Information Theoretically Secure Hypothesis Test for Temporally Unstructured Quantum Computation

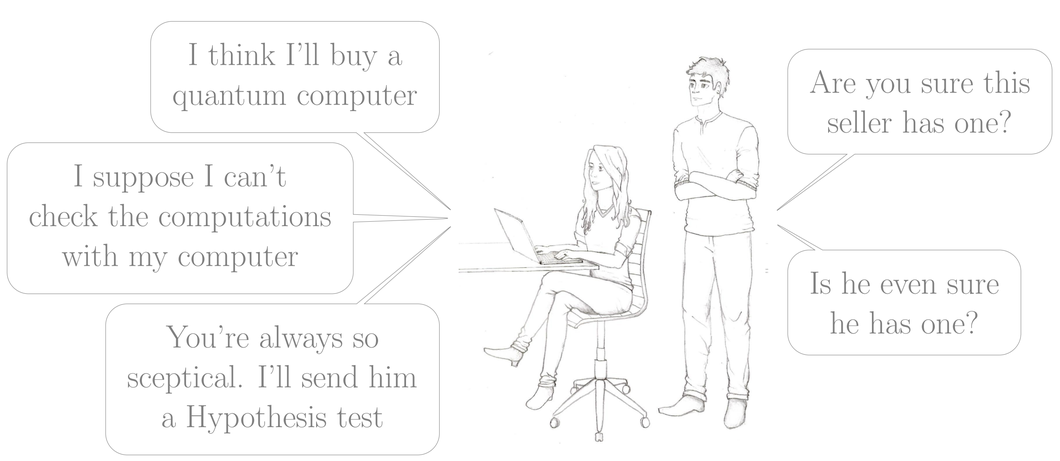
Daniel Mills, Anna Pappa, Theodoros Kapourniotis and Elham Kashefi

School of Informatics, University of Edinburgh, UK

Contact: daniel.mills@ed.ac.uk

Introduction

Quantum computers may revolutionise the technology industry. However:



A well designed *Hypothesis Test* should allow:

- A Client to ensure a malicious Server is capable of quantum computations.
- An engineer to check their machine is capable of quantum computations.

The IQP machine

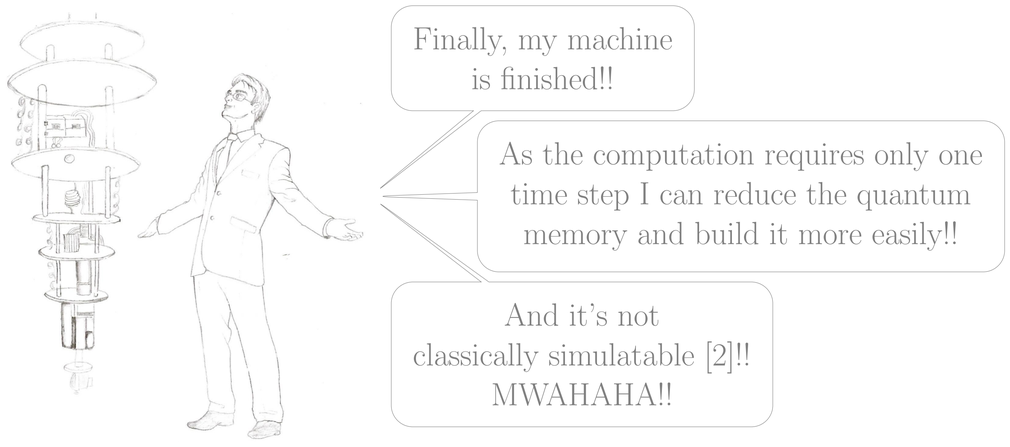
The *Instantaneous Quantum Polytime* [1] machine implements gates of the form:

$$\exp\left\{ i\theta \bigotimes_{i:q_i=1} X_i \right\}$$

where $q \in \{0,1\}^{n_p}$, $\theta \in [0, 2\pi]$, the input is $|0^{n_p}\rangle$ and the output is the resulting state measured in the computational basis. An IQP program may consist of many of these gates, and so many different q. Hence we may represent the whole computation by, for example:

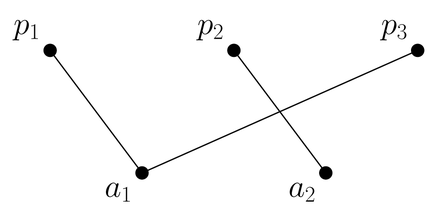
$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

where, in this case, we have two gates defined by $q = (101)$ and $q = (010)$.
The commuting nature of the gates reveals the origin of the word *instantaneous* as gates can be applied in any order, or, in theory, in one time step (instantaneously).



IQP in MBQC

One can implement IQP by first entangling $|+\rangle$ states according to, for example, the following graph. Notice that, as is general, there is a edge between p_j and a_i when $\mathbf{Q}_{ij} = 1$.

