A multi-prover interactive proof for NEXP sound against entangled provers

Thomas Vidick
Massachusetts Institute of Technology

Joint work with Tsuyoshi Ito, NEC Labs

NEXP $\subseteq$ MIP*

Thomas Vidick
Massachusetts Institute of Technology

Joint work with Tsuyoshi Ito, NEC Labs

A multi-prover interactive proof for NEXP sound against entangled provers

Thomas Vidick
Massachusetts Institute of Technology

Joint work with Tsuyoshi Ito, NEC Labs

Entanglement as a resource

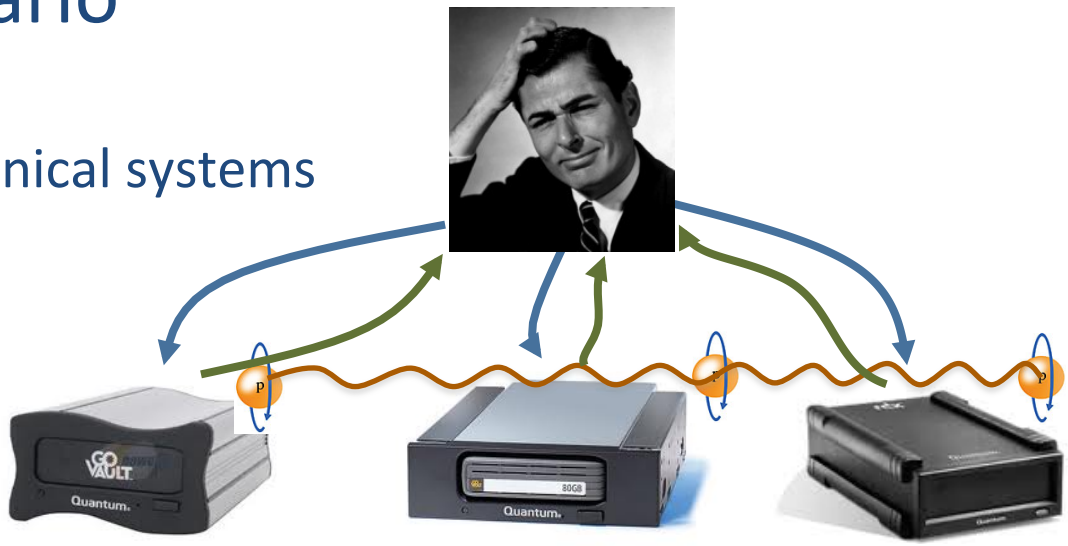
[PR'98]

Goal: ~~minimize weirdness of entanglement~~

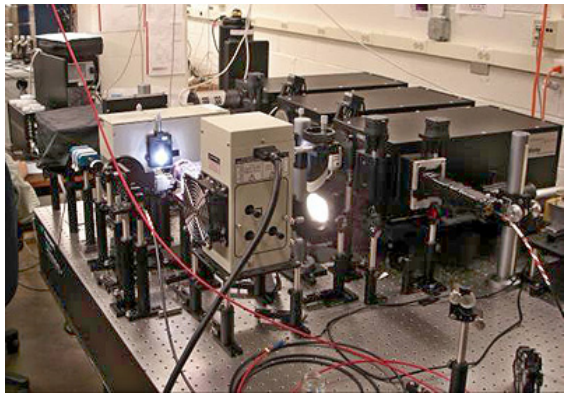
operational characterization
of strengths & limitations

- *Information theory (LOCC)*
  (Chitambar, Monday; Li, Tuesday)
- *Quantum foundations*
  (Palazuelos, Monday)
- *Device-independent cryptography*
  (Colbeck; V., Wednesday)
- *Testing of quantum systems*
  (Reichardt, Monday)
- *Condensed-matter physics*
  (Schuch, Thursday; Brandao; Landau, Friday)

