The complexity of quantum sampling problems

Michael Bremner
with A. Montanaro, D. Shepherd, R. Mann, R. Jozsa, A. Lund, T. Ralph, S. Boixo, S. Isakov, V. Smelyanskiy, R. Babbush, M. Smelyanskiy, N. Ding, Z. Jiang, J. Martinis, H. Neven, R. Mann

Come to Sydney for

TQC 2018

(13th Conference on the Theory of Quantum Computation, Communication and Cryptography)

cute but dangerous animals
Source: http://en.wikipedia.org/wiki/Drop_bear

QSML 2018

(1st International Workshop on Quantum Software and Machine Learning)

amazing architecture

central location

Important dates

Submission deadline:	March 20
Talk notification:	May 10
Late poster submission:	June 8
TQC 2018:	July 16-18
QS workshop:	July 19-20

Location

University of Technology Sydney, Building 11

UTS:QSI
CENTRE FOR QUANTUM SOFTWARE AND INFORMATION

Committees

PC chair: Stacey Jeffrey
(rest of PC to be announced)

Local org.: Marco Tomamichel (chair TQC)
Christopher Ferrie (chair QMLW)
Min-Hsiu Hsieh (co-chair)
Michael Bremner
Runyao Duan

TQC has two tracks: Conference (talk + proceedings) and Workshop (talk only)

For more, visit us at **www.tqc2018.org**

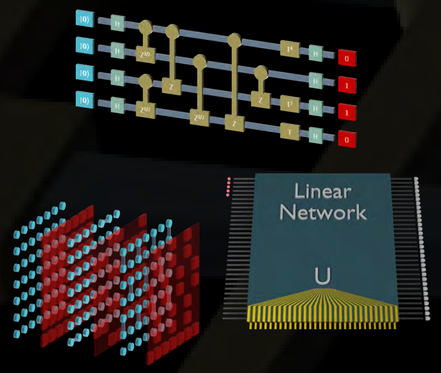
UTS:QSI

CENTRE FOR QUANTUM SOFTWARE AND INFORMATION

PhD and postdoc positions available for 2018!

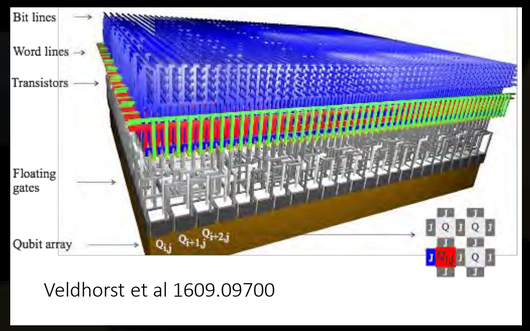
Keep your eyes on qsi.uts.edu.au and @uts_qsi on twitter!

A potential quantum (near) future



Intermediate quantum computing regime:

- Error mitigation
- Testable advantage
- Approximate optimizers
- Quantum simulators



Veldhorst et al 1609.09700

50 qubits | 1,000 | 10,000 | 100,000…

99.7% fidelity

FT qubit

Classical/quantum frontier

<12 months (Google, IBM)

Unambiguous quantum computational supremacy and commercially relevant applications , 2 – 10 years

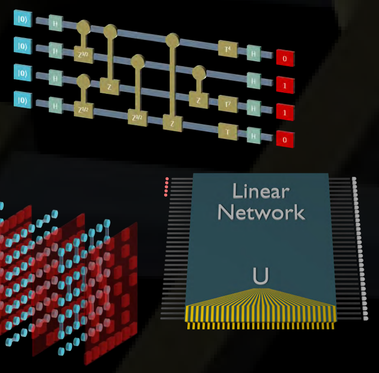
99.99% fidelity

99.999% fidelity

10+ years

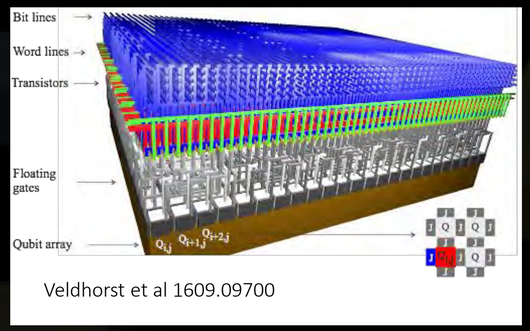
Universal quantum computing…

A potential quantum (near) future



Intermediate quantum computing regime:

- Error mitigation
- Testable advantage
- Approximate optimizers
- Quantum simulators



Veldhorst et al 1609.09700

50 qubits | 1,000 | 10,000 | 100,000…

99.7% fidelity

FT qubit

Classical/quantum frontier

<12 months (Google, IBM)

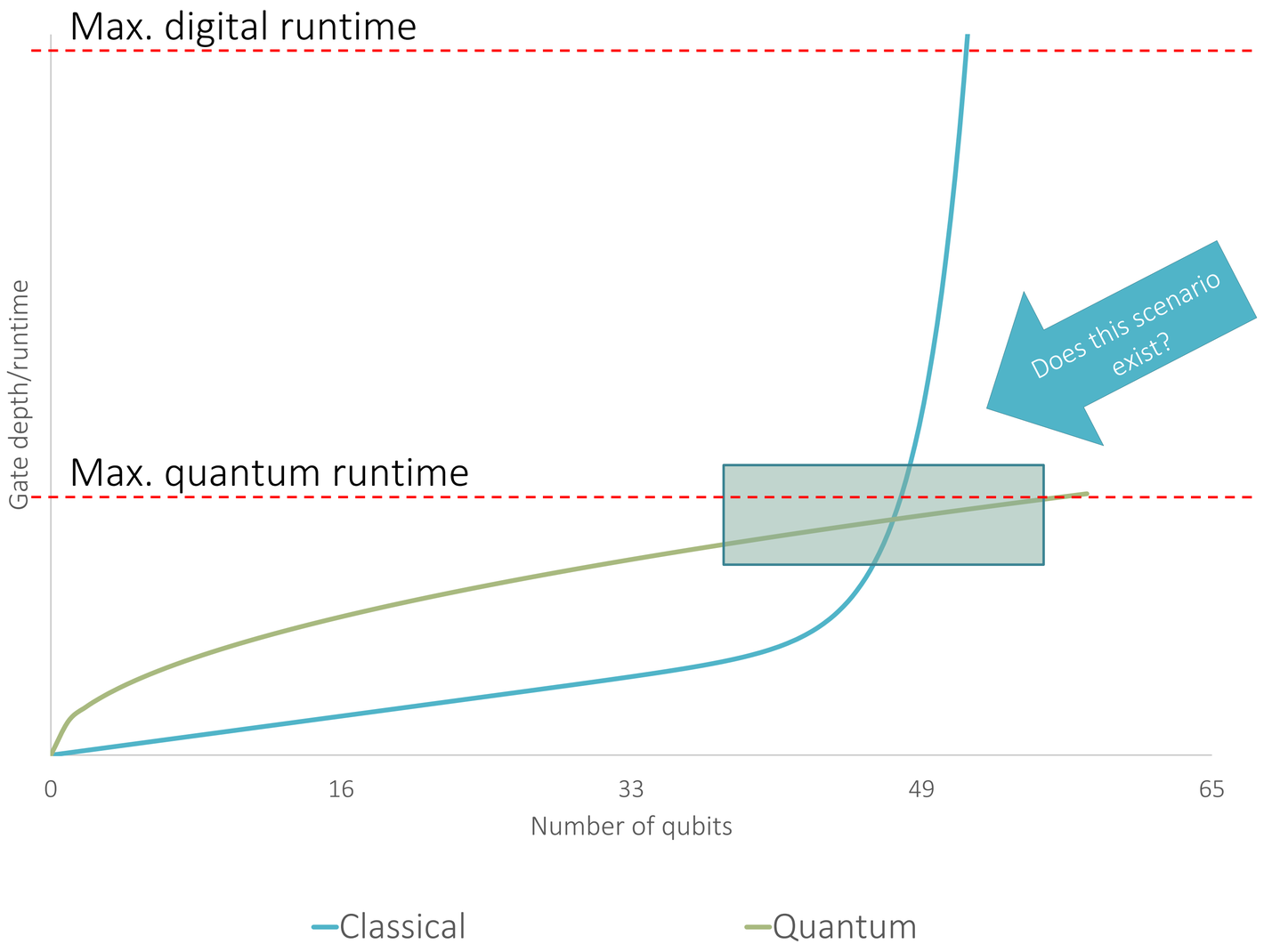
Unambiguous quantum computational supremacy and commercially relevant applications , 2 – 10 years

99.99% fidelity

99.999% fidelity

10+ years

Universal quantum computing…



*Nothing on this plot is to scale!

Beyond classical computing (AKA quantum computational supremacy)

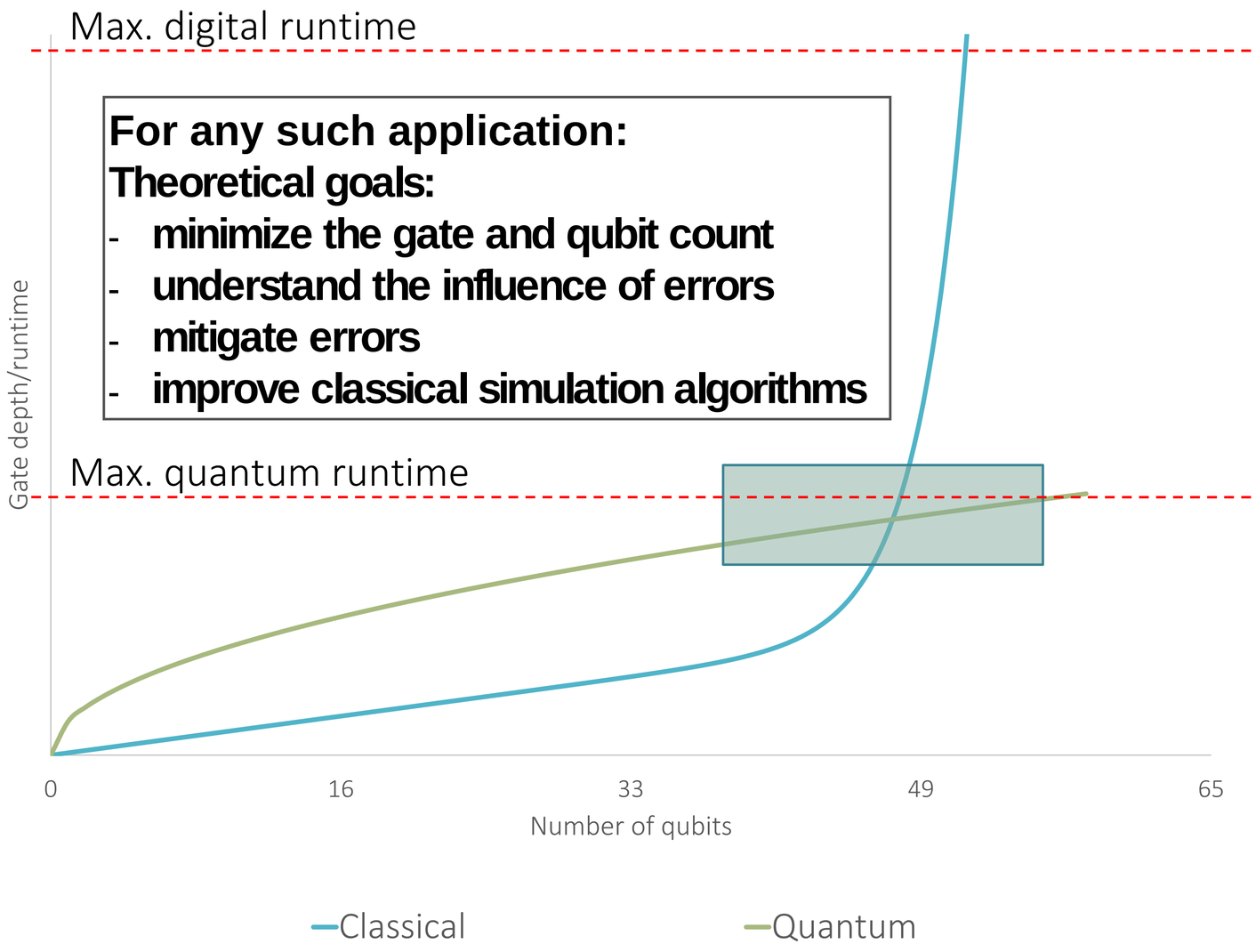
Aim: Perform a quantum computation that cannot be performed classically in any reasonable amount of time.

Key issues:

- Are quantum computers more powerful than classical computers?

- For which computations do the classical and quantum runtimes diverge?

- Can we achieve quantum computational supremacy without fault tolerance?



*Nothing on this plot is to scale!

Beyond classical computing (AKA quantum computational supremacy)

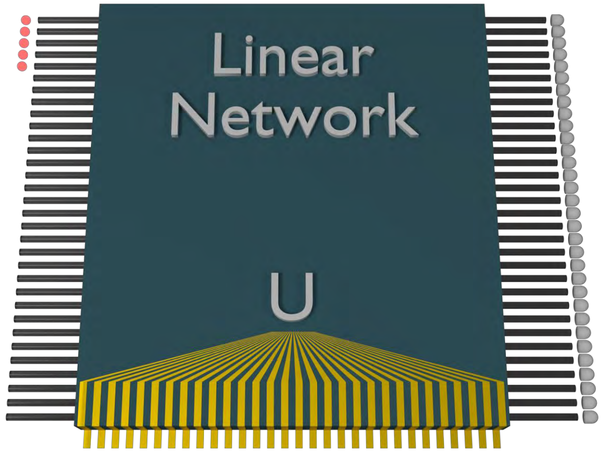
Aim: Perform a quantum computation that cannot be performed classically in any reasonable amount of time.

Key issues:

- Are quantum computers more powerful than classical computers?

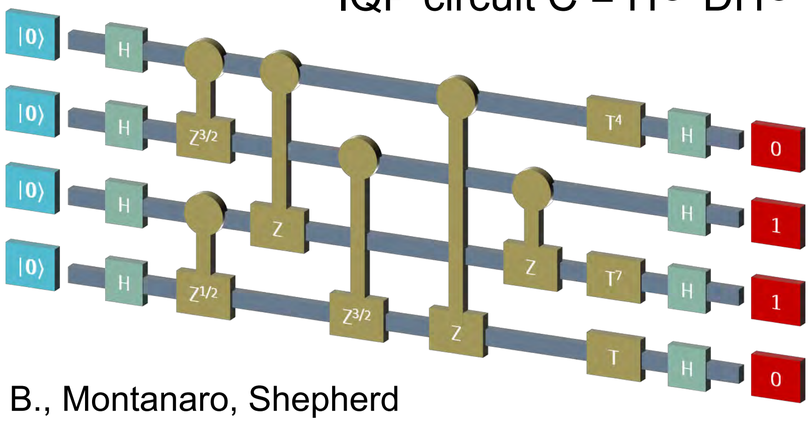
- For which computations do the classical and quantum runtimes diverge?

- Can we achieve quantum computational supremacy without fault tolerance?



A&A STOC ’11, arXiv:1011.3245

IQP circuit $C = H^{\otimes n} D H^{\otimes n}$



B., Montanaro, Shepherd
Phys. Rev. Lett. 117, 080501 (2016),
arXiv:1504.07999

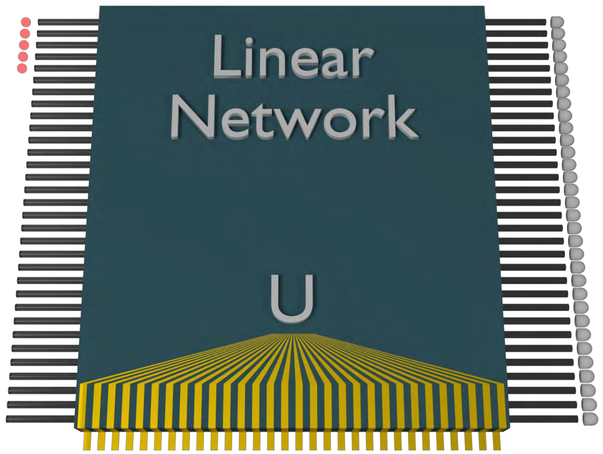
Random circuit sampling

Goal: output samples, x, with probability P(x) defined by a random circuit.

Idea: bound the complexity of sampling via studying the properties of P(x).

Hope: If P(x) is “complex” enough then classical computers can only ever simulate sampling by computing P(x).

Intuition: Random circuits quickly develop long-range entanglement, making them among the hardest to simulate accurately for known classical algorithms.

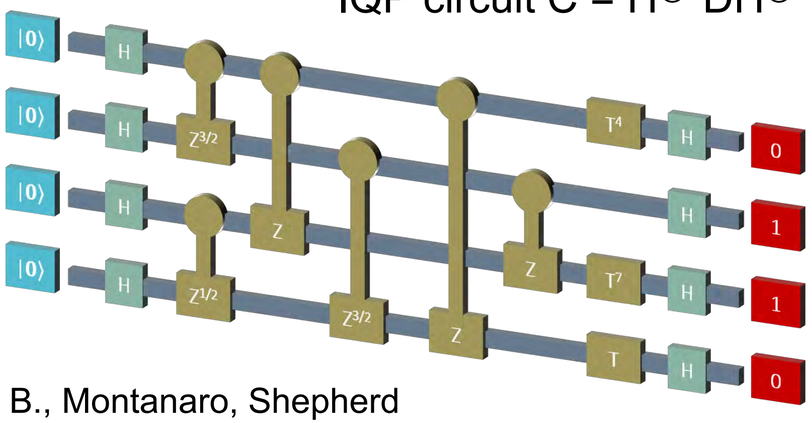


A&A STOC ’11, arXiv:1011.3245

Aaronson and Arkhipov’s **Boson Sampling established a potential advantage over classical computing for sampling random linear optical networks.**

Importantly, the advantage holds for approximate sampling, ruling out classical algorithms outputting samples from R(x) such that $\|P-R\|_1 \leq \varepsilon$ *assuming 2, open, conjectures.*

IQP circuit $C = H^{\otimes n} D H^{\otimes n}$



B., Montanaro, Shepherd
Phys. Rev. Lett. 117, 080501 (2016),
arXiv:1504.07999

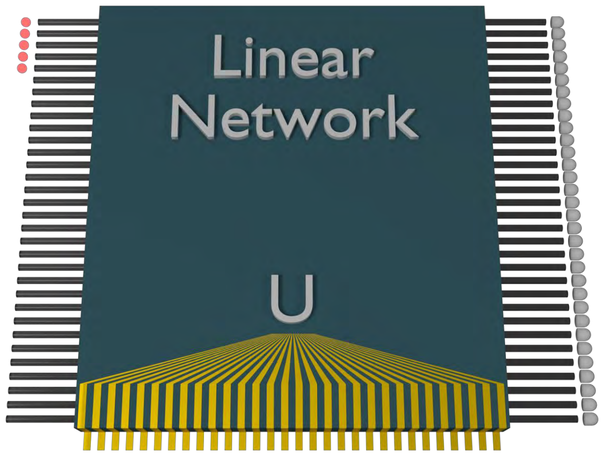
Random circuit sampling

Goal: output samples, x, with probability P(x) defined by a random circuit.

Idea: bound the complexity of sampling via studying the properties of P(x).

Hope: If P(x) is “complex” enough then **classical computers can only ever simulate sampling by computing P(x).**

Intuition: Random circuits quickly develop long-range entanglement, making them among the hardest to simulate accurately for known classical algorithms.



A&A STOC ’11, arXiv:1011.3245

Aaronson and Arkhipov’s Boson Sampling established a potential advantage over classical computing for sampling random linear optical networks.

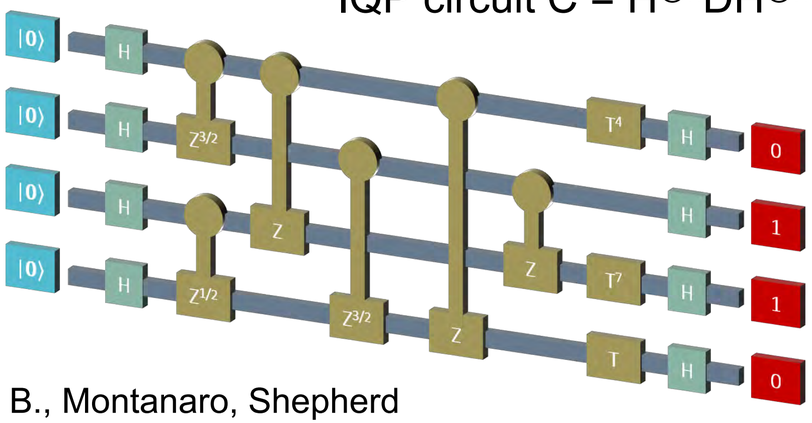
Importantly, the advantage holds for approximate sampling, ruling out classical algorithms outputting samples from R(x) such that $||P-R||_1 \leq \varepsilon$ *assuming 2, open, conjectures.*

IQP Sampling “improves” on Boson **Sampling by proving the equivalent of** the “Permanent anti**-concentration** conjecture”.

It is defined in the quantum circuit model, and yields very low-depth circuits. It also allows the usual machinery of error-correction to apply.

This model is also easily generalized e.g. Boixo et al arXiv:1608.00263.

IQP circuit $C = H^{\otimes n} D H^{\otimes n}$



B., Montanaro, Shepherd
Phys. Rev. Lett. 117, 080501 (2016),
arXiv:1504.07999

Random circuit sampling

Goal: output samples, x, with probability P(x) defined by a random circuit.

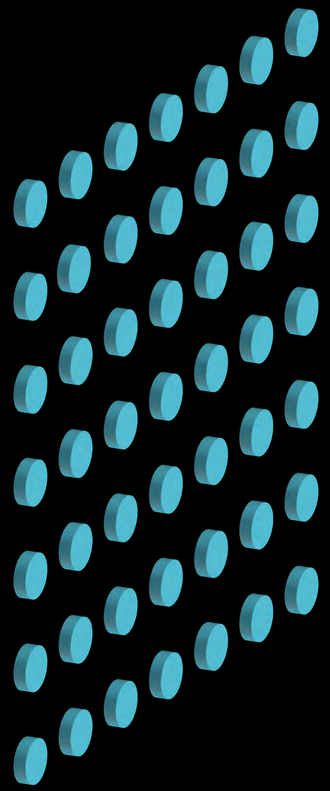
Idea: bound the complexity of sampling via studying the properties of P(x).

Hope: If P(x) is “complex” enough then **classical computers can only ever simulate sampling by computing P(x).**

Intuition: Random circuits quickly develop long-range entanglement, making them among the hardest to simulate accurately for known classical algorithms.

The Google proposal

Supremacy might be achieved with 2d nearest neighbour Xmon superconducting qubit architecture on a 7×7 lattice.

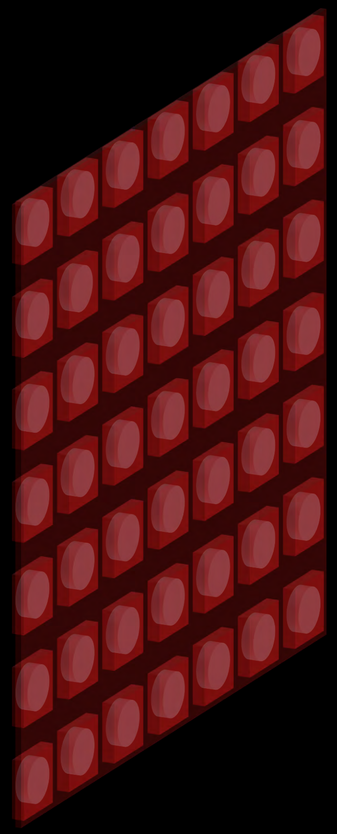


7×7 array of qubits

Boixo et al arXiv:1608.00263, QIP ‘17

The Google proposal

Supremacy might be achieved with 2d nearest neighbour Xmon superconducting qubit architecture on a 7×7 lattice.

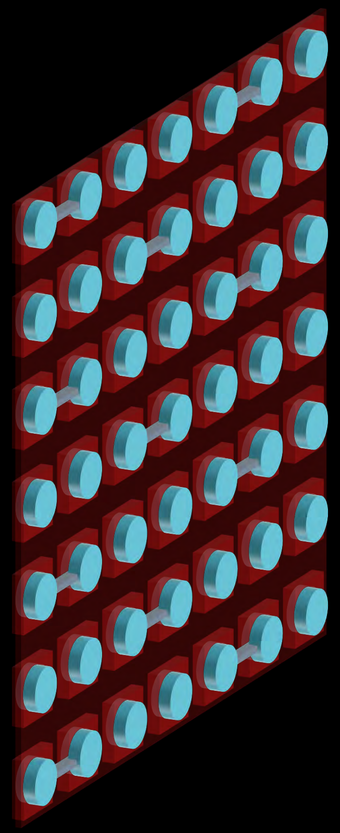


Hadamard gates to create a superposition

Boixo et al arXiv:1608.00263, QIP ‘17

The Google proposal

Supremacy might be achieved with 2d nearest neighbour Xmon superconducting qubit architecture on a 7×7 lattice.



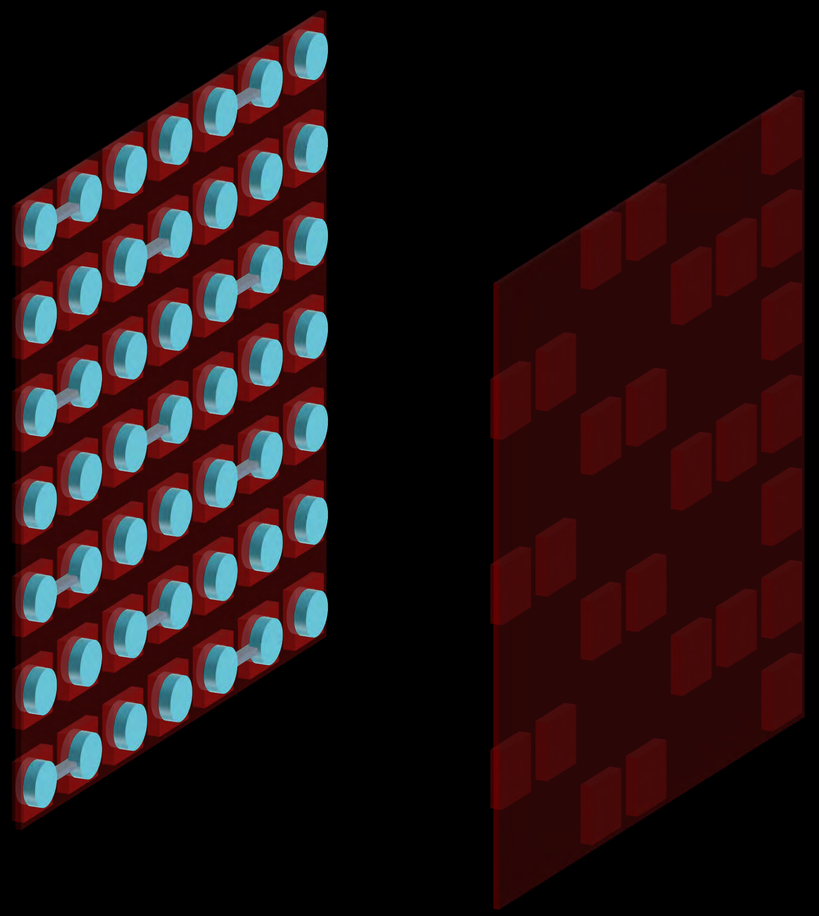
CZ gates to entangle neighbouring qubits

7×7 array of qubits

Boixo et al arXiv:1608.00263, QIP ‘17

The Google proposal

Supremacy might be achieved with 2d nearest neighbour Xmon superconducting qubit architecture on a 7×7 lattice.

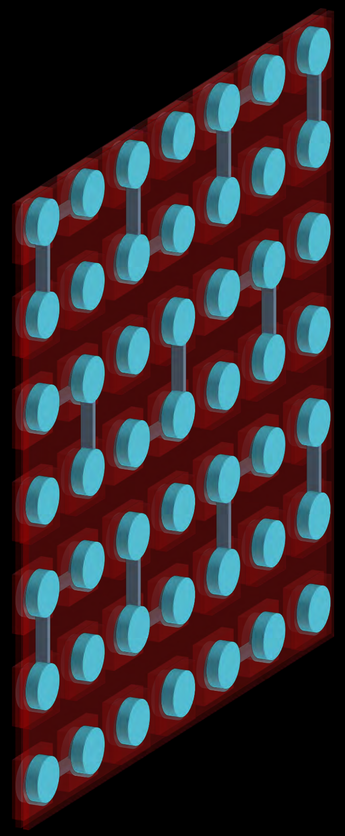


T, $X^{1/2}$, $Y^{1/2}$ gates chosen at random

Boixo et al arXiv:1608.00263, QIP ‘17

The Google proposal

Supremacy might be achieved with 2d nearest neighbour Xmon superconducting qubit architecture on a 7×7 lattice.

