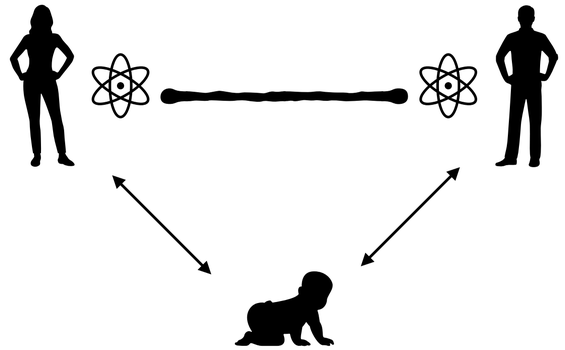
# On the complexity of zero gap MIP*

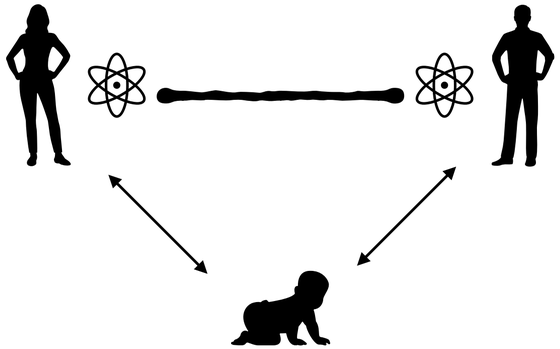


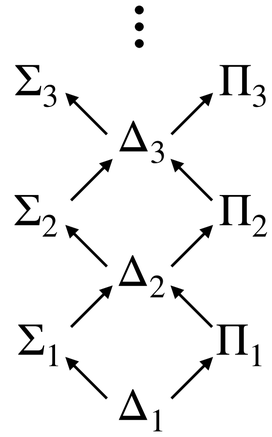

## Seyed Sajjad Nezhadi

with Hamoon Mousavi and Henry Yuen

U of Toronto → Intern @ Agnostiq → U of Maryland (PHD Fall 2020- )

