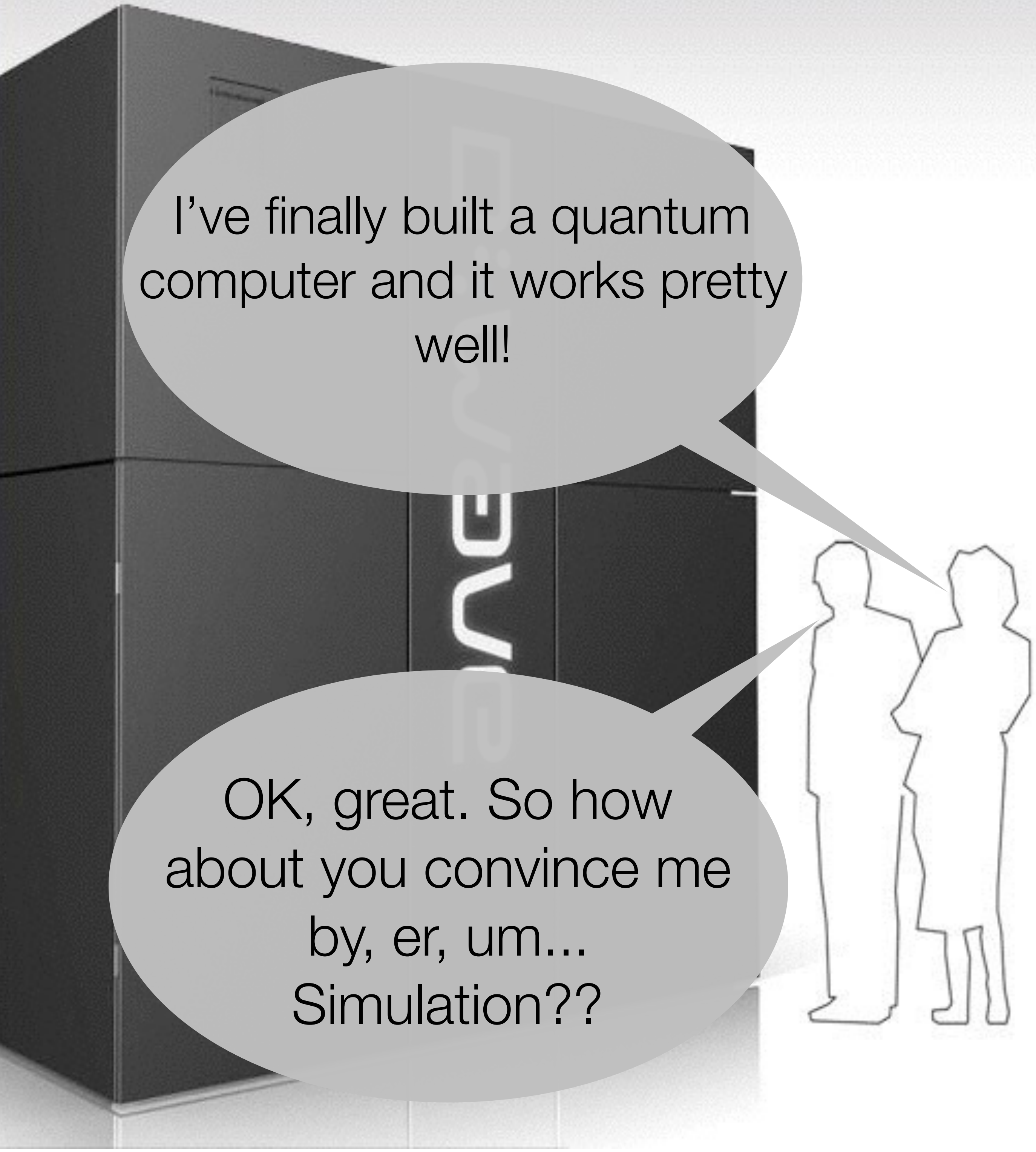
Australian Government
Australian Research Council
LOCKHEED MARTIN
UTS:QCIS
QUANTUM COMPUTATION & INTELLIGENT SYSTEMS

Average-case complexity versus approximate simulation of commuting quantum computations

Michael Bremner, Ashley Montanaro, and Dan Shepherd. arXiv:1504.07999

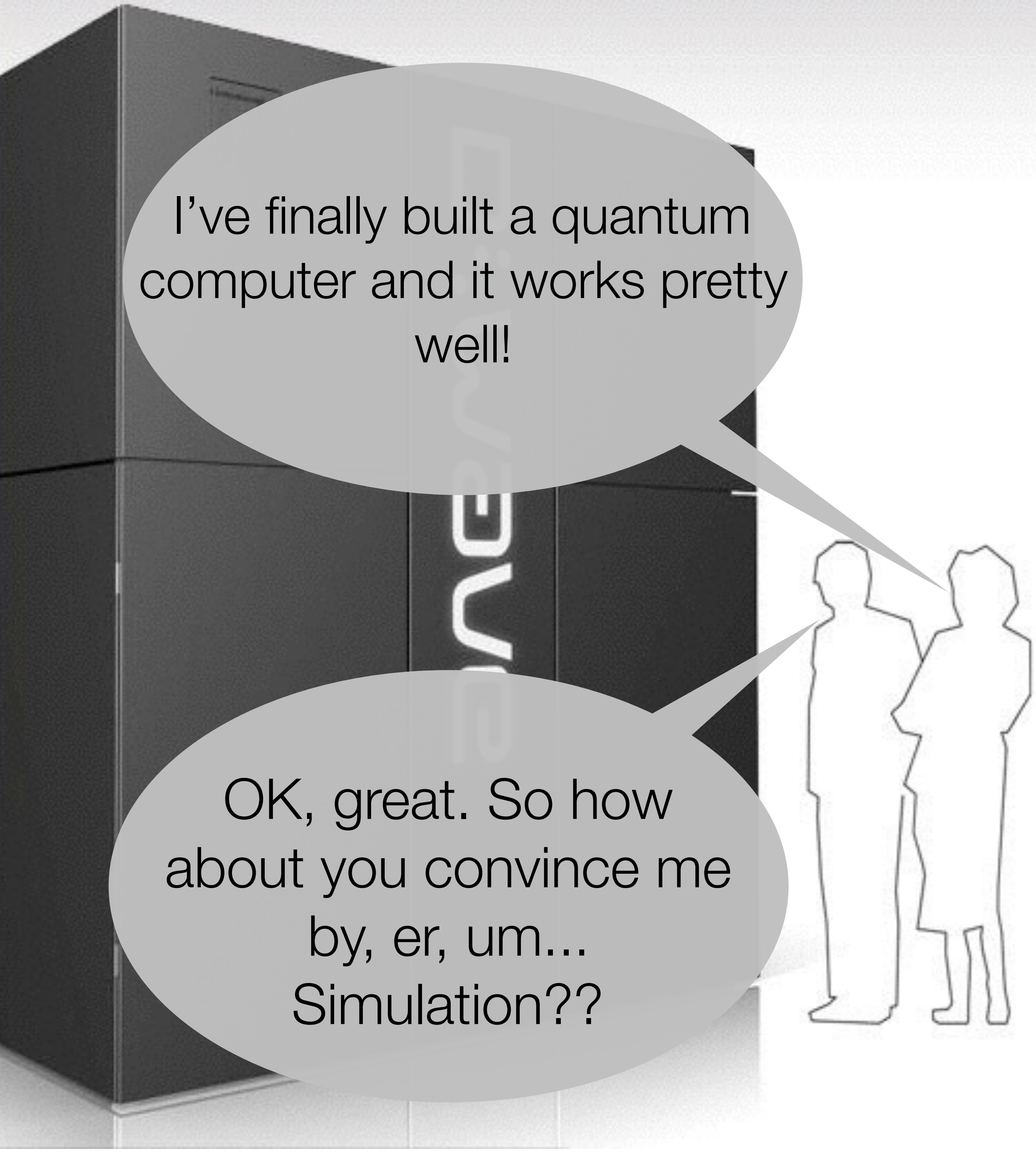
University of BRISTOL
EPSRC
Engineering and Physical Sciences Research Council



What should experimentalists do to demonstrate quantum supremacy in the near future?

- Build gates etc with high fidelity.
- Error-correction.
- Shor’s algorithm.
- Quantum simulation.
- Try to solve other “hard” problems that can be efficiently checked. (e.g. DWave approach)

Challenge: Identify easy quantum computations that are “post-classical”?



What should experimentalists do to demonstrate quantum supremacy in the near future?