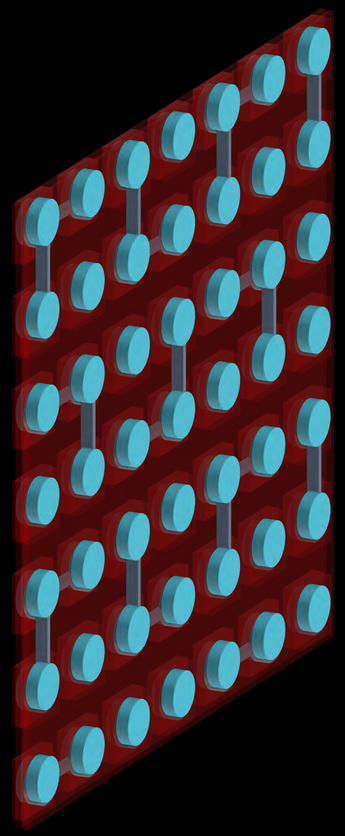


CZ gates to entangle more neighbouring qubits

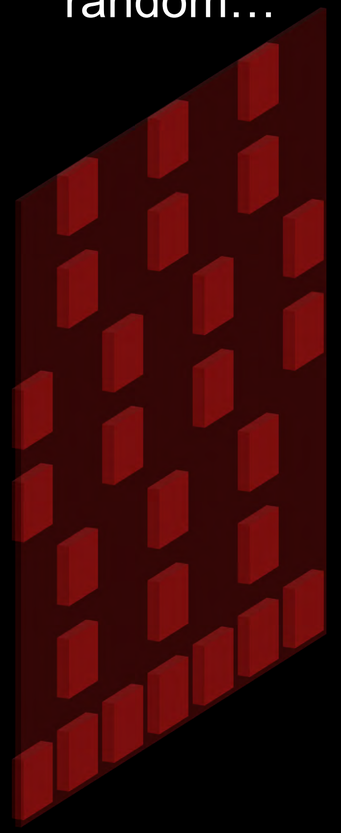
Boixo et al arXiv:1608.00263, QIP ‘17

The Google proposal

Supremacy might be achieved with 2d nearest neighbour Xmon superconducting qubit architecture on a 7×7 lattice.

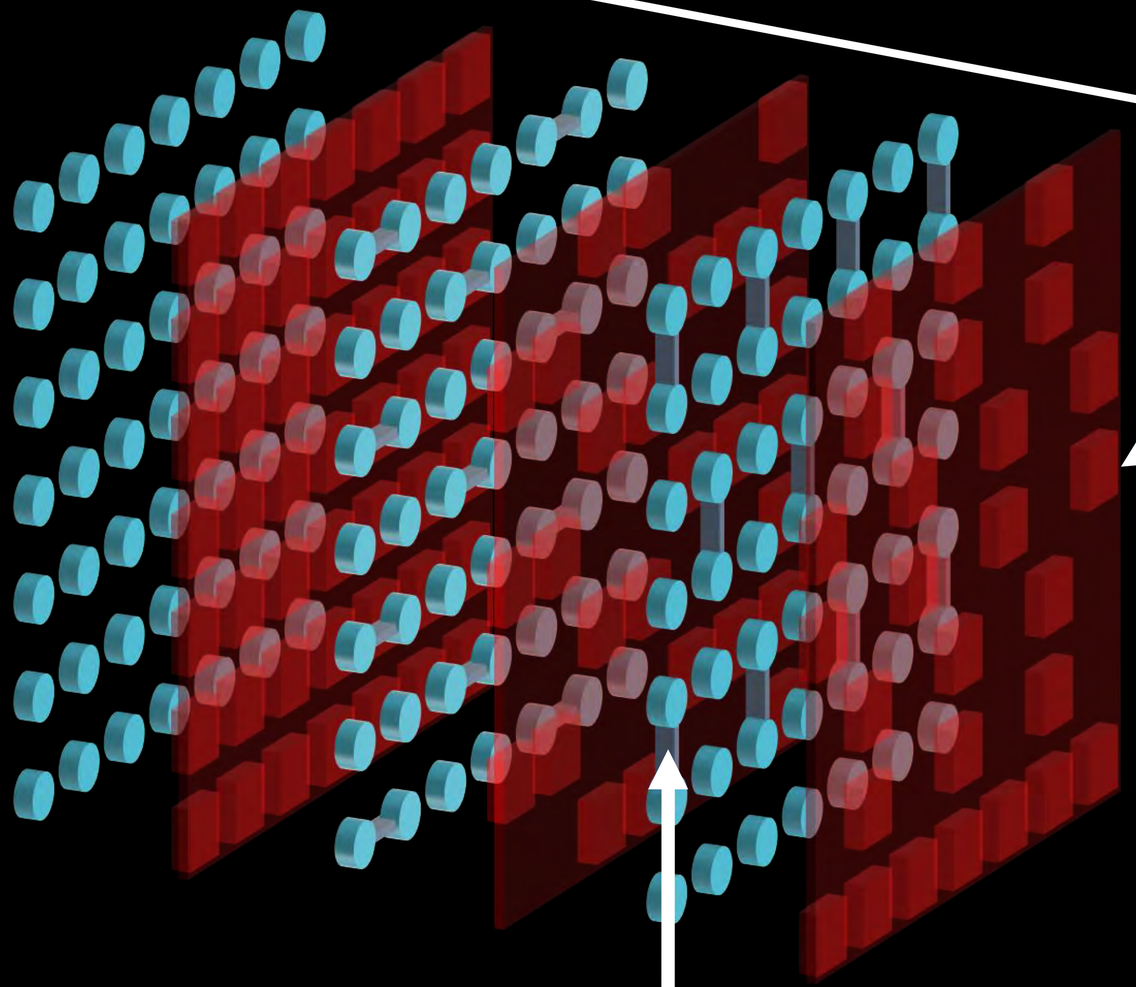


Another round of T, $X^{1/2}$, $Y^{1/2}$ gates chosen at random…



Boixo et al arXiv:1608.00263, QIP ‘17

The Google proposal



H gates

time/depth ~ $O(n^{1/2})$ > 40 layers of gates each with infidelity around ~1/(circuit size)

T, $X^{1/2}$, $Y^{1/2}$ gates

Supremacy might be achieved with 2d nearest neighbour Xmon superconducting qubit architecture on a 7×7 lattice.

7×7 array of qubits

CZ gates

Boixo et al arXiv:1608.00263, QIP ‘17

Google proposal summary

Best known classical complexity is exponential in number of qubits and circuit depth.

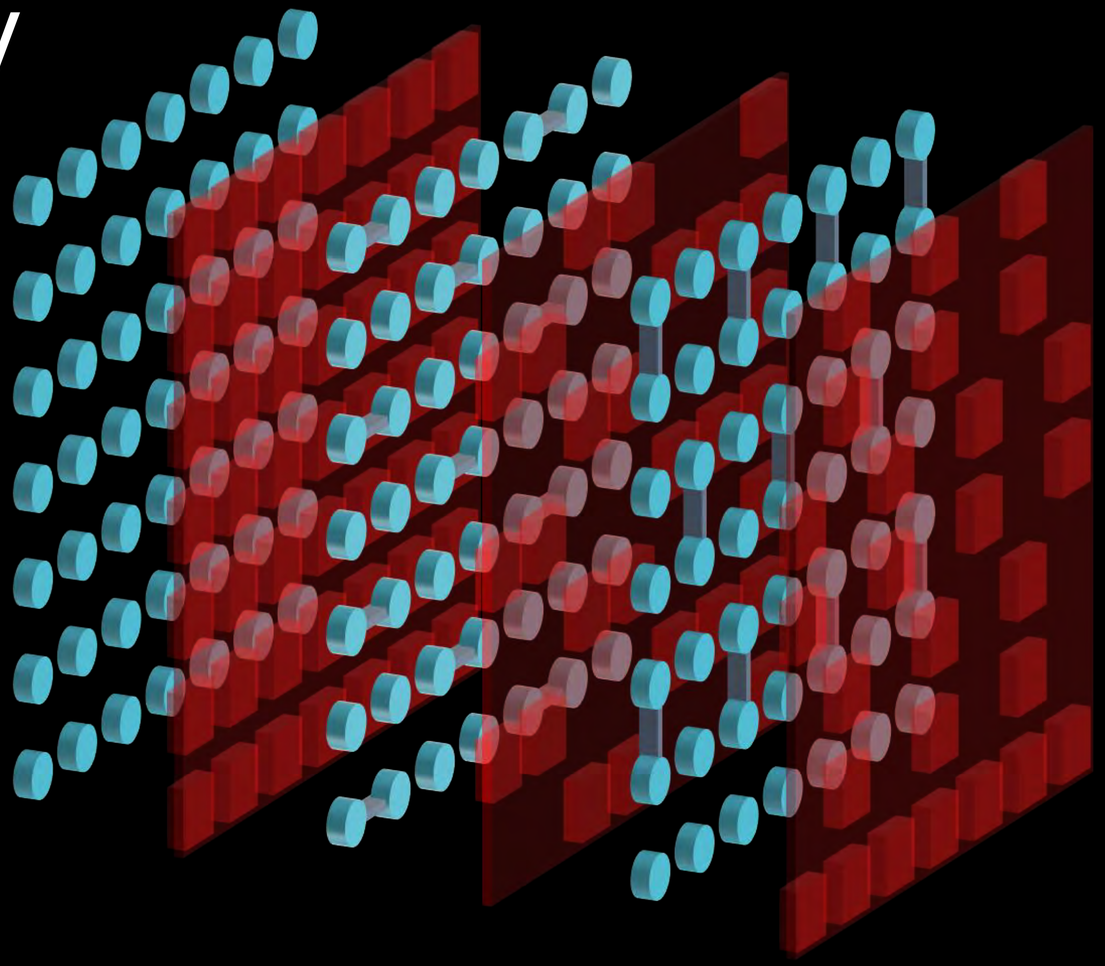
Introduces cross entropy benchmarking to establish validity and as a new methodology for benchmarking large circuits.

Heavy numerical testing to establish:

- level of randomness in the circuit.

- benchmarking.

- and the point at which these circuits surpass “the best” classical computers.



Outline

The worst-case complexity of $P(x) = |\langle x|U|0^n\rangle|^2$ - a crash course in quantum circuit complexity.

Approximate multiplicative sampling

“Approximate sampling” – randomness and Stockmeyer’s approximate counting.

Anticoncentrating circuit families

Time-space tradeoffs – where is the quantum frontier?

Noisy systems and classical approximations.

Verification

Outlook

Worst case complexity of $P(x) = |\langle 0^n | U | 0^n \rangle|^2$

A crash course in quantum circuit complexity

Quantum computers: a brief summary

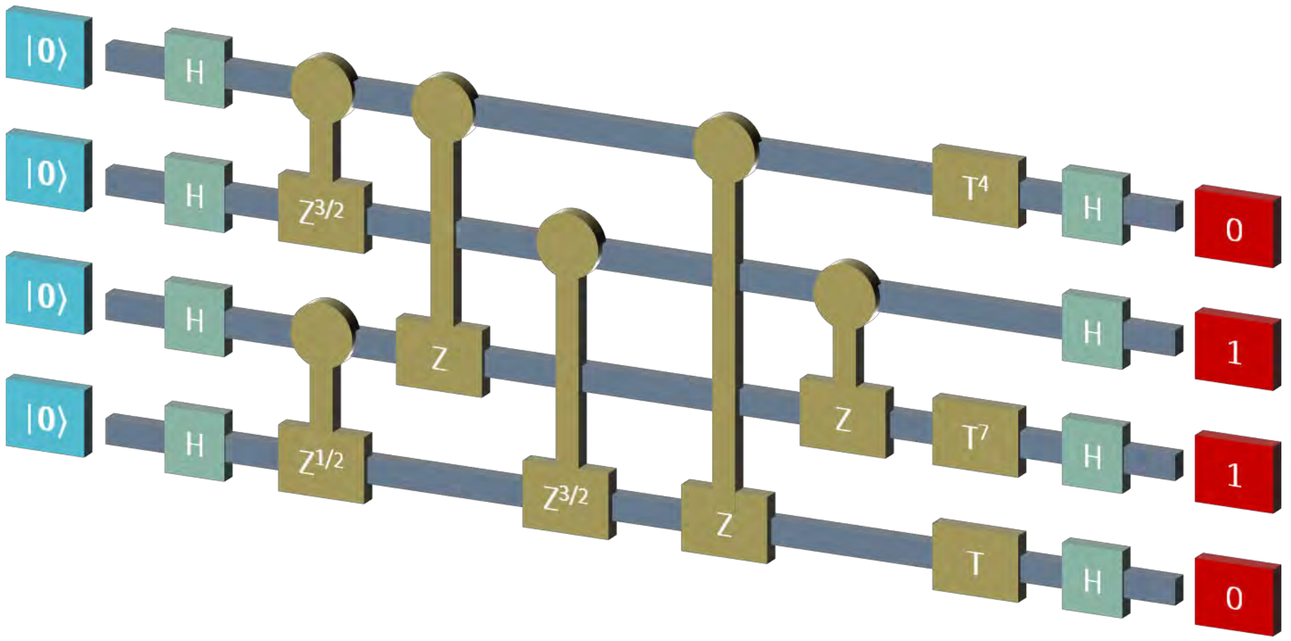
Input: classically easy to describe circuit, U, and input state $|0\rangle^{\otimes n}$.

Output: strings of bits $x \epsilon \{0,1\}^n$ with probability $P(x) = |\langle x|U|0\rangle^{\otimes n}|^2$.

Entangling gates can be acted between any of the qubits.

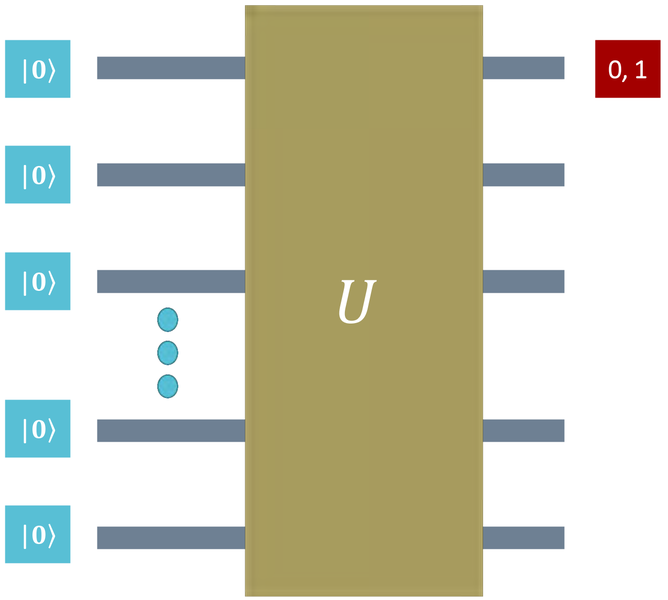
Gates are drawn from a finite gate set e.g. T, H, CZ. Universal gate sets (usually) have some construction that allows you to implement any unitary (assuming arbitrary runtime and ignoring errors)

What is the complexity of P(x)?

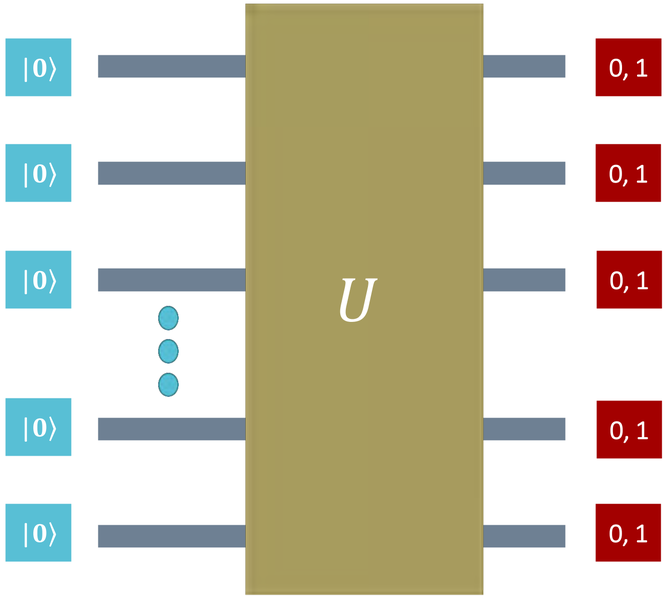


BQP vs SampBQP

BQP:



SampBQP:



BQP is the class of bounded error decision languages that can be decided by measuring a single output qubit from uniformly generated quantum circuits.

SampBQP is the class of problems that can be solved by measuring (or sampling) from the output of uniformly generated quantum circuits.

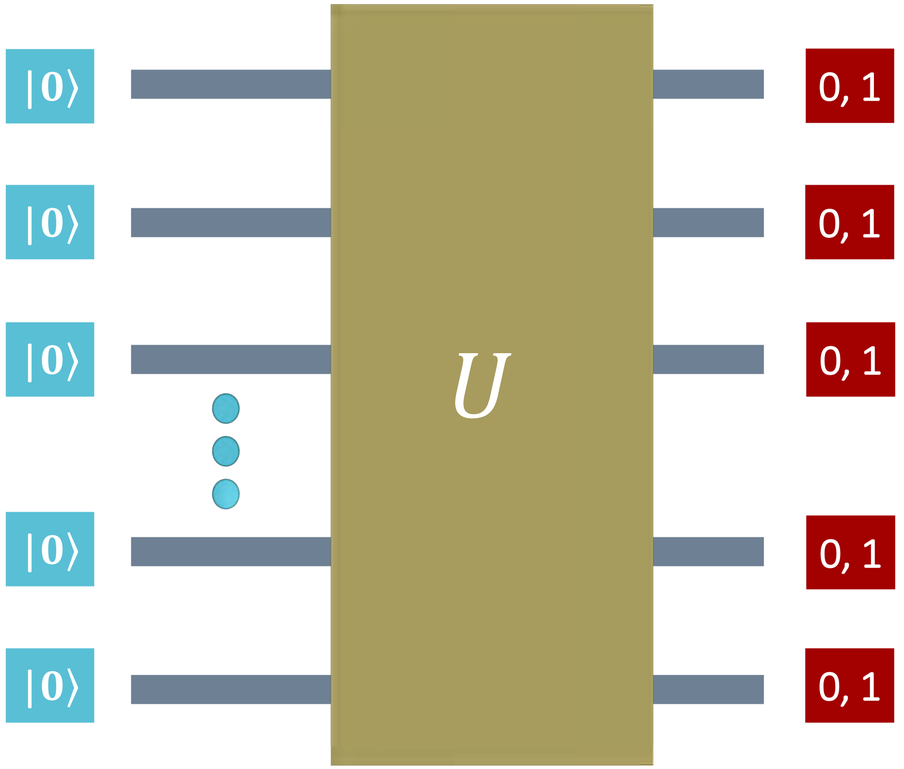
It is clear that BQP is in SampBQP but the converse is unknown. We know for sure that it is not true if we consider languages defined by families of circuits that are not universal for quantum computing – such as Clifford circuits or IQP circuits – under multiplicative errors.

The complexity of $P(x) = |\langle x|U|0\rangle^{\otimes n}|^2$

Input: a classical description of U (and x) polynomial in n.

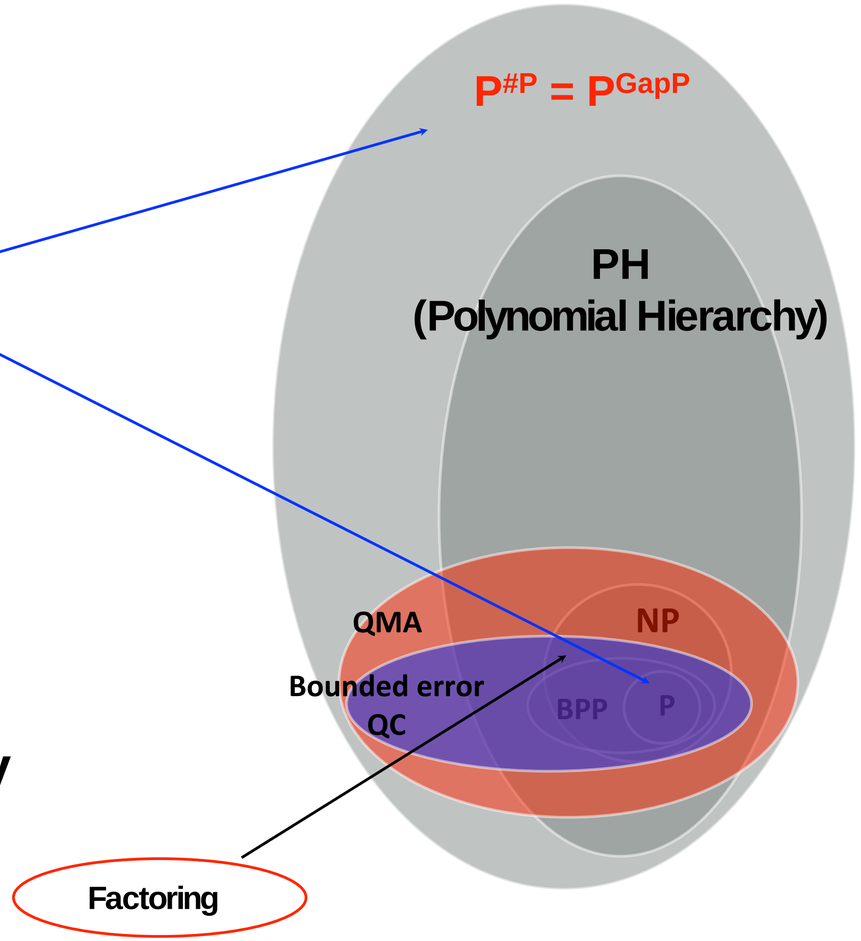
Output: R(x) or x from R(x) in time polynomial in the size of the description of U and the inverse of the error.

Output	Accuracy	Complexity upper bound
$R(x)$	$R(x) = P(x)$ "exact"	GapP
$x \in \{0,1\}$	$\|P - R\|_1 \leq \epsilon$ "additive sampling error"	BQP
$R(x)$	$\|P(x) - R(x)\| < \frac{1}{poly(n)}$ "additive error"	BQP
$x \in \{0,1\}^m$	$\|P - R\|_1 \leq \epsilon$ "additive error"	SampBQP
$x \in \{0,1\}^m$	$\frac{1}{c}P(x) \leq R(x) \leq cP(x), \forall x$ "multiplicative sampling error"	No classical R(x) unless PH = PH_3
$R(x)$	$\|P(x) - R(x)\| \leq \gamma P(x)$ "relative error"	GapP



The complexity of $P(x) = |\langle x|U|0\rangle^{\otimes n}|^2$

Exact Quantum amplitudes/probabilities $\langle x|U|y\rangle$



Importantly we do not believe that QCs can exactly compute P(x) well. The best approximation:
$|f-P(x)| \leq 1/O(poly(n))$

P: decision problems solvable with uniform poly sized circuits
NP: decision problems that can be verified by uniform poly sized circuits
#P: counts the number of inputs to a poly sized circuit that evaluate to 1. i.e. $|\{x:f(x) = 1\}|$
GapP: computes the difference between #P functions. i.e. $|\{x:f(x) = 1\}|-|\{x:f'(x) = 1\}|$.

GapP and quantum computing

- Fortnow and Rogers/Fenner et al (circa ’97): computing the amplitude of a quantum circuit is GapP-complete.

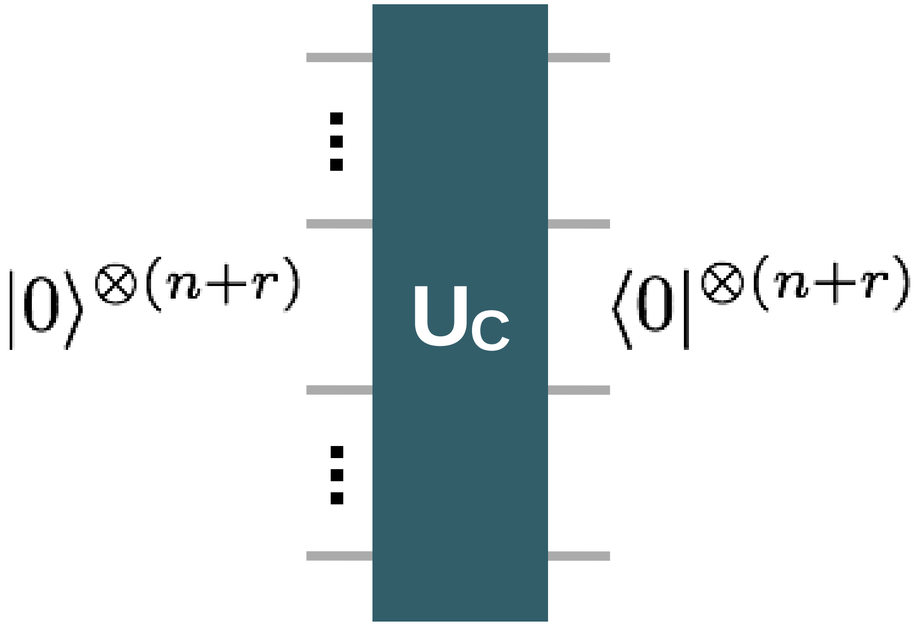
GapP: Let C be a classical circuit that computes a Boolean function $C : \{0,1\}^n \to \{-1,1\}$. Given C as input, compute Δ_C which is given by:

$$\Delta_C := \sum_{x \in \{0,1\}^n} C(x)$$

- GapP generalizes #P to encompass negative valued functions. It isn’t too hard to see that GapP ⊇ #P.

- Relative error (i.e. multiplicative) approximations to GapP-complete problems are still GapP-complete. Implies **$|A\text{-}P(0^n)| \leq \gamma P(0^n)$ is #P-hard. This is not true for #P functions.**

$$\langle 0|^{\otimes(n+r)} U_C |0\rangle^{\otimes n+r} = \frac{\Delta_C}{2^n}$$



Counting by searching

Problem:
Compute Δ_C precisely in time poly(n) given ability to compute the sign of any Δ_C.

$$\Delta_C := \sum_{x \in \{0,1\}^n} C(x)$$

Standard method, but see Aaronson (1109.1674):

Assume we can compute sgn(Δ_C) for C.

Define two alternate circuits C[±k] which are exactly the same as C except they introduce k additional inputs such that C[k](x) = ±1. Hence ΔC[±k] = ΔC ± k.

Algorithm:

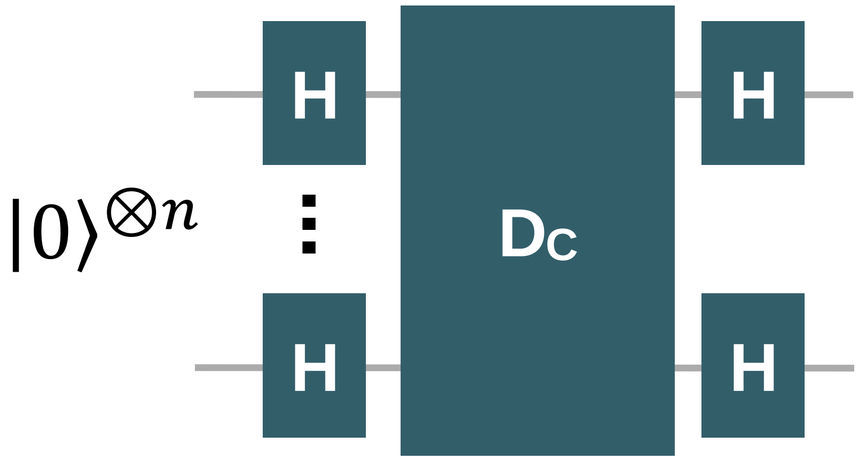
- **Compute the signs of Δ_C[±k] starting with k = 1 and increasing k by factors of two until sgn(Δ_C[k]) ≠ sgn(Δ_C[2k]).**
  - **At this point we know that Δ_C is between k and 2k.**
- **Then compute sgn(Δ_C[3k/2]) etc to ultimately determine the exact value for Δ_C.**
- **The complexity of such a procedure is O(poly(n)).**

GapP and quantum computing

$$\Delta_C := \sum_{x \in \{0,1\}^n} C(x)$$

Consider diagonal D_C with (x,x) entries given by C(x).

