Multiprover interactive protocols with quantum entanglement

Travis Hance

Massachusetts Institute Of Technology

Dec 10, 2012

Multiprover interactive proofs (classical)

Definition

MIP is the class of languages which admit an interactive protocol with multiple provers with constant soundness and completeness.

Theorem (Babai-Fortnow-Lund (1991))

$MIP = NEXP$.

- The inclusion MIP $\subseteq$ NEXP is trivial.
  - Nondeterministically guess an (exponentially large) prover strategy, and check that it works, using exponential time.

Multiprover interactive proofs (classical)

Definition

MIP is the class of languages which admit an interactive protocol with multiple provers with constant soundness and completeness.

Theorem (Babai-Fortnow-Lund (1991))

$MIP = NEXP$.

- The inclusion MIP $\subseteq$ NEXP is trivial.
  - Nondeterministically guess an (exponentially large) prover strategy, and check that it works, using exponential time.

Multiprover interactive proofs (classical)

Definition

MIP is the class of languages which admit an interactive protocol with multiple provers with constant soundness and completeness.

Theorem (Babai-Fortnow-Lund (1991))

$MIP = NEXP$.

- The inclusion MIP $\subseteq$ NEXP is trivial.
  - Nondeterministically guess an (exponentially large) prover strategy, and check that it works, using exponential time.

Multiprover interactive proofs (quantum)

Definition

MIP* is the class of languages which admit an interactive protocol with multiple provers with constant soundness and completeness where the provers may start with an entangled state.

Theorem (Ito-Vidick (2012))

$MIP^* \supseteq NEXP$.

Multiprover interactive proofs (quantum)

Definition

MIP* is the class of languages which admit an interactive protocol with multiple provers with constant soundness and completeness where the provers may start with an entangled state.

Theorem (Ito-Vidick (2012))

$MIP^* \supseteq NEXP$.

An interactive protocol

To show NEXP $\subseteq$ MIP, we need a NEXP-complete problem.

NEXP-complete problem (Papadimitriou-Yannakakis (1986))

Succinct 3-colorability. Consider an exponentially large graph G with vertices $\{0,1\}^n$, represented by its adjacency matrix, which is given by a polynomial-sized circuit $C : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Is G 3-colorable?

NEXP-complete problem (Ito-Vidick (2012))

Succinct 3-colorability (arithmetized). Given a field $\mathbb{F}$, an element $\alpha \in \mathbb{F} \backslash \{0,1\}$, and an arithmetic circuit for a polynomial $f(\alpha, \boldsymbol{z}, \boldsymbol{b}_1, \boldsymbol{b}_2, a_1, a_2)$ with $\boldsymbol{z} \in \{0,1\}^r$ and $\boldsymbol{b}_1, \boldsymbol{b}_2 \in \{0,1\}^n$, and $a_1, a_2 \in \mathbb{F}$. Does there exist a mapping $A : \{0,1\}^n \to \{0,1,\alpha\}$ such that

$$f(\alpha, \boldsymbol{z}, \boldsymbol{b}_1, \boldsymbol{b}_2, A(\boldsymbol{b}_1), A(\boldsymbol{b}_2)) = 0$$

for all $\boldsymbol{z}, \boldsymbol{b}_1, \boldsymbol{b}_2$?

An interactive protocol

There exist single-prover protocols for the **AND problem** for sufficiently large fields $\mathbb{F}$.

Problem (Babai-Fortnow-Lund (1991))

AND Problem. Suppose you are given oracle access to $h : \mathbb{F}^k \to \mathbb{F}$ and promised it is a polynomial of degree at most d in each variable. Does $h(\boldsymbol{x}) = 0$ for all $\boldsymbol{x} \in \{0,1\}^k$?

- Can be used to show coNP $\subseteq$ IP.
- Protocol has following form: V uniformly and randomly chooses an $\boldsymbol{x} \in \mathbb{F}^k$. Then he interacts with P and reads $h(\boldsymbol{x})$ from the oracle, accepting based on the interaction and the value of $h(\boldsymbol{x})$.

