# Rational Proofs with Multiple Provers

Jing Chen, Samuel McCauley, Shikha Singh

## Abstract

Interactive proofs model a world where a verifier delegates computation to an untrustworthy prover, verifying the prover's claims before accepting them. Rational proofs are simple and efficient alternative to interactive proofs, in which, the prover is *rational* rather than untrustworthy—he may lie, but only to increase his payment. Azar and Micali [STOC 2012] posed the following open problem: ***Are multiple provers more powerful than one for rational proofs?*** We provide a model that extends rational proofs to allow multiple provers and fully characterize the power of this model.

## Introduction

Multi-prover interactive proofs (MIP) and rational interactive proofs (RIP) are two important extensions of interactive proof systems.

Multiple provers are more powerful than one for classical interactive proofs, that is, MIP = NEXP, while, IP = PSPACE.

Rational proofs are no more powerful than interactive proofs (i.e., RIP = PSPACE).

Previous work on rational proofs considers a *single* rational prover.

We extend the model of rational proofs to allow for multiple provers.

## Multi-Prover Rational Proofs

Combines elements of rational proofs and classical multi-prover interactive proofs.

Models computation outsourcing applications, such as Amazon's Mechanical Turk, where payments are used to incentivize a team of rational workers.

Correctness is often ensured by crosschecking answers, which is an essential part of MRIP.

Prover's are collaborative—their answers need to match, even though they cannot communicate with each other.

## The Model

Several computationally-unbounded provers communicate with a polynomial-time randomized verifier who wants to determine the membership of an input string in a language.

The provers can pre-agree on a strategy but cannot communicate with each other once the protocol begins.

At the end of the protocol, the verifier computes a total payment for the provers based on the input, his own randomness, and the messages exchanged.

This total payment may be distributed in any predetermined way by the verifier or the provers themselves.

*In a multi-prover rational interactive protocol (MRIP) any strategy of the provers that maximizes their expected payment leads the verifier to the correct answer.*

## Distribution of Payments

Rational provers in MRIP work as a team to maximize the total payment received.

Any pre-specified distribution of this sum is allowed (should not depend on the transcript).

In the model of MRIP with *non-cooperative provers* each prover receives an individual payment based on the final transcript.

The answers of the provers are cross-checked for verification—implicit collaboration is required, but only to optimize an individual's payment.

We require a *maximum subgame-perfect equilibrium* among the provers, under which the verifier receives the correct solution.

We conjecture that the power of the two classes—rational proofs with cooperative and non-cooperative provers—is equivalent.

## The Power of Multi-Prover Rational Proofs: MRIP = $\mathsf{EXP}^{\|\mathsf{NP}}$

We exactly characterize the class MRIP by showing that a language has a multi-prover rational interactive proof if and only if it is decidable by a deterministic exponential-time oracle Turing machine with non-adaptive access to an NP oracle. Thus, multiple provers are more powerful than one for rational proofs.

## MRIP Protocols for NEXP

The naive protocol for NEXP uses the corresponding MIP protocol as a subroutine.

We construct a simpler, more efficient protocol for NEXP using *proper scoring rules.*

Scoring rules are an essential tool used in the construction of rational proofs.