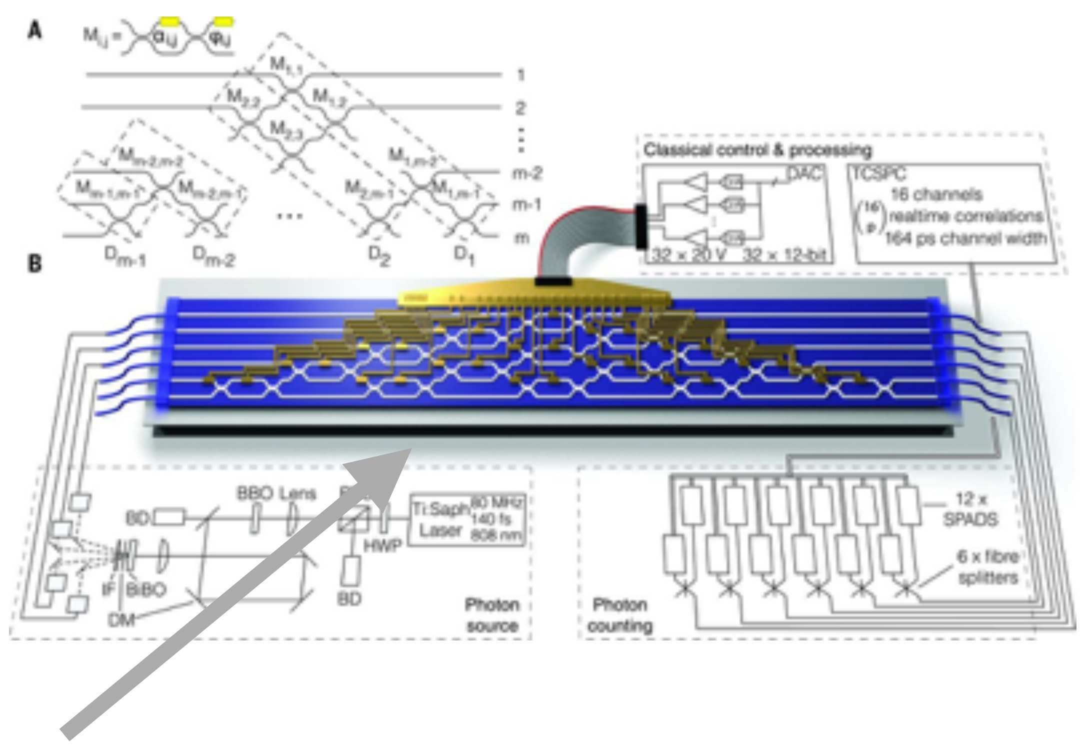
- Build gates etc with high fidelity.
- Error-correction.
- Shor's algorithm.
- Quantum simulation.
- Try to solve other "hard" problems that can be efficiently checked. (e.g. DWave approach)

Challenge: Identify ~~easy~~ quantum computations that are "post-classical"?

Boson Sampling [Aaronson and Arkhipov '10]: Can R($\mathbf{x}$) approximate P($\mathbf{x}$) in polynomial time?

0100001110, 1001001010, 10011000101, …

P($\mathbf{x}$)



vs

R($\mathbf{x}$)

Random LO circuit

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

No. If:

1. The PH is infinite
2. The Permanent anti-concentration conjecture is true
3. The Gaussian Permanent Approximation Conjecture is true

Our main result: IQP Sampling

If the "average case" complexity of multiplicative approximations to either:

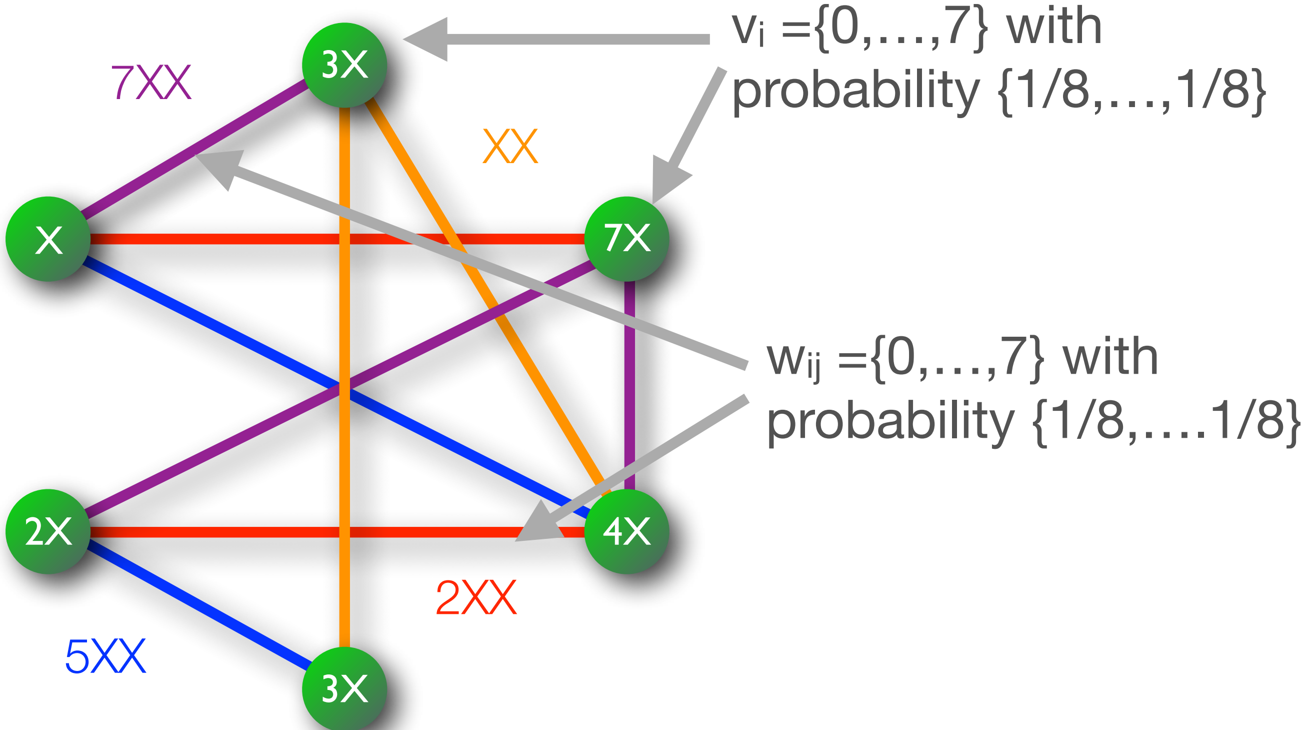
1) The complex temperature Ising model partition functions, or

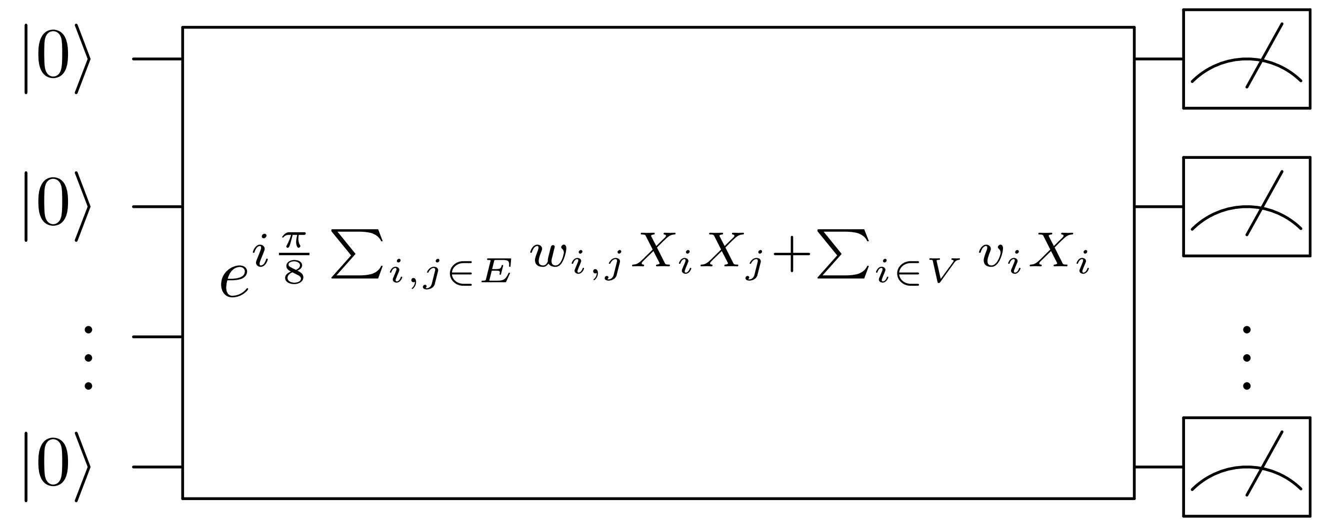
2) The gap of degree 3 polynomials

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

- This "improves" on Boson Sampling by proving the equivalent of the "Permanent anti-concentration conjecture". (also see arXiv/1507.05592)
- Our techniques are simple enough to generate new conjectures and classically difficult to quantum circuit families.

