CLASSICAL SIMULATION OF COMMUTING QUANTUM COMPUTATIONS IMPLIES COLLAPSE OF THE POLYNOMIAL HIERARCHY

Michael Bremner, Richard Jozsa and Dan Shepherd

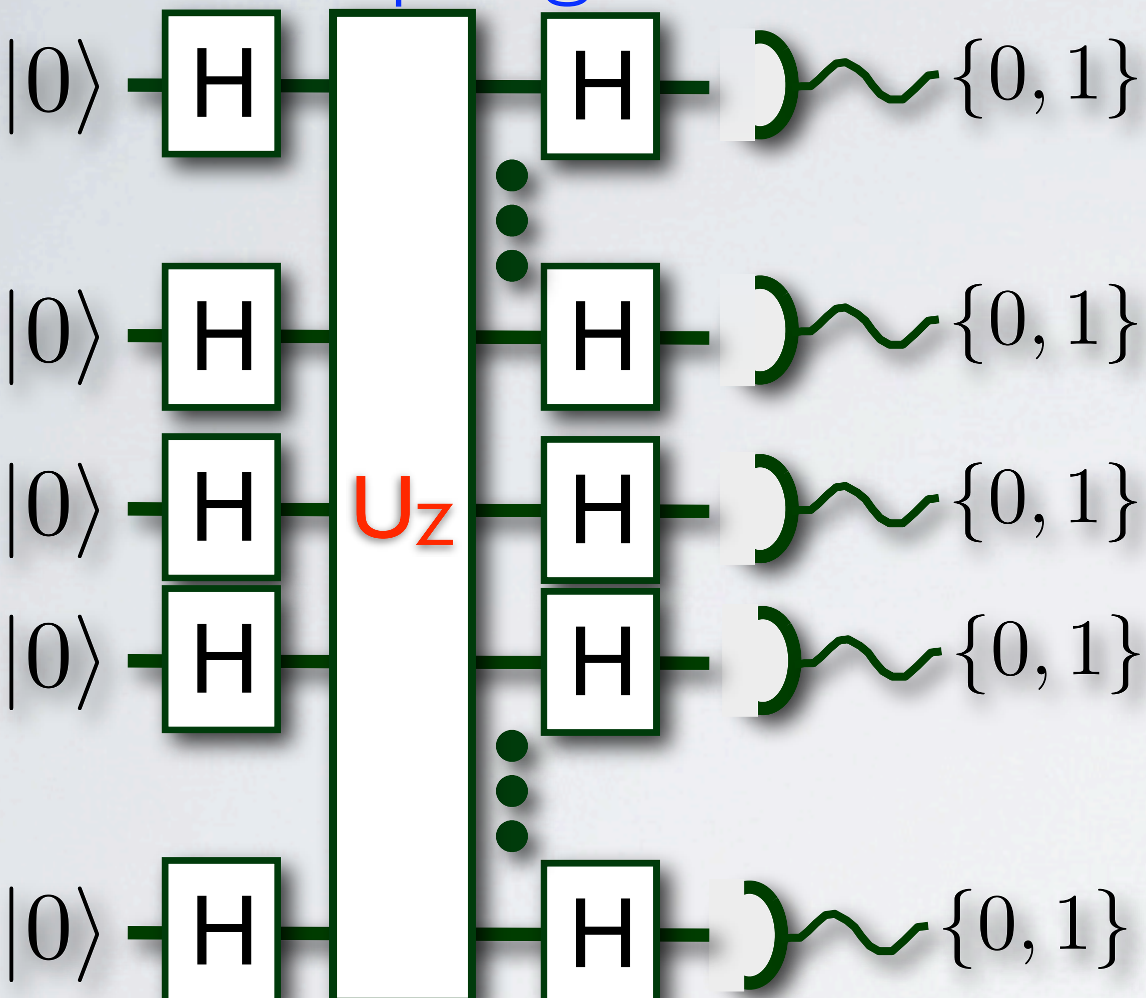
To appear: Proc. R. Soc. A. arXiv:1005.1407
+ D. Shepherd, arXiv:1005.1744

WHY?

- Motivation: Can we build a convincing complexity theoretic argument that quantum computers are not classically simulable? Can we do it with non-universal gate sets?
  - ~~Because I hate classical CS theory so much that I want to crush it with its own tools ..~~
  - Because I love experimentalists and quantum computers are hard to build.

PAY ATTENTION NOW

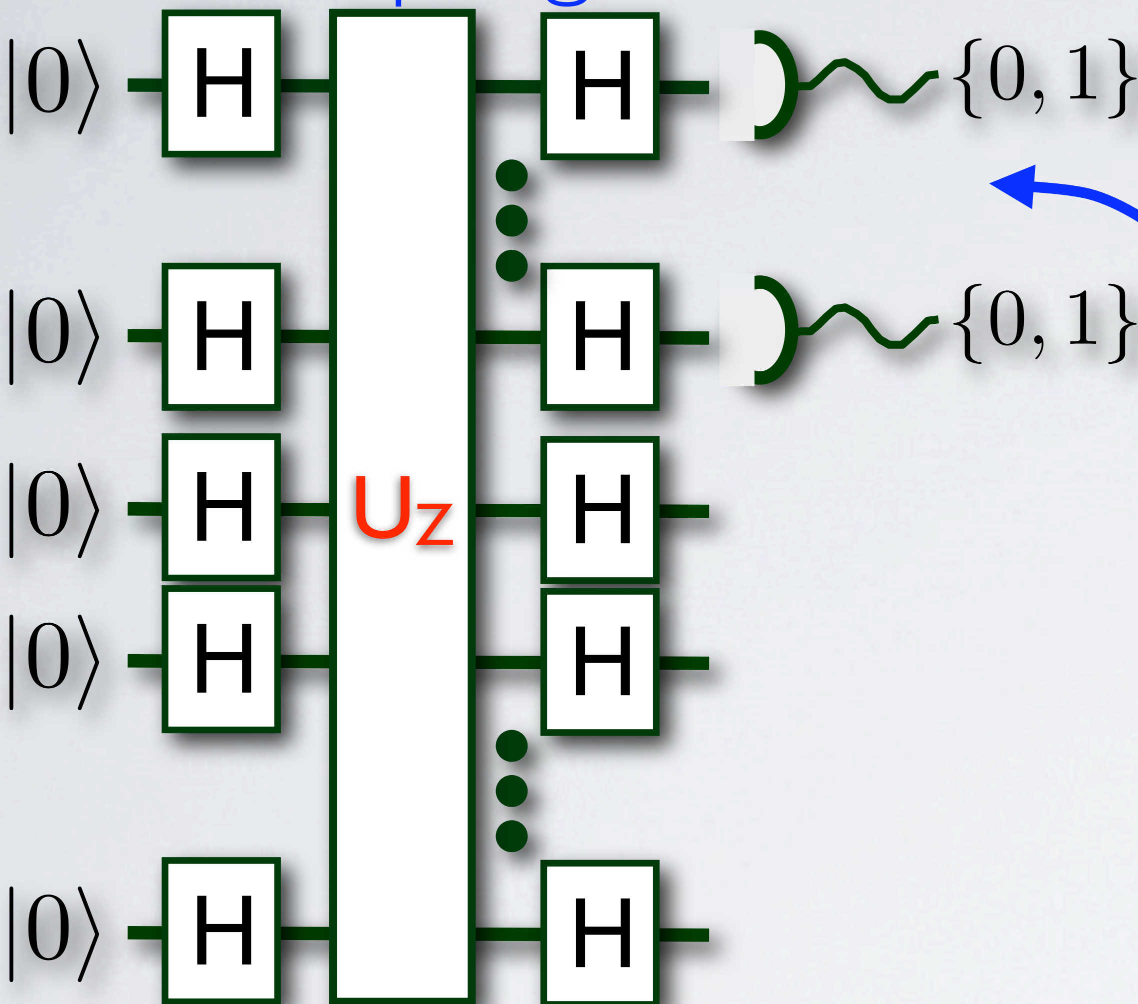
IQP sampling:



Given **n** bit string, **w**, the circuit C_w is uniformly generated (in poly n time). The resulting output distribution is P_w. U_Z is Z-diagonal.

PAY ATTENTION NOW

IQP sampling:



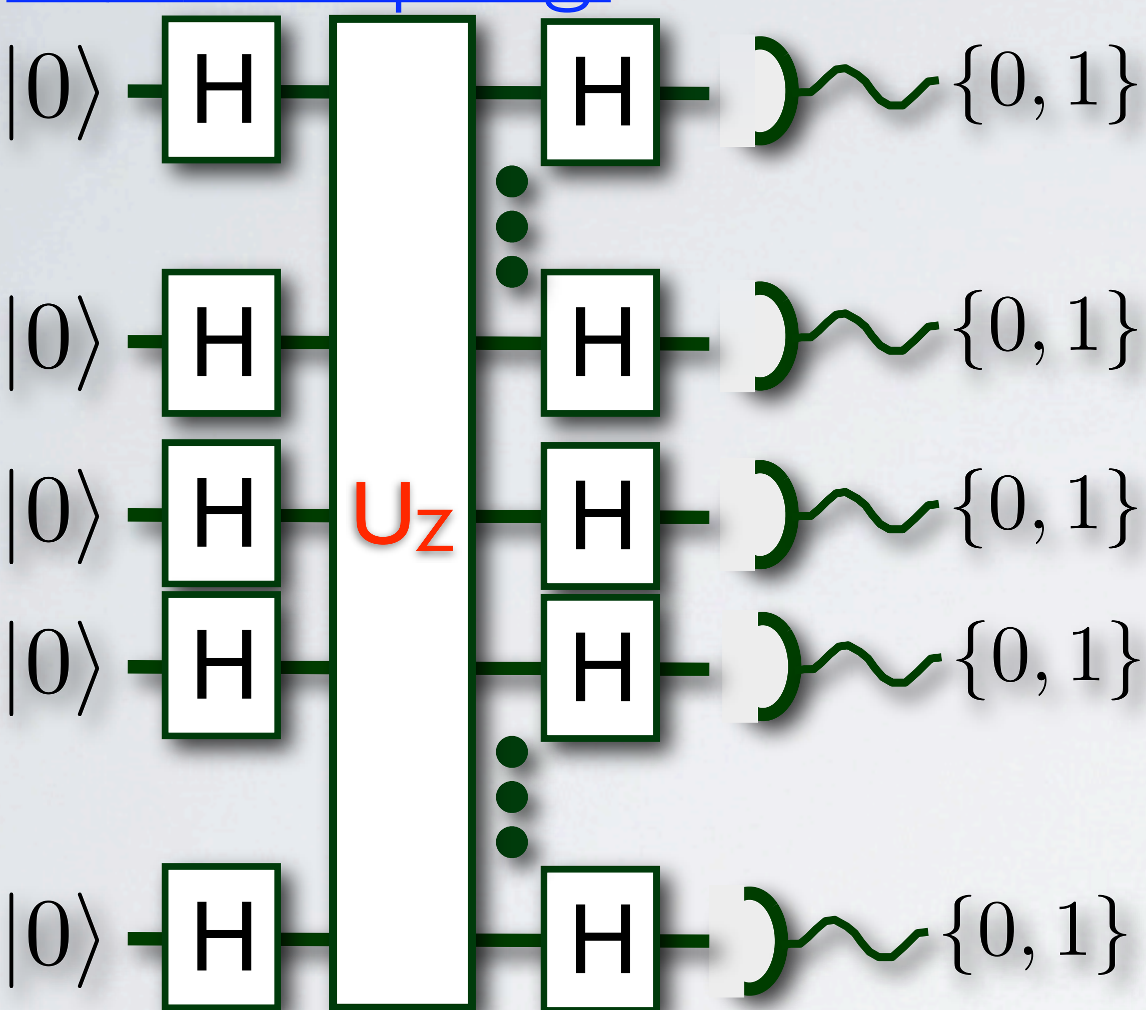
IQP is easy theorem: If the output of uniform (poly-time/size) IQP circuits is restricted to O(log n) may be sampled (without approximation) by a classical randomized process that runs in time O(poly n).