$$MIP_0^* = \Pi_2$$






Entangled Provers

Arithmetical Hierarchy

$$MIP_0^* = \Pi_2$$

Multi-prover Interactive Proofs

Zero Gap

Second Level

**Exactly computing the value of an entangled non-local game is harder than solving the Halting problem**

**Previously it was known to be undecidable [Slofstra '17]**

$$\Pi_2 \subseteq MIP_0^*[\tilde{3}]$$

Number of provers

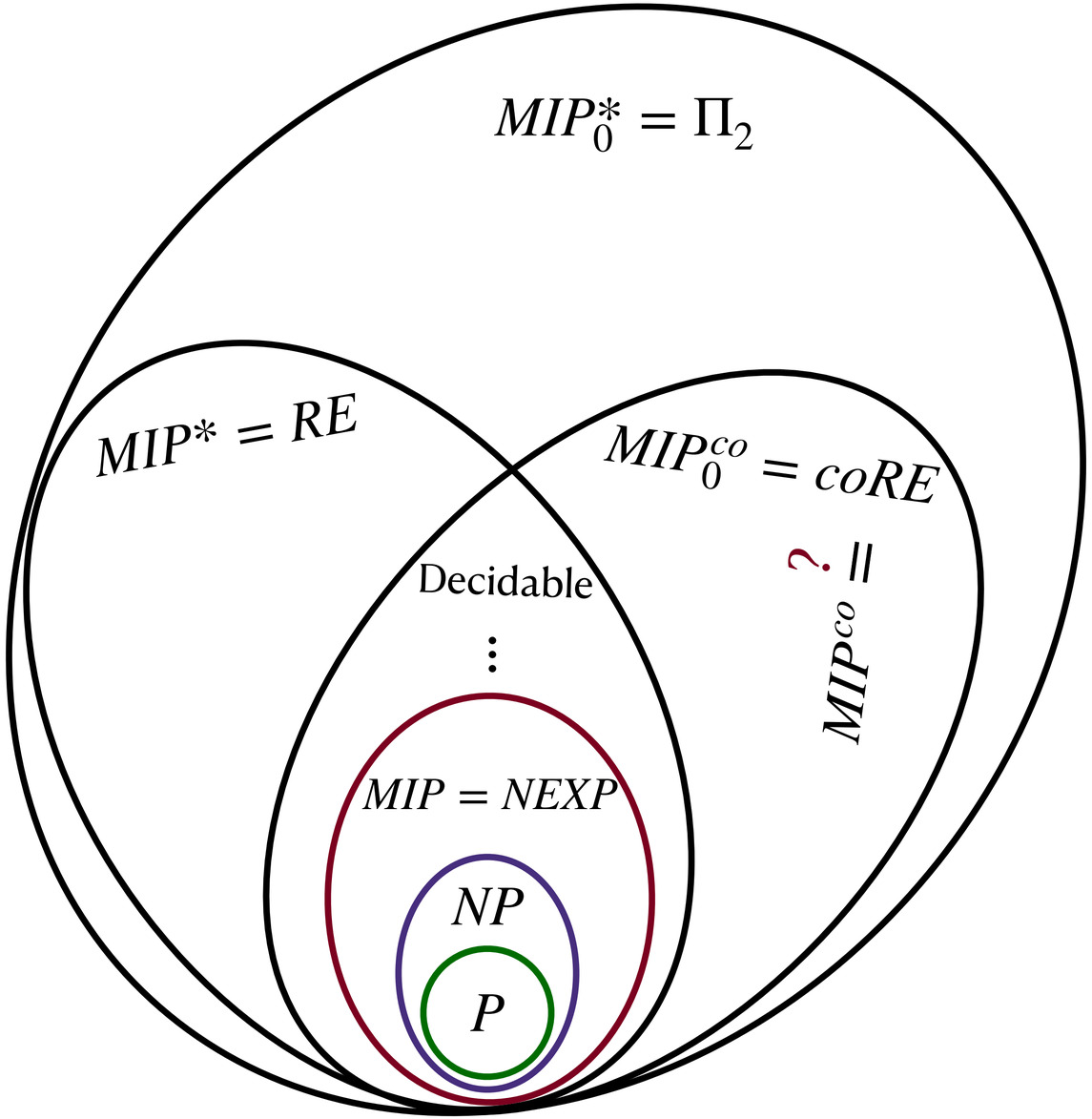


**Tsirelson's problem has a negative answer for 3 players**

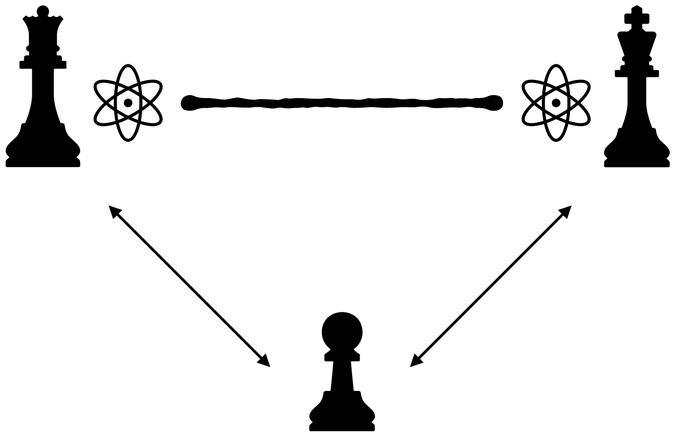
**i.e. commuting correlations ≠ tensor product correlations**

**Showing $\Pi_2 \subseteq MIP_0^*[2]$ refutes Connes' Embedding Problem**

# Complexity Landscape of Entangled Multi-prover Interactive Proofs



# Non-local Games



A non-local game $\mathcal{G}$ is played between a verifier and multiple entangled cooperating provers who cannot communicate with each other once the game starts.

