Lecture 4 - Delegating quantum computations (2/2)

Thursday, 30 January 2025 13:46

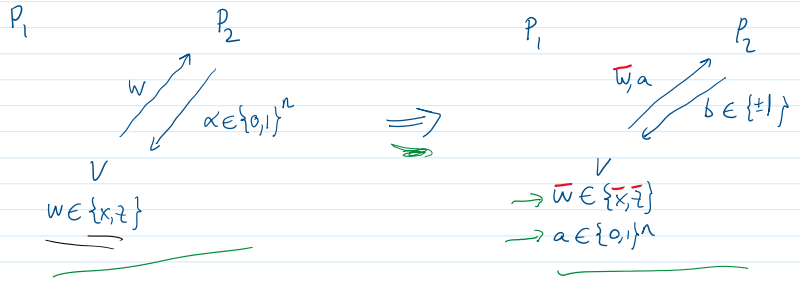
Where we are :

Goal : develop a classical verifier, quantum prover protocol for delegating a quantum computation.

Intermediate goal : do it in the two-prover model

Intermediate intermediate goal : Force a prover to measure n qubits in prescribed bases (X or Z).

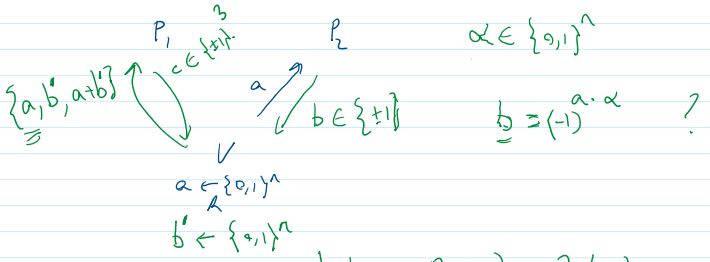
Shifting the goal :



$2^n + 2^n$ questions : $(\bar{X}, a) \rightarrow$ P_2 measures X on n qubit $\rightarrow \alpha \in \{0,1\}^n$ return $(-1)^{a \cdot \alpha}$

$(\bar{Z}, b) \rightarrow$ P_2 measures Z on n qubit $\rightarrow \beta \in \{0,1\}^n$ return $(-1)^{b \cdot \beta}$

Classical case : linearity testing



. check : $P_1(a) = P_2(a)$

$\propto P_1(a+b') = P_1(a) \cdot P_1(b')$

Analysis : Let $f : \{0,1\}^n \rightarrow \{\pm 1\}$ be P_2's answer function.

Consistency $\Rightarrow$ P_1 answers $\{a, b, a+b\}$ with $f(a), f(b), f(a+b)$

$\Rightarrow$ $f(a+b) = f(a) f(b)$ $\forall a, b$

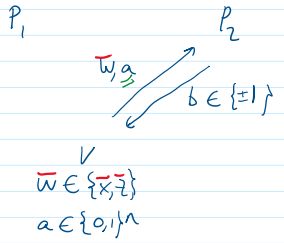
$\Rightarrow \forall a,\ f(a) = (-1)^{a \cdot \alpha}$ for some α.

More generally: (P_1, P_2) succeed w.p. $\geq 1-\varepsilon$

$\Rightarrow \exists \alpha,\ |\hat{f}(\alpha)|^2 \geq 1 - O(\varepsilon)$

Group perspective: we checked that $f: \{0,1\}^n \to \{\pm 1\}$ is a representation of the group $\mathbb{Z}_2^n$ $\quad f(a+b) = f(a) f(b)$

Back to the quantum case:



In general, P_2 applies observable $\bar{W}(a)$ to obtain answer b from question a

Q: What conditions guarantee $\bar{W}(a) \simeq \bar{X}(a) = \bar{X}^{a_1} \otimes \cdots \otimes \bar{X}^{a_n}$ $(\bar{W} = \bar{X})$

$\bar{W}(b) \simeq \bar{Z}(b) = \bar{Z}^{b_1} \otimes \cdots \otimes \bar{Z}^{b_n}$ $(\bar{W} = \bar{Z})$

