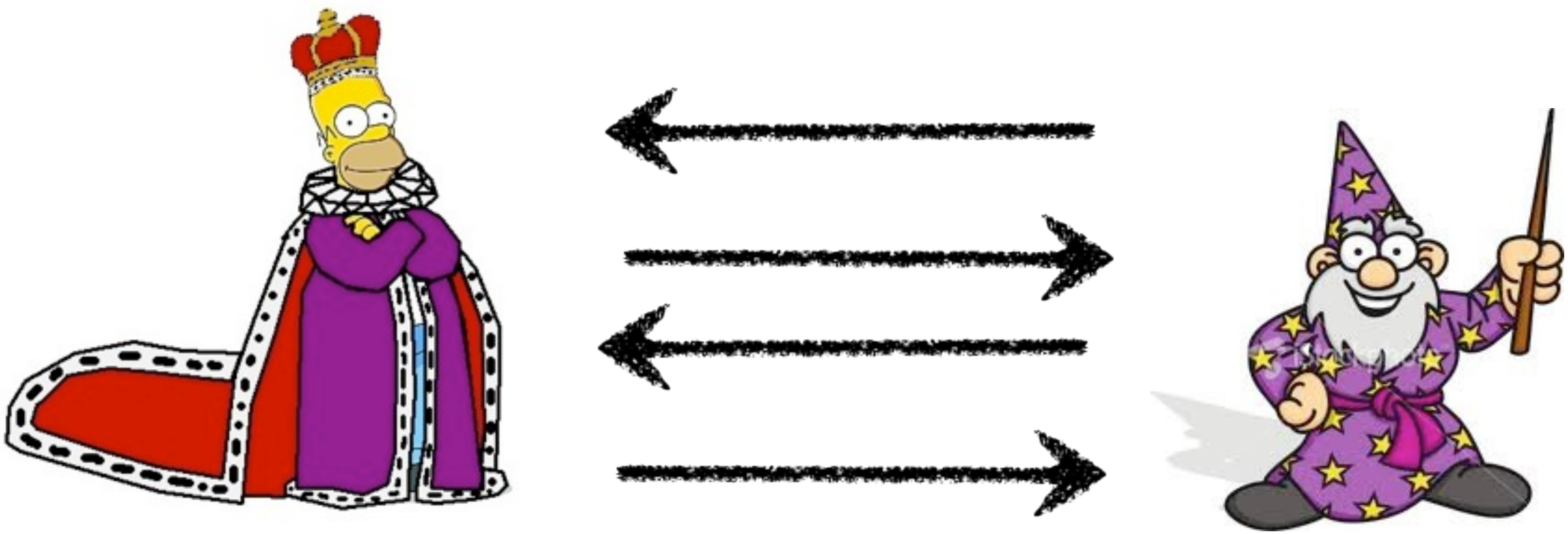
Rational Proofs

Azar Micali

Central Question

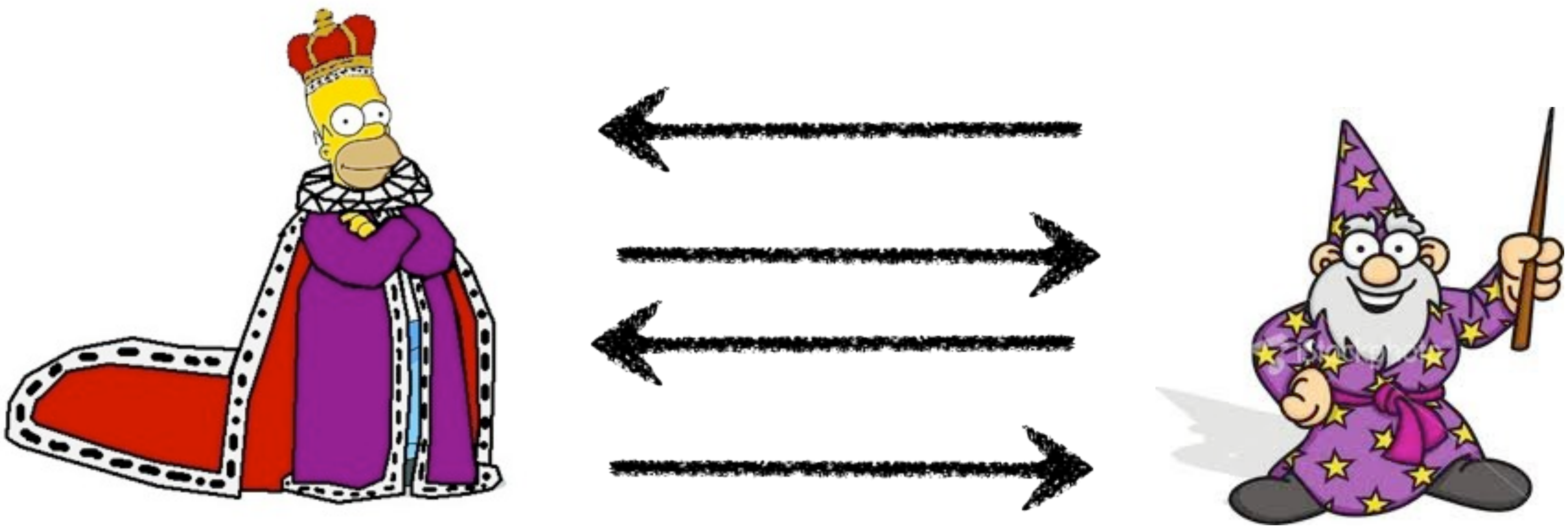
$x \in L$?



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

Interactive Proofs

$x \in L$?



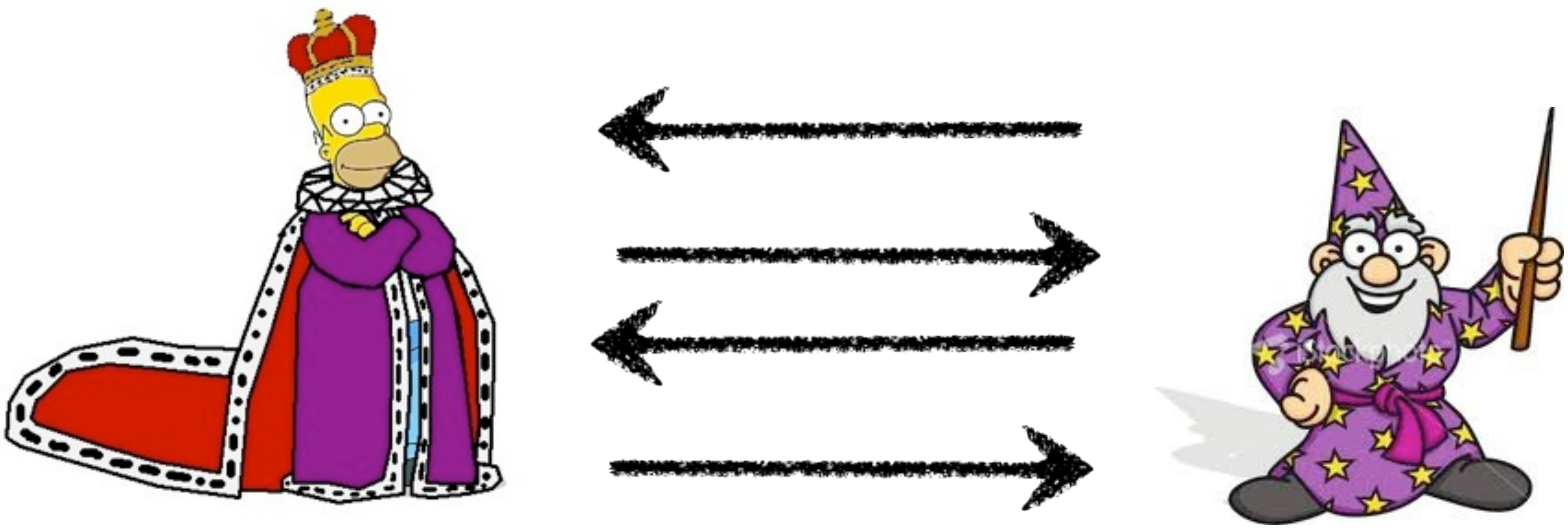
IP

AM

[GMR 85, BM 85]

Interactive Proofs

$x \in L$?



IP = PSPACE
[LFKN 90, Shamir 90]

And they lived happily ever after...

Many Centuries Later...

$x \in L$?

Centuries Later...

$x \in L$?

Centuries Later...

$x \in L$?

$#*#!

Centuries Later...

$x \in L$?

$#*#!

Goldman Sachs citi JPMorgan

Centuries Later...

$x \in L$?

$#*#!

Goldman Sachs

citi

JPMorgan

How to pay a Math Expert?

x in L?

How to pay a Math Expert?

x in L?

Fixed Price:

Correct Proof : $1
Incorrect Proof: $0

Can we do better?

x in L?

Can we do better?

x in L?

Can we prove more theorems?

Can we prove them faster?

Can we do better?

x in L?

Fewer Rounds?

Our Central Question

x in L?

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

Rational MA

L ∈ Rational MA iff

L ∈ Rational MA iff

π output function (poly time)

R reward function (poly time)

L ∈ Rational MA iff

π output function (poly time)

R reward function (poly time)

x in L?

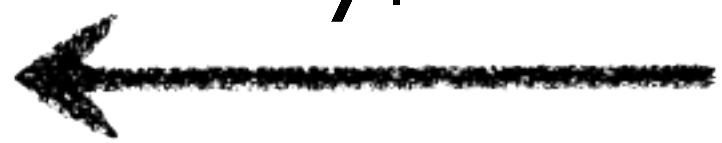
L ∈ Rational MA iff

π output function (poly time)

R reward function (poly time)

x in L?

y_1



$L \in$ Rational MA iff

π output function (poly time)

R reward function (poly time)

x in L?

y_1

random r_1

L ∈ Rational MA iff

π output function (poly time)

R reward function (poly time)

x in L?

y_1

random r_1

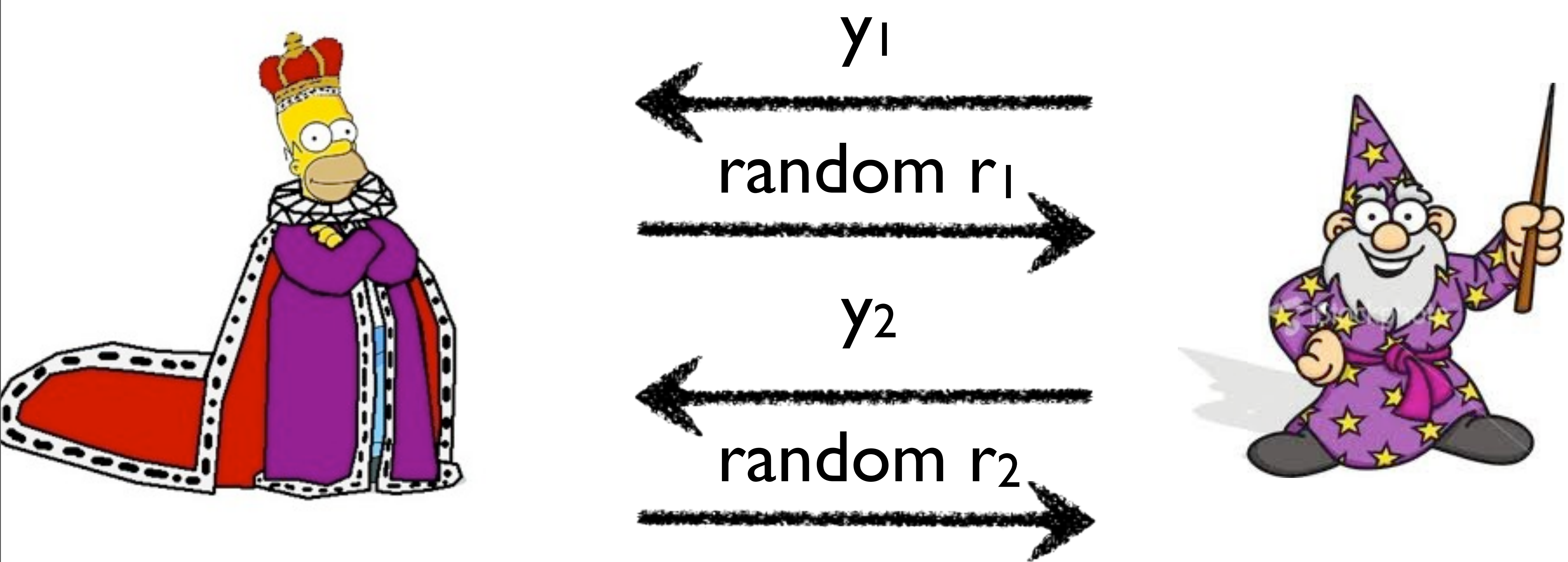
y_2

L ∈ Rational MA iff

π output function (poly time)

R reward function (poly time)

x in L?



L ∈ Rational MA iff

π output function (poly time)

R reward function (poly time)

x in L?

y_1

←

random r_1

→

y_2

←

random r_2

→

...

L ∈ Rational MA iff

π output function (poly time)

R reward function (poly time)

x in L?

y_1 ←

random r_1 →

y_2 ←

random r_2 →

...

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

$L \in$ Rational MA iff

π output function (poly time)

R reward function (poly time)

x in L?

y_1 ←

random r_1 →

y_2 ←

random r_2 →

...

$R(x,T) =$ 

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

L ∈ Rational MA iff

π output function (poly time)

R reward function (poly time)

x in L?

y_1

random r_1

y_2

random r_2

...

Output = π(x,T)

R(x,T) = 

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

L ∈ Rational MA iff

π output function (poly time)

R reward function (poly time)

x in L?

y_1 ←

random r_1 →

y_2 ←

random r_2 →

...

Output = $\pi(x,T)$

R(x,T) = 

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

No Verification!

L ∈ Rational MA iff

π output function (poly time)

R reward function (poly time)

x in L?

y_1

random r_1

y_2

random r_2

...

Output = $\pi(x,T)$

R(x,T) = 

L ∈ Rational MA iff

π output function (poly time)

R reward function (poly time)

x in L?

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)]

L ∈ Rational MA iff

x in L?

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)]

L ∈ Rational MA iff

x in L?

y_1 ←

random r_1 →

y_2 ←

random r_2 →

...