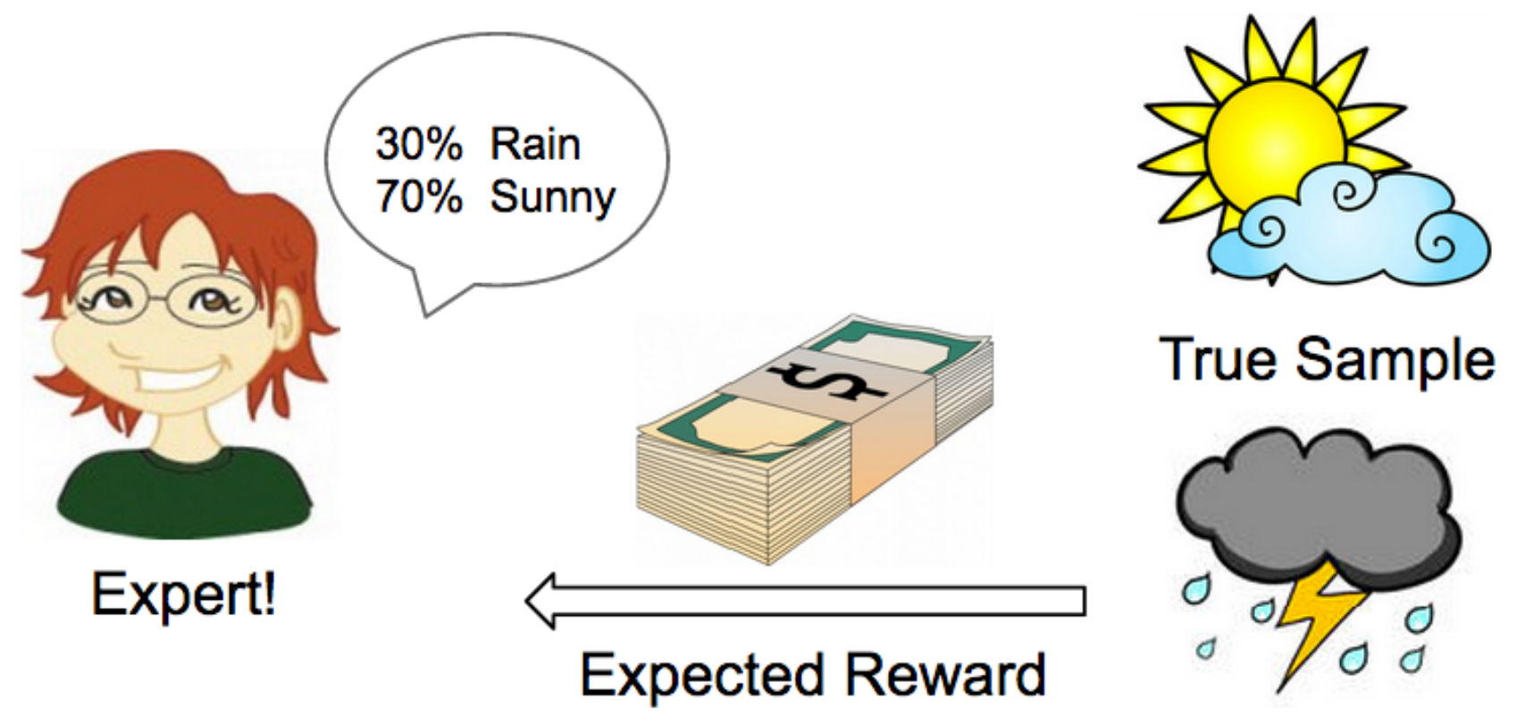

Figure 1: Proper scoring rules ensure an expert maximizes his total expected reward by reporting the correct distribution.

