Rational Proofs

Pablo Azar  Silvio Micali
Central Question

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

\[ f(x) ? \]

IP

AM

[ GMR 85, BM 85]
Interactive Proofs

\[ f(x)? \]

\[ \text{IP} = \text{PSPACE} \]

[ LFKN 90, Shamir 90]

And they lived happily ever after...
Many Centuries Later...

f(x)?
Centuries Later...

f(x)?
Centuries Later...

f(x)?

$#*#!

Wednesday, August 15, 12
Centuries Later...

$f(x)$?

$#$*#$!
Centuries Later...

f(x)?

$#*#!$
How to pay a Math Expert?
f(x)?
How to pay a Math Expert?

Correct Proof: $1
Incorrect Proof: $0

Fixed Price:

Wednesday, August 15, 12
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?

Can we prove more theorems?
Can we prove them faster?
Can we do better?

f(x)?

Fewer Rounds?
Our Central Question

What's the largest class of problems for which we can guarantee correctness of solution using monetary incentives?
Rational MA
\( f \in \text{Rational MA}[k] \iff \)
\[ f \in \text{Rational MA}[k] \iff \]

\[ \Pi \text{ output function (poly time)} \]

\[ R \text{ reward function (randomized poly time)} \]
$f \in \text{Rational MA}[k]$ iff

- $\Pi$ 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)?
\( f \in \text{Rational MA}[k] \iff \)

- \( \Pi \) 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)?

γ₁

random r₁

γ₂
\[ f \in \text{Rational MA}[k] \text{ iff} \]

\[ \Pi \text{ output function (poly time)} \]

\[ R \text{ reward function (randomized poly time)} \]

\[ f(x) ? \]

\[ \gamma_1 \]

\[ \text{random } r_1 \]

\[ \gamma_2 \]

\[ \text{random } r_2 \]
\( f \in \text{Rational MA}[k] \) iff

\( \Pi \) output function (poly time)

\( R \) reward function (randomized poly time)

\[ f(x) \]

\( y_1 \)

\( \text{random } r_1 \)

\( y_2 \)

\( \text{random } r_2 \)

\( \ldots \)
\( f \in \text{Rational MA}[k] \text{ iff } \)

\[ \Pi \text{ output function (poly time)} \]

\[ R \text{ reward function (randomized poly time)} \]

\[ f(x)? \]

\[ y_1 \]

\[ \text{random } r_1 \]

\[ y_2 \]

\[ \text{random } r_2 \]

\[ \ldots \]

Transcript \( T = (y_1, r_1, \ldots, y_k) \)
\[ f \in \text{Rational MA}[k] \iff \]

\text{\Pi output function (poly time)}

\text{\R reward function (randomized poly time)}

\[ f(x)? \]

\[ y_1 \quad \text{random } r_1 \quad y_2 \quad \text{random } r_2 \quad \ldots \]

\[ \text{Transcript } T = (y_1, r_1, \ldots, y_k) \]

\[ \R(x, T) = \]
\[ f \in \text{Rational MA}[k] \text{ iff} \]

\begin{itemize}
  \item \(\Pi\) output function (poly time)
  \item \(R\) reward function (randomized poly time)
\end{itemize}

\[ f(x) \]
\[ y_1 \]
\[ \text{random } r_1 \]
\[ y_2 \]
\[ \text{random } r_2 \]
\[ \pi(x,T) \]

Output = \(\pi(x,T)\)

Transcript \(T = (y_1, r_1, ..., y_k)\)

\[ R(x,T) = \]
\( f \in \text{Rational MA}[k] \text{ iff} \)

\[ \pi \text{ output function (poly time)} \]
\[ R \text{ reward function (randomized poly time)} \]

\[ f(x) ? \]
\[ y_1 \]
\[ \text{random } r_1 \]
\[ y_2 \]
\[ \text{random } r_2 \]
\[ \ldots \]

\[ \text{Output } = \pi(x, T) \]

\[ \text{Transcript } T = (y_1, r_1, \ldots, y_k) \]

No Verification!
$f \in \text{Rational MA}[k] \iff$

- $\Pi$ output function (poly time)
- $R$ reward function (randomized poly time)

\[ f(x) \]?

\[ \gamma_1 \]

\[ \text{random } r_1 \]

\[ \gamma_2 \]

\[ \text{random } r_2 \]

\[ \ldots \]