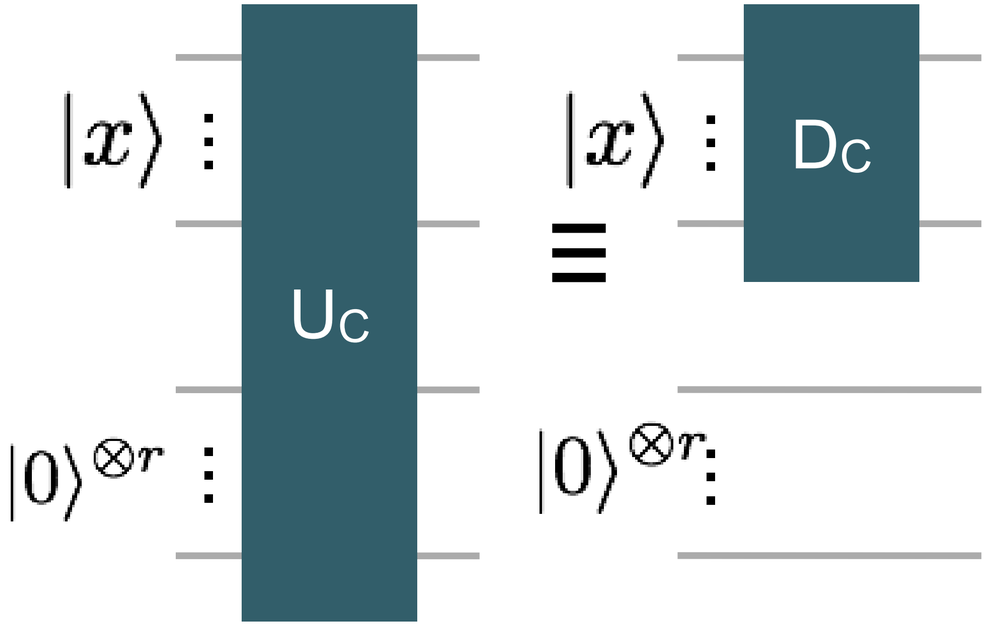
$$\begin{aligned}
\langle 0|^{\otimes n} \tilde{D}_C |0\rangle^{\otimes n} &= \langle 0|^{\otimes n} H^{\otimes n} D_C H^{\otimes} n |0\rangle^{\otimes n} \\
&= \left(\frac{1}{\sqrt{2^n}} \sum_{x' \in \{0,1\}^n} \langle x'| \right) D_C \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \right) \\
&= \frac{1}{2^n} \sum_{x,x' \in \{0,1\}^n} C(x)\delta(x,x') \\
&= \frac{\Delta_C}{2^n}
\end{aligned}$$



- **If we know the amplitude and n** we can compute Δ_C **precisely.**
- **Note: if there is any additive error in the amplitude in will be multiplied by 2^n - which is terrible!**
- **D_C is not uniformly generated.**

Uniform generation

- D_C can be generated by the "standard" tricks of reversible computation and the phase-kickback trick (see any lecture series on QC or Mike and Ike) via a uniformly generated circuit U_C.
- U_C be performed with Toffoli, Hadamard and X gates at a cost of (approximately) no more than the classical cost of performing C reversibly.
- This requires the use of r ancilla "scratch and output" qubits - where r < |C|.



$$U_C|x\rangle \otimes |0\rangle^{\otimes r} = C(x)|x\rangle \otimes |0\rangle^{\otimes r}$$

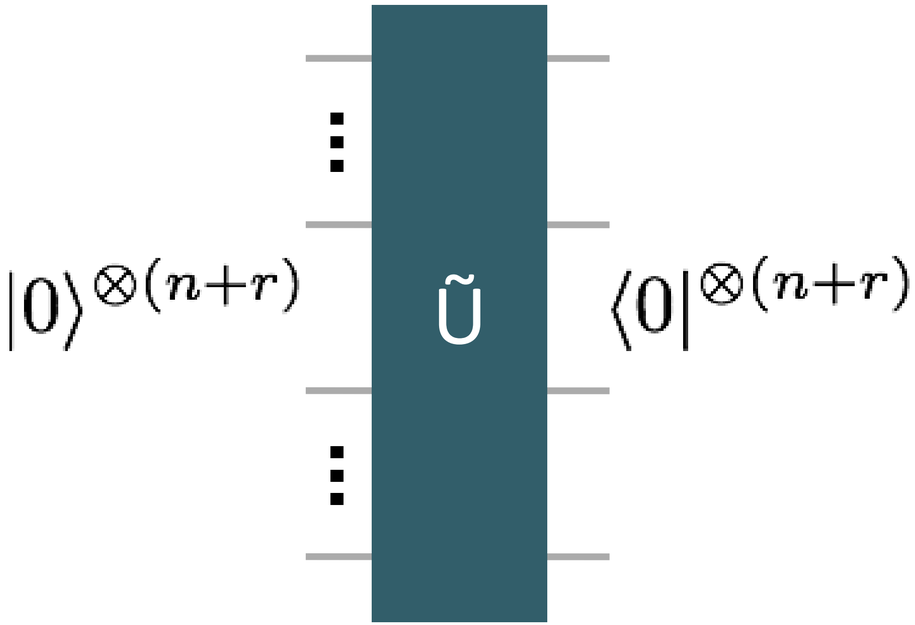
GapP and quantum computing

$$\Delta_C := \sum_{x \in \{0,1\}^n} C(x)$$

So we see computing the sign of an amplitude for a general quantum circuit is GapP-hard.

$$\langle 0|^{\otimes(n+r)} H^{\otimes n} U_C H^{\otimes n} |0\rangle^{\otimes(n+r)}$$
$$= \langle 0|^{\otimes(n+r)} \tilde{U} |0\rangle^{\otimes(n+r)} = \Delta_C / 2^n$$

It is possible to show that computing the corresponding probability is also GapP hard to within constant relative error via similar, but more complicated, arguments. (see appendix of BMS'15) i.e. finding an approximation A such **that $|A\text{-}P(0^n)| \leq \gamma P(0^n)$ is also GapP-complete.**

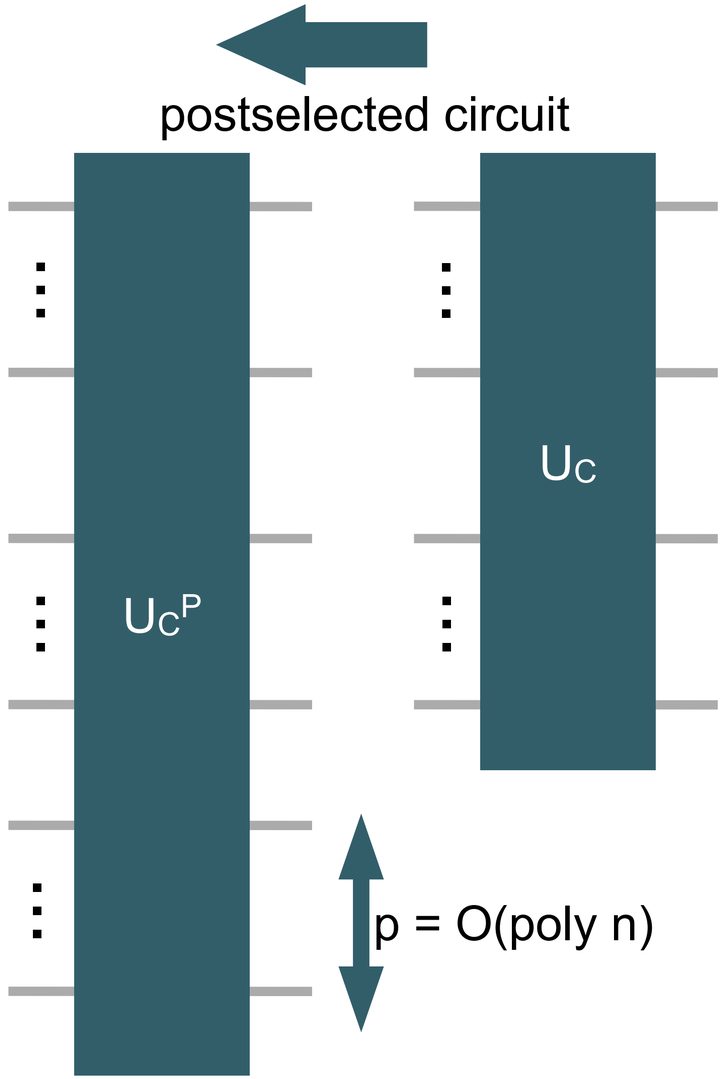


Key to the argument is that U_C necessarily must use a classically universal set of quantum gates.

This can be relaxed significantly both (1) to non-universal gate sets, and (2) to gate sets with algebraic entries.

Post-selection and depth reduction

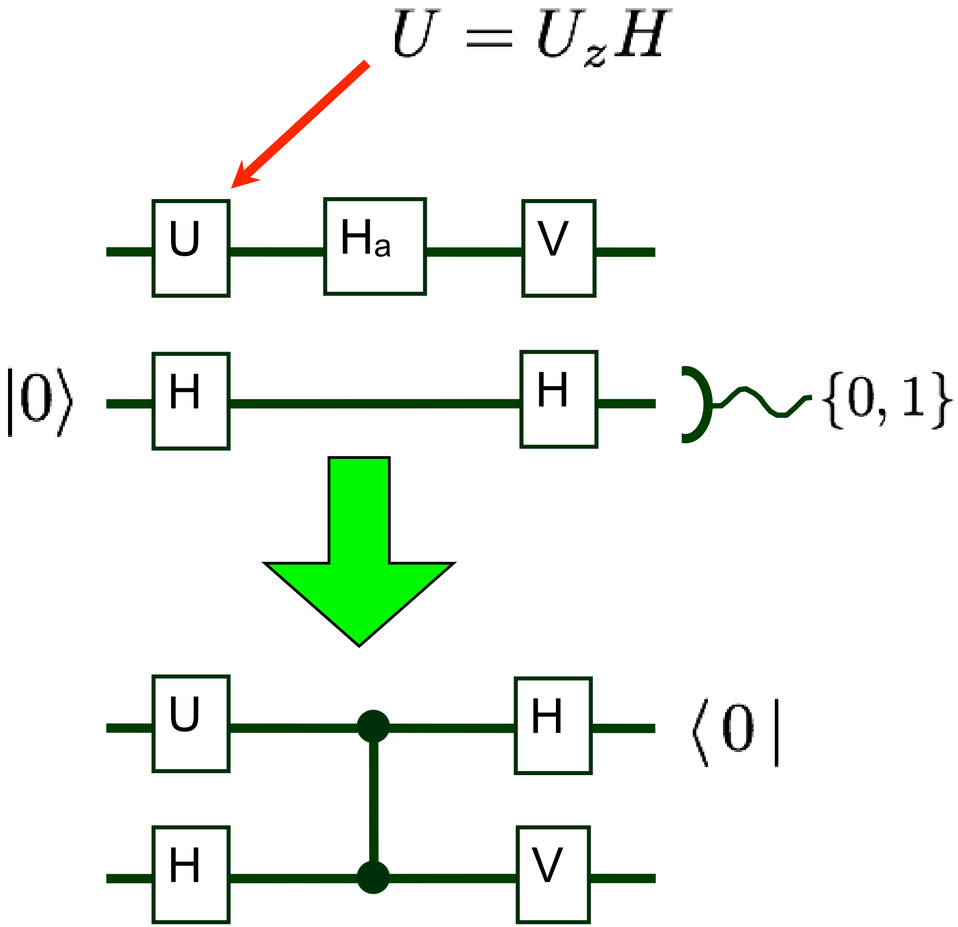
- **Post-selection, the act of disregarding all but the desired outcome from some register on your device, can be used to lower the depth of a circuit while maintaining it's amplitude up to a known factor.**
- **This means that the complexity relative error approximation is maintained.**
- **This key trick was used in Terhal and DiVincenzo (quantph/0205133) to argue that constant depth circuits cannot be classically sampled.**
- **Post-selection gadgets typically are derived from identities used in measurement based quantum computing.**
- **Typically we find the expression:** $\Pr_{U^P}(x, 0 \ldots 0) = \frac{1}{2^p} \Pr_{U}(x)$



* (See, Goldberg and Guo arXiv:1409.5627, Fuji and Morimae arXiv:1311.2128 and our paper.)

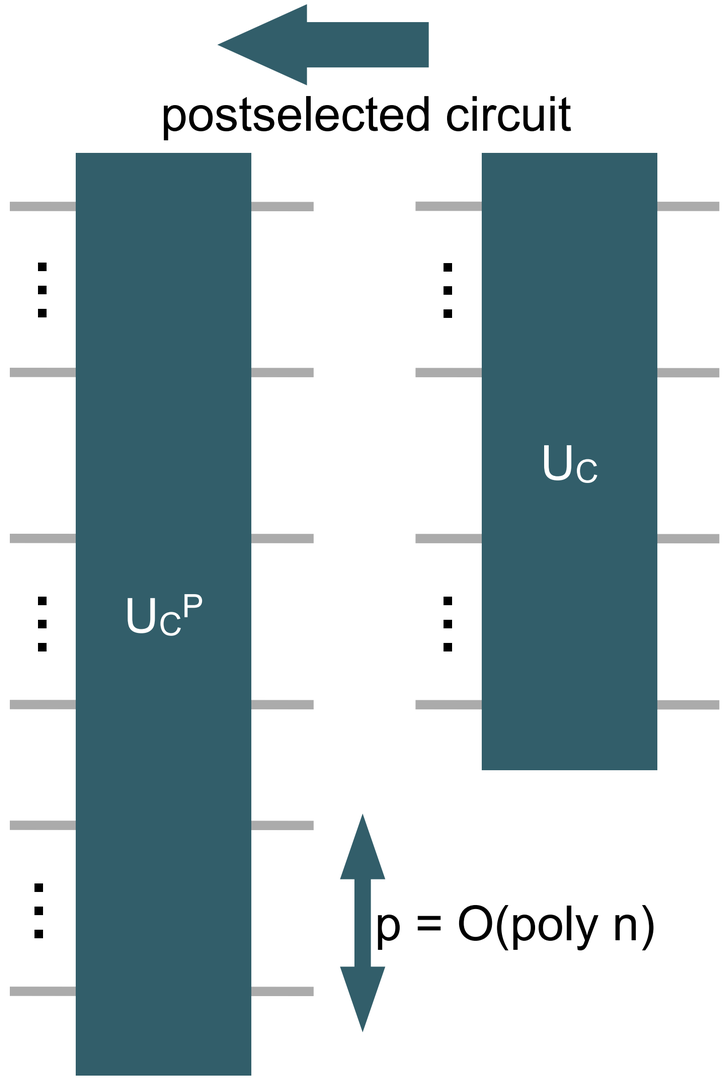
Post-selection and the Hadamard gadget

- **Take any circuit in BQP expressed in terms of the following universal gate set: H, Z, CZ, $e^{i(\pi/8)Z}$.**
- We can “remove” intermediate H’s with a “Hadamard gadget”.
- **As there are at most p = O(poly n) Hadamards then we will add O(poly n) new qubits.**
- **See Bremner, Jozsa, and Shepherd arXiv:1005.1407.**



Circuit classes that are universal under postselection can have GapP-complete amplitudes

- Circuits constructed from universal gate sets.
- Constant depth circuits.
- Linear optics without feedforward - i.e. Boson Sampling systems. Amplitudes are also proportional to matrix permanents! (See A+A)
- IQP circuits, i.e. circuits with all-commuting gates. Amplitudes are also proportional to partition functions, polynomial gaps and weight enumerator/Tutte polynomials.*
- Corresponding probabilities are always #P-hard even with relative error approximations. $|A-P(0^n)|\leq\gamma P(0^n)$



* (See, Goldberg and Guo arXiv:1409.5627, Fuji and Morimae arXiv:1311.2128 and our paper.)

Approximate multiplicative sampling

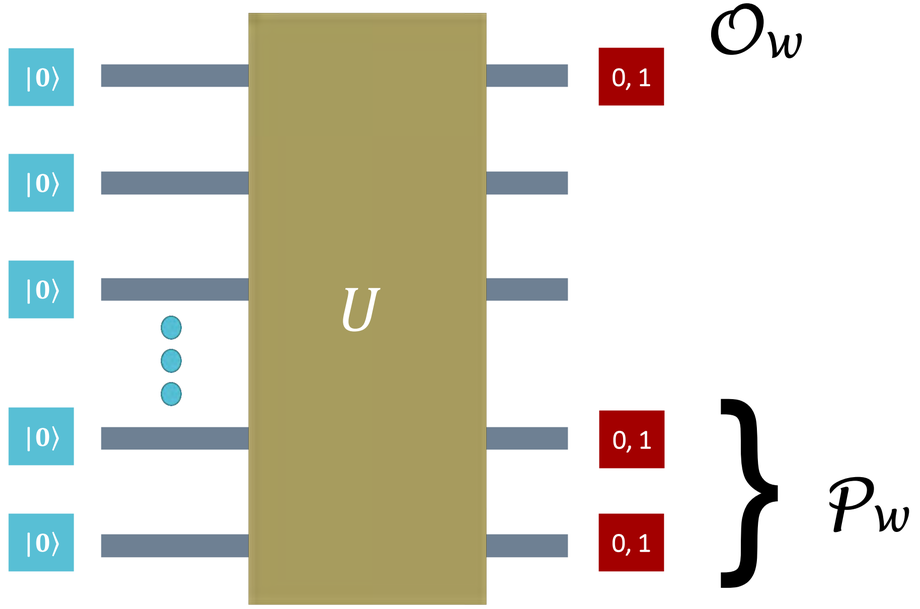
Post-selection for bounding sampling complexity

Post-selected decision languages

Definition (postBQP):

A language L is in the class postBQP (resp. postBPP) iff there is an error tolerance $0 < \varepsilon < 1/2$ and a uniform family $\{C_w\}$ of post-selected quantum (resp. randomised classical) circuits with a specified single line output register O_w (for the L-membership decision problem) and a specified (generally O(poly(n))-line) post-selection register P_w such that:

(i) if $w \in$ L then prob$[\mathcal{O}_w = 1 | \mathcal{P}_w = 00\ldots0] \geq 1-\varepsilon$ and
(ii) if $w \notin$ L then prob$[\mathcal{O}_w = 0 | \mathcal{P}_w = 00\ldots0] \geq 1-\varepsilon$.



$$\text{prob}(\mathcal{O}_w = x | \mathcal{P}_w = 00\ldots0) = \frac{\text{prob}(\mathcal{O}_w = x \ \& \ \mathcal{P}_w = 00\ldots0)}{\text{prob}(\mathcal{P}_w = 00\ldots0)}$$

Multiplicative sampling is hard: If the output probability distributions generated by uniform families of SampBQP circuits could be weakly classically simulated to within multiplicative error $1 \leq c < 2^{1/2}$ then postBPP = PP.

Proof sketch:

Given L ∈ **postBQP**, then there is a uniform family of post-selected circuits C_w that can decide the language with the following error bounds:

(i) if $w \in L$ then $S(1) = \text{prob}[\mathcal{O}_w = 1 \,|\, \mathcal{P}_w = 00\ldots0] \geq \frac{1}{2}+\delta$

(ii) if $w \notin L$ then $S(0) = \text{prob}[\mathcal{O}_w = 0 \,|\, \mathcal{P}_w = 00\ldots0] \geq \frac{1}{2}+\delta$

for, $0 < \delta \leq 1/2$.

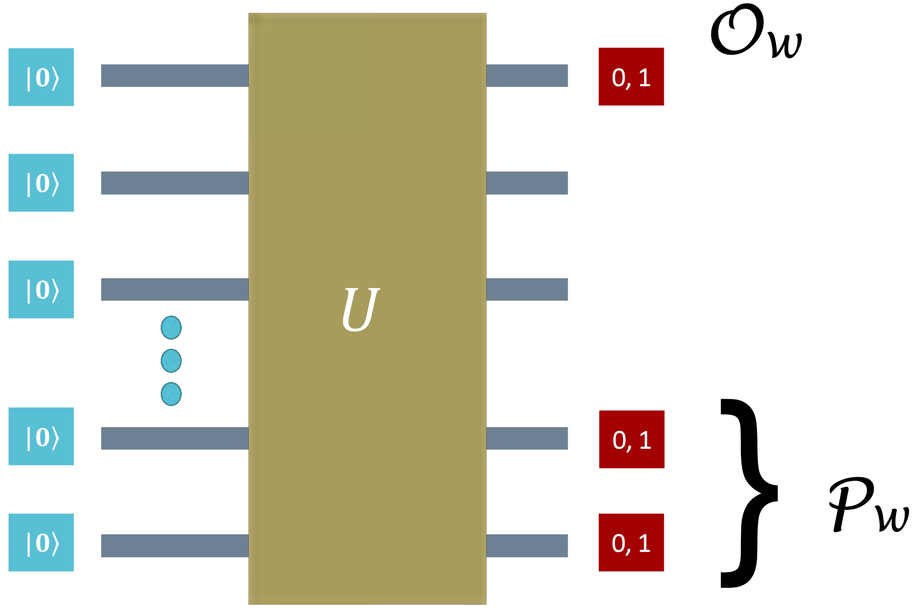
$$\text{prob}(\mathcal{O}_w = x | \mathcal{P}_w = 00...0) = \frac{\text{prob}(\mathcal{O}_w = x \;\&\; \mathcal{P}_w = 00...0)}{\text{prob}(\mathcal{P}_w = 00...0)}$$

Assumption: there is a uniform family of classical (polytime) randomized circuits C'_w that fulfill the multiplicative error criteria for :

$$\frac{1}{c}\,\text{prob}[\mathcal{Y}_w = \mathbf{y}] \leq \text{prob}[\mathcal{Y}'_w = \mathbf{y}] \leq c\,\text{prob}[\mathcal{Y}_w = \mathbf{y}]$$

and define the *post-selected success probability*:

$$S'_w(x) = \frac{\text{prob}(\mathcal{O}'_w = x \;\&\; \mathcal{P}'_w = 00...0)}{\text{prob}(\mathcal{P}'_w = 00...0)}$$



Which satisfies the following condition:

$$\frac{1}{c^2} S_w(x) \leq S'_w(x) \leq c^2 S_w(x)$$

From this you can show C'_w will decide L with bounded error if $1 \leq c < 2^{1/2}$. □

Multiplicative sampling is hard: If the output probability distributions generated by uniform families of SampBQP circuits could be weakly classically simulated to within multiplicative error $1 \leq c < 2^{1/2}$ then postBPP = PP.

Proof sketch:

Given L ∈ **postBQP**, then there is a uniform family of post-selected circuits C_w that can decide the language with the following error bounds:

(i) if $w \in L$ then $S(1) = \text{prob}[\mathcal{O}_w = 1 \,|\, \mathcal{P}_w = 00\ldots0] \geq \frac{1}{2}+\delta$

(ii) if $w \notin L$ then $S(0) = \text{prob}[\mathcal{O}_w = 0 \,|\, \mathcal{P}_w = 00\ldots0] \geq \frac{1}{2}+\delta$

for, $0 < \delta \leq 1/2$.

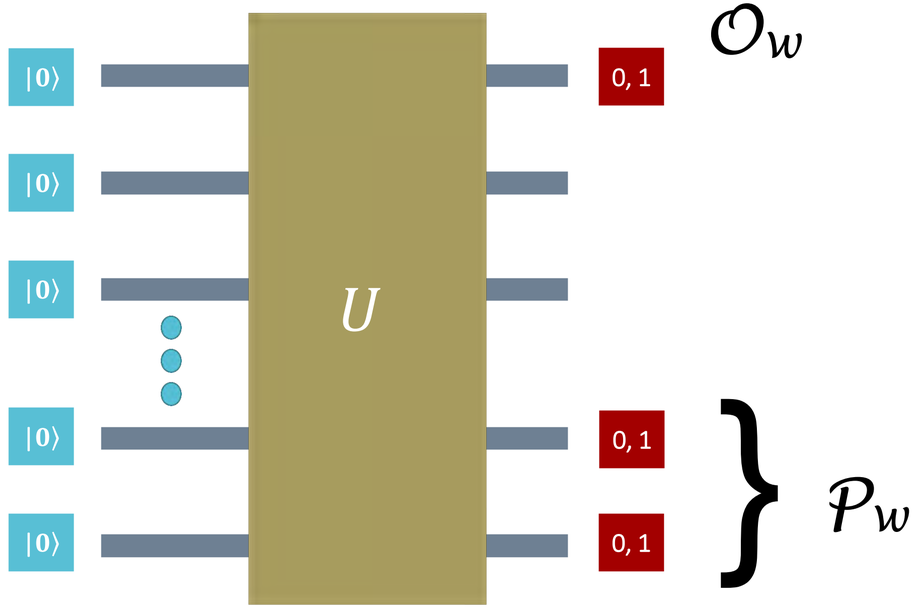
$$\text{prob}(\mathcal{O}_w = x | \mathcal{P}_w = 00\ldots0) = \frac{\text{prob}(\mathcal{O}_w = x \;\&\; \mathcal{P}_w = 00\ldots0)}{\text{prob}(\mathcal{P}_w = 00\ldots0)}$$

Assumption: there is a uniform family of classical (polytime) randomized circuits C'_w that fulfill the multiplicative error criteria for :

$$\frac{1}{c}\,\text{prob}[\mathcal{Y}_w = \mathbf{y}] \leq \text{prob}[\mathcal{Y}'_w = \mathbf{y}] \leq c\,\text{prob}[\mathcal{Y}_w = \mathbf{y}]$$

and define the *post-selected success probability*:

$$S'_w(x) = \frac{\text{prob}(\mathcal{O}'_w = x \;\&\; \mathcal{P}'_w = 00\ldots0)}{\text{prob}(\mathcal{P}'_w = 00\ldots0)}$$



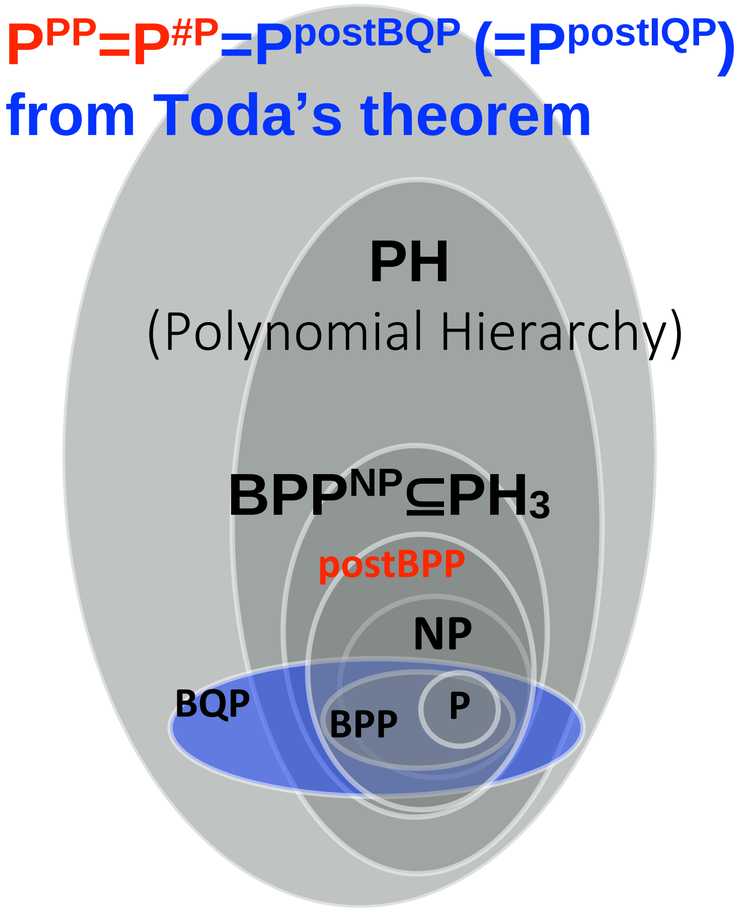
Which satisfies the following condition:

$$\frac{1}{c^2} S_w(x) \leq S'_w(x) \leq c^2 S_w(x)$$

From this you can show C'_w will decide L with bounded error if $1 \leq c < 2^{1/2}$. □

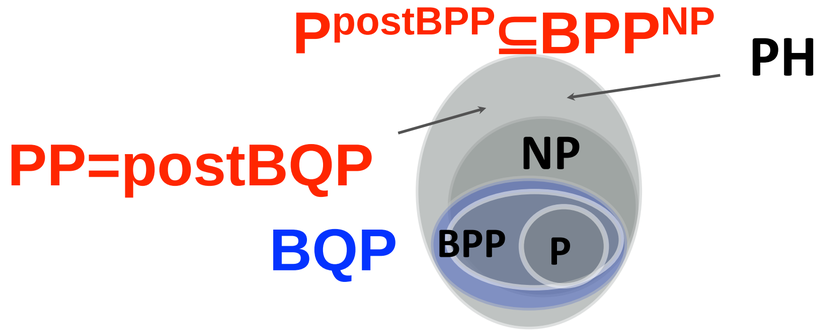
“Proof”

If classical computers can simulate the quantum Ising model to within a reasonable approximation, then PostBQP = PostIQP = PostBPP.



