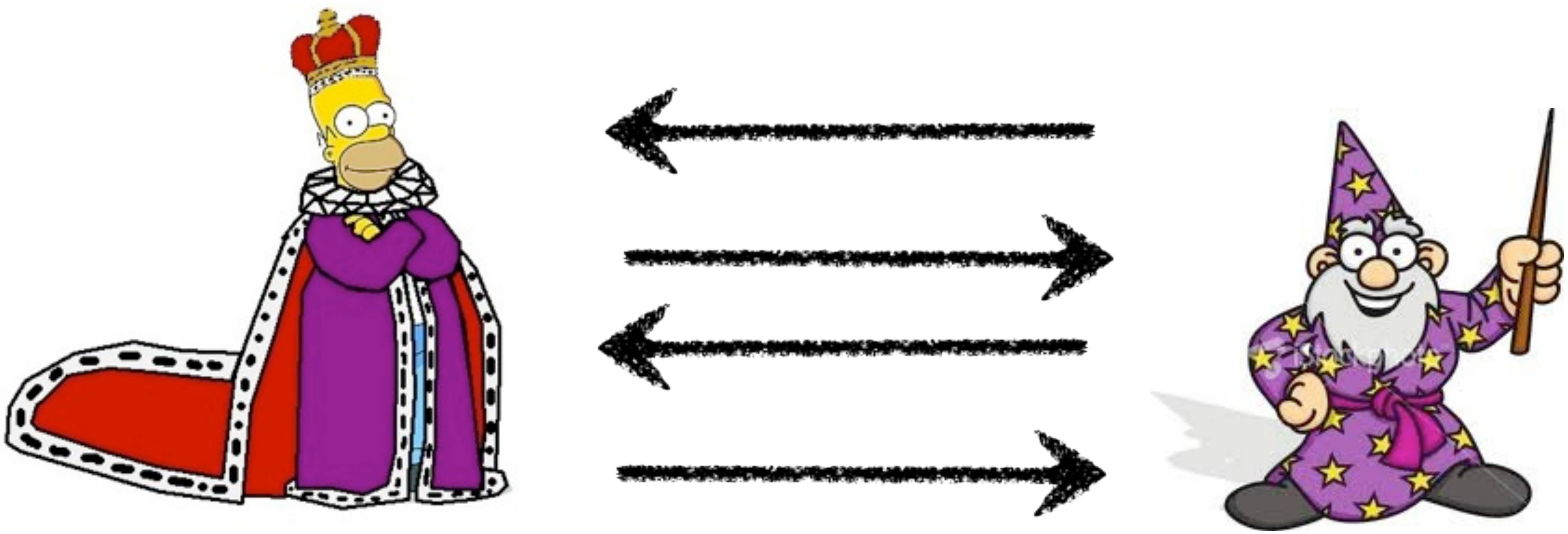
Rational Proofs

Pablo Azar Silvio Micali

Central Question

f(x)?

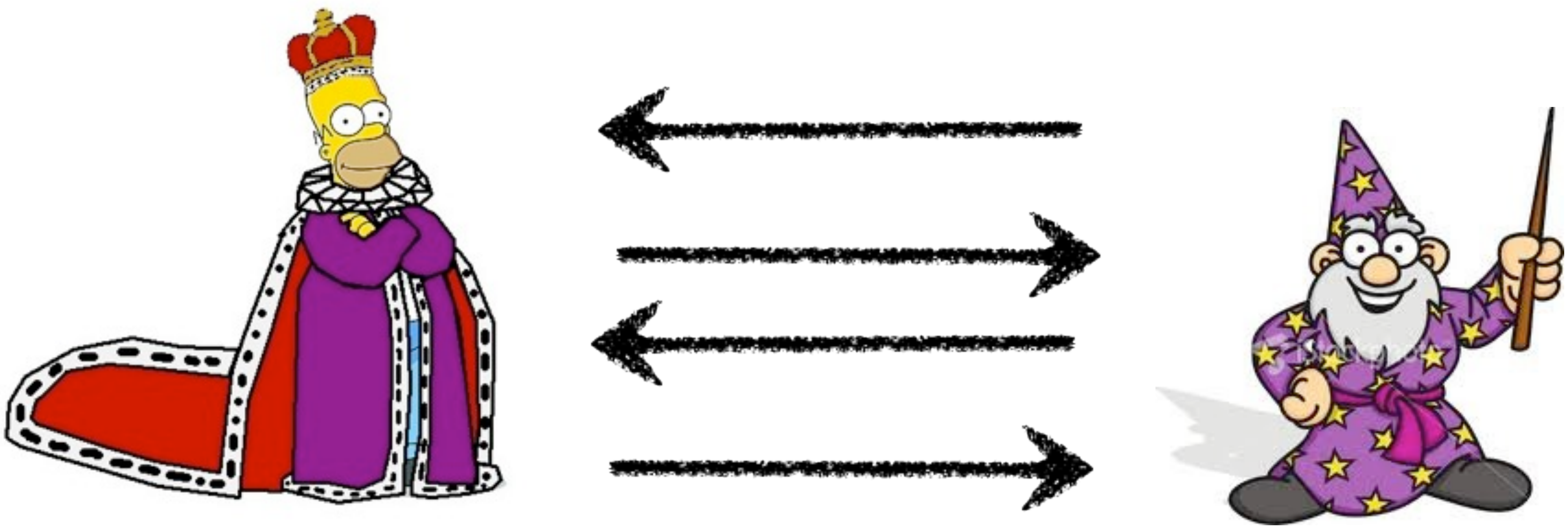


Arthur   Merlin

What problems have efficient proofs?
(Rounds, Communication, Time)

Interactive Proofs

f(x)?