O(log n) qubits

Given **n** bit string, **w**, the circuit **C_w** is uniformly generated (in poly n time). The resulting output distribution is **P_w**. **U_Z** is Z-diagonal.

PAY ATTENTION NOW

IQP sampling:



Given **n** bit string, **w**, the circuit C_w is uniformly generated (in poly n time). The resulting output distribution is P_w. U_Z is Z-diagonal.

U_Z is a circuit with O(poly n) Z, CZ, $e^{i(\pi/8)}$ gates.

IQP is easy theorem: If the output of uniform (poly-time/size) IQP circuits is restricted to O(log n) may be sampled (without approximation) by a classical randomized process that runs in time O(poly n).

IQP is hard theorem: If the output of uniform (poly-time/size) IQP circuits could be weakly classically efficiently simulated to within 41% ($1 \leq c < 2^{1/2}$) *multiplicative error*, then the Polynomial Hierarchy would collapse to within it's 3rd level.

SO, ARE WE DONE?

- Not really, there is a really big problem with this theorem, *it isn't clear* that a quantum computer can simulate an IQP circuit to within a constant multiplicative error!!!!
- What is simulation?
- Ultimately we are determining the cost of:
  - Strong simulation: explicitly calculating any probability in ***P****w* and its marginals. [Terhal and DiVincenzo '02: Strong simulation of *constant depth* quantum circuits results in a collapse of the PH. (quant-ph/0205133]
  - Weak simulation: approximately sample from ***P****w* with ***R****w*. [Multiplicative simulation results : us and Aaronson and Arkhipov '10]
  - Strong implies weak.

IQP is hard theorem: If the output of uniform (poly-time/size) IQP circuits could be weakly classically efficiently simulated to within 41% ($1 \leq c < 2^{1/2}$) *multiplicative error*, then the Polynomial Hierarchy would collapse to within it's 3rd level.

Weak multiplicative simulation:

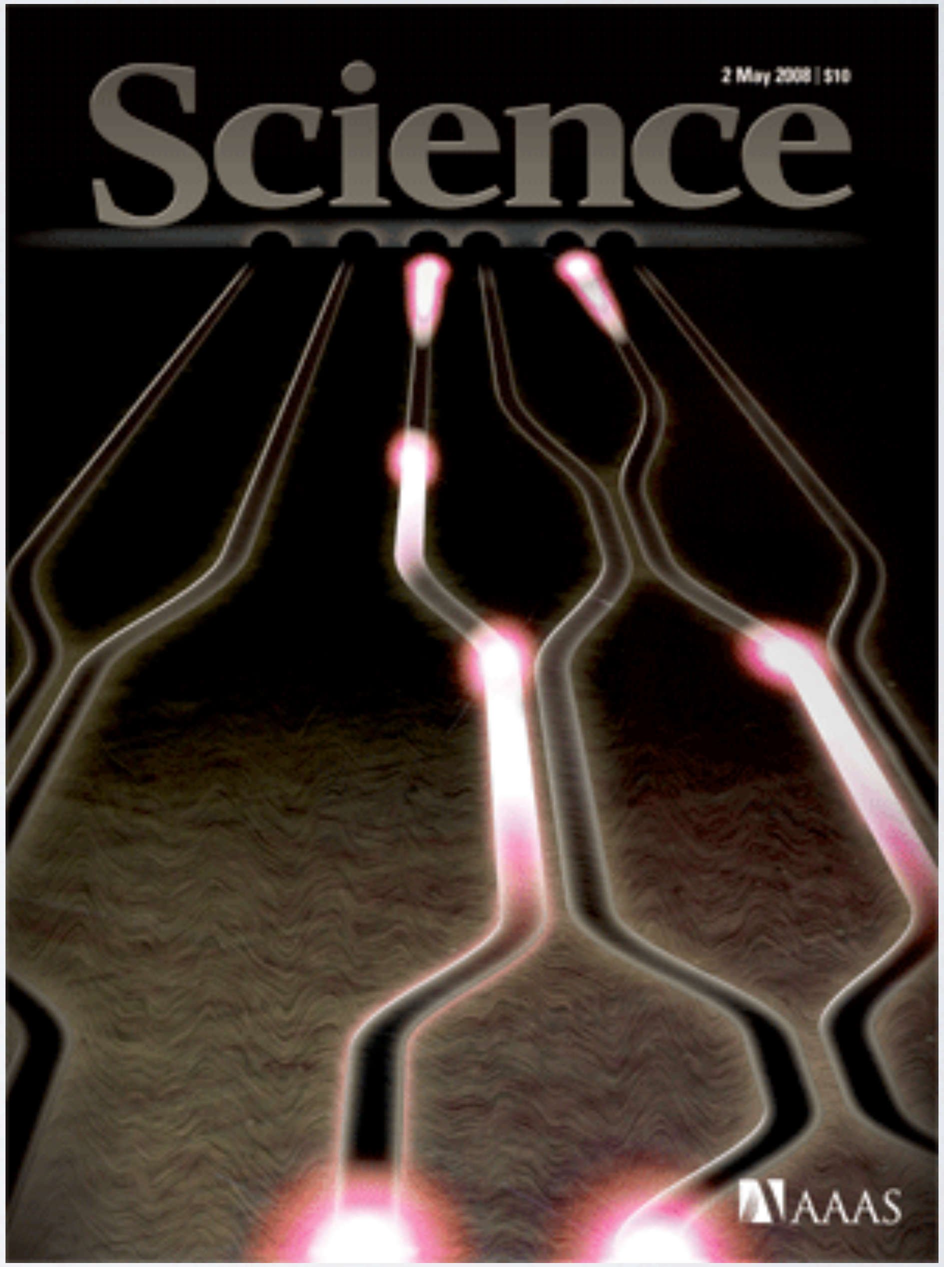
$$\frac{1}{c}\,\mathrm{prob}[P_w = x] \leq \mathrm{prob}[R_w = x] \leq c\,\mathrm{prob}[P_w = x]$$

Weak additive simulation, eg:

$$\sum_x |\mathrm{prob}[P_w = x] - \mathrm{prob}[R_w = x]| \leq \epsilon$$ ✓

A&A AND ADDITIVE ERRORS

- **If BOSONSAMPLING can be classically simulated in polytime with multiplicative error then PH collapses.** [Aaronson and Arkhipov QIP '10, arXiv:1011.3245]
- **If BOSONSAMPLING can be classically simulated with additive error in polytime then the PH collapses** - so long as:
  - The Permanent-of-Gaussians conjecture is true, and
  - The Permanent anti-concentration conjecture is true.
- Argument relies heavily on the use of **#P-complete** counting problems with a natural relationship to Bosonic systems.
- Does not hold (we think!) for decision languages based on post-selection.



MUA SLIDE (SLEEP TIME?)