“Proof”

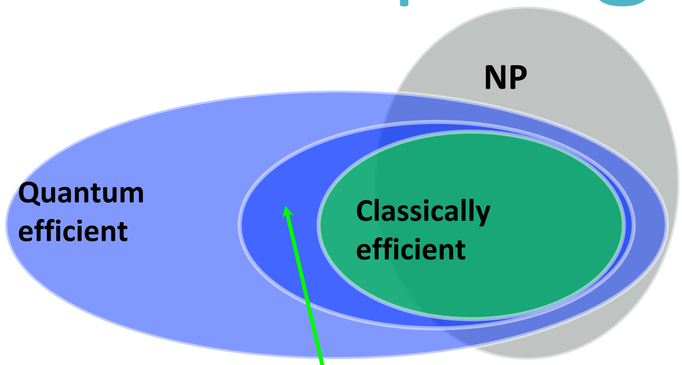
If classical computers can simulate the quantum Ising model to within a reasonable approximation, then PostBQP = PostIQP = PostBPP.



Approximate multiplicative sampling

Similar arguments have been made for quite a few “intermediate” models of quantum computing.

Unfortunately, we will see that none of them are really sufficient for “quantum supremacy” experiments.



- IQP (Bremner, Josza, Shepherd): quantum circuits constructed from commuting gates.
- Constant depth circuits (Terhal and DiVincenzo) + (BJS)
- BosonSampling (Aaronson and Arkhipov): linear optics without adaptive measurements.
- DQC1 (Fujii, Morimae, Fitzsimmons): quantum circuits with only 1 “clean” qubit.
- Circuits of 2-local commuting gates (Adam Bouland, Laura Mańcinska, and Xue Zhang arXiv:1602.04145).
- IQP circuits with local noise models (Fujii and Tamate, arXiv:1406.6932v3)
- Constant-depth Boson Sampling (Brod arXiv:1412.6788)
- Boson Sampling with all manner of noise models (many authors)

Quantum computing: the fine print

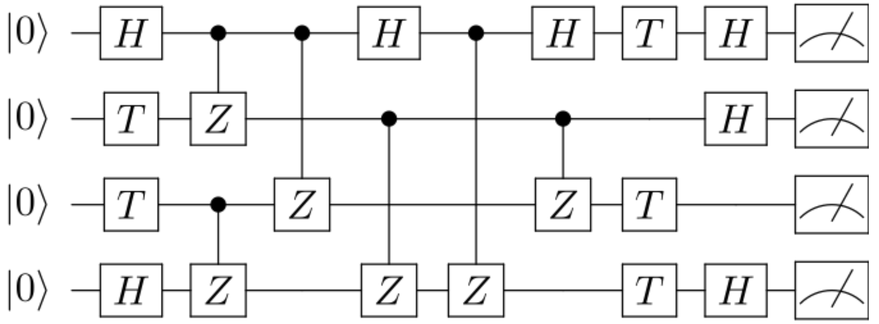
Input:
A simple description of a probability distribution $P(x)=|\langle x|C|0\rangle|^2$, usually in the form of a quantum circuit or physical system.

It is “simple” in the size of the system, n.

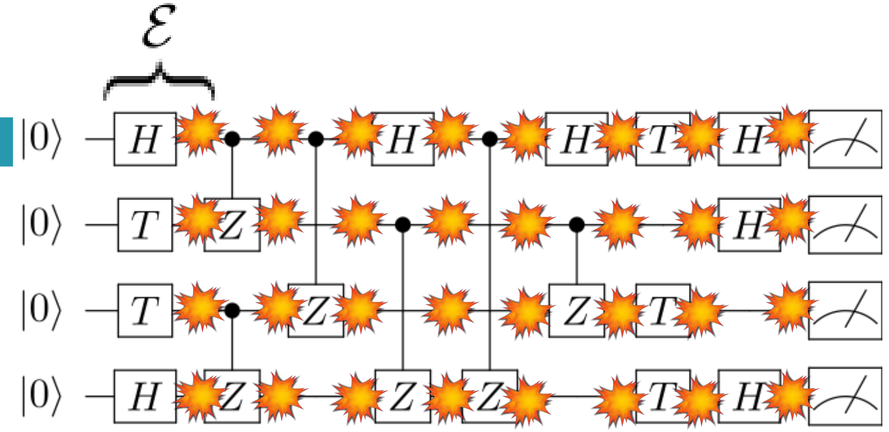
Output:
x, with probability R(x) in such that $||P-R|| \leq \varepsilon$ in time poly(n, ε^{-1}).

Approximation is fundamental to quantum computing

finite gate set



physical noise



tomography

ρ?

Quantum computing is a digital model of computing, this demands that the gate set be finite, which ultimately means that outputs are always approximate.

Additive vs multiplicative approximations

Additive

$$\|P - R\|_1 = \sum_x |P(x) - R(x)| \leq \epsilon$$

vs

Multiplicative

$$\frac{1}{c}P(x) \leq R(x) \leq cP(x), \forall x$$

Consider 2 distributions:

P = (1/2,1/2 - w, w) and R = (1/2,1/2,0)

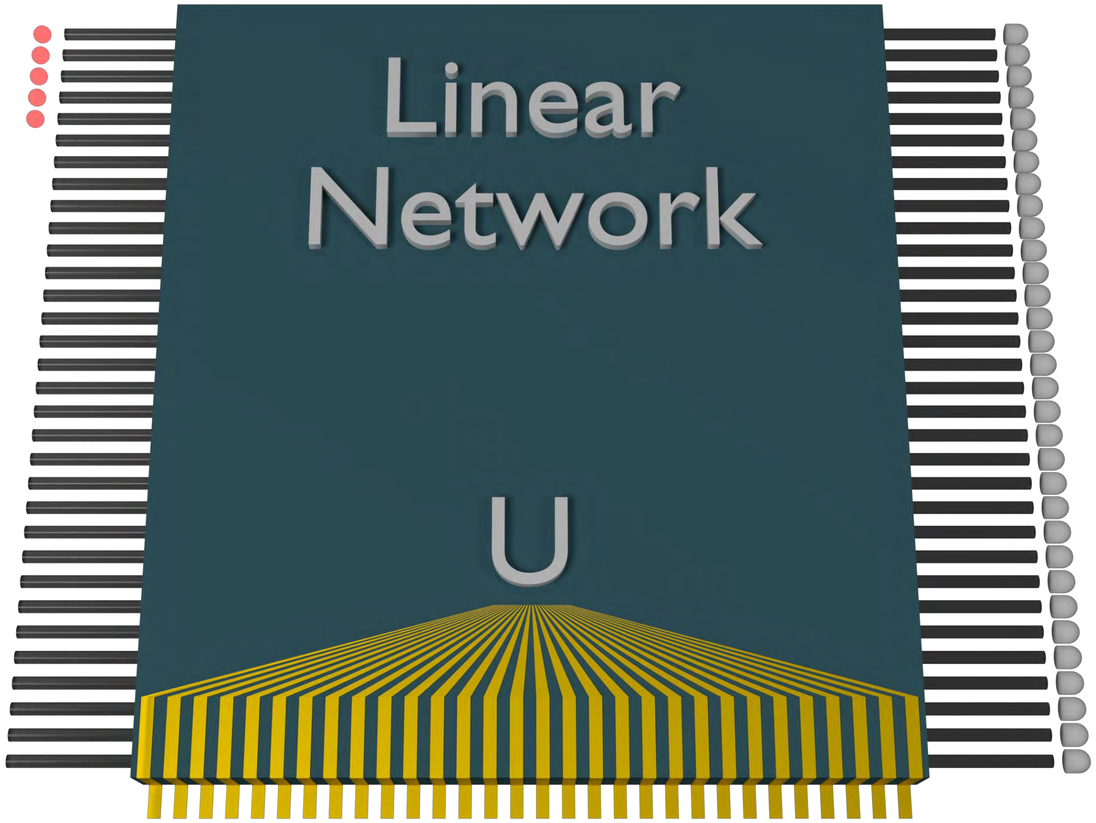
where w is ridiculously small for whatever measure of ridiculousness you want.

$||P-R||_1 = 2w$. If we want $||P-R||_1 \leq \varepsilon$, ε only has to be small (not ridiculously small).

Whereas R can never approximate P to within any multiplicative factor. $(1/c)w \not\leq 0 \leq cw$

“Approximate sampling”

Randomness and Stockmeyer counting.



Aaronson and Arkhipov's great idea!

If you could simulate linear optics classically, and if you have a BPP^{NP} machine, you might be able to use Stockmeyer's theorem to compute complex matrix permanents. This would cause a PH collapse.

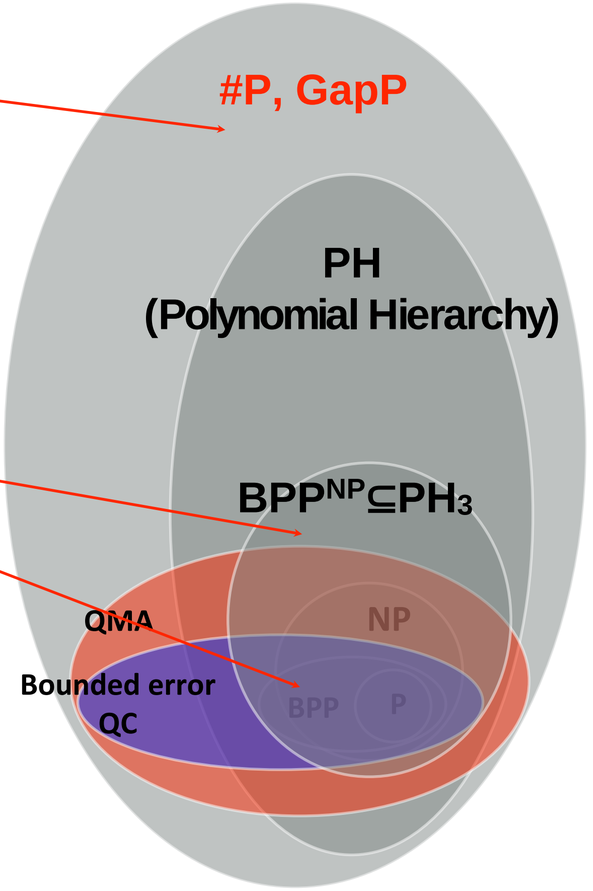
Importantly, we will randomly chosen circuits are particularly well approximated via Stockmeyer counting.

Relative error approximations: $|A_x - f| \leq \gamma f$, bounding classical complexity

There are classes of $f = \langle x|U|y \rangle$ that stay GapP-hard even with approximation.

Stockmeyer's algorithm can give a relative error approximation A_x for functions f that are inside #P inside BPP^{NP}.

This does not work for GapP-hard functions unless the PH collapses.



Terhal and DiVincenzo '02, Bremner, Jozsa, Shepherd/Aaronson and Arkhipov '10: GapP-hardness of relative error approximations of $\langle x|U|y \rangle$ for constant depth circuits, IQP circuits, linear optics, and any family universal for quantum computation with post-selection.

This implies that there are no classical efficient algorithms for such circuit families that can achieve a multiplicative error bound without a collapse of the PH.

Stockmeyer's counting theorem

There exists an FBPP^{NP} machine which, for any boolean function $f:\{0,1\}^n \to \{0,1\}$, can approximate

$$p = \Pr_x[f(x) = 1] = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} f(x)$$

to within a relative error $|\tilde{p} - p| < \epsilon p$ for $\epsilon = \Omega[1/poly(n)]$, given oracle access to f.

- This theorem implies that any function in #P has a good relative error approximation inside the Polynomial Hierarchy.

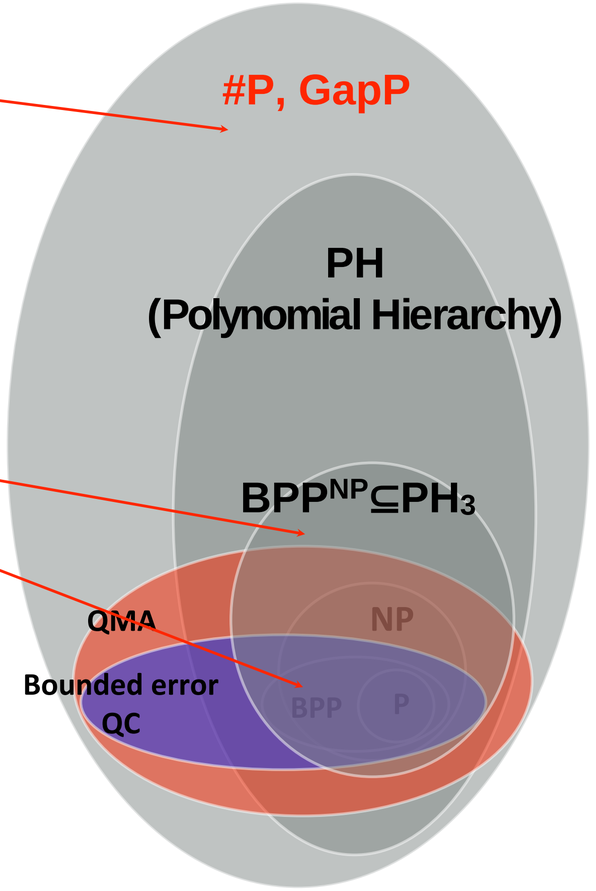
- In the case of quantum sampling if we want to approximate, say, $\mathrm{P(y)} = |\langle y|U|0^n\rangle|^2$, and we had an efficient classical sampler then $f(x) = \delta_{x,y}$.

Relative error approximations: $|A_x - f| \leq \gamma f$, bounding classical complexity

There are classes of $f = \langle x|U|y \rangle$ that stay GapP-hard even with approximation.

Stockmeyer's algorithm can give a relative error approximation A_x for functions f that are inside #P inside BPP^{NP}.

This does not work for GapP-hard functions unless the PH collapses.

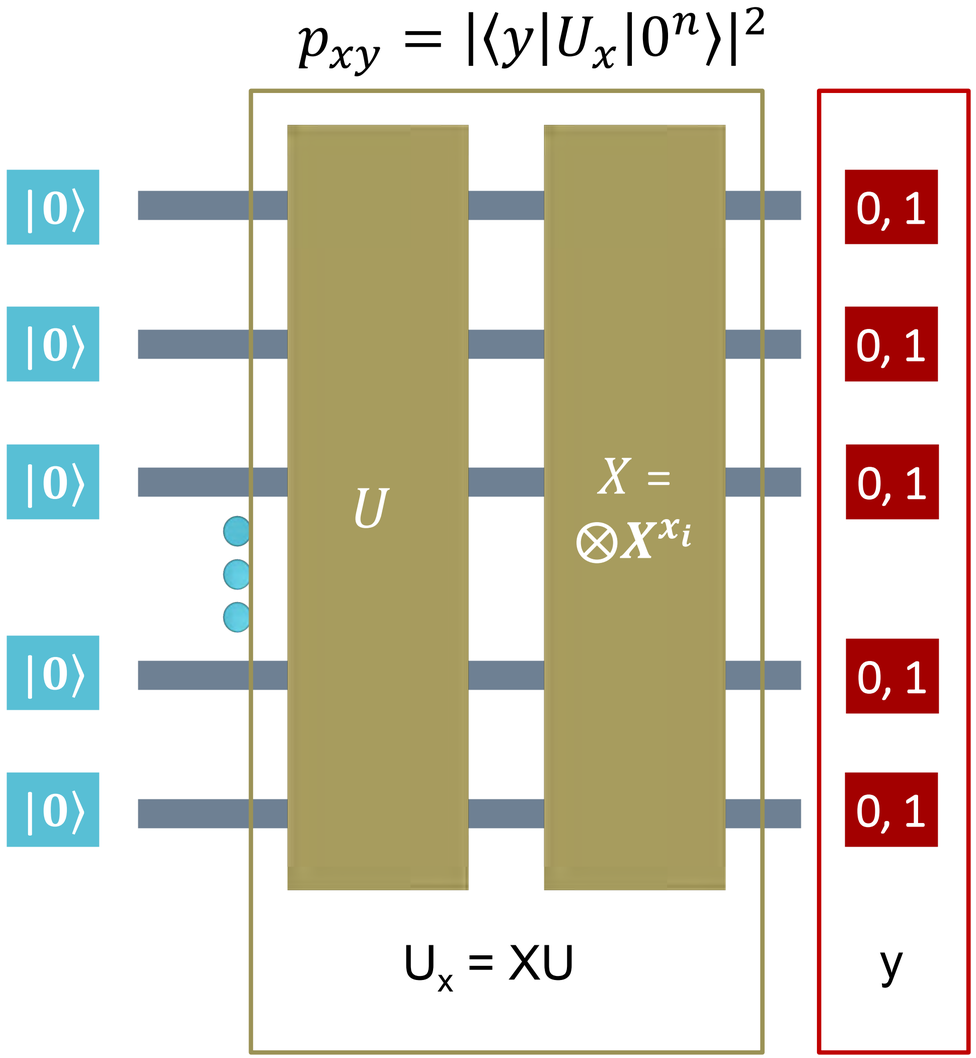


The "quantum random circuit sampling" argument:

If there exists *sufficiently accurate** efficient classical samplers for the outputs from *sufficiently random* U, Stockmeyer's algorithm can be used to approximate $f = \langle x|U|y \rangle$ (which could be GapP-hard).

* sufficiently accurate = constant 1-norm distance

Stockmeyer and random circuits

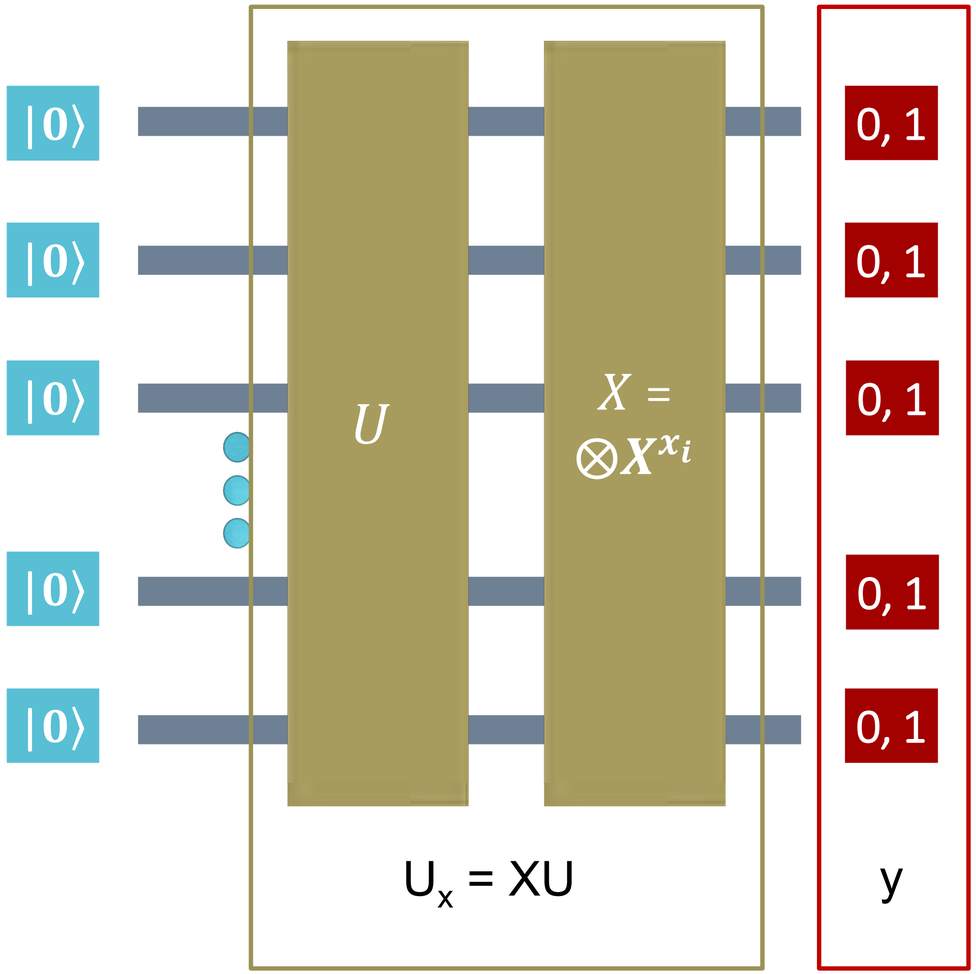


Stockmeyer and random circuits

$$\|p - q\|_1 = \sum_{y \in \{0,1\}^n} |p_{xy} - q_{xy}| \leq \epsilon$$

$$p_{xy} = |\langle y|U_x|0^n\rangle|^2$$

$$q_{xy} = \Pr[A \text{ outputs } y \text{ on input } U_x]$$

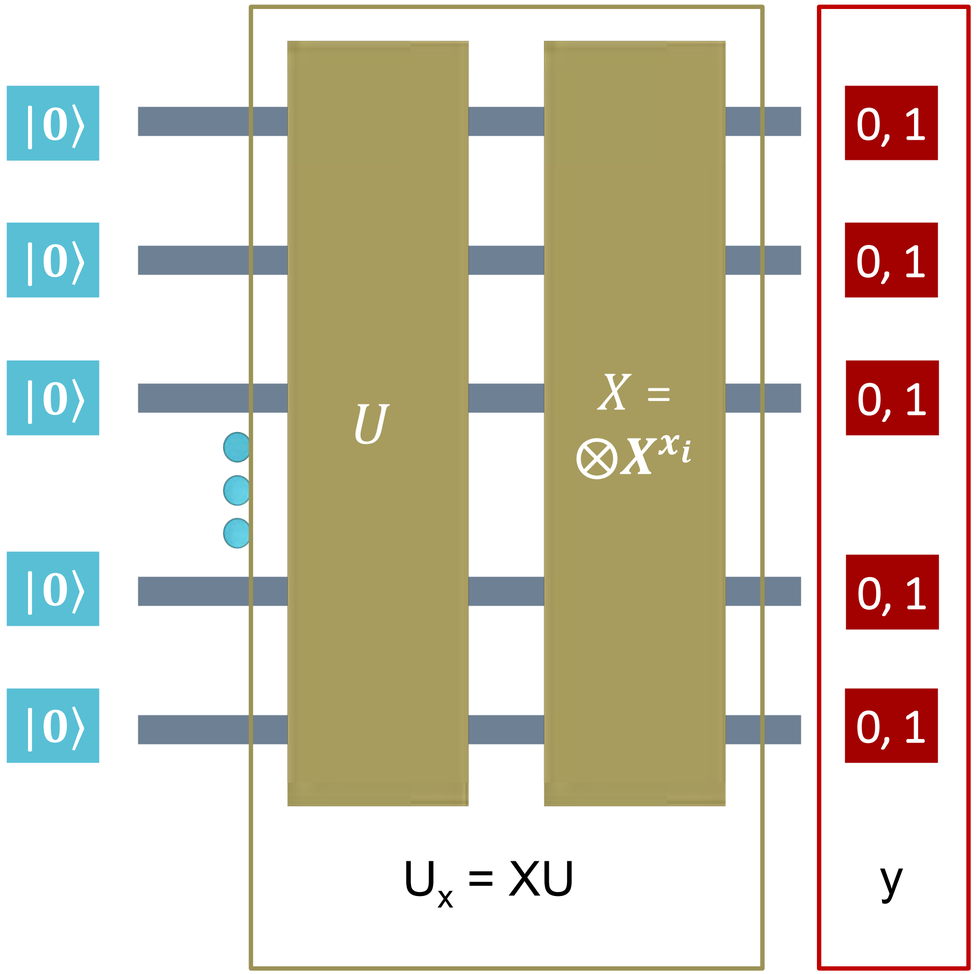


Stockmeyer and random circuits

$$\|p - q\|_1 = \sum_{y \in \{0,1\}^n} |p_{xy} - q_{xy}| \leq \epsilon$$

$$p_{xy} = |\langle y|U_x|0^n\rangle|^2$$

$$q_{xy} = \Pr[A \text{ outputs } y \text{ on input } U_x]$$



+NP

Lemma: Given U, let U_x be the product XU where $X = \bigotimes X^{x_i}$ for a choice of bitstring $x \in \{0,1\}^n$.

Given an efficient classical sampler A for U_x with l_1 accuracy ϵ and an $FBPP^{NP}$ machine we can use Stockmeyer's algorithm to approximate P_{x0} to additive error:

$$O\left(\frac{(1 + o(1))\epsilon}{2^n \delta} + \frac{|\langle 0^n|U_x|0^n\rangle|^2}{poly(n)}\right)$$

with probability at least $1 - \delta$ over the choice of x.

Stockmeyer and random circuits

$$\|p-q\|_1 = \sum_{y\in\{0,1\}^n} |p_{xy} - q_{xy}| \leq \epsilon$$

For any choice of y we can use Stockmeyer's algorithm to produce an approximation

$|\tilde{q} - q_{0y}| \leq \frac{q_{0y}}{poly(n)}$ in FBPP^{NP}.

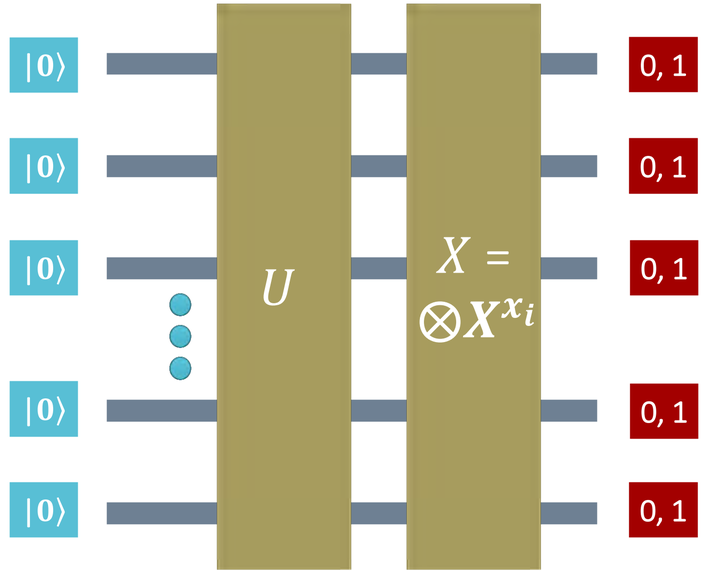
Then,

$$|\tilde{q}_y - p_{0y}| \leq |\tilde{q}_y - q_{0y}| + |q_{0y} - p_{0y}| \leq \frac{q_{0y}}{poly(n)} + |q_{0y} - p_{0y}|$$

$$\leq \frac{(p_{0y}+|q_{0y}-p_{0y}|)}{poly(n)} + |q_{0y} - p_{0y}|$$

$$= \frac{p_{0y}}{poly(n)} + |q_{0y} - p_{0y}|(1 + \frac{1}{poly(n)})$$

$$p_{xy} = |\langle y|U_x|0^n\rangle|^2$$



$$q_{xy} = \Pr[A \text{ outputs } y \text{ on input } U_x]$$

+NP

Stockmeyer and random circuits

$$\|p-q\|_1 = \sum_{y\in\{0,1\}^n} |p_{xy} - q_{xy}| \leq \epsilon$$

For any choice of y we can use Stockmeyer's algorithm to produce an approximation

$$|\tilde{q} - q_{0y}| \leq \frac{p_{0y}}{poly(n)} + |q_{0y} - p_{0y}|(1 + \frac{1}{poly(n)})$$

Then as A approximates outputs of U_0 to l_1 error ϵ we find from Markov's inequality that:

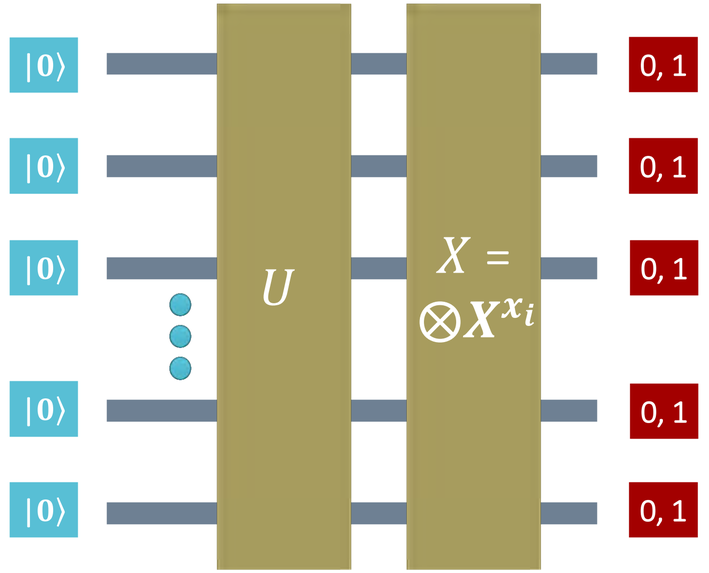
$$\Pr_y\left[|q_{0y} - p_{0y}| \geq \frac{\epsilon}{2^n\delta}\right] \leq \delta$$

For any $0 \leq \delta \leq 1$ where y is picked uniformly at random.

$$|\tilde{q}_y - p_{0y}| \leq \frac{p_{0y}}{poly(n)} + \frac{\epsilon(1+\frac{1}{poly(n)})}{2^n\delta}$$

With probability $1-\delta$ over the choice of y. But, p_{0y} $= |\langle y|U_0|0^n\rangle|^2 = |\langle 0^n|U_y|0^n\rangle|^2 = p_{y0}$.

$$p_{xy} = |\langle y|U_x|0^n\rangle|^2$$



$$q_{xy} = \Pr[A \text{ outputs } y \text{ on input } U_x]$$

+NP

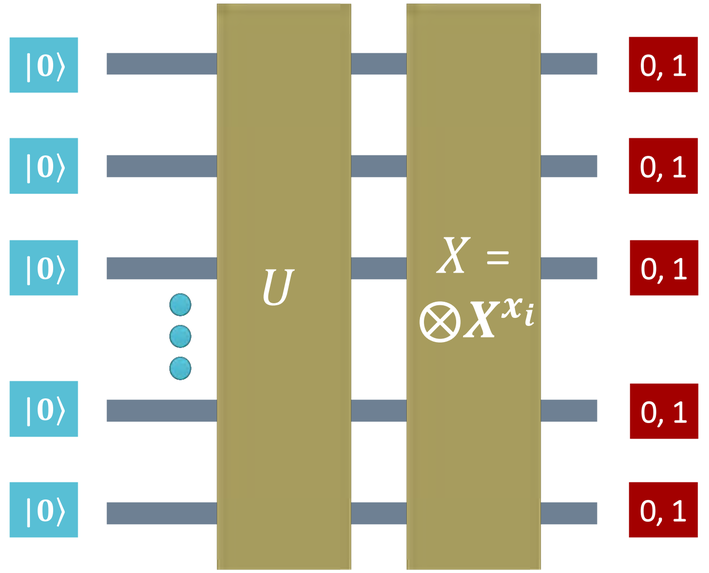
Relative error approximations

$$\|p - q\|_1 = \sum_{y \in \{0,1\}^n} |p_{xy} - q_{xy}| \leq \epsilon$$

$$|\tilde{q}_y - p_{y0}| \leq \frac{p_{0y}}{poly(n)} + \frac{\epsilon(1+\frac{1}{poly(n)})}{2^n \delta}$$

When does this yield a relative error approximation to p_{0y}? When $p_{0y} \geq \alpha . 2^{-n}$.

$$P_{xy} = |\langle y|U_x|0^n\rangle|^2$$



$$q_{xy} = \Pr[A \text{ outputs } y \text{ on input } U_x]$$

Corollary

Let U be randomly chosen from some family F. Apply a random X to U (note: this step is not required depending on the family F). Assume there exists constants $\alpha, \beta > 0$ such that:

$$\Pr_{U_x \in F}[|\langle 0^n|U_x|0^n\rangle|^2 \geq \alpha . 2^{-n}] \geq \beta$$

Assume also that A can simulate the output of any U up to l_1 error $\epsilon = \frac{\alpha\beta}{8}$. Then Stockmeyer's algorithm gives a relative error approximation of ¼ +o(1) for a $\beta/2$ fraction of U.