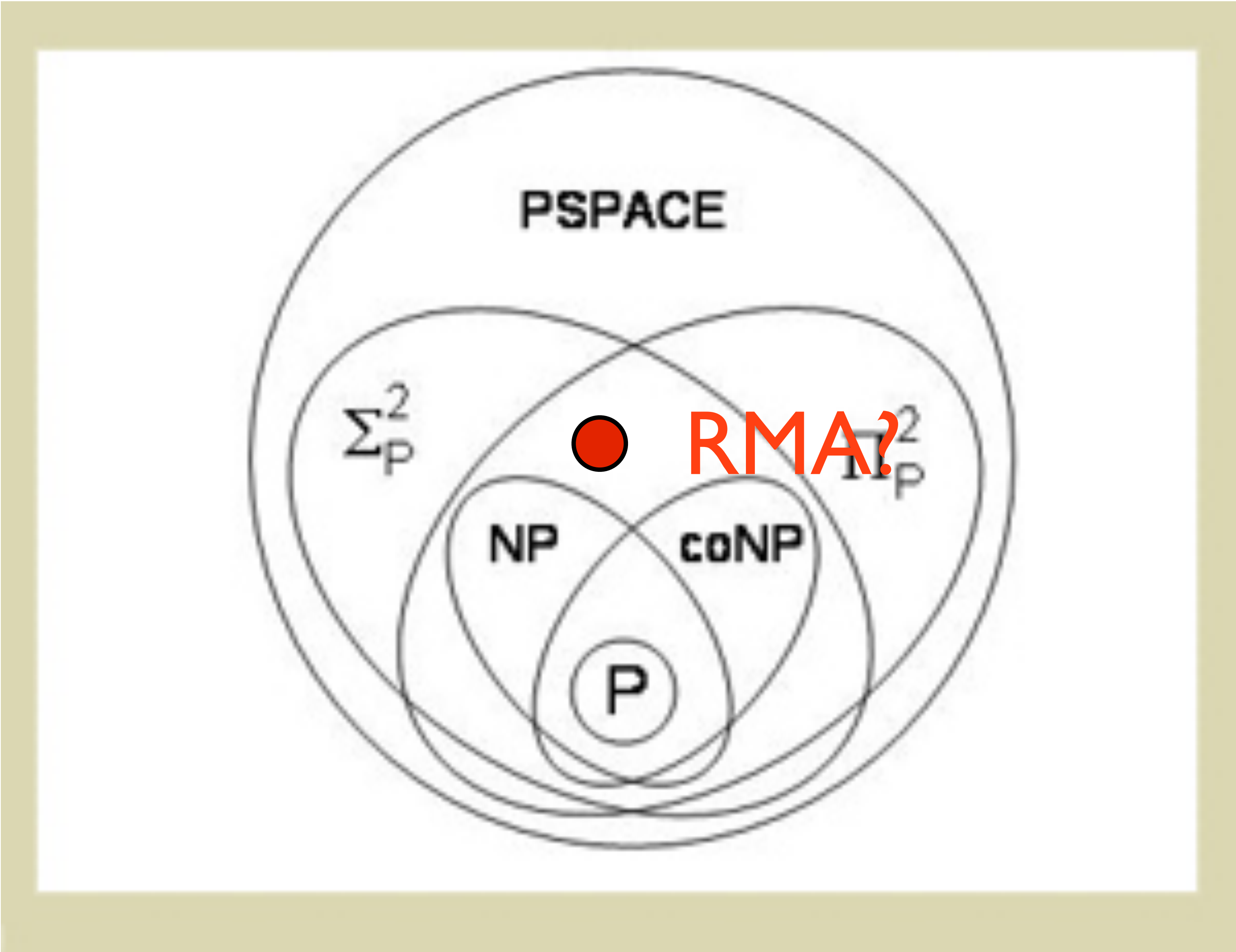
$\pi(x,T^*) = L(x)$

$R(x,T^*) =$ 

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

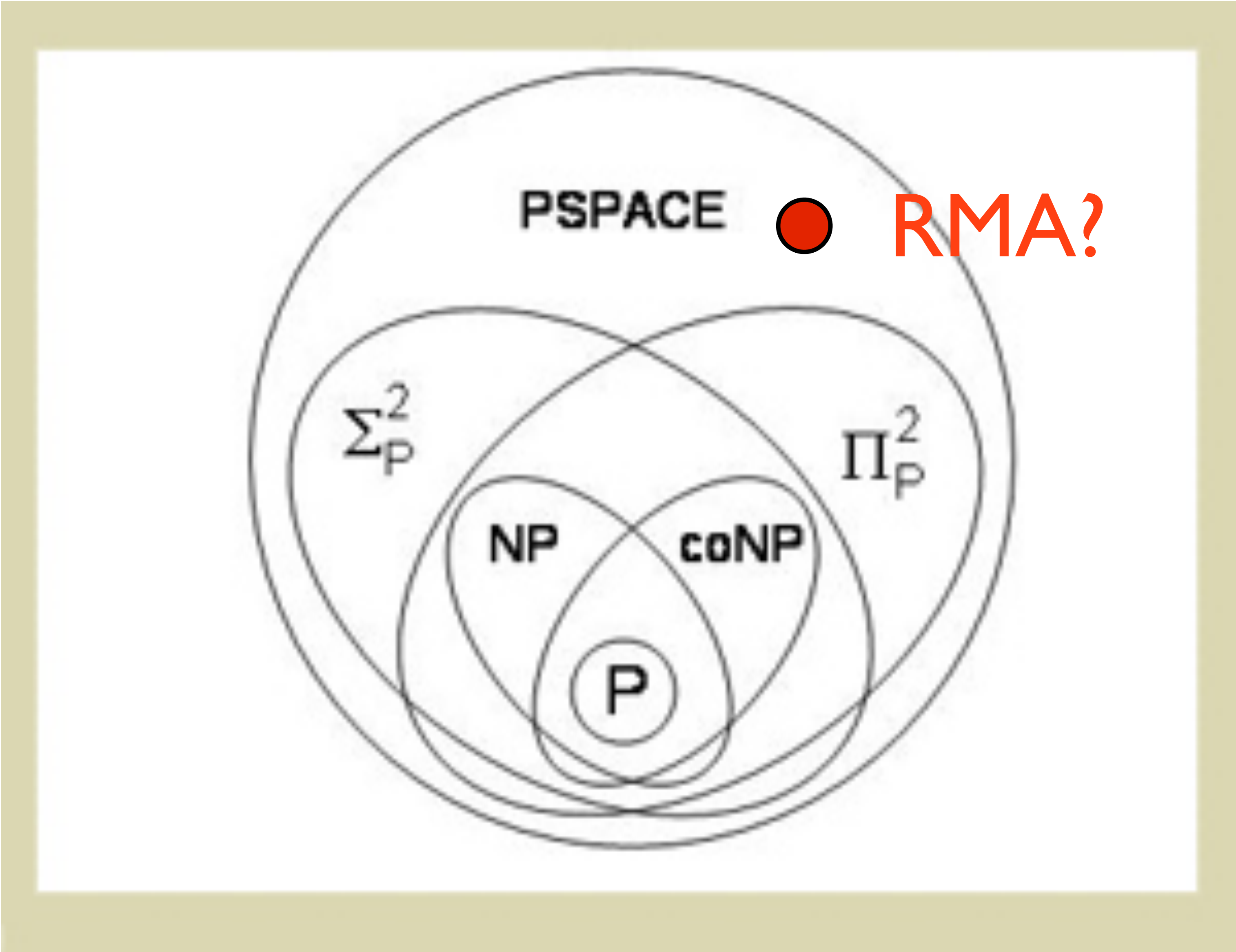
Our Central Question

Where does RMA fit?



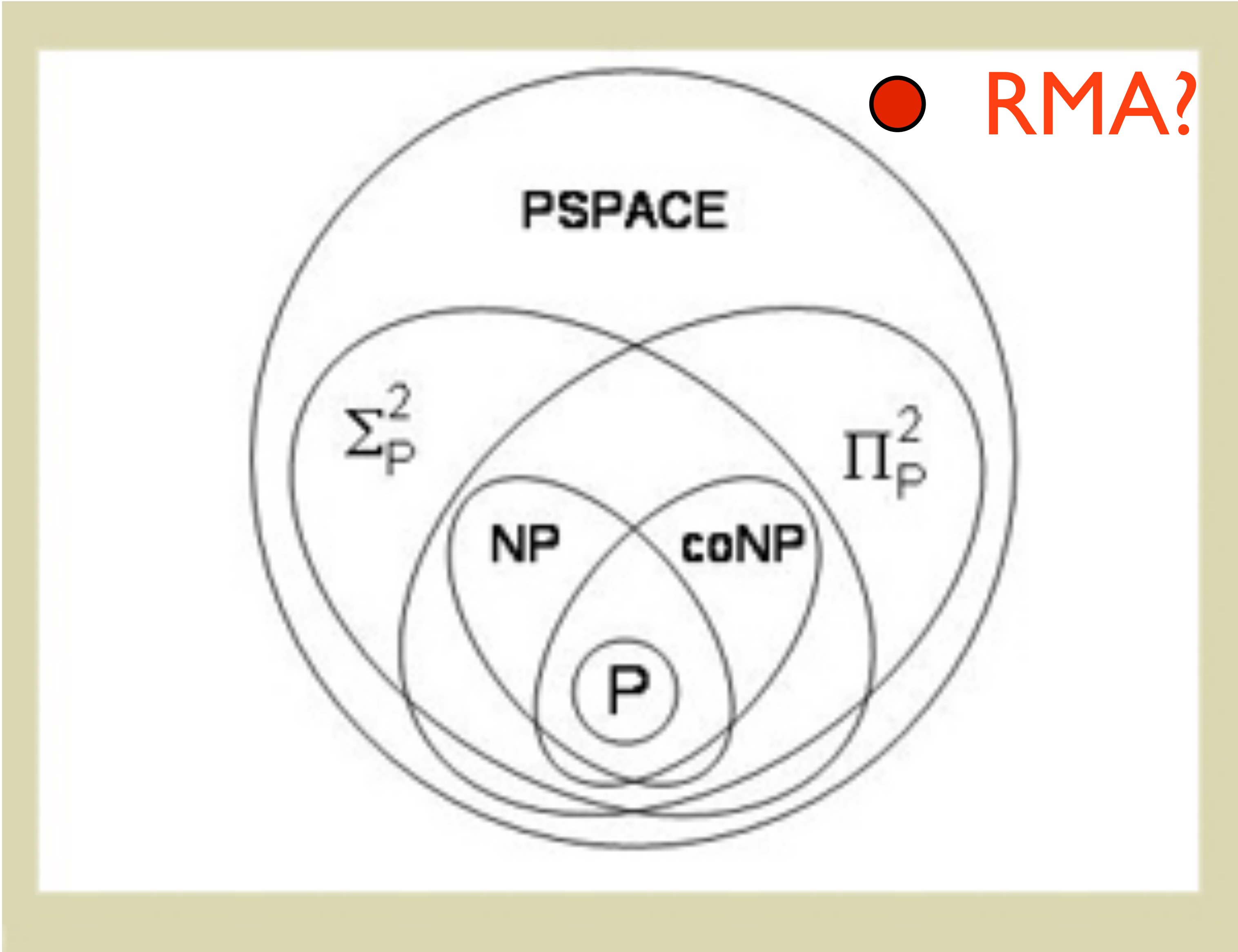
Our Central Question

Where does RMA fit?



Our Central Question

Where does RMA fit?



Theorem 1

$$\#P \subset RMA[?]$$

Theorem 1

$$\#P \subset RMA[1]$$

Theorem 1

$$\#P \subset RMA[1]$$

Remark: #P is not in MA unless polynomial hierarchy collapses!

Theorem 1

$$\#P \subset RMA[1]$$

Need to:

1. Formally define RMA[1]
2. Recall definition of #P
3. Prove the Theorem

RMA[1]

f(x)?

R(x,y)

π (x,y)

RMA[1]

f(x)?

y

R(x,y)

π (x,y)

RMA[1]

f(x)?

y

R(x,y) = 

R(x,y)

π (x,y)

RMA[1]

f(x)?

y

R(x,y) =

R(x,y)

π (x,y)

Choose y*

$$y^* = argmax_y E_r[R(x,y,r)]$$

RMA[1]

f(x)?

y

R(x,y) = 

R(x,y)

π (x,y*) =f(x)

Choose y*

$$y^* = argmax_y E_r[R(x,y,r)]$$

RMA[1]

$f:\{0,1\}^* \rightarrow \{0,1\}^*$ is in RMA[1] if there exist

1. A polynomial $p(n) > 0$

2. A randomized polynomial time function $R(x,y)$ such that, for every $x \in \{0,1\}^n$, there exists a unique $y^* \in \{0,1\}^{p(n)}$ maximizing $E[R(x,y)]$

3. A polynomial time function $\pi(x,y)$ such that $\pi(x,y^*) = f(x)$

Proof Sketch

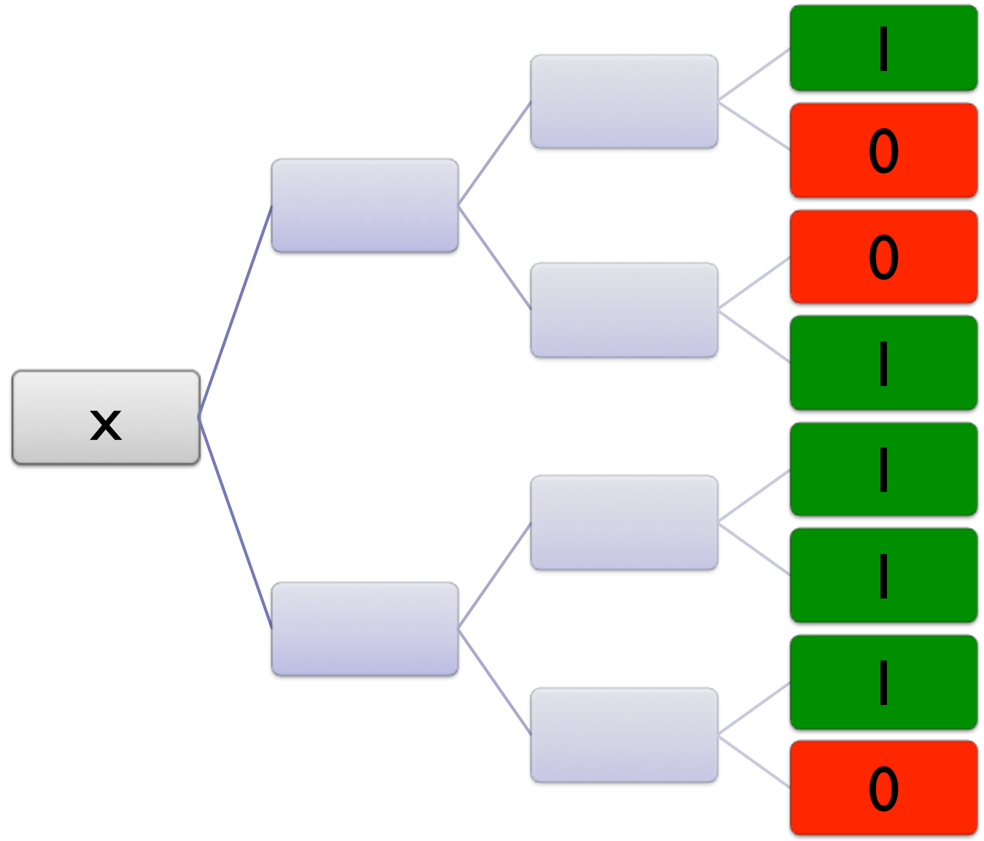
$$\#P \subset RMA[1]$$

Recall #P

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

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

$Output: \ \#\{y : M(x,y) = 1\}$



M ∈ P

#P Problems

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} ?

$2^{301} + 13$

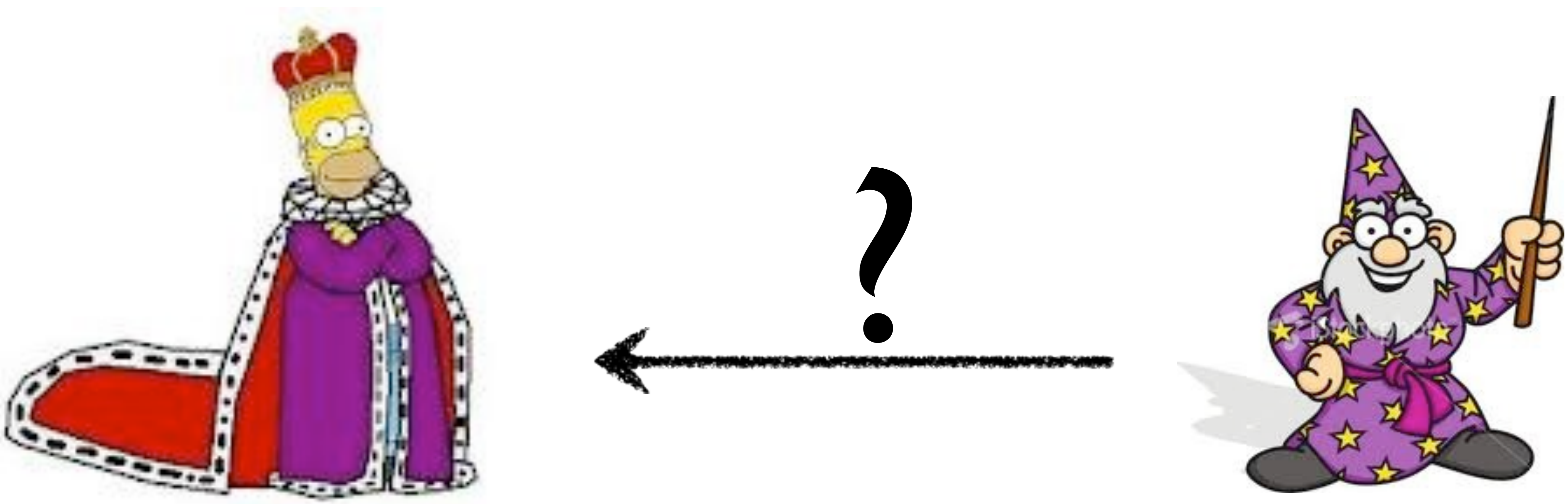
#P Problems

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

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

#{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} ?

$2^{301} + 13$

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

#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} ?

