Rational Proofs with Multiple Provers

Jing Chen, Samuel McCauley, Shikha Singh
Department of Computer Science
Outline of the Talk

RATIONAL

INTERACTIVE PROOFS

with

MULTI-PROVERs
Interactive Proofs
[GMR, BM 85]

• All-powerful Merlin (Prover) interacts with a polynomial-time, probabilistic Arthur (Verifier)

• $\text{IP} = \text{PSPACE}$ [Shamir 92]

Proof that $x \in L$

Is it true?
Multi-Prover Interactive Proofs [BGKW 88]

- Provers work together to convince the verifier
- Once protocol begins, provers cannot communicate
- MIP = NEXP [BFL 90]

Is it true?

Proof that $x \in L$
Classical Interactive Proofs

- Merlin can be arbitrary: dishonest or malicious
Rational Interactive Proofs
[AM 12]

- Arthur promises Merlin a reward for proving the theorem correctly
- Merlin is rational: he wants to maximize this reward

What proof maximizes reward?
Rational Interactive Proofs
[AM 12]

• Arthur computes the reward based on the transcript and his randomness

• Correctness is ensured by Merlin’s rationality!

Proof that $x \in L$

How to pay to incentivize truthfulness?
Rational Interactive Proofs
[AM 12]

• Lead to simple and efficient protocols
• Constant rounds: RIP is more powerful
• Polynomial rounds: RIP = IP
Delegation of Computation

- Computation is becoming a commodity
- Should be able to verify correctness
- Pay money in exchange for services
Delegation of Computation

- Super-efficient rational proofs [AM 13, GHRV 14, ZB 14, GHRV 16], IP for Muggles [GKR 08]
Delegation of Computation

- *Super-efficient* rational proofs [AM 13, GHRV 14, ZB 14, GHRV 16], IP for Muggles [GKR 08]
- All existing work involves a *single rational prover*
Arthur has two Merlins
what if?

Arthur has two Merlins
He can crosscheck their answers!
Arthur has two Merlins
He can crosscheck their answers!

In classical interactive proofs, two provers increase the power of the system

Multi-prover $\text{IP} = \text{NEXP}$ BFL 91

$\text{IP} = \text{PSPACE}$ Shamir 90
Arthur has **two** Merlins
He can crosscheck their answers!

“Are *multiple Merlins* more powerful than one in rational proofs?”- AM 12
We introduce: MRIP

*Multi-Prover Rational Interactive Proofs*
Multi-Prover Rational Interactive Proofs

- A way to outsource computation to multiple service providers
- A natural extension of RIP and MIP
MRIP: The Model

- Provers can pre-agree on a joint strategy
- They cannot communicate once the protocol begins
- At the end, the verifier computes a total reward
- [Correctness] Any strategy of the provers that maximizes the total reward leads the verifier to the right answer
Warm Up: MRIP for \textbf{NEXP}

\[ x \in L \text{ or } x \not\in L \]
Warm Up: MRIP for NEXP

\[ x \in L \text{ or } x \notin L \]

If claim \( x \in L \)
Warm Up: MRIP for **NEXP**

If claim $x \in L$  

→ Y  

Accept

$x \in L$ or $x \not\in L$
Warm Up: MRIP for $\text{NEXP}$

If claim $x \in L$ then $Y$ and Accept

$x \in L$ or $x \not\in L$

MIP for NEXP
Warm Up: MRIP for NEXP

If claim $x \in L$, Accept

$x \in L$ or $x \notin L$

MIP for NEXP

Acc

Rej

End

$\$
Warm Up: MRIP for NEXP

If claim $x \in L$

$\begin{array}{c}
\text{Y} \\
\text{Accept} \\
\text{End} \\
\text{End}
\end{array}$

$\begin{array}{c}
\text{N} \\
\text{Reject} \\
\text{End} \\
\text{End}
\end{array}$

$x \in L$ or $x \not\in L$
Warm Up: MRIP for **NEXP**

![Diagram showing the process of MRIP for NEXP]