+NP

Relative error approximations

$$\left|\tilde{q}_y - p_{y0}\right| \leq \frac{p_{0y}}{poly(n)} + \frac{\epsilon(1+\frac{1}{poly(n)})}{2^n \delta}$$

When does this yield a relative error approximation to p_{0y}? When $p_{0y} \geq \alpha . 2^{-n}$.

Corollary

Let U be randomly chosen from some family F. Apply a random X to U (note: this step is not required depending on the family F). Assume there exists constants $\alpha, \beta > 0$ such that:

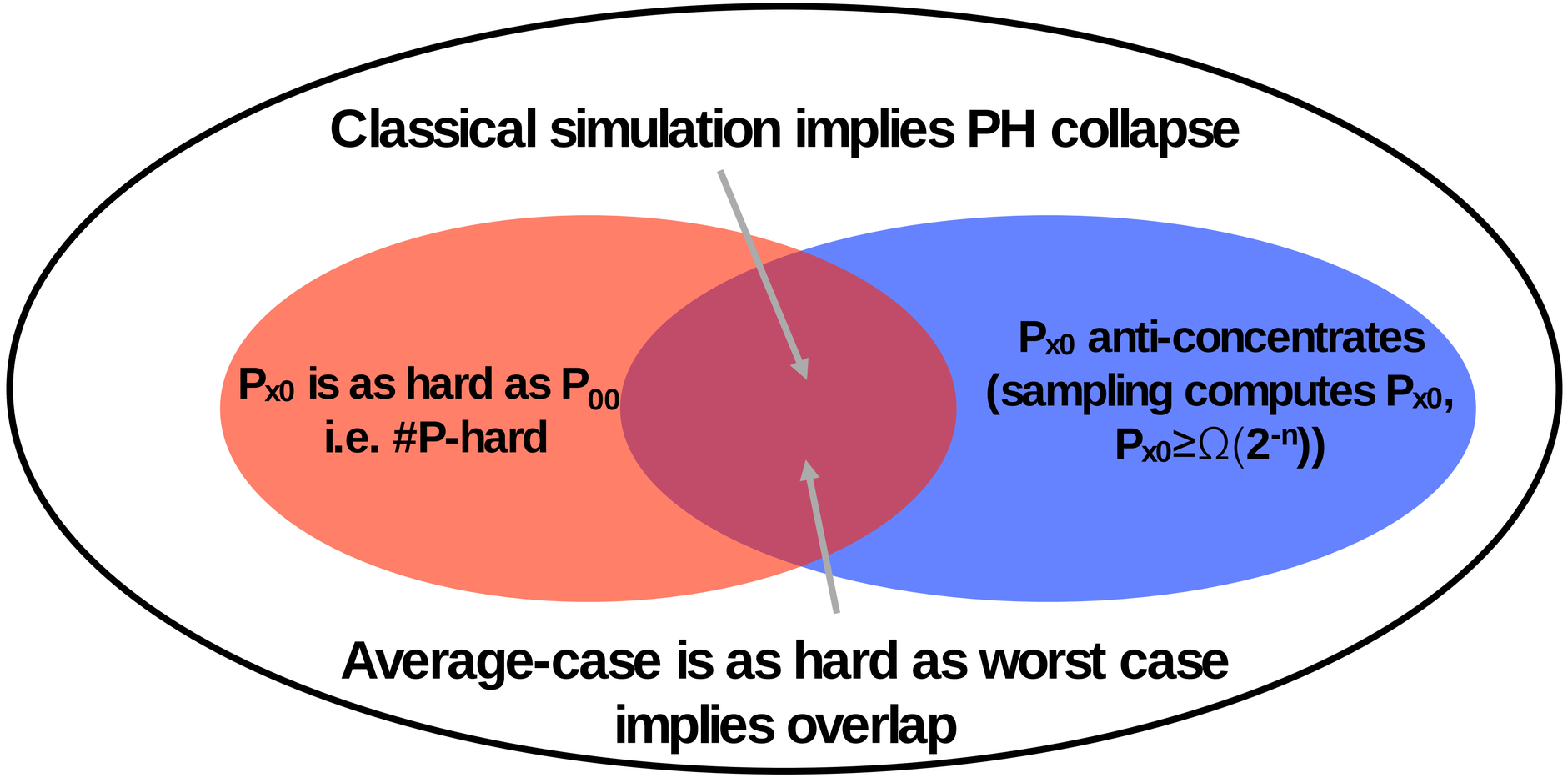
$$\Pr_{U_x \in F}[|\langle 0^n | U_x | 0^n \rangle|^2 \geq \alpha . 2^{-n}] \geq \beta$$

We call this property "anticoncentration".

Assume also that A can simulate the output of any U up to l_1 error $\epsilon = \frac{\alpha\beta}{8}$. Then Stockmeyer's algorithm gives a relative error approximation of ¼ +o(1) for a $\beta/2$ fraction of U.

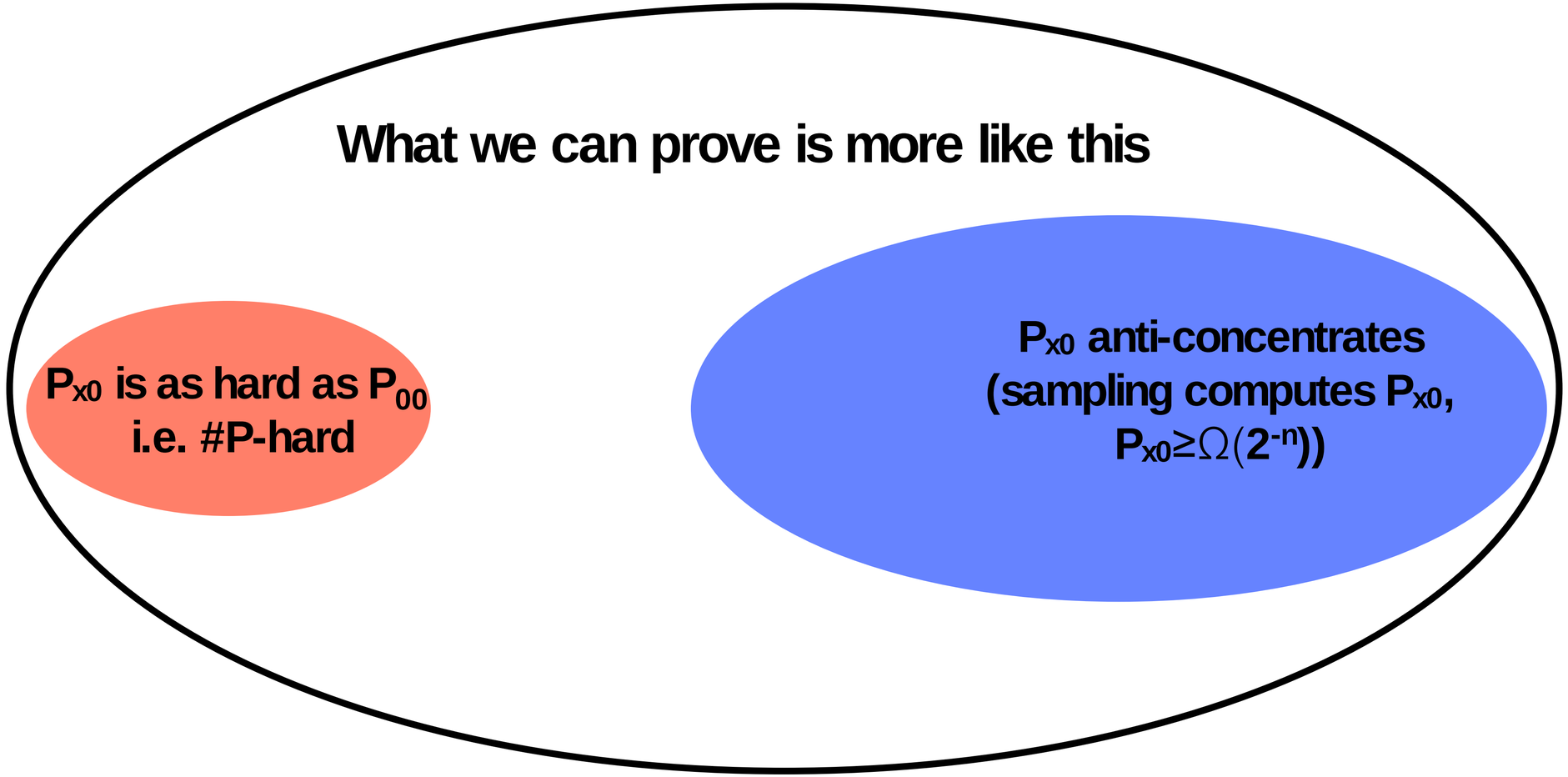
Random quantum circuit sampling arguments

E.g. some family of U_x where computing $P_{00} = |\langle 0^n|U_0|0^n\rangle|^2$ is #P-hard even up to relative error approximation in the *worst-case*



Random quantum circuit sampling arguments

E.g. some family of U_x where computing $P_{00} = |\langle 0^n|U_0|0^n\rangle|^2$ is #P-hard even up to relative error approximation in the *worst-case*



Random circuit sampling arguments

Challenge is to identify circuit families that:

1) Display anticoncentration on an output register “growing like n”.

2) Have #P-hard amplitudes in the worst-case. i.e. post-selected family is equivalent to postBQP.

3) Are sufficiently complex such that it is likely that random instances are also #P-hard.

4) As a bonus it would be nice to know which instances are likely to be classically hard so that we can estimate classical runtimes.

Anticoncentrating circuit families

Random circuit families might be hard to classically approximate.

Anticoncentration proof methods

Over the last few years a number of circuit families have been shown to anticoncentrate. The proof techniques fall into 3 categories:

1) Direct calculation.
   - For random choices over IQP circuits.

2) Using the theory of k-designs, and their connection to the Haar distribution.
   - Where “hard” circuits are randomly chosen circuits from either universal gate sets or conjugated Clifford circuits.

3) Use measurement/post-selection gadgets to demonstrate anticoncentration on a subset of output qubits.
   - Where the circuits are deterministically chosen and the randomness emerges from the measurement randomness.

Paley-Zygmund inequality

Typically we will want to demonstrate anti concentration on systems of n qubits, in which case we want to show that the following inequality is satisfied:

$$\Pr_{U_x \in F}[|\langle 0^n|U_x|0^n\rangle|^2 \geq \alpha.2^{-n}] \geq \beta$$

One method doing this is via the Paley-Zygmund inequality (R>0, 0<α<1):

$$\Pr\left[R \geq \alpha\mathbb{E}[R]\right] \geq (1-\alpha)^2 \frac{\mathbb{E}[R]^2}{\mathbb{E}[R^2]}$$

Where $R = |\langle 0|U_x|0\rangle|^2$ and the expectation is over the choice of U_x in F. The challenge is to bound the moments of R with respect to this choice.

Interestingly, it isn't too hard to see that if this choice is with respect to the Haar measure on SU(N) then we see anticoncentration directly.

k-designs and anticoncentation

If U_x is drawn from the Haar measure on $U(2^n)$ (or equivalently the Porter-Thomas distribution) then $\mathbb{E}[|\langle 0|U_x|0\rangle|^2] = 2^{-n}$ and $\mathbb{E}[|\langle 0|U_x|0\rangle|^4] = \frac{2}{2^n(2^n+1)}$. Substituting this directly into Paley-Zygmund:

$$\Pr[|\langle 0|U_x|0\rangle|^2 \geq \alpha 2^{-n}] \geq \frac{(1-\alpha)^2}{2}$$

Hence the Haar measure anticoncentrates.

Typical circuits on the Haar measure have exponential depth, hence they cannot generally be made – however for our purposes we only need agreement with the Haar measure up to the 2nd moment of the output distributions.

This can be achieved with either an exact, and it turns out, an approximate unitary 2-design.

Approximate k-designs and anticoncentation

Theorem (see Hangleiter et al 1706.03786v3 and Mann and Bremner '17):

Let U be drawn from an ϵ relative approximate k-design on the group U(N) then matrix elements of U anticoncentrate:

$$\Pr[|\langle 0|U_x|0\rangle|^2 \geq \alpha(1-\epsilon)2^{-n}] \geq \frac{(1-\alpha)^2(1-\epsilon)^2}{2(1+\epsilon)}$$

Furthermore, this can be done in depth $O(n \log 1/\epsilon)$. This follows from the results of Bradao, Harrow, and Horodecki '16.

Similar results have also been obtained with respect to "conjugated Clifford circuits", see Bouland, Fitzsimmons, and Koh 1709.01805.

IQP Sampling

If the “average case” complexity of relative error approximations to either:

1) The complex temperature Ising model partition functions, or

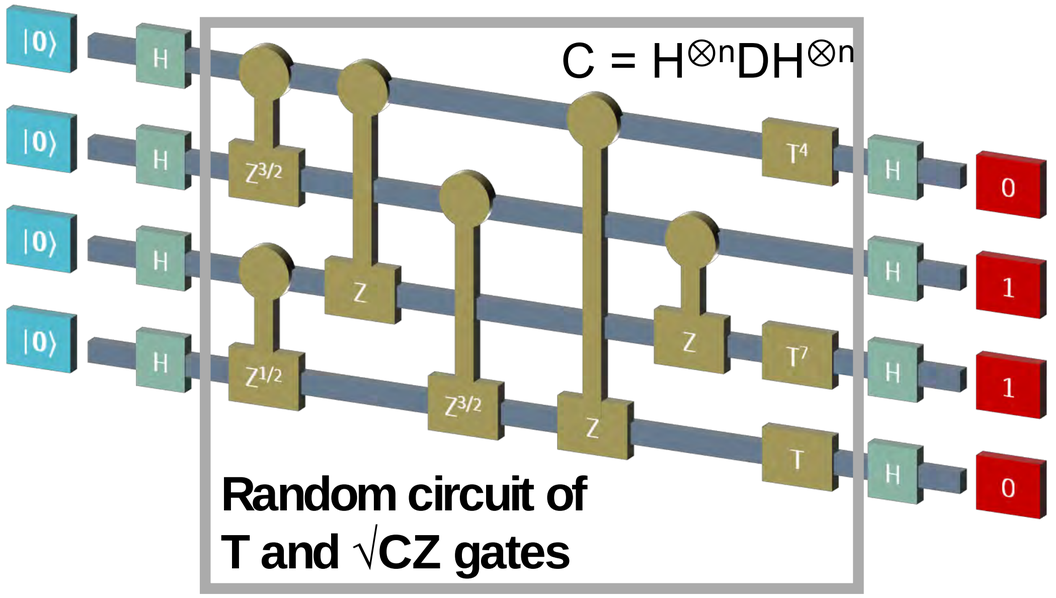
2) The gap of degree 3 polynomials*

is #P-hard, then quantum computers cannot be efficiently classically simulated to within *constant variation distance* without a collapse of the PH.

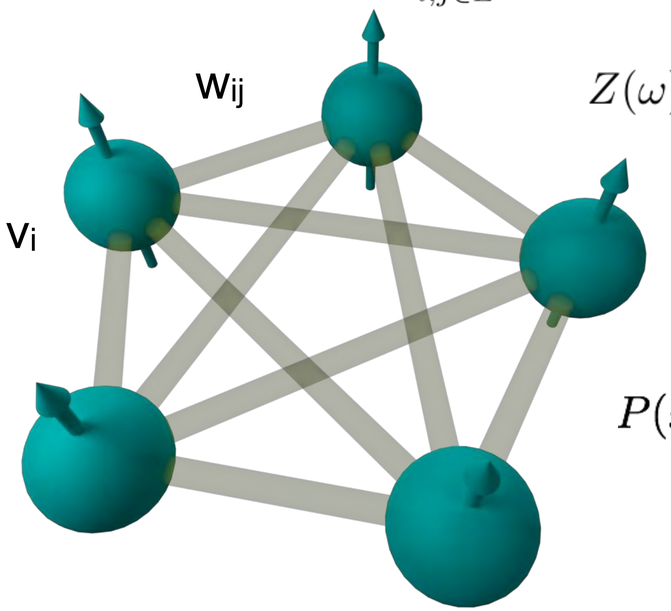
(BMS, Phys. Rev. Lett. **117**, 080501 (2016), arXiv:1504.07999)

This has been improved to sparse Ising models with O(n log n) interactions.

(BMS Quantum **1**, 8 (2017), arXiv:1610.01808).



Ising model: $H = \sum_{i,j \in E} w_{ij} X_i X_j + \sum_{i \in V} v_i X_i$



$$Z(\omega) = \mathrm{Tr}\left[\omega^H\right], \omega = e^{i\frac{\pi}{8}}$$

$$P(x) = |\langle x|e^{i\frac{\pi}{8}H}|0\rangle^{\otimes n}|^2 = \frac{|Z(e^{i\frac{\pi}{8}})|^2}{2^n}$$

Post-classical family 2: Degree 3 polynomials

$$f(x) = \sum_{i,j,k} \alpha_{i,j,k} x_i x_j x_k + \sum_{i,j} \beta_{ij} x_i x_j + \sum_i \gamma_i x_i \mod 2$$

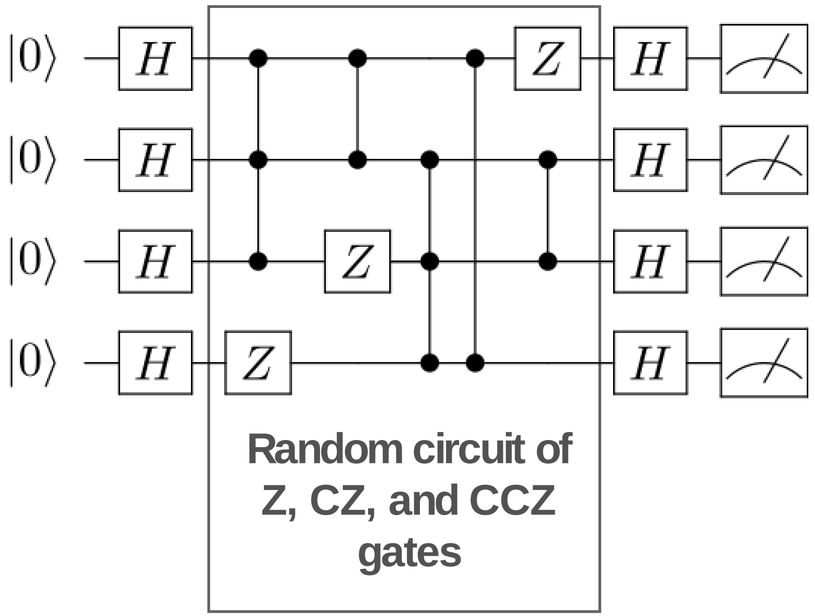
$\alpha_{ijk}, \beta_{ij}, \gamma_i \in$ **{0,1} randomly chosen.**

Sample from $U_f|0\rangle^{\otimes n}$ - the fourier transform of f(x)

*If conjecture (2) is true then there is no efficient classical algorithm that can sample from any R(**x**) such that:*

$||P(\mathbf{x}) - R(\mathbf{x})||_1 \leq 1/192$

(Unless the PH collapses)



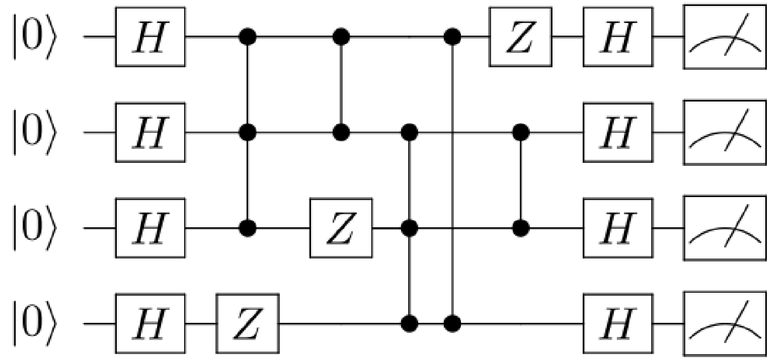
Polynomial gaps and IQP: Conjecture 2

$$f(x) = \sum_{i,j,k} \alpha_{i,j,k} x_i x_j x_k + \sum_{i,j} \beta_{ij} x_i x_j + \sum_i \gamma_i x_i \mod 2$$

$$\mathrm{ngap}(f) = \frac{1}{2^n} \left(|\{x : f(x) = 0\}| - |\{x : f(x) = 1\}| \right)$$

These amplitudes are proportional to the gap of degree-3 polynomials over F_2, long known to be #P-hard to compute.

$$|\langle 0|^{\otimes n} \mathcal{C}_f |0\rangle^{\otimes n}|^2 = \frac{\mathrm{gap}(f)^2}{2^n}$$



If $\alpha_{ijk}, \beta_{ij}, \gamma_i \in \{0,1\}$ are randomly chosen.

- **Then IQP sampling gives (with constant probability):**

$$\left| A_\times - \mathrm{ngap}(f)^2 \right| \leq \left(\frac{1}{4} + o(1) \right) \mathrm{ngap}(f)^2$$

- **If ngap(f)^2 is #P-hard on a constant fraction of instances then classical simulation of IQP circuits leads to a collapse of the PH.**
- **This parameter choice leads to #P-hardness of the *worst-case* complexity of ngap(f). See our paper.**

The Google proposal

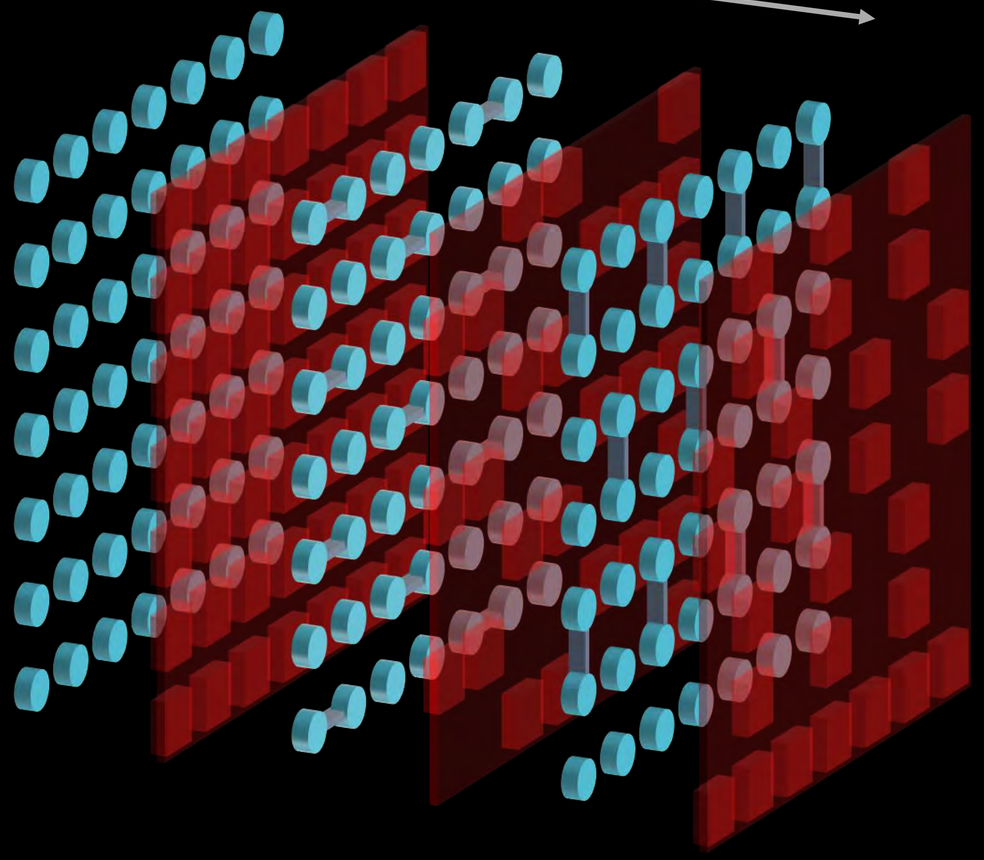
Low-depth quantum circuit sampling where gates are randomly drawn from CZ, T, $X^{1/2}$, $Y^{1/2}$ up to at least depth $O(n^{1/2})$.

Classical hardness is based on the following assumptions:

(1) That the output probabilities of these probability distributions “anti-concentrate” at this depth. This has been heavily numerically tested, and proven for higher depth.

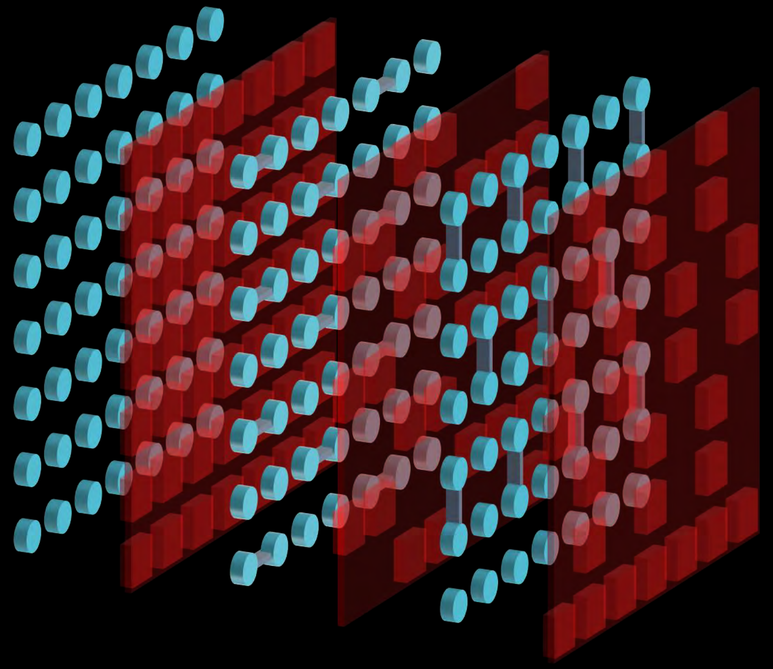
(2) That the average case complexity of the (complex) partition function of quasi 3d Ising models is as hard as the worst-case complexity.

time/depth ~ $O(n^{1/2})$ > 40 layers of gates each with infidelity ~1/(circuit size)



Boixo et al arXiv:1608.00263, QIP ‘17

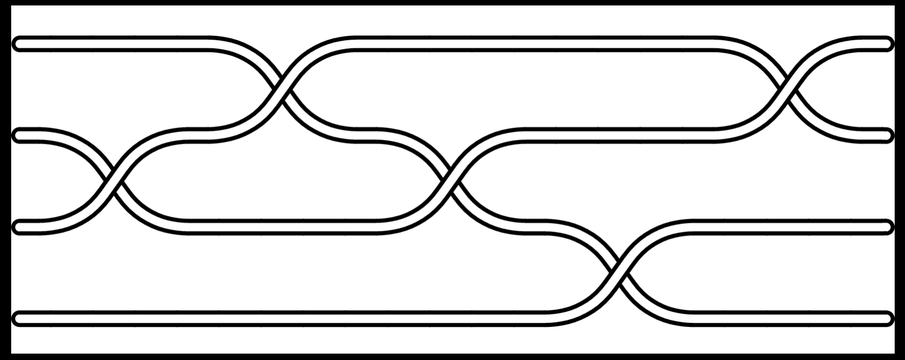
Random circuits and Jones polynomials



The Google proposal can be formalized in terms of approximate unitary 2 designs (Hangleiter et al arXiv:1706.03786).