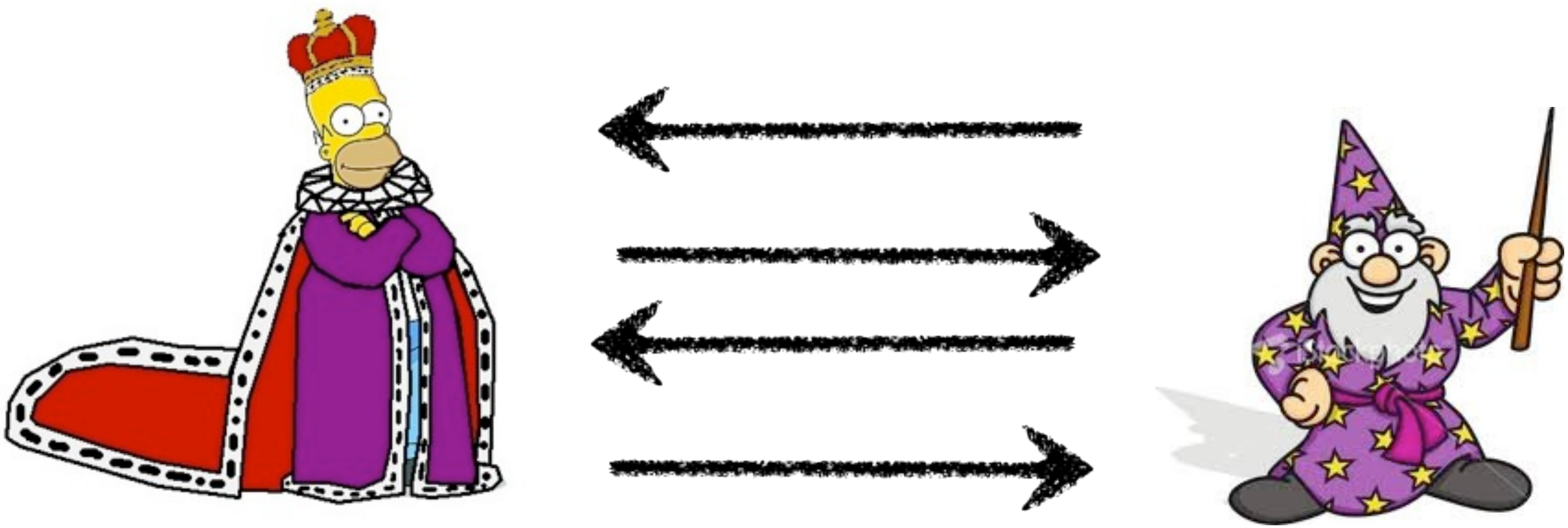
IP

AM

[GMR 85, BM 85]

Interactive Proofs

f(x)?



IP = PSPACE

[LFKN 90, Shamir 90]

And they lived happily ever after...

Many Centuries Later...

f(x)?

Centuries Later...

f(x)?

Centuries Later...

f(x)?

$#*#!

Centuries Later...

f(x)?

$#*#!

Goldman Sachs

citi

JPMorgan

Centuries Later...

f(x)?

$#*#!

How to pay a Math Expert?

f(x)?

How to pay a Math Expert?

f(x)?

Fixed Price: Correct Proof : $1
Incorrect Proof: $0

How to pay a Math Expert?

f(x)?

Fixed Price:

Correct Proof : $1
Incorrect Proof: $0

Can we do better?

f(x)?

Can we do better?

f(x)?

Can we prove more theorems?

Can we prove them faster?

Can we do better?

f(x)?

Fewer Rounds?

Our Central Question

f(x)?

What's the largest class of problems for which we can guarantee correctness of solution using monetary incentives?

Rational MA

$f \in$ Rational MA[k] iff

f ∈ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

f ∈ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

f(x)?

f ∈ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

f(x)?

y_1

f ∈ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

f(x)?

y_1

random r_1

f ∈ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

f(x)?

y_1

random r_1

y_2

$f \in$ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

f(x)?

y_1

random r_1

y_2

random r_2

f ∈ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

f(x)?

y_1

random r_1

y_2

random r_2

...

f ∈ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

f(x)?

y_1

random r_1

y_2

random r_2

...

Transcript $T = (y_1, r_1, \ldots, y_k)$

$f \in$ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

$f(x)$?

y_1

random r_1

y_2

random r_2

...

$R(x,T) =$ 

Transcript $T = (y_1, r_1, \ldots, y_k)$

$f \in$ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

f(x)?

y_1

random r_1

y_2

random r_2

...