Post-classical family 1: Random Ising circuits





$$H = \sum_{i,j\in E} w_{ij}X_iX_j + \sum_{i\in V} v_iX_i$$

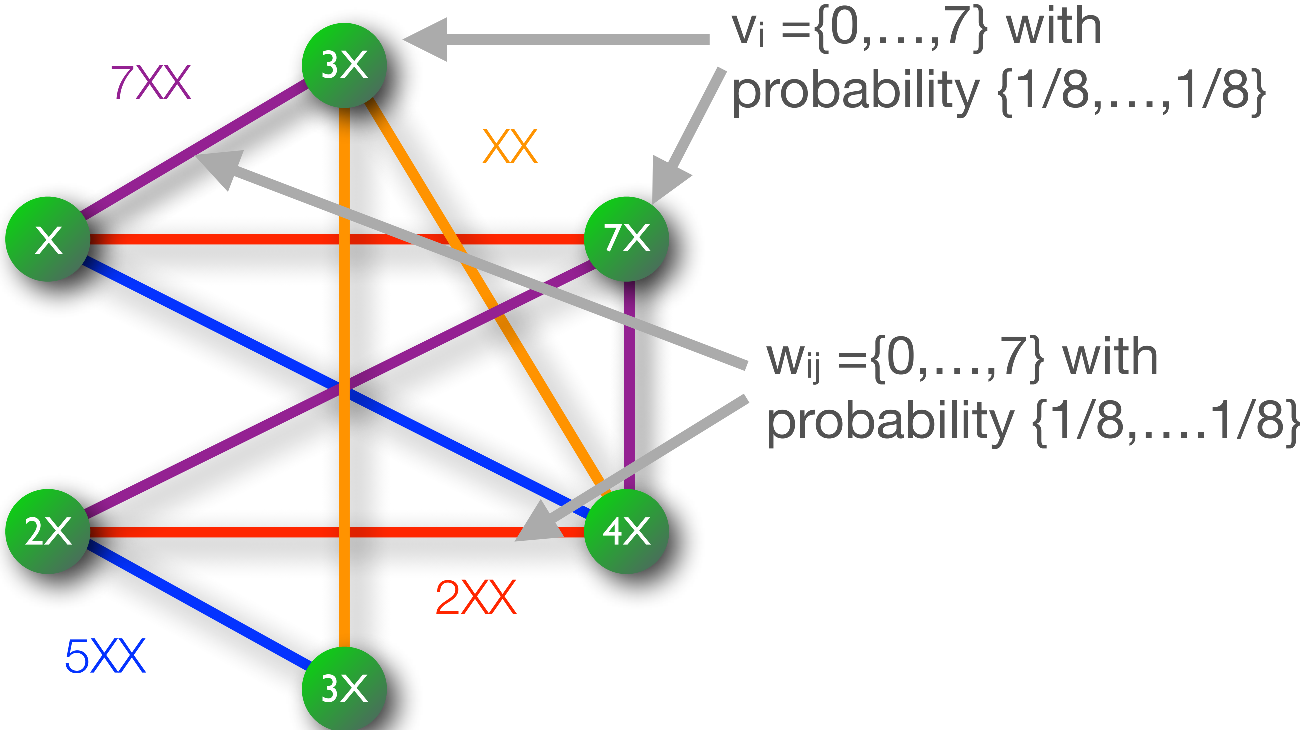
Sample from $e^{i\pi/8H}|0\rangle^{\otimes n}$

*If conjecture (1) 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)

Post-classical family 1: Random Ising circuits



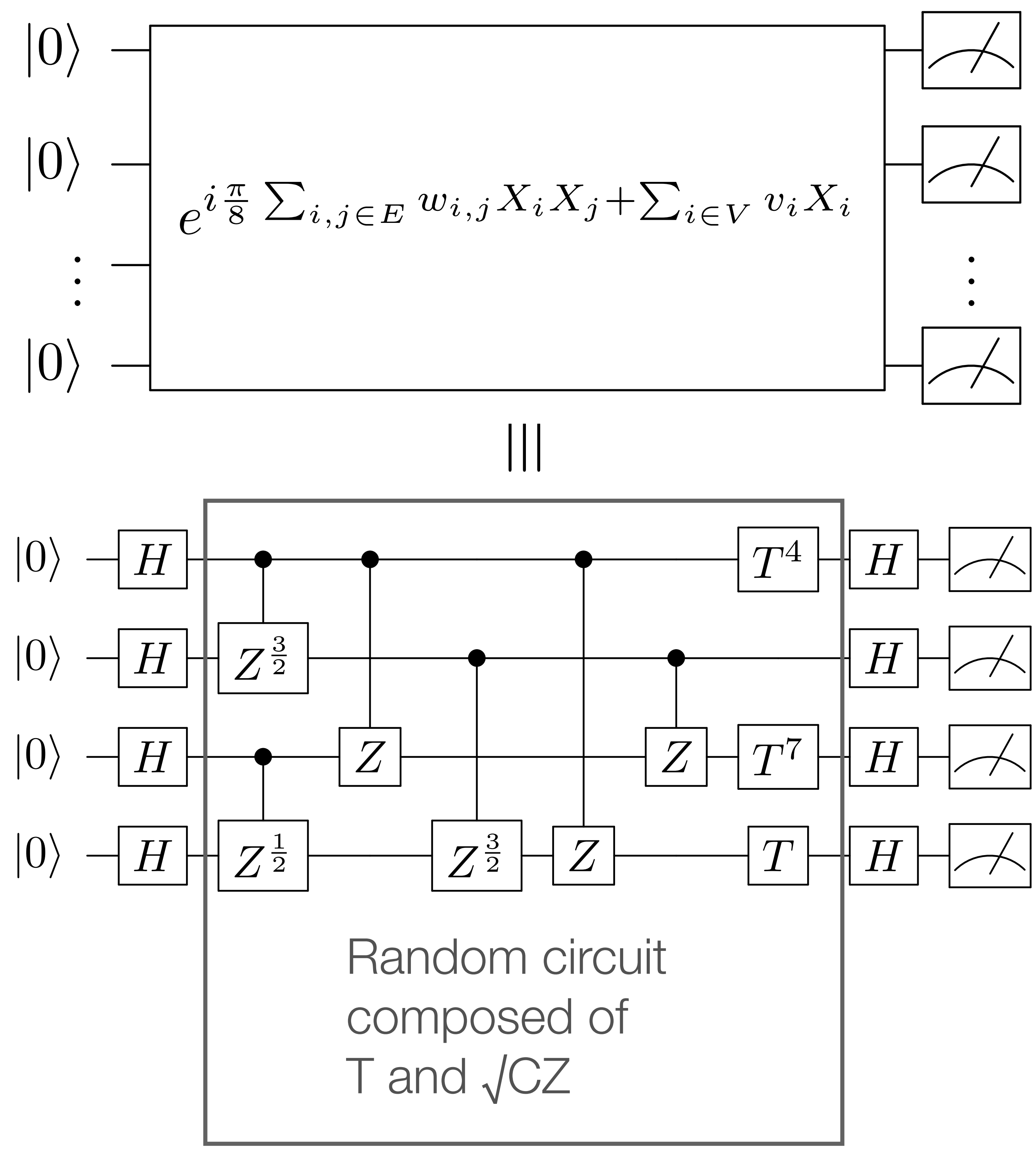
$$H = \sum_{i,j\in E} w_{ij} X_i X_j + \sum_{i \in V} v_i X_i$$

Sample from $e^{i\pi/8H}|0\rangle^{\otimes n}$

*If conjecture (1) is true then there is no efficient classical algorithm that can sample from any R(**x**) such that:*

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

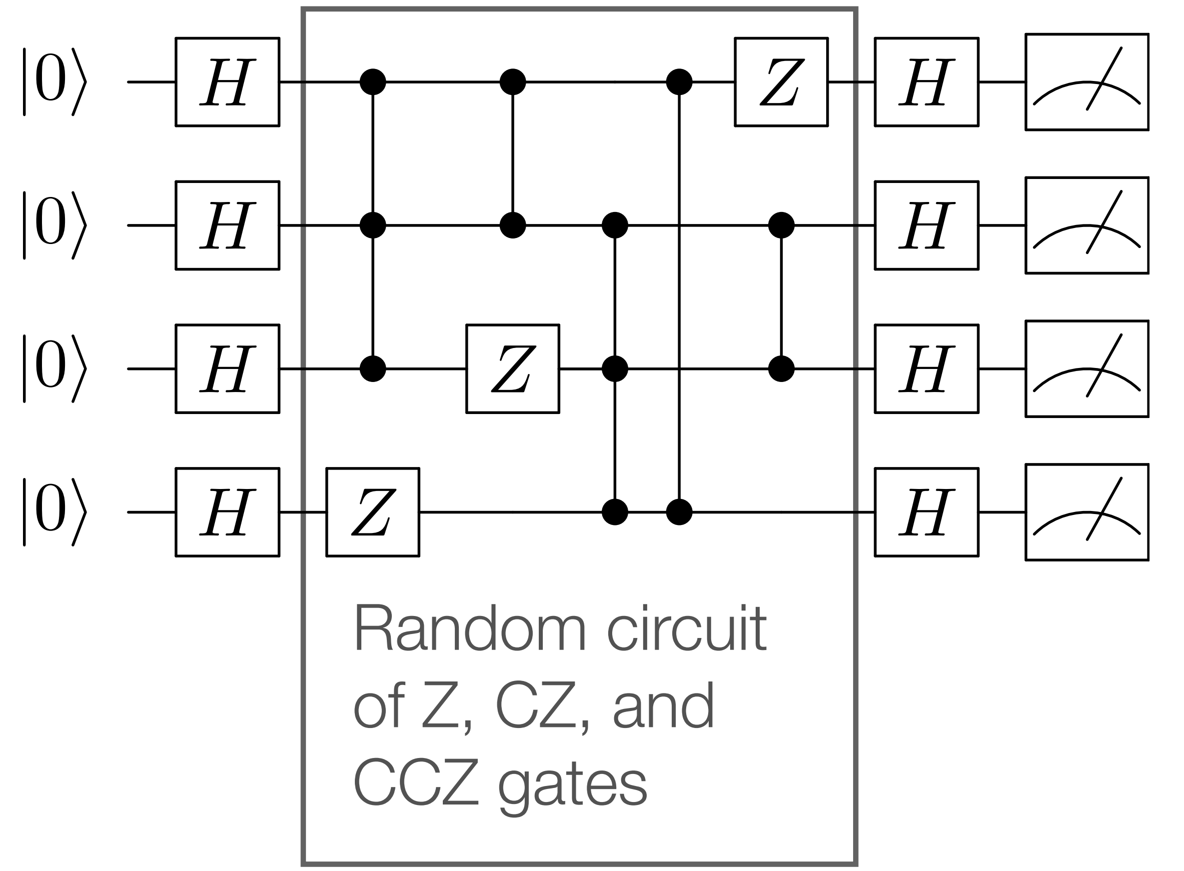
(Unless the PH collapses)