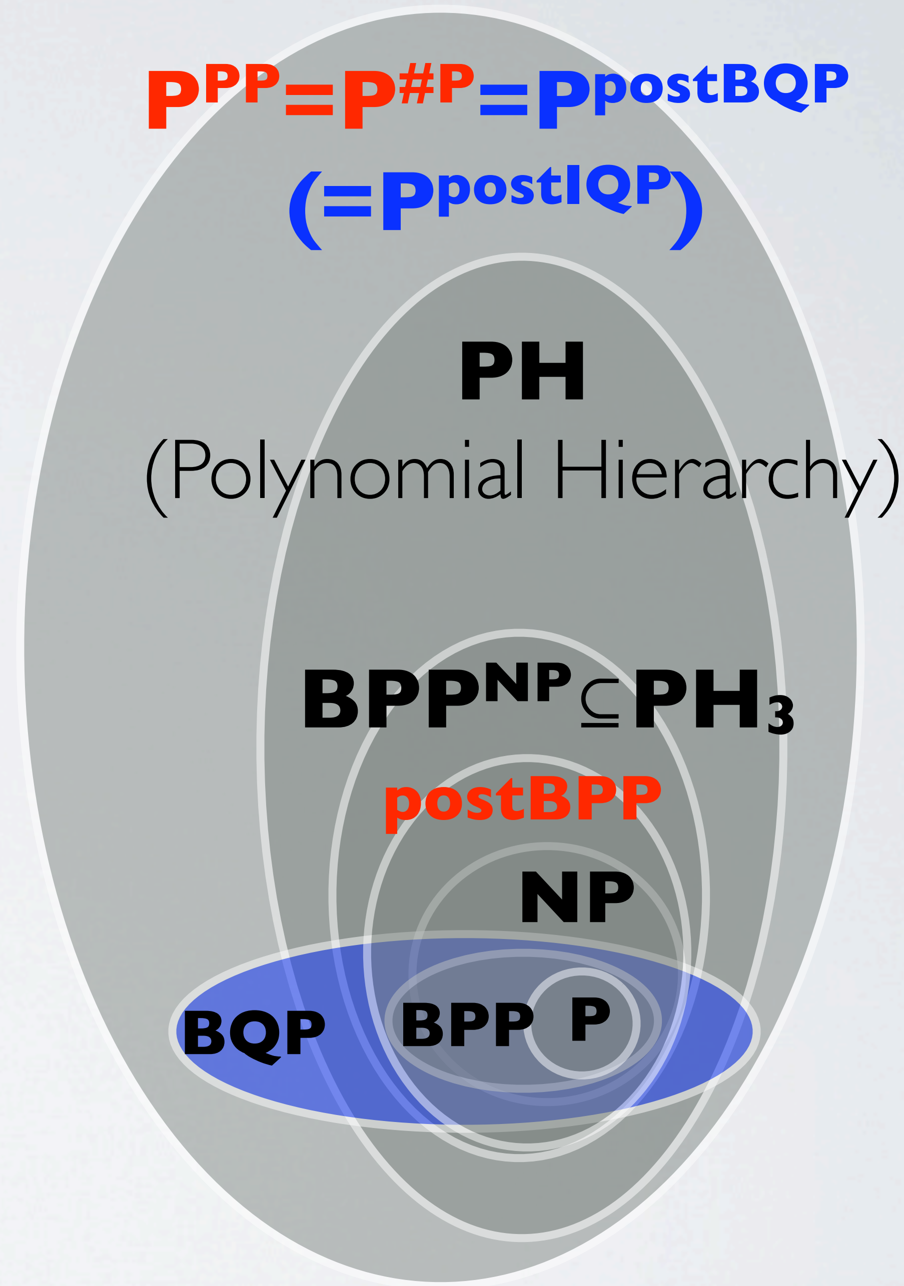
- Aaronson ’04: postBQP=PP

  (=postIQP)

- Toda’s Theorem ’91: PH$\subseteq$ P^{PP}=$P^{\#P}$

- Han et al ’97:
  postBPP (BPP_{path})$\subseteq$$BPP^{NP}$$\subseteq$$PH_3$

- *If* postIQP (or postBQP) = postBPP
  then $P^{postBPP} \subseteq P^{BPP^{NP}} \subseteq BPP^{NP}$.



$$PH = \bigcup_k \Delta_k, k \to \infty$$

$$\Delta_1 = P, \Delta_{k+1} = P^{N\Delta_k}$$

MUA SLIDE (SLEEP TIME?)

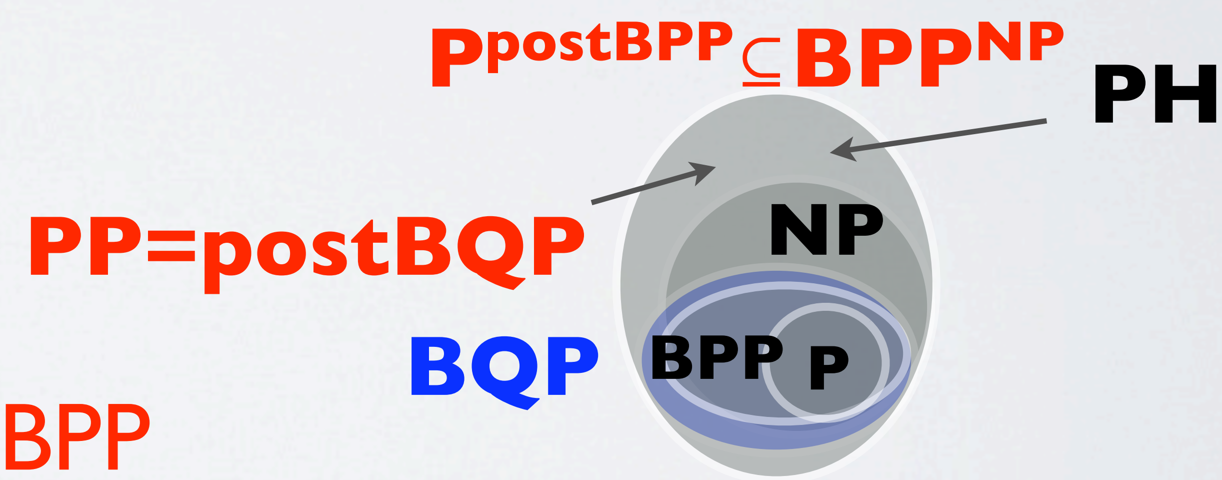
- Aaronson '04: postBQP=PP

  (=postIQP)

- Toda's Theorem '91: PH$\subseteq$ P^{PP}=$P^{\#P}$

- Han et al '97:
  postBPP (BPP_{path})$\subseteq$$BPP^{NP}$$\subseteq$$PH_3$

- *If* postIQP (or postBQP) = postBPP
  then $P^{postBPP}$ $\subseteq$ $P^{BPP^{NP}}$ $\subseteq$ BPP^{NP}.



$$PH = \bigcup_k \Delta_k, k \to \infty$$

$$\Delta_1 = P, \Delta_{k+1} = P^{N\Delta_k}$$

MUA SLIDE (SLEEP TIME?)

What kind of simulation could cause this collapse?

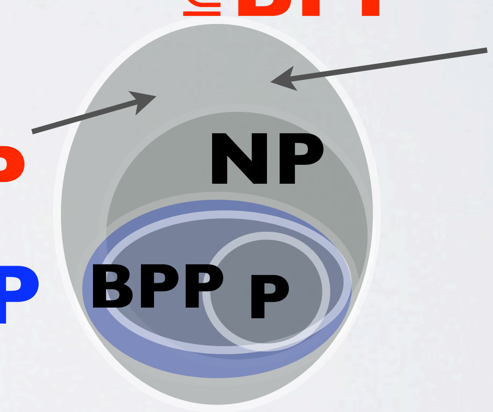
- Aaronson '04: postBQP=PP

  (=postIQP)

- Toda's Theorem '91: PH$\subseteq$ P^{PP}=P$^{\#P}$

- Han et al '97:
  postBPP (BPP$_{path}$)$\subseteq$BPP^{NP}$\subseteq$PH$_3$

- *If* postIQP (or postBQP) = postBPP
  then P^{postBPP} $\subseteq$ P$^{BPP^{NP}}$ $\subseteq$ BPP^{NP}.



$$PH = \bigcup_k \Delta_k, k \to \infty$$

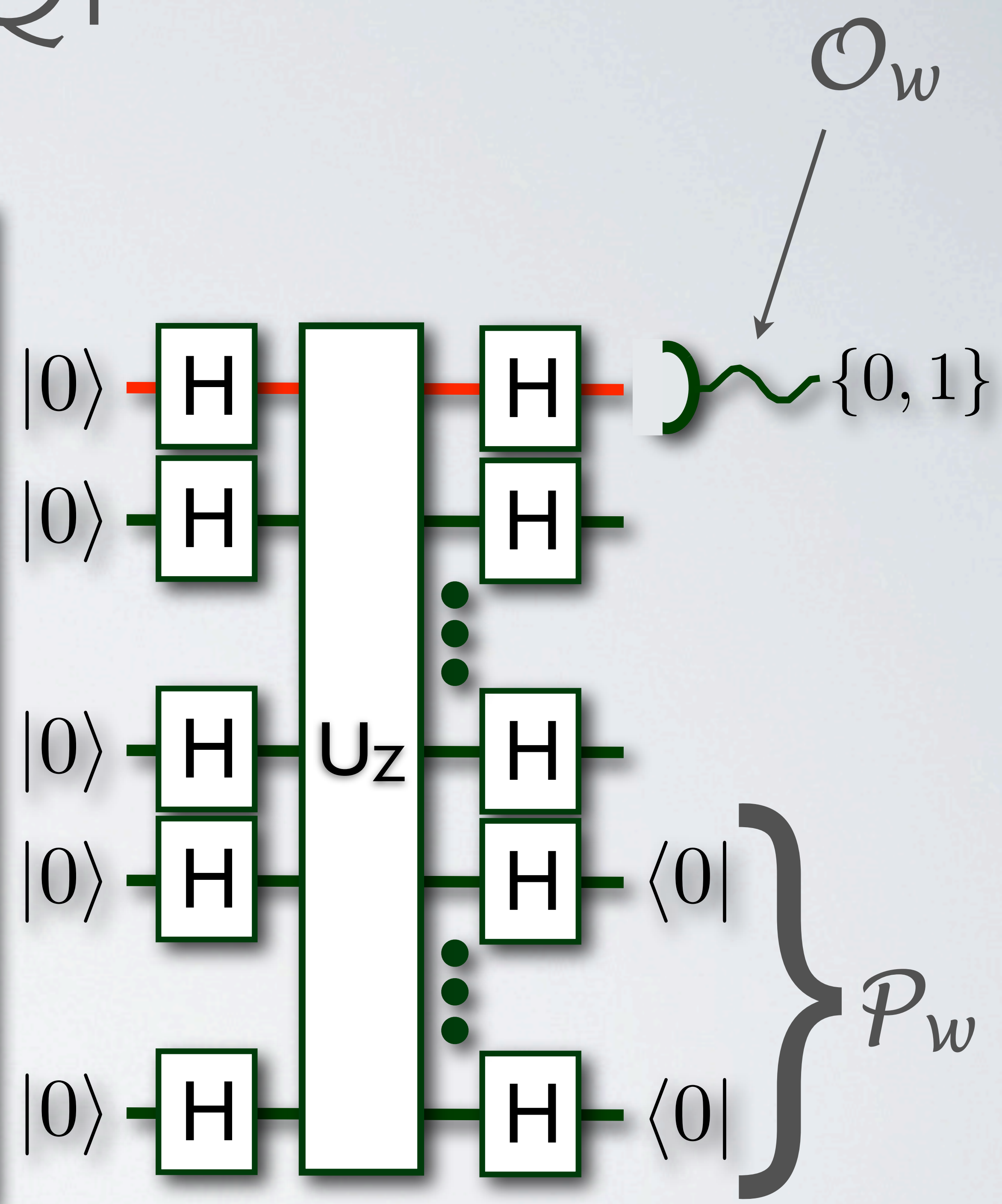
$$\Delta_1 = P, \Delta_{k+1} = P^{N\Delta_k}$$

POSTIQP

Definition (postIQP):

A language L is in the class postIQP (resp. postBQP or postBPP) iff there is an error tolerance $0 < \varepsilon < 1/2$ and a uniform family $\{C_w\}$ of post-selected IQP (resp. quantum or 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 $\text{prob}[\mathcal{O}_w = 1 | \mathcal{P}_w = 00\ldots0] \geq 1-\varepsilon$ and
(ii) if $w \notin L$ then $\text{prob}[\mathcal{O}_w = 0 | \mathcal{P}_w = 00\ldots0] \geq 1-\varepsilon$.



