Bar-Ilan University
אוניברסיטת בר-אילן

BIU
Center for Research in Applied Cryptography and Cyber Security

The 11th BIU Winter School on Cryptography in a Quantum World

February 14-17, 2021

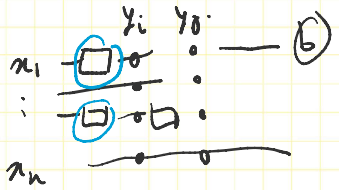
Thomas Vidick
California Institute of Technology

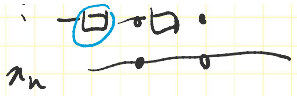
Delegation of quantum computations

Thomas Vidick, Caltech

Part II: *Delegation with two quantum provers*

Two-prover delegation



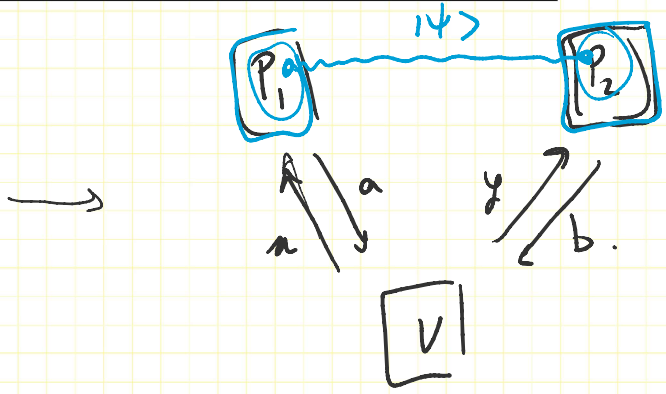


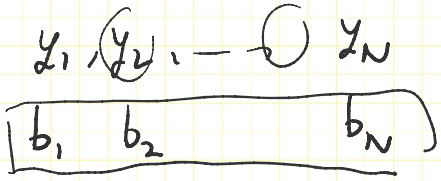
- Classical computations:
  - [BFLS'10] verify non-deterministic polytime computation using polylog verifier
  - Based on probabilistically checkable proofs (PCP): interpret computation as local constraint satisfaction problem ("tableau") and encode satisfying assignment in locally checkable code.

- Quantum computations: No good notion of PCP! Either:
  - Delegate circuit on a gate-by-gate basis, many repetitions to bring soundness down;
  - Hamiltonian model: check preparation of history state certificate for computation.

- Main challenge is to classically test that provers have/measure qubits as directed

Two quantum provers sharing entanglement





1-round protocols:

$|\psi\rangle \in H_A \otimes H_B$.

P_1: $\forall x$, $\{A_a^x\}_a$ on H_A

P_2: $\forall y$ $\{B_b^y\}_b$ H_B

$A_a^x \geq 0$ $\sum_a A_a^x = \mathbb{1}$.

$$p(a,b \mid x,y) = \langle\psi| A_a^x \otimes B_b^y |\psi\rangle$$

$$B_{b_N}^{y_N} \cdots B_{b_2}^{y_2} B_{b_1}^{y_1} |\psi\rangle$$

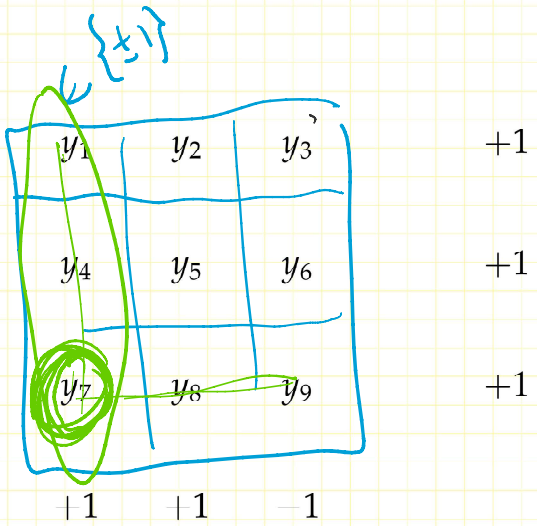
$$\cdots B_{b_2}^{y_2}|\psi\rangle \; B_{b_1}^{y_1}|\psi\rangle$$

