Verification of Quantum Superiority

QuIVER 2018

Daniel Mills

26-29 October 2018

The University of Edinburgh

Content

Quantum Superiority

Superiority Hypothesis

The set of samples I have in my posetion were drawn from a distribution produced by a classical computer [1] [2]

[1] In a reasonable amount of time

[2] Disproving this null hypothesis would demonstrate quantum superiority [1]

A Recipe

Ingredients:

- A computational problem [3]
- A reason to believe there is a separation between the classical and quantum runtime
- A method of verifying the outcome

Cooking time: polynomial

Serves: you right extended Church-Turing thesis

[3] Not necessarily of practical interest

Factoring [2] as an Instance of our Recipe

- A computational problem:
    - Factoring

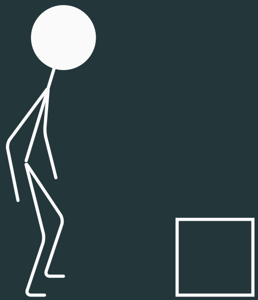
Factoring [2] as an Instance of our Recipe

- A computational problem:
  - Factoring
- A reason to believe there is a separation between the classical and quantum runtime
  - Well... we've tried our best for a while now

Factoring [2] as an Instance of our Recipe

- A computational problem:
  - Factoring
- A reason to believe there is a separation between the classical and quantum runtime
  - Well... we've tried our best for a while now
- A method of verifying the outcome
  - We can multiply the factors

Superiority by Factoring Soon Becomes Daunting [3]



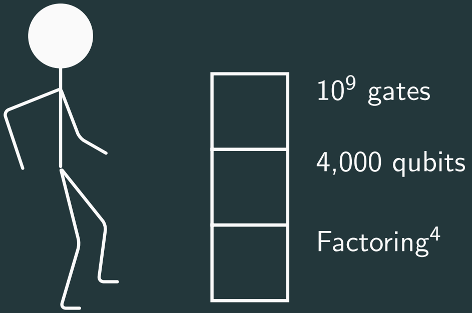
Factoring[4]

[4] Of a 2048 bit number, which is basically impossible for a classcal computer

Superiority by Factoring Soon Becomes Daunting [3]

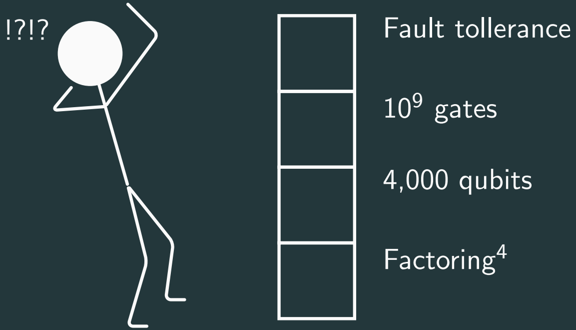
[4] Of a 2048 bit number, which is basically impossible for a classcal computer

Superiority by Factoring Soon Becomes Daunting [3]



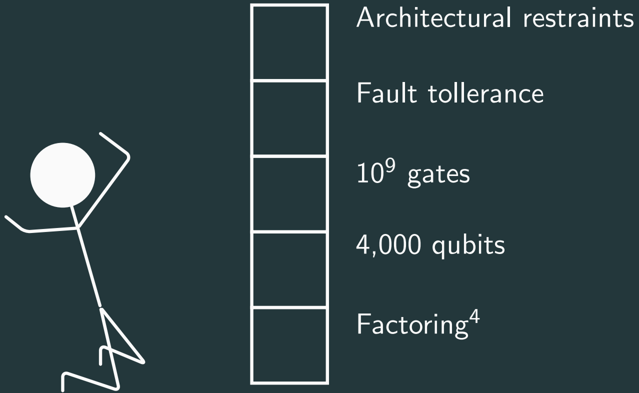
[4] Of a 2048 bit number, which is basically impossible for a classcal computer

Superiority by Factoring Soon Becomes Daunting [3]



[4] Of a 2048 bit number, which is basically impossible for a classcal computer

Superiority by Factoring Soon Becomes Daunting [3]



[4] Of a 2048 bit number, which is basically impossible for a classcal computer

A New Ingrediant

Ingredients:

- A computational problem [5]
- A reason to believe there is a separation between the classical and quantum runtime
- A method of verifying the outcome
- An implementation on a near-term device

[5] Not necessarily of practical interest

Simpler Quantum Computers

Linear optical network:

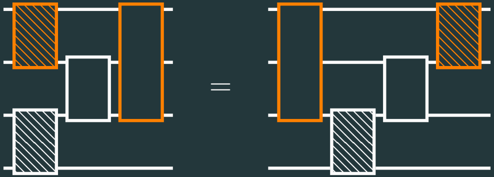
Photons are counted at the end

Boson Sampling Chalenges

- Randomised single photon source has inherently poor scaling
    - Scattershot boson sampling?
- Lossy systems
- Some way to go
    - Can implement ~ 5 photons, ~ 10 modes
    - Can simulate ~ 30 photons ... on a laptop [5]

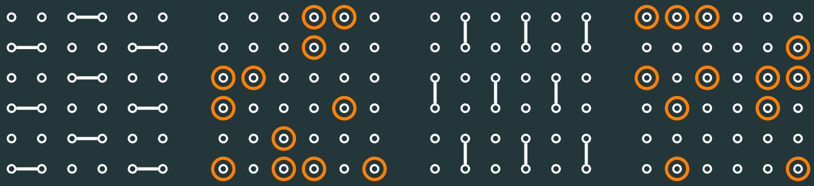
Instantaneous Quantum Polytime [6, 7]

Commuting gates:



Random Quantum Circuits [8]

Alternating entanglement patterns and random gates:



Hardness Results

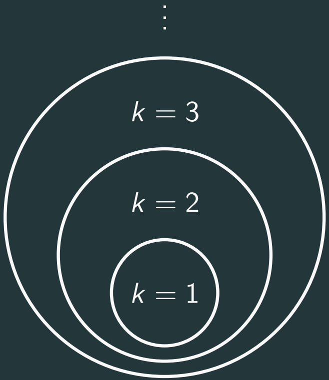
Polynomial Hierarchy

- $f(x) \in \text{NP} \implies f(x) = \vee_y g(x, y)$
- k^{th} level of PH has k alternating quantuifers
  - $f(x) = \vee_{y_1} \wedge_{y_2} \ldots \wedge_{y_k} g(x, y_1, \ldots, y_k)$
- It is conjectured k^{th} and $k+1^{th}$ level of PH are not equal
  - If it is then there is a colapse to k^{th} level - " it's the k^{th} level all the way down"

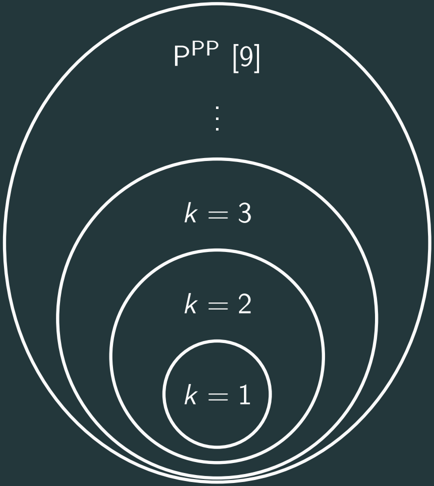
Post-Selection

- A computation takes input strings x and outputs strings y and z
- we condition on z and output y
- Allowing post selection on exponentially unlikely outcomes is very powerful

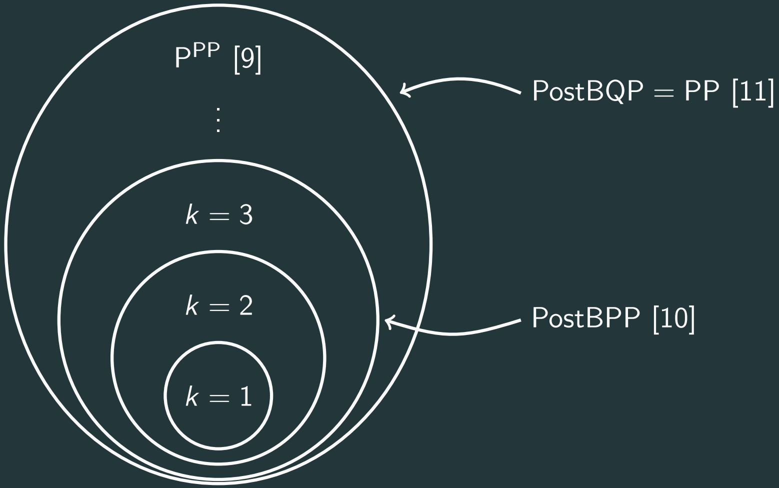
What is the Layout?