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

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

Proof sketch:

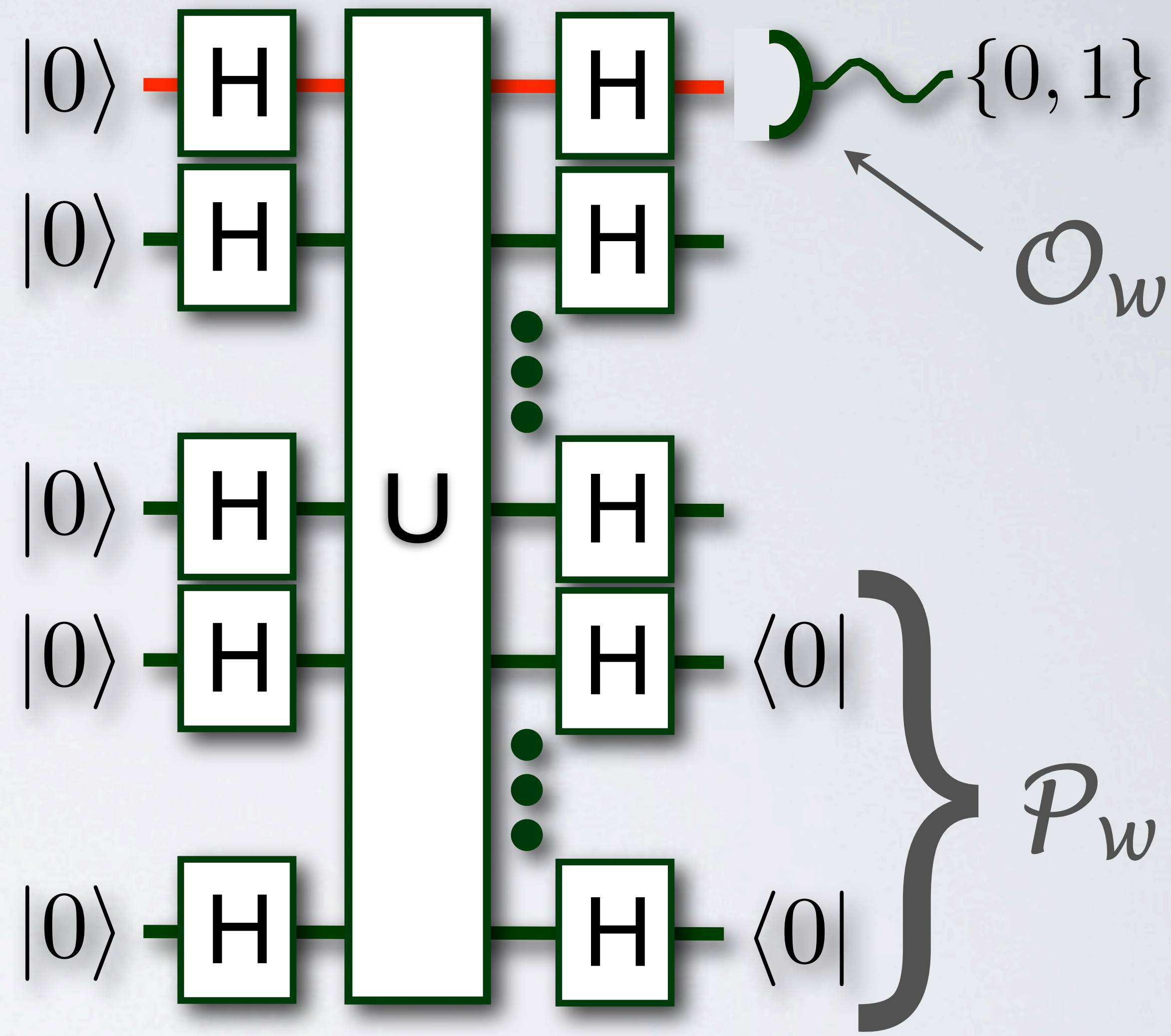
Given L ∈ **postIQP**, then there is a uniform family of post-selected circuits C_w that can decide the language with the following error bounds:

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

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

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 $1 \leq c < 2^{1/2}$. □

POSTIQP = PP

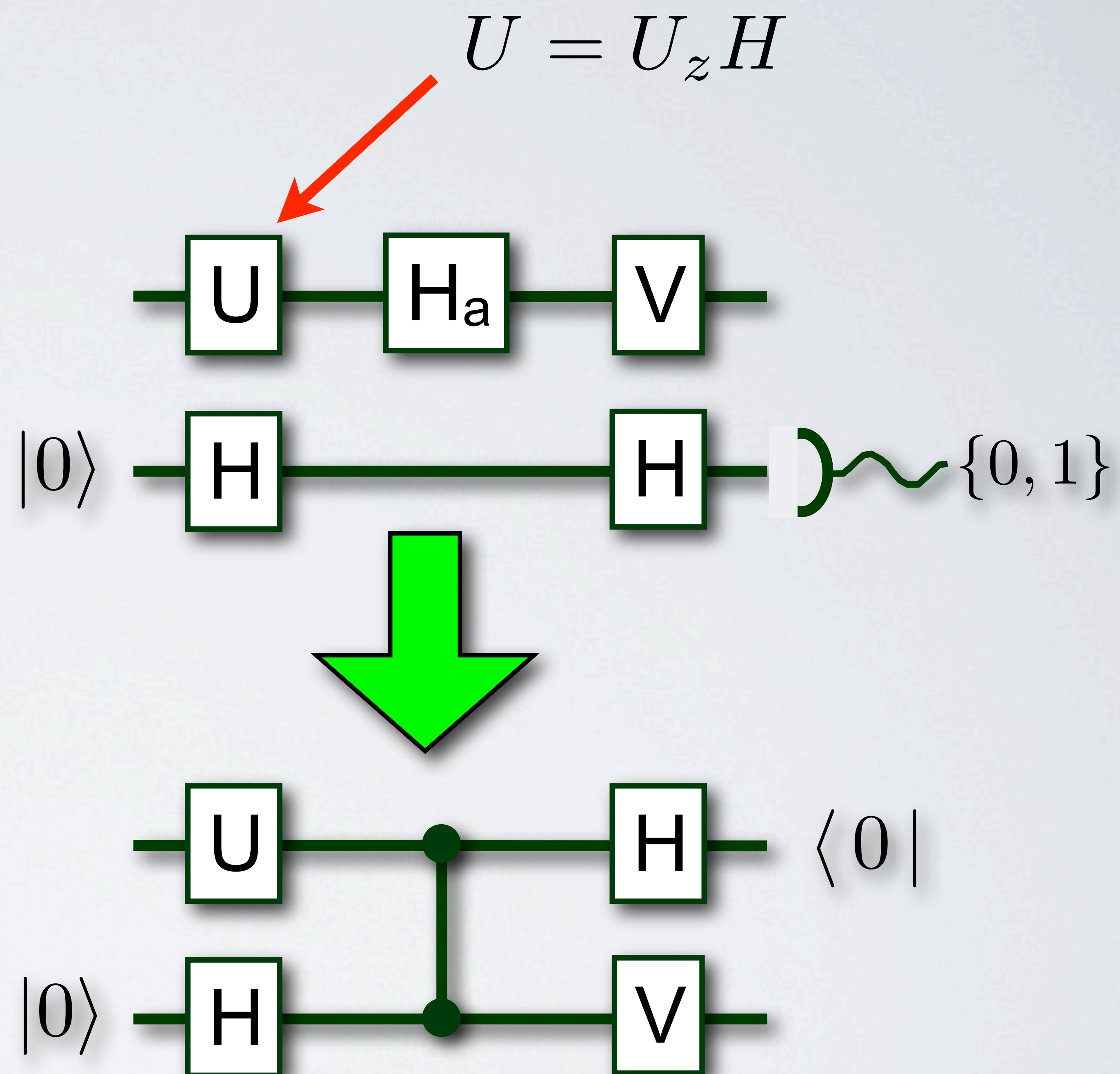
Proof by construction using **postBQP =PP**:

- Take any circuit in BQP expressed in terms of the following universal gate set: H, Z, CZ, $e^{i(\pi/8)Z}$.
- Only need to “remove” intermediate H’s to make a circuit in IQP.
- “Hadamard gadget” does this.
- As there are at most O(poly n) Hadamards then we will only ever add O(poly n) new qubits.