Output = $\pi(x,T)$

R(x,T) = 

Transcript $T = (y_1, r_1, \ldots, y_k)$

$f \in$ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

f(x)?

y_1

random r_1

y_2

random r_2

...

Output = $\pi(x,T)$

R(x,T) =

Transcript $T = (y_1, r_1, \ldots, y_k)$

No Verification!

f ∈ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

f(x)?

y_1

random r_1

y_2

random r_2

...

Output = π(x,T)

R(x,T) = 

f ∈ Rational MA[k] iff

π output function (poly time)

R reward function (randomized poly time)

f(x)?

y_1

random r_1

y_2

random r_2

...

Output = π(x,T)

R(x,T) =

Merlin chooses Transcript T* that maximizes E[R(x,T)]

$f \in$ Rational MA[k] iff

f(x)?

y_1

random r_1

y_2

random r_2

...

Output = $\pi(x,T)$

$R(x,T)$ = 

Merlin chooses Transcript T* that maximizes $E[R(x,T)]$

$f \in$ Rational MA[k] iff

f(x)?

y_1

random r_1

y_2

random r_2

...

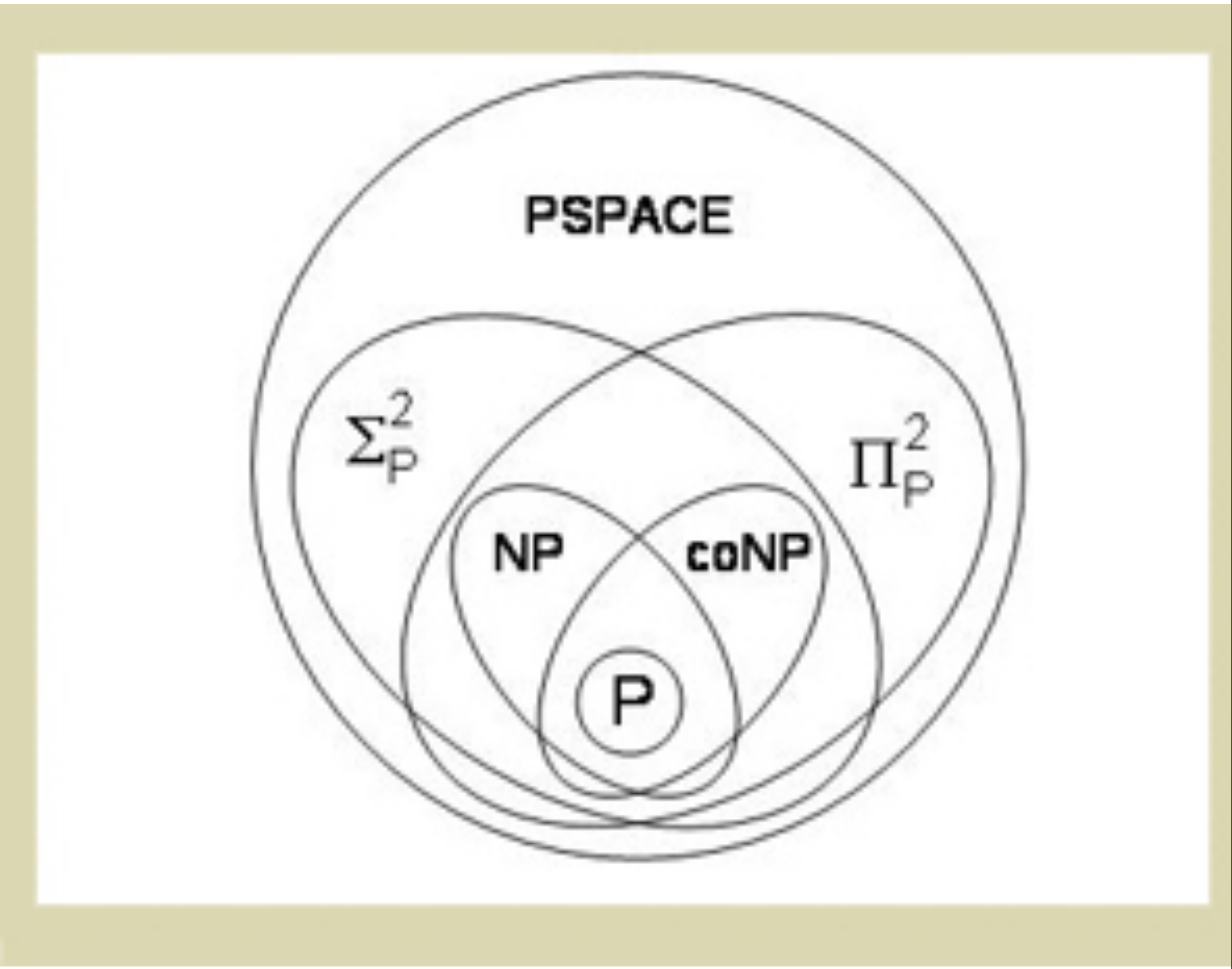
$\pi(x,T^*) = f(x)$

$R(x,T^*) =$ 

Merlin chooses Transcript T* that maximizes E[R(x,T)]

Our Central Question

Where does RMA[k] fit?