The typical scenario



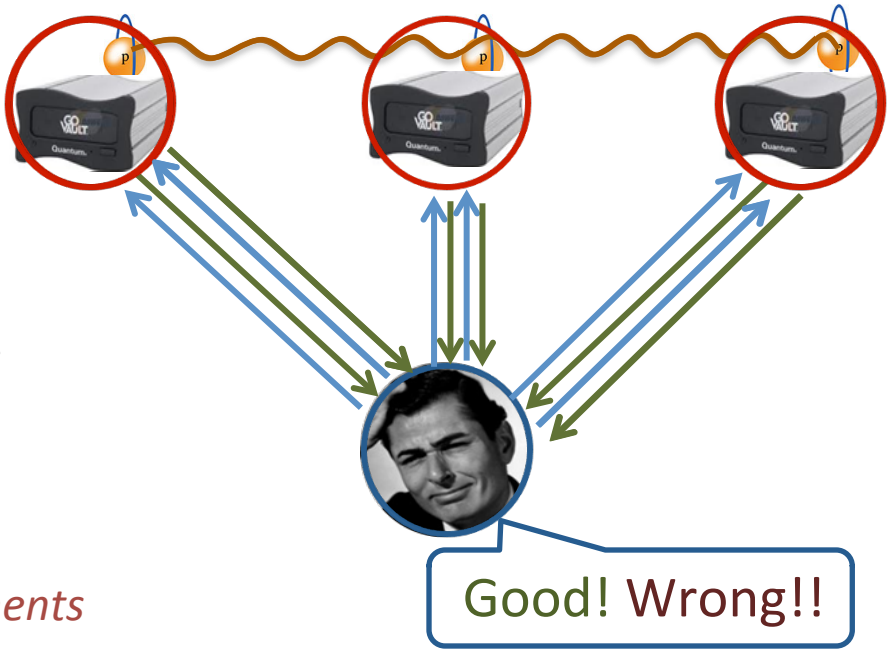
- Two or more quantum mechanical systems
  - Implicitly known
    (e.g. many-body Hamiltonian)
  - Partially characterized
    (e.g. bounded dimension)
  - Completely unknown
    (e.g. adversarial system in crypto)



- Local measurements on each system
  - Can be known (e.g. measure energy; tomography)
  - Or not (device-independent crypto; testing;
    Bell inequality violations)

- User interacts and collects statistics
  - Given system description, predict statistics?
  - Given observed statistics, reverse-engineer system ??

Multiplayer games



Model interaction of classical "referee" with quantum "players"

- Referee asks questions; players answer
- Referee decides to accept/reject

$\omega\uparrow^*(G)$:= max. prob. acceptance

optimize over *all states* and *all measurements*

- Basic question: given game, what is the maximum probability of acceptance?
  - *Given Bell inequality, what is the largest possible violation?*

    Ex: "CHSH game": random questions $x,y \subset \{0,1\}$; check answers $a \oplus b = x \wedge y$. $\omega\uparrow^*(G) \approx 0.85\ldots$
  - *Does there exist a tripartite entangled state satisfying certain constraints?*

- Meta question: What is the complexity of computing $\omega\uparrow^*(G)$?

The complexity of entangled games

Given game G, how hard is it to compute $\omega\uparrow*(G)$?

- Sounds pretty hard…
  - Optimize over *all states* and *all measurements* (no a priori dimension bound!)
  - Years of experience have not brought many algorithms
    (max. violation of $I\downarrow 3322$ inequality only known to 7 digits; tripartite setting seems out of reach)
  - [KKTM… …ayers, 2 bit-answers)
- But
  - For a… a un… (and vice-versa) …tion inequalities): exact algorithm *SDP-based*
  - [CJPP;RV'12] …-player quantum XOR games: approximation algorithm, *SDP-b…ed*
  - [KRT'10] Unique games: approximation algorithm, *SDP-bas…*
  - [PNA;DLTW'09] General 1-round games: *hierarchy of SDPs*, …
  - [Pre'07;Ito'12] *Linear program* for no-signaling strategies