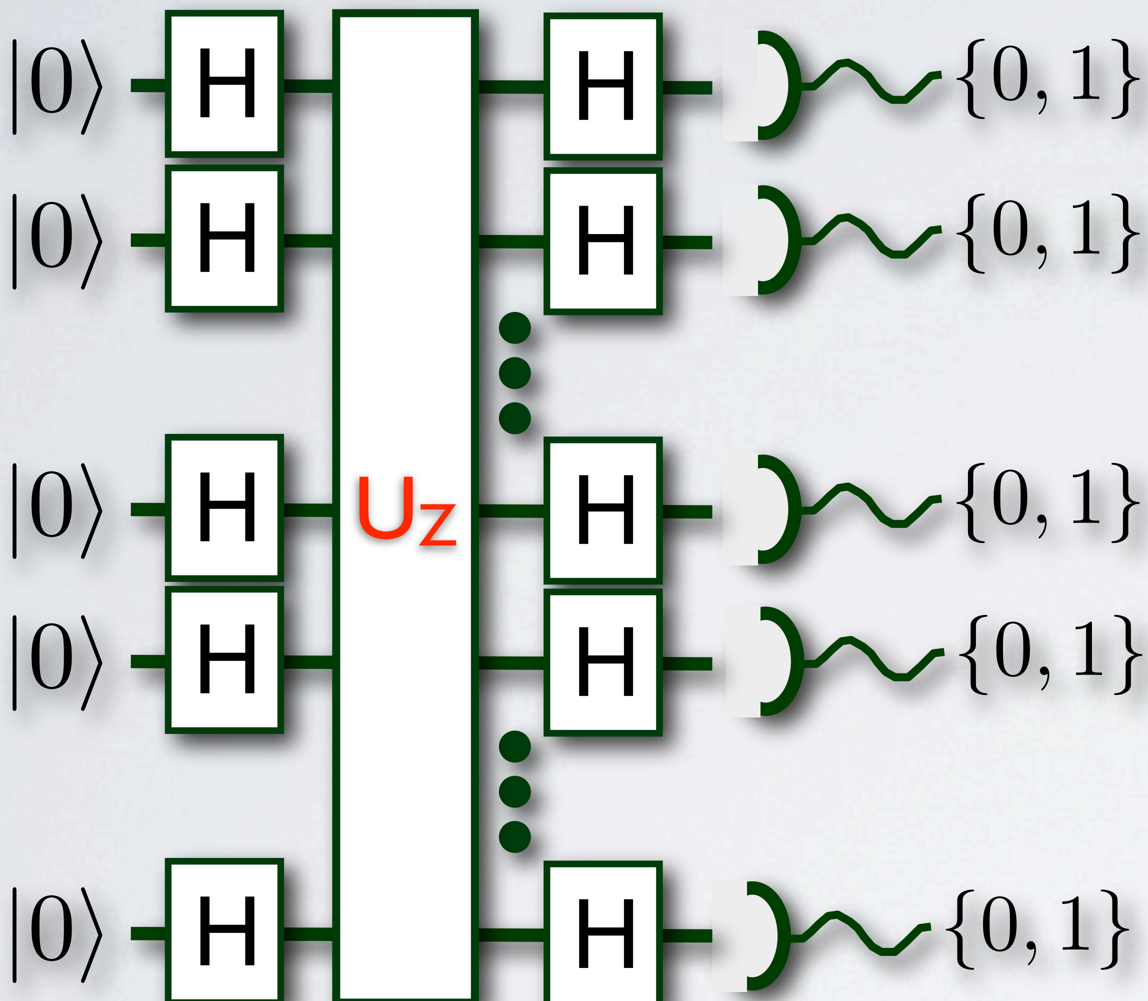
$\square$

Note: An alternate proof can be used to show that the subset of IQP circuits for which this holds is inside QNC^0.

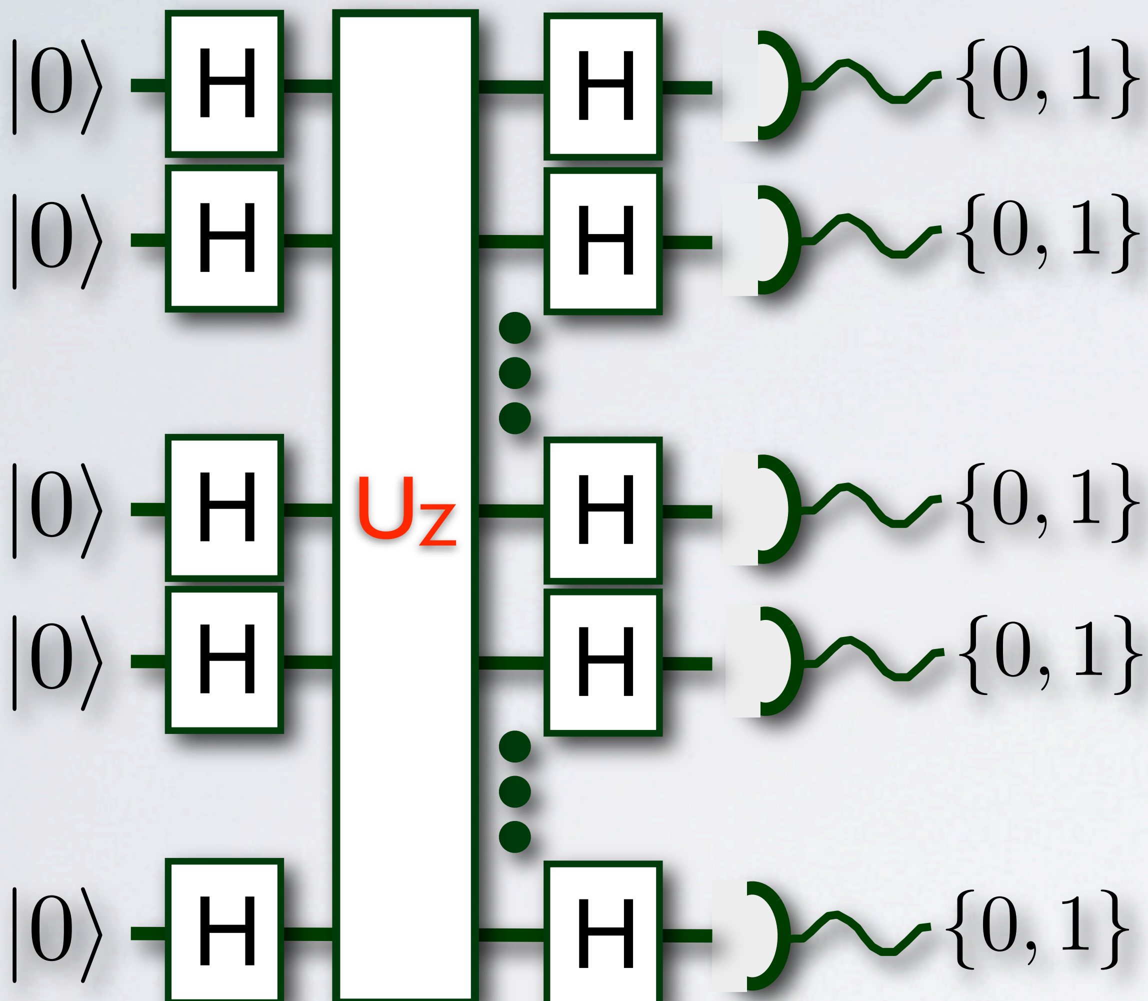
- The same proof shows that this holds for n.n. interactions in 2d.



WHY IQP? (PHYSICSISH)

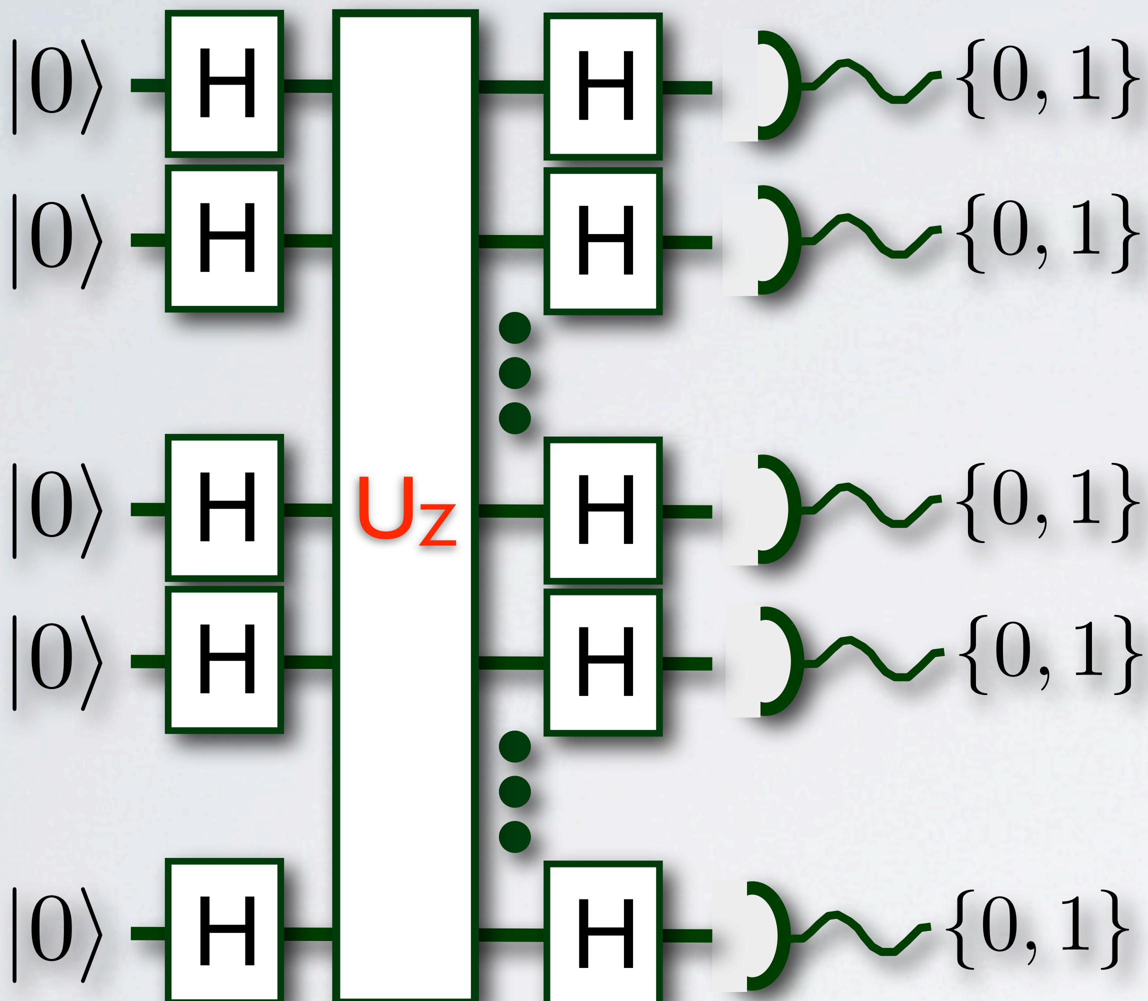


WHY IQP? (PHYSICSISH)