Theorem 1

$$\boxed{\#P \subset RMA[?]}$$

Theorem 1

$$\boxed{\#P \subset RMA[1]}$$

Proof Sketch

$$\boxed{\#P \subset RMA[1]}$$

#P Problems

$$\text{Input: } M : \{0,1\}^n \times \{0,1\}^{poly(n)} \to \{0,1\}$$

$$x \in \{0,1\}^n$$

#P Problems

$$\text{Input: } M : \{0,1\}^n \times \{0,1\}^{poly(n)} \to \{0,1\}$$

$$x \in \{0,1\}^n$$

#{y : M(x,y) = 1} ?

#P Problems

$$\text{Input: } M : \{0,1\}^n \times \{0,1\}^{poly(n)} \to \{0,1\}$$

$$x \in \{0,1\}^n$$

#{y : M(x,y) = 1} ?

$2^{301} + 13$

#P Problems

$$\text{Input: } M : \{0,1\}^n \times \{0,1\}^{poly(n)} \to \{0,1\}$$
$$x \in \{0,1\}^n$$

#{y : M(x,y) = 1} ?

$2^{301} + 13$

?

#P Problems

$$\text{Input: } M : \{0,1\}^n \times \{0,1\}^{poly(n)} \to \{0,1\}$$

$$x \in \{0,1\}^n$$

#{y : M(x,y) = 1} ?

$2^{301} + 13$

#P Problems

$$\text{Input: } M : \{0,1\}^n \times \{0,1\}^{poly(n)} \to \{0,1\}$$

$$x \in \{0,1\}^n$$

#{y : M(x,y) = 1} ?

$2^{301} + 13$

$M(x, y_1), M(x, y_2), \ldots$ $\longleftarrow$

#P Problems

Input: $M : \{0,1\}^n \times \{0,1\}^{poly(n)} \to \{0,1\}$

$x \in \{0,1\}^n$

#{y : M(x,y) = 1} ?

$2^{301} + 13$

$M(x, y_1), M(x, y_2), \ldots$

No 1-round proof so far

Economics To The Rescue!

Asymmetric Information

Arthur

Merlin

Asymmetric Information

Information

Arthur

Merlin

Asymmetric Information

Information

Arthur

Merlin

What is information?

Asymmetric Information

Information

Arthur

Merlin

What is information?

How do we guarantee it is correct?

Computation View

x, f

Verifier

Prover

Computation View

x, f

Verifier

Prover

Information is output of a hard to compute function

Computation View

x, f

Verifier

Prover

Information is output of a hard to compute function

Correctness guaranteed by proof

Economics View

Decision Maker

Agent

Economics View

$\mathcal{D}$

Decision Maker

Agent

Information: distribution $\mathcal{D}$ over Ω = states of the world

Economics View

$$\xleftarrow{\quad\mathcal{D}\quad}$$

Decision Maker — Agent

Information: distribution $\mathcal{D}$ over Ω = states of the world

Correctness from incentives

Proper Scoring Rules

[Good 52, Brier 50]

Proper Scoring Rules

[Good 52, Brier 50]

$$\Omega = \{ \quad , \quad \}$$

$$\mathcal{D} \in \Delta(\Omega)$$

Proper Scoring Rules

[Good 52, Brier 50]

$$\Omega = \{ \quad , \quad \}$$

$$\mathcal{D} \in \Delta(\Omega)$$

$$\mathcal{D}(Boston) = 60\%$$

$$\mathcal{D}(NewYork) = 40\%$$

Proper Scoring Rules

[Good 52, Brier 50]

$\Omega = \{ \quad , \quad \}$

$\mathcal{D} \in \Delta(\Omega)$

$\mathcal{D}(Boston) = 60\%$

$\mathcal{D}(NewYork) = 40\%$

$\mathcal{D}$

Proper Scoring Rules

[Good 52, Brier 50]

$$\Omega = \{ \quad , \quad \}$$

$$\mathcal{D} \in \Delta(\Omega)$$

$$\mathcal{D}(Boston) = 60\%$$

$$\mathcal{D}(NewYork) = 40\%$$

$$\xleftarrow{\qquad\qquad \mathcal{P} \qquad\qquad}$$

Proper Scoring Rules

[Good 52, Brier 50]

$$\Omega = \{ \quad , \quad \}$$

$$\mathcal{D} \in \Delta(\Omega)$$

$$\omega \leftarrow \mathcal{D}$$

$$\mathcal{D}(Boston) = 60\%$$

$$\mathcal{D}(NewYork) = 40\%$$

$$\xleftarrow{\quad\mathcal{P}\quad}$$

Proper Scoring Rules

[Good 52, Brier 50]