$2^{301} + 13$

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

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

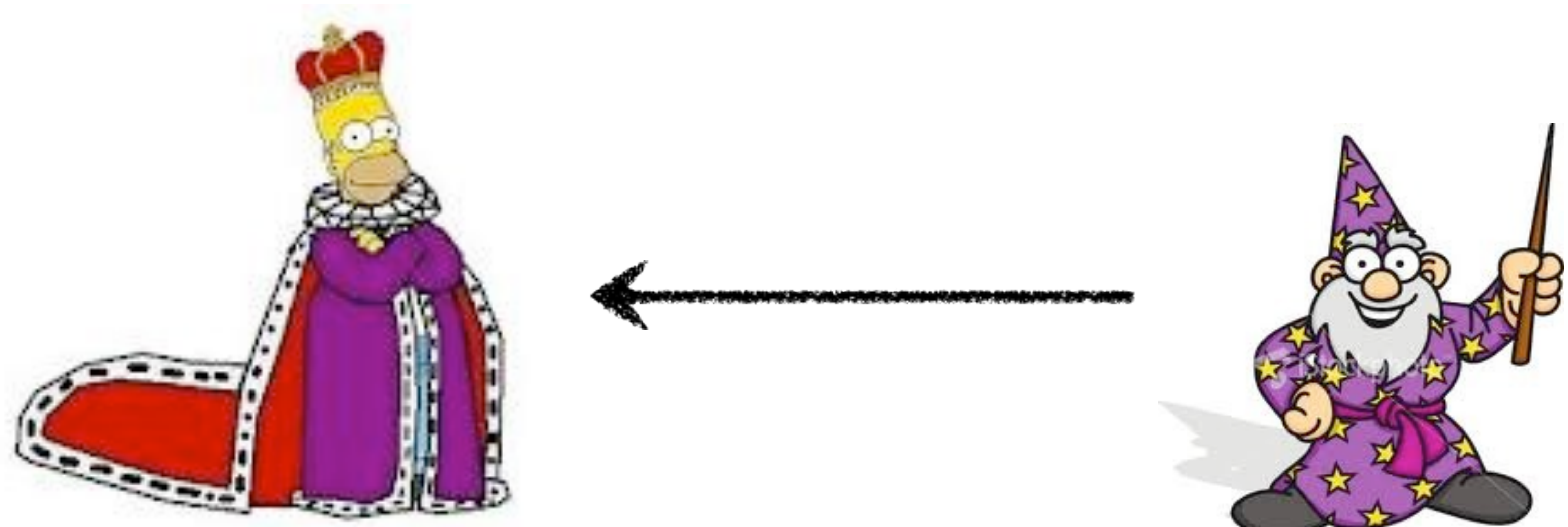
Merlin

What is information?

How do we guarantee it is correct?

Computation View

x, L

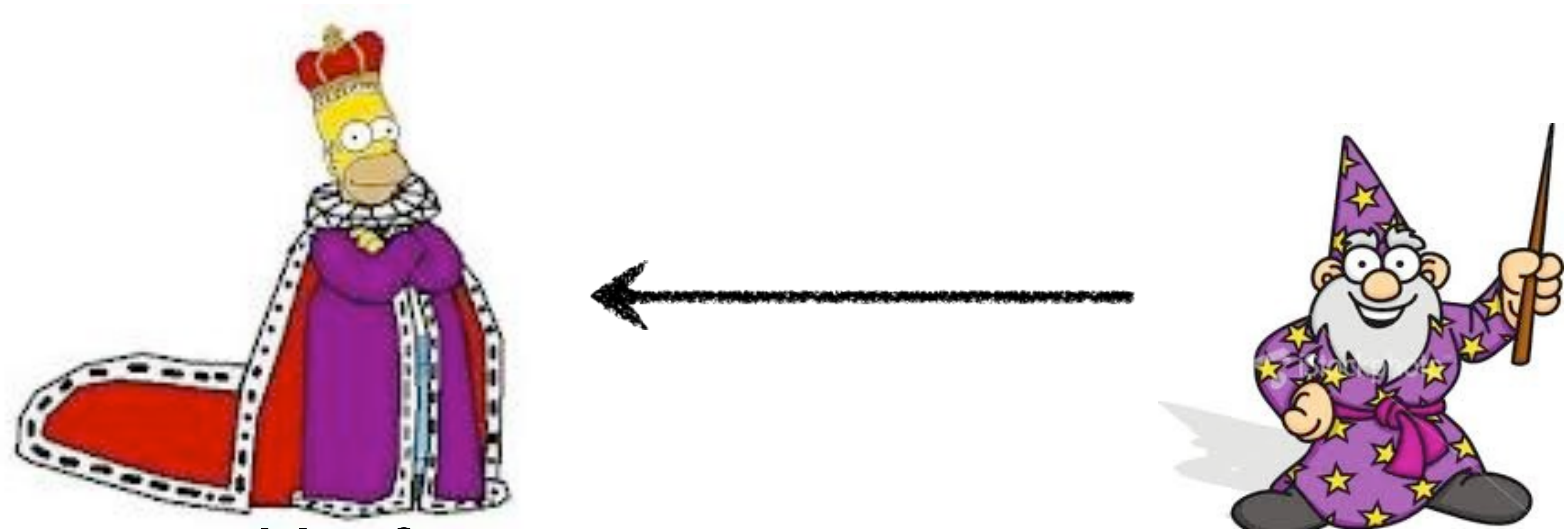


Verifier

Prover

Computation View

x, L



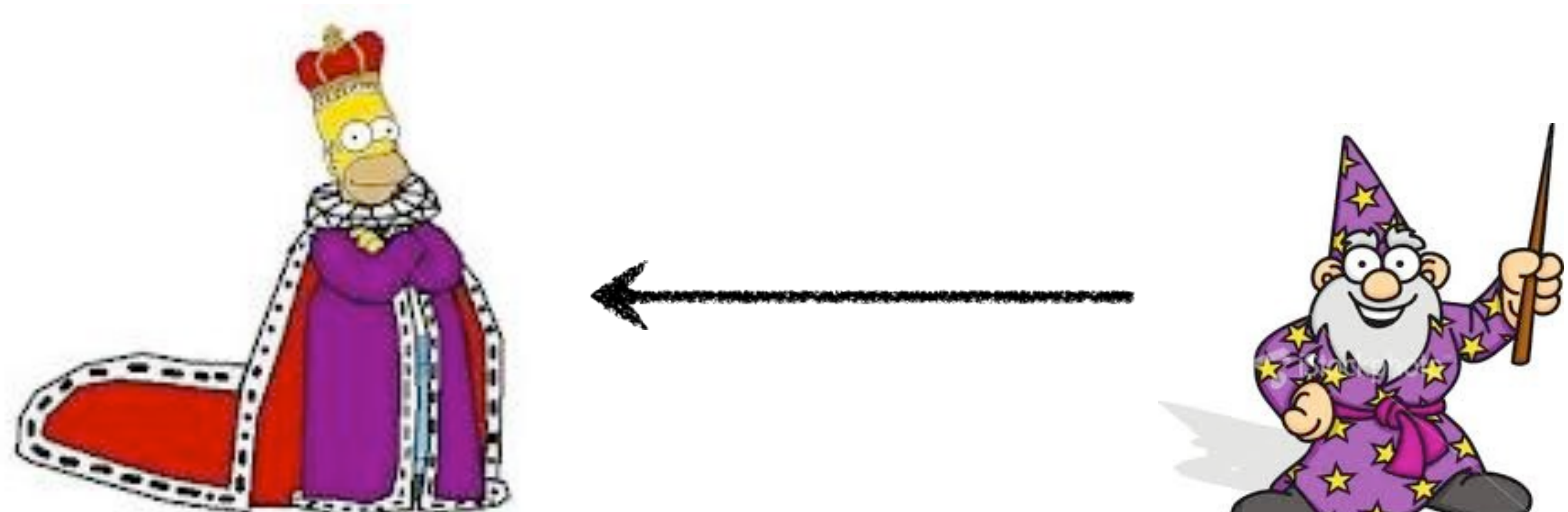
Verifier

Prover

Information is output of a hard to compute function

Computation View

x, L



Verifier

Prover

Information is output of a hard to compute function

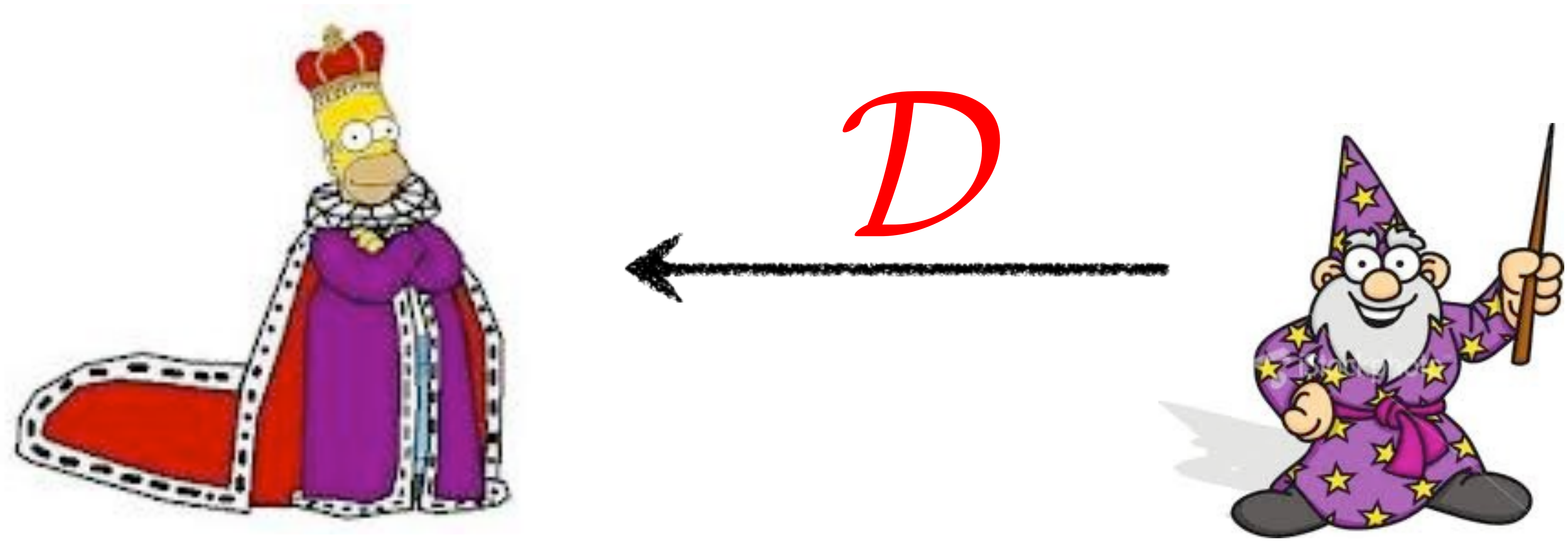
Correctness guaranteed by proof

Economics View

Principal

Agent

Economics View



Principal Agent

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

Economics View

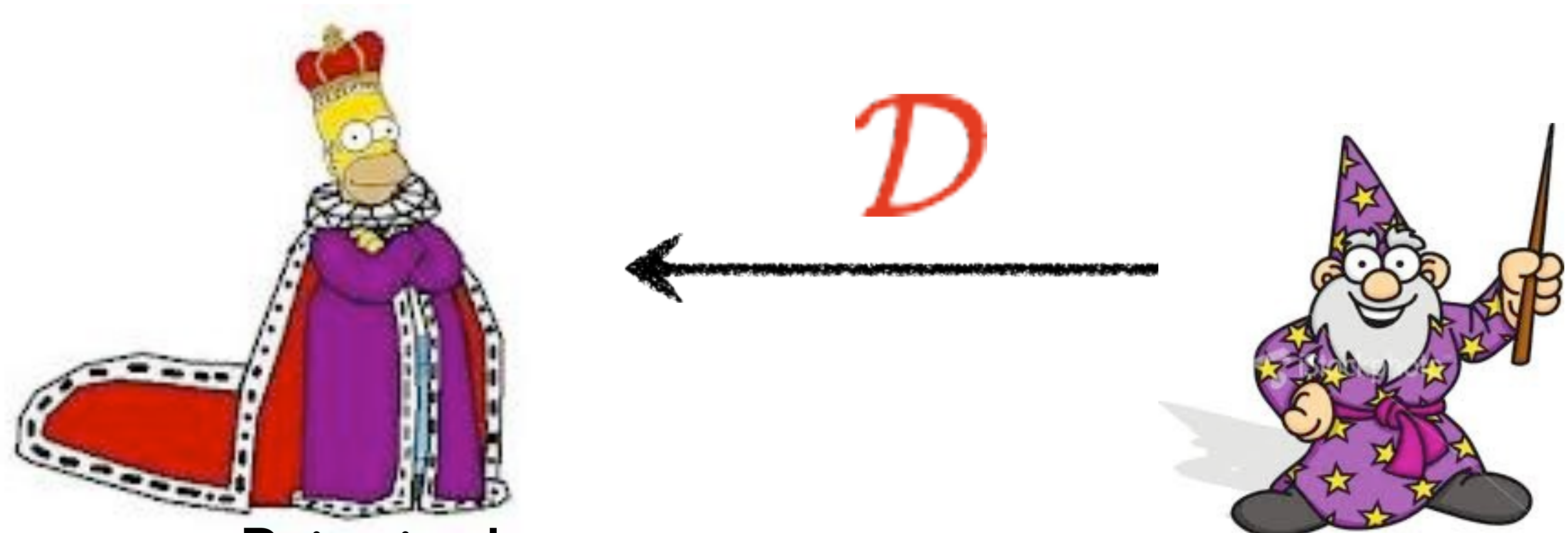
$\xleftarrow{\mathcal{D}}$

Principal Agent

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

Correctness from incentives

Economics View

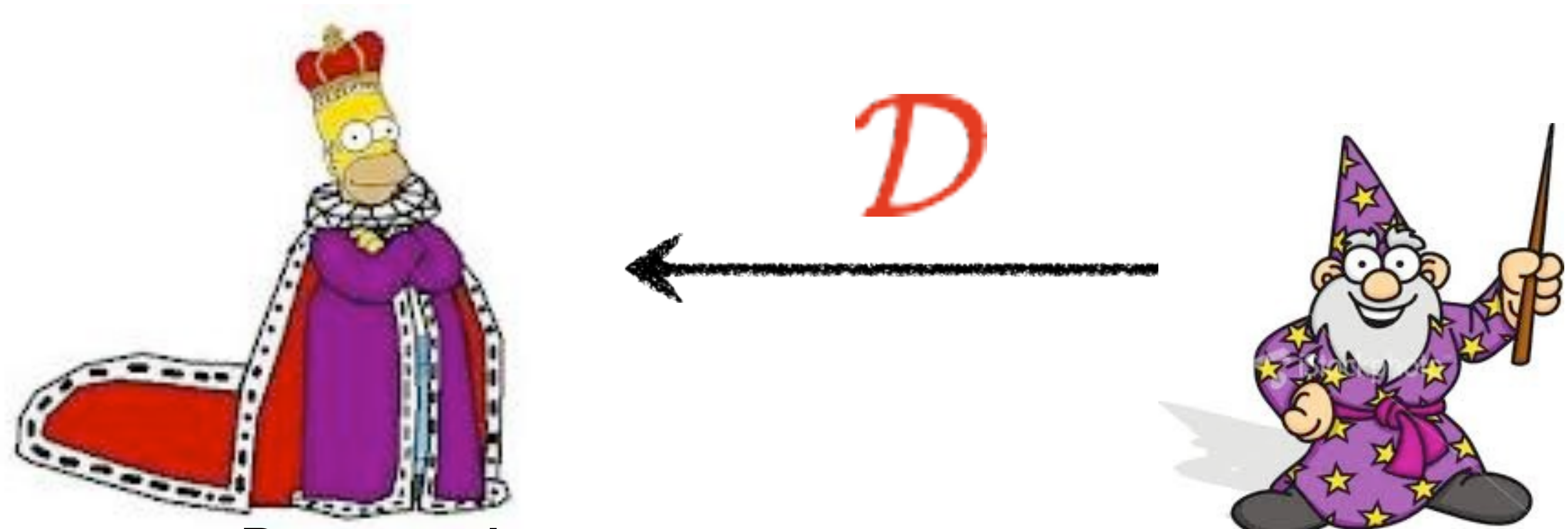


Principal

Agent

Q: How do we guarantee D is correct?

Economics View



Principal

Agent

Q: How do we guarantee D is correct?

A: Proper Scoring Rules!