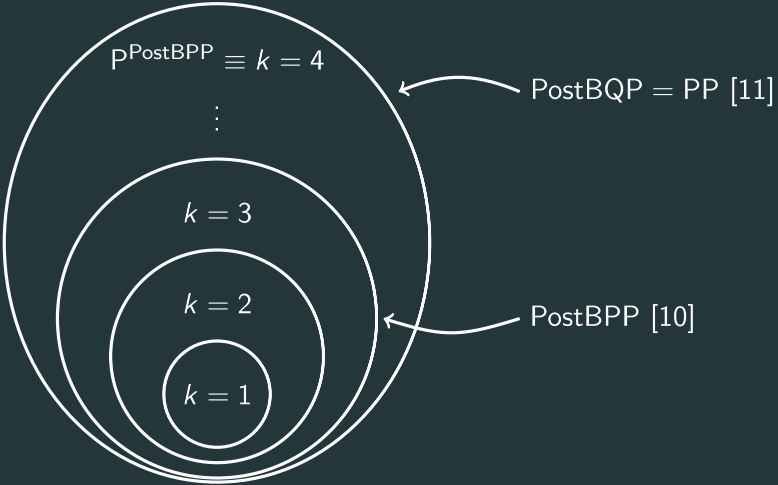
What is the Layout?



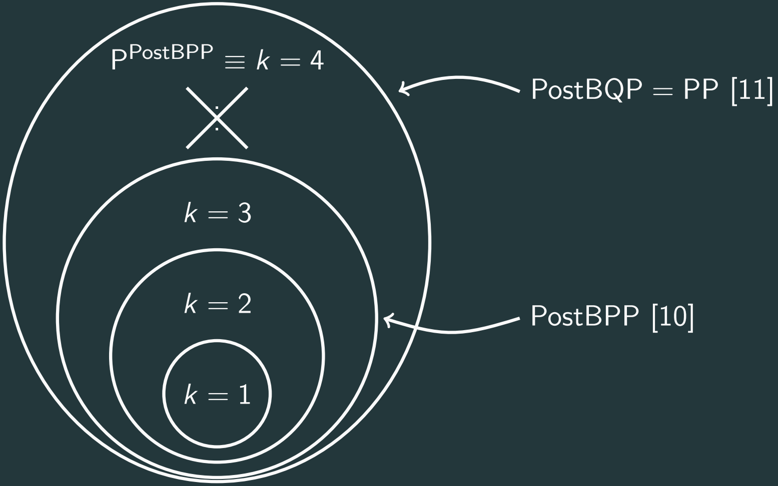
What is the Layout?



What if PostBQP = PostBPP**?**



What if PostBQP = PostBPP?



Problem with Complexity Theory

- Asymptotic complexity results tell us little about near term implementations!
  - We would prefer a more fine grained complexity complexity like "this computation takes time 2^n on n qubits" [12]

Problem with Complexity Theory

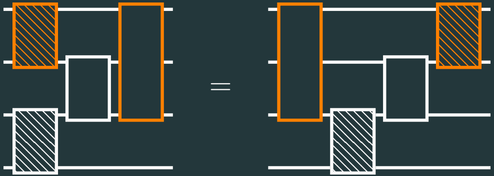
- Asymptotic complexity results tell us little about near term implementations!
  - We would prefer a more fine grained complexity complexity like "this computation takes time 2^n on n qubits" [12]
- Worst case results teach us nothing about which computation implements to use
  - We have some average case hardness results based on stronger conjectures

Problem with Complexity Theory

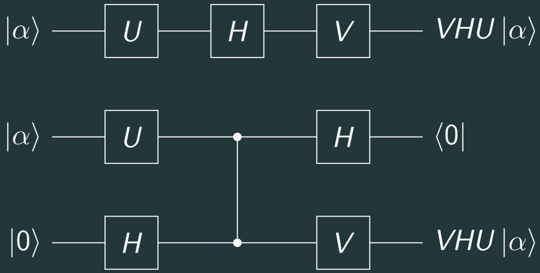
- Asymptotic complexity results tell us little about near term implementations!
    - We would prefer a more fine grained complexity complexity like "this computation takes time 2^n on n qubits" [12]
- Worst case results teach us nothing about which computation implements to use
    - We have some average case hardness results based on stronger conjectures
- $\mathrm{BPP} = \mathrm{BQP} \not\Rightarrow \mathrm{PostBQP} = \mathrm{PostBPP}$

Instantaneous Quantum Polytime [6, 7]

Commuting gates:



IQP Superiority [13]



Multiplicative vs Additive Error

$$(1-\epsilon)\, q\left(0^n\right) \leq p\left(0^n\right) \leq (1+\epsilon)\, q\left(0^n\right)$$

vs

$$\sum_z \left|p\left(z\right) - q\left(z\right)\right| \leq \epsilon$$

IQP Additive Superiority [14]

- For two classes of problems, a classical sampler, acurate up to good additive error in the worst case, must be acurate in multiplicative error in the average case.