$\Pi(x,T) = \pi(x,T)$

$R(x,T) =$

Wednesday, August 15, 12
\[ f \in \text{Rational MA}[k] \text{ iff} \]
\[ \forall \text{ output function (poly time)} \]
\[ \exists \text{ reward function (randomized poly time)} \]
\[ f(x) ? \]
\[ \gamma_1 \]
\[ \text{random } r_1 \]
\[ \gamma_2 \]
\[ \text{random } r_2 \]
\[ \text{...} \]
\[ \text{Output } = \pi(x,T) \]
\[ \text{Merlin chooses Transcript } T^* \text{ that maximizes } E[R(x,T)] \]
\[ f \in \text{Rational MA}[k] \text{ iff } \]

\[ f(x)? \]

\[ \gamma_1 \quad \text{random } r_1 \quad \gamma_2 \]

\[ \quad \text{random } r_2 \quad \ldots \]

\[ R(x,T) = \]

Output = \( \pi(x,T) \)

Merlin chooses Transcript \( T^* \) that maximizes \( E[R(x,T)] \)
\[ f \in \text{Rational MA}[k] \text{ iff } f(x) \]

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

\[ \pi(x, T^*) = f(x) \]

\[ R(x, T^*) = \]
Our Central Question

Where does $\text{RMA}[k]$ fit?
Theorem I

\[ \#P \subset RMA[?] \]
Theorem 1

\[ \#P \subseteq RMA[1] \]
Proof Sketch

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

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

$x \in \{0, 1\}^n$
#P Problems

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

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

$\#\{y : M(x, y) = 1\}$?
$\#P$ Problems

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

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

$\#\{y : M(x,y) = 1\} \approx 2^{301} + 13$
#P Problems

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

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

$\#\{y : M(x, y) = 1\} \ ? \ 2^{301} + 13$
\#P Problems

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

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

$2^{301} + 13$
#P Problems

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

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

\( 2^{301} + 13 \)

\( M(x, y_1), M(x, y_2), \ldots \)
#P Problems

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

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

$\#\{y : M(x,y) = 1\} \leq 2^{301} + 13$

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

No 1-round proof so far
Economics To The Rescue!
Asymmetric Information

Arthur

Merlin
Asymmetric Information

Arthur

Information

Merlin
Asymmetric Information

What is information?
Asymmetric Information

What is information?

How do we guarantee it is correct?
Computation View

Verifier

Prover

x, f
Computation View

Information is **output** of a **hard to compute function**

Verifier

\[ x, f \]

Prover

Wednesday, August 15, 12
Computation View

Verifier

Information is output of a hard to compute function

Prover

Correctness guaranteed by proof
Economics View

Decision Maker

Agent
Economics View

Decision Maker
Information: distribution $\mathcal{D}$ over $\Omega = \text{states of the world}$
Economics View

Decision Maker
Information: distribution $\mathcal{D}$ over $\Omega = \text{states of the world}$

Agent
Correctness from incentives
Proper Scoring Rules

[Good 52, Brier 50]
Proper Scoring Rules

[Good 52, Brier 50]

\[ \Omega = \{ \text{Boston}, \text{NY} \} \]

\[ \mathcal{D} \in \Delta(\Omega) \]
Proper Scoring Rules

[Good 52, Brier 50]

\[ \Omega = \{ \text{Boston, NewYork} \} \]

\[ D \in \Delta(\Omega) \]

\[ D(\text{Boston}) = 60\% \]

\[ D(\text{New York}) = 40\% \]
Proper Scoring Rules

[Good 52, Brier 50]

\[ \Omega = \{\text{Boston}, \text{NewYork}\} \]
\[ D \in \Delta(\Omega) \]

\[ D(\text{Boston}) = 60\% \]
\[ D(\text{NewYork}) = 40\% \]
Proper Scoring Rules