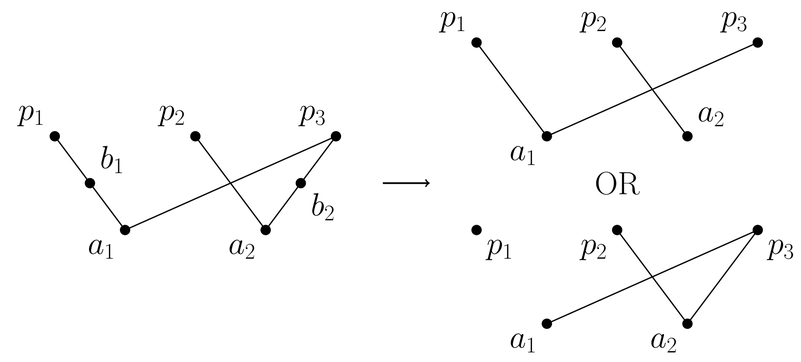


$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

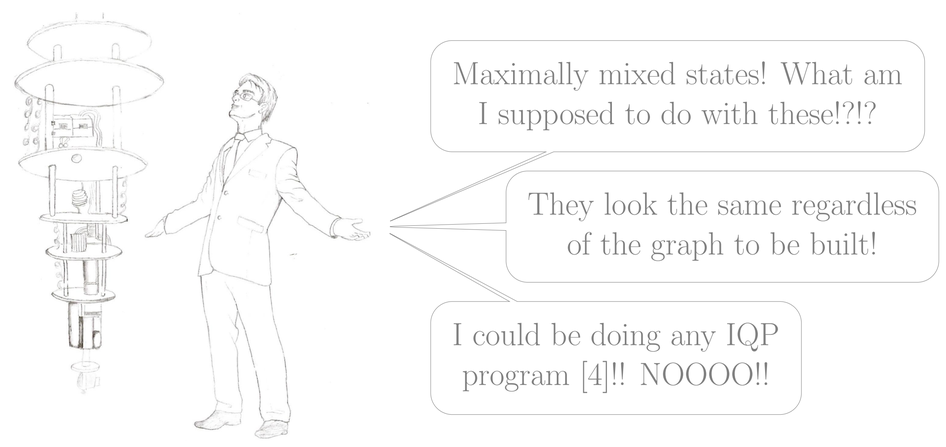
The results of Hadamard basis measurements on qubits p_j, corrected according to the results of Y-Z plane measurements on qubits a_i, constitutes the output.

Blind IQP

By implementing *bridge* or *break* operations [3] on the intermediate qubits, b_k, one can replace them with a connection between their neighbours, or not, respectively.



Many different graphs can be created in this way. This can be done on the Server's side by sending only what looks, to the Server, to be single qubit maximally mixed states.



The graph building process for one graph is indistinguishable from that of any other so the graph is *hidden*. Hence, the Server can first build and then measure the appropriate state for an IQP computation in two measurement rounds, without knowing the computation.

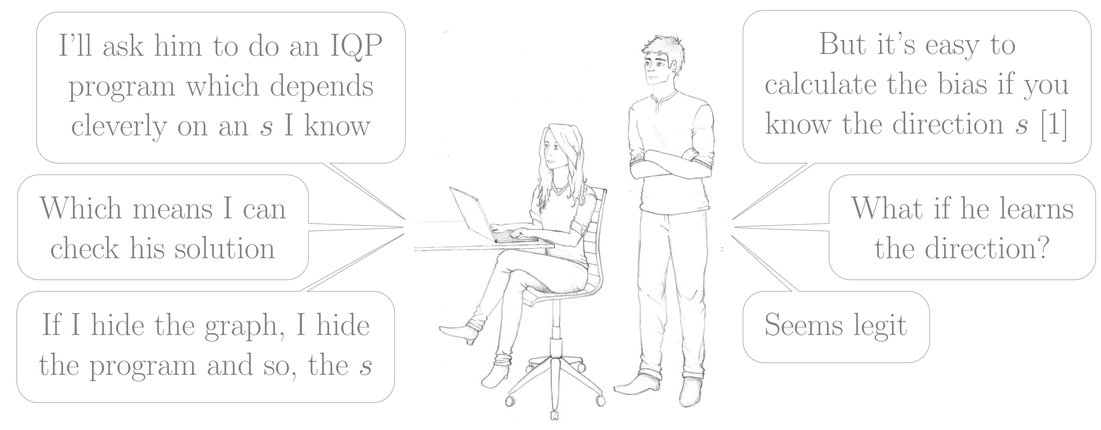
Hypothesis Test

There are three key conditions that a hypothesis test must meet:

- A Client asks a Server to perform a hard to classically simulate IQP computation.
- The Client can check the solution to this computation because they know some secret structure that makes this checking processes efficient.
- The Server must be unable to uncover this structure in polynomial time.

We will use the *bias* of a random variable, $X \in \{0,1\}^{n_p}$, in a direction $s \in \{0,1\}^{n_p}$.

$$\text{Bias}\,(X, s) = \mathbb{P}\left(X \cdot s^T = 0\right)$$



Hence, by sending single qubits, an otherwise classical Client can ask a Server to produce an output, about which they know some information. They can use this information to check if the output is the one requested, and so if it is sampled from an IQP distribution.

References

[1] Dan Shepherd and Michael J Bremner. Temporally unstructured quantum computation.

[2] Michael J Bremner, Richard Jozsa, and Dan J Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy.

[3] Joseph F Fitzsimons and Elham Kashefi. Unconditionally verifiable blind computation.

[4] Daniel Mills, Anna Pappa, Theodoros Kapourniotis, and Elham Kashefi. Information theoretically secure hypothesis test for temporally unstructured quantum computation.

Many thanks to Joanne Mills for the drawings.