$$\langle I_{3322}\rangle := -\langle A_2\rangle - \langle B_1\rangle - 2\langle B_2\rangle + \langle A_1B_1\rangle + \langle A_1B_2\rangle + \langle A_2B_1\rangle + \langle A_2B_2\rangle - \langle A_1B_3\rangle + \langle A_2B_3\rangle - \langle A_3B_1\rangle + \langle A_3B_2\rangle$$

$$\max \mathrm{Tr}(A\downarrow 0 \cdot X)$$
$$\text{s.t. } \mathrm{Tr}(A\downarrow i \cdot X) = b\downarrow i$$
$$X \geq 0$$

- Main result: no constant-factor approximation algorithm for $\omega\uparrow*$

  (unless NP $\subseteq$ DTIME($2\uparrow \mathrm{polylog}\, n$))

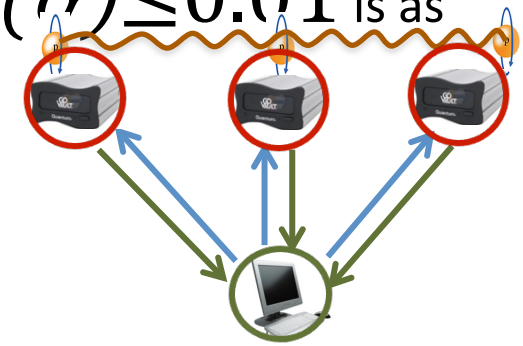
Showing hardness: interactive proof systems

- Let L be a "hard" language (e.g. 3-SAT), φ an instance (formula)
- Goal: distinguishing $\omega\uparrow^*_{\varphi}(G) \geq 0.99$ from $\omega\uparrow^*_{G\downarrow\varphi}(G) \leq 0.01$ is as hard as deciding L

$x\downarrow 1 \vee x\downarrow 2 \vee x\downarrow 5$
$x\downarrow 3 \vee x\downarrow 5 \vee x\downarrow 2$
$x\downarrow 1 \vee x\downarrow 4 \vee x\downarrow 2$

SAT $\Rightarrow$ $\omega\uparrow^*(G) \geq 0.99$

UNSAT $\Rightarrow$ $\omega\uparrow^*(G) \leq 0.01$



|Q| could be exp(|x|)

MIP* = { L s.t. $\exists x \rightarrow G\downarrow x$ computable in time poly($|\varphi|$) }

!! *Protocol* $G\downarrow x$, input size = $|x| \approx$ size(circuit for $R\downarrow x$) *Game* G, input size = |Q||A|

Some known results

MIP

- NEXP $\subseteq$ MIP [BFL'91]
- MIP $\subseteq$ NEXP [Folklore]
- Restricted classes:
  - MIP = MIP(2 provers, 1 round, const. answer length)
  - $\bigoplus$MIP = NEXP [Has'01]

MIP*

- MIP(1 prover)=PSPACE $\subseteq$ MIP*
- MIP* $\subseteq$??
- $\bigoplus$MIP* $\subseteq$ PSPACE [CHTW'04,Weh'06] (Efficient algorithm follows from semidefinite programming)
- MIP* = MIP*(1 round) [Ito'12]
- Number of provers?

MIP^{ns} (no-signaling strategies)

- MIP^{ns} $\subseteq$ EXP [Pre'07] (LP formulation)
- $MIP^{ns}(2,1)$ $\subseteq$ PSPACE [Ito'12]

NEXP $\subseteq$ MIP*: entanglement does not weaken the power of multi-prover interactive proofs

> Thm: Every language in NEXP has a 3-prover, poly-round proof system sound against entangled provers

- Constant-factor NP hardness for $\omega\uparrow^*(G)$ in 3-player, poly-round games (under quasi-polynomial reductions)
- Can reduce to 4-prover, 1-round, factor (1+1/polylog(|Q|)) (using [Ito'12])