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]

$\Omega = \{$ BOSTON RED SOX , NY $\}$

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

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

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

$\mathcal{D}$ ←

Proper Scoring Rules

[Good 52, Brier 50]

$\Omega = \{ \; , \; \}$

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

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

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

$\mathcal{P}$

Proper Scoring Rules

[Good 52, Brier 50]

$\Omega = \{$ Boston Red Sox , New York Yankees $\}$

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

$\omega \leftarrow \mathcal{D}$

$\mathcal{P}$

$\longleftarrow$

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

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

Proper Scoring Rules

[Good 52, Brier 50]

$\Omega = \{$ BOSTON RED SOX , NY $\}$

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

$\omega \leftarrow \mathcal{D}$

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

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

$\mathcal{P}$

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

Proper Scoring Rules

$\Omega = \{\ \text{[Boston Red Sox logo]}\ ,\qquad \}, \mathcal{D} \in \Delta(\Omega)$

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

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

$\omega \leftarrow \mathcal{D}$

$\mathcal{P}$

$\longleftarrow$

$= S(\mathcal{P},\ \text{[Boston Red Sox logo]}\ )$

$\longrightarrow$

Proper Scoring Rules

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

$\omega \leftarrow \mathcal{D}$

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

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

$\mathcal{P}$

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

Proper Scoring Rules

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

$\omega \leftarrow \mathcal{D}$

$$\mathcal{D}(Boston) = 60\%$$
$$\mathcal{D}(NewYork) = 40\%$$

$\mathcal{P}$

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

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

Proper Scoring Rules

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

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

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

$\omega \leftarrow \mathcal{D}$

$\mathcal{P}$

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

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

Quadratic Scoring Rule

[Brier 1950]

$$S(\mathcal{D}, \omega) = 2\mathcal{D}(\omega) - \sum_{x \in supp(\mathcal{D})} \mathcal{D}(x)^2 - 1$$

Quadratic Scoring Rule

[Brier 1950]

$$S(\mathcal{D}, \omega) = 2\mathcal{D}(\omega) - \sum_{x \in supp(\mathcal{D})} \mathcal{D}(x)^2 - 1$$

Truthful
Bounded

Quadratic Scoring Rule

[Brier 1950]

$$S(\mathcal{D}, \omega) = 2\mathcal{D}(\omega) - \sum_{x \in supp(\mathcal{D})} \mathcal{D}(x)^2 - 1$$

1. D hard to encode
2. S hard to compute
3. Different settings

Quadratic Scoring Rule

[Brier 1950]

$$S(\mathcal{D}, \omega) = 2\mathcal{D}(\omega) - \sum_{x \in supp(\mathcal{D})} \mathcal{D}(x)^2 - 1$$

1. D hard to encode
2. S hard to compute
3. Different settings

#P Problems

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

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

$2^{301} + 13$

#P Problems

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

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

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

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

Reduce the problem to question about probabilities

#P Problems

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

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

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

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

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

Need to incentivize him to reveal q

How do scoring rules apply?

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

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

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

How do scoring rules apply?

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

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

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

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

How do scoring rules apply?

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

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

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

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

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

How do scoring rules apply?

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

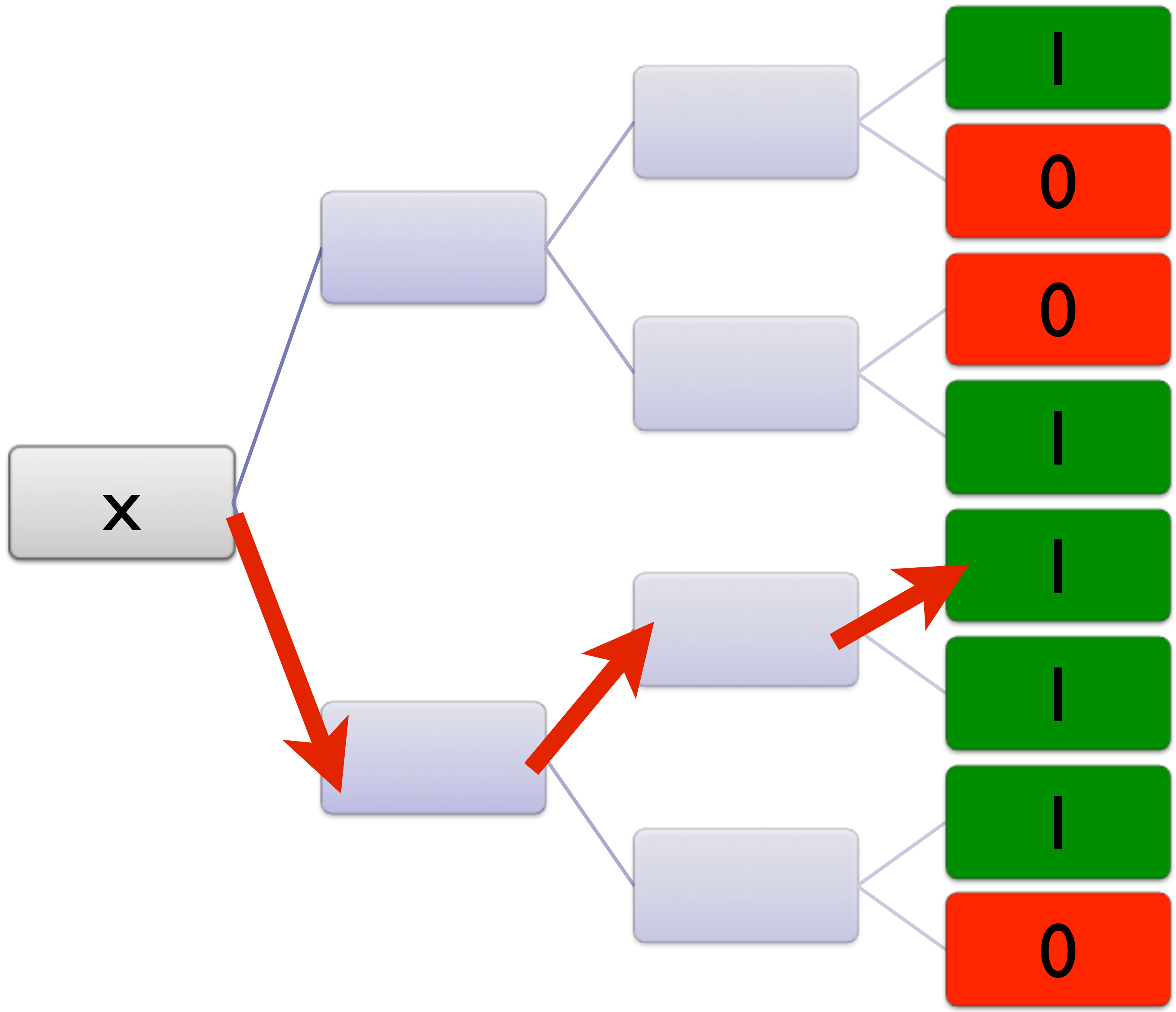
$$\mathcal{D}(1) = Pr_y[M(x,y) = 1]$$

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

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

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

Sampling ω = M(x,Unif)



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

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

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

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

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

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

$$\mathcal{P}$$

Our Rational Proof for #P

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

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

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

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

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

$$\mathcal{P}$$

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

Our Rational Proof for #P

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

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

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

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

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

$$\mathcal{P}$$

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

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

Theorem 1

$$\#P \subset RMA[1]$$

Theorem 1

$$\#P \subset RMA[1]$$

Zero-Knowledge Rational Proof!

Theorem 1

$$\#P \subset RMA[1]$$

Zero-Knowledge Rational Proof!

Computationally Sound Rational Proof!

Theorem 2

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

Theorem 2

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

There are things money can't buy

Theorem 2

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

Economics View: Computational Limit on Contracts

Proof Sketch

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

RMA[1]

A Language L is in RMA[1] if there exist

1. A polynomial p(n)
2. A randomized polynomial time function R(x,y) such that, for every $x \in \{0,1\}^n$, there exists a unique $y^* \in \{0,1\}^{p(n)}$ maximizing $E[R(x,y)]$
3. A polynomial time predicate $\pi(x,y)$ such that $\pi(x,y^*) = L(x)$

RMA[1]

A Language L is in RMA[1] if there exist

1. A polynomial p(n)
2. A randomized polynomial time function R(x,y) such that, for every $x \in \{0,1\}^n$, there exists a unique $y^* \in \{0,1\}^{p(n)}$ maximizing $E[R(x,y)]$
3. A polynomial time predicate $\pi(x,y)$ such that $\pi(x,y^*) = L(x)$

Need to show any such L is in $NP^{\#P}$

Use $NP^{\#P}$ to find y* that maximizes E[R(x,y)]

Use $NP^{\#P}$ to find y* that maximizes E[R(x,y)]

- f(y) = E[R(x, y)] only takes $2^{poly(n)}$ possible values

Use $NP^{\#P}$ to find y* that maximizes E[R(x,y)]

- f(y) = E[R(x, y)] only takes $2^{poly(n)}$ possible values

- f(y) can be computed in $P^{\#P}$ for a given y

Use $NP^{\#P}$ to find y* that maximizes E[R(x,y)]

- f(y) = E[R(x, y)] only takes $2^{poly(n)}$ possible values
- f(y) can be computed in $P^{\#P}$ for a given y
- Can non-deterministically choose y* maximizing f(y)

Use $NP^{\#P}$ to find y* that maximizes E[R(x,y)]

- $f(y) = E[R(x, y)]$ only takes $2^{poly(n)}$ possible values
- $f(y)$ can be computed in $P^{\#P}$ for a given y
- Can non-deterministically choose y* maximizing f(y)
- Given y*, can compute $\pi(x,y^*)$ in polynomial time to determine whether $x \in L$ or $x \notin L$

Computing $E[R(x,y)]$ in $P^{\#P}$

Computing E[R(x,y)] in $P^{\#P}$

- More generally, let g(x) be a randomized polynomial time function

Computing E[R(x,y)] in $P^{\#P}$

- More generally, let g(x) be a randomized polynomial time function
- Will show that $E_r[g(x,r)]$ can be computed in $P^{\#P}$

Computing E[R(x,y)] in $P^{\#P}$

- More generally, let g(x) be a randomized polynomial time function
- Will show that $E_r[g(x,r)]$ can be computed in $P^{\#P}$
- Let z = g(x,r). Let z_i be its i^{th} bit.

Computing E[R(x,y)] in $P^{\#P}$

- More generally, let g(x) be a randomized polynomial time function
- Will show that $E_r[g(x,r)]$ can be computed in $P^{\#P}$
- Let z = g(x,r). Let z_i be its i^{th} bit.
- It suffices to compute $E_r[z_i]$. Let M_i be randomized polynomial time Turing Machine computing $z_i = g_i(x,r)$

Computing E[R(x,y)] in $P^{\#P}$

- More generally, let g(x) be a randomized polynomial time function
- Will show that $E_r[g(x,r)]$ can be computed in $P^{\#P}$
- Let z = g(x,r). Let z_i be its i^{th} bit.
- It suffices to compute $E_r[z_i]$. Let M_i be randomized polynomial time Turing Machine computing $z_i = g_i(x,r)$
- $E_r[z_i]$ is proportional to the number of accepting paths in M_i. Thus, it can be computed with a #P query.

Results so far

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

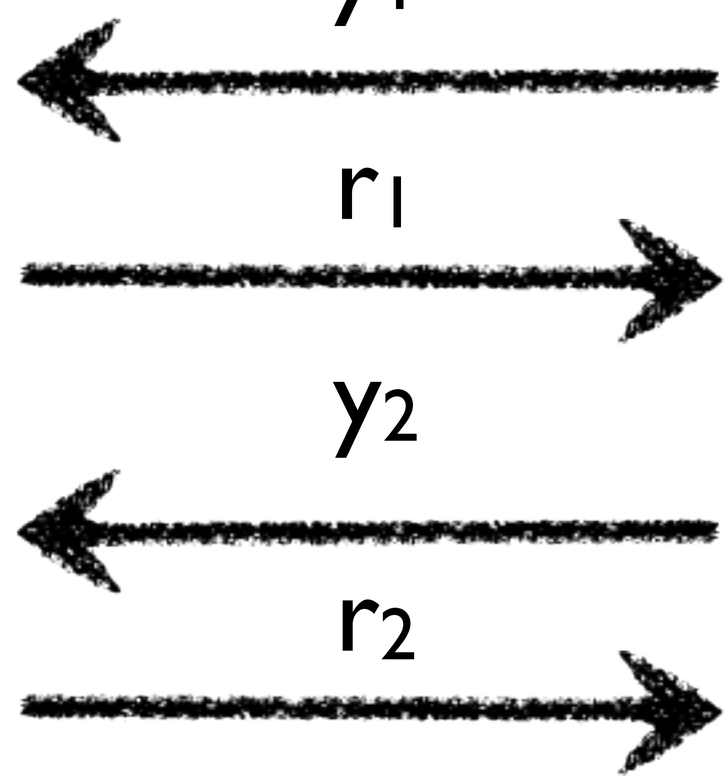
Results so far

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

- Rational Merlin Arthur proofs much more powerful than classical Merlin Arthur
- Only one round used
- What if we have more rounds?

Rational MA

x in L?



π output function

R reward function

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

$R(x,T^*) =$ 

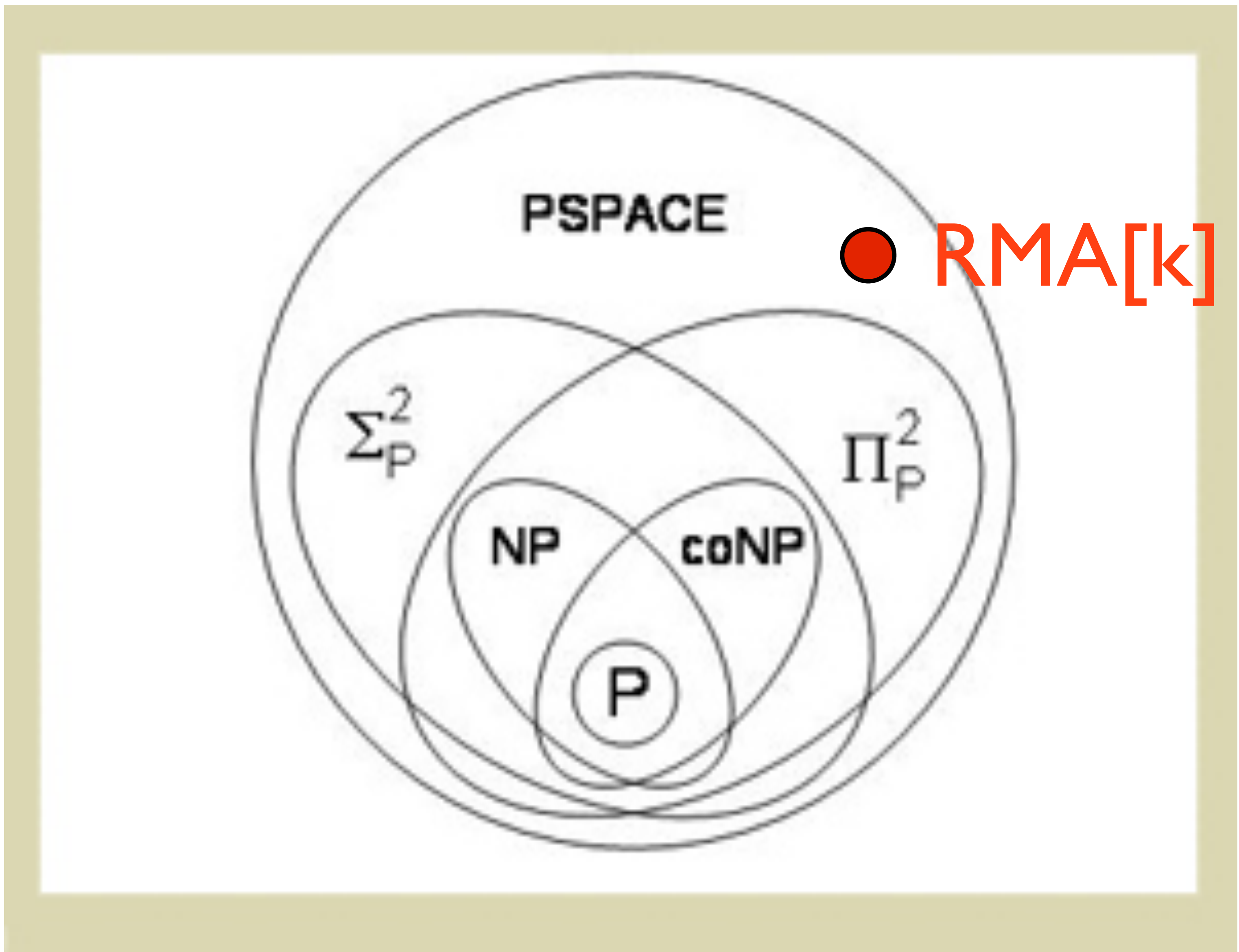
Merlin chooses Transcript T* that maximizes E[R(x,T)]

Our Next Question

Where does RMA[2] fit?