## MRIP = MRIP(2,5)

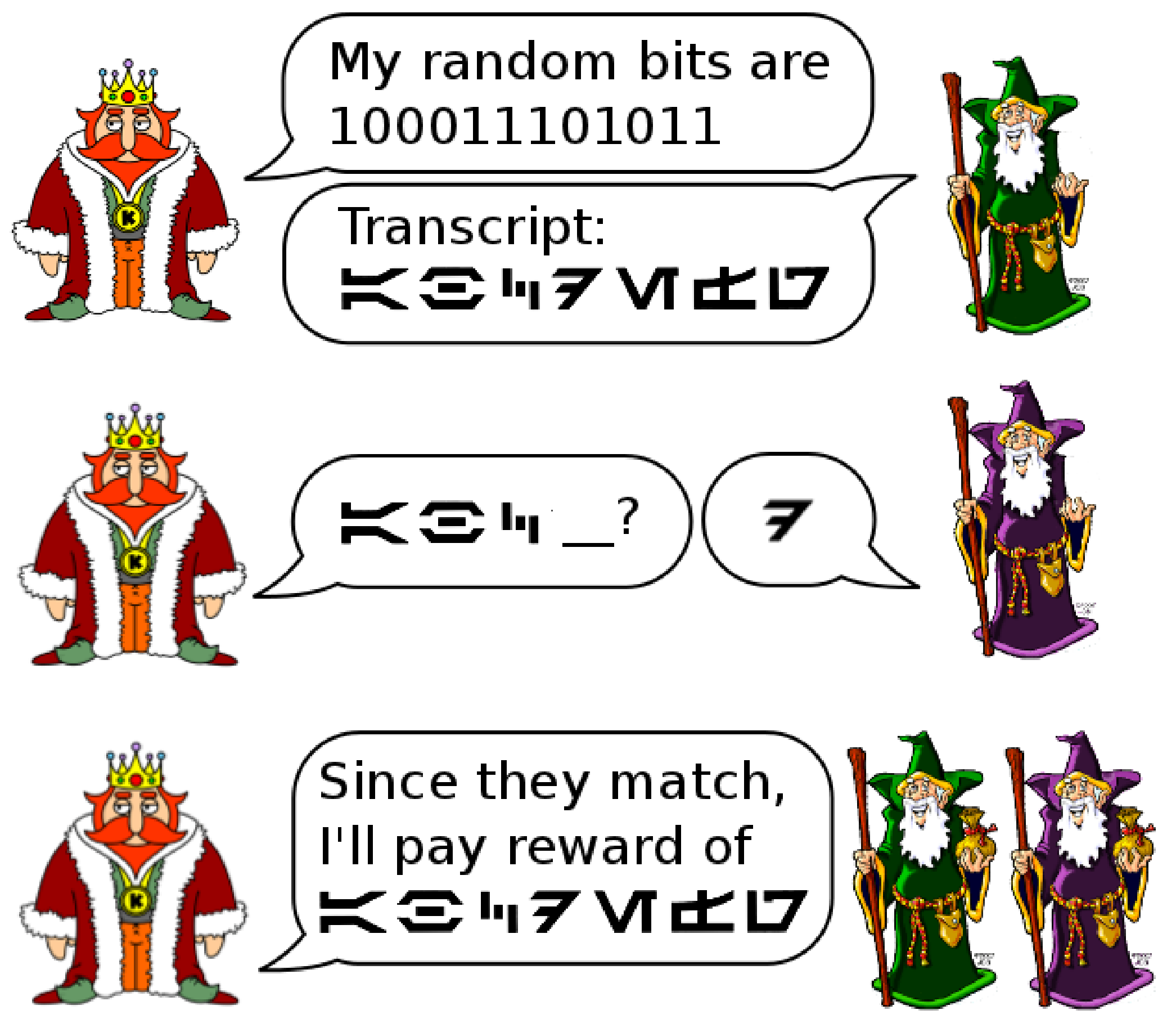
My random bits are 100011101011
Transcript:
?
Since they match, I'll pay reward of

Figure 2: Any MRIP protocol can be simulated by 2 provers in 5 rounds of communication. The verifier cross-checks a random message of the transcript by quering the second prover.

## Utility Gap

Rational proofs assume that the provers always act to maximize their payment. However, how much do they lose by lying?

We show that requiring a noticeable (polynomial) utility gap results in protocols for a different, possibly smaller, complexity class: $\mathsf{P}^{\|\mathsf{NEXP}}$.

