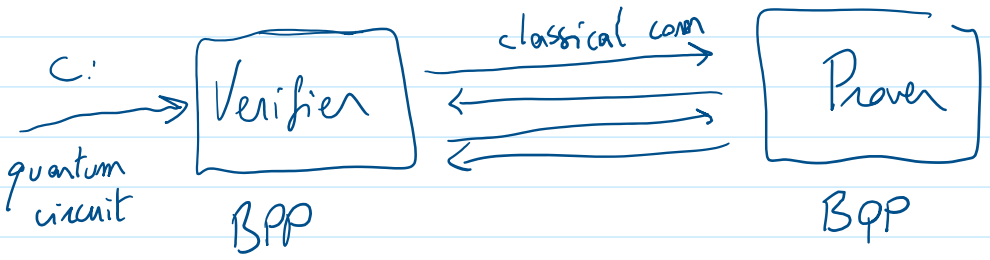
Lecture 1 - Interactive tests of quantumness

Thursday, 16 January 2025 12:13

Thomas Vidick, Weizmann → EPFL, thomas.vidick@epfl.ch

How to delegate a quantum computation ?



Completeness : if C returns 1 wp $\geq \frac{2}{3}$, $\exists$ prover that is accepted whp

Soundness : if C returns 1 wp $\leq \frac{1}{3}$. every prover is rejected whp.

Part A : Tests of quantumness

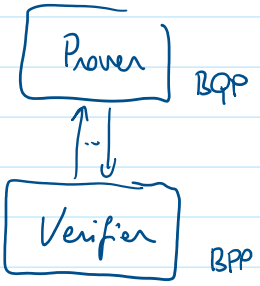
→ identify unique aspects of quantum and provide classical tests for them

Part B : Classical delegation of quant. computation

→ Combine Part A with techniques from [illegible] (PFHE) and complexity (IP)

→ Combine Part A with techniques from cryptography (QFHE) and complexity (IP)

Tests of quantumness:



Completeness: $\exists$ q. prover, accepted w.p. $\geq \frac{2}{3}$

Soundness: $\forall$ class. prover (polytime), ——— $\leq \frac{1}{3}$

Require BQP ≠ BPP

Known approaches:

- Factor / break a classically hard but quantumly easy assumption
  - ✗ requires specific comp ass.
  - ✓ simple
  - ✗ not efficient for q. prover
  - ✗ not very useful.

- Sampling from otput dist. of a random circuit
  - ✓ fairly practical (Google '2019)
  - ✗ not verifiable.
  - ✗ not useful.

- Nonlocal games / Bell tests
  - ✓ practical '69
  - ✓ very useful
  - ✗ ~~hard~~ hard to scale.

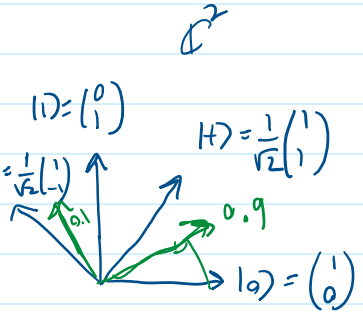
- Interactive test based on post-quantum crypto assumption
  - ✓ theoretically very nice
  - ✗ not quite practical

How to test a device for quantum behaviour ?
→ what is unique to quantum

- uncertainty principle.
- entanglement.

Later : - Some complexity theory (interactive proofs)
- Some cryptography (Quantum FHE)

Measurements and uncertainty



Quantum state $|\psi\rangle \in \mathbb{C}^d$

Measurement: basis $\{|v_i\rangle\}$

outcome $\{\lambda_i\}$

$P_r(\lambda_i) = |\langle v_i|\psi\rangle|^2$

Observable $O = \sum_i \lambda_i |v_i\rangle\langle v_i|$ ← $v_i v_i^T$

$E_{|\psi\rangle}[\lambda] = \sum_i P_r(\lambda_i)\cdot\lambda_i$

$= \sum_i |\langle v_i|\psi\rangle|^2 \lambda_i$

$= \langle\psi| O |\psi\rangle$

Ex: comp. basis $|0\rangle \to +1$, $|1\rangle \to -1$ ($|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$)

$Z = +1\cdot|0\rangle\langle 0| - 1\cdot|1\rangle\langle 1| = \begin{pmatrix}1&0\\0&-1\end{pmatrix}$

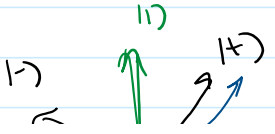
Hadamard basis $|+\rangle \to 1$, $|-\rangle \to -1$ $\quad X = \begin{pmatrix}0&1\\1&0\end{pmatrix}$

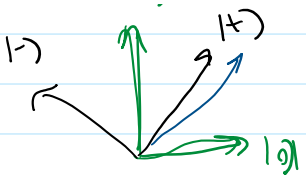
$\begin{pmatrix}1&0\\0&1\end{pmatrix}$

$(I, X, Z, Y = iXZ)$ are the Pauli matrices.

Fact: (I, X, Z, Y) are an orthonormal basis of $\mathbb{C}^{2\times 2}$ for $\langle A, B\rangle = \frac{1}{2}\mathrm{Tr}(A^\dagger B) = \frac{1}{2}\sum_{ij}\overline{A_{ij}}\,B_{ij}$

Proof: check it □





Thm (Heisenberg uncertainty)

$\forall |\psi\rangle \in \mathbb{C}^2$, $|\langle\psi|X|\psi\rangle|^2 + |\langle\psi|Z|\psi\rangle|^2 \leq \underbrace{\||\psi\rangle\|^2}_{1}$

$\underbrace{\qquad\qquad\qquad\qquad}_{1}$

Proof Let $\rho = |\psi\rangle\langle\psi|$. Then $\rho \in \mathbb{C}^{2\times 2}$ is psd with $\mathrm{Tr}(\rho) = \langle\psi|\psi\rangle = 1$.