$$\Omega = \{ \quad , \quad \}$$

$$\mathcal{D} \in \Delta(\Omega)$$

$$\omega \leftarrow \mathcal{D}$$

$$\mathcal{D}(Boston) = 60\%$$

$$\mathcal{D}(NewYork) = 40\%$$

$$\mathcal{P}$$

$$= S(\mathcal{P}, \omega)$$

Proper Scoring Rules

$\Omega = \{ \quad , \quad \}, \mathcal{D} \in \Delta(\Omega)$

$\mathcal{D}(Boston) = 60\%$

$\mathcal{D}(NewYork) = 40\%$

$\omega \leftarrow \mathcal{D}$

$\mathcal{P}$

$= S(\mathcal{P}, \quad)$

Proper Scoring Rules

$\Omega = \{ \quad , \quad \}, \mathcal{D} \in \Delta(\Omega)$

$\mathcal{D}(Boston) = 60\%$

$\mathcal{D}(NewYork) = 40\%$

$\omega \leftarrow \mathcal{D}$

$\mathcal{P}$

$= S(\mathcal{P}, \quad)$

Proper Scoring Rules

$\Omega = \{ \quad , \quad \}, \mathcal{D} \in \Delta(\Omega)$

$\mathcal{D}(Boston) = 60\%$

$\mathcal{D}(NewYork) = 40\%$

$\omega \leftarrow \mathcal{D}$

$\mathcal{P}$

$= S(\mathcal{P}, \quad)$

$$60\% \cdot S(\mathcal{P}, Boston) + 40\% S(\mathcal{P}, NY)$$

Proper Scoring Rules

$\Omega = \{ \quad , \quad \}, \mathcal{D} \in \Delta(\Omega)$

$\mathcal{D}(Boston) = 60\%$

$\mathcal{D}(NewYork) = 40\%$

$\omega \leftarrow \mathcal{D}$

$\mathcal{P}$

 $= S(\mathcal{P}, \quad)$

$$\max_{\mathcal{P}}[\, 60\% \cdot S(\mathcal{P}, Boston) + 40\% S(\mathcal{P}, NY) \,]$$

#P Problems

$$\text{Input: } M : \{0,1\}^n \times \{0,1\}^{n^c} \rightarrow \{0,1\}$$
$$x \in \{0,1\}^n$$

#{y : M(x,y) = 1} ?

$2^{301} + 13$

#P Problems

$$\text{Input:} \quad M : \{0,1\}^n \times \{0,1\}^{n^c} \to \{0,1\}$$
$$x \in \{0,1\}^n$$

$\Pr_y[M(x,y) = 1]$?

$$\frac{2^{301} + 13}{2^{n^c}}$$

Reduce the problem to question about probabilities

#P Problems

$$\text{Input: } M : \{0,1\}^n \times \{0,1\}^{n^c} \rightarrow \{0,1\}$$
$$x \in \{0,1\}^n$$

$Pr_y[M(x,y) = 1]$?

$$\frac{2^{301} + 13}{2^{n^c}}$$

Merlin knows $q = Pr_y[M(x,y) = 1]$

Need to incentivize him to reveal q

Our Rational Proof for #P

$$\Omega = \{0,1\}, \mathcal{D} \in \Delta(\Omega)$$

$$\mathcal{D}(1) = q$$
$$\mathcal{D}(0) = 1 - q$$

Our Rational Proof for #P

$$\Omega = \{0, 1\}, \mathcal{D} \in \Delta(\Omega)$$

$$\mathcal{D}(1) = Pr_y[M(x, y) = 1]$$

$$\mathcal{D}(1) = q$$

$$\mathcal{D}(0) = 1 - q$$

Our Rational Proof for #P

$$\Omega = \{0,1\}, \mathcal{D} \in \Delta(\Omega)$$

$$\mathcal{D}(1) = Pr_y[M(x,y) = 1]$$

$$\omega = \{M(x,y) : y \leftarrow \{0,1\}^{poly(n)}\}$$

$$\mathcal{D}(1) = q$$

$$\mathcal{D}(0) = 1 - q$$

Our Rational Proof for #P

$$\Omega = \{0,1\}, \mathcal{D} \in \Delta(\Omega)$$

$$\mathcal{D}(1) = Pr_y[M(x,y) = 1]$$

$$\omega = \{M(x,y) : y \leftarrow \{0,1\}^{poly(n)}\}$$

$$\mathcal{D}(1) = q$$

$$\mathcal{D}(0) = 1 - q$$

Our Rational Proof for #P

$$\Omega = \{0,1\}, \mathcal{D} \in \Delta(\Omega)$$

$$\mathcal{D}(1) = Pr_y[M(x,y) = 1]$$

$$\omega = \{M(x,y) : y \leftarrow \{0,1\}^{poly(n)}\}$$

$$\mathcal{D}(1) = q$$

$$\mathcal{D}(0) = 1 - q$$

Our Rational Proof for #P

$$\Omega = \{0,1\}, \mathcal{D} \in \Delta(\Omega)$$

$$\mathcal{D}(1) = Pr_y[M(x,y) = 1]$$

$$\omega = \{M(x,y) : y \leftarrow \{0,1\}^{poly(n)}\}$$

$$\mathcal{D}(1) = q$$

$$\mathcal{D}(0) = 1 - q$$

$$\xleftarrow{\quad\mathcal{P}\quad}$$

Our Rational Proof for #P

$$\Omega = \{0,1\}, \mathcal{D} \in \Delta(\Omega)$$

$$\mathcal{D}(1) = Pr_y[M(x,y) = 1]$$
$$\omega = \{M(x,y) : y \leftarrow \{0,1\}^{poly(n)}\}$$