What about RMA[3]?

RMA[64]?

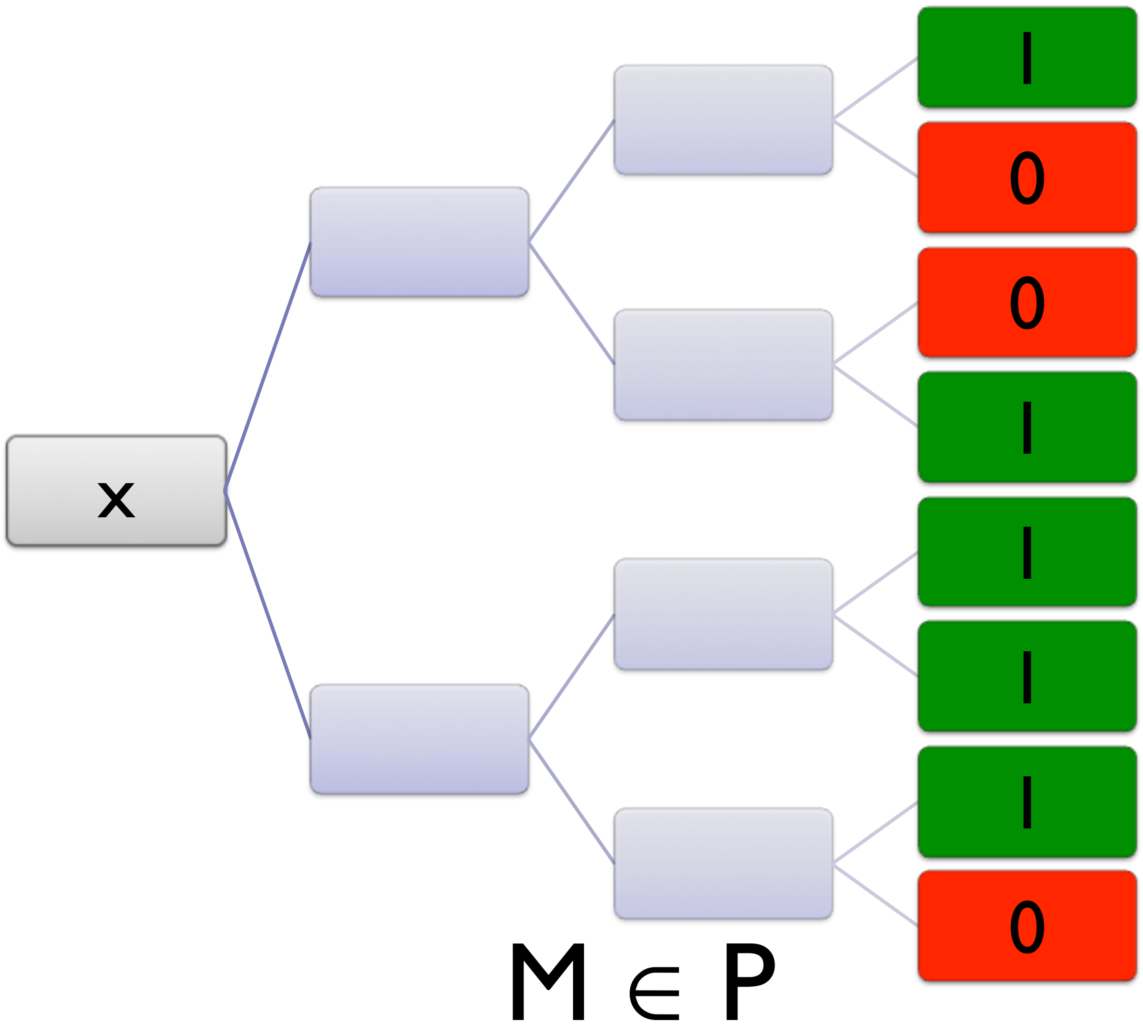


The Counting Hierarchy

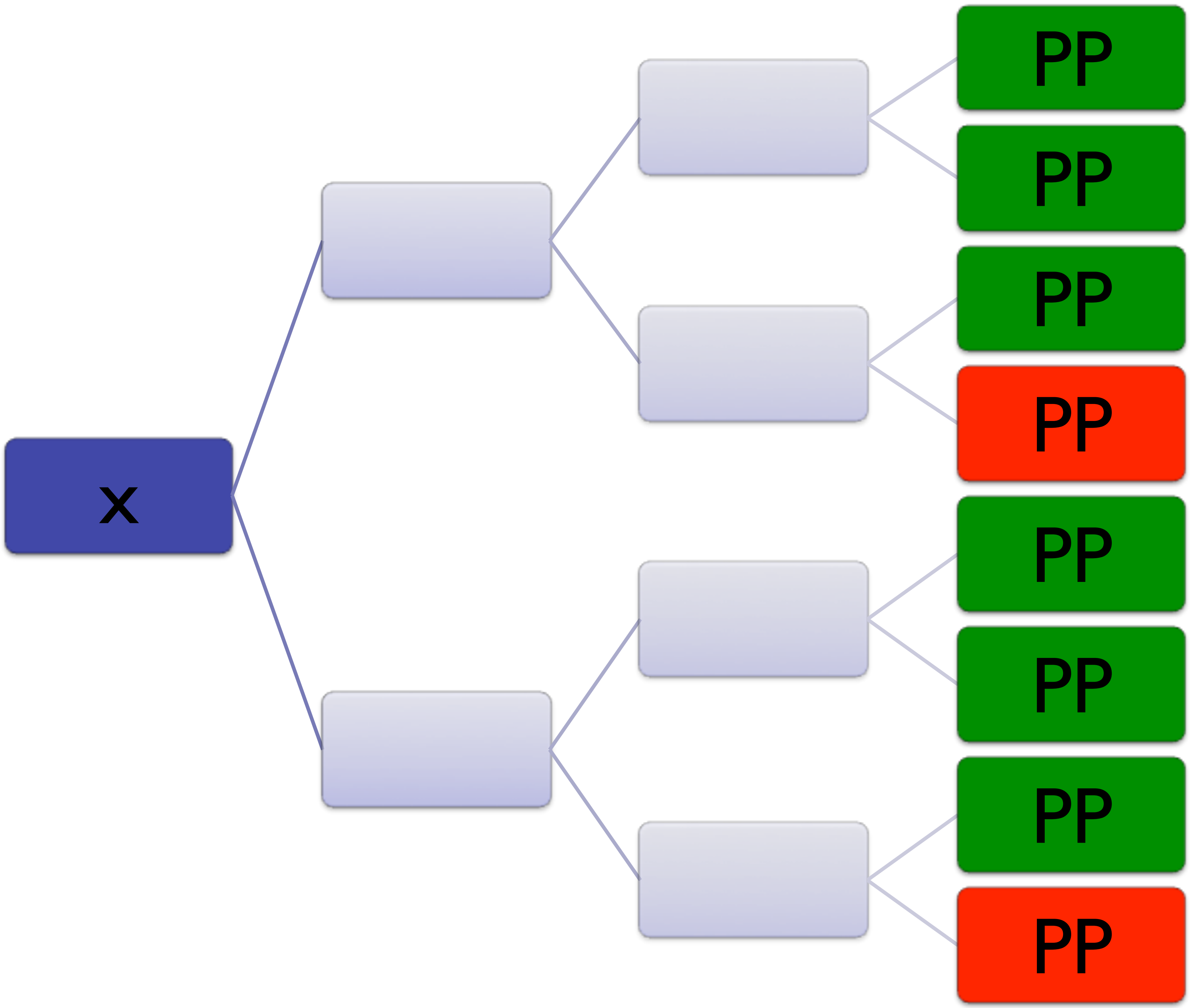
$CP_1 = PP$

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

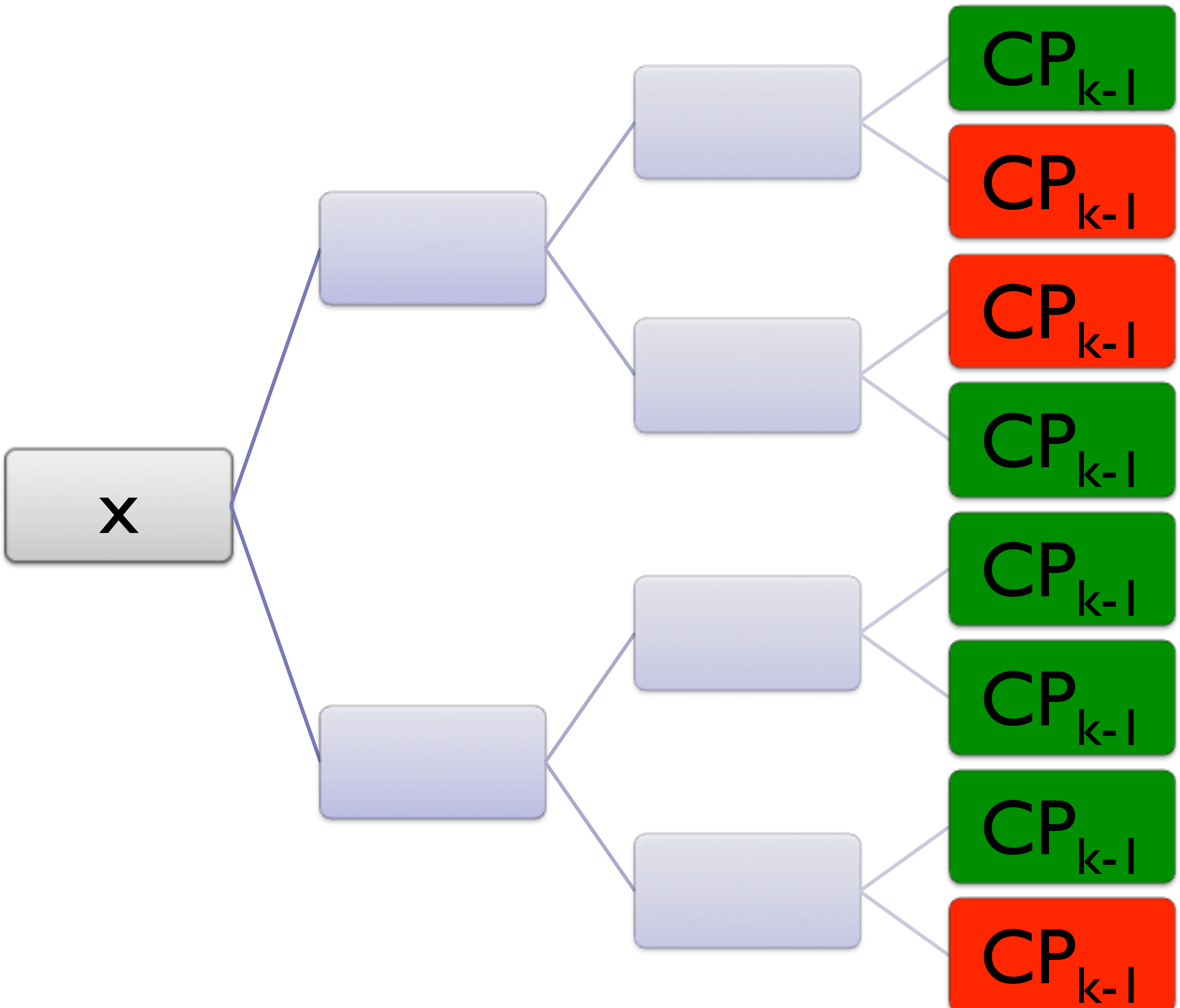
$Output : |y : M(x,y) = 1| > |y : M(x,y) = 0|?$



$$CP_2 = PP^{PP}$$

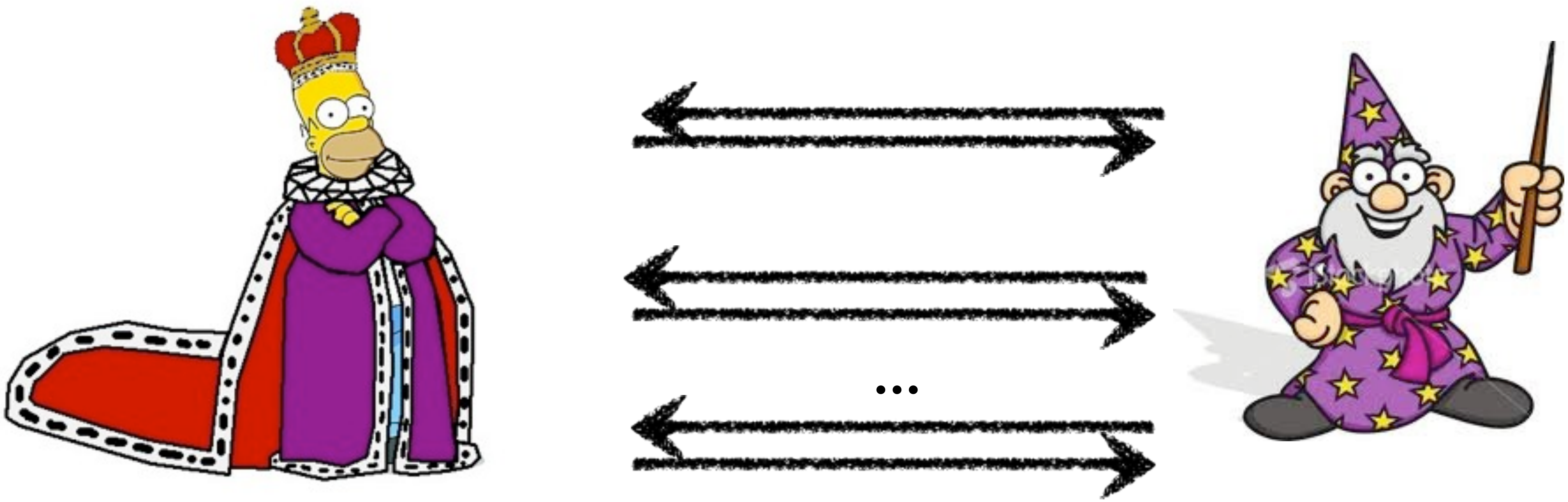


$$CP_k = PP^{CP_{k-1}} = PP^{PP^{\cdot^{\cdot^{\cdot^{PP}}}}}$$

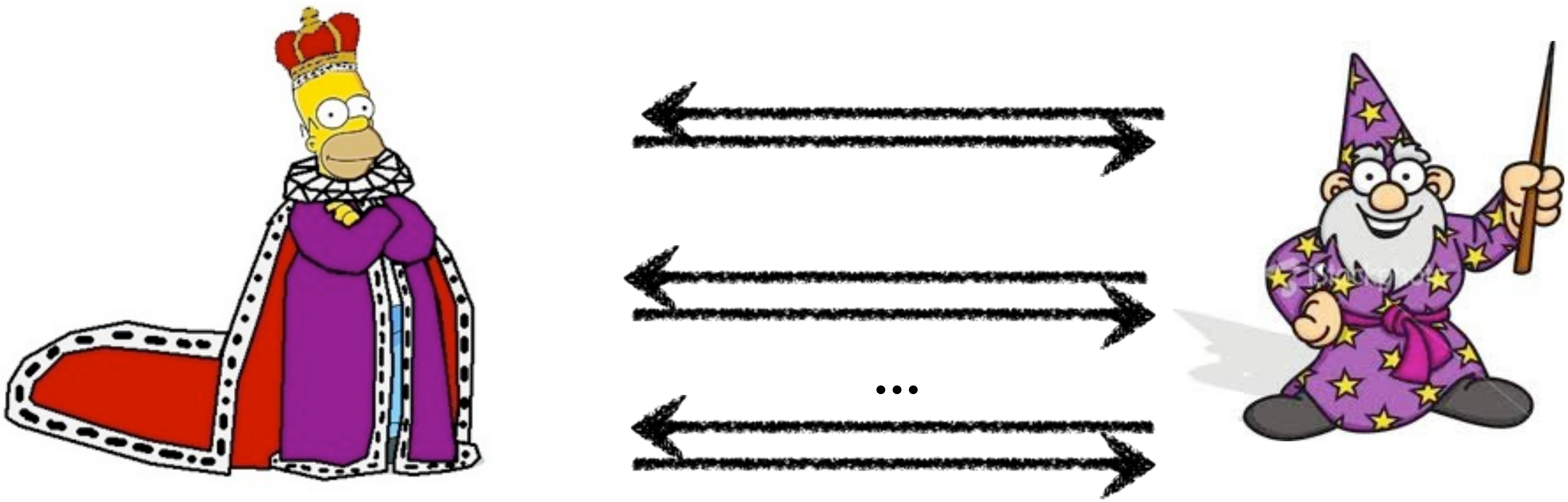


[Wagner, Toran]