The complexity of simulating approximate unitary designs can be related to the complexity of *relative error* approximations to Jones polynomials over randomly chosen braids.

This allows for a natural conjecture that in which the complexity scales simply with the size of the circuit – in this case depth ~ the number of braids.



Mann and Bremner arXiv:1711.00686

	#P-hard worst case/ multiplicative	"anti-concentration"	#P-hard exact average case
Quantum circuits	Y	?	Y (Fefferman and Umans 1507.05592)
Boson Sampling	Y (AA '10)	?	Y (AA '10)
IQP Sampling, complete graph $O(n^2)$ gates	Y (BMS 1504.07999)	Y (BMS 1504.07999)	?
IQP Sampling, sparse graph $O(\sqrt{n} \log n)$ depth n.n. gates - optimal	Y	Y (BMS 1610.01808)	?
O(1) depth n.n. Universal gates	Y (Terhal and DiVincenzo, quant-ph/0205133)	Y? (Gao et al 1607.04947, Bermejo-Vega et al 1703.00466, Miller et al 1703.11002)	?
O(1) depth n.n. IQP	Y (BJS 1005.1407, Goldberg and Guo 1409.5627)	? (see box above)	?
$O(\sqrt{n} \log^2 n)$ depth n.n. Haar random gates	Y, ? (From above)	Y, ? (Brown and Fawzi, 1307.0632)	?
Random circuits from Porter-Thomas/t-designs	Y, Boixo et al 1608.00263, Mann and Bremner 1711.00686	Y O(n) depth Hangleiter 1706.03786, Mann and Bremner 1711.00686 . ? $O(n^{1/2})$ (Boixo et al 1608.00263),	?
Commuting 2-local gates	Y (Bouland, Mančinska, and Zhang, QIP'16)	Y, ?	?
Clifford circuits	N	Y, ? (Brown and Fawzi, 1307.0632)	N
Clifford with product input	Y (Jozsa and Van Nest, 1305.6190/Koh 1512.07892), Bouland 1709.01805	Y, ? (Brown and Fawzi, 1307.0632) Y (Bouland 1709.01805)	?

	#P-hard worst case/ multiplicative	"anti-concentration"	#P-hard exact average case
Quantum circuits	Y	?	Y (Fefferman and Umans 1507.05592)
Boson Sampling	Y (AA '10)	?	Y (AA '10)
IQP Sampling, complete graph $O(n^2)$ gates	Y (BMS 1504.07999)	Y (BMS 1504.07999)	?
IQP Sampling, sparse graph $O(\sqrt{n} \log n)$ depth n.n. gates - optimal	Y	Y (BMS 1610.01808)	?
O(1) depth n.n. Universal gates	Y (Terhal and DiVincenzo, quant-ph/0205133)	Y? (Gao et al 1607.04947, Bermejo-Vega et al 1703.00466, Miller et al 1703.11008)	?
O(1) depth n.n. IQP	Y (Bremner, Montanaro, Shepherd 1504.07999, Gosset and Nagaj 1409.5627)	? (see box above)	?
$O(\sqrt{n} \log^2 n)$ depth n.n. Haar random gates	Y, ? (From above)	Y, ? (Brown and Fawzi, 1307.0632)	?
Random circuits from Porter-Thomas/t-designs	Y, Boixo et al 1608.00263, Mann and Bremner 1711.00686	Y O(n) depth Hangleiter 1706.03786, Mann and Bremner 1711.00686 . ? $O(n^{1/2})$ (Boixo et al 1608.00263),	?
Commuting 2-local gates	Y (Bouland, Mańcinska, and Zhang, QIP'16)	Y, ?	?
Clifford circuits	N	Y, ? (Brown and Fawzi, 1307.0632)	N
Clifford with product input	Y (Jozsa and Van Nest, 1305.6190/Koh 1512.07892), Bouland 1709.01805	Y, ? (Brown and Fawzi, 1307.0632) Y (Bouland 1709.01805)	?

None of these models have made any progress on the #P-hard relative error in the average case.

Any proof of this is likely to require non-relativising techniques – see Aaronson and Chen arXiv:1612.05903

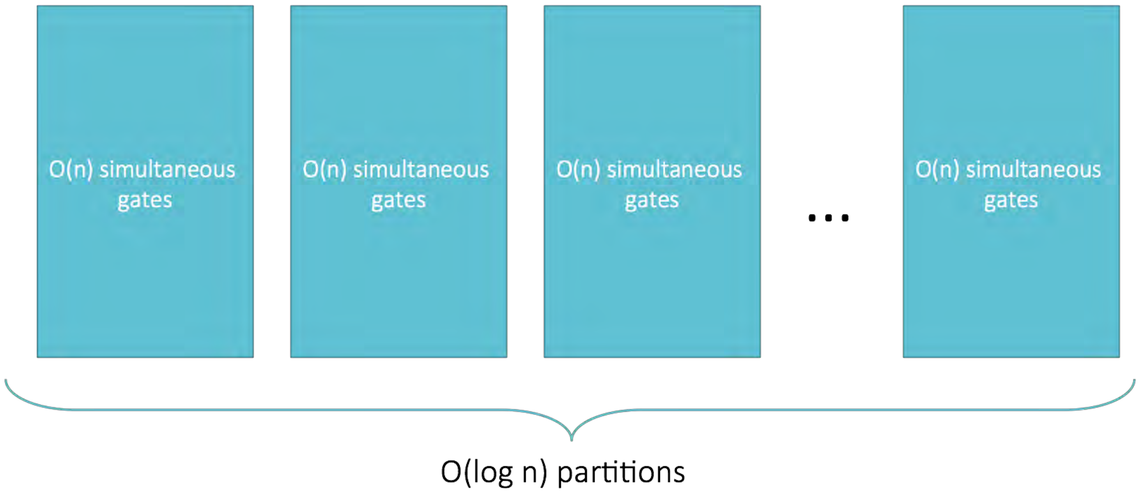
Time-space tradeoffs

Where is the quantum frontier?

Sparse IQP Sampling in ~ $n^{1/2}$ depth circuits

(1) Prove that *sparse* IQP circuits anticonentrate, demonstrating that they cannot be classically simulated without a collapse in the PH, assuming #P-hardness of approximations to sparse, complex, Ising models.
- This construction has O(n log n) 2 qubit gates. ~ O(log n) gates per qubit.

(2) Use edge colouring algorithms to decompose circuit into O(log n) partitions of simultaneous gates



(3) Via standard results on sorting networks [2] each of these partitions can be implemented with depth $O(n^{1/2})$ in a universal nearest neighbour architecture.

This leads to an overall depth of $O(n^{1/2}\log n)$.

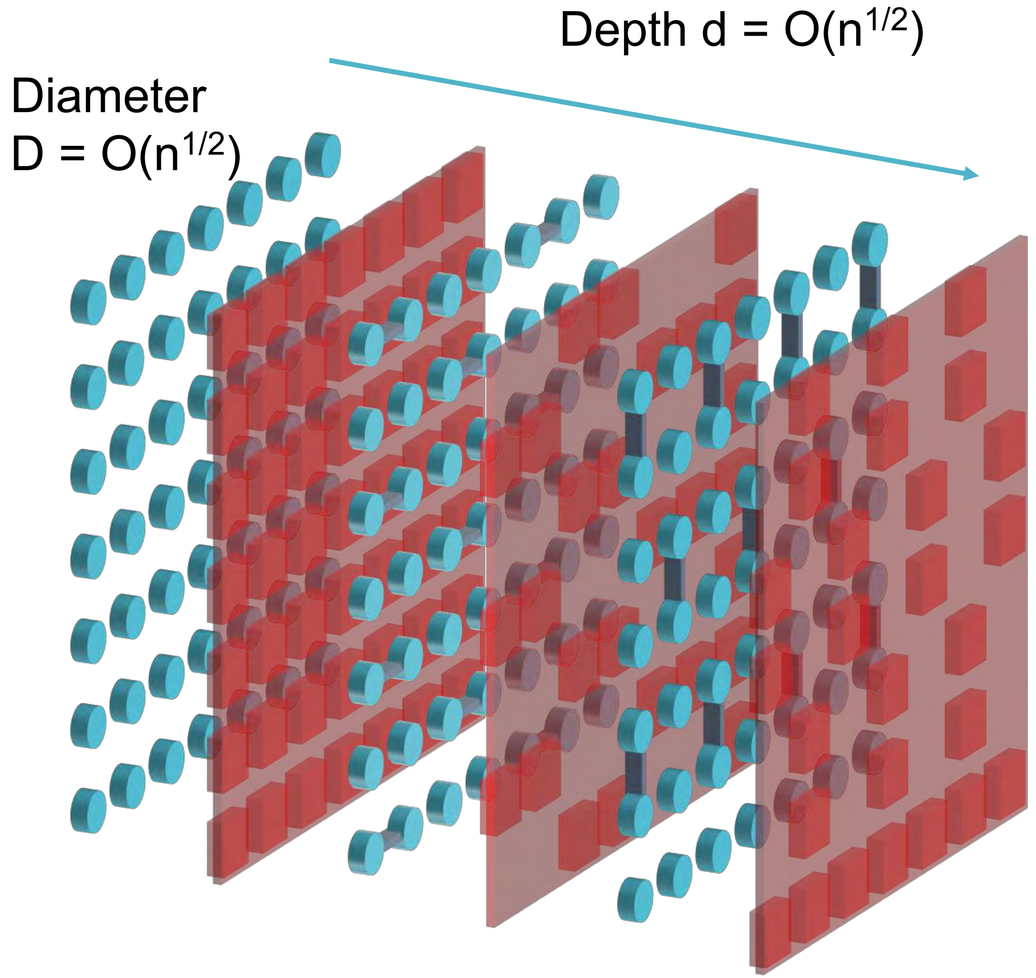
Depth optimality from geometry for sparse counting problems

Tensor network algorithms can compute $p = |\langle 0^n|U|0^n\rangle|^2$ in time $\min(O(2^n), O(2^{dD}))$, where d is depth and D is the diameter of the circuit.

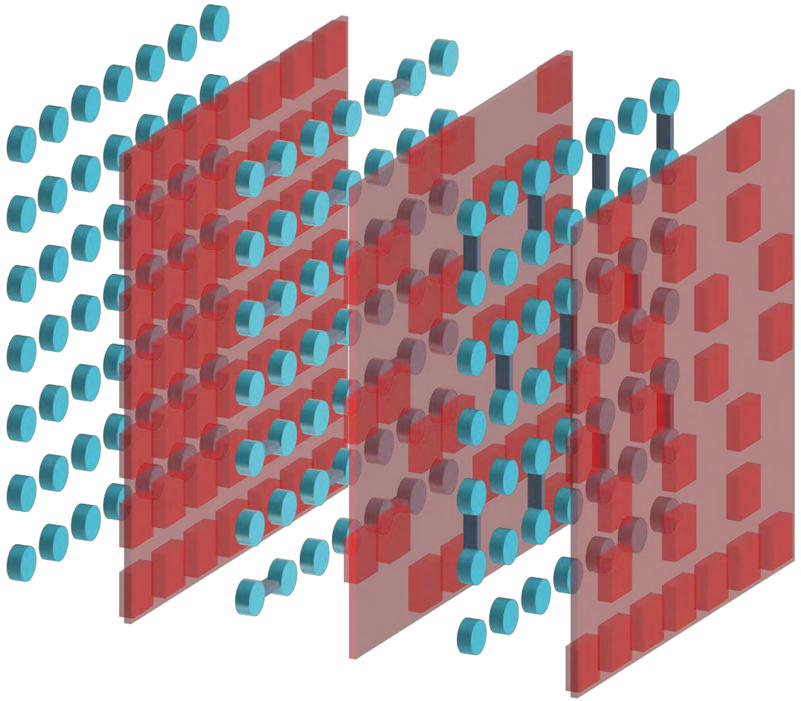
E.g.:
If there were a sub $d = O(n^{1/2})$ circuit for sparse IQP circuits p could be computed in sub exponential time – contradicting the fact that sparse Tutte polynomials/Ising models are hard for the exponential time hypothesis.

Hence bound of $d = O(n^{1/2}\log n)$ is essentially optimal for IQP circuits.

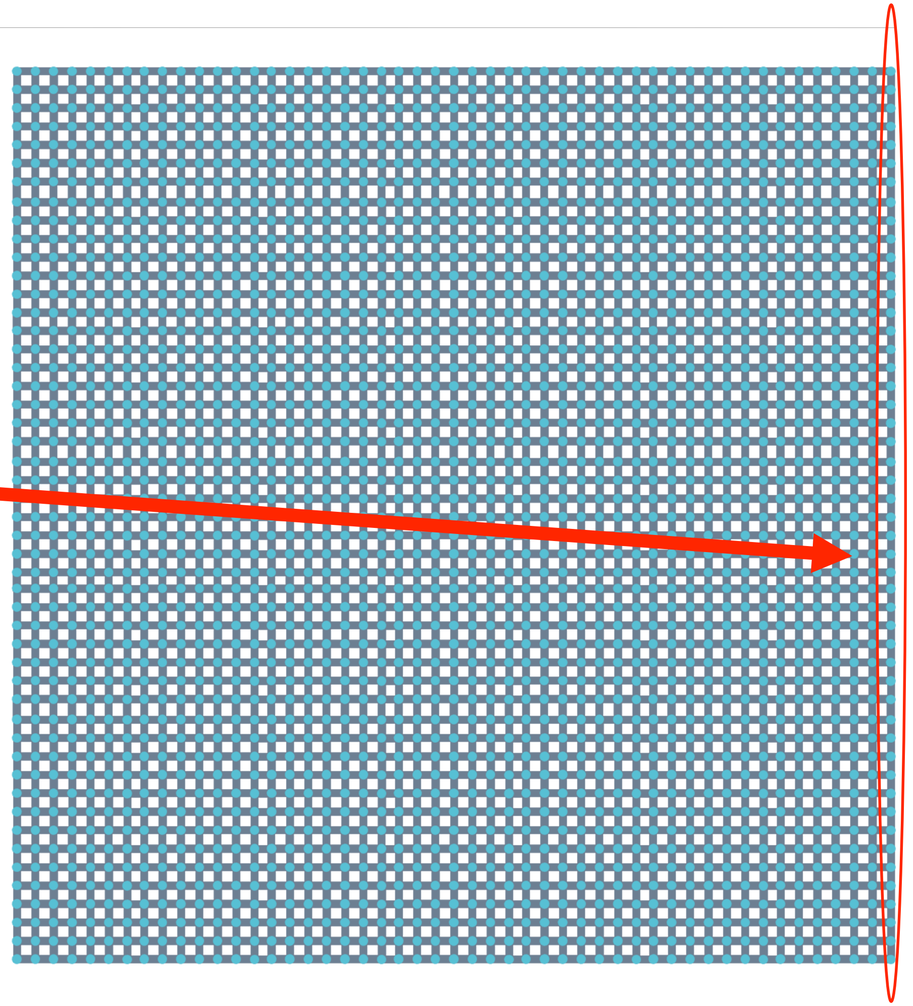
Note that the Google proposal (arXiv:1608.00263) scales larger than $d = O(n^{1/2})$.



Complexity of low-depth, structured circuits, quantum simulators, and MBQC



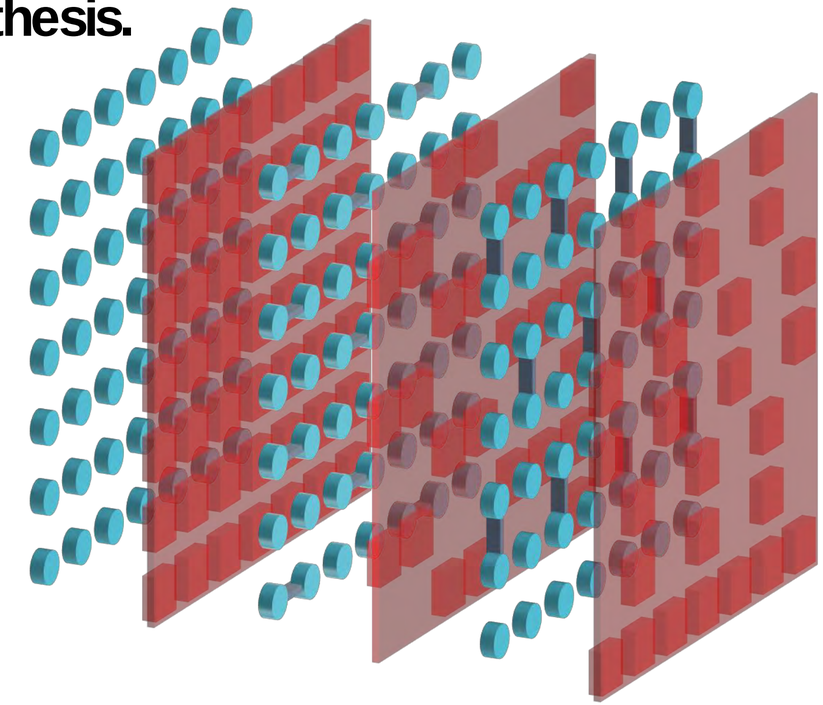
via



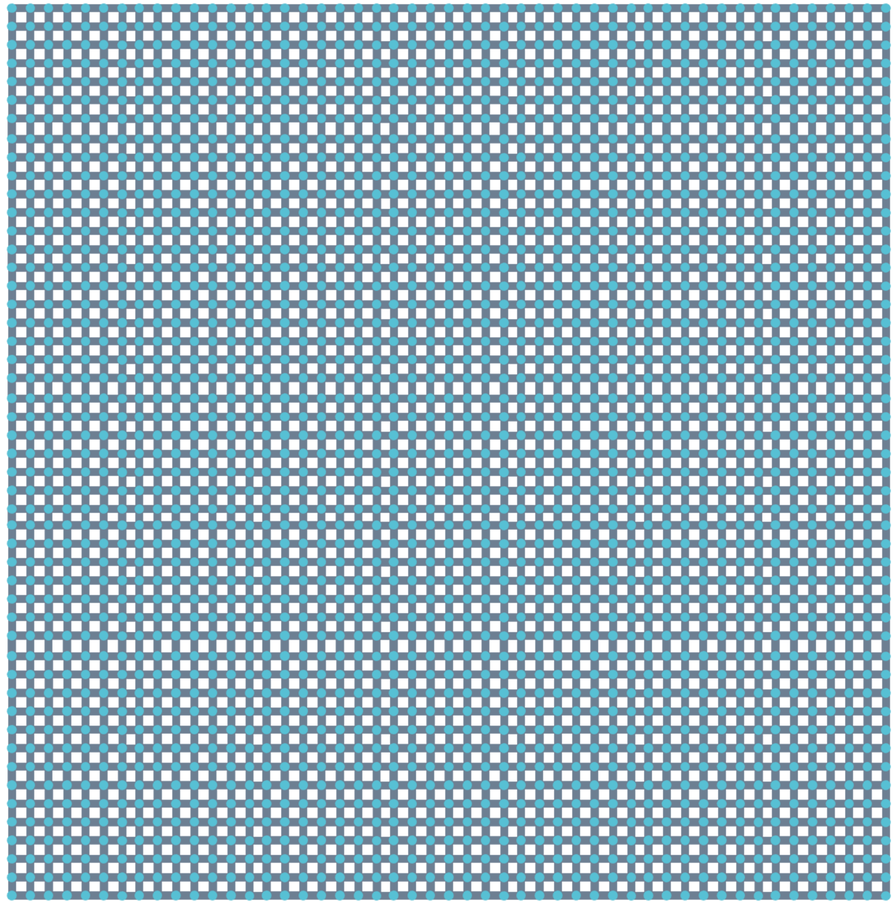
Gao et al 1607.04947, Bermejo-Vega et al 1703.00466, Miller et al 1703.11002 all demonstrated that either random IQP or approximate 2-designs/PT distributions can appear across a subset of qubits given appropriate initial graph states and measurement choices.

Time-space tradeoffs

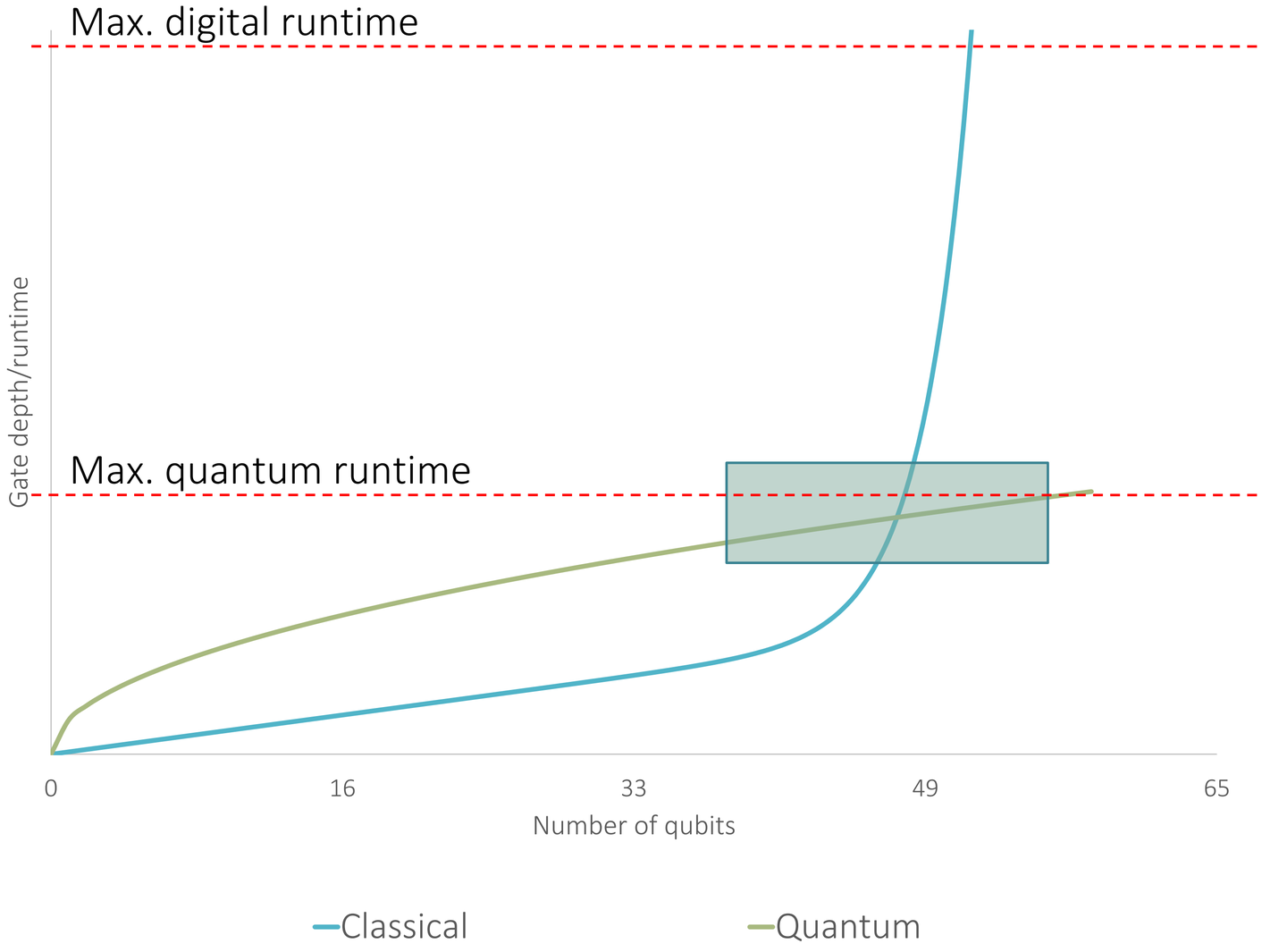
If the circuit depth in a 2D architecture is sub $n^{1/2}$ then we know that typical circuits will not be solving “the hardest” instances of #P**-hard problems (scaling like n) without a violation of the exponential time hypothesis.**



VS



Below $n^{1/2}$ depth we begin to trade qubits vs gates. For example if we go to constant depth we must have a polynomial increase in the number of qubits.



*Nothing on this plot is to scale!

Where is the "quantum frontier"?

Depends on the amount of noise, the model, and the best classical simulation algorithms.

- "Around 50 qubits" for the Google model. See Boixo et al '16, Boixo et al 1712.0538, and Haener and Steiger 1704.01127.

- Around 60-70 qubits for sparse IQP (see v4 of Google paper).

- Above 50 photons for BosonSampling based on numerical testing with realistic loss parameters, see Neville et al 1705.00686, Clifford^2 1706.01260 later in this conference.

Noisy systems and classical simulation

Where is the quantum frontier, again?

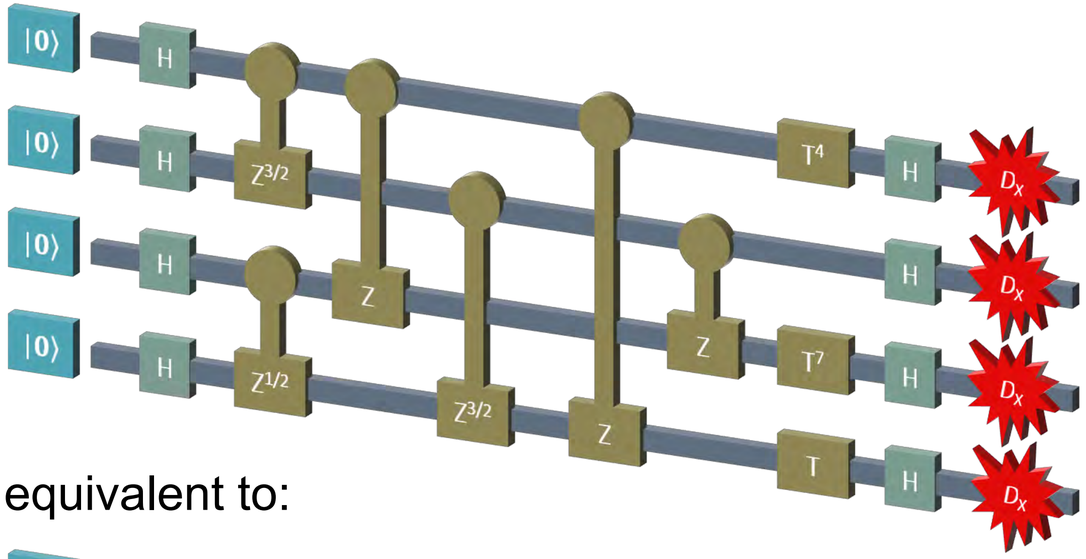
Noisy IQP simulation (BMS arXiv:1610.01808)

Anticoncentrating IQP circuits with constant-rate measurement depolarising noise can be classically simulated with runtime $n^{O(\log(\alpha/\delta)/\varepsilon)}$ where α is a constant measuring the amount of anti-concentration, δ is the level of accuracy and ε is the depolarisation rate.

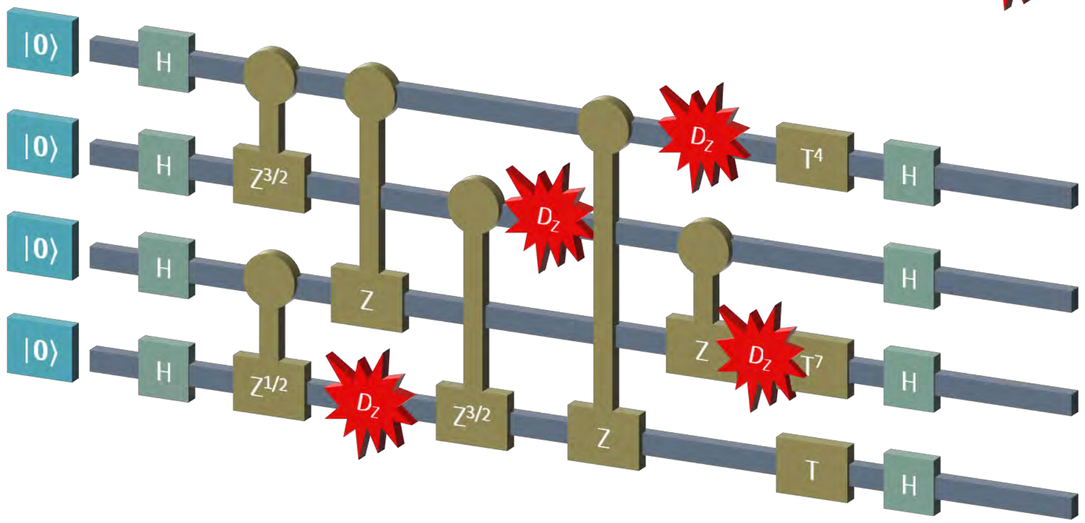
Such noisy circuits are well outside the constant 1-norm additive error scenario - the l_1 distance grows like O(n) for this error model.