$$\mathcal{D}(1) = q$$
$$\mathcal{D}(0) = 1 - q$$

$$\xleftarrow{\mathcal{P}}$$

$$= S(\mathcal{P}, \omega)$$

$$\longrightarrow$$

Our Rational Proof for #P

$$\Omega = \{0,1\}, \mathcal{D} \in \Delta(\Omega)$$

$$\boxed{\begin{array}{c} \mathcal{D}(1) = Pr_y[M(x,y)=1] \\ \omega = \{M(x,y) : y \leftarrow \{0,1\}^{poly(n)}\} \end{array}}$$

$$\mathcal{D}(1) = q$$
$$\mathcal{D}(0) = 1-q$$

$$\xleftarrow{\quad\mathcal{P}\quad}$$

$$= S(\mathcal{P}, \omega)$$

$$\longrightarrow$$

$$\mathcal{D} = argmax_{\mathcal{P}}\{q \cdot S(\mathcal{P},1) + (1-q)\cdot S(\mathcal{P},0)\}$$

Theorem 1

$$\boxed{\#P \subset RMA[1]}$$

Theorem 1

$$\boxed{\#P \subset RMA[1]}$$

Zero-Knowledge Rational Proof!

Theorem 1

$$\boxed{\#P \subset RMA[1]}$$

Zero-Knowledge Rational Proof!

Computationally Sound Rational Proof!

Theorem 2

$$\boxed{RMA[1] \subset P^{NP^{\#P}}}$$

Thank you Lance!

Theorem 2

$$RMA[1] \subset P^{NP^{\#P}}$$

There are things money can't buy

Thank you Lance!

Theorem 2

$$RMA[1] \subset P^{NP^{\#P}}$$

Economics View: Computational Limit on Contracts

Thank you Lance!