Theorem 3

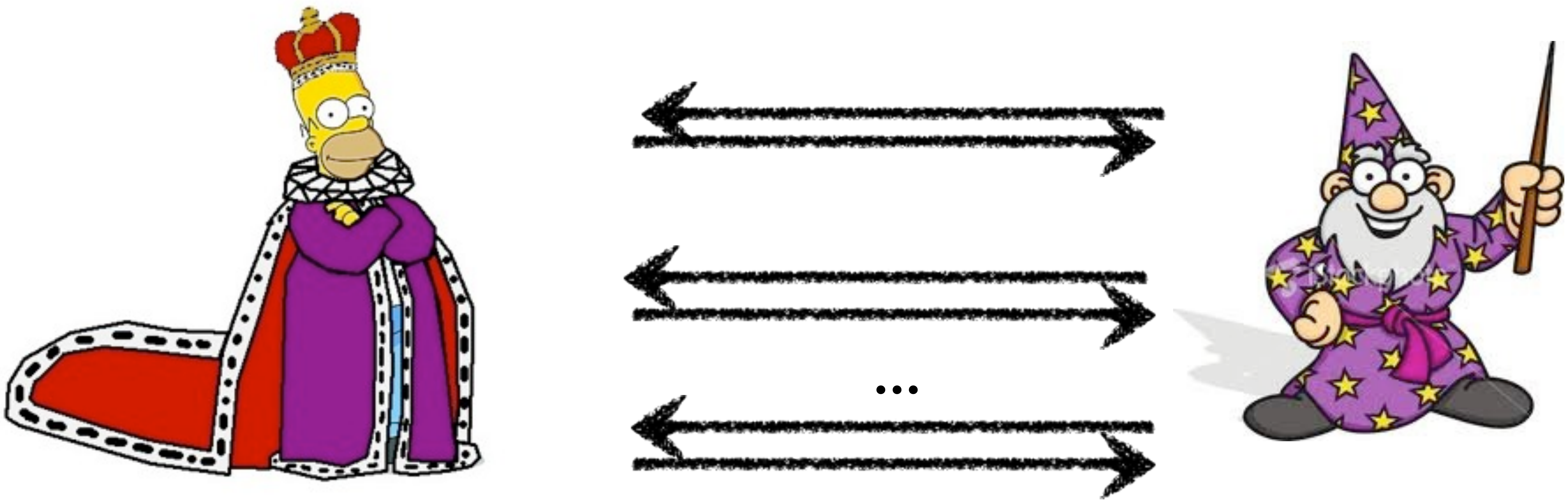


Theorem 3



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

Theorem 3

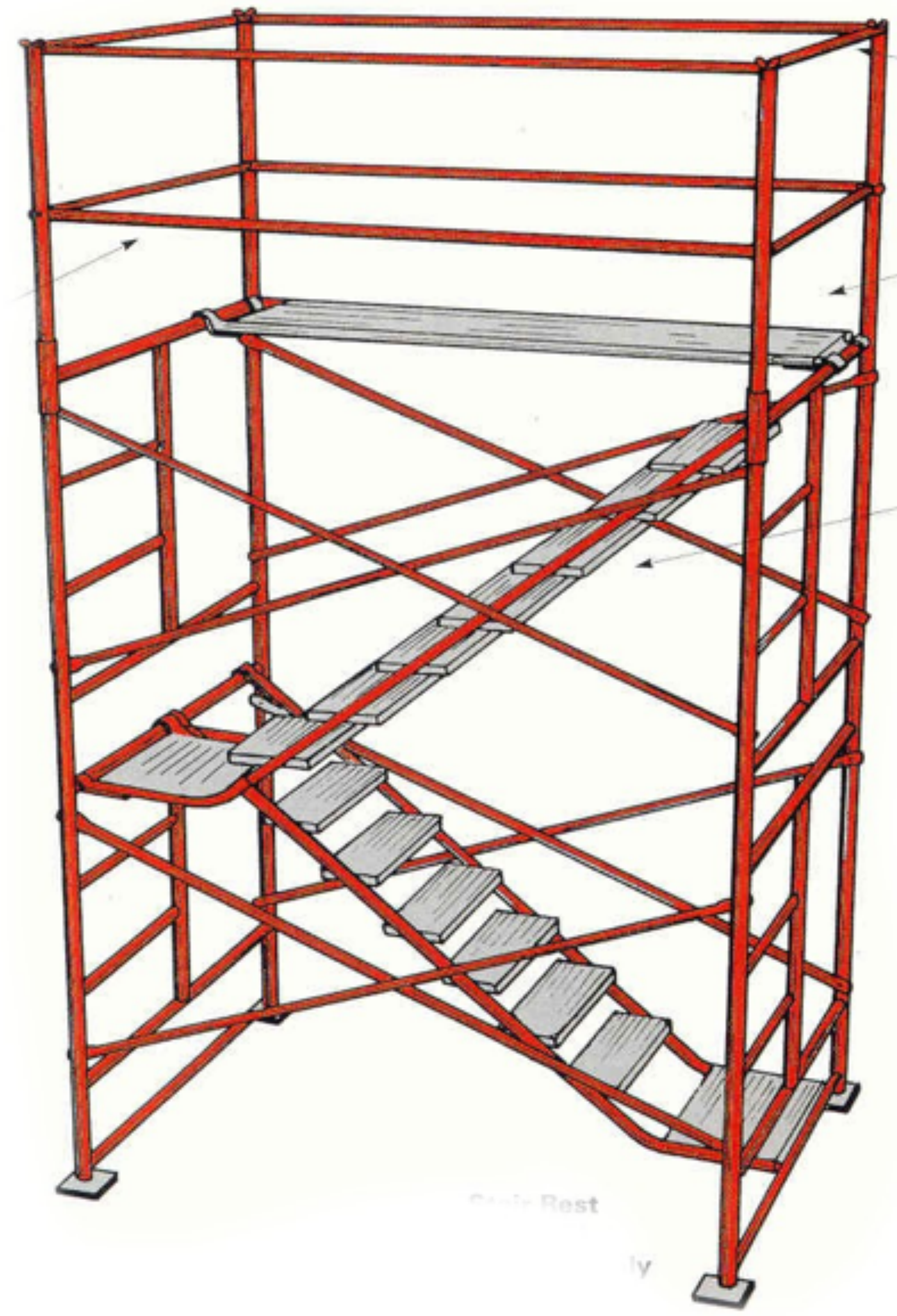


$$CP_k \subset RMA[k] \subset CP_{k+1}$$

$$P^{PP} \subset RMA[1] \subset NP^{PP} \subset PP^{PP} \subset RMA[2] \subset PP^{PP^{PP}} \ldots$$

Open Question

Does CH Collapse?



Old Analogy

Q: Does CH Collapse?

A: Not if it behaves like PH

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

New Analogy

Q: Does CH Collapse?

A: Yes if it behaves like AM

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

Summary of Contributions

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

A tight connection

Proper Scoring Rules ⇄ Interactive Proofs

A tight connection

Proper Scoring Rules ⇄ Interactive Proofs

THANK YOU!

Proof Sketch

Proof Sketch

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

Our Rational Proof for PP

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

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

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

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

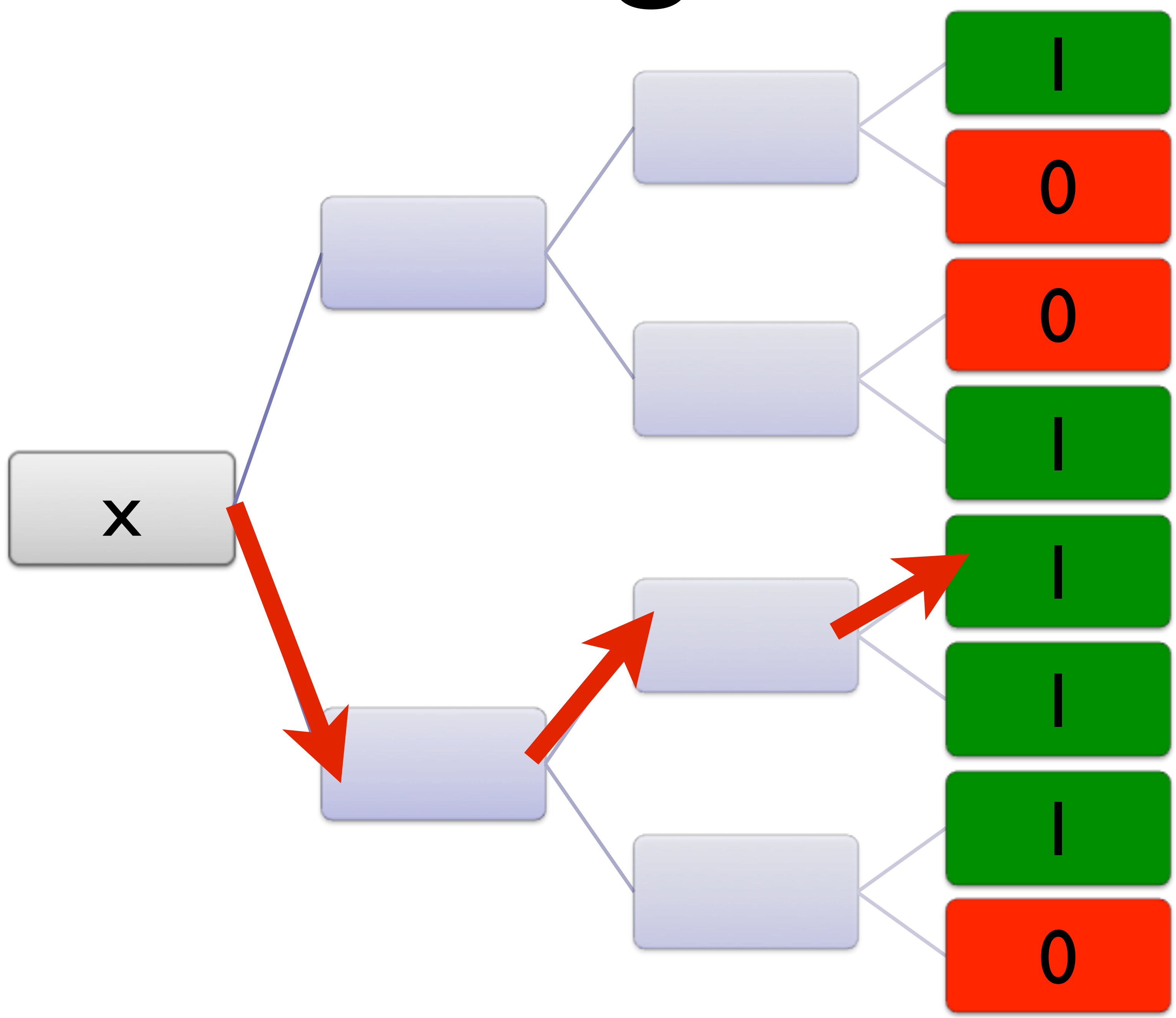
$$\mathcal{D}(0) = 1 - q$$

$$\mathcal{P}$$

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

Need to compute M(x,y)
Easy when M is polynomial time

Reminder: Generating ω for PP



Our Rational Proof for CP_k

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

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

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

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

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

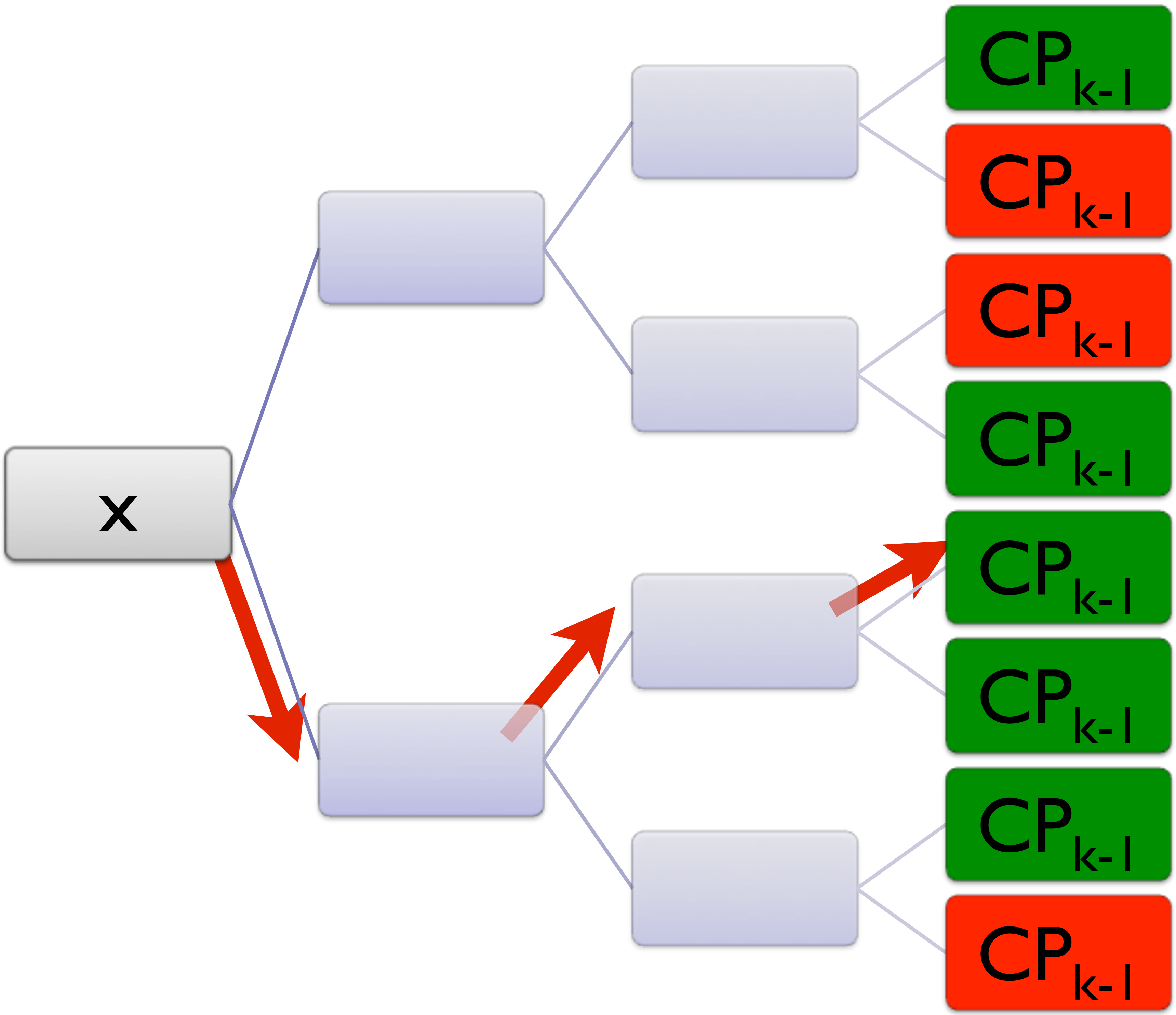
$$\mathcal{P}$$

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

Need to compute M(x,y)