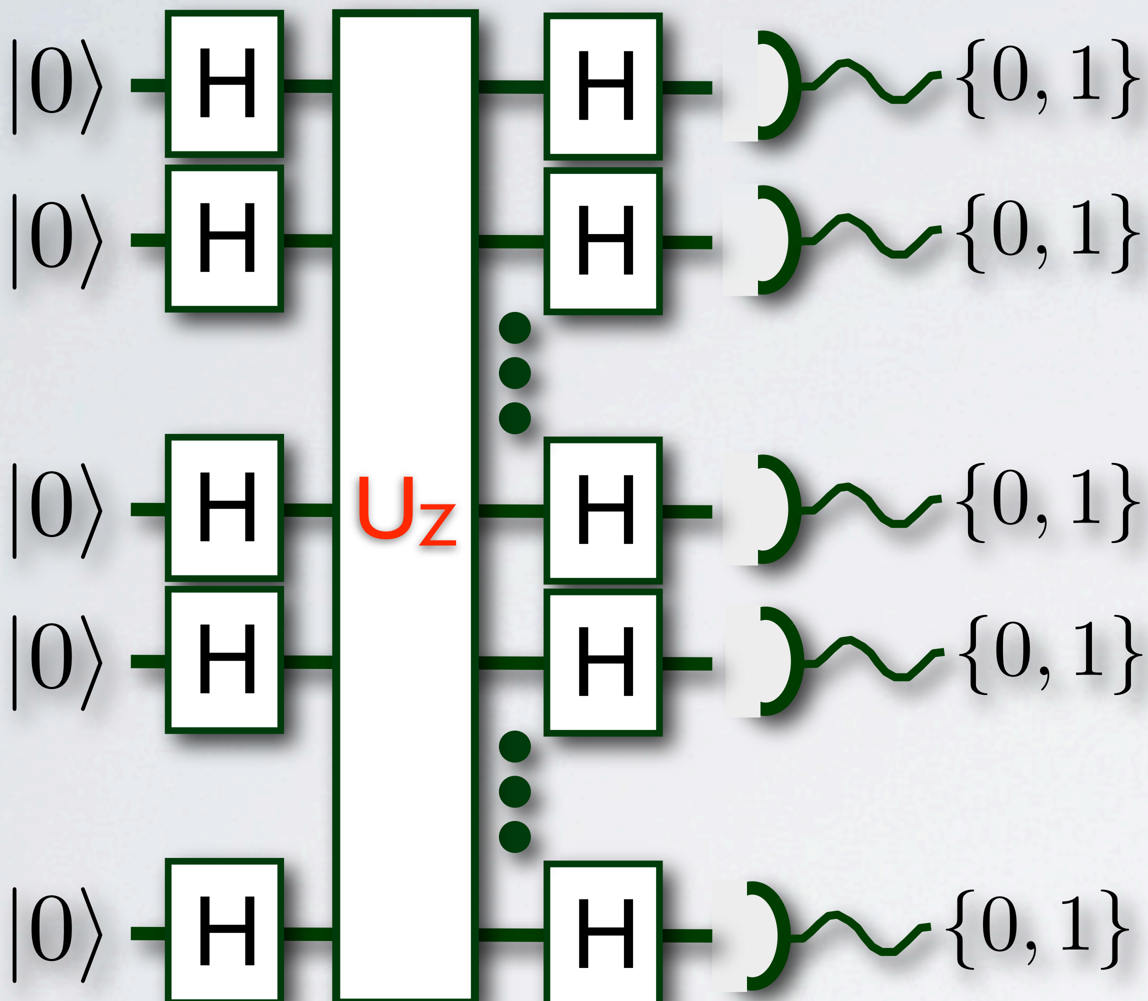
- ~~The math is really easy.~~

WHY IQP? (PHYSICSISH)



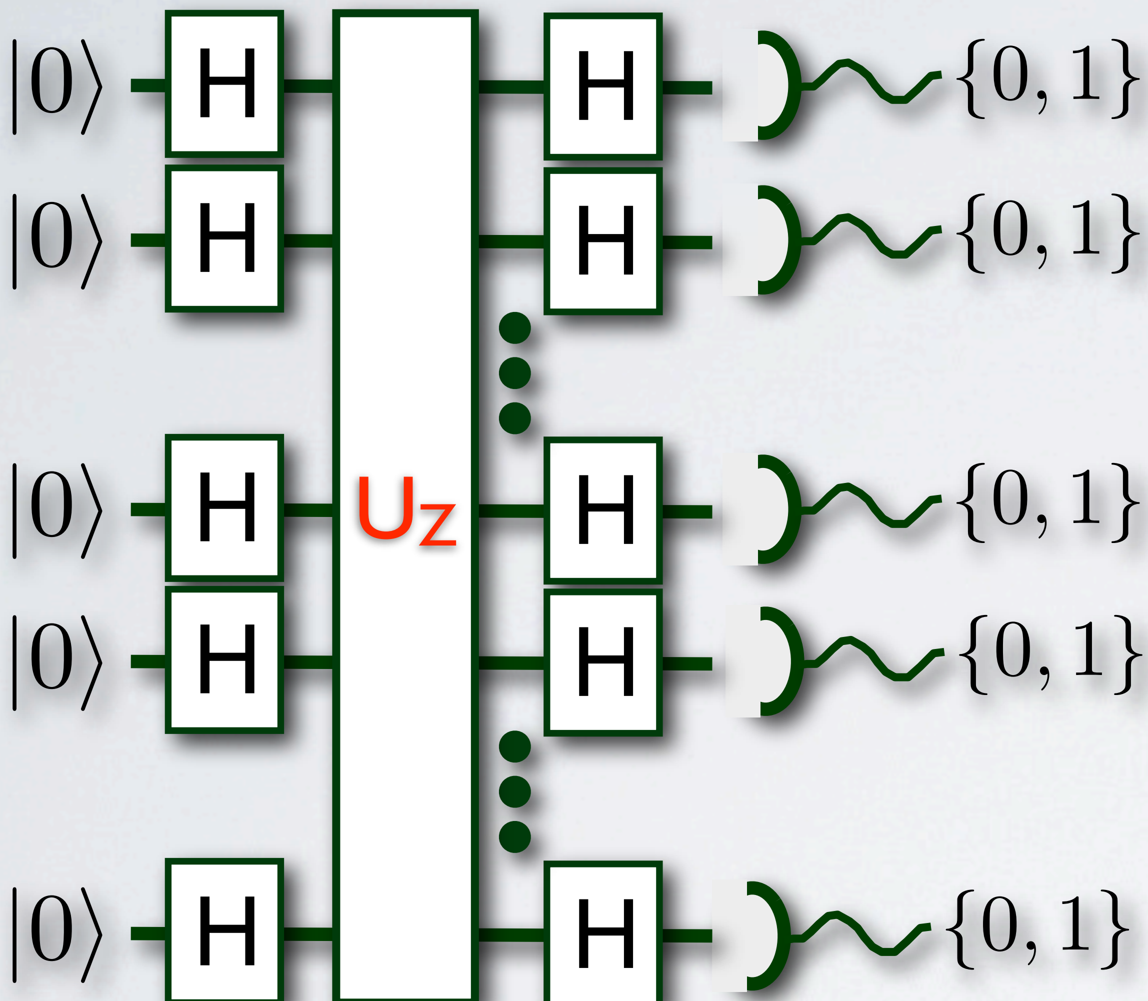
- ~~The math is really easy.~~
- It has really interesting physical properties for implementation:

WHY IQP? (PHYSICSISH)



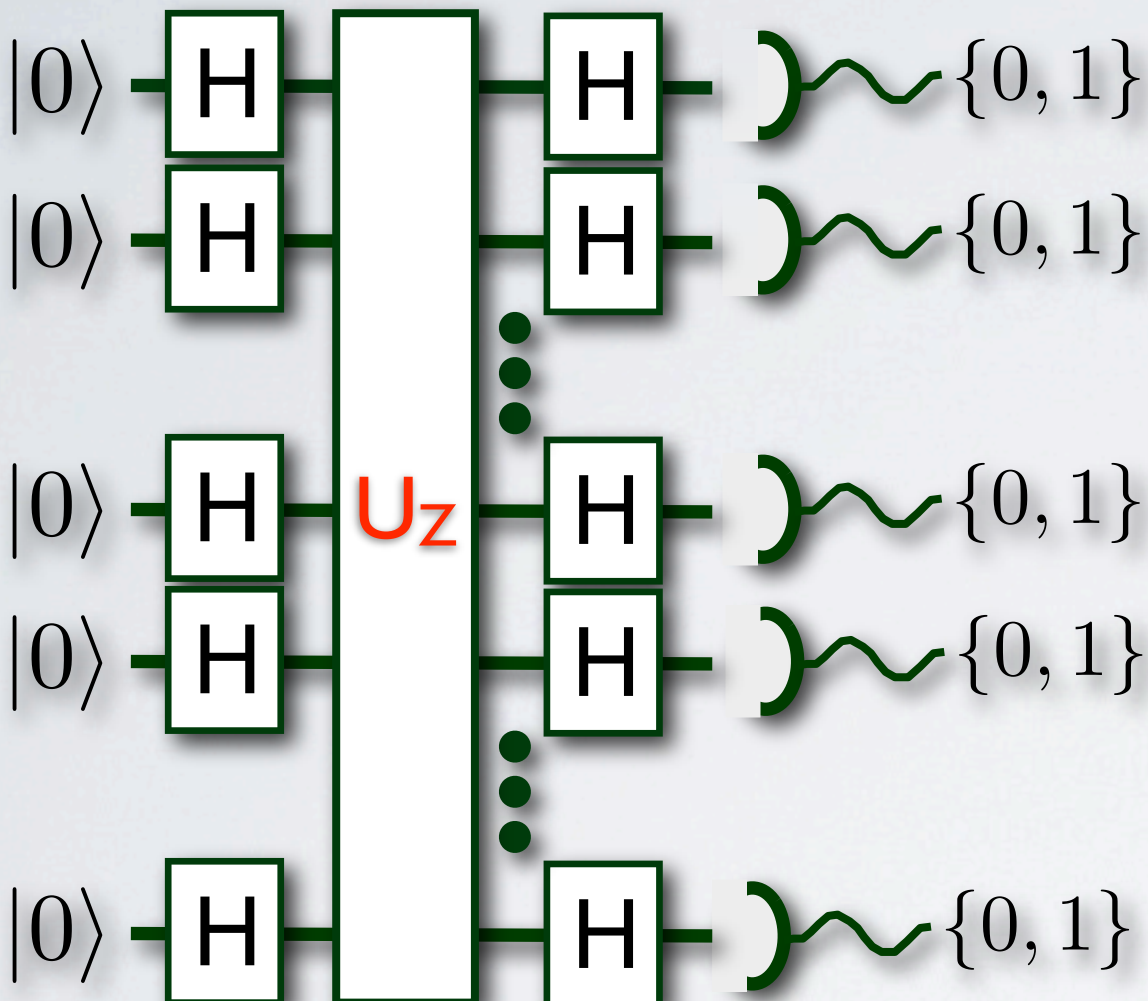
- ~~The math is really easy.~~
- It has really interesting physical properties for implementation:
  - Implemented by non-adaptive graph state computation.