[6] One advantage if IQP is that it is simpler to show anticoncentration results.
[7] Analagouse to [4] but can prove anticoncentration

IQP Additive Superiority [14]

- For two classes of problems, a classical sampler, acurate up to good additive error in the worst case, must be acurate in multiplicative error in the average case.
- Can use Stockmeyer to estimate individual output probabilities up to small multiplicatie error.
  - True because of anticoncentration [6]

[6] One advantage if IQP is that it is simpler to show anticoncentration results.
[7] Analagouse to [4] but can prove anticoncentration

IQP Additive Superiority [14]

- For two classes of problems, a classical sampler, acurate up to good additive error in the worst case, must be acurate in multiplicative error in the average case.
- Can use Stockmeyer to estimate individual output probabilities up to small multiplicatie error.
    - True because of anticoncentration [6]
- This gives an algorithm for computing multiplicative approximation to large fraction of class.

[6] One advantage if IQP is that it is simpler to show anticoncentration results.
[7] Analagouse to [4] but can prove anticoncentration

IQP Additive Superiority [14]

- For two classes of problems, a classical sampler, acurate up to good additive error in the worst case, must be acurate in multiplicative error in the average case.
- Can use Stockmeyer to estimate individual output probabilities up to small multiplicatie error.
  - True because of anticoncentration [6]
- This gives an algorithm for computing multiplicative approximation to large fraction of class.
- This causes a collapse of PH , assuming some conjectures about the two classes. [7]

[6] One advantage if IQP is that it is simpler to show anticoncentration results.
[7] Analagouse to [4] but can prove anticoncentration

IQP Superiority

- Arbitrarily small constant noise on each qubit at the end of IQP circuit makes [15] easy up to additive error.

Random Circuit Superiority: 3 Main Arguments

1. No known simulation using reasonable amount of memory
2. IQP-esque complexity results giving asymptotic hardness
3. Circuits have properties we expect of hard distributions

Intuative Initial Arguments

$$
\begin{aligned}
\text{Close to Porter-Thomas} &\implies \text{Behaves like chaotic system} \\
&\implies \text{Small perturbation} = \text{large divergence} \\
&\implies \text{Must store full state} \\
&\implies \text{Hard to simulate}
\end{aligned}
$$

Verification

Verification

Options:

1. Direct certification
2. Classically simulate small instances
3. Statistical test of some properties we expect.

Verification Using HOG [16]

Problem
HOG - Heavey Output Generation

Given as input a random quantum circuit C, generate output strings $x_1, ..., x_k$ at least a $\frac{2}{3}$ fraction of which have greater than median probability in C's output distribution.

Verification Using HOG [16]

Problem
HOG - Heavey Output Generation

Given as input a random quantum circuit C, generate output strings $x_1, ..., x_k$ at least a $\frac{2}{3}$ fraction of which have greater than median probability in C's output distribution.

Conjecture
QUATH - QUantum THreshold assumption

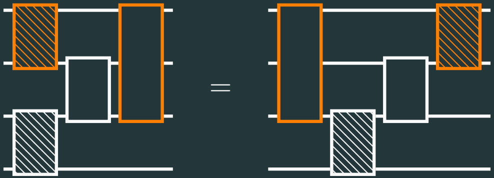
There is no polynomial-time classical algorithm that takes as input a description of a random quantum circuit C, and which guesses whether $|\langle 0^n| C |0^n\rangle|^2$ is greater than or less than the median of all 2^n of the $|\langle 0^n| C |x\rangle|^2$

Verification of Random Circuits Using Entropy Benchmarking

- Measures closeness of output to perfect circuit
- Takes exponential time classically
  - Maybe that's okay?

Instantaneous Quantum Polytime Machine [6]

Commuting gates:



In particular:

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

where $q \in \{0,1\}^{n_p}$, $\theta \in [0, 2\pi]$.