- **Truth:** $x \in L$
- $x \notin L$

**If claim** $x \in L$

- **Y** → Accept
- **N** → Reject

**Reject**

- **$\$$** → End

**MIP for NEXP**

- **Acc**
- **Rej**

- **$\$$** → End
Warm Up: MRIP for NEXP

Truth: $x \in L$

If claim $x \in L$

Accept

MIP for NEXP

Prob = 1

End

$x \in L$

End

$\$$

Reject

$\$$
Warm Up: MRIP for NEXP

Truth: $x \not\in L$

If claim $x \in L$

Accept

Prob $\leq \frac{1}{3}$

MIP for NEXP

Acc

End

Rej

End

Reject

$\$$

End

$x \in L$
Warm Up: MRIP for **NEXP**

If claim $x \in L$

- **Y**: Accept
- **N**: Reject

Truth: $x \not\in L$

MIP for NEXP

- **Acc**: $$$ \rightarrow \text{End}
- **Rej**: $\$$ \rightarrow \text{End}
More Efficient MRIP for NEXP

• MIP protocols are often complicated, or computation and communication intensive

• We construct a simple, linear time MRIP protocol for NEXP
More Efficient MRIP for NEXP

- Construct MRIP for an NEXP-complete language

*Use Brier’s Scoring Rule:*  
\[ \text{BSR}(D, \omega) = 2D(\omega) - \sum_{\omega \in \Sigma} D(\omega)^2 - 1 \]
Oracle 3SAT [BFL 91]: Given a Boolean 3-CNF $B$, does there exist a function $A$ such that for all $w$, $B(w, A(b_1), A(b_2), A(b_3))$ is satisfied, where $b_1b_2b_3$ is a suffix of $w$?
MRIP for NEXP-Complete Language

Oracle 3SAT [BFL 91]: Given a Boolean 3-CNF \( B \), does there exist a function \( A \) such that for all \( w \) \( B(w, A(b_1), A(b_2), A(b_3)) \) is satisfied, where \( b_1b_2b_3 \) is a suffix of \( w \)?

- A has \( 2^{|w|} \) solutions = \( B \) satisfied with probability 1
- Verifier cannot obtain true sample for the scoring rule
  - Use second prover to help sample
- What if prover is honest about a bad choice of \( A \)?
  - BSR maximized when all or none satisfied
Is MRIP strictly more powerful?

• Recall:
  • MRIP contains MIP
  • However, with a single prover: RIP = IP [AM 12]
MRIP is Closed under Complement

- A rational Merlin correctly reports $x \in L$ or $x \not\in L$
- MRIP contains NEXP, so MRIP also contains coNEXP
MRIP vs RIP and MIP

- Assuming $NEXP \neq coNEXP$:
- MRIP is more powerful than both RIP and MIP
Exactly How Powerful is MRIP?

Theorem: \( MRIP = EXP^{NP} \)

Exponential-time Turing Machine with non-adaptive access to an NP oracle
MRIP = \text{EXP}^{||\text{NP}} (\text{proof sketch})

Lemma: \text{EXP}^{||\text{NP}} = \text{EXP}^{||\text{poly-NEXP}}

To show: \text{MRIP} = \text{EXP}^{||\text{poly-NEXP}}
MRIP = EXP||^{NP} (proof sketch)

- Divide computation into 3 parts
- EXP protocol uses DC circuit characterization
- Challenge: compose rewards together as a final reward which incentivizes truth in each protocol
When paying for (verifiable) computation, we can solve more difficult problems by employing multiple provers and cross-checking their answers!
Ask us questions separately and cross-check the results to get better answers
Fewer provers and rounds

• For MIP 2 provers, 1 round suffice [FL92]

I only know so many Merlins...
Fewer provers and rounds

- For MIP 2 provers, 1 round suffice [FL92]

Theorem: *Two provers and five* rounds achieve the full power of MRIP.

I only know so many Merlins...
This slide is intentionally left blank.
So far, truthfulness guarantees *maximum* reward.

But how much do the provers lose by lying?

We call this loss the *utility gap*.

I don’t get out of bed for less than $10,000 a day…
MRIP with Utility Gap

- Polynomial gap: $P^{\text{||NEXP}}$
- Constant gap: Contains both NEXP and coNEXP

Compare to $\text{EXP}^{\text{||NP}}$ for MRIP with arbitrary gap
Conclusion and Future Directions

- How to exploit the rationality of two provers
- What does this mean in terms of delegation of computation?
- Scale down our protocols
- Interesting connections to existing models
- Streaming Interactive Proofs [CTY 11, etc.]
Questions?

Err..

Thank You!
2 Provers and 5 Rounds are Sufficient

My random coin flips are:

H   T   H   T   T

Transcript:

01, 100, 1, 110, ?

11100

Since your answers match (don’t match), your reward is:

$   $   $   $   $