A: $\bar{W}(a)\,\bar{W}(a') = \bar{W}(a+a')$ $\quad \forall \bar{W} \in \{\bar{X}, \bar{Z}\}$

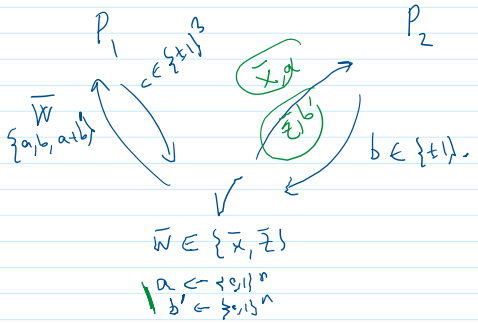
$\bar{X}(a)\,\bar{Z}(b) = (-1)^{a \cdot b}\,\bar{Z}(b)\,\bar{X}(a)$

Rk These relations define the Pauli group $\mathbb{Z}_2 \wr \mathbb{Z}_2^n$

It has a unique irreducible rep. that sends $-1 \to -I$.

It is given by the Pauli matrices of dim $2^n \times 2^n$

Game With_n :



wp $\frac{1}{3}$ do :

wp $\frac{1}{3}$ do: Test 1 : anticommutation: case $a \cdot b = 1 \pmod 2$

Play a variant of MS game where

P_1 receives row/column ℓ + pair (a, b')

P_2 receives square j + pair (a, b')

unless $j = 2 \Rightarrow$ receive "$\bar{X}, a$"

$j = 4 \Rightarrow$ receive "$\bar{Z}, b$"

Test 2 : commutation : case $a \cdot b = 0 \pmod 2$

Skip details (simple consistency game)

Analysis : P_2 measurement associated with questions "$\bar{X}, a$" and "$\bar{Z}, b$" induce $\bar{X}(a), \bar{Z}(b)$ s.t. $\bar{X}(a)\bar{Z}(b) = (-1)^{a \cdot b} \bar{Z}(b)\bar{X}(a)$.

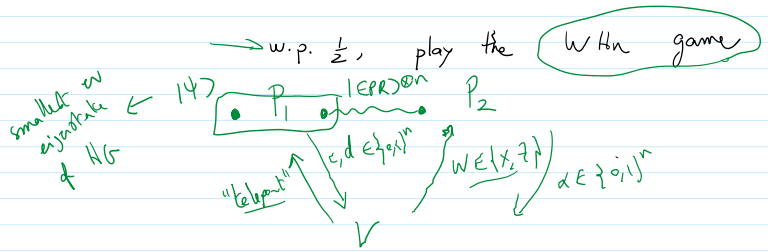
$\bar{X}(a)\bar{X}(a') = \bar{X}(a+a')$, $\bar{Z}(b)\bar{Z}(b') = \bar{Z}(b+b')$

By lemma 1', up to a change of basis they are equivalent to honest n-qubit X, Z measurements.

Back to the Grilo protocol.

Input : Graph $G = (V, E) \rightarrow$ Hamiltonian H_G.

Protocol : w.p. $\frac{1}{2}$, play the teleportation game



Theorem: The Grilo protocol has $c-s \geq 1/\text{poly}$
Communication is $O(n)$

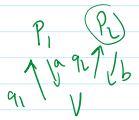
Rk With more work, get: $c = 1 - \text{negl}$
$s < 1$

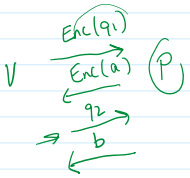
communication $V \to P$ $\text{polylog}(n)$
$P \to V$ $O(n)$

Need:
- more efficient multi-qubit test, with com. $\text{polylog}(n)$
- quantum-safe PRG

(Open: total communication $\text{polylog}(n)$, no computational assumption, BQP power) "quantum games PCP conjecture"

Final step: Compile into single-prover game with computational soundness (QFHE)





- Natarajan-Zhang '22
  Metger-Natarajan-Zhang '23
  "succinct argument" for BQP/QMA