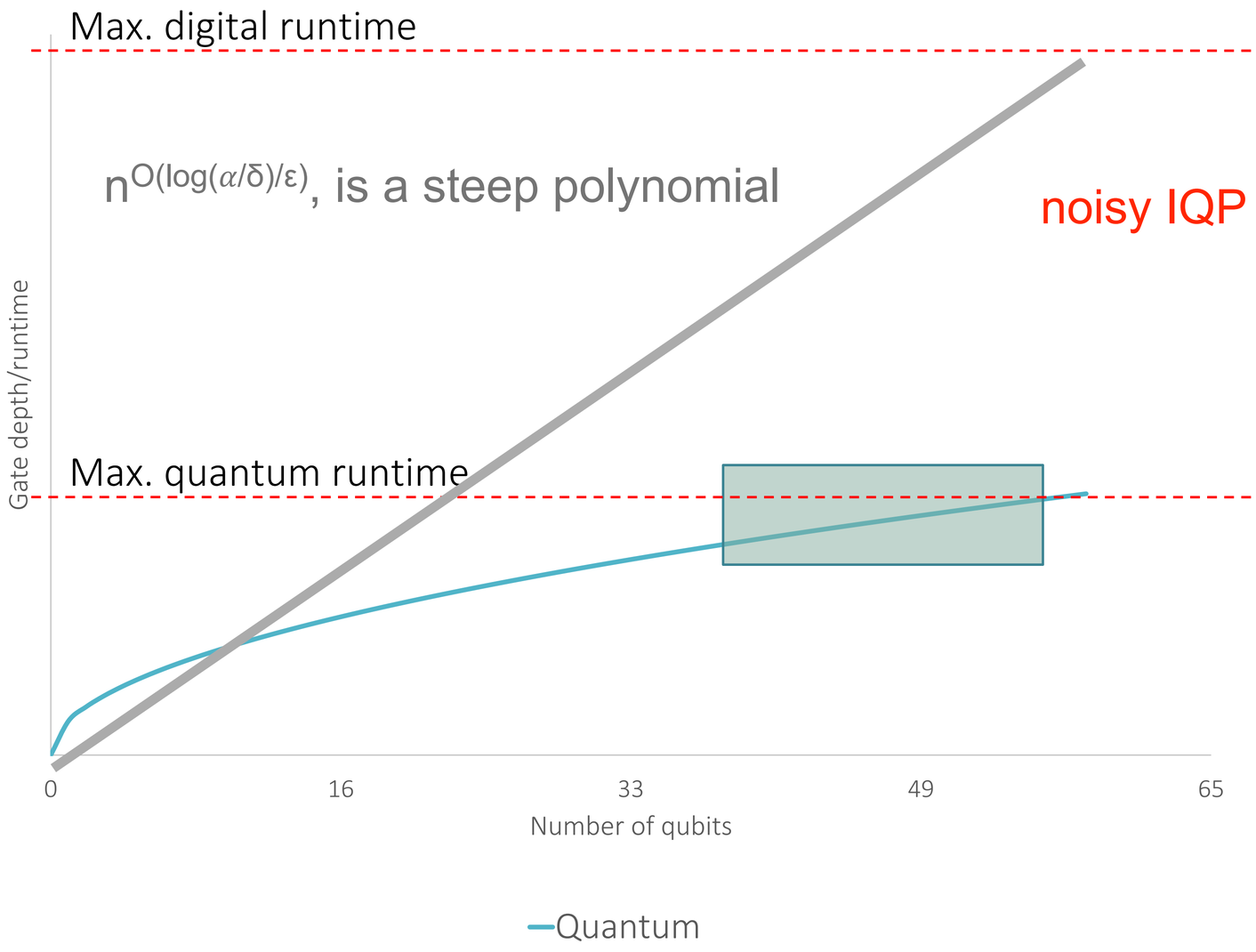
In the regime where we have a quantum advantage $\epsilon \leq n^{-1}$ this runtime is necessarily exponential.

This can be extended to the Google model (1706.08913, 1708.01875) and also holds for Simon's problem!



equivalent to:





*Nothing on this plot is to scale!

Noise and computational supremacy without error correction

Aim: Perform a quantum computation that cannot be performed classically in any reasonable amount of time.

Key issues:

- Are quantum computers more powerful than classical computers?

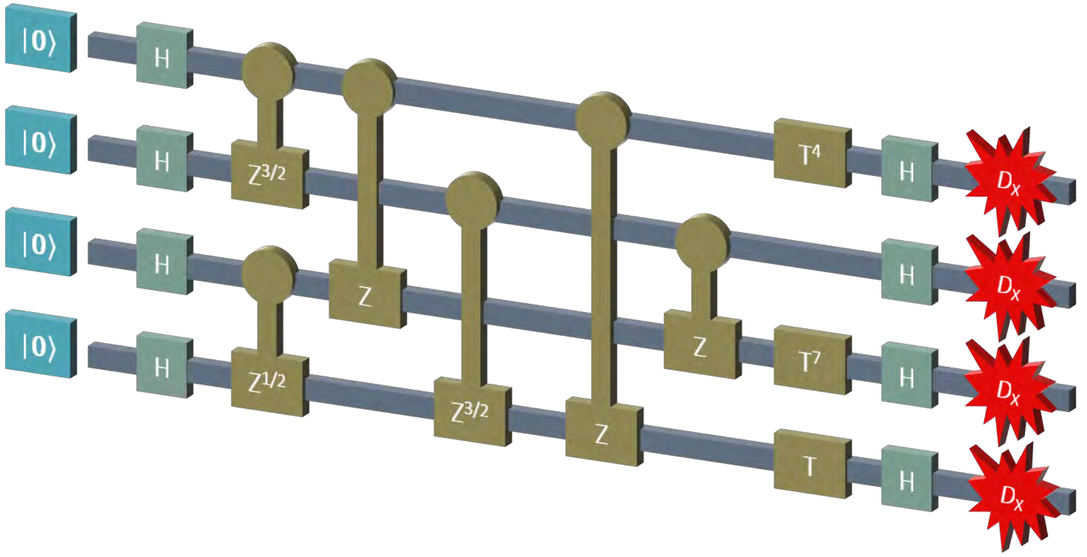
- For which computations do the classical and quantum runtimes diverge?

- Can we achieve quantum computational supremacy without fault tolerance?

Simulating noisy IQP circuits

Ideal: $p(x) = |\langle x|H^{\otimes n}DH^{\otimes n}|0\rangle|^2$, Noisy: p_n

Goal: Sample from p_n' such that $\|p_n - p_n'\|_1 \leq \delta$



Key facts:

- **Noisy system is far from the ideal, $\|p - p_n\|_1 \sim O(n)$**
- **There is a simple description of the effect of this noise in the Fourier transform basis:**

$$\hat{p}_n(s) = (1-\epsilon)^{|s|}\hat{p}(s)$$

- **This noise model is equivalent to single-qubit dephasing throughout the circuit (with different rates).**

$$\mathcal{D}_\epsilon = (1-\epsilon)\rho + \epsilon\frac{I}{2}$$
$$\equiv (1-\epsilon)\rho + \epsilon X\rho X = \mathcal{D}_X$$

Simulating noisy IQP circuits

3 Steps:

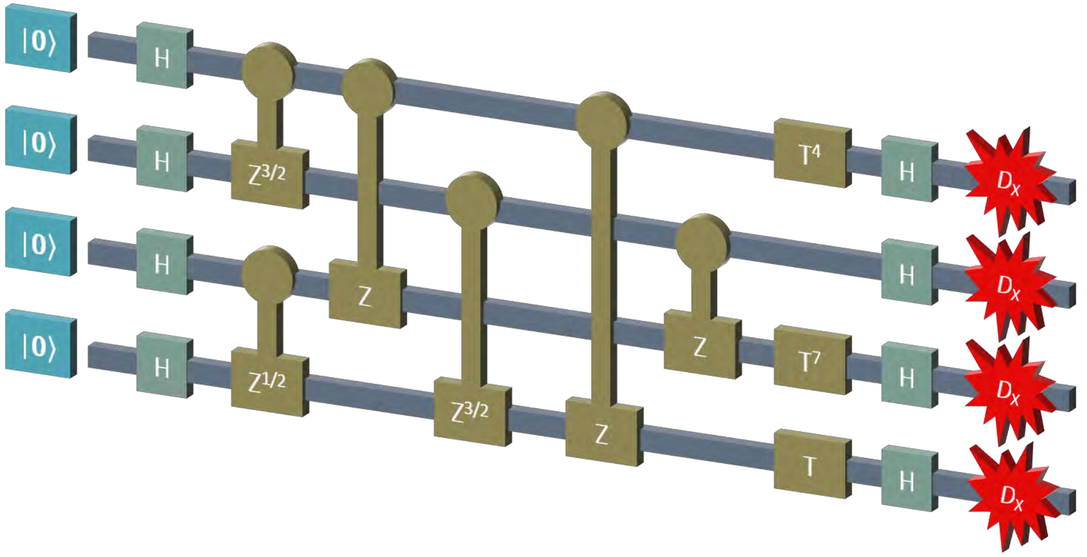
(1) Calculate a description of a function q_n with O(poly n) Fourier coefficients that approximates p_n such that $\|q_n - p_n\|_1 \leq \delta$.

- **For $|s| \leq O(\log((\alpha/\delta)/\varepsilon))$, $\hat{q}_n(s) = (1-\epsilon)^{|s|}\hat{p}'(s)$**
- **Else, $\hat{q}_n = 0$**
- **Compute estimate of the F.T. of p in time $n^{O(\log(\alpha/\delta)/\varepsilon)}$**

$$|\hat{p}'(s) - \hat{p}(s)| \leq O(\delta n^{-O(\log(\alpha/\delta)\epsilon)})2^{-n}$$

(2) Show we can calculate all the marginals of q_n efficiently.

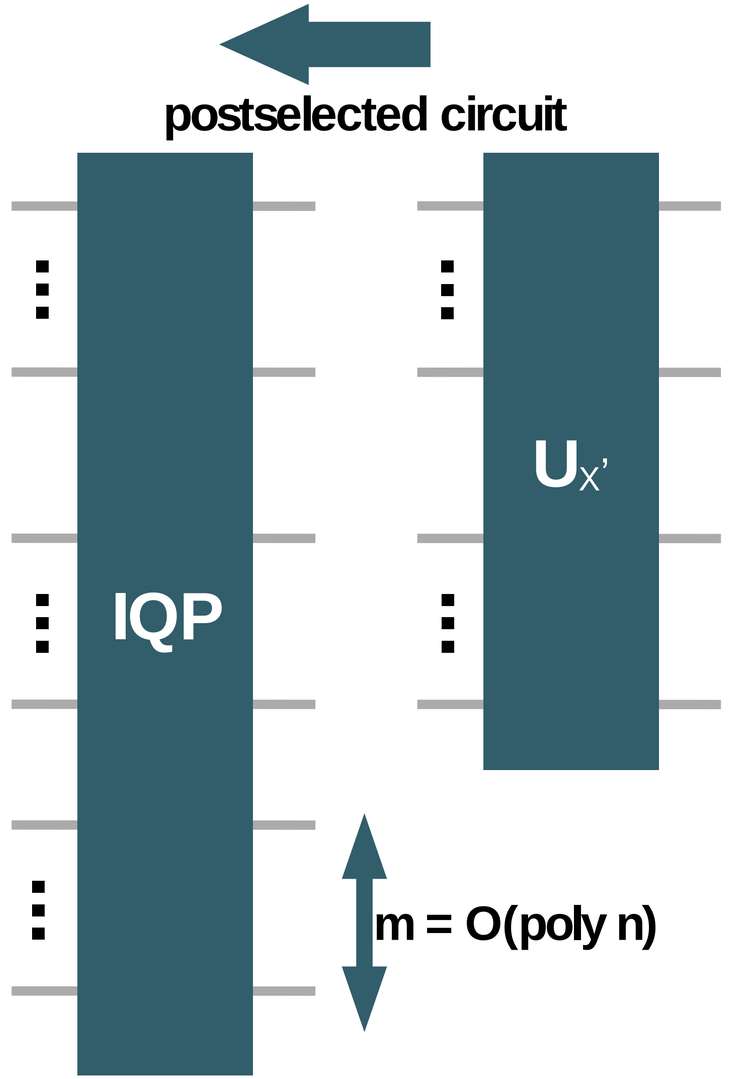
(3) This allows us to sample from p_n' such that:
$\|p_n' - p_n\|_1 \leq O(\delta)$



$$\mathcal{D}_\epsilon = (1-\epsilon)\rho + \epsilon\frac{I}{2}$$
$$\equiv (1-\epsilon)\rho + \epsilon X\rho X = \mathcal{D}_X$$

Classical simulation of noisy chaotic quantum circuits

- Yung and Gao arXiv:1706.08913 extended the noisy IQP simulation algorithm to “chaotic quantum circuits”, i.e. the Google proposal.
- The algorithm involves converting a chaotic circuit to a random, anticoncentrated, IQP circuit.
- This process allows errors on gates to be “teleported” to the “end” of the IQP circuit - allowing simulation of random Pauli-errors on the chaotic circuit.
- Runntime is $(n+m)^{O(\log(\alpha/\delta)/\varepsilon))}$ for a circuit of m gates and n qubits.

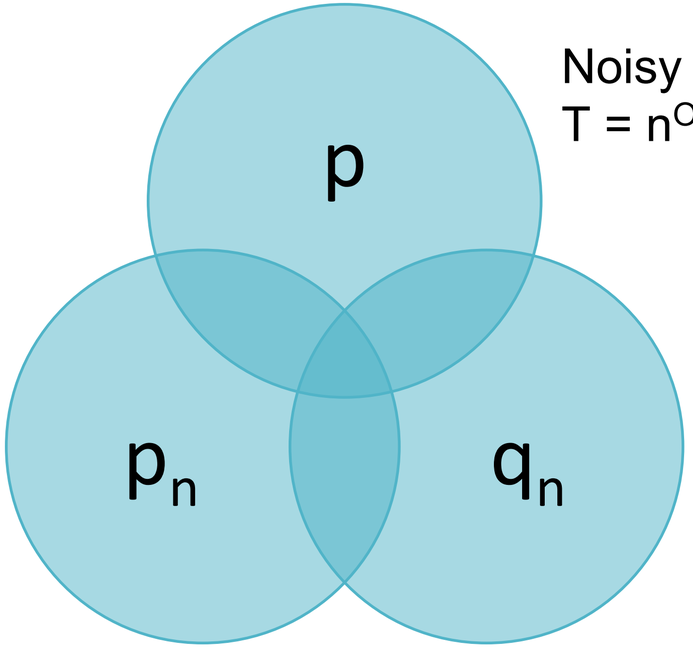


$$P_{IQP}(x,x') = P_{qc}(x|U_{x'})P(x')$$

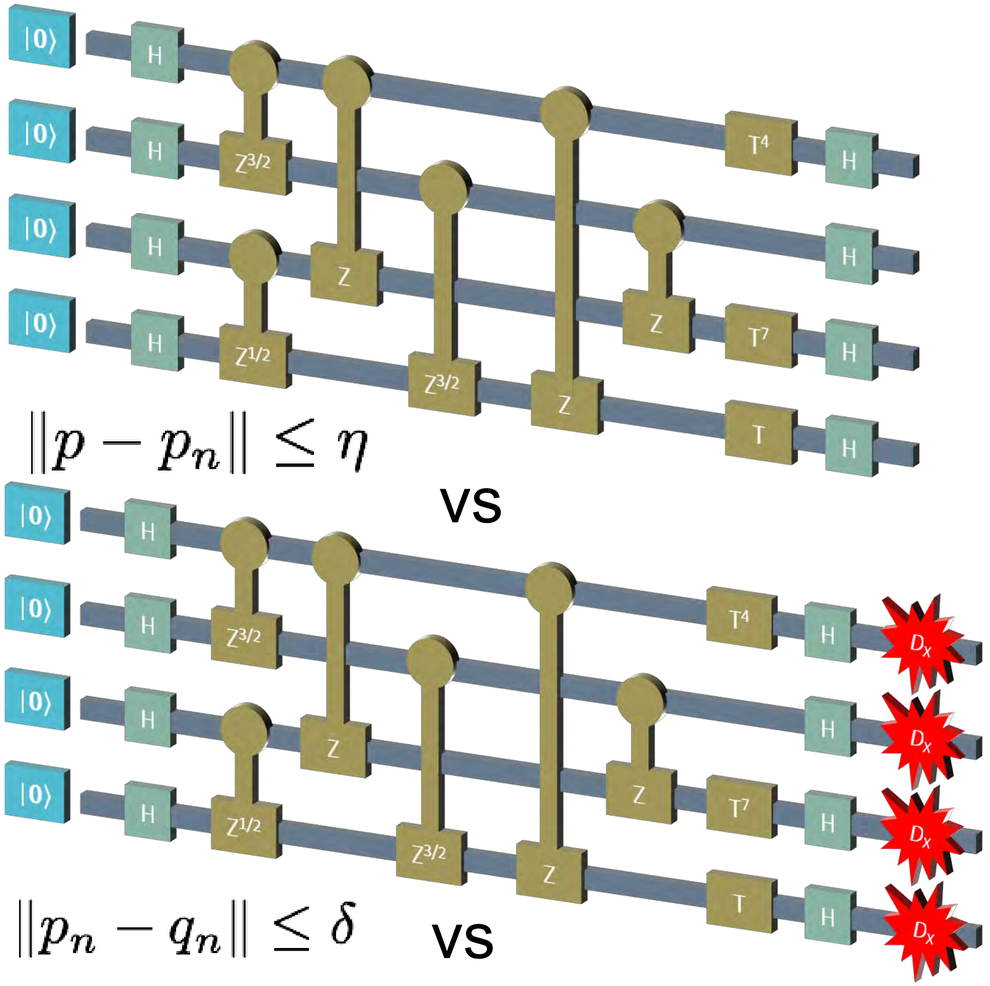
$$P_{IQP}(x,x') = \frac{1}{2^m}|\langle x|U_{x'}|\psi_{in}\rangle|^2 = \frac{1}{2^m}P_{qc}(x|U_{x'})$$

Bad runntimes are a feature arXiv:1708.01875

ε < 1/n



Noisy simulation runtime
$T = n^{O(\log(\alpha/\delta)/\varepsilon)} = O(n^n)$

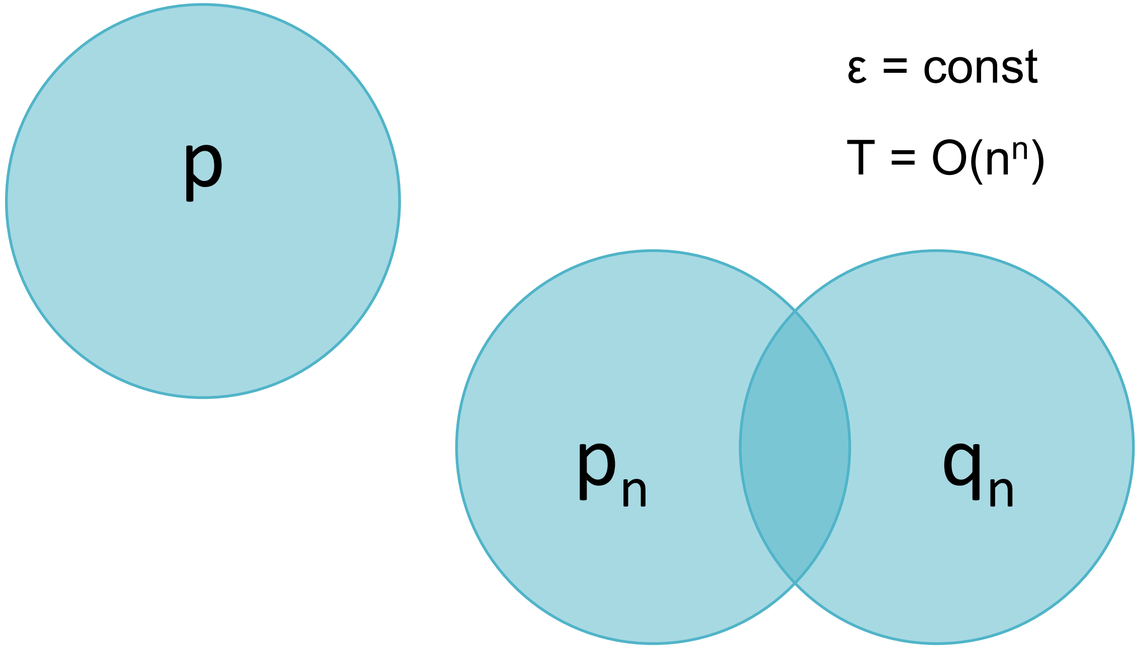


The distance between $||p-p_n|| \sim n\varepsilon$, and so to get within a "constant" total variation distance $\varepsilon < 1/n$ or you need error correction.

$\varepsilon < 1/n$ leads to a runntime of $O(n^n)$, considerably more than the exact simulation runntime $O(2^n)$.

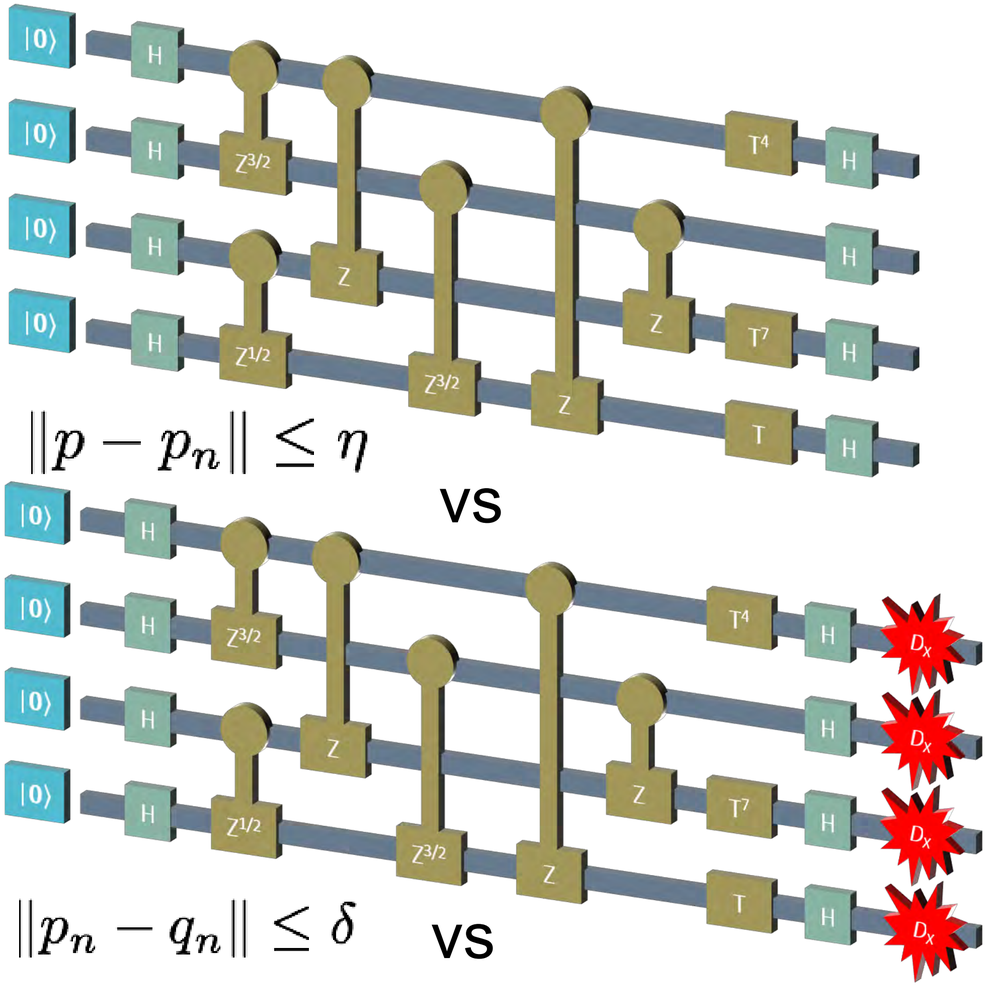
Experimental "goal" is to have gate/qubit error rates below O(1/(n+m)) - in Google's case something like this can be achieved if there is an upper bound of 50 qubits and depth 40.

Bad runntimes are a feature arXiv:1708.01875



ε = const

T = $O(n^n)$



The noisy simulation runntime is $n^{O(\log(\alpha/\delta)/\varepsilon))}$ which comes from the number of terms required to be computed to have $||p_n\text{-}q_n|| \leq \delta$.

The distance between $||p\text{-}p_n|| \sim n\varepsilon$, and so to get within a “constant” total variation distance ε > constant (independent of the system size) this algorithm is efficient.

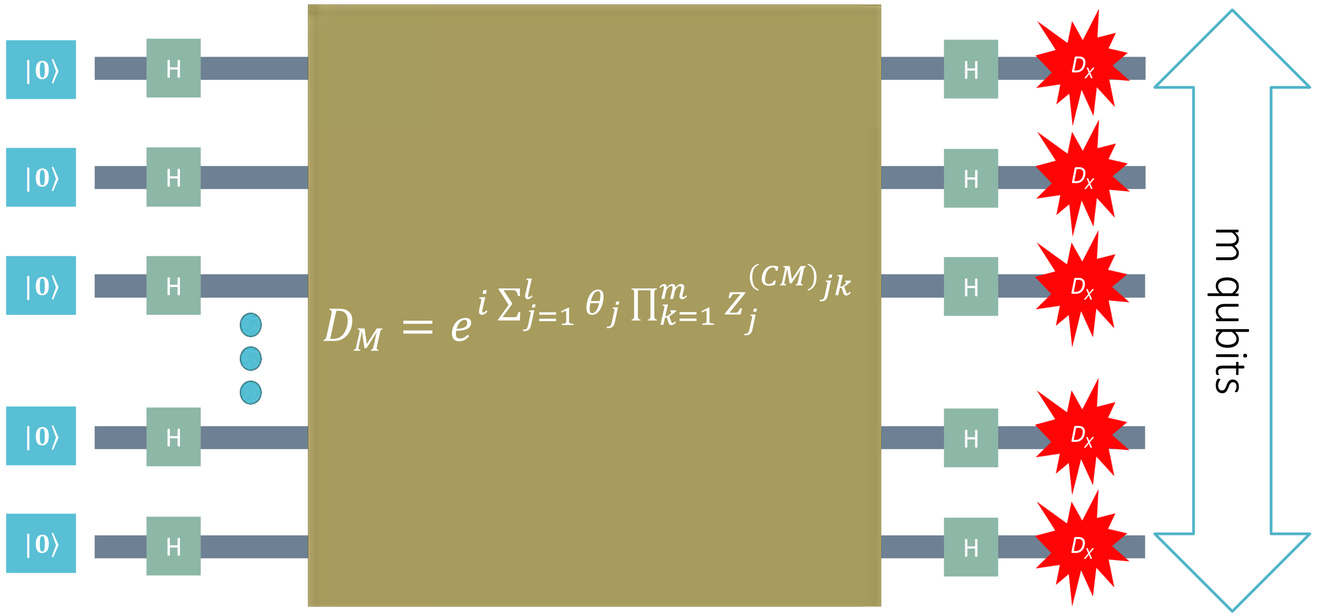
However in this regime you can heurstically show that such circuits can be simulated by a simple coin toss!

