unit
Working Tape
Output Tape
Oracle Tape
Oracle O
z
Yes
z
O
y

Oracles


Oracle-Turing-Machine
Input Tape
Control-
Unit
Working Tape
Output Tape
Oracle Tape
Oracle O
z
Yes
z
O
y
y

Oracles


Oracle-Turing-Machine
Input Tape
Control-
Unit
Working Tape
Output Tape
Oracle Tape
Oracle O
z
Yes
z
O
y
No
y

Relativizable Proofs

Relativizable Proofs

Known: $P \subseteq NP$

Relativizable Proofs

Known: $\mathrm{P} \subseteq \mathrm{NP}$

Same method: $\forall O\ [\mathrm{P}^O \subseteq \mathrm{NP}^O]$

Relativizable Proofs

Known: $\mathrm{P} \subseteq \mathrm{NP}$

Same method: $\forall O \; [\mathrm{P}^O \subseteq \mathrm{NP}^O]$

$\Rightarrow$ method is relativizable (i.e., works relative to all oracles)

Relativizable Proofs

Known: $\mathrm{P} \subseteq \mathrm{NP}$

Same method: $\forall O\ [\mathrm{P}^O \subseteq \mathrm{NP}^O]$

$\Rightarrow$ method is relativizable (i.e., works relative to all oracles)

50 years experience:
almost all known proofs in structural complexity theory are relativizable

Relativizable Proofs

Known: $\mathrm{P} \subseteq \mathrm{NP}$

Same method: $\forall O\ [\mathrm{P}^O \subseteq \mathrm{NP}^O]$

$\Rightarrow$ method is relativizable (i.e., works relative to all oracles)

50 years experience:
almost all known proofs in structural complexity theory are relativizable

Thm. [BGS75] $\quad \exists O\ [\mathrm{P}^O = \mathrm{NP}^O]$

Relativizable Proofs

Known: $\mathrm{P} \subseteq \mathrm{NP}$

Same method: $\forall O\ [\mathrm{P}^O \subseteq \mathrm{NP}^O]$

$\Rightarrow$ method is relativizable (i.e., works relative to all oracles)

50 years experience:
almost all known proofs in structural complexity theory are relativizable

Thm. [BGS75] $\quad \exists O\ [\mathrm{P}^O = \mathrm{NP}^O]$

Cor. Proofs for $\mathrm{P} \neq \mathrm{NP}$ have to be nonrelativizable

Relativizable Proofs

Known: $\mathrm{P} \subseteq \mathrm{NP}$

Same method: $\forall O\ [\mathrm{P}^O \subseteq \mathrm{NP}^O]$

$\Rightarrow$ method is relativizable (i.e., works relative to all oracles)

50 years experience:
almost all known proofs in structural complexity theory are relativizable

Thm. [BGS75] $\quad \exists O\ [\mathrm{P}^O = \mathrm{NP}^O]$

Cor. Proofs for $\mathrm{P} \neq \mathrm{NP}$ have to be nonrelativizable

Oracles indicate the difficulty of proving a statement

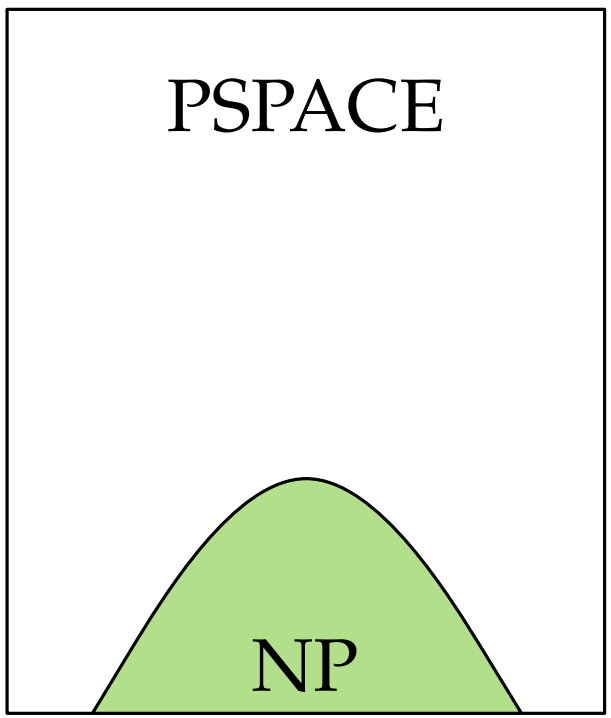
Our Results

Our Results

Thm. [EG25] $\exists O$ [PH^O is infinite and all $L \in \mathrm{PSPACE}^O \setminus \mathrm{NP}^O$ have no optimal proof system]