WHY IQP? (PHYSICSISH)



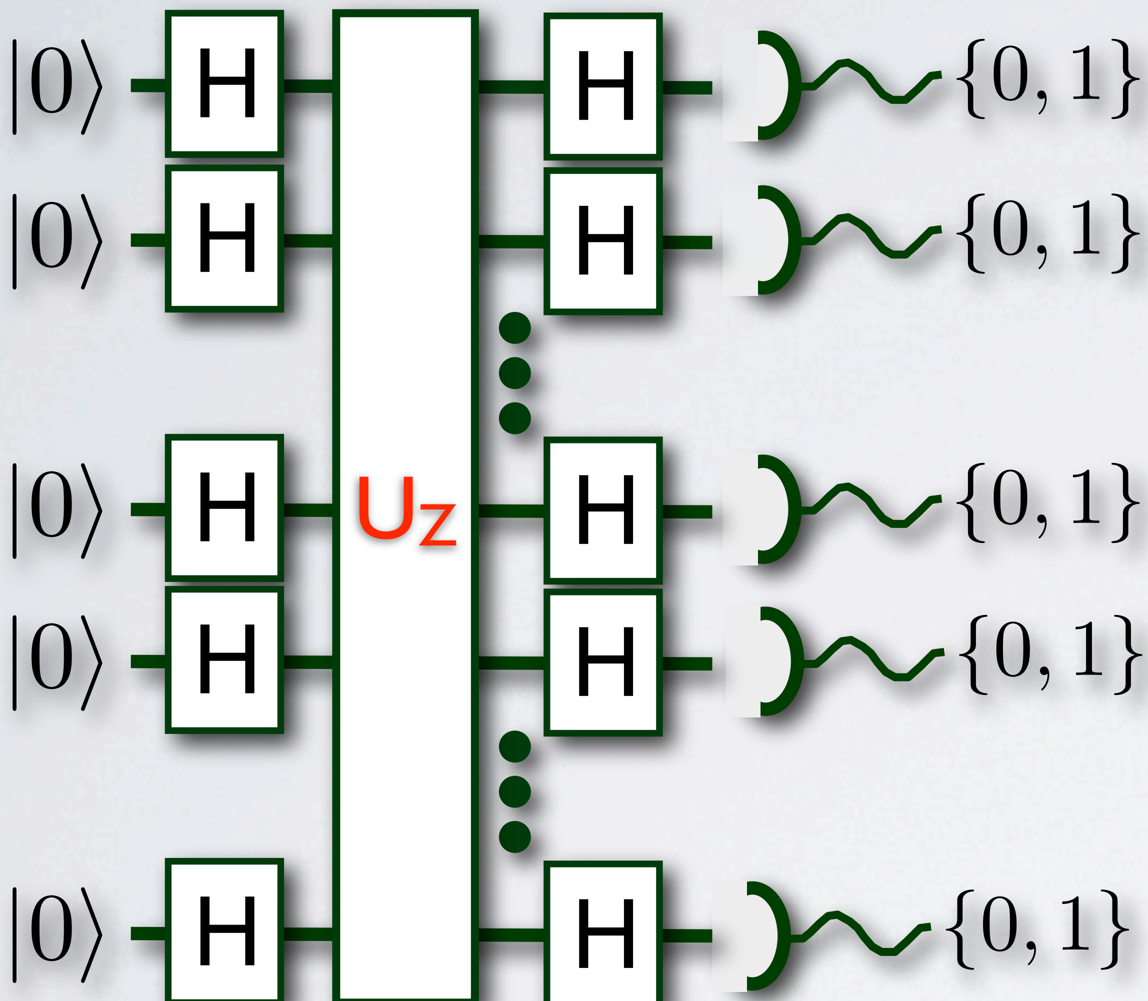
- ~~The math is really easy.~~
- It has really interesting physical properties for implementation:
  - Implemented by non-adaptive graph state computation.
  - In some solid-state systems evolution speeds are biased.

WHY IQP? (PHYSICSISH)



- ~~The math is really easy.~~
- It has really interesting physical properties for implementation:
  - Implemented by non-adaptive graph state computation.
  - In some solid-state systems evolution speeds are biased.
- IQP circuits have better thresholds in biased noise models tailored to superconducting qubit architectures. [Aliferis et al 09]

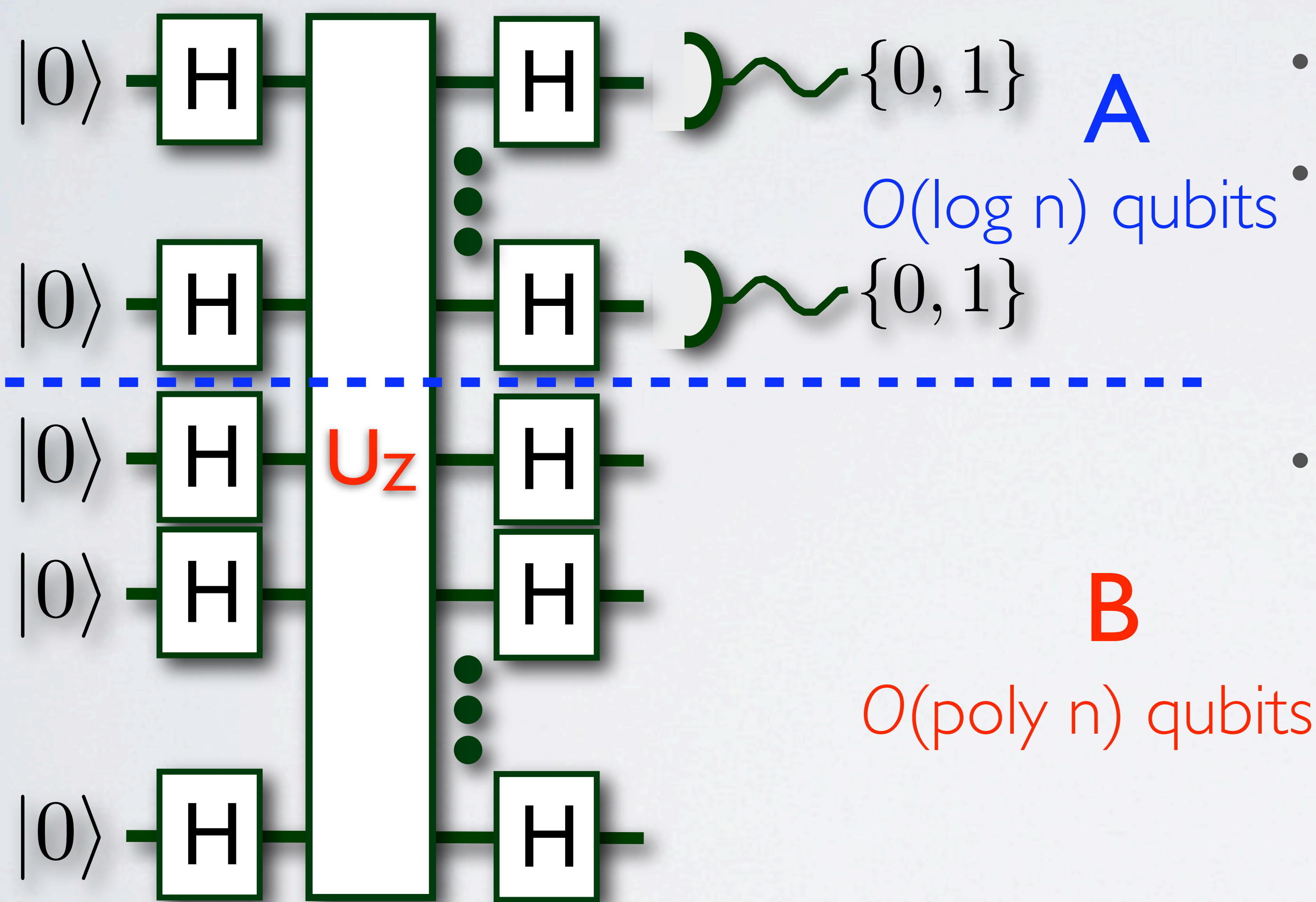
WHY IQP? (PHYSICSISH)



- ~~The math is really easy.~~
- It has really interesting physical properties for implementation:
  - Implemented by non-adaptive graph state computation.
  - In some solid-state systems evolution speeds are biased.
- IQP circuits have better thresholds in biased noise models tailored to superconducting qubit architectures. [Aliferis et al 09]
- Quantum simulations

WHY IQP? (CSISH)