Counting Hierarchy

$$CH = CP_0 \cup CP_1 \cup CP_2 \cup \ldots$$

Counting Hierarchy

$$CH = CP_0 \cup CP_1 \cup CP_2 \cup \ldots$$

$$CP_0 = P$$

Counting Hierarchy

$$CH = CP_0 \cup CP_1 \cup CP_2 \cup \ldots$$

$$CP_0 = P$$

$$CP_1 = PP$$

Counting Hierarchy

$$CH = CP_0 \cup CP_1 \cup CP_2 \cup \ldots$$

$$CP_0 = P$$

$$CP_1 = PP$$

$$CP_2 = PP^{CP_1} = PP^{PP}$$

Counting Hierarchy

$$CH = CP_0 \cup CP_1 \cup CP_2 \cup \ldots$$

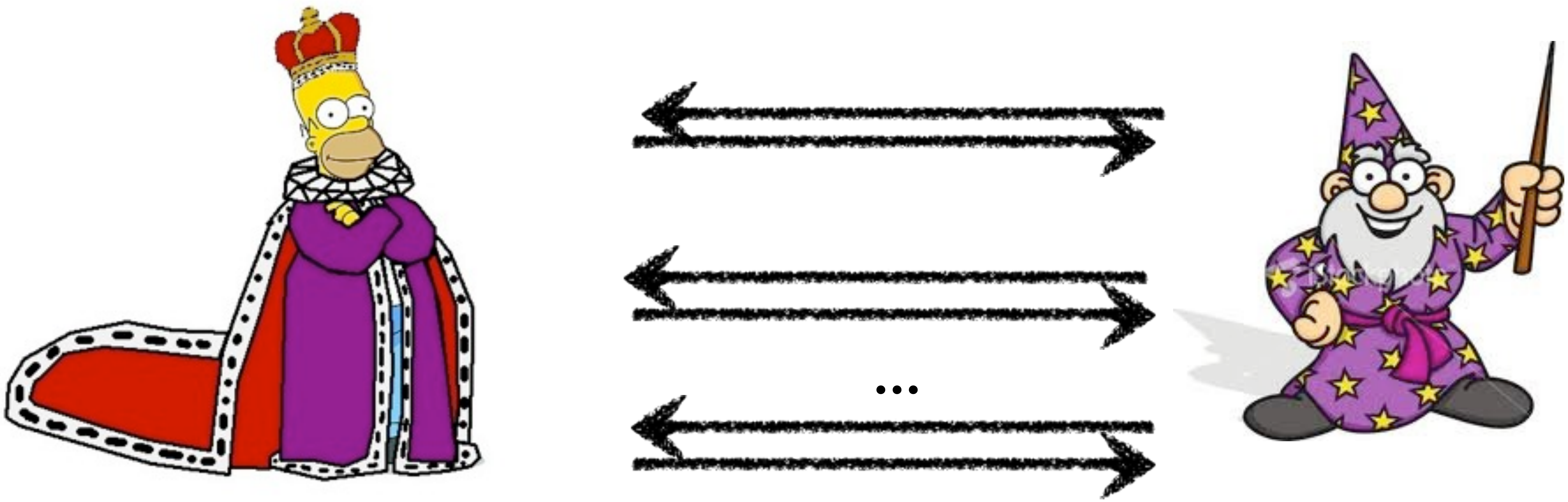
$$CP_0 = P$$

$$CP_1 = PP$$

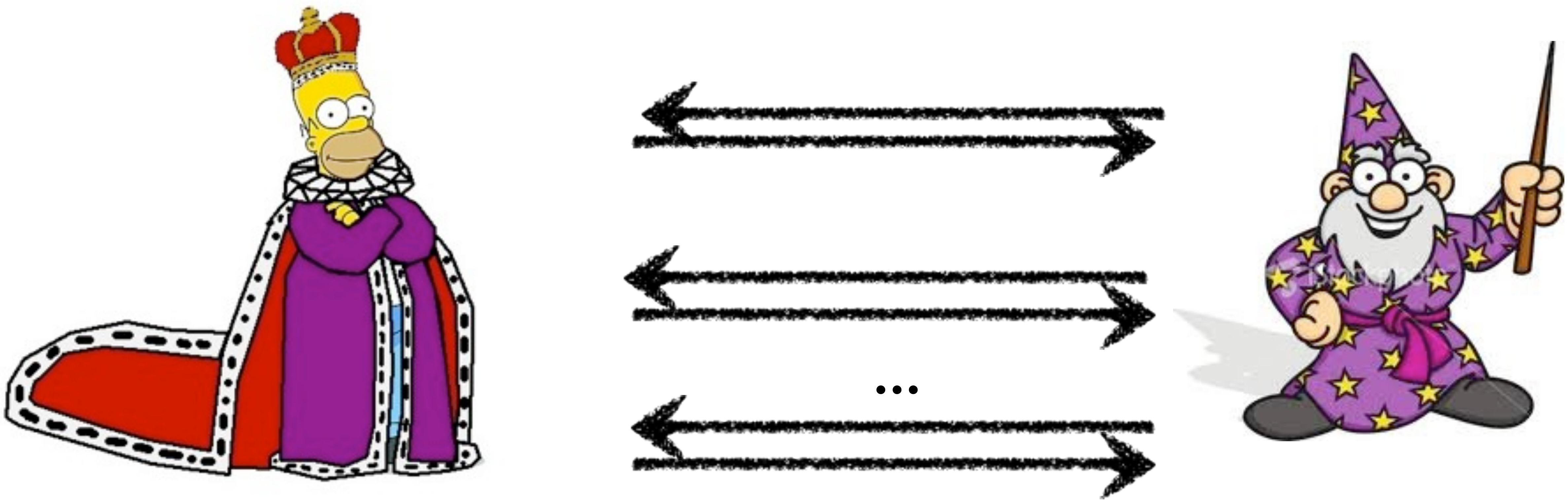
$$CP_2 = PP^{CP_1} = PP^{PP}$$

$$CP_k = PP^{CP_{k-1}} = PP^{PP^{\cdots^{PP}}}$$

Theorem 3

