Verification and Utilisation of Noisy Intermediate Scale Quantum Technology

Daniel Mills Elham Kashefi

daniel.mills@ed.ac.uk

What's the motivation?

Quantum computers may revolutionise the technology industry. However:

I'm going to build a quantum computer.

Good luck, it's hard.

Okay, maybe one of the small ones which are easier to build.

You know, the ones that do some but not all quantum computations.

If it is not very quantum how do you know it is not just classical?

Ummm...

Also, these devices experience errors so the output might be random.

Golly, I didn't think about these things.

What's the point of all this anyway?

Well... I want to do some machine learning...

Sounds like a lot of buzzwords.

We suggest:

- *IQP* as a small (*non-universal*) quantum computer to explore.
- A *Hypothesis test* to confirm some quantumness.
- *Numerical simulations* to judge the effect of noise.
- *Machine learning* using IQP devices as a useful application.

What tools are we using?

Qubits: Classically a bit can be in the state 1 or 0. Quantumly these states are represented by $|1\rangle$ and $|0\rangle$ which we call the *computational basis*. A quantum bit, or *qubit*, can also be in the 'half $|0\rangle$, half $|1\rangle$' *Hadamard basis*:

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad , \qquad |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Measurement: If we *measure* $|+\rangle$ *in the computational basis* we are equally likely to obtain $|0\rangle$ or $|1\rangle$. Measuring in the Hadamard basis produces $|+\rangle$ with certainty. More generally, the state $|\psi\rangle = \alpha|a\rangle + \beta|b\rangle$, if measured in the $\{|a\rangle, |b\rangle\}$ basis, will produce $|a\rangle$ and $|b\rangle$ with probabilities α^2 and β^2 respectively.

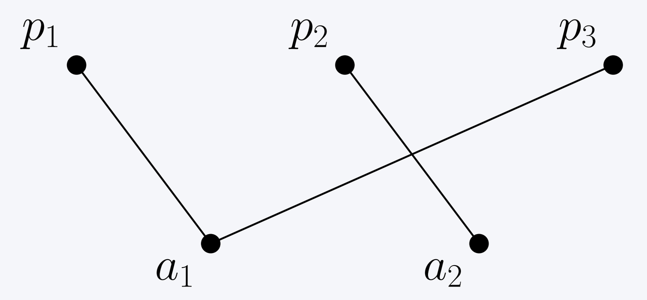
Entanglement: Given $|+\rangle$ and $|0\rangle$ we can write the *composite system*:

$$|+\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

We can *entangle* these states by applying a CNOT gate (acting on each binary string as if classical) to obtain $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. If one measures the first qubit, $|0\rangle$ is obtained with probability $\frac{1}{2}$. The state must then switch to $|00\rangle$ and you will measure the second qubit in the state $|0\rangle$. However, if you measure the second and not the first then you will obtain $|0\rangle$ with probability $\frac{1}{2}$. But how does the second qubit know if you have or have not measured the first?!?

What is this "IQP" computer?

IQP is implemented by entangling $|+\rangle$ states according to edges of *IQP graphs*:



This entangled state is then measured to obtain a classical bit string as output.

How can we test we have an IQP computer? [1]

How are you going to check you have a quantum computer?

Unlike classical computers, quantum computers can factor large numbers.

That's the most famous application. If it can do that I'll know.

You need a universal machine for that.

Fine! How about I send a hypothesis test.

A *Hypothesis Test* allows a user to check a device has the power of IQP by:

- Solving a problem that is hard for a classical computer but easy quantumly.
- Allowing a classical user a means to check the solution.

Factoring does this (given factors, multiply together to check) but is too hard for an IQP machine. Instead, we use the *bias* of the output distribution.

Bias (x, s) = "*probability the output, x, is orthogonal to s*"

I'll ask the device to implement an IQP graph depending on an s I know.

The bias is a function of s so I can check the outcome.

If the graph depends on s wouldn't a classical machine know s?

Then they can calculate the bias in the same way you did?

In quantum computing you can use some tricks to hide the graph!

What about experimental noise? [2]

Building a quantum computer will be hard since qubits are noisy.

A noisy quantum computer is still a quantum computer.

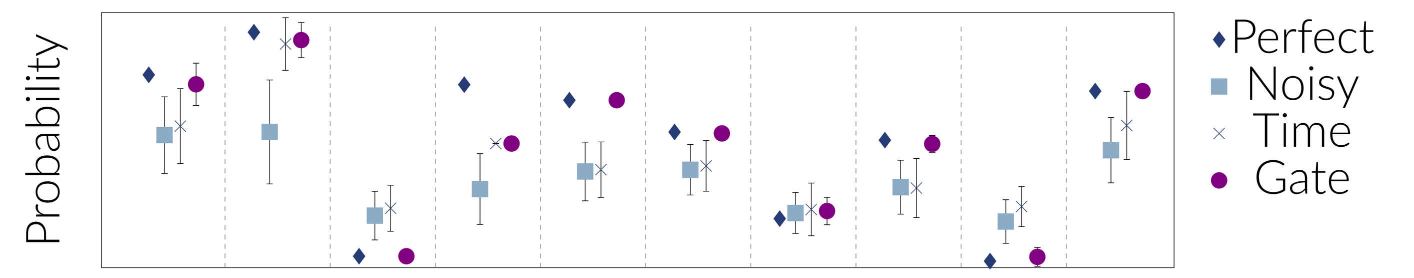
Actually if it is too noisy the output might just be totally random.