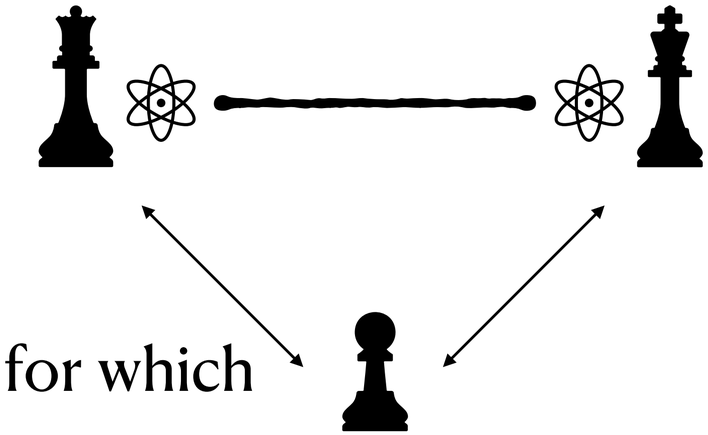
The verifier samples questions for the provers and the provers attempt to respond according to a quantum entangled strategy $\mathcal{S}$ that maximize their winning probability.

The probability of wining a game $\mathcal{G}$ with strategy $\mathcal{S}$ is denoted $\omega^*(\mathcal{G}, \mathcal{S})$

The maximum winning probability of a game $\mathcal{G}$ is denoted $\omega^*(\mathcal{G}) := \sup_{\mathcal{S}} \omega^*(\mathcal{G}, \mathcal{S})$

$\omega^*(\mathcal{G}) = 1$ does not mean that $\exists \mathcal{S} \,.\, \omega^*(\mathcal{G}, \mathcal{S}) = 1$

# $MIP^*$



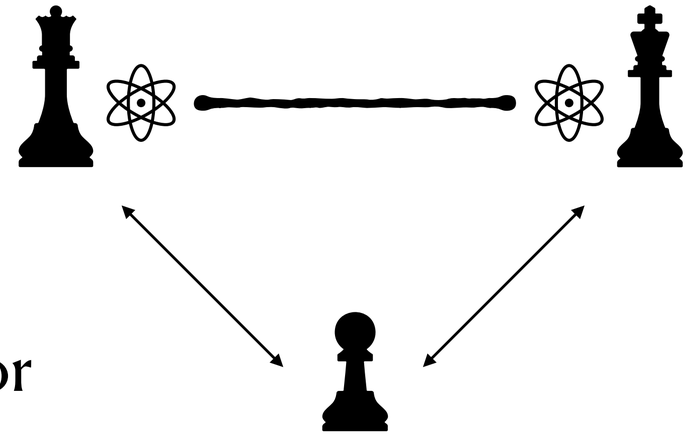
$MIP^*[k]$ consists of languages $L \subseteq \{0,1\}^*$ for which there exists a $k$-prover uniform family of games $\{\mathcal{G}_x\}$

$$\text{If } x \in L \text{ then } \omega^*(\mathcal{G}_x) = 1$$

$$\text{If } x \notin L \text{ then } \omega^*(\mathcal{G}_x) \underbrace{<}_{\text{Constant Gap}} \frac{1}{2}$$

$$MIP^* = \bigcup_{k \geq 2} MIP^*[k]$$

# $MIP_0^*$



$MIP_0^*$ consists of languages $L \subseteq \{0,1\}^*$ for which there exists a uniform family of games $\{\mathcal{G}_x\}$