- Proof based on [BFL'91] protocol showing NEXP $\subseteq$ MIP
  - poly-round *sum-check test* with one of the provers [LFKN]
  - single-round *multilinearity test* with three provers
- Key point: soundness of multilinearity test *against entangled provers*
  - *Show test "immune" to collusion from entanglement*

Using multiple provers

- Given a system of linear equations over $\mathbb{F}_2 = \{0,1\}$

$$(E_1): u_1 + u_2 + u_3 = 0 \qquad (E_4): u_1 + u_4 + u_7 = 0$$
$$(E_2): u_4 + u_5 + u_6 = 0 \qquad (E_5): u_2 + u_5 + u_8 = 0$$
$$(E_3): u_7 + u_8 + u_9 = 1 \qquad (E_6): u_3 + u_6 + u_9 = 0$$

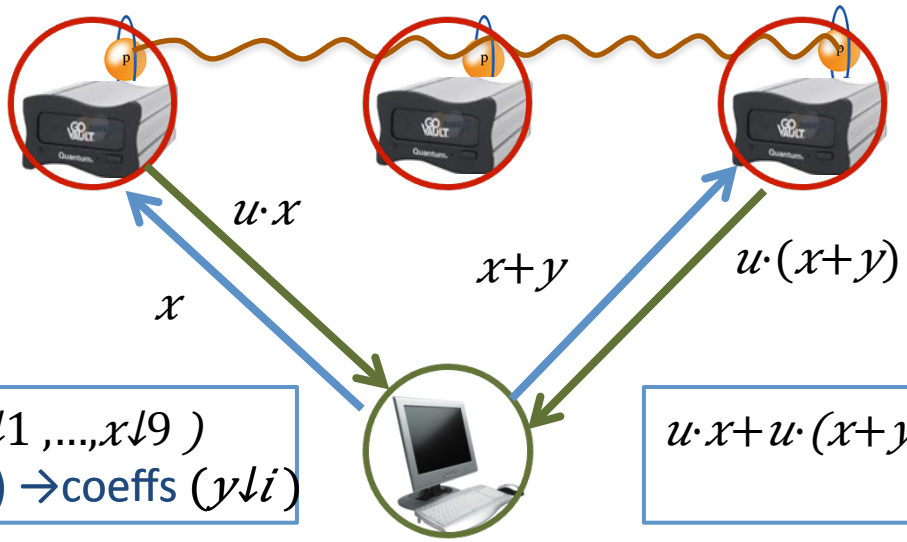
- Is there an assignment satisfying *most* equations?
- ~~Idea 1: ask for best solution $(u_1, u_2, \ldots, u_9)$~~
  - Works, but lots of communication prover → referee
  - Goal = check for *existence* of good solution… no need to see it!
- Idea 2: Suppose we knew provers: $(x_1, \ldots, x_9) \mapsto u \cdot x = u_1 x_1 + \cdots u_9 x_9$ (some u, most x)

Using multiple provers

- Given a system of linear equations over $\mathbb{F}_2 = \{0,1\}$

$$(E_1): u_1 + u_2 + u_3 = 0 \qquad (E_4): u_1 + u_4 + u_7 = 0$$
$$(E_2): u_4 + u_5 + u_6 = 0 \qquad (E_5): u_2 + u_5 + u_8 = 0$$
$$(E_3): u_7 + u_8 + u_9 = 1 \qquad (E_6): u_3 + u_6 + u_9 = 0$$

- Idea 2: Suppose we knew provers: $(x_1, \ldots, x_9) \mapsto u_1 x_1 + \cdots u_9 x_9$ (solve u, most x)