I could produce random numbers with a classical computer.

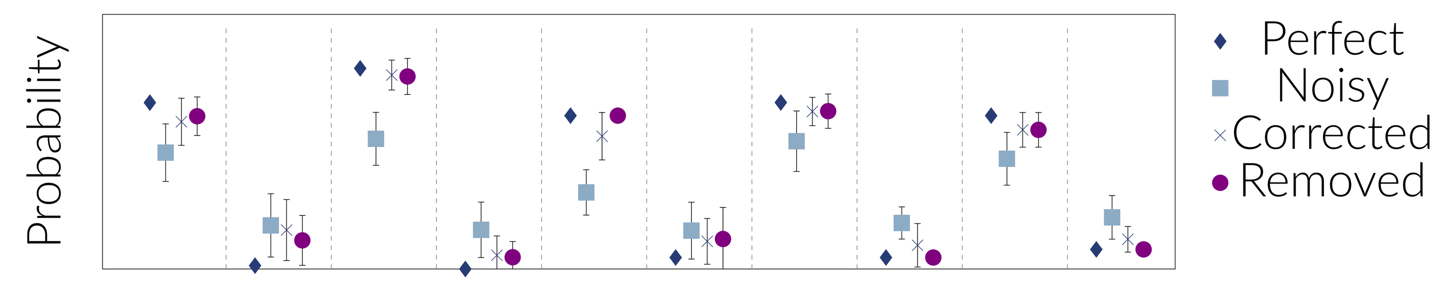
You're always so picky!!

Okay, let's numerically model the impact of different types of noise.

Only Gate Based Noise and Only Time Based Noise: We compare the impact of gate based noise (applying the wrong gate) and time based noise (decay of data over time). Notice that time based noise has the greatest impact.



Error Corrected Dephasing: Further simulations showed the greatest errors result from dephasing (errors due to the accuracy of measurement in some basis being better than others). We studied the impact that a simple error correction code would have on the noise. It would seem to be substantial.

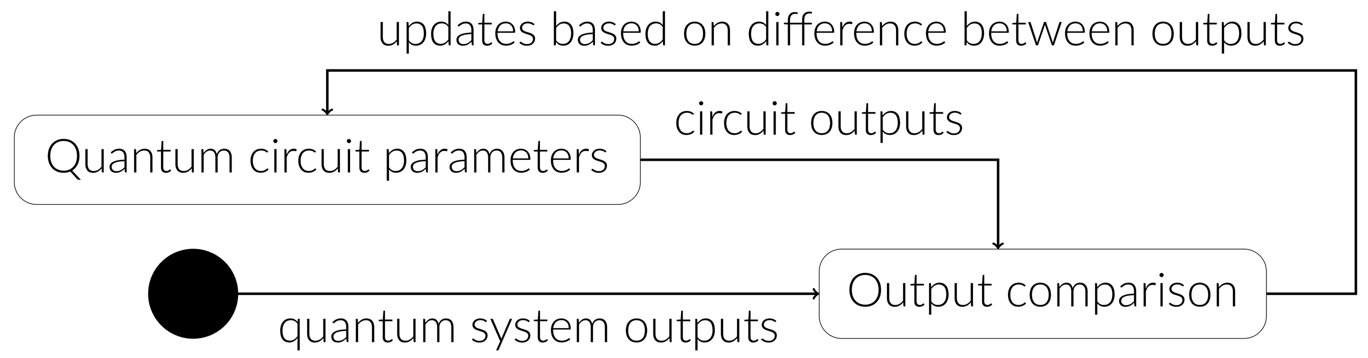


What can we do with these IQP devices? [3]

What a complicated paperweight.

Sarcasm is the lowest form of wit. Actually it's useful too!!

By reproducing the outputs of natural quantum systems, such as molecules or black holes, quantum computers will help in the development of drugs and in understanding fundamental physics.



'Learning' the correct IQP graph configuration to reproduce the statistics of our natural quantum system, as outlined above, is one exciting application.

Checkmate.

Okay, you've got me.

References

[1] Daniel Mills, Anna Pappa, Theodoros Kapourniotis, and Elham Kashefi. Information theoretically secure hypothesis test for temporally unstructured quantum computation. *arXiv preprint arXiv:1704.01998*, 2017.

[2] Iskren Vankov, Daniel Mills, Petros Wallden, and Elham Kashefi. Methods for classically simulating noisy networked quantum architectures. *arXiv preprint arXiv:1803.04167*, 2018.

[3] Brian Coyle, Daniel Mills, Vincent Danos, and Elham Kashefi. The born supremacy: Quantum advantage and training of an ising born machine. *Work in progress. See poster by the same name at this event*, 2019.

Many thanks to my sponsors for supporting this work:

EPSRC Engineering and Physical Sciences Research Council

THE UNIVERSITY of EDINBURGH informatics

EPSRC Centre for Doctoral Training in Pervasive Parallelism