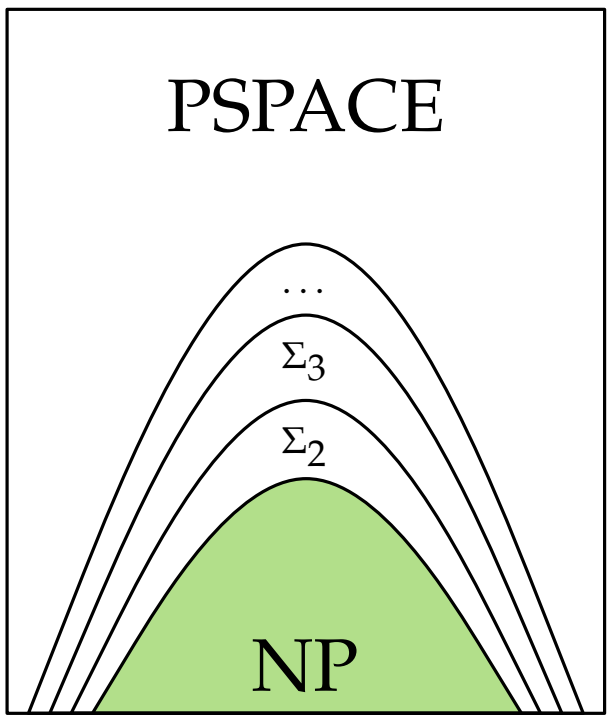
Our Results

Thm. [EG25] $\exists O$ [PH^O is infinite and all $L \in \mathrm{PSPACE}^O \setminus \mathrm{NP}^O$ have no optimal proof system]



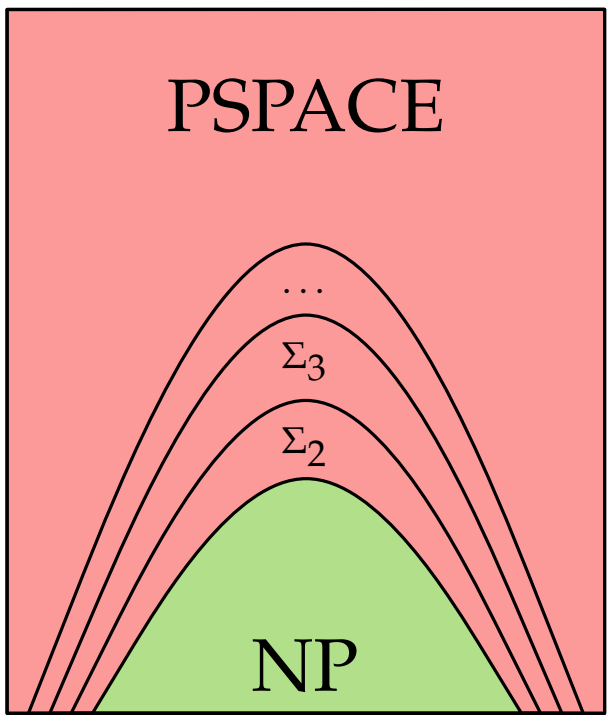
Our Results

Thm. [EG25] $\exists O$ [PH^O is infinite and all $L \in \mathrm{PSPACE}^O \setminus \mathrm{NP}^O$ have no optimal proof system]