## The Power of Rational Proofs

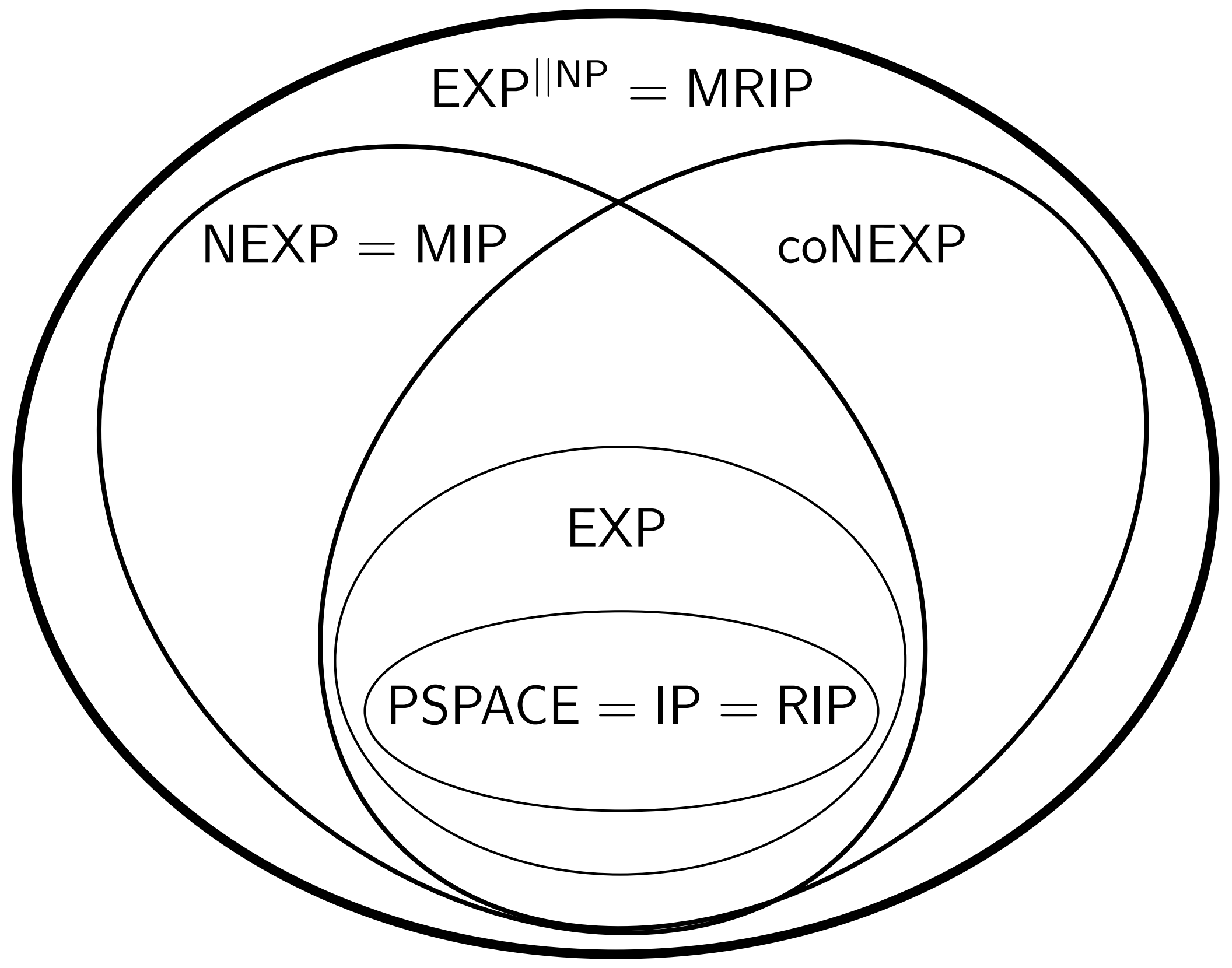

Figure 3: The relative power of some interactive proof systems. The separation between complexity classes is conjectured.

## MRIP vs Similar Models

Refereed games capture the strategic nature of provers, but do not allow collaboration.

MIP protocols are robust against arbitrary provers but are complicated and inefficient.

MRIP achieves its full power with only five rounds of interaction, while RIP is less powerful when restricted to constant rounds.

## Additional Information

Contact: jingchen@cs.stonybrook.edu
smccauley@cs.stonybrook.edu
shiksingh@cs.stonybrook.edu