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:*

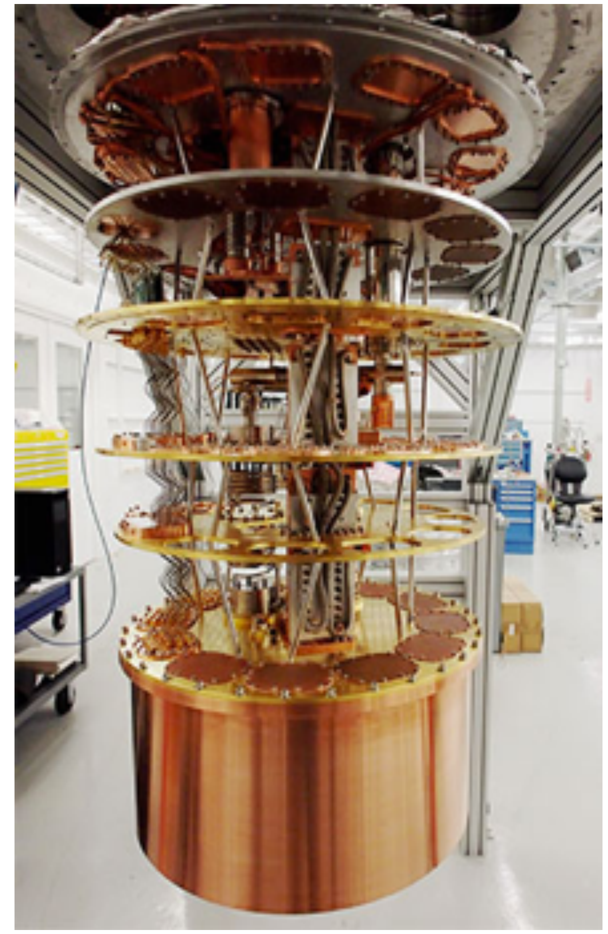
$||P(\mathbf{x}) - R(\mathbf{x})||_1 \leq 1/192$

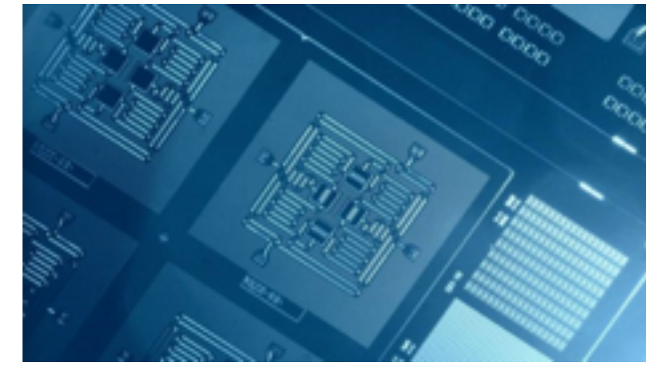
(Unless the PH collapses)

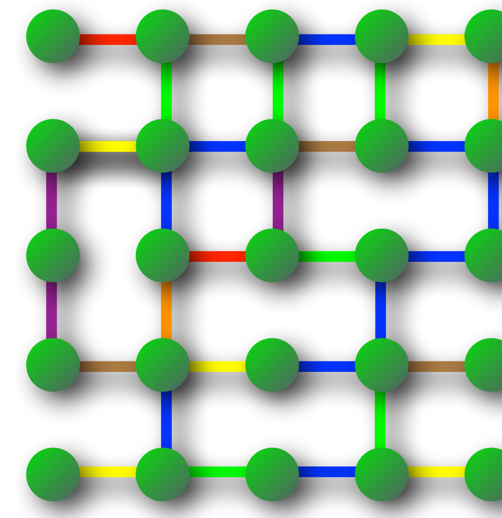
All are examples of IQP circuits (Instantaneous Quantum Polytime)

Implementation

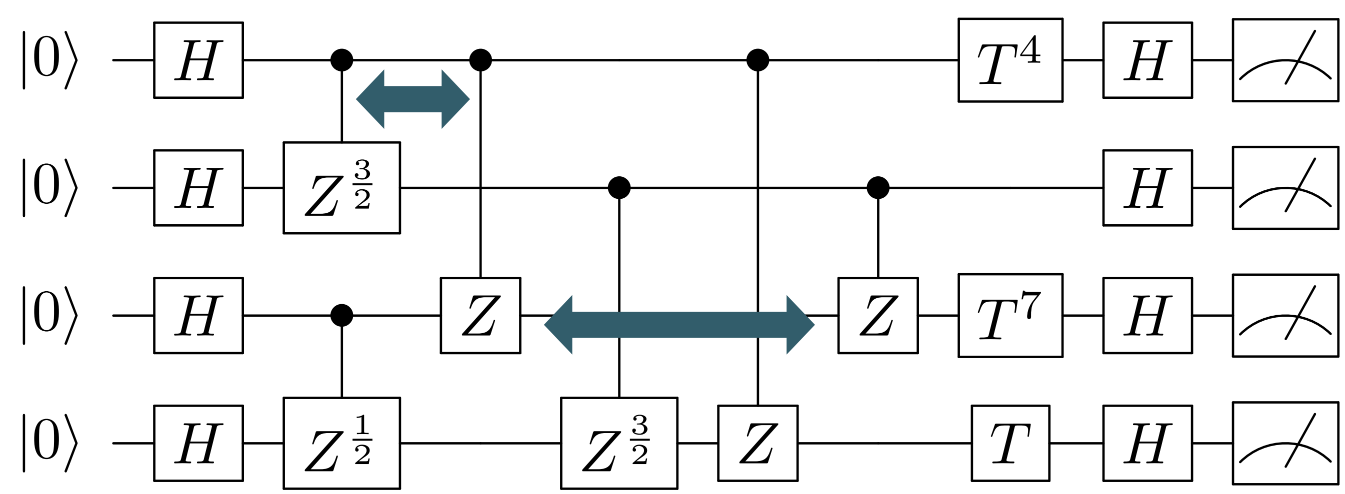
- Ising circuits are drawn from the *complete* graph on n vertices.
    - Requires $O(n^2)$ gates 2-local long-range commuting gates.
    - Depth is O(log n) with a universal gate set.
    - Depth is O(n) with a 2D, universal, nearest neighbour architecture.
- Our results imply that with high probability a randomly chosen Ising circuit will have quantum supremacy.
- The commuting gates can allow for better fault-tolerance thresholds.
- Requires circuit accuracy to only *constant* variation distance.



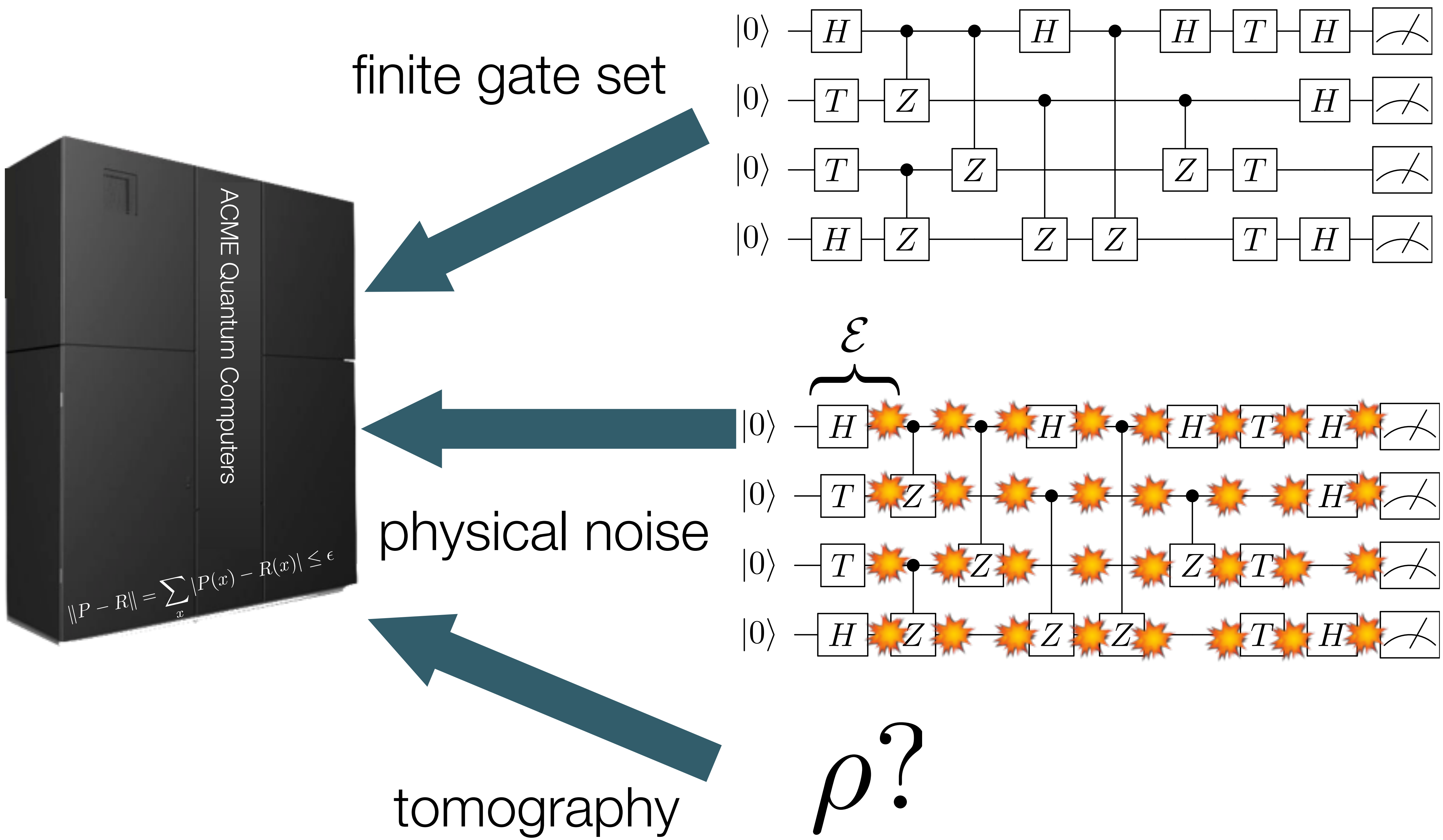




VS



Additive bounds are essential



Wait, Mick, didn't you give this talk like 5 years ago?