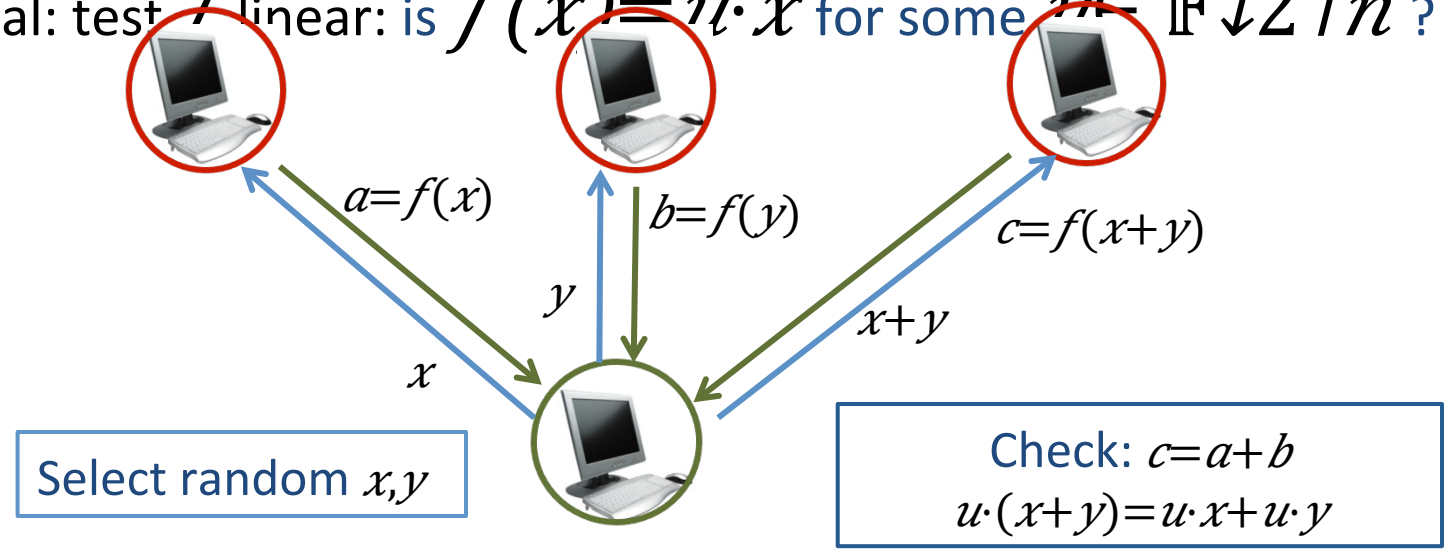
- Random $x = (x_1, \ldots, x_9)$
- Random eq. $(E) \rightarrow$ coeffs (y_i)

$u \cdot x + u \cdot (x+y) = u \cdot y$
$= $ r.h.s. of (E)?

- Referee can check satisfiability without seeing solution!
- Catch: how do we check provers: $(x_1, \ldots, x_9) \mapsto u \cdot x$ (for *unknown* u!)

The Blum-Luby-Rubinfeld linearity test

- Three provers, apply same function f: $\mathbb{F}_2^n \to \mathbb{F}_2$
- Goal: test f linear: is $f(x) = u \cdot x$ for some $u \in \mathbb{F}_2^n$?



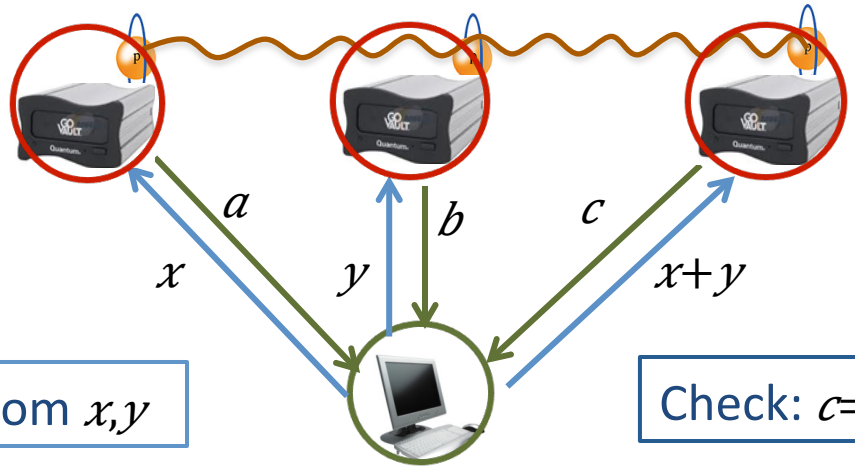
Theorem (BLR). Suppose provers succeed w.p. $1-\epsilon$.