Protocol for succinct 3-colorability:

- Let $h(\boldsymbol{z}, \boldsymbol{b}_1, \boldsymbol{b}_2) = f(\alpha, \boldsymbol{z}, \boldsymbol{b}_1, \boldsymbol{b}_2, A(\boldsymbol{b}_1), A(\boldsymbol{b}_2))$.
- View A as multilinear function $\mathbb{F}^n \to \mathbb{F}$.
- Run the AND test with one prover, say V_3, letting V_1 and V_2 provide $A(\boldsymbol{b}_1)$ and $A(\boldsymbol{b}_2)$ when you need to compute $h(\boldsymbol{z}, \boldsymbol{b}_1, \boldsymbol{b}_2)$.
- Problem: V_1 or V_2 might not use the same A, or they might use a non-multilinear A. Instead of the above, we might instead randomly choose to do either:
  - **Consistency test.** V randomly chooses $\boldsymbol{b}$ and requests that each prover return $A(\boldsymbol{b})$, and checks that all answers agree.
  - **Linearity test.** V randomly chooses $i \in \{1, \ldots, n\}$ and randomly chooses $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3$, differing only in the i^{th} coordinate. Then, V asks prover P_i for $y_i := A(\boldsymbol{b}_i)$, and checks that

$$\frac{y_2 - y_1}{b_{2,i} - b_{1,i}} = \frac{y_3 - y_2}{b_{3,i} - b_{2,i}} = \frac{y_1 - y_3}{b_{1,i} - b_{3,i}}$$

Showing soundness

- **Technical challenge:** show that this protocol is sound.
- **Harder technical challenge:** show that this protocol is sound when the provers have entanglement.
- Idea: Show that if the provers can succeed in the linearity and consistency tests, then we can replace each prover by a prover that always answers with a linear function without affecting the outcome by much. Thus in the AND test, we can treat those provers as an oracle for A.
- Then the protocol is sound by validity of the test for the AND problem.

Quantum measurement

- Suppose a prover is sent $\boldsymbol{x} = (x_1, \ldots, x_n)$.
- Each prover is suppose to respond with an element of $\mathbb{F}$ given $\boldsymbol{x} \in \mathbb{F}^n$.
- We assume that each prover makes his measurement depending on the value $\boldsymbol{x}$ he received, where the measurement has outcomes in $\mathbb{F}$, which he sends to the verifier.
- Define a measurement of *arity* k be a measurement that depends only on $x_{k+1}, \ldots, x_k$, and which returns a multilinear function g in k variables. When a prover makes an arity k measurement, he returns $g(x_1, \ldots, x_k)$.
- Show that we can replace an arity k measurement with an arity $k+1$ measurement.
- Apply iteratively: show that we can replace the prover V_i by a prover V_i' whose measurement is independent of $\boldsymbol{x}$. However, the linear function g which V_i applies might still depend on the outcome of the measurement.

Quantum measurement

- Given two families quantum measurements $\{A_x^a\}$ and $\{B_x^a\}$ of arities k and ℓ, we measure their "closeness" by a measure called the *inconsistency*.
- Suppose V_1 measures using A and V_2 measures using B, and P sends x to both of them. Define

$$\mathrm{INC}(A, B) := \Pr_{x \in \mathbb{F}^n}\left[\begin{array}{c} V_1 \text{ and } V_2 \text{ measure linear functions} \\ \text{which are inconsistent with each other.} \end{array} \right]$$

Going from arity k to $k+1$

Two steps, both analogous to but harder than corresponding results in Babai-Fortnow-Lund. Suppose that $\{A_x^a\}_a$ is the measurement that the prover uses. VERY informally:

- Self-improvement lemma: If $\{R_x^g\}_g$ is a family of measurements with low $\mathrm{INC}(A, R)$, we can find another family of measurements $\{T_x^g\}_g$ with even lower $\mathrm{INC}(A, T)$.
  - But we have to use sub-measurements, which succeed with probability less than 1.
- Pasting lemma: given a measurement $\{T_x^g\}_g$ of arity k with sufficiently low $\mathrm{INC}(A, T)$, we can find a family of sub-measurements or arity $k+1$ with low $\mathrm{INC}(V, T)$.