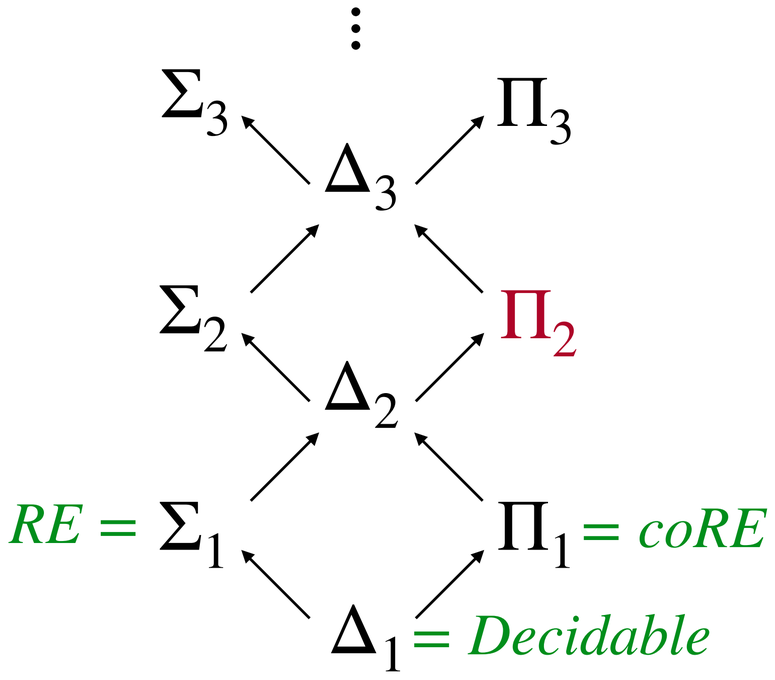
If $x \in L$ then $\omega^*(\mathcal{G}_x) = 1$

If $x \notin L$ then $\omega^*(\mathcal{G}_x) \underbrace{<}_{\text{Zero Gap}} 1$

Similarly $MIP_0^* = \bigcup_{k \geq 2} MIP_0^*[k]$

The problem of deciding if a non-local game $\mathcal{G}$ has perfect winning probability is complete for $MIP_0^*$

# Arithmetical Hierarchy




All classes in the Arithmetical Hierarchy are provably distinct

In particular $\Pi_2$ strictly contains both *RE* and *coRE*

# Recursively Enumerable

$RE$ consists of languages $L \subseteq \{0,1\}^*$ for which there exists a Turing Machine $\mathscr{M}$

If $x \in L$ then $\mathscr{M}(x)$ accepts

If $x \notin L$ then $\mathscr{M}(x)$ runs forever

The Halting problem is complete for RE

$RE$ consists of languages $L \subseteq \{0,1\}^*$ that can be defined as

$$L = \{x \in \{0,1\}^* \mid \exists n \,.\, \overbrace{P(x,n)}^{\text{Decidable}}\}$$

# $\Pi_2$

$\Pi_2$ consists of languages $L \subseteq \{0,1\}^*$ for which there exists a Turing Machine $\mathscr{M}$

If $x \notin L$ then $\mathscr{M}(x)$ accepts given an oracle for the Halting problem

If $x \in L$ then $\mathscr{M}(x)$ runs forever

$\Pi_2$ consists of languages $L \subseteq \{0,1\}^*$ that can be defined as

$$L = \{x \in \{0,1\}^* \mid \underbrace{\forall n \,.\, \exists m \,.}_{\text{Number of quantifiers corresponds to level of Arithmetical Hierarchy}} \overbrace{P(x, n, m)}^{\text{Decidable}}\}$$

$$MIP_0^* \subseteq \Pi_2$$

$$\omega^*(\mathcal{G}) = 1$$

Decidable

$$\forall \epsilon \; \exists \mathcal{S} \; \omega^*(\mathcal{G}, \mathcal{S}) > 1 - \epsilon$$

The non-local game $\mathcal{G}$ can be played perfectly

For any constant gap $\epsilon$ there exists an $MIP^*$ strategy $\mathcal{S}$ for the game $\mathcal{G}$ that succeeds with probability greater than $1 - \epsilon$