Instantaneous Quantum Polytime Machine [6]

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

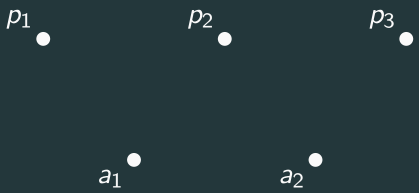
An IQP program may consist of many of these gates, and so many different q. Hence we may represent the whole computation by, for example:

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

where, in this case, we have two gates defined by $q = (101)$ and $q = (010)$.

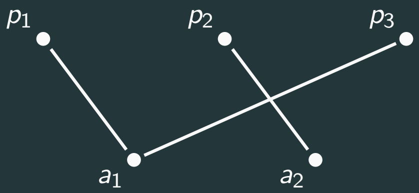
The input is $|0^{n_p}\rangle$ and the output is the resulting state measured in the computational basis.

IQP in MBQC



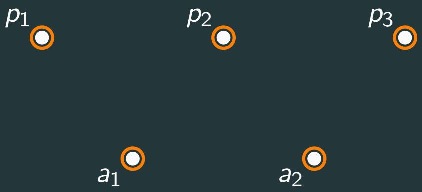
$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

IQP in MBQC



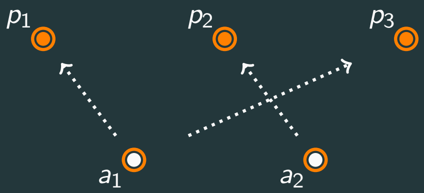
$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

IQP in MBQC



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

IQP in MBQC



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

IQP in MBQC

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

Bridge and Break [17]

$cZ_{1,2}cZ_{2,3}\,|0/1\rangle \otimes |\phi\rangle$

$|0\rangle$ or $|1\rangle$

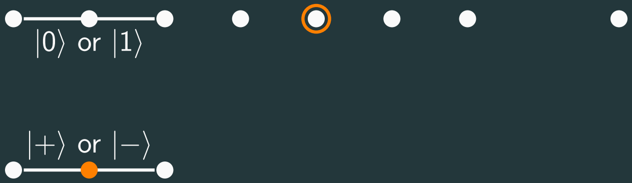
Bridge and Break [17]

$$Z_1^{0/1} Z_3^{0/1} \left|0/1\right\rangle \otimes \left|\phi\right\rangle$$

$|0\rangle$ or $|1\rangle$

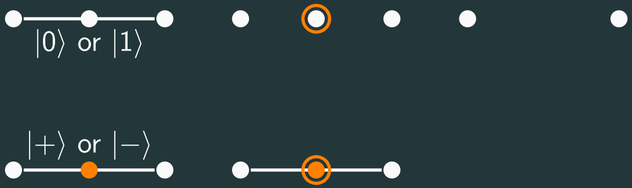
Bridge and Break [17]

Bridge and Break [17]



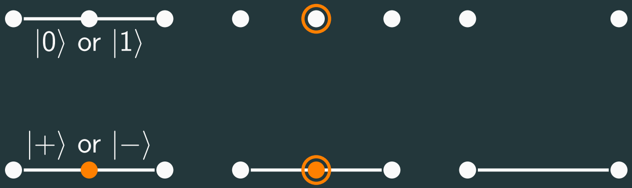
$cZ_{1,2}cZ_{2,3}\,|+/-\rangle \otimes |\phi\rangle$

Bridge and Break [17]



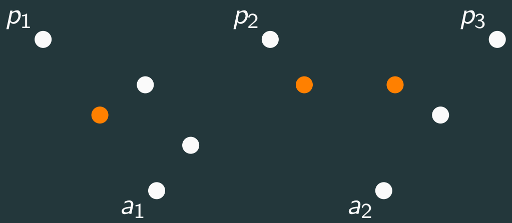
$$cZ_{1,2}cZ_{2,3}\,|+/-\rangle \otimes |\phi\rangle$$

Bridge and Break [17]