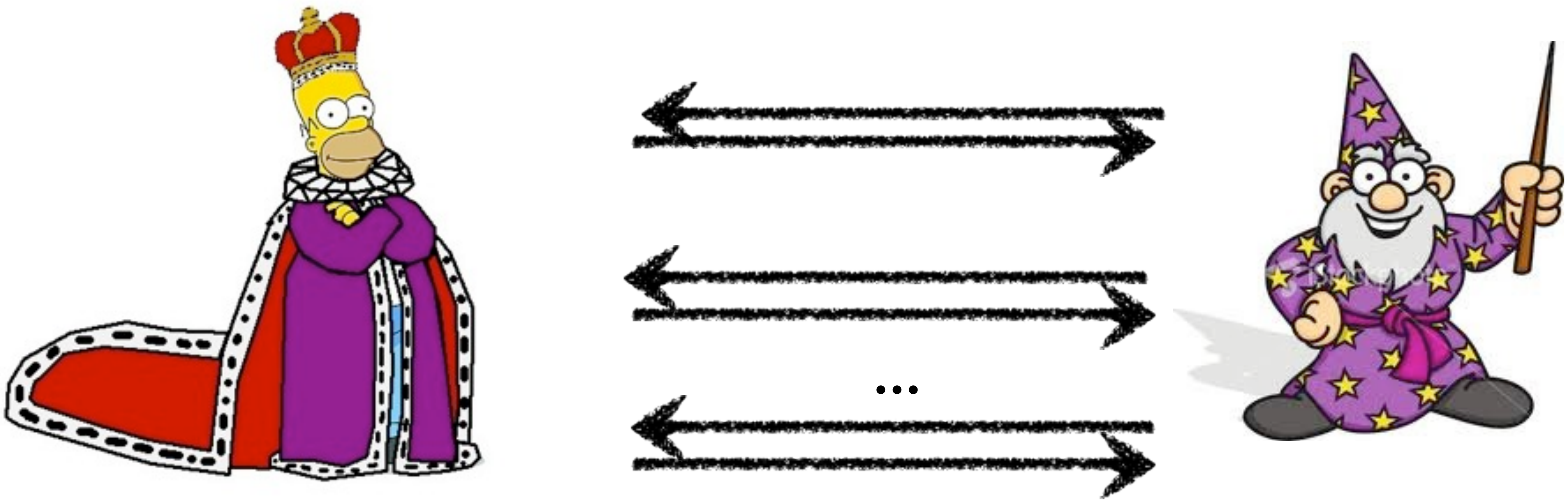


Theorem 3



$$CP_k \subset RMA[k] \subset CP_{2k+1}$$

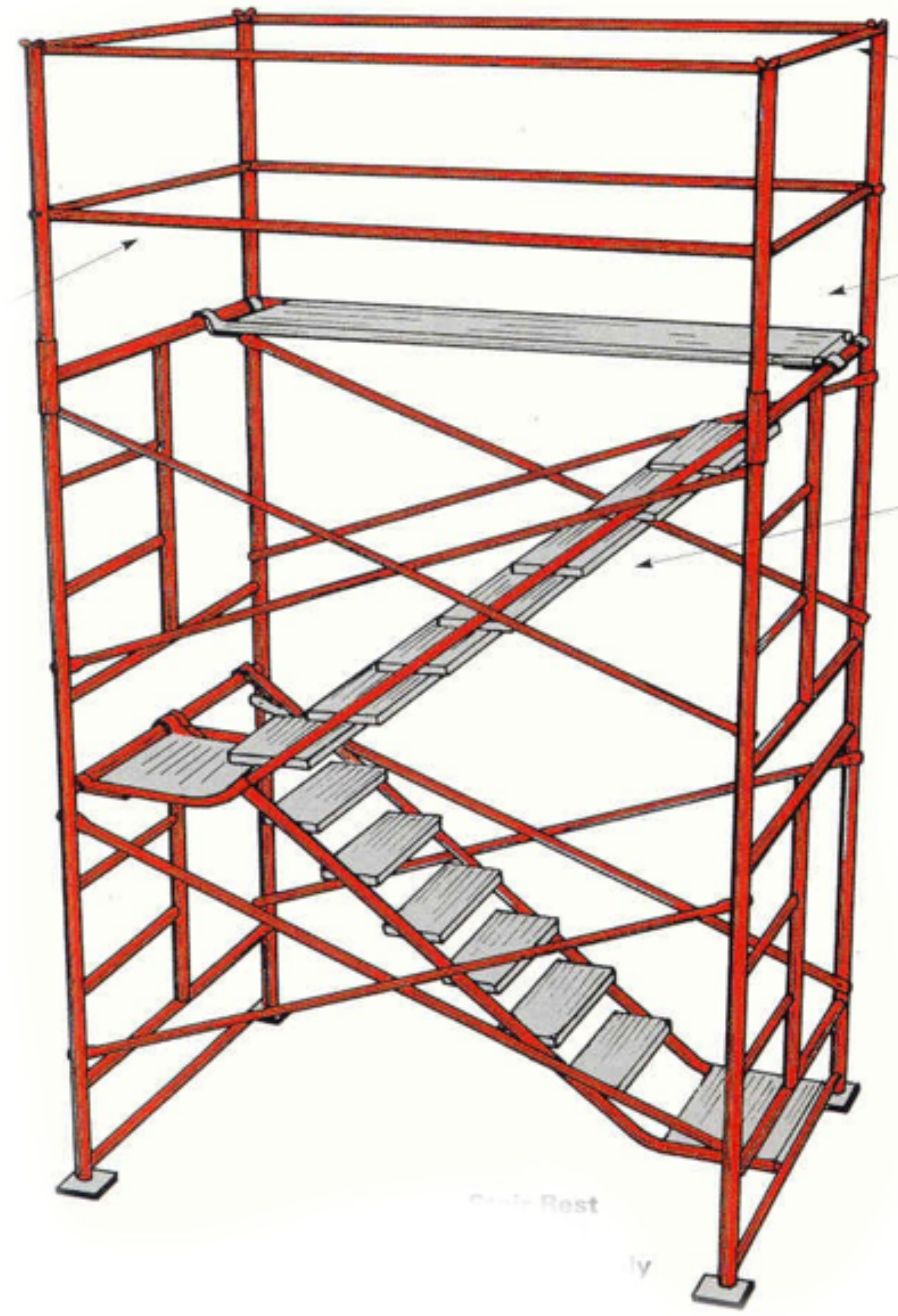
Theorem 3



$$RMA = CH$$

Open Question

Does CH Collapse?



Old Analogy

Q: Does CH Collapse?

A: Not if it behaves like PH

$$NP^{NP^{\cdots^{NP}}}$$

$$\cdots$$

$$NP^{NP}$$

$$NP$$

$$PP^{PP^{\cdots^{PP}}}$$

$$\cdots$$

$$PP^{PP}$$

$$PP$$

New Analogy

Q: Does CH Collapse?

A: Yes if it behaves like AM

$AM[k]$	$PP^{PP^{\cdot^{\cdot^{\cdot^{PP}}}}}$
$\cdots$	$\cdots$
$AM[2]$	PP^{PP}
$AM[1]$	PP

Summary of Contributions

- New Complexity Class RMA
- Short Rational Proofs for #P
- Constant-Round Rational Proofs = CH

THANK YOU!