Our Results

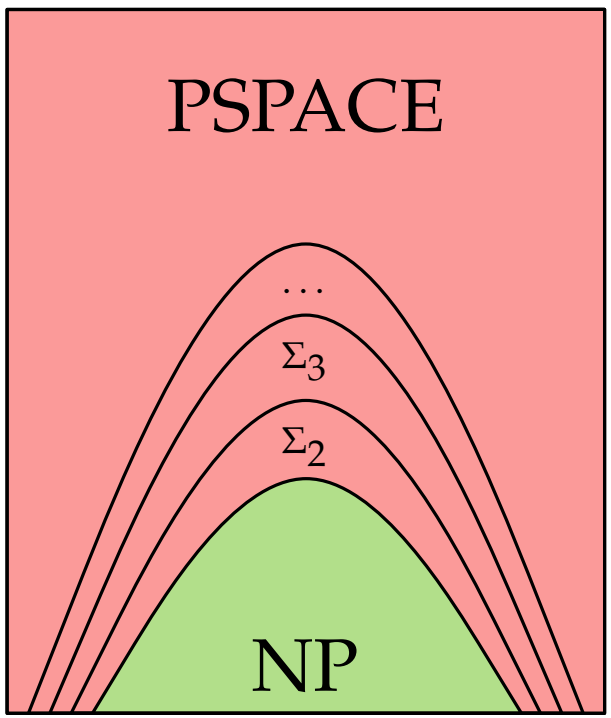
Thm. [EG25] $\exists O$ [PH^O is infinite and all $L \in \mathrm{PSPACE}^O \setminus \mathrm{NP}^O$ have no optimal proof system]



Our Results

Thm. [EG25] $\exists O$ [PH^O is infinite and all $L \in \mathrm{PSPACE}^O \setminus \mathrm{NP}^O$ have no optimal proof system]

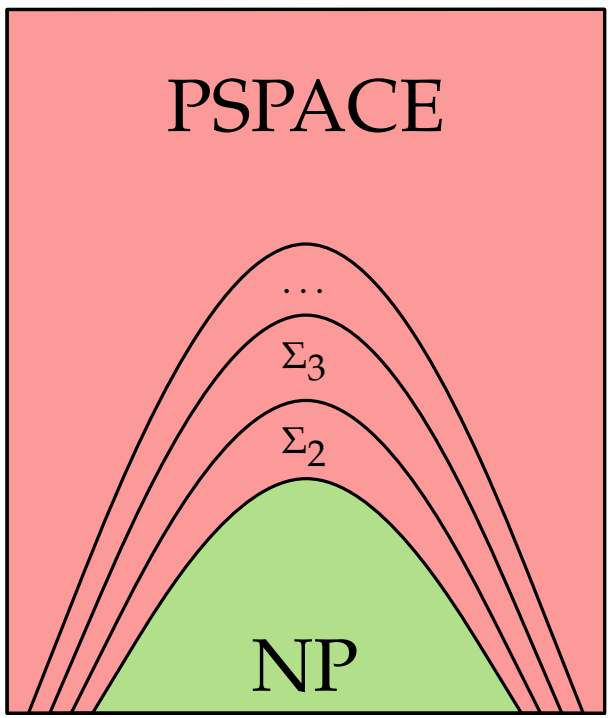
Thm. [EG25] $\exists O$ [$\mathrm{NP}^O \neq \mathrm{coNP}^O$ and all $L \in \mathrm{RE}^O \setminus \mathrm{NQP}^O$ have no optimal proof system]

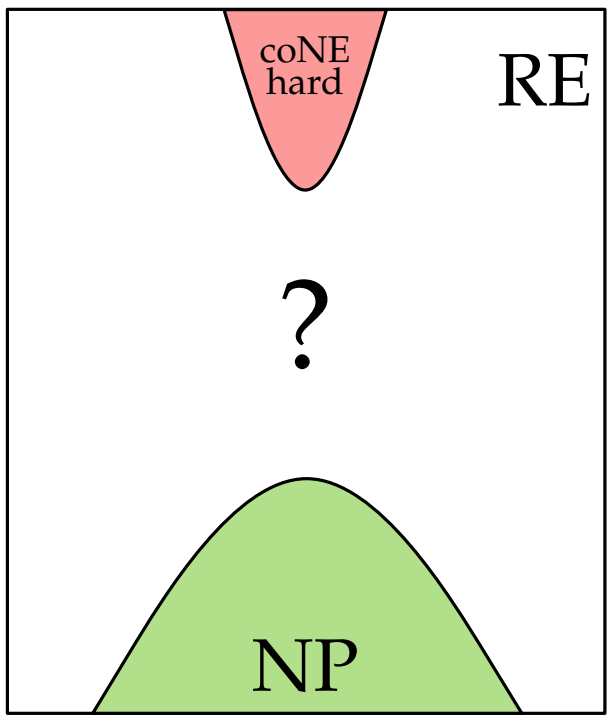


Our Results

Thm. [EG25] $\exists O$ [PH^O is infinite and all $L \in \mathrm{PSPACE}^O \setminus \mathrm{NP}^O$ have no optimal proof system]