- Kulpe et al '24
  Compilation preserves the game value for any game, asymptotically

$$\omega_{max}(G_{comp}) := \limsup_{\lambda \to \infty} \{ \omega_\lambda(G_{comp}) \mid \{S_\lambda\} : \text{ptime strategy in } G_{comp} \}$$

Thm: $\omega_{max}(G_{comp}) \leq \omega_{qc}(G)$

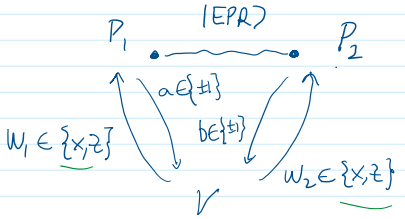
Open question: can we show bounds on the speed of convergence, as a function of δ?

Obstacle:

Open questions about single-prover, classical-verifier delegation:

- Weaken computational assumptions
- Information-theoretic soundness
- "Doubly efficient" protocols for bounded time and space.

Using quantum entanglement to control randomness:

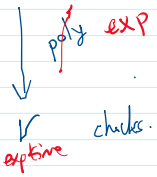


- If $W_1 = W_2$, $(a, b) \sim (c, c)$ with $c \sim_U \{\pm 1\}$
- If $W_1 \neq W_2$, $(a, b) \sim (c, d)$ with $c, d \sim_U \{\pm 1\}$ independent.

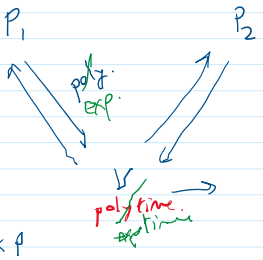
$\Rightarrow$ The Magic Square game and its compiled version are tests for randomness.

P

Def: NP / MA

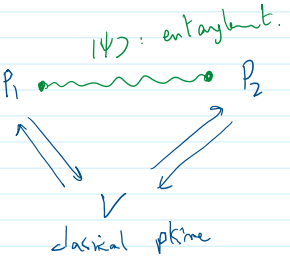


MIP



$MIP_{exp} = NEXP$

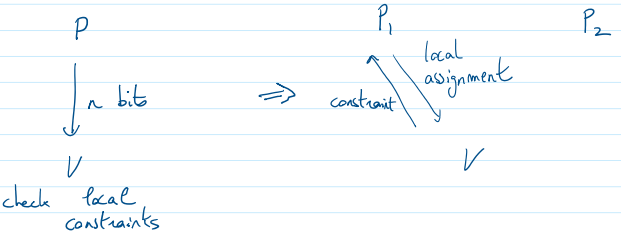
MIP^*



Thm Babai - Fortnow - Lund '91

$MIP = NEXP$

Idea:



Benefit: exp. reduced comm.

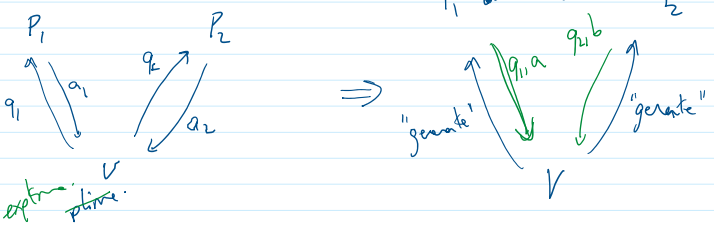
Cost: randomness + 2 provers.

Th Natarajan - Wright '19

$MIP^* \supseteq NEEXP$

$\supseteq NEXP$

Idea:



Benefit: n-qubit test requires polylog(n) bit questions.

Th Ji et al. '22 $MIP^* = RE$

$RE \subseteq MIP^k$ (2 provers)

MIP^k (k provers) $\subseteq RE$

Iterate the previous idea and take a "limit".

Open questions about 2-prover quantum interactive proofs:

- Does $QMA \subseteq MIP^*$ with $-$ polylog(n) com. ($QMA = BQP$) $-$ BQP prover.
- $NTIME(poly(s)) \subseteq MIP^* \subseteq DTIME(2^{poly(s)})$ (quantum space s, honest prover)

  What is the right answer?
- Does the number of provers affect these questions?