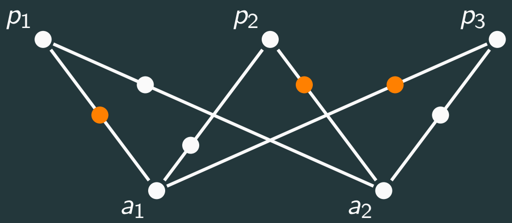


$$S_1^{f(+/-,s)} S_3^{f(+/-,s)} Z_{1,3} |\phi\rangle$$

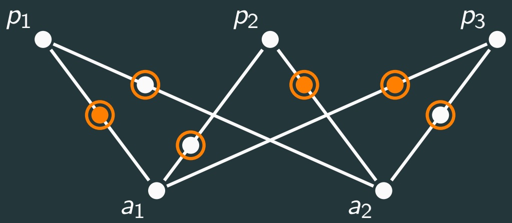
IQP By Bridge and Break



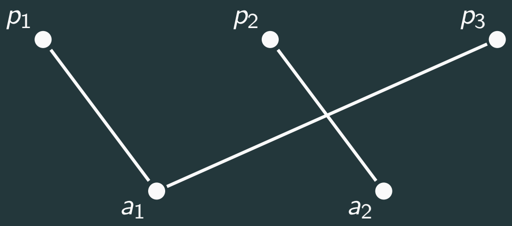
IQP By Bridge and Break



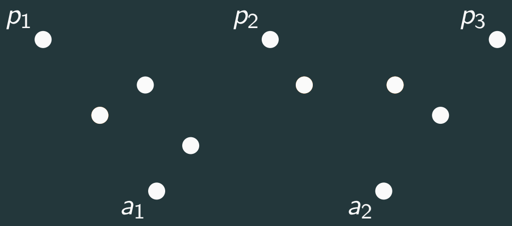
IQP By Bridge and Break



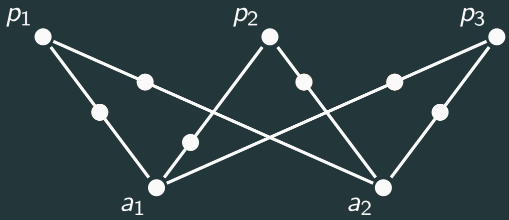
IQP By Bridge and Break



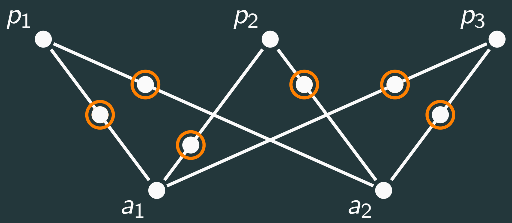
IQP By Bridge and Break



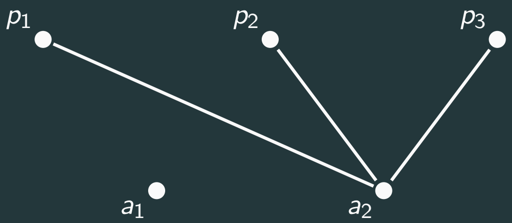
IQP By Bridge and Break



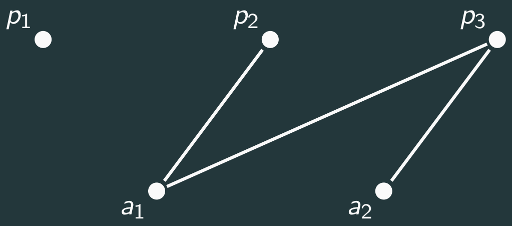
IQP By Bridge and Break



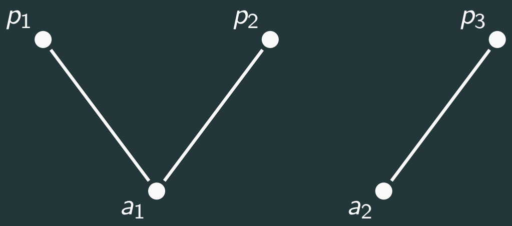
IQP By Bridge and Break



IQP By Bridge and Break



IQP By Bridge and Break



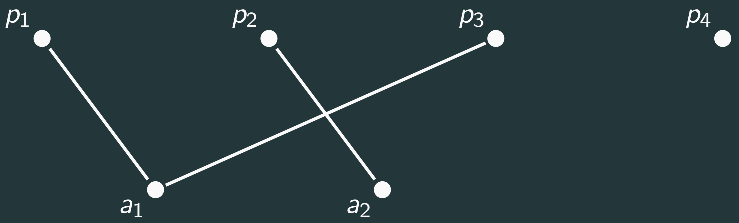
Hypothesis Test

Bias of a random variable, $X \in \{0,1\}^{n_p}$, in a direction $s \in \{0,1\}^{n_p}$.