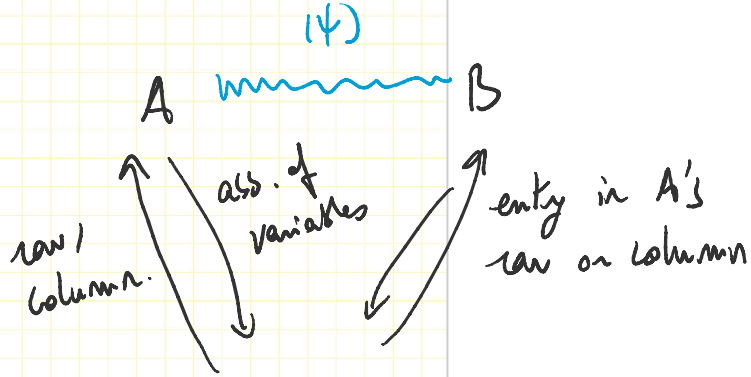
$a,b \in \{\pm 1\}$

$$E[ab] = \langle\psi| A^x \otimes B^y |\psi\rangle$$

$+\langle\psi| A_{+1}^x - A_{-1}^x \quad B_{+1}^y - B_{-1}^y$

The Magic Square game





✓
- consistent
- A's answers satisfy constraint.

Claim: max prob (succes) = $\frac{17}{18}$.

max prob (succes, quantum) = 1.

Quantum solution

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad Y = iXZ$$

$I \otimes Z$	$Z \otimes I$	$Z \otimes Z$	$+\mathrm{Id}$
$X \otimes I$	$I \otimes X$	$X \otimes X$	$+\mathrm{Id}$
$X \otimes Z$	$Z \otimes X$	$Y \otimes Y$	$+\mathrm{Id}$
$+\mathrm{Id}$	$+\mathrm{Id}$	$-\mathrm{Id}$	

$|\psi\rangle = |EPR\rangle_{AB} |EPR\rangle_{A'B'}$

Rigidity

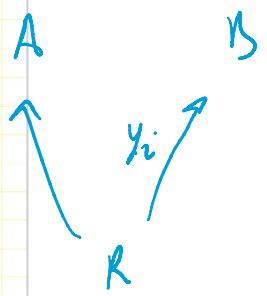
Theorem. *Suppose that two players sharing a state* $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ *succeed with probability* 1 *in the Magic Square game. Let* $B_1, \ldots, B_9$ *be Bob's observables in the game. Then*

$$B_2 B_4 = -B_4 B_2 .$$

$$B_2 B_4 = (B_1 B_3)(B_6 B_5)$$
$$= - B_1 B_9 B_5$$

$$B_4 B_2 = (B_1 B_7)(B_8 B_5)$$
$$B_1 B_9 B_5$$

y_1	y_2	y_3	$+1$
y_4	y_5	y_6	$+1$
y_7	y_8	y_9	$+1$
$+1$	$+1$	-1	



Rigidity

Corollary. *Suppose that two players sharing a state* $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ *succeed with probability* 1 *in the Magic Square game. Let* $B_1, \ldots, B_9$ *be Bob's observables in the game. Then there is a unitary* $V_B : \mathcal{H}_B \to \mathbb{C}^2_{B'} \otimes \mathcal{H}_{B''}$ *such that*

$$\begin{array}{ccc} \mathcal{H}_B & \xrightarrow{V} & \mathbb{C}^2_{B'} \otimes \mathcal{H}_{B''} \\ {\scriptstyle B_2,\, B_4}\downarrow & & \downarrow{\scriptstyle Z\otimes \mathrm{Id},\; X\otimes \mathrm{Id}} \\ \mathcal{H}_B & \xrightarrow{V} & \mathbb{C}^2_{B'} \otimes \mathcal{H}_{B''} \end{array}$$

Furthermore,

$$V_A \otimes V_B |\psi\rangle = |EPR\rangle_{A'B'} \otimes |aux\rangle_{A''B''} .$$

$B_2 B_4 = -B_4 B_2$

Pf Assume $\dim(H) = 2$.

