

**Thomas Vidick**  
California Institute of Technology

# Delegation of quantum computations

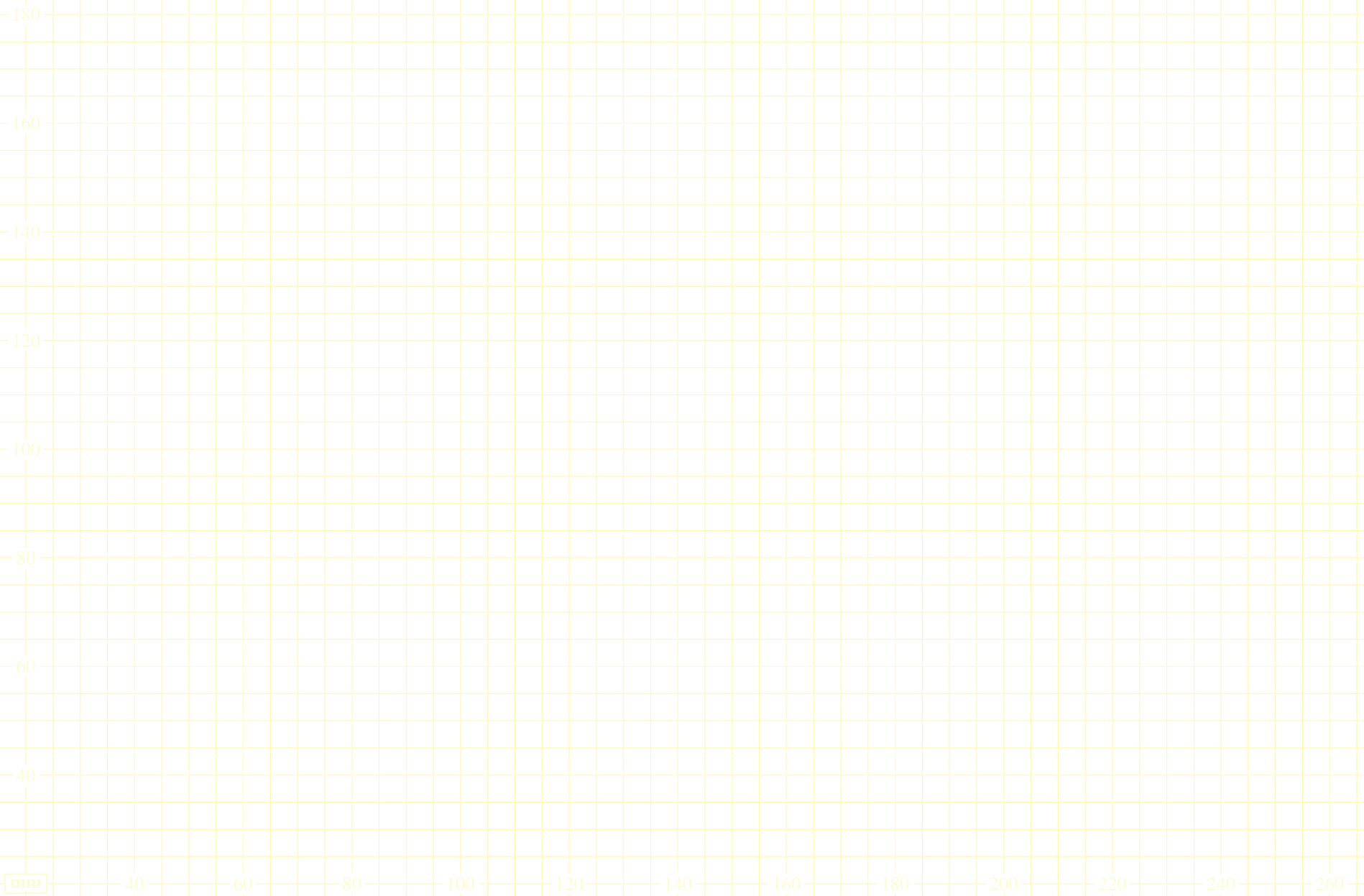
Thomas Vidick, Caltech

Part II: *Delegation with two quantum provers*

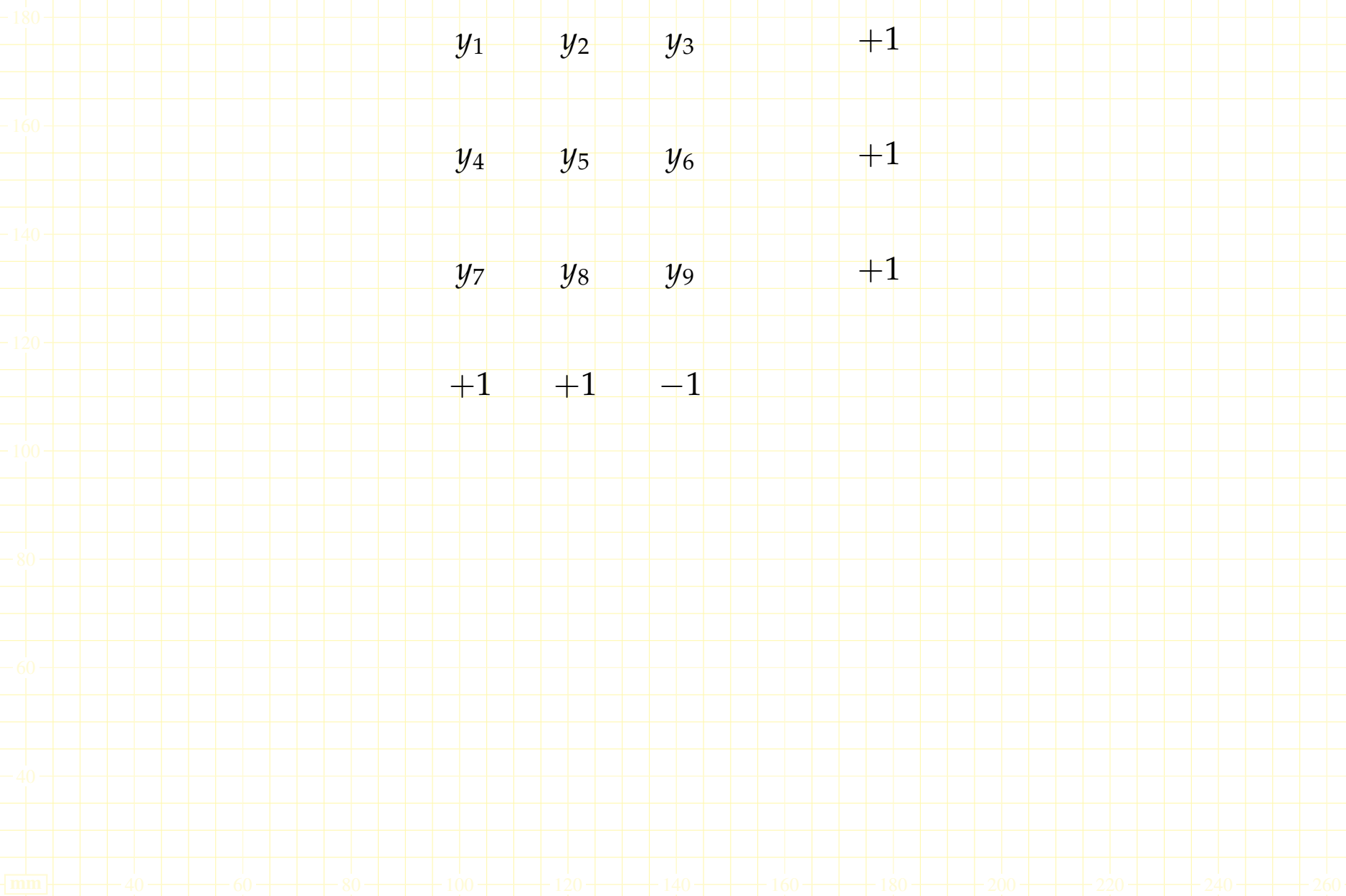
## Two-prover delegation

- 180 • Classical computations:
  - 160 – [BFLS'10] verify non-deterministic polytime computation using polylog verifier
  - 140 – Based on probabilistically checkable proofs (PCP): interpret computation as local constraint satisfaction problem (“tableau”) and encode satisfying assignment in locally checkable code.
  - 120
- 100 • Quantum computations: No good notion of PCP! Either:
  - 80 – Delegate circuit on a gate-by-gate basis, many repetitions to bring soundness down;
  - Hamiltonian model: check preparation of history state certificate for computation.
  - 60
- 40 • Main challenge is to classically test that provers have/measure qubits as directed

## Two quantum provers sharing entanglement



## The Magic Square game



## Quantum solution

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

$$I \otimes Z \quad Z \otimes I \quad Z \otimes Z \quad + \text{Id}$$

$$X \otimes I \quad I \otimes X \quad X \otimes X \quad + \text{Id}$$

$$X \otimes Z \quad Z \otimes X \quad Y \otimes Y \quad + \text{Id}$$

$$+ \text{Id} \quad + \text{Id} \quad - \text{Id}$$

## 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  $B_1, \dots, B_9$  be Bob's observables in the game. Then*

$$B_2 B_4 = -B_4 B_2 .$$