Thm. [EG25] $\exists O$ [$\mathrm{NP}^O \neq \mathrm{coNP}^O$ and all $L \in \mathrm{RE}^O \setminus \mathrm{NQP}^O$ have no optimal proof system]

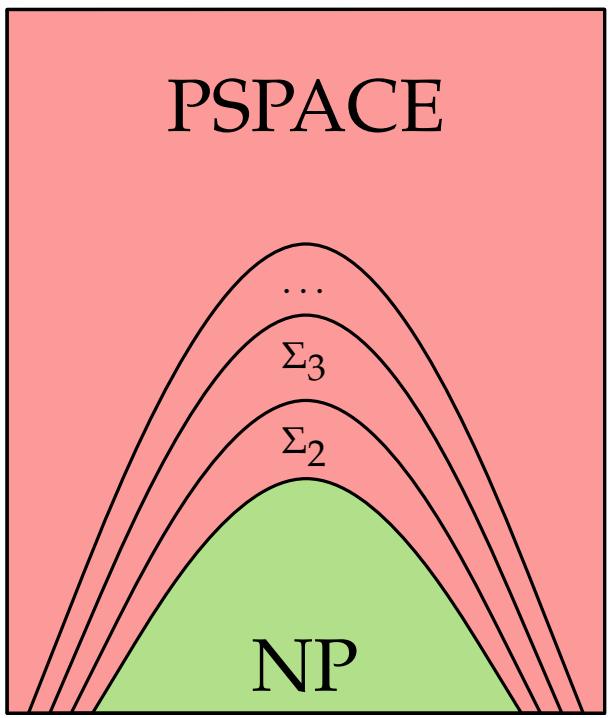


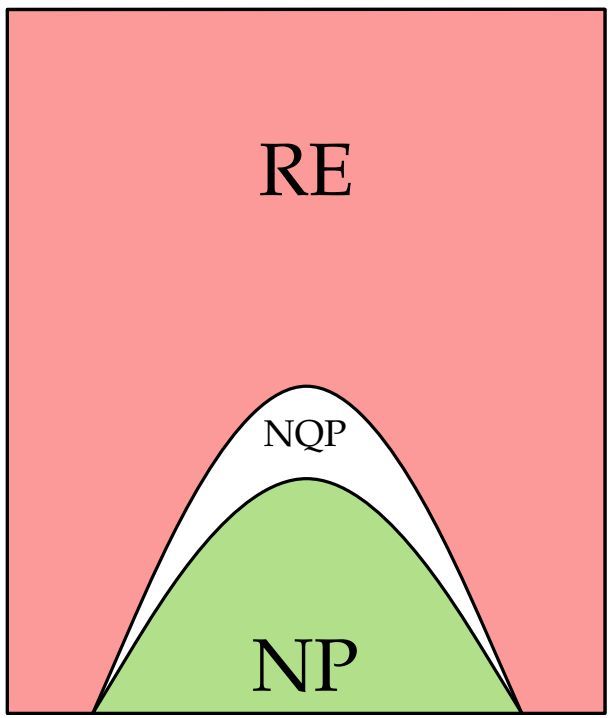


Our Results

Thm. [EG25] $\exists O$ [PH^O is infinite and all $L \in \mathrm{PSPACE}^O \setminus \mathrm{NP}^O$ have no optimal proof system]

Thm. [EG25] $\exists O$ [$\mathrm{NP}^O \neq \mathrm{coNP}^O$ and all $L \in \mathrm{RE}^O \setminus \mathrm{NQP}^O$ have no optimal proof system]





Our Results

Are there sets outside NP with optimal proof systems?

Negative Answer

- implies NP $\neq$ coNP
- relativization barrier for plausible assumptions

$\Downarrow$

Provably difficult!

Positive Answer

—

$\Downarrow$

Feasible?

