Oracularization and 2-Prover 1-Round Interactive Proofs against Nonlocal Strategies

> Tsuyoshi Ito (McGill U) Hirotada Kobayashi (NII & JST) Keiji Matsumoto (NII & JST)

> > arXiv:0810.0693

QIP 2009, January 12–16, 2009

# Interactive proof

[Babai 1985] [Goldwasser, Micali, Rackoff 1989]



Verifier: randomized poly-time

- $x \in L \Rightarrow$  prob. of acceptance must be  $\geq c$
- $x \notin L \Rightarrow$  prob. of acceptance must be  $\leq s$

Prover: infinitely powerful computationally

### IP=PSPACE [Shamir 1992]

# Multi-prover interactive proof (MIP) [Ben-Or, Goldwasser, Kilian, Wigderson 1988]



2 or more provers are kept separated

Provers together try to convince V

V can "cross-check" the provers' answers

MIP=NEXP [Babai, Fortnow, Lund 1991]

Note: Shared randomness between provers does *not* change the computational power

# Computational power of MIP

[Feige, Lovász 1992]

- NEXP MIP with
  - Poly provers
  - Poly rounds

- MIP with
  - 2 provers
  - 1 rounds
- Bounded 2-sided error Exp-small 1-sided error

Oracularization technique:

Poly-prover poly-round (with some restriction)  $\rightarrow$  2-prover 1-round



- Each column has odd parity
- Each row has even parity

Max. winning probability = 17/18 in the classical world **1 using prior-entanglement** 

# Effect of quantum nonlocality on MIP

Entanglement gives provers more power

- Honest provers use nonlocality
  - $\rightarrow$  The power of MIP might increase
- Dishonest provers also use nonlocality
  - $\rightarrow$  Existing MIP protocols become unsound

????  $MIP* \subseteq MIP = NEXP$ 

# Related results about MIP in quantum world (1)

 $\oplus$ MIP(2,1),  $\oplus$ MIP\*(2,1):

2 provers, 1 round, 1-bit answer, verifier only look at the XOR of the answers

 With some constant 2-sided error, ⊕MIP\*(2,1)⊆EXP ⊊ NEXP=⊕MIP(2,1) (unless EXP=NEXP) [Cleve, Høyer, Toner, Watrous 2004]

Entanglement makes the class smaller!

 NP⊆⊕MIP\*(2,1) with constant 2-sided error [Cleve, Gavinsky, Jain 2007]

# Related results about MIP in quantum world (2)

- Trivially, MIP\* $\supseteq$ IP=PSPACE
- [Kempe, Kobayashi, Matsumoto, Toner, Vidick 2008]:
  - PSPACE⊆MIP\* with
    - 2 provers, 1 round, 1 1/poly soundness error
  - NEXP  $\subseteq$  MIP\* with
    - 3 provers, 1 round,  $1 1/\exp$  soundness error
  - NEXP  $\subseteq$  QMIP (quantum messages) with 2 provers, 1 round, 1-1/exp soundness error
- NEXP  $\subseteq$  MIP\* with

3 provers, 1 round,  $1 - 1/\exp$  soundness error, 1-bit answer [Ito, Kobayashi, Preda, Sun, Yao 2008]

# Related results about MIP in quantum world (3)

- [Ben-Or, Hassidim, Pilpel 2008]: NEXP has 2-prover 2-round protocol with constant soundness in new model with
  - Quantum interaction
  - Classical communication between provers
  - Without prior-entanglement

# Our results

PSPACE⊆MIP\*

with 2 provers, 1 round, exp-small 1-sided error

- 2 provers are more useful than 1, even with entanglement
- Soundness holds for more powerful **no-signaling** provers

#### • NEXP $\subseteq$ MIP\*

with 2 provers, 1 round,  $1 - 1/\exp 1$ -sided error

 Limitation of independent sampling: Known 2-prover protocols for NEXP really has error probability 1 – 1/exp in some cases

# No-signaling provers

p(a,b|s,t) is called **no-signaling** when

- $p(a,b|s,t) \ge 0$
- $\sum_{a,b} p(a,b|s,t) = 1$
- $\sum_{a} p(a,b|s,t)$  does not depend on s
- $\sum_{b} p(a,b|s,t)$  does not depend on t