Semi-classical error correction

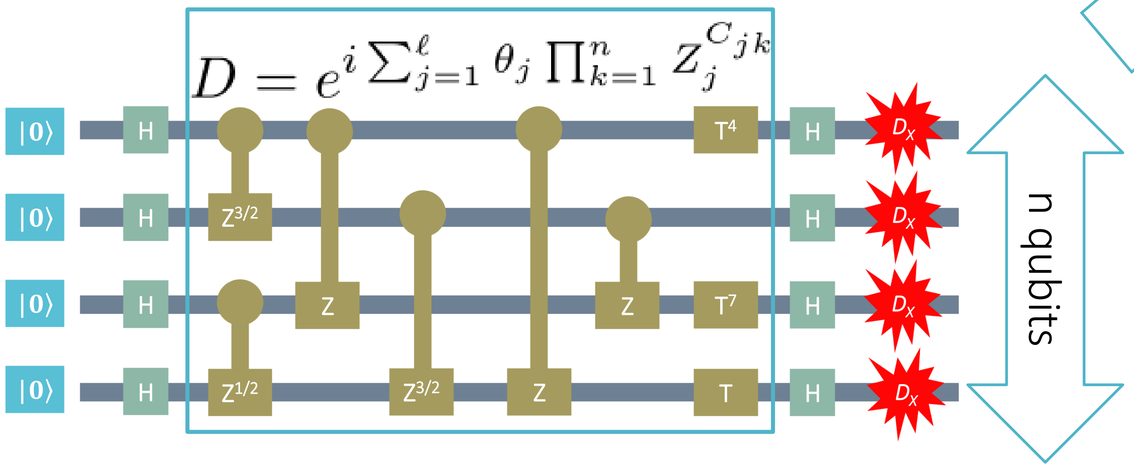
Measurement depolarizing noise can be corrected on any IQP circuit via a classical encoding, M, on the *binary* circuit description, C.

This results in a corrected circuit with 1-norm distance δ for per-qubit error rate $\epsilon < 1$.

(BMS Quantum **1**, 8 (2017), arXiv:1610.01808)



Encoding

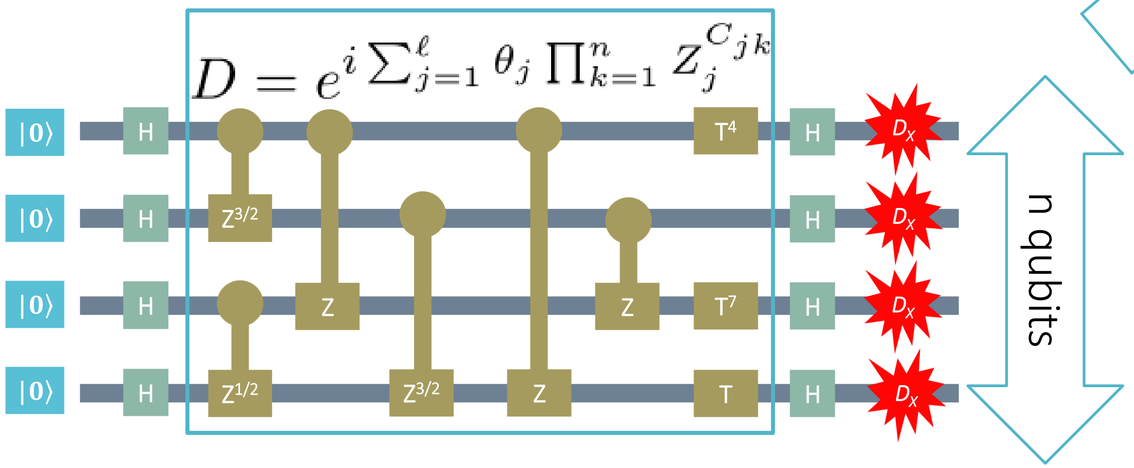


Semi-classical error correction

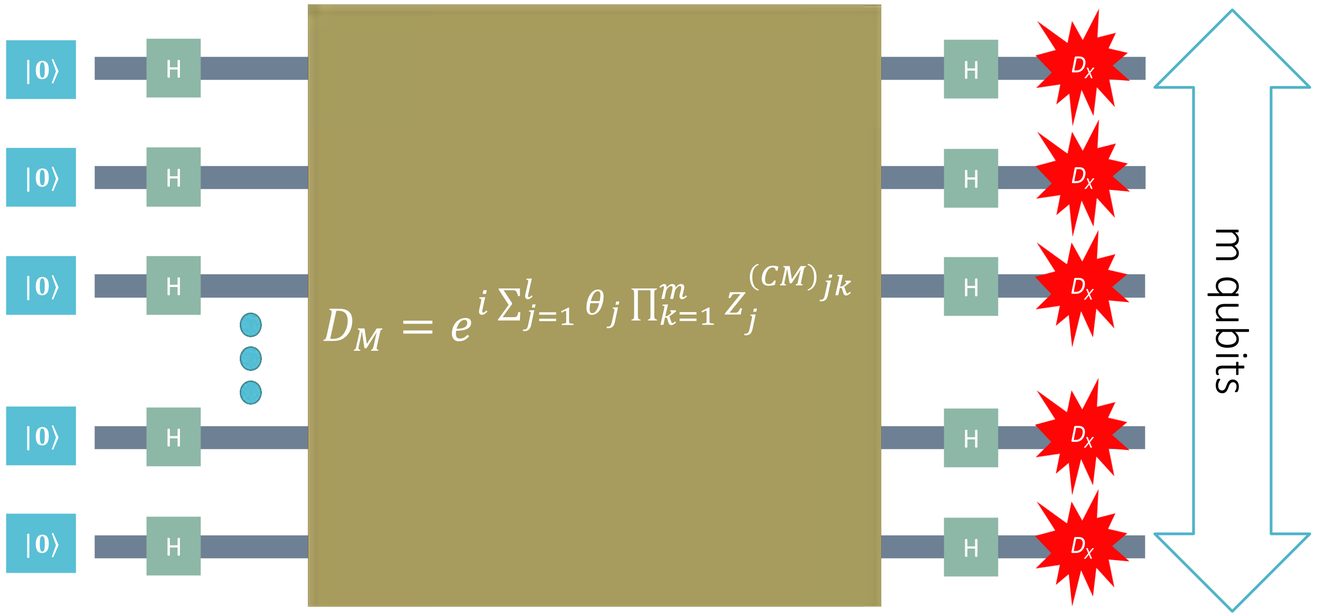
Measurement depolarizing noise can be corrected on any IQP circuit via a classical encoding, M, on the *binary* circuit description, C.

This results in a corrected circuit with 1-norm distance δ for per-qubit error rate $\epsilon < 1$.

(BMS Quantum **1**, 8 (2017), arXiv:1610.01808)



Encoding



$$\langle x| \prod_{k=1}^{m} Z_j^{(CM)_{jk}} |x\rangle = \langle Mx| \prod_{k=1}^{n} Z_j^{C_{jk}} |Mx\rangle$$

$\langle x|D_M|x\rangle = \langle Mx|D|Mx\rangle$ and so we classically decode.

Any “good” code will work. For the bitflip code D_M is an O(log n) factor larger than D. Shannon’s noiseless coding theorem implies that a constant overhead is possible.

D_M is potentially much more complicated than D, with the potential for multi-qubit gates.

Verification

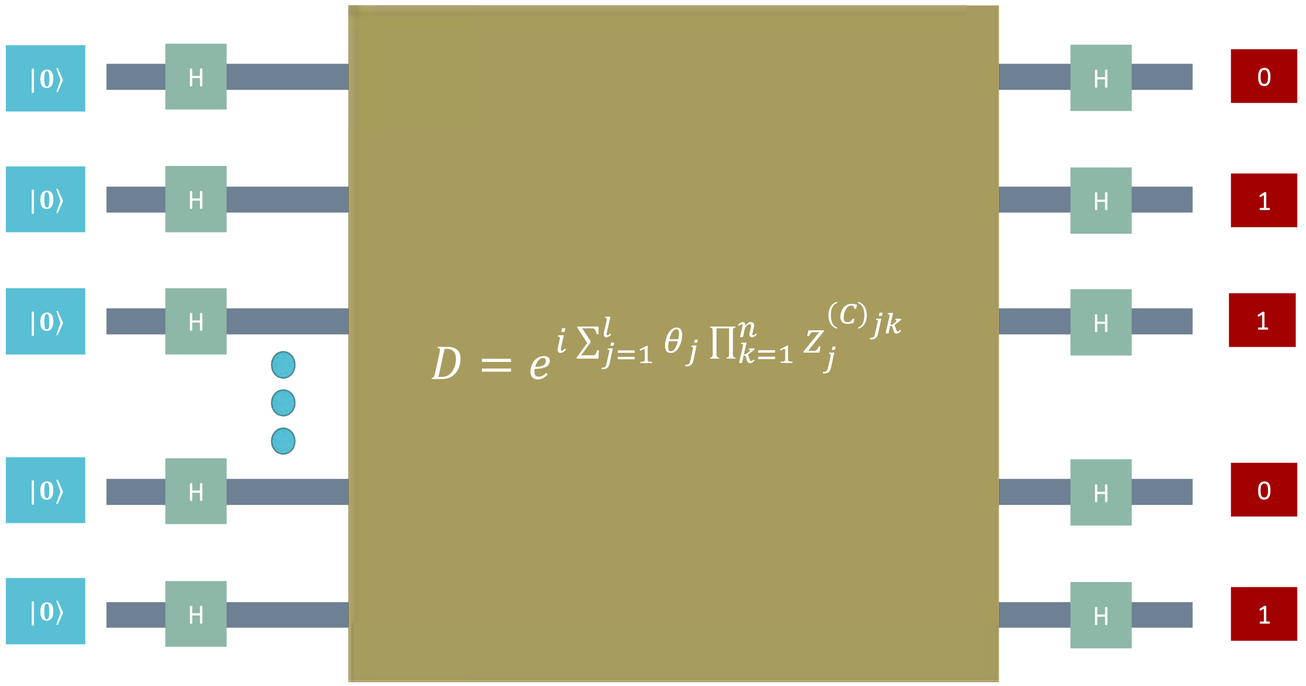
Verification

In general, complete black box verification is likely too hard. However:

- Physical verification need not be “black box”, we are free to implement many circuits on a device to gain confidence that it works.
- Fidelity estimates via the cross entropy for sufficiently random circuits (Boixo et al 1608.00263) - requires computing a #P-hard problem for this estimate.
- IQP circuits can be verified in certain architectures (see Bermejo-Vega et al 1703.00466).
- Aaronson and Chen arXiv:1612.05903 , Heavy output generation: Given as input a random quantum circuit C (drawn from some suitable ensemble), generate output strings x_1 , . . . , x_k , at least a 2/3 fraction of which have greater than the median probability in C’s output distribution. Assuming the QUATH assumption is true. Again requires computing the median, which is generally computationally difficult.
- IQP samplers can be tested with pseudo-random circuits, assuming cryptographic assumptions (Shepherd and MJB, Proc. R. Soc. A 465, 1413-1439 (2009), arXiv:0809.0847).

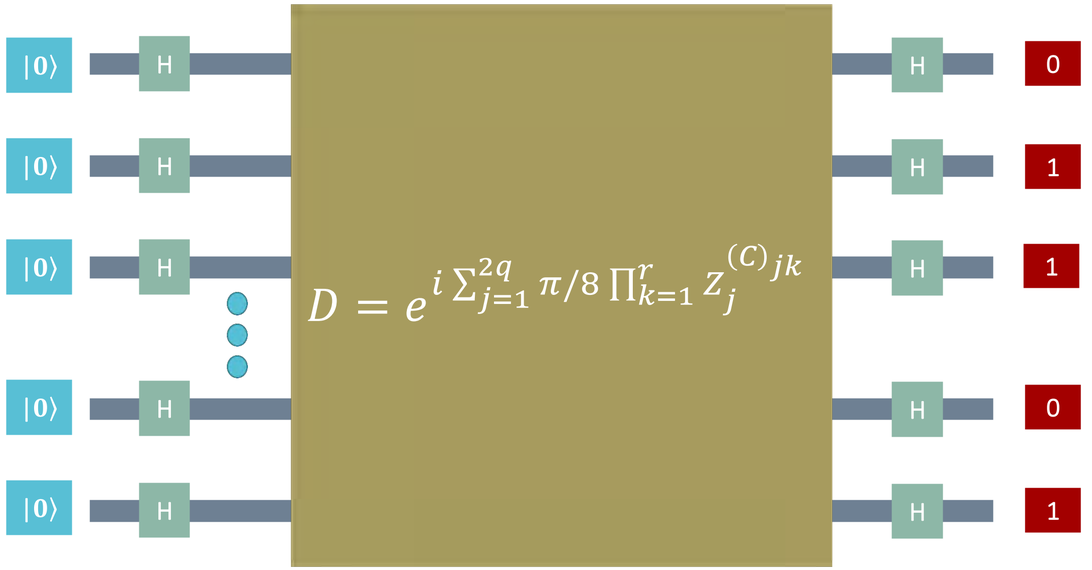
Cryptographic verification

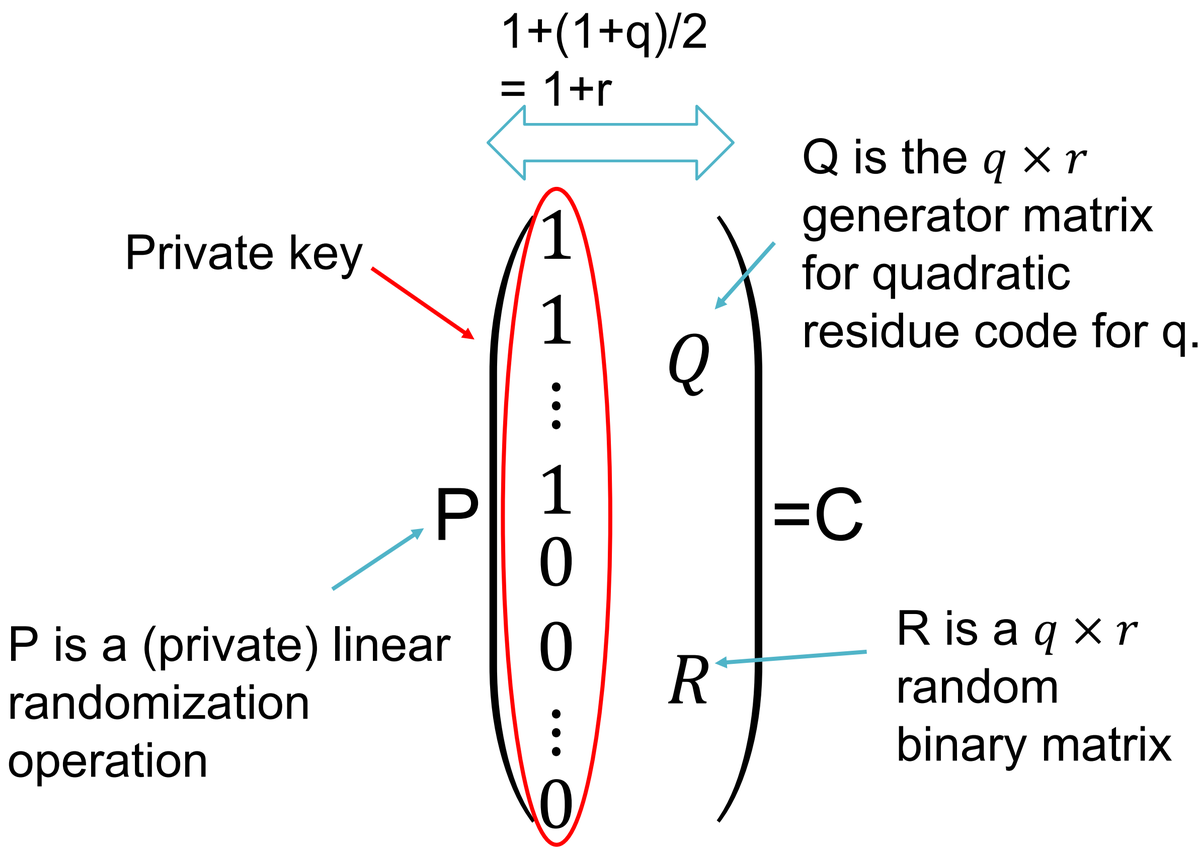
- For IQP circuits P(x) ~ WEP(C) the weight enumerator polynomial of a linear binary code generated by the columns of C.
- If we choose C carefully we can determine properties of P(x) and WEP(C).
- Importantly, while sampling x might be hard, it isn't always hard to detect a bias in a set of samples. That is, for a string $s \in \{0,1\}^n$ we can sometimes determine with what probability x.s=0.
- We can use such properties to create a cryptographic protocol to hide a chosen bias to create a private/public key pair for testing IQP circuits.



Cryptographic verification

- Choose a large prime q = 7 mod 8 to define a quadratic residue code of length q. It will have rank, r = (q+1)/2.
- Q is an example of a singly punctured doubly even code as quadratic residue codes are a parity bit short of being self-dual
- C constitutes a public key, with the private key defined by the leftmost column prior to randomization.
- This defines a string s for which the probability of x.s = 0 is ~ 85%. This probability depends only on Q and not R.
- 2nd order cryptanalysis of the Hamiltonian (i.e. the rowspace of C) suggests random samples avoid s with probability 75%. This makes it both difficult to learn s and to reproduce the correct probability of x.s without simulating the circuit.





Cryptographic verification

Conjecture 1: Sampling from random IQP circuits is classically difficult.

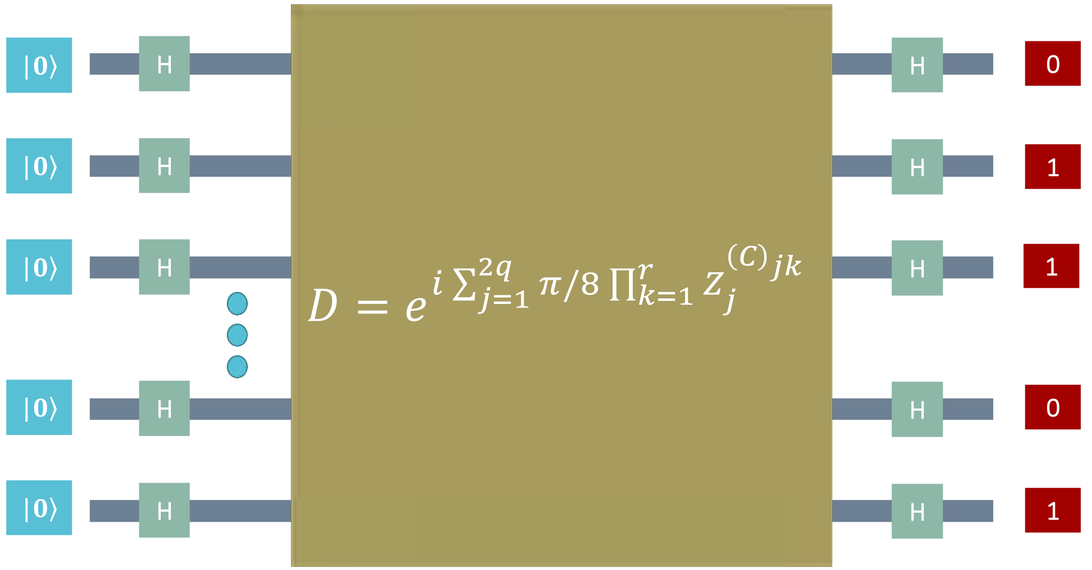
Conjecture 2: With high probability C cannot be distinguished from a random binary matrix.

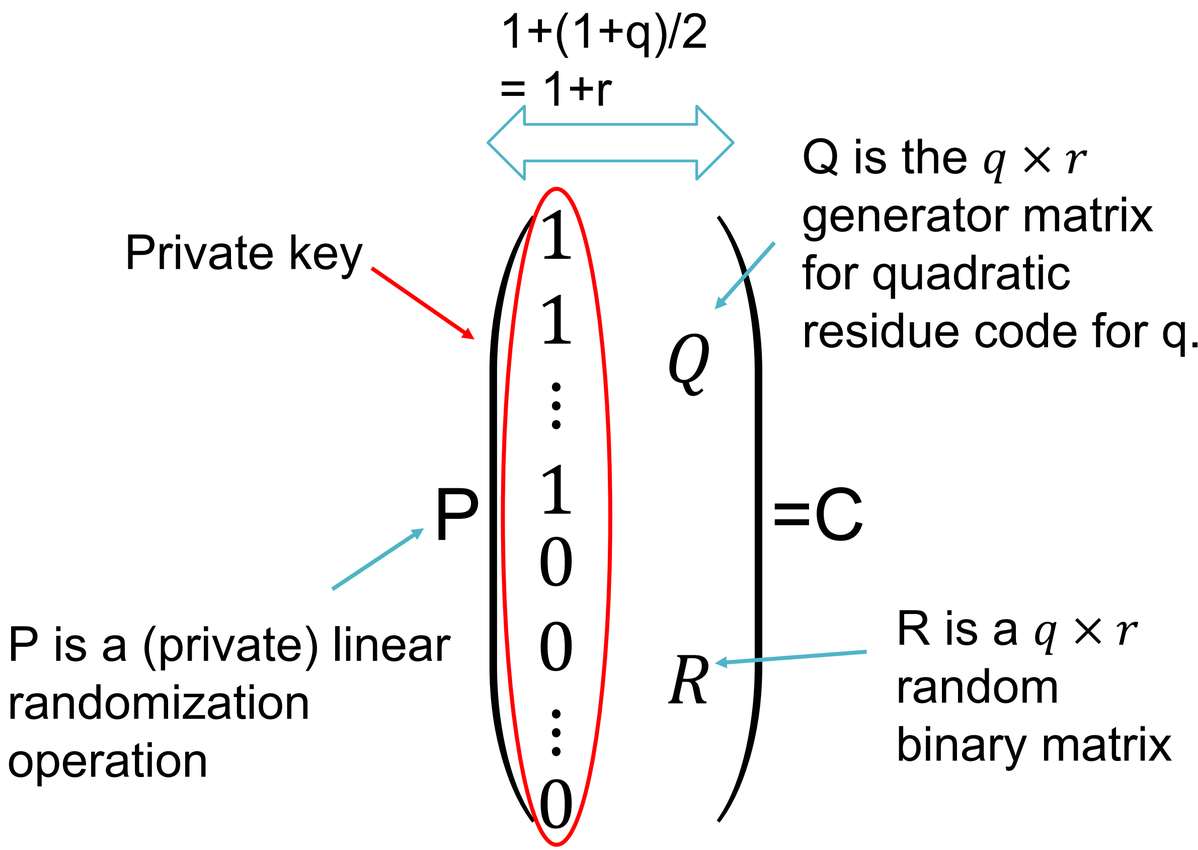
Conjecture 3: s cannot be found in polytime given C.

Example: Challenge problem with r = 244 i.e. 244 qubits are required. Note that this is with quite a high gate count (>1000).

Obvious challenges: Prove the above, make this easier, and find new examples.

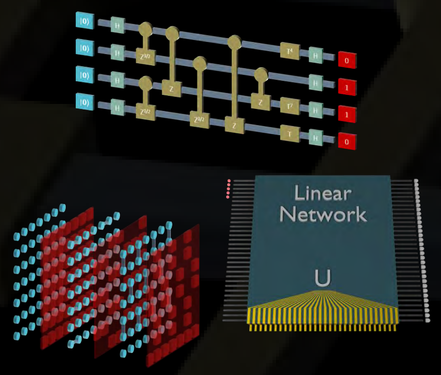
See: Shepherd and MJB, Proc. R. Soc. A 465, 1413-1439 (2009), arXiv:0809.0847.





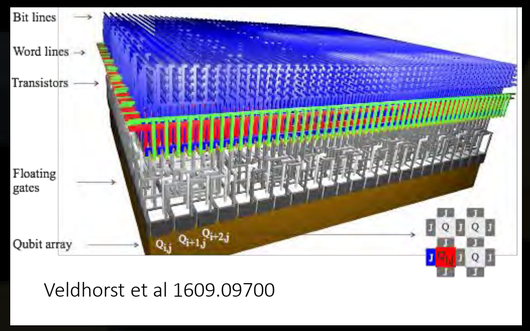
Outlook

A potential quantum (near) future



Intermediate quantum computing regime:

- Error mitigation
- Testable advantage
- Approximate optimizers
- Quantum simulators



Veldhorst et al 1609.09700

50 qubits | 1,000 | 10,000 | 100,000…

99.7% fidelity

FT qubit

Classical/quantum frontier

<12 months (Google, IBM)

Unambiguous quantum computational supremacy and commercially relevant applications , 2 – 10 years

99.99% fidelity

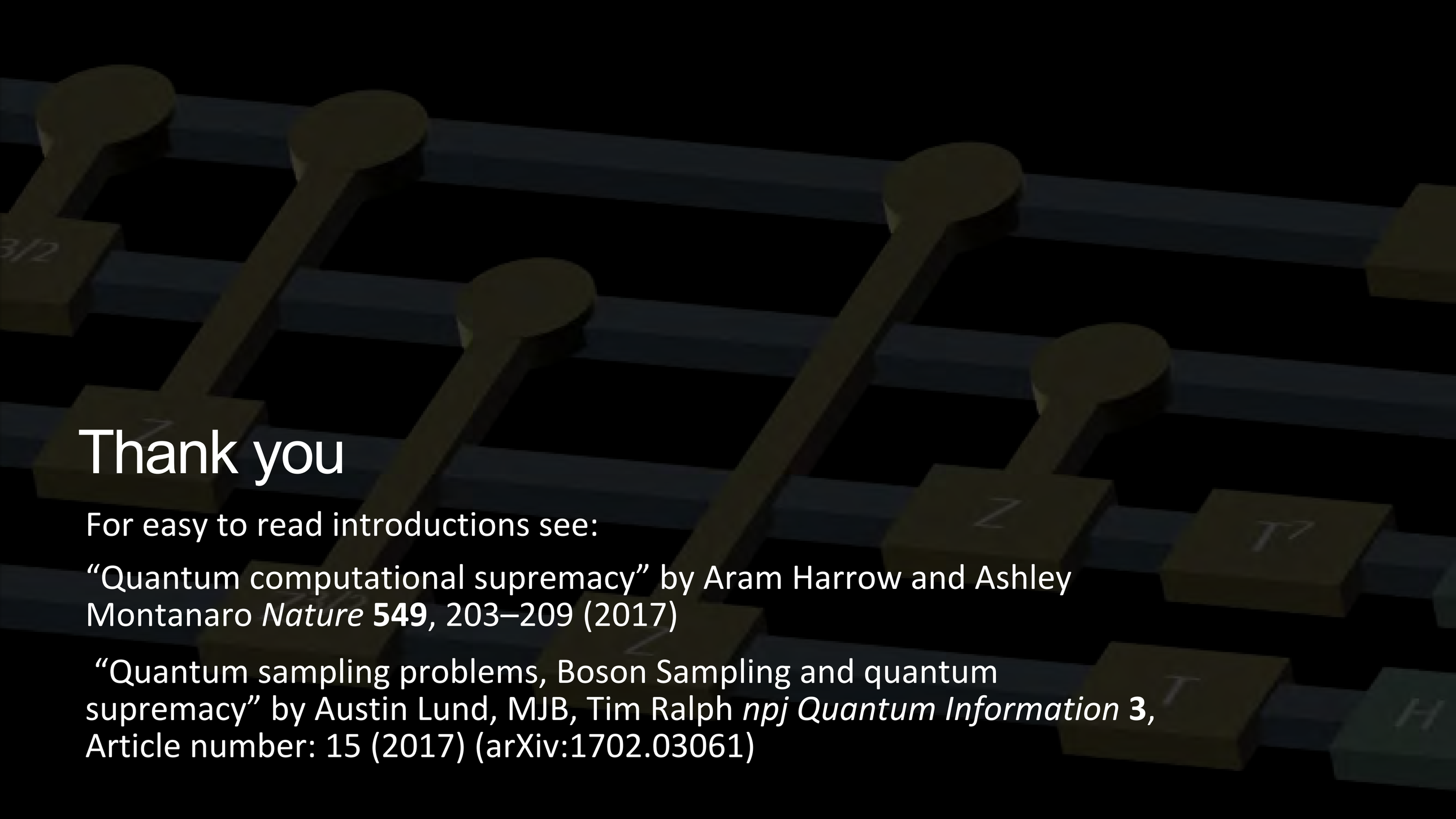
99.999% fidelity

10+ years

Universal quantum computing…

Open questions

- Can we use these techniques to “prove” advantage over classical algorithms for more “more structured” problems, such as for optimization (e.g. QAOA see 1703.06199 and 1602.07674) or for general quantum simulations?
- How much noise is too much noise? When is error correction a necessity? Can we make do without it?
- How many qubits are required to outperform classical computers for other tasks with a quantum advantage? E.g. we know that 512 bit RSA needs 1026 logical qubits or 256 bit elliptic curves require 2330 (1706.06752).
- How do we attack the open average-case complexity conjectures? What other conjectures can be made?
  - Aaronson and Chen (1612.05903) have shown that resolving these conjectures is likely to be difficult, but what can we learn from them - i.e. can we better connect them to one another and other results in complexity theory.
- What else is there? E.g. Bravyi, Gosset and Koenig arXiv:1704.00690.



Thank you

For easy to read introductions see:

“Quantum computational supremacy” by Aram Harrow and Ashley Montanaro *Nature* **549**, 203–209 (2017)

“Quantum sampling problems, Boson Sampling and quantum supremacy” by Austin Lund, MJB, Tim Ralph *npj Quantum Information* **3**, Article number: 15 (2017) (arXiv:1702.03061)