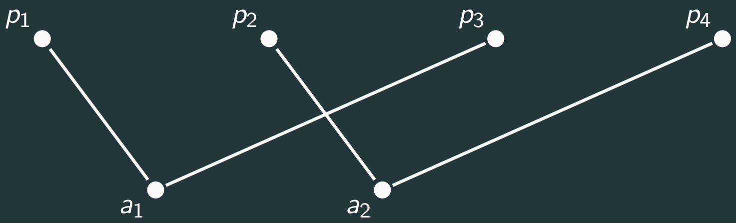
$$\mathbb{P}\left(X \cdot s^T = 0\right) = \mathit{Bias}\left(X, s\right)$$

Can be easily calculated, for some special IQP computations (depending on s), if one knows s [6].

Hypothesis Test

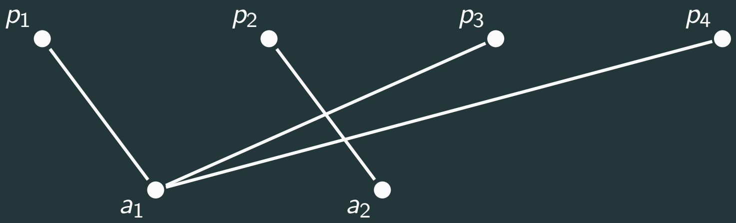


Hypothesis Test



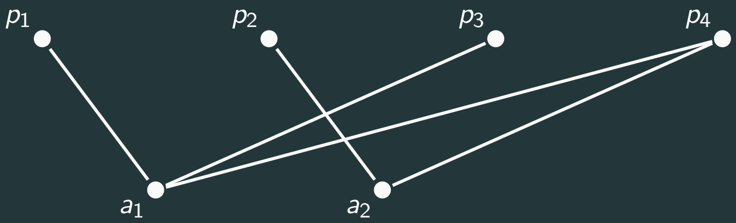
$$Bias\,(X, s_1) = p$$

Hypothesis Test



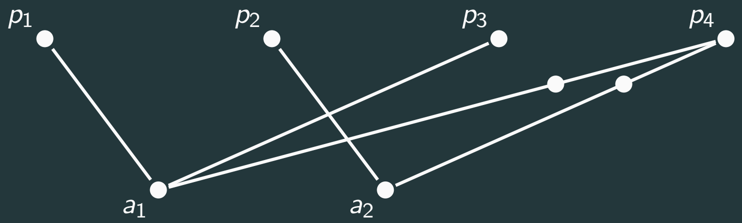
$$Bias\left(X, s_2\right) = p$$

Hypothesis Test

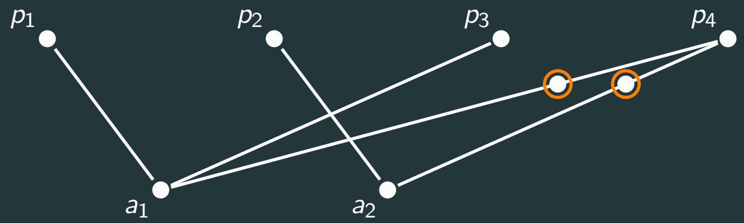


$$Bias\,(X, s_3) = p$$

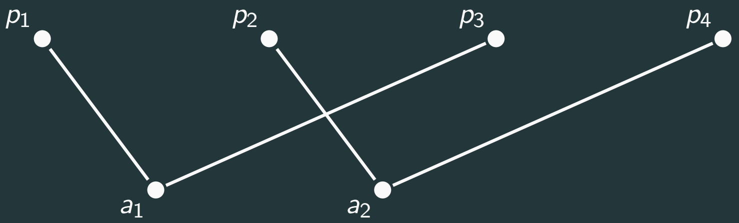
Hypothesis Test



Hypothesis Test



Hypothesis Test



The Hypothesis Test Outline

Three conditions for a successful hypothesis test:

The Hypothesis Test Outline

Three conditions for a successful hypothesis test:

- The Server must complete a hard computations
  - Computation bias calculation is hard

The Hypothesis Test Outline

Three conditions for a successful hypothesis test:

- The Server must complete a hard computations
  - Computation bias calculation is hard
- The Client knows a secret property allowing them to check the outcome
  - The Client knows the direction s

The Hypothesis Test Outline

Three conditions for a successful hypothesis test:

- The Server must complete a hard computations
    - Computation bias calculation is hard
- The Client knows a secret property allowing them to check the outcome
    - The Client knows the direction s
- The Server hides the secret property
    - Using blind IQP

Conclusion

Conclusion

- VERIFICATION OF SOME PROPERTY (BUT NOT THE WHOLE THING) IS INTERESTING!