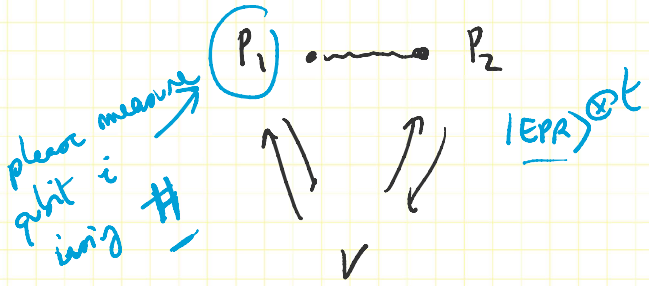
Then $B_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$ ± 1.

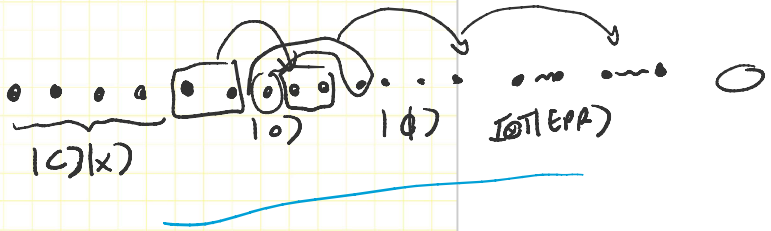
$B_4 B_2 = -B_2 B_4 \to B_4 = \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \to \times$

General: Jordan's lemma.

General : Jordan's lemma.

The RUV protocol





Given as input a circuit $\mathcal{C}$. Perform one of the following four tests with equal probability:

1. Play $t = \text{poly}(|\mathcal{C}|)$ sequential Magic Square (MS) games with the two provers. If the fraction of successes is below $1 - \delta$ then reject.
2. Execute a state tomography protocol in which Bob is asked to perform measurements that correspond to $t/2$ magic states. Alice is instructed to play t MS games. Alice's measurement outcomes are used to check the results reported by Bob.
3. Execute a process tomography protocol in which Alice is instructed to perform Bell basis measurements according to the pattern that corresponds to the teleportation-based circuit associated with $\mathcal{C}$. Bob is instructed to play t MS games. Bob's measurement outcomes are used to verify that Alice is reporting the correct outcomes for her Bell measurements.
4. Orchestrate the computation of $\mathcal{C}$: instruct Bob to prepare the magic states as in step 2, and Alice to perform Bell basis measurements as in step 3. Use the measurement outcome reported by Alice for the output qubit as the output of the computation (after having applied the required Pauli corrections).

- Verifier is classical
- bulky
  poor completeness / soundness gap
- many rounds.

Verification in the Hamiltonian model

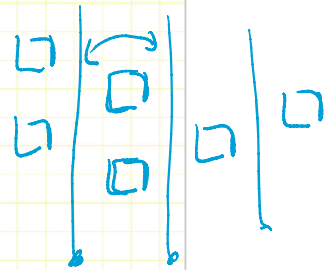
Theorem. *For any integer $n \geq 1$ there is $m = \mathrm{poly}(n)$ such that the following holds. Given a poly-size quantum circuit $\mathcal{C}$ acting on n qubits and an input x for $\mathcal{C}$ there exist efficiently computable real weights $\{\alpha_P : P \in \{I,X,Z\}^{\otimes m}\}$ such that $\sum_P |\alpha_P| = 1$ and moreover if*

$$H_{\mathcal{C}} = \sum_{P \in \{I,X,Z\}^{\otimes m}} \alpha_P P$$

then:

- *(Completeness) If $\mathcal{C}$ accepts x with probability at least $2/3$ then $\lambda_{min}(H_{\mathcal{C}}) \leq -\frac{2}{3}$.*
- *(Soundness) If $\mathcal{C}$ accepts x with probability at most $1/3$ then $\lambda_{min}(H_{\mathcal{C}}) \geq \frac{2}{3}$.*