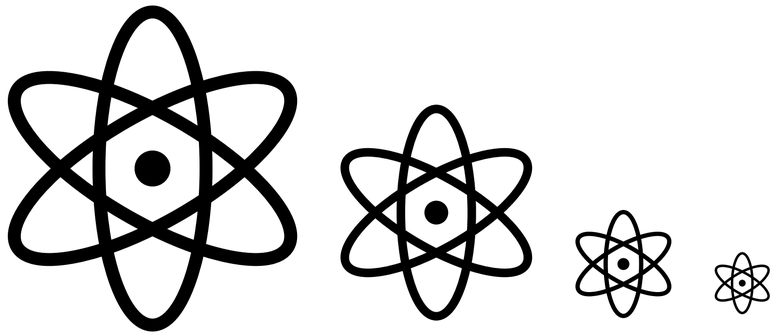
$$\Pi_2 \subseteq MIP_0^*[3]$$

$$coRE \subseteq MIP_0^*[3]$$

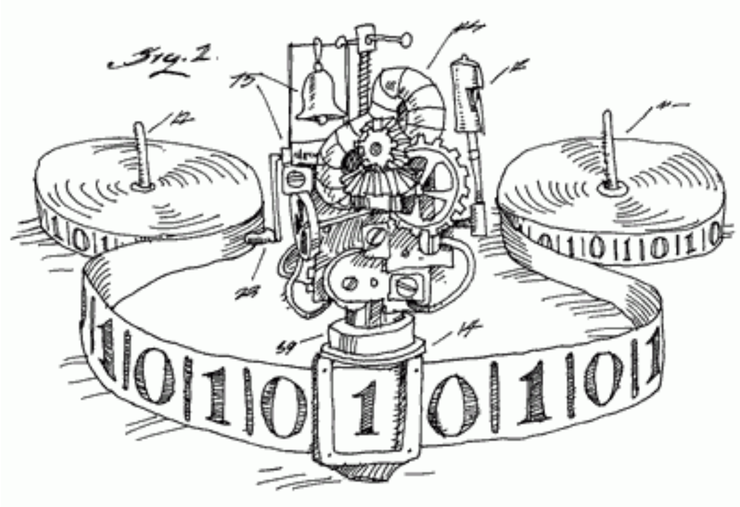
Fitzsimons et al. ‘19

$$MIP^*[2] = RE$$

Ji et al. ‘20



Protocol Compression




Halting Protocol

# Compression

Given a family of non-local games $\{\mathcal{G}_n\}$ there exists an efficiently computable family of games $\{\mathcal{G}_n^{\#}\}$ such that:

$$\omega^*(\mathcal{G}_n^{\#}) \geq \frac{1}{2} + \frac{1}{2}\omega^*(\mathcal{G}_n)$$

$$\omega^*(\mathcal{G}_n) < 1 \implies \omega^*(\mathcal{G}_n^{\#}) < 1$$

The runtime of verifiers for $\{\mathcal{G}_n^{\#}\}$ is *polylogarithmic* in the runtime of verifiers for $\{\mathcal{G}_n\}$

# Compression

$coRE \subseteq MIP_0^*$

Using compression we can circumvent having to enumerate over all $n \in \mathbb{N}$

Family of games $\mathcal{G}_n$

$\sim$

Reject if $\neg P(n)$

Otherwise play the compressed game $\mathcal{G}^{\#}_{n+1}$

NOT RECURSIVE!