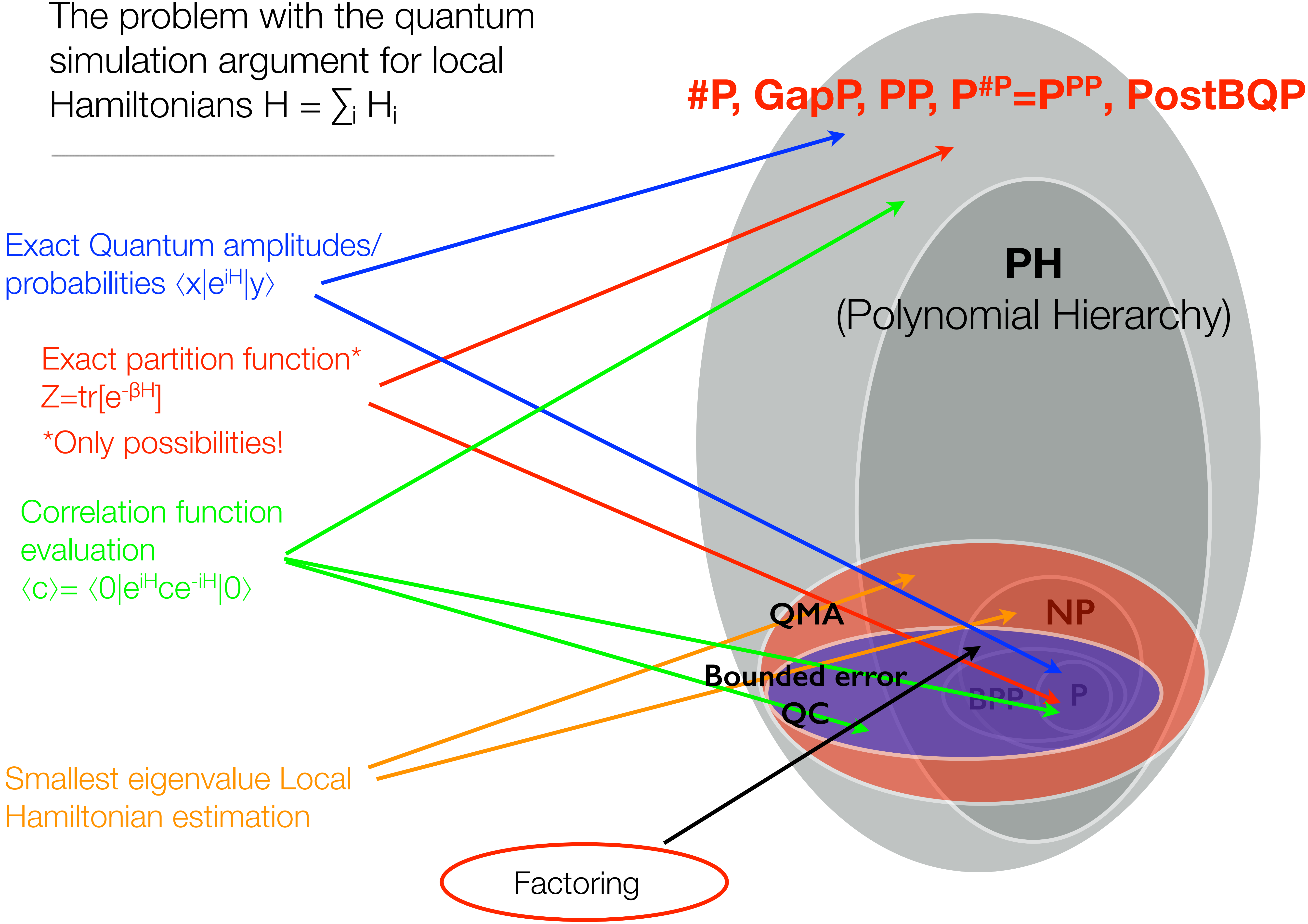
Additive vs Multiplicative

$$\|P - R\|_1 = \sum_x |P(x) - R(x)| \leq \epsilon \quad \text{vs} \quad \frac{1}{c} P(x) \leq R(x) \leq c P(x), \; \forall x$$

- MB, Jozsa, and Shepherd '11 proved that there exist IQP circuits that cannot be efficiently classically simulated up to constant multiplicative error unless the PH collapses.
- It is unlikely that every "multiplicatively quantum supreme" circuit is also "additively quantum supreme".
- BJS result has been recently extended to circuits of 2-local commuting gates - see Adam Bouland, Laura Mančinska, and Xue Zhang's talk on Tuesday.

Why can’t I just simulate <insert my favourite quantum system>?

The problem with the quantum simulation argument for local Hamiltonians $H = \sum_i H_i$

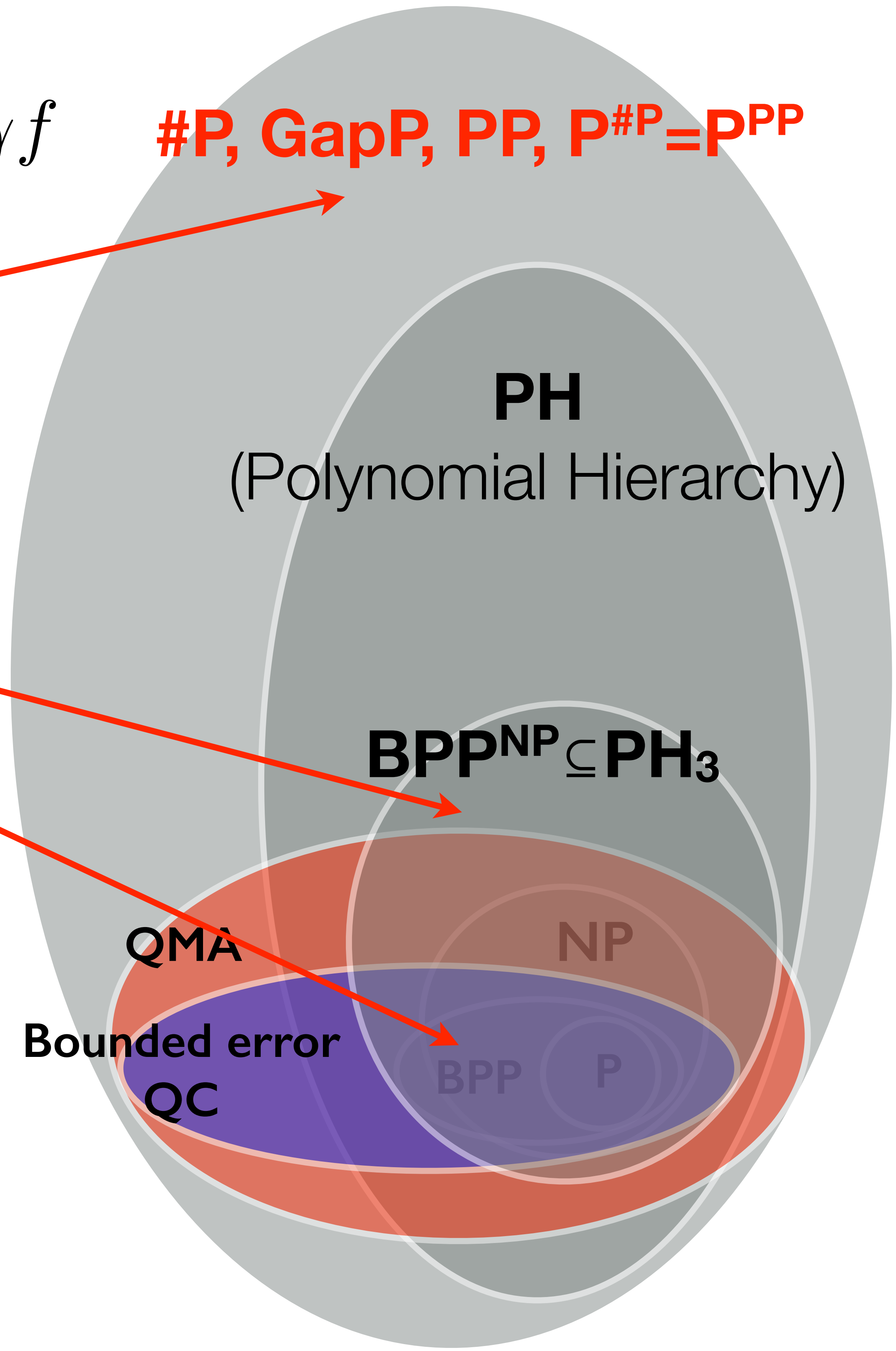


Multiplicative approximations: $|A_\times - f| \leq \gamma f$

GapP complete problems remain GapP complete. (i.e. can never have an FPRAS)