Hard when M is CP_{k-1}

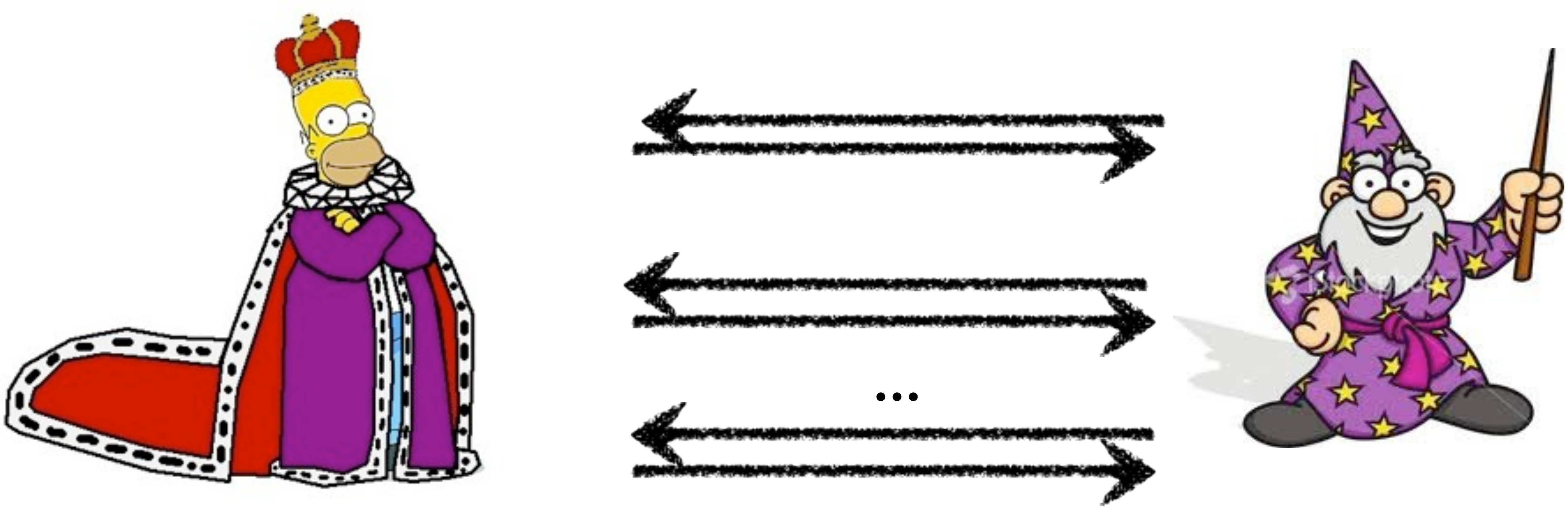
Generating ω for CP_k



$$CP_k \subset DRMA[k]$$

Define an intermediate class k-DRMA such that

$$CP_k \subset k\text{-}DRMA \subset DRMA[k]$$

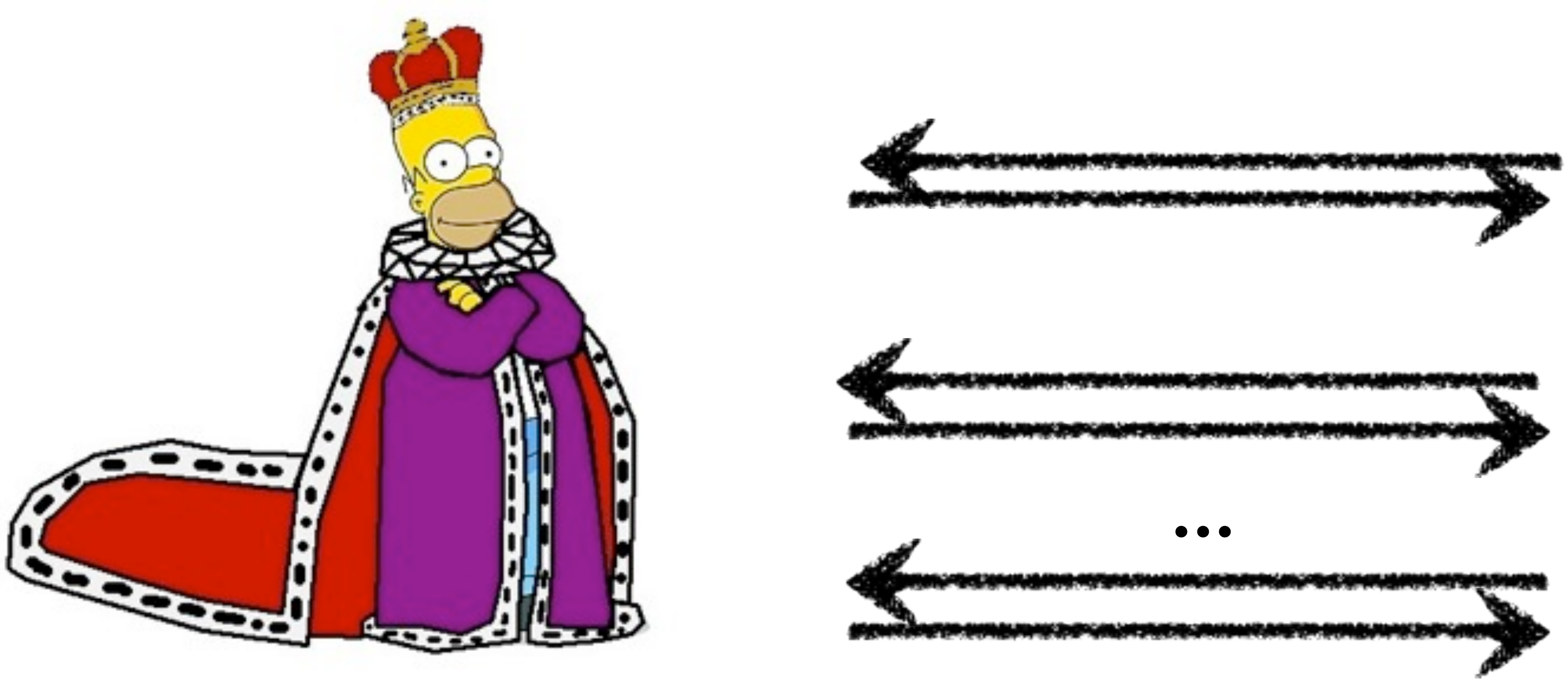


DRMA[k]

$$CP_k \subset DRMA[k]$$

Define an intermediate class k-DRMA such that

$$CP_k \subset k\text{-}DRMA \subset DRMA[k]$$

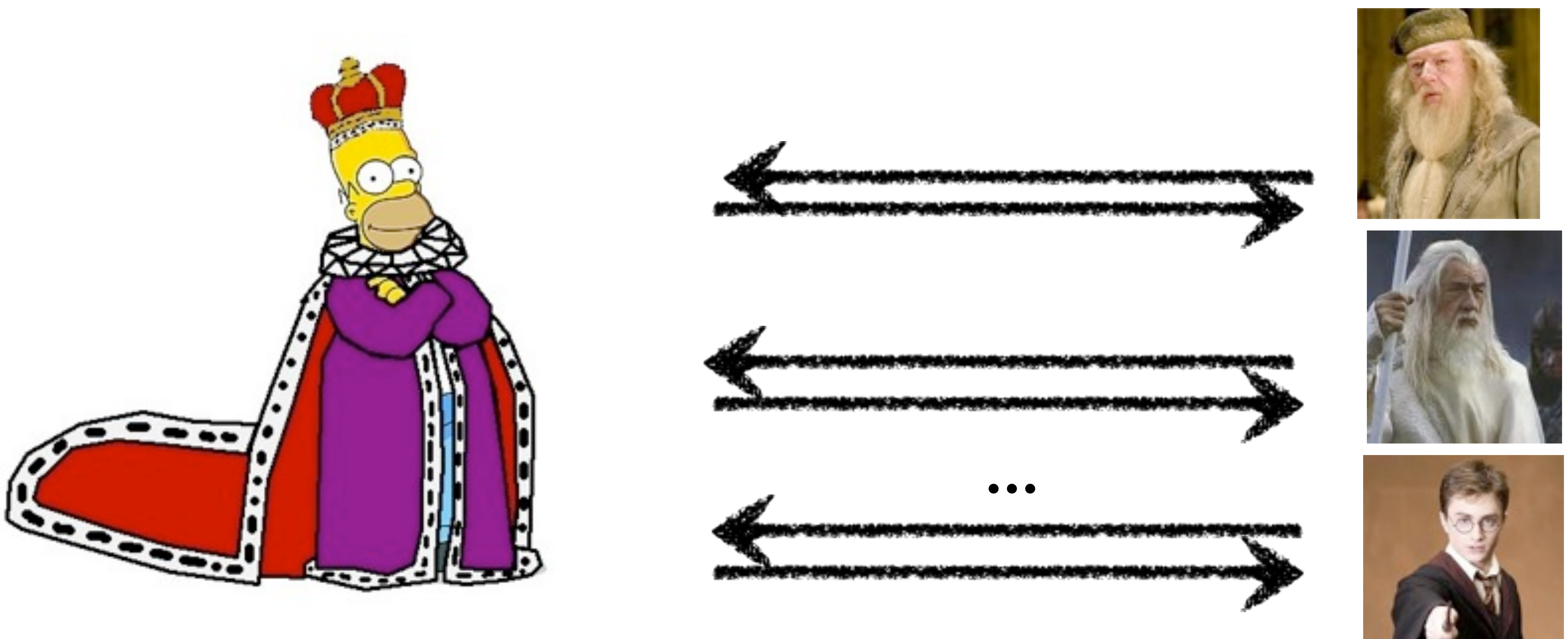


k-DRMA: Arthur interacts once with each of k Merlins

$$CP_k \subset DRMA[k]$$

Define an intermediate class k-DRMA such that

$$CP_k \subset k\text{-}DRMA \subset DRMA[k]$$



k-DRMA: Arthur interacts once with each of k Merlins

$CP_k \subset k\text{-}DRMA$

$CP_k \subset k\text{-}DRMA$

- By induction

$CP_k \subset k\text{-}DRMA$

- By induction
- Base case: $PP \subset 1\text{-}DRMA$ 

$CP_k \subset k\text{-}DRMA$

- By induction
- Base case: $PP \subset 1\text{-}DRMA$
- Assume $CP_{k-1} \subset (k-1) - DRMA$

$CP_k \subset k\text{-}DRMA$

- By induction
- Base case: $PP \subset 1\text{-}DRMA$ 
- Assume $CP_{k-1} \subset (k-1) - DRMA$
- Need to show $CP_k = PP^{CP_{k-1}} \subset k\text{-}DRMA$