Decidable

$\sim$

$\forall n \in \mathbb{N} \,.\, P(n)$ is True $\Leftrightarrow$ The game $\mathcal{G}_1$ can be played perfectly

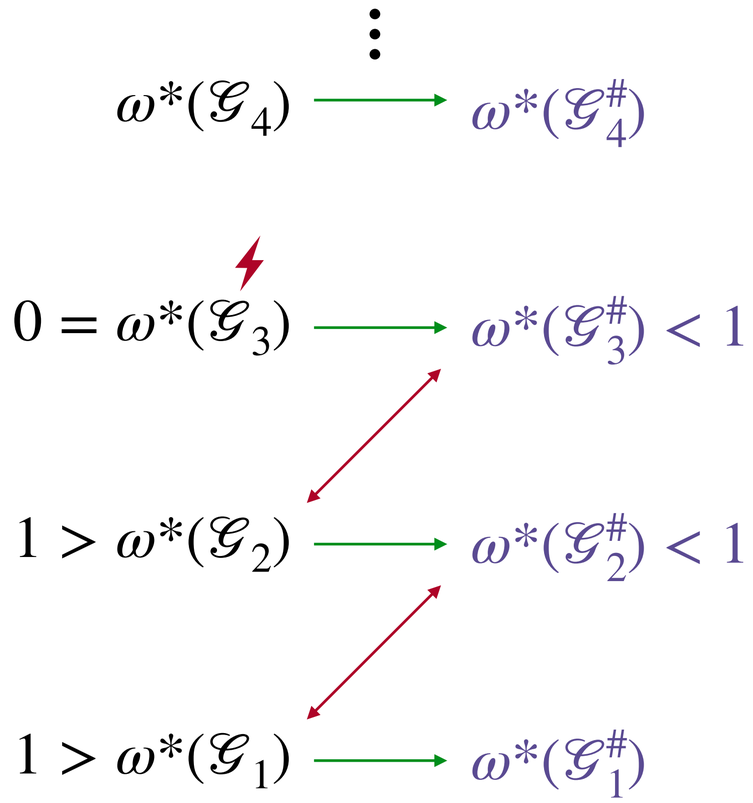
# Compression

## Analysis

$$\omega^*(\mathcal{G}_n) = \omega^*(\mathcal{G}^{\#}_{n+1})$$

$$\omega^*(\mathcal{G}_n) < 1 \implies \omega^*(\mathcal{G}^{\#}_n) < 1$$

If $\neg P(3)$ by construction $\omega^*(\mathcal{G}_3) = 0$
then we can guarantee that $\omega^*(\mathcal{G}_1) < 1$