[Good 52, Brier 50]

$$\Omega = \{ \text{Boston}, \text{New York} \}$$

$$D \in \Delta(\Omega)$$

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

$$D(\text{New York}) = 40\%$$
Proper Scoring Rules

[Good 52, Brier 50]

\[ \Omega = \{ \text{Boston}, \text{NewYork} \} \]

\[ D \in \Delta(\Omega) \]

\[ \omega \leftarrow D \]

\[ D(\text{Boston}) = 60\% \]
\[ D(\text{NewYork}) = 40\% \]
Proper Scoring Rules

\[ \Omega = \{ \text{Boston, NewYork} \} \]
\[ D \in \Delta(\Omega) \]
\[ \omega \leftarrow D \]

\[ D(\text{Boston}) = 60\% \]
\[ D(\text{NewYork}) = 40\% \]
Proper Scoring Rules

\[ \Omega = \{ \text{Boston}, \text{New York} \}, \mathcal{D} \in \Delta(\Omega) \]

\[ \omega \leftarrow \mathcal{D} \]

\[ \mathcal{P} = S(\mathcal{P}, \text{Boston}) \]

\[ \mathcal{D}(\text{Boston}) = 60\% \]

\[ \mathcal{D}(\text{New York}) = 40\% \]
Proper Scoring Rules

\[ \Omega = \{ \text{, } \text{NY} \} , \mathcal{D} \in \Delta(\Omega) \]

\[ \omega \leftarrow \mathcal{D} \]

\[ \mathcal{P} \]

\[ = S(\mathcal{P}, \text{NY}) \]

\[ \mathcal{D}(\text{Boston}) = 60\% \]

\[ \mathcal{D}(\text{NewYork}) = 40\% \]
Proper Scoring Rules

\[ \Omega = \{ \text{B}, \text{NY} \} , \mathcal{D} \in \Delta(\Omega) \]

\[ \omega \leftarrow \mathcal{D} \]

\[ \mathcal{P} = S(\mathcal{P}, \text{NY}) \]

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

\[ \mathcal{D}(\text{Boston}) = 60\% \]

\[ \mathcal{D}(\text{NewYork}) = 40\% \]
Proper Scoring Rules

\[ \Omega = \{ \text{Boston}, \text{New York} \}, \mathcal{D} \in \Delta(\Omega) \]

\[ \omega \leftarrow \mathcal{D} \]

\[ \mathcal{P} \]

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

\[ \mathcal{D}(\text{Boston}) = 60\% \]

\[ \mathcal{D}(\text{New York}) = 40\% \]
#P Problems

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

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

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

$\Pr_y[M(x,y) = 1] ? \frac{2^{301} + 13}{2^{n^c}}$

Reduce the problem to question about probabilities
#P Problems

Input: \( M : \{0, 1\}^n \times \{0, 1\}^{n^c} \to \{0, 1\} \)
\[ x \in \{0, 1\}^n \]

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

Merlin knows \( q = \Pr_y[M(x,y) = 1] \)
Need to incentivize him to reveal \( q \)

\[ \frac{2^{301} + 13}{2^{n^c}} \]
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 \( \#P \)

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

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

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

\[
\mathcal{D}(1) = q \quad \mathcal{D}(0) = 1 - q
\]
Our Rational Proof for $\#P$

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

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

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

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

$$\mathcal{D}(0) = 1 - q$$
Our Rational Proof for \#P

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

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

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

\[ \mathcal{D}(1) = q \]

\[ \mathcal{D}(0) = 1 - q \]
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 $\#P$

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

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

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

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

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

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

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

\[ CH = CP_0 \cup CP_1 \cup CP_2 \cup \ldots \]

\[ CP_0 = P \]

\[ CP_1 = PP \]

\[ CP_2 = PP^{CP_1} = PP^{PP} \]

\[ CP_k = PP^{CP_{k-1}} = PP^{PP \ldots PP} \]
Theorem 3
Theorem 3

\[ CP_k \subset RMA[k] \subset CP_{2k+1} \]
Theorem 3

\[ \text{RMA} = \text{CH} \]
Open Question

Does CH Collapse?
Old Analogy

Q: Does CH Collapse?
A: Not if it behaves like PH
New Analogy

Q: Does CH Collapse?
A: Yes if it behaves like AM

\[
\begin{align*}
AM[k] \\
... \\
AM[2] \\
AM[1]
\end{align*}
\]

\[
\begin{align*}
PPPP...PP \\
... \\
PPPP \\
PP
\end{align*}
\]
Summary of Contributions

• New Complexity Class RMA
• Short Rational Proofs for #P
• Constant-Round Rational Proofs = CH
THANK YOU!