Both answers aren't known to have unlikely consequences!

Our Results

Are there sets outside NP with optimal proof systems?

Negative Answer

- implies NP $\neq$ coNP
- relativization barrier for plausible assumptions

$\Downarrow$

Provably difficult!

Positive Answer

- relativization barrier for "almost all" sets

$\Downarrow$

Feasible?

Both answers aren't known to have unlikely consequences!

Our Results

Are there sets outside NP with optimal proof systems?

Negative Answer

- implies NP $\neq$ coNP
- relativization barrier for plausible assumptions

$\Downarrow$

Provably difficult!

Positive Answer

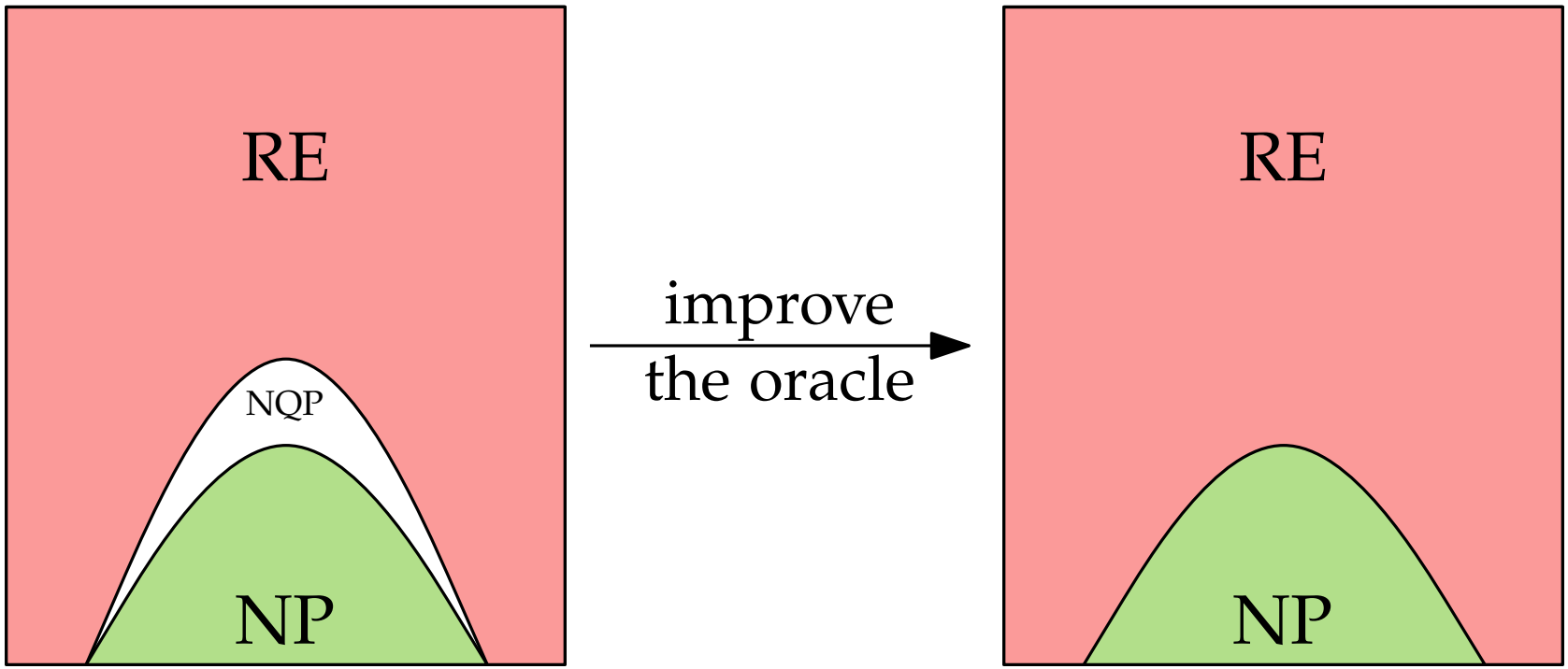
- relativization barrier for "almost all" sets

$\Downarrow$

~~Feasible?~~

Explains why no such set is known

Both answers aren't known to have unlikely consequences!

From NQP to NP?

From NQP to NP?