References

[1] John Preskill. Quantum computing and the entanglement frontier. *arXiv preprint arXiv:1203.5813*, 2012.

[2] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, Nov 1994. doi:10.1109/SFCS.1994.365700.

[3] Thomas Häner, Martin Roetteler, and Krysta M Svore. Factoring using 2n+ 2 qubits with toffoli based modular multiplication. *arXiv preprint arXiv:1611.07995*, 2016. URL `https://arxiv.org/abs/1611.07995`.

[4] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing*, STOC '11, pages 333–342, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0691-1. doi:10.1145/1993636.1993682. URL `http://doi.acm.org/10.1145/1993636.1993682`.

[5] Alex Neville, Chris Sparrow, Raphaël Clifford, Eric Johnston, Patrick M Birchall, Ashley Montanaro, and Anthony Laing. Classical boson sampling algorithms with superior performance to near-term experiments. *Nature Physics*, 13 (12):1153, 2017. doi:10.1038/nphys4270.

[6] Dan Shepherd and Michael J Bremner. Temporally unstructured quantum computation. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 2009. ISSN 1364-5021. doi:10.1098/rspa.2008.0443. URL `http://rspa.royalsocietypublishing.org/content/early/2009/02/18/rspa.2008.0443`.

[7] Michael J. Bremner, Richard Jozsa, and Dan J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 467(2126):459–472, 2011. ISSN 1364-5021. doi:10.1098/rspa.2010.0301. URL `http://rspa.royalsocietypublishing.org/content/467/2126/459`.

[8] Sergio Boixo, Sergei V Isakov, Vadim N Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, Michael J Bremner, John M Martinis, and Hartmut Neven. Characterizing quantum supremacy in near-term devices. *Nature Physics*, 14 (6):595, 2018. doi:10.1038/s41567-018-0124-x.

[9] S. Toda. Pp is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991. doi:10.1137/0220053. URL `https://doi.org/10.1137/0220053`.

[10] Yenjo Han, Lane A. Hemaspaandra, and Thomas Thierauf. Threshold computation and cryptographic security. In K. W. Ng, P. Raghavan, N. V. Balasubramanian, and F. Y. L. Chin, editors, *Algorithms and Computation*, pages 230–239, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg. ISBN 978-3-540-48233-8.

[11] Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 461, pages 3473–3482. The Royal Society, 2005. URL `https://arxiv.org/abs/quant-ph/0412187`.

[12] Alexander M Dalzell, Aram W Harrow, Dax Enshan Koh, and Rolando L La Placa. How many qubits are needed for quantum computational supremacy? *arXiv preprint arXiv:1805.05224*, 2018. URL `https://arxiv.org/abs/1805.05224`.

[13] Michael J. Bremner, Richard Jozsa, and Dan J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 467(2126):459–472, 2011. ISSN 1364-5021. doi:10.1098/rspa.2010.0301. URL `http://rspa.royalsocietypublishing.org/content/467/2126/459`.

[14] Michael J. Bremner, Ashley Montanaro, and Dan J. Shepherd. Average-case complexity versus approximate simulation of commuting quantum computations. *Phys. Rev. Lett.*, 117:080501, Aug 2016. doi:10.1103/PhysRevLett.117.080501. URL `https://link.aps.org/doi/10.1103/PhysRevLett.117.080501`.

[15] Michael J. Bremner, Ashley Montanaro, and Dan J. Shepherd. Achieving quantum supremacy with sparse and noisy commuting quantum computations. *Quantum*, 1:8, April 2017. ISSN 2521-327X. doi:10.22331/q-2017-04-25-8. URL `https://doi.org/10.22331/q-2017-04-25-8`.

[16] Scott Aaronson and Lijie Chen. Complexity-theoretic foundations of quantum supremacy experiments. *arXiv preprint arXiv:1612.05903*, 2016. URL `https://arxiv.org/abs/1612.05903`.

[17] Joseph F. Fitzsimons and Elham Kashefi. Unconditionally verifiable blind quantum computation. *Phys. Rev. A*, 96: 012303, Jul 2017. doi:10.1103/PhysRevA.96.012303. URL https://link.aps.org/doi/10.1103/PhysRevA.96.012303.