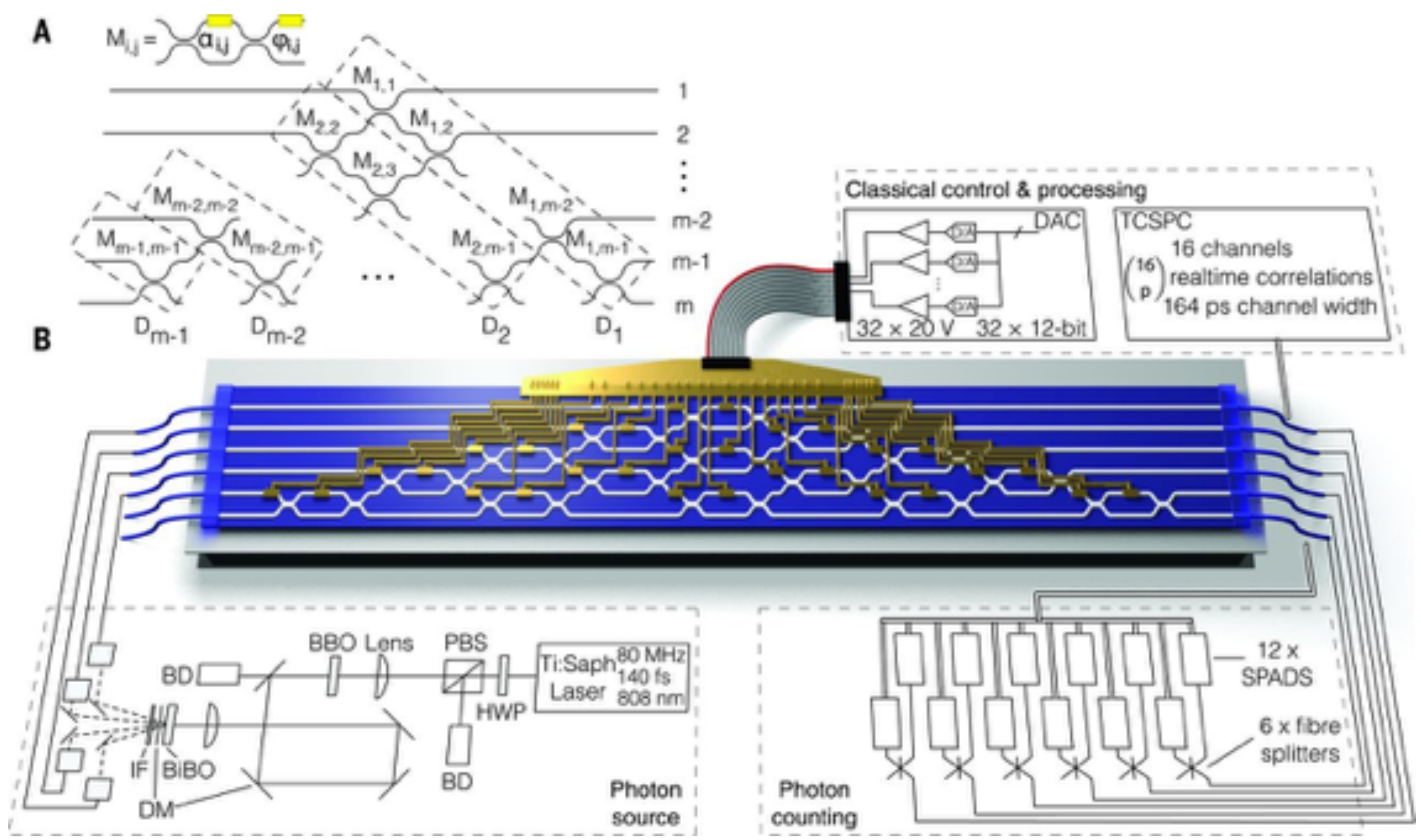
#P functions go here!

Stockmeyer (STOC '83):
Any function in #P can be approximated to within a constant factor with high probability in BPP^{NP}. This can be generalized to any sum of non-negative real numbers.



#P: Sharp P
The class of function problems of the form "compute f(x)", where f is the number of accepting paths of an NP machine.

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.

- If you use random circuits then this isn't ridiculously hard to prove!

GapP and quantum computing

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

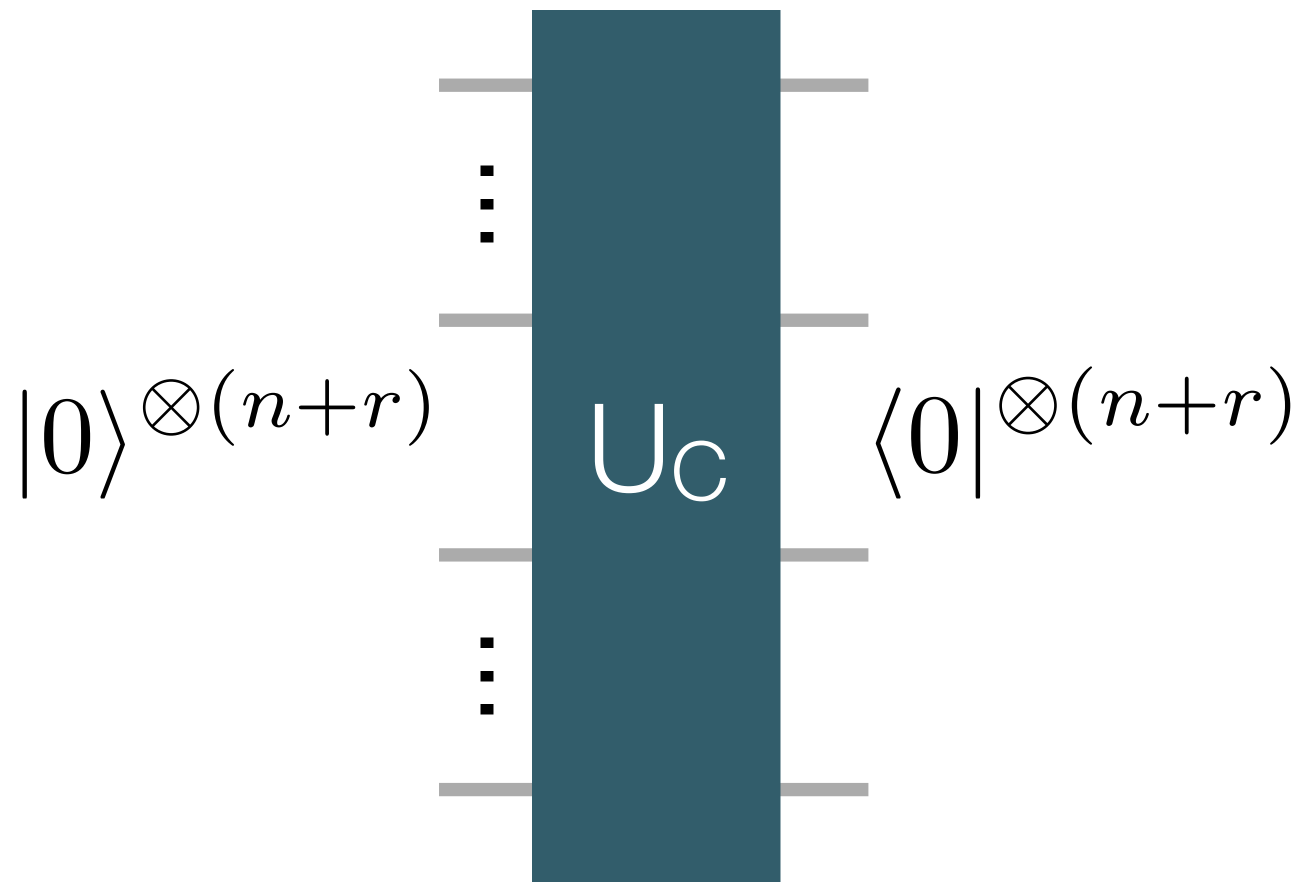
  GapP: Let C be a classical circuit that computes a Boolean function C : $\{0,1\}^n \to \{-1,1\}$. Given C as input, compute Δ_C which is given by:

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

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

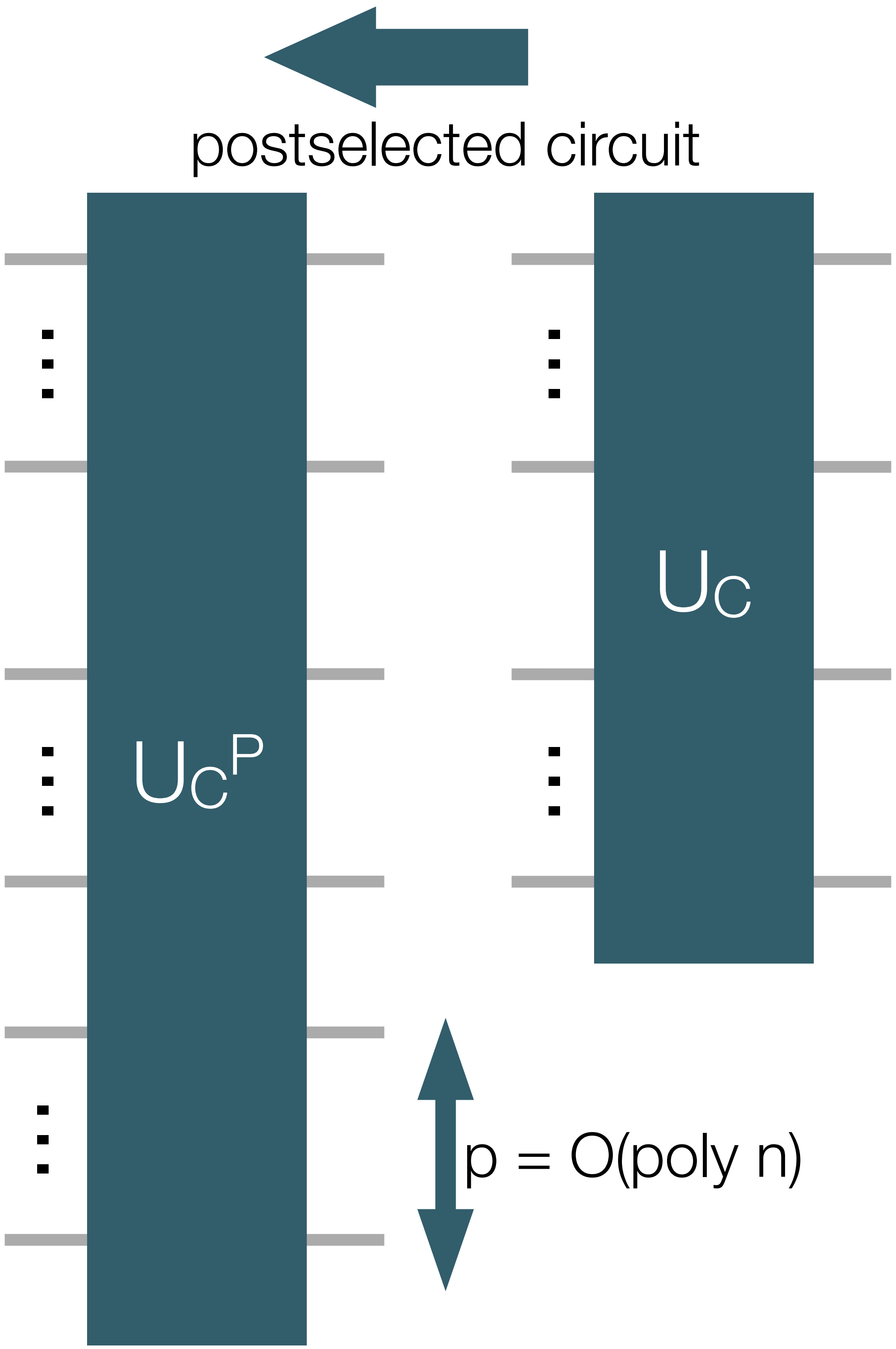
- Multiplicative approximations to GapP-complete problems are still GapP-complete. Implies **$|A-P(0^n)| \leq \gamma P(0^n)$ is #P-hard.**

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



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

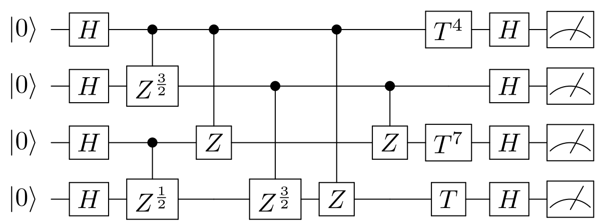
- Circuits constructed from universal gate sets.
- Linear optics without feedforward - i.e. Boson Sampling systems. Also proportional to matrix permanents! (See A+A)
- IQP circuits, i.e. circuits with all-commuting gates. Also proportional to partition functions, polynomial gaps and weight enumerator/Tutte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



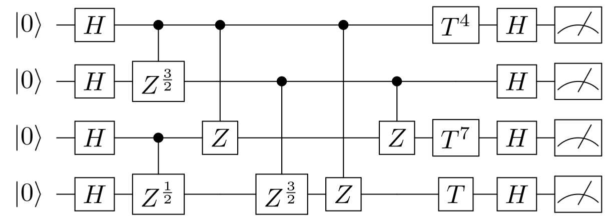
* (See, Goldberg and Guo arXiv:1409.5627, Fuji and Morimae arXiv:1311.2128 and our paper.)

IQP sampling: rough idea

Want to know P(0)



(1) Write circuit



(1') Circuit description of P(x)

+NP

(2) 0100001110, 1001001010, …
according to R(x)

$$\Pr_x\left[|P(x) - R(x)| \geq \frac{\epsilon}{2^n \delta}\right] \leq \delta$$

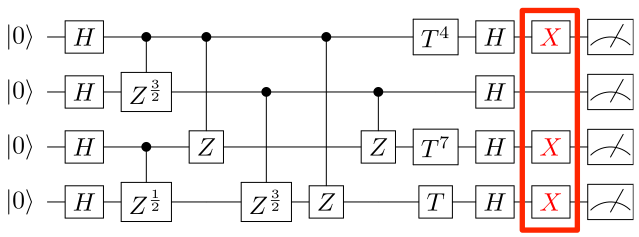
(3) Stockmeyer counting algorithm:
|A-R(0)|≤(1/poly(n))R(0)

(3') $|A - P(x)| \leq \frac{P(x)}{\mathrm{poly}(n)} + \frac{\epsilon(1 + 1/\mathrm{poly}(n))}{2^n \delta}$

No bound on P(0) 😢

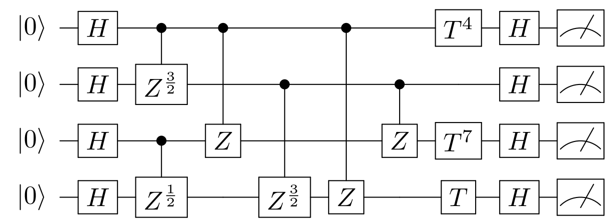
IQP sampling

Want to know P’(0)



(1) Hide P’ in P

+NP



(1’) Circuit description of P(x)

P’ is hidden by P:
Achieved through a random choice of P’(0) and P(x)

(2) 0100001110, 1001001010, …
according to R(x)

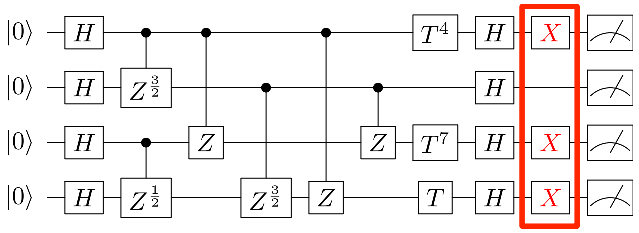
$$\Pr_x\left[|P(x)-R(x)| \geq \frac{\epsilon}{2^n\delta}\right] \leq \delta$$

(3) Stockmeyer counting algorithm:
|A-R’(0)|≤(1/poly(n))R’(0)

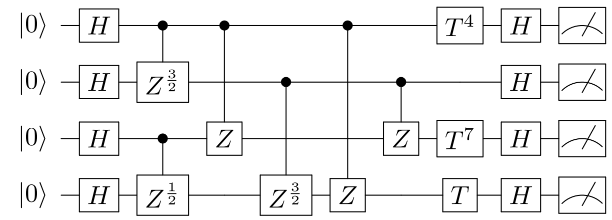
(3’) $$|A - P'(0)| \leq \frac{P'(0)}{\mathrm{poly}(n)} + \frac{\epsilon(1+1/\mathrm{poly}(n))}{2^n\delta}$$

IQP sampling: a PH collapse in the random case?

Want to know P’(0)



(1) Hide P’ in P



(1’) Circuit description of P(x)

+NP

P’ is hidden by P:
Achieved through a random choice of P’(0) and P(x)

(2) 0100001110, 1001001010, …
according to R(x)

$$\Pr_x\left[|P(x)-R(x)| \geq \frac{\epsilon}{2^n\delta}\right] \leq \delta$$

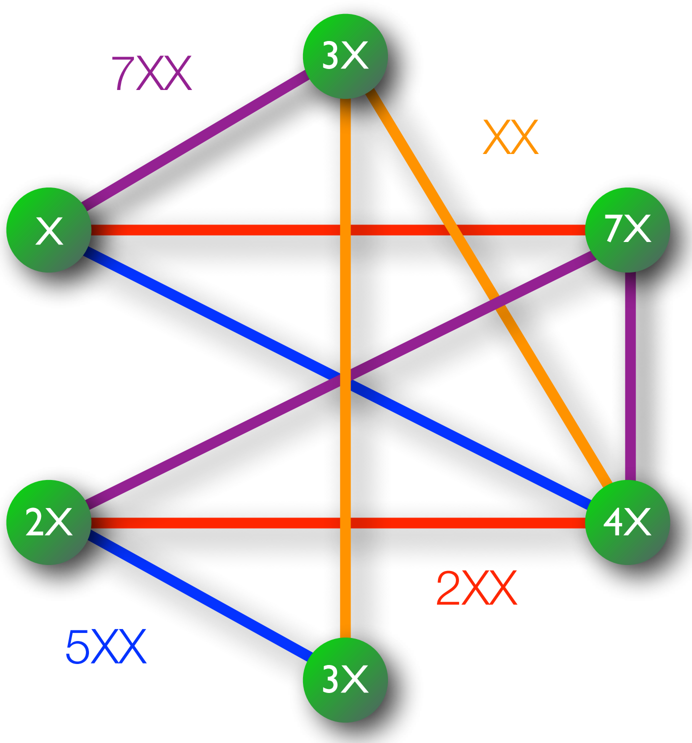
(3) Stockmeyer counting algorithm:
|A-R’(0)|≤(1/poly(n))R’(0)

(3’) $|A - P'(0)| \leq \gamma P'(0)$

If P’(0) = $\Omega(2^{-n})$ (or “anti-concentrates”) we get a multiplicative approximation.