Unentangled provers  $\subseteq$  Entangled provers  $\subseteq$  No-signaling provers

MIP with no-signaling provers  $\subseteq$  EXP [Preda]



[KKMTV] proved  $1 - 1/O(r^2)$  soundness error against entangled provers We prove 1 - 1/O(r) soundness error against **no-signaling** provers

# Analysis of soundness (1)

**Suppose:** P<sub>1</sub> and P<sub>2</sub> have a no-signaling strategy to convince V with prob.  $1 - \varepsilon$ , with small  $\varepsilon$ 



 $p(a_1, \dots, a_r; b_1, \dots, b_k | q_1, \dots, q_r; q_1, \dots, q_k) \text{ no-signaling}$   $\Rightarrow p_1(a_1, \dots, a_r | q_1, \dots, q_r) \text{ and } p_2(b_1, \dots, b_k | q_1, \dots, q_k) \text{ are well-defined}$   $q_1, \dots, q_r \longrightarrow \bigoplus_{i=1}^{P_1} \longrightarrow a_1, \dots, a_r \qquad q_1, \dots, q_k \longrightarrow \bigoplus_{i=1}^{P_2} \longrightarrow b_1, \dots, b_k$ 





This P behaves similarly to  $P_1$ 

⇒ If  $x \notin L$ , P<sub>1</sub> and P<sub>2</sub> cannot be accepted w.p. much higher than  $2^{-n}$ (Contradiction!) ⇒  $x \in L$ 

## Final step: Parallel repetition

Running the protocol poly times in parallel → Soundness error becomes exp-small [Holenstein 2007]

Resulting protocol exactly the same as [Cai, Condon, Lipton 1994]

# Implication

Oracularization of 1-prover IP protocols works even if 2 provers are just no-signaling

> Cf. 1-prover constant-round IP is weak:  $IP(k)=AM \subseteq \Pi_2 P$ [Goldwasser, Sipser 1986 & Babai, Moran 1988]

If we want constant-round interactive proof with exp-small error, asking 2 provers is more powerful than asking 1 prover even if 2 provers are entangled (unless the polynomial hierarchy collapses)

## 2-prover 1-round protocol for NEXP

### 3-query PCP for $L \in NEXP$



Provers can cheat with entanglement (Kochen-Specker game, Magic Square game) [Cleve, Høyer, Toner, Watrous 2004] Dummy question prevents perfect cheating

3-query PCP for  $L \in NEXP$ 



High acceptance prob.

All the measurements by provers are almost commuting Soundness error at most  $1 - 1/O(|Q|^2) = 1 - 1/\exp(|Q|^2)$ against entangled provers

Similar to [Kempe, Kobayashi, Matsumoto, Toner, Vidick 2008]



- Each column has odd parity
- Each row has even parity

# Limit of independent sampling



# Summary

2-prover 1-round protocol for PSPACE with **exp-small** soundness error against **no-signaling** provers based on oracularization technique

2-prover 1-round protocol for NEXP with  $1 - 1/\exp$  soundness error against entangled provers using oracularization with dummy question

**Independent sampling** seems to impose limitation on soundness

- The above protocol for NEXP
- Quantum 2-prover 1-round protocol for NEXP by [KKMTV08]

# Open problems

- Better soundness for EXP & NEXP
- Upper bound for MIP\*
  - [Doherty, Liang, Toner, Wehner] [Navascués, Pironio, Acín] imply 2-prover 1-round MIP\*⊆Recursive assuming finite-dim entanglement suffices
- Characterization of MIP<sup>ns</sup>, MIP with no-signaling provers
  - PSPACE  $\subseteq$  MIP<sup>ns</sup>  $\subseteq$  EXP (upper bound based on LP [Preda])
- Parallel repetition for MIP\*
- Alternative to oracularization
  - Parallelization
    - Possible using quantum answers from provers [Kempe, Kobayashi, Matsumoto, Vidick 2007]
  - Reducing the number of provers