$y_1$	$y_2$	$y_3$	+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  $B_1, \dots, B_9$  be Bob's observables in the game. Then there is a unitary  $V_B : \mathcal{H}_B \rightarrow \mathbb{C}_{B'}^2 \otimes \mathcal{H}_{B''}$  such that*

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

Furthermore,

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

## The RUV protocol

180

160

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).

140

120

100

80

60

40

20

0

180

160

140

120

100

80



## Verification in the Hamiltonian model

**Theorem.** For any integer  $n \geq 1$  there is  $m = \text{poly}(n)$  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  $\lambda_{\min}(H_{\mathcal{C}}) \geq \frac{2}{3}$ .

## The Grilo protocol

180

160

Given a circuit  $\mathcal{C}$  and input  $x$ , let  $H_{\mathcal{C}}$  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  $P' \in \{I, B_1, \dots, B_9\}^{m'}$  uniformly at random. Select  $P \in \{I, X, Z\}^m$  according to  $|\alpha_P|$ . Let  $t_1, \dots, t_m$  be such that for all  $i \in \{1, \dots, m\}$ ,

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

- (a) Send  $t_1, \dots, t_m$  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  $i \in \{1, \dots, m\}$  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  $\prod_i d_i = \text{sign}(\alpha_P)$ .

## 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?