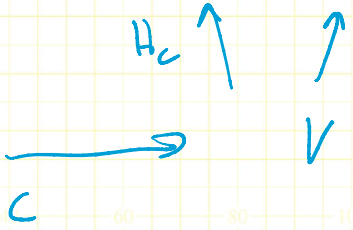
$\frac{1}{\mathrm{poly}}$



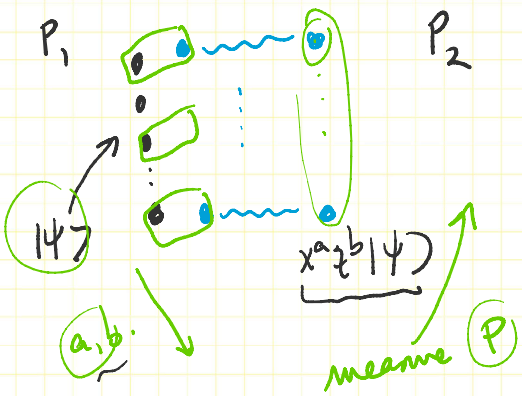
$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots$

$|\psi\rangle = \frac{1}{\sqrt{T}} \sum_{t=1}^{T} |\psi_t\rangle$

P P : prepare a $|\psi\rangle$ s.t. $\langle\psi|H_{\mathcal{C}}|\psi\rangle = \lambda_{min}(H_{\mathcal{C}}) \leq -\frac{2}{3}$



The Grilo protocol



$$H_C = \sum_P \alpha_P P$$

$$\langle\psi|H_C|\psi\rangle \leq 0$$

$$= \sum_P \alpha_P \langle\psi|P|\psi\rangle$$

$$\langle\psi|x^a z^b P x^a z^b|\psi\rangle$$

Given a circuit $\mathcal{C}$ and input x, let H_C be the m-qubit associated Hamiltonian.

Perform either of the following with probability $1-p$ and p, respectively:

1. Execute an m'-qubit entanglement test with both provers.
2. Select $P' \in \{I, B_1, \ldots, B_9\}^{m'}$ uniformly at random. Select $P \in \{I, X, Z\}^m$ according to $|\alpha_P|$. Let $t_1, \ldots, t_m$ be such that for all $i \in \{1, \ldots, m\}$,

$$P'_{t_i} = B_2 \text{ (if } P_i = Z), \qquad P'_{t_i} = B_4 \text{ (if } P_i = X), \qquad P'_{t_i} = I \text{ (if } P_i = I)$$

   (a) Send $t_1, \ldots, t_m$ to Alice and P' to Bob.

   (b) Alice replies with $a, b \in \{0,1\}^m$ and Bob with $c \in \{-1,1\}^{m'}$.

   (c) For $i \in \{1, \ldots, m\}$ let $d_i = (-1)^{a_i} c_{t_i}$ if $P_i = Z$ and $d_i = (-1)^{b_i} c_{t_i}$ if $P_i = X$.

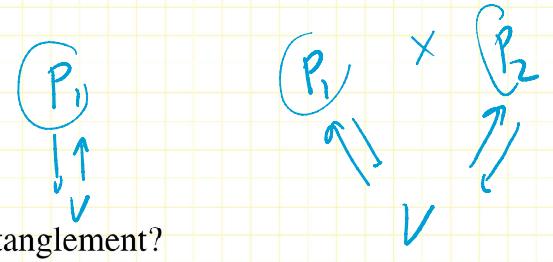
   (d) Accept if $\prod_i d_i = \text{sign}(\alpha_P)$.

verifier is classical ✓

1 - sound ✓

Efficient two-prover delegation

- Need test for multi-qubit entanglement + Pauli measurements: "Pauli braiding test" [NV'18] extends BLR linearity test.
- Combine with PCP techniques to obtain polylog classical verification of quantum polytime computation (**). (Also QMA languages given adequate access to a witness.)



Open questions

- Two-prover delegation of quantum computation with no entanglement?
- (**) Can we get rid of the setup/CRS?
- Quantum PCP?
- Efficient verification without circuit-to-Hamiltonian?
- Efficient entanglement tests are not noise-tolerant. Delegation with noisy entanglement?

200
180
160
140
120
100
80
60
40
mm
40
60
80
100
120
140
160
180
200
220
240
260