Our Rational Proof for CP_k

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

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

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

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

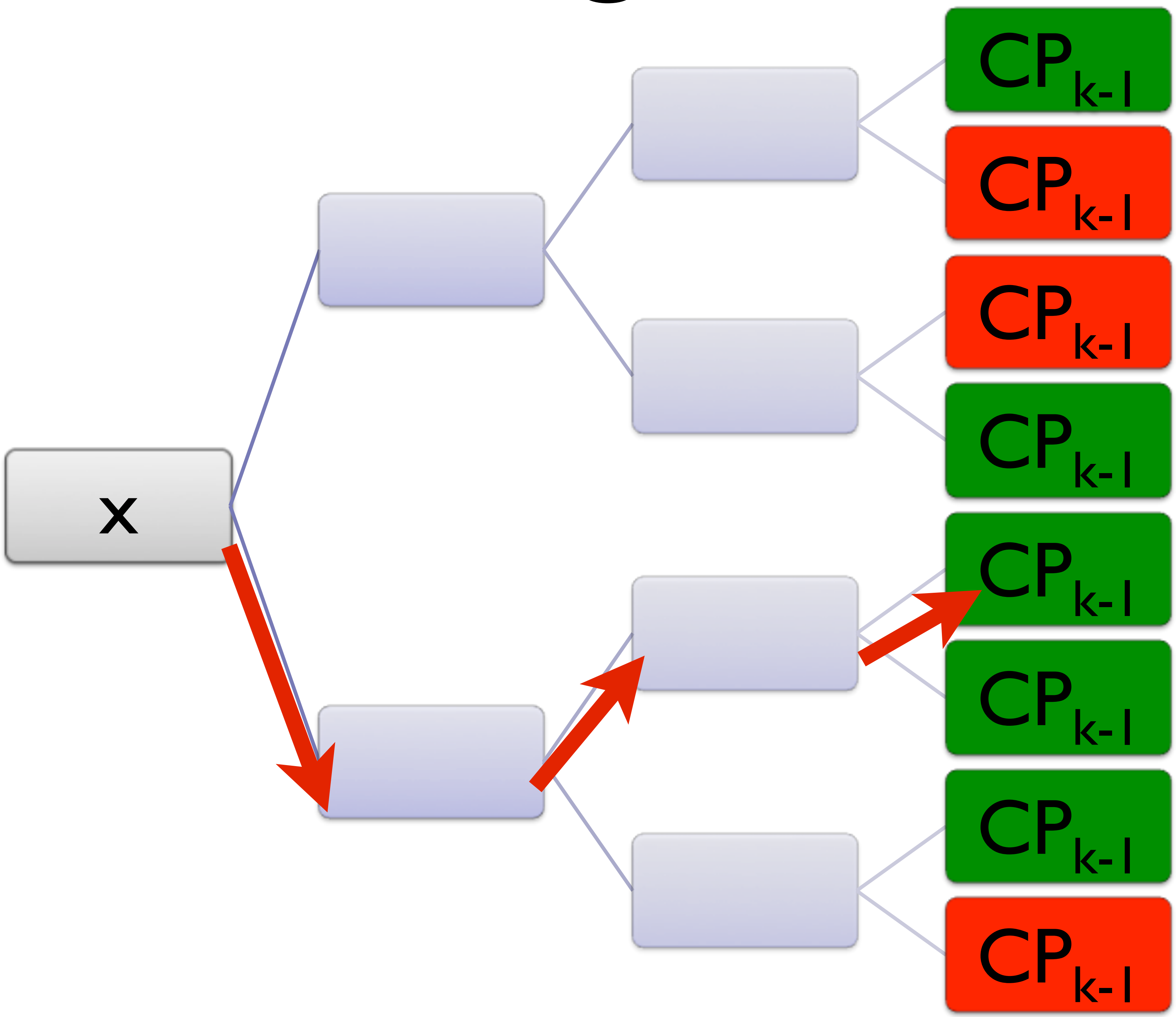
$$\mathcal{D}(0) = 1 - q$$

$$\mathcal{P}$$

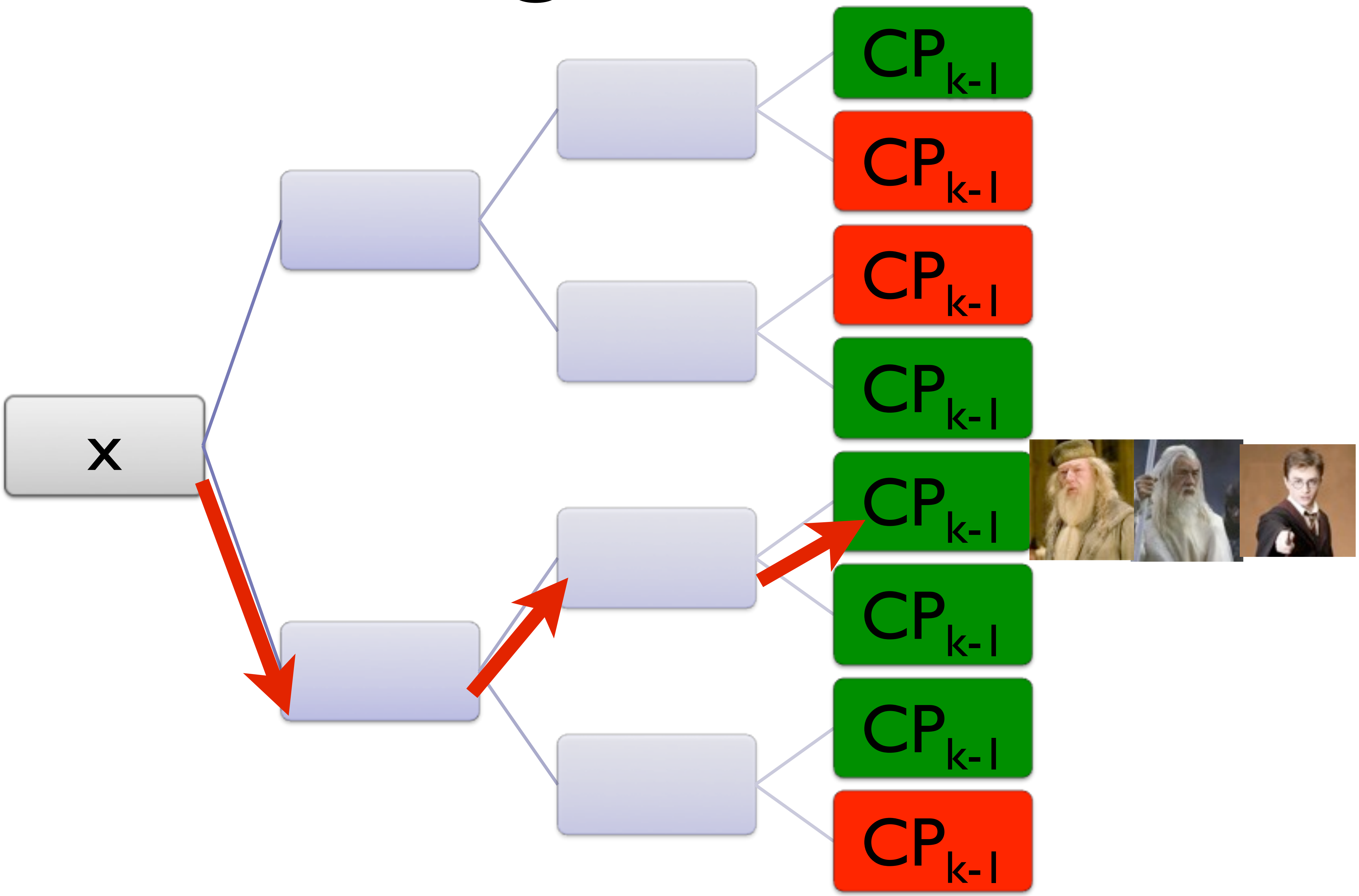
$$= S(\mathcal{P}, \omega)$$

Need to compute M(x,y)
Hard when M is CP_{k-1}

Generating ω for CP_k

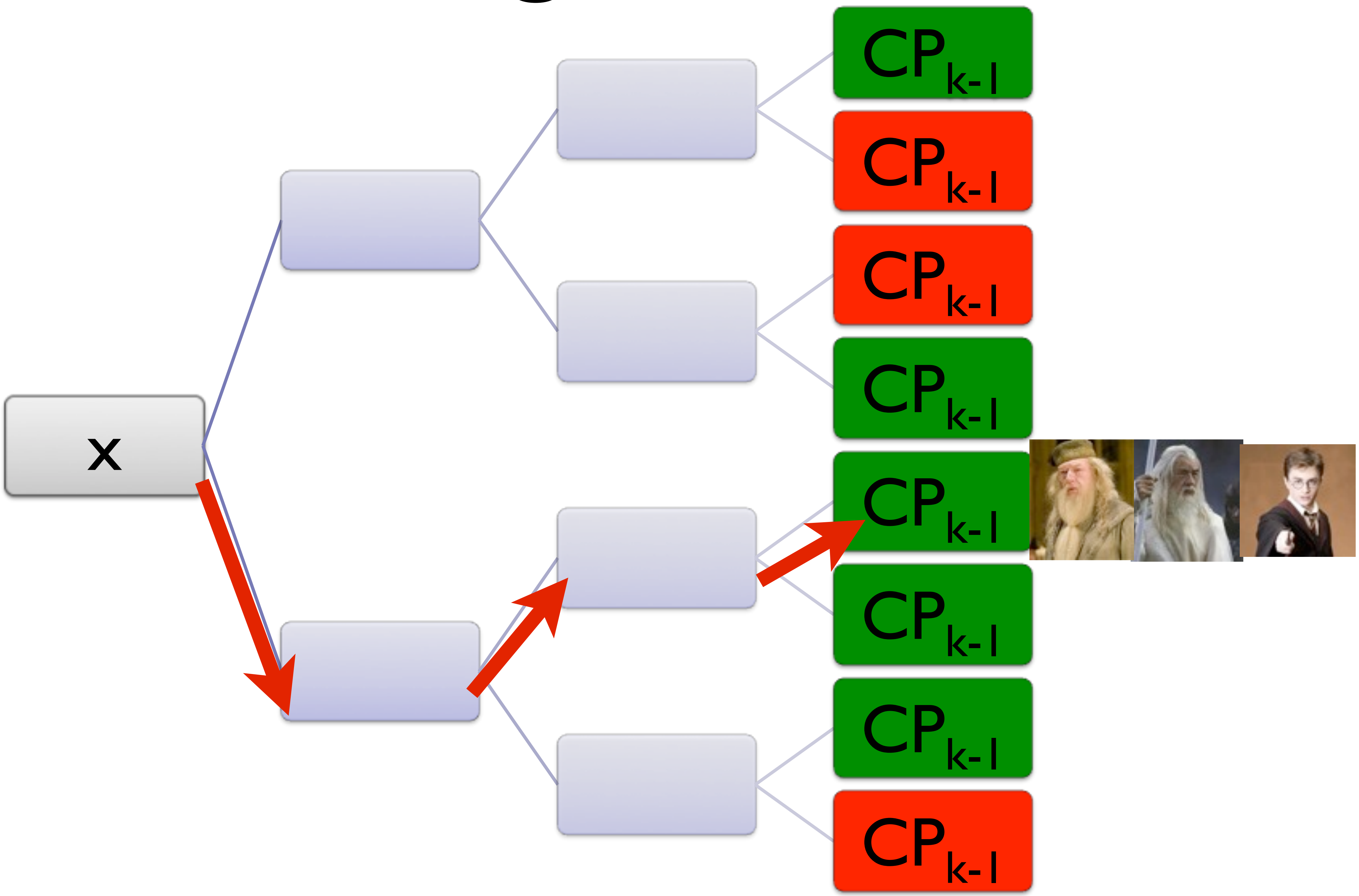


Generating ω for CP_k



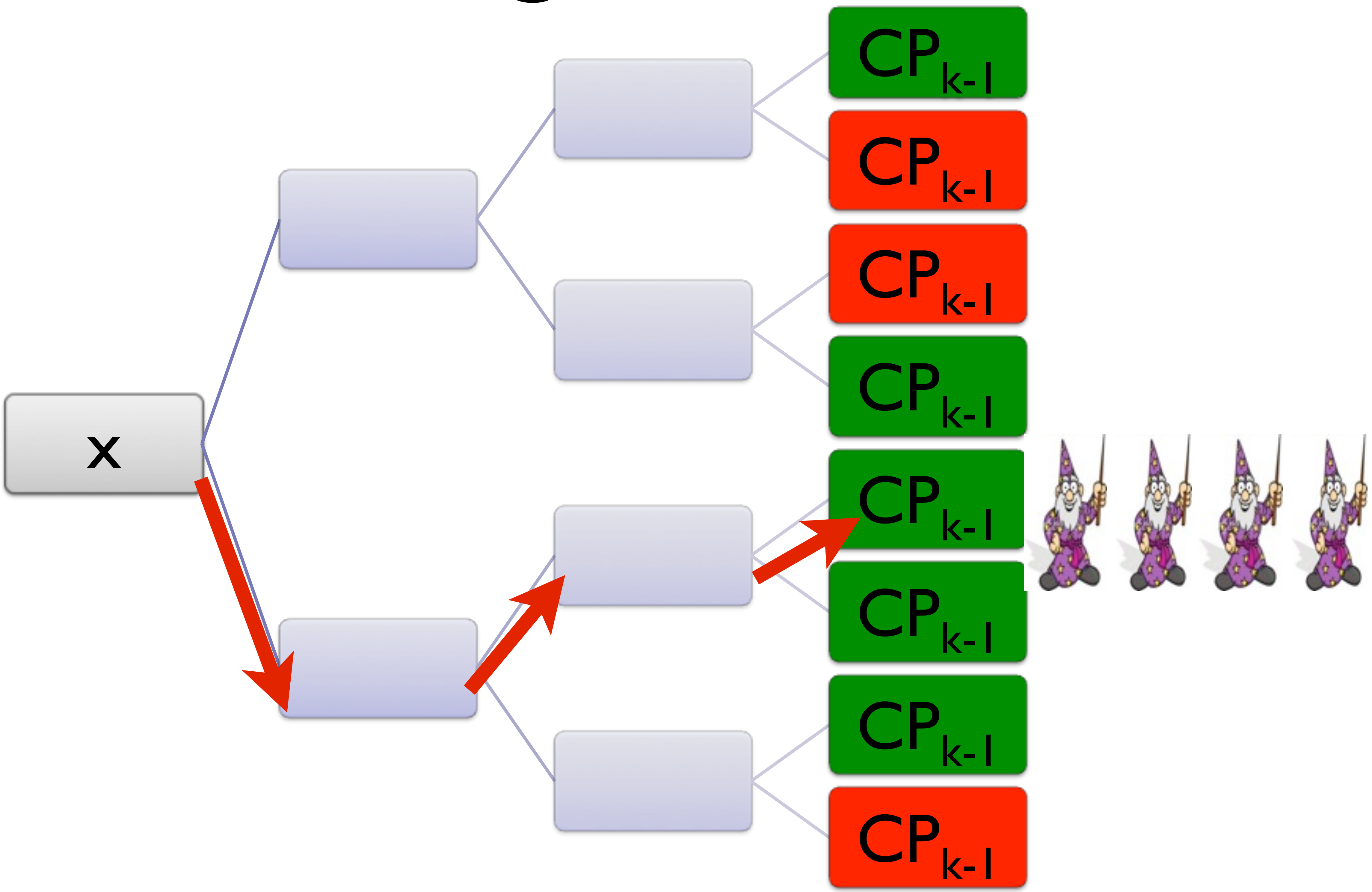
Use k-1 remaining queries to solve CP_{k-1} problem

Generating ω for CP_k



Why can't we ask k queries to 1 Merlin instead?

Generating ω for CP_k



Why can't we ask k queries to 1 Merlin instead?

From k Merlins to k rounds

Recall

$$CP_k \subset k\text{-}DRMA \subset DRMA[k]$$

Need to show

$$k - DRMA \subset DRMA[k]$$

Problem: Merlin may lie today to get better reward tomorrow

From k Merlins to k rounds

Recall

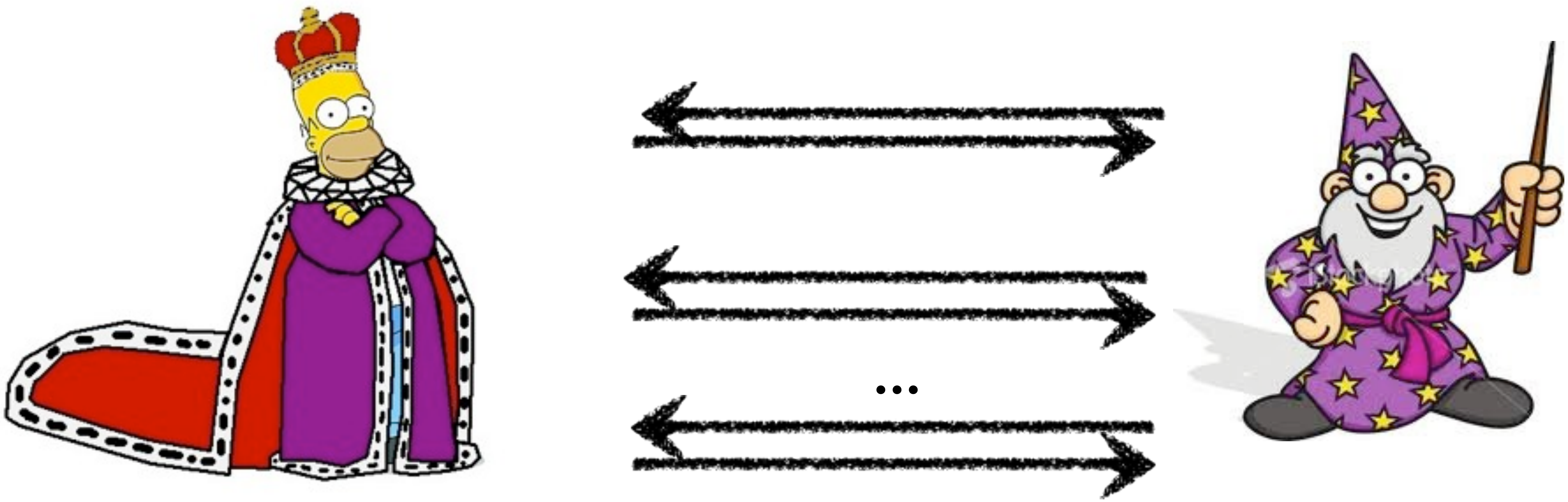
$$CP_k \subset k\text{-}DRMA \subset DRMA[k]$$

Need to show

$$k - DRMA \subset DRMA[k]$$

Solution Sketch: Make tomorrow's reward really small compared to today's

Theorem 3

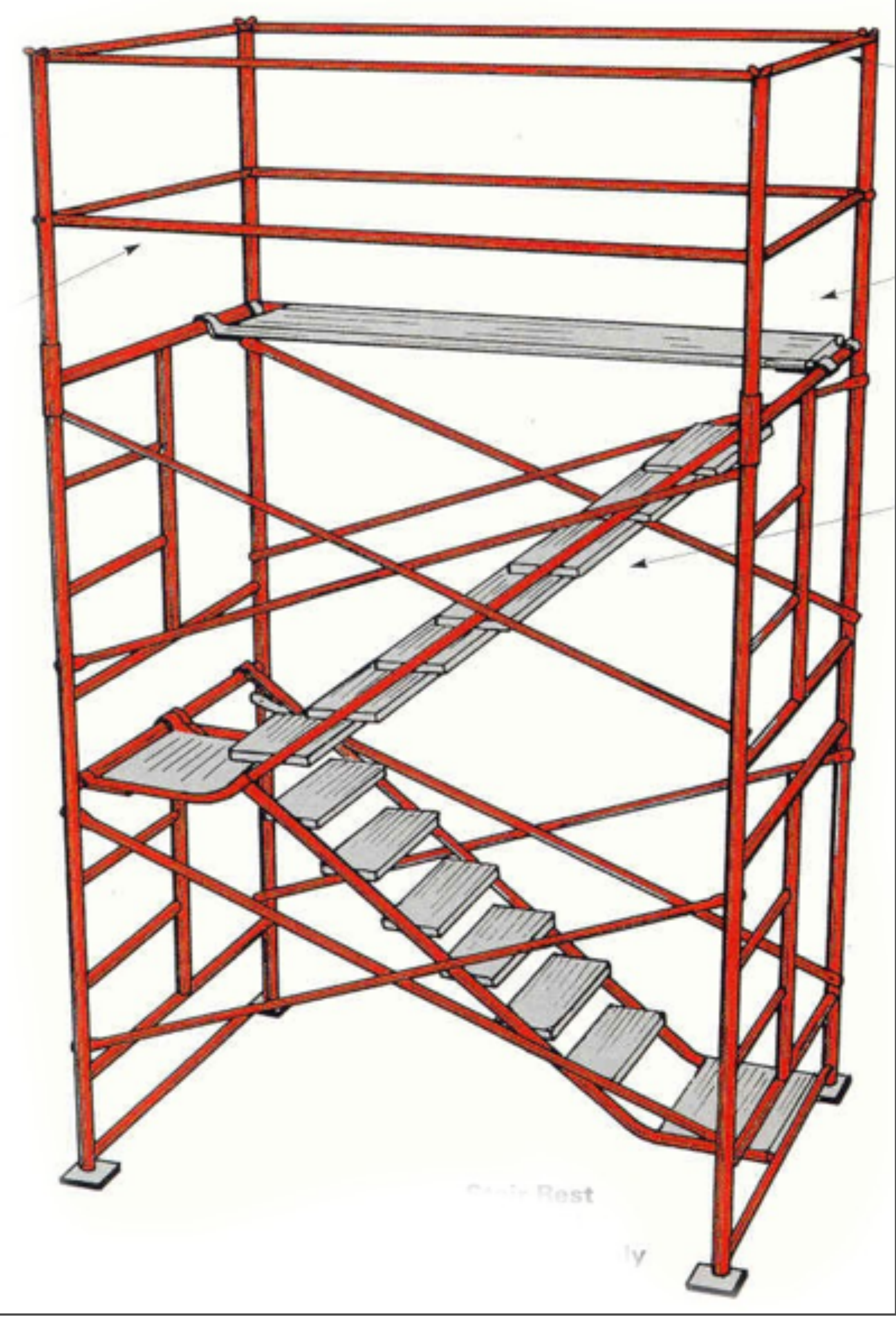


$$CP_k \subset RMA[k] \subset CP_{k+1}$$

$$P^{PP} \subset RMA[1] \subset NP^{PP} \subset PP^{PP} \subset RMA[2] \subset PP^{PP^{PP}} \ldots$$

Open Question

Does CH Collapse?



Summary of Contributions

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

A tight connection

Proper Scoring Rules ⟶ Interactive Proofs

Proper Scoring Rules ⟵ Interactive Proofs

A tight connection

Proper Scoring Rules ⟶ Interactive Proofs

Proper Scoring Rules ⟵ Interactive Proofs

THANK YOU!