# Compression

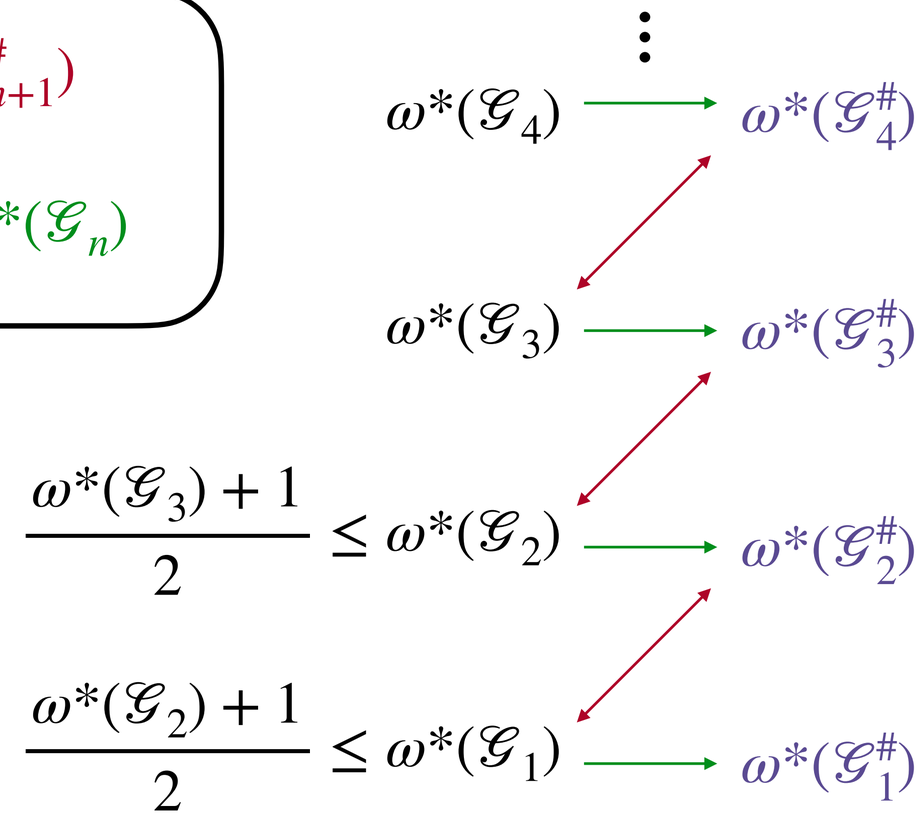
## Analysis

$$\omega^*(\mathcal{G}_n) = \omega^*(\mathcal{G}^{\#}_{n+1})$$

$$\omega^*(\mathcal{G}^{\#}_n) \geq \frac{1}{2} + \frac{1}{2}\omega^*(\mathcal{G}_n)$$

If $\forall n \in \mathbb{N} \,.\, P(n)$ then we can guarantee:

$$\omega^*(\mathcal{G}_1) \geq \lim_{k\to\infty} \frac{\omega^*(\mathcal{G}_{k+1})}{2^k} + \sum_{i=1}^{k} \frac{1}{2^i} = 1$$



# Halting Game

Given a Turing Machine $\mathscr{M}$ there exists an efficiently computable non-local game $\mathscr{G}^{\mathscr{M}}$

If $\mathscr{M}$ eventually halts then $\omega^*(\mathscr{G}^{\mathscr{M}}) = 1$

If $\mathscr{M}$ runs forever then $\omega^*(\mathscr{G}^{\mathscr{M}}) < 1$

# Halting Game

Decidable

$\exists n \in \mathbb{N} \,.\, P(n)$ is True

Turing Machine $\mathscr{M}$

```
n ← 0
While ¬P(n):
    n ← n + 1
```

Eventually Halts

Therefore the corresponding Halting game $\mathscr{G}^{\mathscr{M}}$ decides the RE formula

# Proof Overview

RE formula

$\forall n \in \mathbb{N} \,.\, \exists m \in \mathbb{N} \,.\, P(n, m)$ is True

$\Leftrightarrow$

Turing Machine $\mathscr{M}_n$

$\forall n \in \mathbb{N} \,.$

$m \leftarrow 0$

While $\neg P(n, m)$:

$m \leftarrow m + 1$

Eventually Halts

Therefore if $\forall n \in \mathbb{N}$ the game $\omega^*(\mathscr{G}^{\mathscr{M}_n}) = 1$, then the $\Pi_2^0$ formula is accepted

# Proof Overview

Using compression we can circumvent having to enumerate over all $n \in \mathbb{N}$

Family of games $\mathscr{G}_n$

$\sim$

Reject if the game $\mathscr{G}^{\mathscr{M}_n}$ is lost

Otherwise play the compressed game $\mathscr{G}^{\#}_{n+1}$

$\forall n \in \mathbb{N}.\omega^*(\mathscr{G}^{\mathscr{M}_n}) = 1$ is True

The game $\mathscr{G}_1$ can be played perfectly

# Proof Overview

$\Pi_2$ formula

$\forall n \in \mathbb{N} \,.\, \exists m \in \mathbb{N} \,.\, P(n, m)$ is True

$MIP_0^*$

The corresponding game $\mathcal{G}_1$ can be played perfectly

Therefore every $\Pi_2$ formula can be decided by a corresponding $MIP_0^*$ protocol

# Open Questions

$$\Pi_2 \overset{?}{\subseteq} MIP_0^*[2]$$

# Open Questions

$$MIP^{co} \stackrel{?}{=} {}_{co}RE$$