If |A-P’(0)| ≤ γP’(0) is #P-hard *on average* the PH collapses

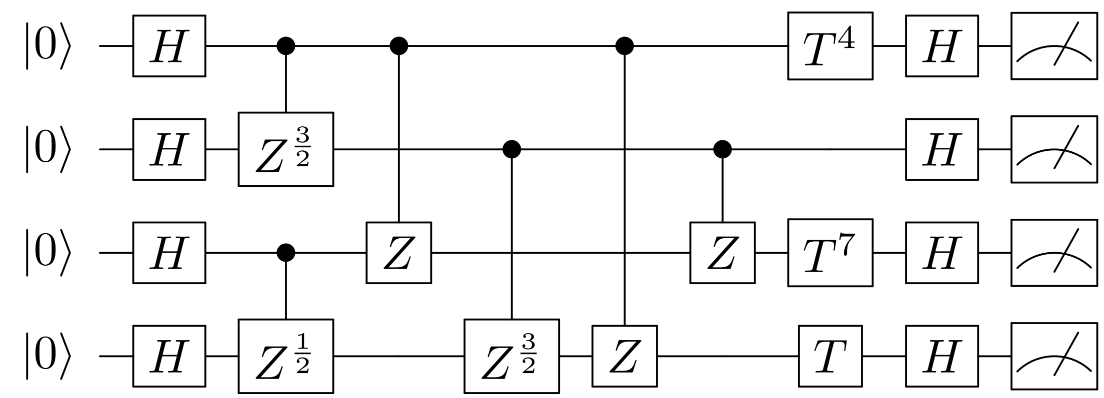
Ising models and IQP



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

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

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



These amplitudes are proportional to the complex Ising model (long known to be #P-hard).

- If w_{ij} and $v_i \in \{0,\ldots,7\}$ are uniformly randomly chosen.
- Then IQP sampling gives (with constant probability):

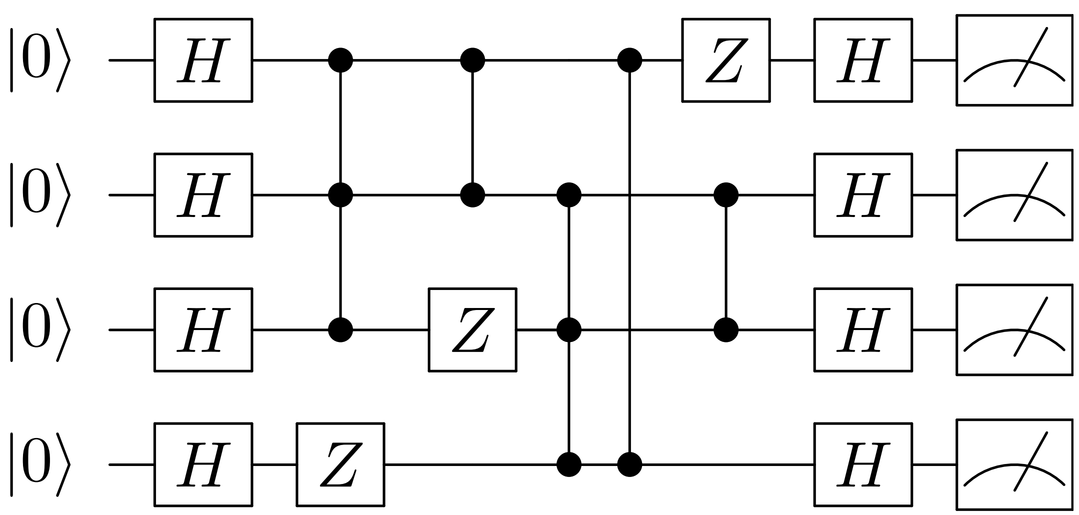
$$\left|A_\times - |Z|^2\right| \leq \left(\frac{1}{4} + o(1)\right)|Z|^2$$

- If $|Z|^2$ is #P-hard on average, then we are done!
- This parameter choice leads to #P-hardness of the *worst-case* complexity of Z. See, Goldberg and Guo arXiv:1409.5627, Fuji and Morimae arXiv:1311.2128 and our paper.

Polynomial gaps and IQP

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

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



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

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

- 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 $\mathrm{ngap}(f)^2$ is #P-hard on average we are done!
- This parameter choice leads to #P-hardness of the *worst-case* complexity of ngap(f). See our paper.

Boson Sampling ingredients	IQP (1504.07999)	
Amplitudes are #P-hard to precisely compute $$\langle S\vert\phi(U)\vert T\rangle = \frac{\mathrm{Per}(U_{S,T})}{\sqrt{s_1!\dots s_m!t_1!\dots t_m!}}$$	Common to q. circuit class that is universal with post-selection (in which case the problem is GapP-complete).	✓
Probabilities are #P-hard to multiplicatively approximate $$\frac{1}{g}\mathrm{Per}(A)^2 \leq R(A) \leq g\mathrm{Per}(A)^2$$	Actually a property of GapP-completeness.	✓
Gaussian matrices can be hidden in Haar random matrices enabling a LO sampler to estimate $\vert\mathrm{GPE}\vert^2_{\pm}$ in $\mathrm{BPP}^{\mathrm{NP}}$.	An obfuscation circuit can be built in IQP enabling an IQP sampler to estimate $\vert\langle \mathbf{x}\vert\mathrm{IQP}\vert\mathbf{0}\rangle\vert^2_{\pm}$ in $\mathrm{BPP}^{\mathrm{NP}}$.	✓
There are classes of Per(A) known to anti-concentrate. Fairly good evidence that this is true for Gaussian Permanents. This enables $\vert\mathrm{GPE}\vert^2_{\pm}$ to approximate $\vert\mathrm{GPE}\vert_{\times}$	$\vert\langle \mathbf{x}\vert\mathrm{IQP}\vert\mathbf{0}\rangle\vert^2$ anti-concentrates for random Ising models and for randomly chosen degree 3 polynomials (in F_2).	✓
GPE randomly-self-reduces. It is not clear that $\vert\mathrm{GPE}\vert_{\times}$ also randomly self reduces.		

Why these circuit classes?

- The commuting properties of these circuits make it possible to prove the anti-concentration bound.

- Follows from the Paley-Zygmund inequality (R>0, 0<α<1):

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

  and a lot of counting of roots of unity…

- There may be other choices of IQP circuit that allow for anti-concentration, however they will probably always need sufficient depth.

Boson Sampling ingredients	IQP (1504.07999)	
Amplitudes are #P-hard to precisely compute $$\langle S\|\phi(U)\|T\rangle = \frac{\mathrm{Per}(U_{S,T})}{\sqrt{s_1!\dots s_m! t_1! \dots t_m!}}$$	Common to q. circuit class that is universal with post-selection (in which case the problem is GapP-complete).	✓
Probabilities are #P-hard to multiplicatively approximate $$\frac{1}{g}\mathrm{Per}(A)^2 \leq R(A) \leq g\mathrm{Per}(A)^2$$	Actually a property of GapP-completeness.	✓
Gaussian matrices can be hidden in Haar random matrices enabling a LO sampler to estimate $\|\mathrm{GPE}\|^2_{\pm}$ in $\mathrm{BPP}^{\mathrm{NP}}$.	An obfuscation circuit can be built in IQP enabling an IQP sampler to estimate $\|\langle \mathbf{x}\|\mathrm{IQP}\|\mathbf{0}\rangle\|^2_{\pm}$ in $\mathrm{BPP}^{\mathrm{NP}}$.	✓
There are classes of Per(A) known to anti-concentrate. Fairly good evidence that this is true for Gaussian Permanents. This enables $\|\mathrm{GPE}\|^2_{\pm}$ to approximate $\|\mathrm{GPE}\|_{\times}$	$\|\langle \mathbf{x}\|\mathrm{IQP}\|\mathbf{0}\rangle\|^2$ anti-concentrates for random Ising models and for randomly chosen degree 3 polynomials (in F_2).	✓
GPE randomly-self-reduces. It is not clear that $\|\mathrm{GPE}\|_{\times}$ also randomly self reduces.	We don't know of any tools for proving that $A_{\times}$ is hard on average.	✗

Evidence for our conjecture

For

- GapP-complete problems are always randomly self-reducible.
- complex Ising model is #P-hard with almost all choices of parameters. See Goldberg and Guo, arXiv:1409.5627
- Similarly, #P-hardness of the Ising model follows from Baharona's work on spin glasses.
- Both these arguments require a deterministic choice over parameters - whereas our conjectures demand a random choice.

Against

- In the exact case the GPE problems is hard on average because linear interpolation can be used to reduce any instance of the GPE to the random case.
- This technique does not work for the Ising model.
- This technique also does not work for the $|GPE|_{\times}$ either.
- Something really new has to be invented!

Other circuit classes?

- Fefferman and Umans (arXiv:1507.05592) recently argued that there exist circuit families drawn from universal gate sets that cannot be classically efficiently additively approximated - proving the equivalent of the random-self reducibility conjecture.
- However the anti-concentration conjecture seems difficult for such circuits.
- Can the commuting 2-local gates results of Bouland, Mančinska, and Zhang be be extended to show new families of circuits, and corresponding conjectures, that imply quantum supremacy?
- Are there any circuits of lower depth than IQP circuits that are quantum supreme?

What's next?

- Obviously, prove the conjectures - or find new conjectures that can be proved more easily.
- Find a convincing argument for the verification of Boson/ IQP Sampling experiments.
- Discover new quantum algorithms that somehow use the post-classicality of IQP or Boson Sampling-like circuits.

Thank you!

(Also, we have PhD and postdoc opportunities at UTS in Australia - if you are interested come see me!)