Expand $\rho = \alpha_I I + \alpha_x X + \alpha_z Z + \alpha_y Y$

$\mathrm{Tr}(\rho^2) = \mathrm{Tr}(\rho) = 1 = \alpha_I^2 + \alpha_x^2 + \alpha_z^2 + \alpha_y^2$

$\alpha_x = \mathrm{Tr}(X\rho) = \langle\psi|X|\psi\rangle$

$\alpha_z = \mathrm{Tr}(Z\rho) = \langle\psi|Z|\psi\rangle$ □

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $XZ = -ZX$

Rk: Uncertainty valid $\forall A, B$ $A^2 = B^2 = I$ $AB = -BA$

Lemma 1: If $A^2 = B^2 = I$ and $AB = -BA$ then $\exists$ unitary U s.t. $UAU^\dagger = X \otimes I$, $UBU^\dagger = Z \otimes I$

$\left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$, $\left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$

Testing quantum uncertainty

The Magic Square (game)

9 variables $y_1, \dots, y_9 \in \{\pm 1\}$

$y_i \in \mathbb{C}^{d \times d}$

Hermitian

$y_i^2 = I$

	c_1	c_2	c_3	
r_1	y_1	y_2	y_3	$+I$
r_2	y_4	y_5	y_6	$+I$
r_3	y_7	y_8	y_9	$+1$
	$+1$	$+1$	I	

Non-commutative solution:

$X \otimes I \cdot I \otimes Z = X \otimes Z$

$X \otimes I_2$	$I \otimes X$	$X \otimes X$	$I \otimes I$
$I \otimes Z$	$Z \otimes I$	$Z \otimes Z$	
$X \otimes Z$	$Z \otimes X$	$-Y \otimes Y$	
		$-I \otimes I$	

Lemma 2: If $y_1, \dots, y_9$ are a (non-commutative) solution to the Magic Square, then $y_2 y_4 = -y_4 y_2$

Proof $y_2 y_4 = y_1 y_5 \cdot y_4$

$= y_4 y_2 =$

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

An interactive proof for checking MS solution:

1st attempt:

Prover

ℓ? ↑ ↓ $a \in \{\pm 1\}^3$

Verifier

Select $\ell \in \{r_1, r_2, r_3, c_1, c_2, c_3\}$.

check parity constraint

Select $\ell \in \{r_1, r_3, c_1, c_3\}$.

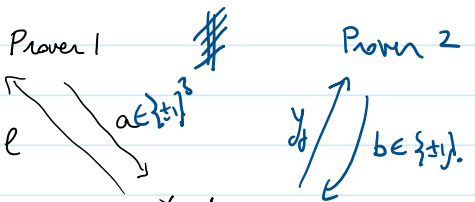
check parity constraint

✓ Q prover succeed.

✗ C prover succeeds.

- Prepare any state $|\psi\rangle \in \mathbb{C}^4$
- Jointly measure $Y_{j_1}, Y_{j_2}, Y_{j_3}$ where $\ell = \{j_1, j_2, j_3\}$
- Return outcomes $a_1, a_2, a_3 \in \{\pm 1\}$

2nd attempt:



Select $\ell \in \{r_i, c_i\}$

Check parity of a

Select $y_j \in \ell$ at random

check consistency

✓ Classical prover succeeds w.p. $\leq \frac{17}{18}$

✓ Quantum prover ——— 1

Entanglement

Def $|\psi\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ is entangled if

$|\psi\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$

ex: • $|\phi_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$

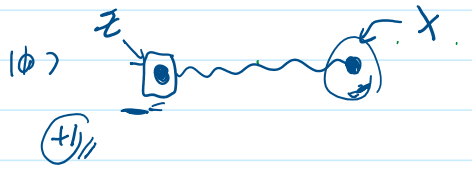
• $|\phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle|i\rangle$

Fact For any observable O, s.t. $O^2 = I$,

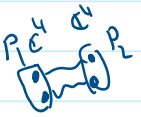
$\langle \phi_d | O \otimes O | \phi_d \rangle = 1$

Proof: $\langle \phi_d | A \otimes B | \phi_d \rangle = \frac{1}{d} \mathrm{Tr}(A^T B)$

Proof: $\langle \phi_d | A \otimes B | \phi_d \rangle = \frac{1}{d} \mathrm{Tr}(A^T B)$



Quantum strategy for MS game:



P_1 and P_2 share $|\phi_4\rangle$ = 2 EPR pairs

P_1 receives ℓ → measures $Y_{\ell 1}$, $Y_{\ell 2}$, $Y_{\ell 3}$ → $a \in \{\pm 1\}^3$

P_2 receives d → measures Y_d → $b \in \{\pm 1\}$

Succeeds w.p. 1 in both tests.

→ Nonlocal test of quantumness

Lemma 1: If $A^2 = B^2 = I$ and $AB = -BA$ then
$\exists$ unitary U s.t. $UAU^\dagger = X \otimes I$
$UBU^\dagger = Z \otimes I$

+

Lemma 2: If $Y_1, \ldots, Y_9$ are a (non-commutative) solution to the Magic Square, then $Y_2 Y_4 = -Y_4 Y_2$

Theorem: Suppose P_1, P_2 succeed in MS game w.p. $\geq 1-\varepsilon$.
Let $B_1, \ldots, B_9$ be observables measured by P_2
let $|\psi\rangle$ be the shared entanglement
Then: $\| I \otimes (B_2 B_4 + B_4 B_2) |\psi\rangle \|^2 = O(\varepsilon)$