Then $\exists u$ s.t. $f(x)=u \cdot x$ for at least $1-6\epsilon$ fraction of x

Proof. (1) Success $1-\epsilon \Rightarrow \exists u, |f(u)| \geq 1-2\epsilon$.

(2) f and $u \cdot x$ agree on all but ϵ fraction of x.

The *entangled-prover* linearity test



- To answer $x \in \mathbb{F}_2^n$, prover measures $|\Psi\rangle$ using $\{A_{x,0}, A_{x,1}\}$

$$p_{a,b,c|x,y,z} = \langle\Psi| A_{x,a} \otimes A_{y,b} \otimes A_{z,c} |\Psi\rangle$$

- Q

Lemma. Suppose provers succeed w.p. $1-\epsilon$.
Then ∃ .t. provers are *ndistinguishable* from:

answer x with $u \cdot x$

The *entangled-prover* linearity test

Lemma. Suppose provers succeed w.p. $1-\epsilon$.
Then $\exists \{M\uparrow u\}$ s.t. provers are $\sqrt{\epsilon}$-*indistinguishable* from:
(i) measure using $\{M\uparrow u\}$, get same u w.h.p.
(ii) answer x with $\mathrm{u}\cdot x$

- $\{M\uparrow u\}$ *independent* of x : could measure before game starts
  → We identified a *basis* in which the provers are *classical*

- $\{M\uparrow u\}$ easy to define! $M\uparrow u = |A(u)\rangle\uparrow 2 = |E\downarrow x\,[(-1)\uparrow u\cdot x\, A\downarrow x]\rangle\uparrow 2$

- Work is in relating new $\{M\uparrow u\}$-provers to original $\{A\downarrow x\uparrow a\}$-provers
- Indistinguishable?
  - Need strong enough notion to extend to bigger proof system
  - Cannot hope for too much (e.g. operator norm)
  - We use *consistency*: $\mathrm{E}\downarrow x \sum u,a:\ u\cdot x\neq a\uparrow$ ▒ $\langle\Psi|A\downarrow x\uparrow a \otimes M\uparrow u \otimes \mathrm{Id}|\Psi\rangle$

Summary

- Approximating the entangled value $\omega^{*}(G)$ of a multiplayer game is computationally hard: MIP = NEXP $\subseteq$ MIP*
- Proof: linearity/multilinearity tests are "entanglement-robust"

Questions

- What is the importance of the number of provers?
  - What is the complexity of 2-prover MIP?
- Constant answer size, constant rounds, constant soundness?
  - Would give some analogue of classical PCP theorem [V., in preparation]
- Is there a more direct argument? (de Finetti theorems?)
- Use of linearity/multilinearity tests in other settings
  - Soundness against entangled players should be useful elsewhere

Thank you!

Financial support from

The multilinearity test

- Tests that $f:\mathbb{F}^m \to \mathbb{F}$ is linear in each variable
  - $n=2: f(x,y)=axy+bx+cy+d$
- Test: pick a coordinate $i \in [n]$ and check linearity in i-th direction
- Analysis: by induction
  - Reconstruct linear approximations $f(x,y) \approx \ell_y(x)$ for every fixed y
  - Interpolate to recover $f(x,y) \approx \mathrm{bilin}(x,y)$
- Error blows up: key step of ``self-correction''
  - Challenging step in the entangled-prover case

Theorem. Suppose provers succeed w.p. $1-\epsilon$ in ML-test
Then $\exists \{M,g\}$ s.t. provers are $(\epsilon^c \cdot n^d + n^e/m)$ *–indist.* from:
(i) measure using $\{M,g\}$, get same u w.h.p.
(ii) answer x with $g(x)$