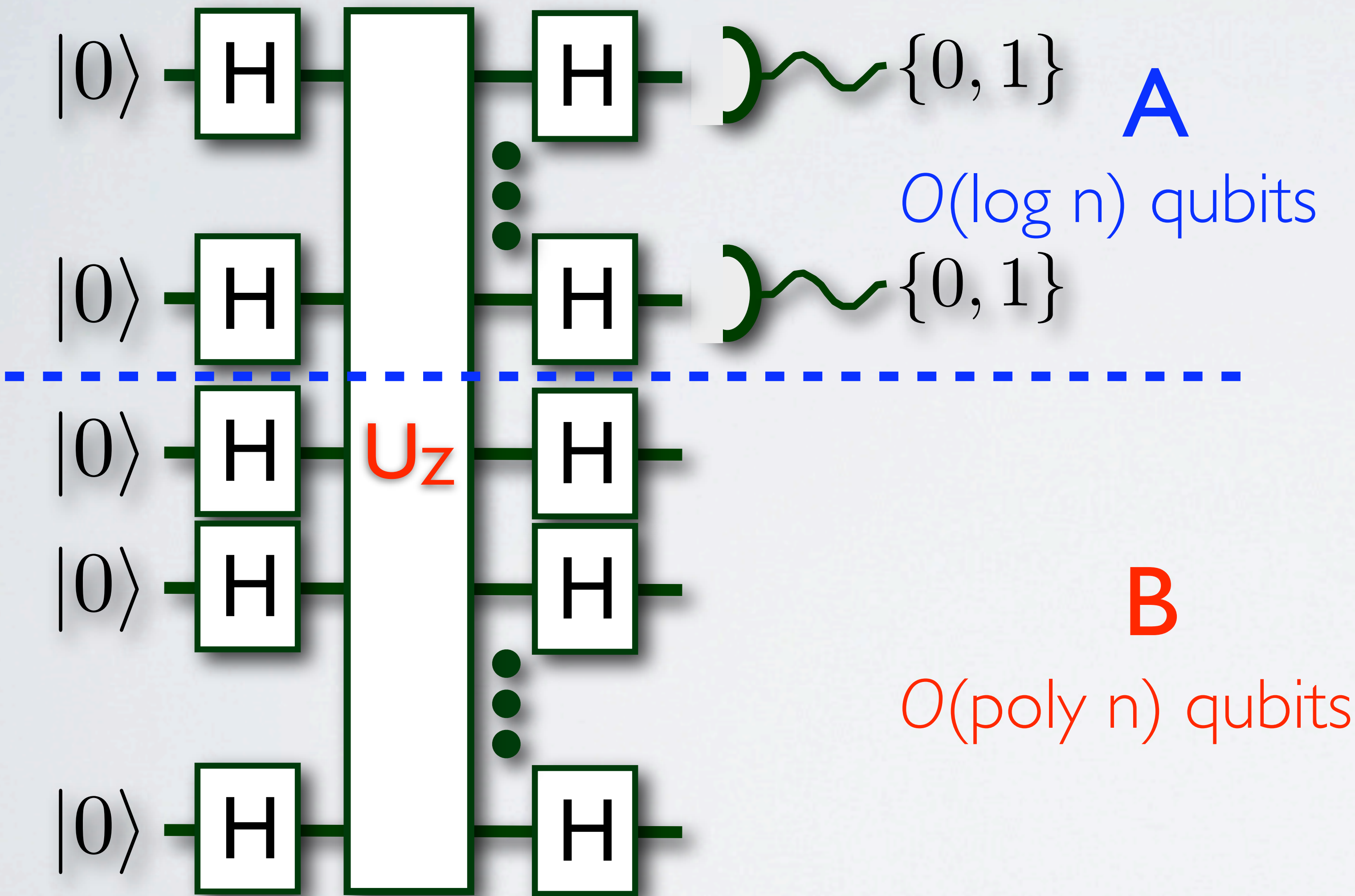
IQP is easy theorem: If the output of uniform (poly-time/size) IQP circuits is restricted to O(log n) may be sampled (without approximation) by a classical randomized process that runs in time O(poly n).



- ~~The math is really easy.~~
- This is certainly not true for BQP, QNC, QNC^0_f otherwise factoring is in BPP!
- We can use classical simulations to randomly verify outcomes.
  - Thus we might be able to construct tests to verify the success of experiments.

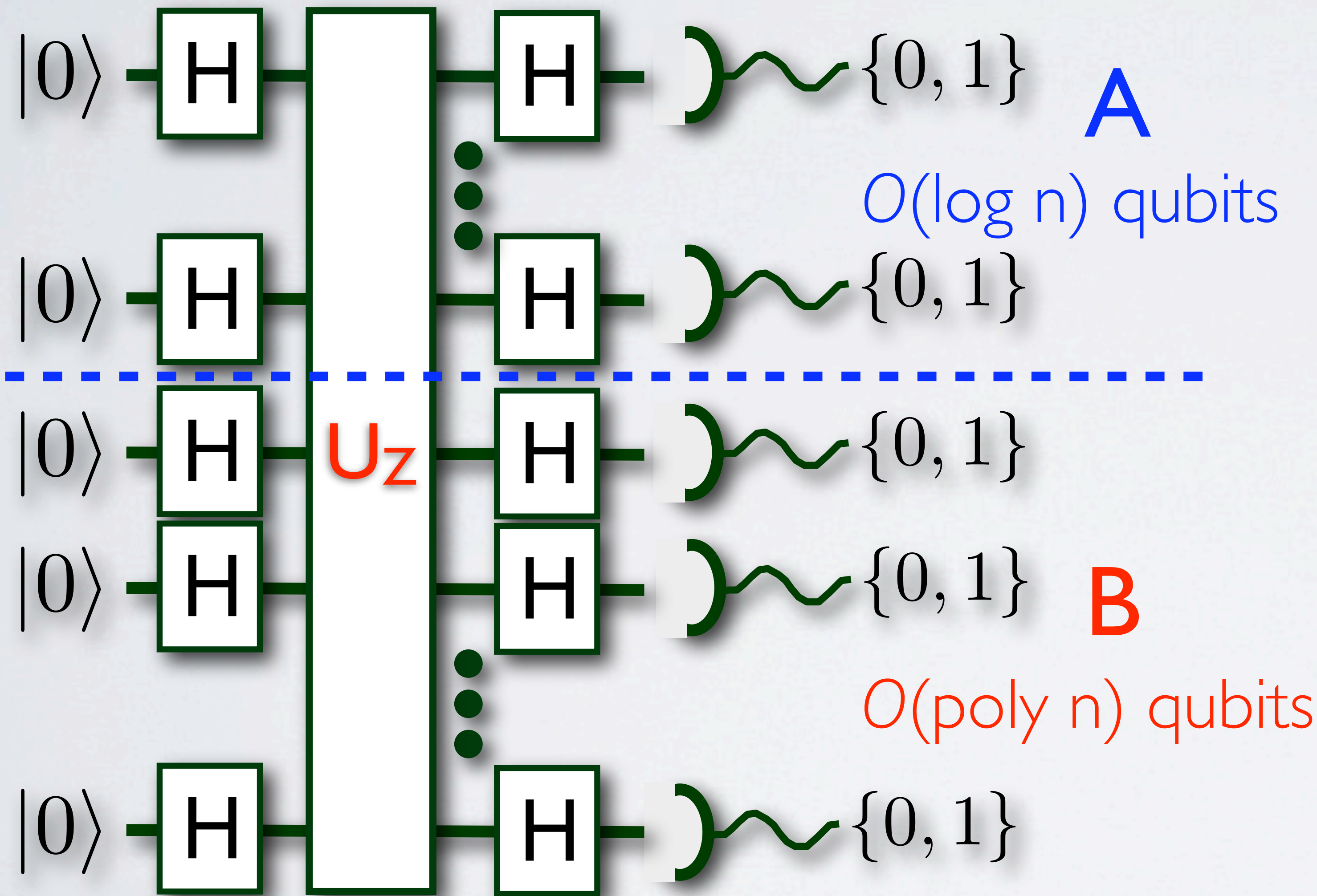
WHY IQP? (CSISH)

IQP is easy theorem: If the output of uniform (poly-time/size) IQP circuits is restricted to O(log n) may be sampled (without approximation) by a classical randomized process that runs in time O(poly n).



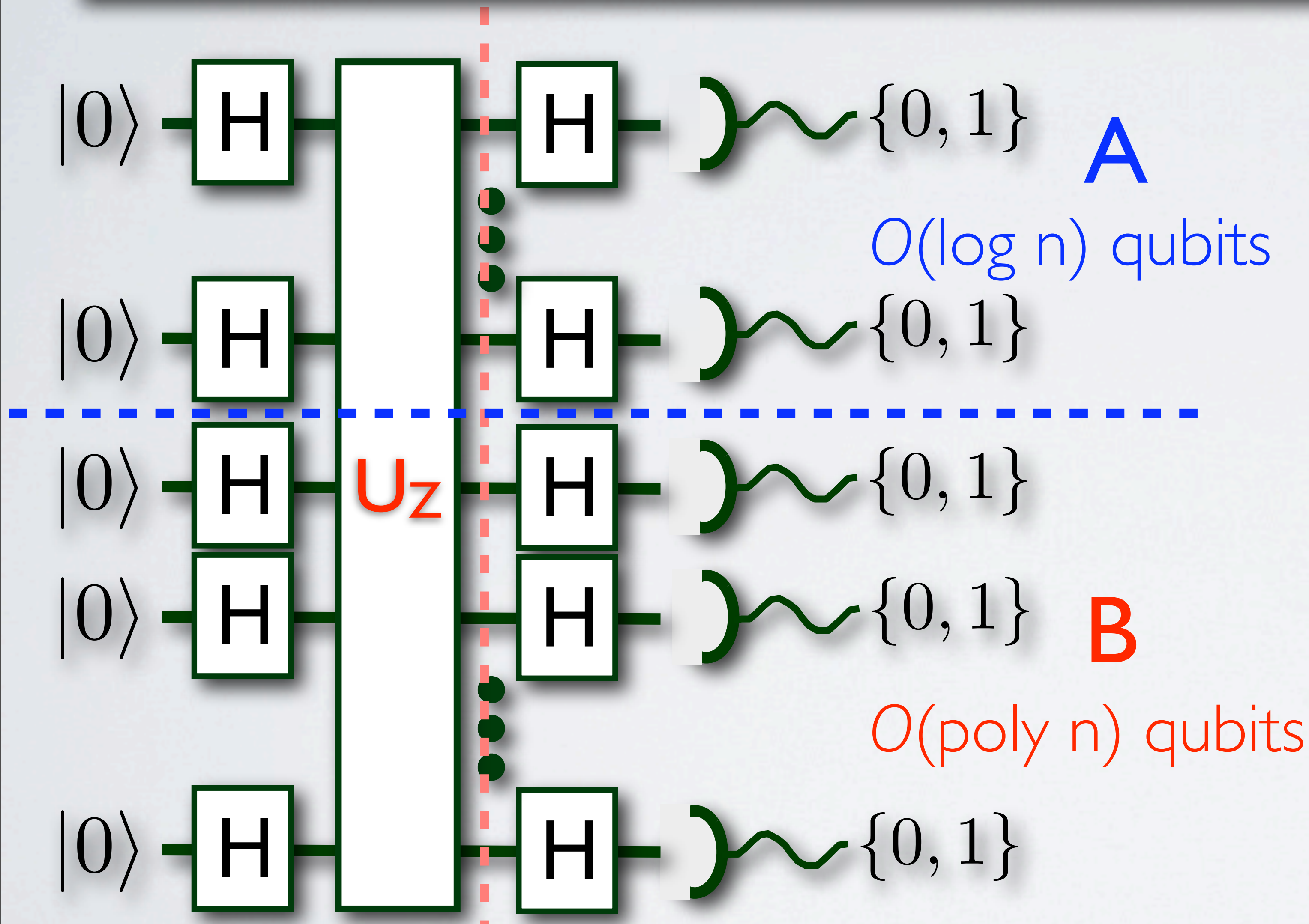
WHY IQP? (CSISH)

IQP is easy theorem: If the output of uniform (poly-time/size) IQP circuits is restricted to O(log n) may be sampled (without approximation) by a classical randomized process that runs in time O(poly n).



WHY IQP? (CSISH)

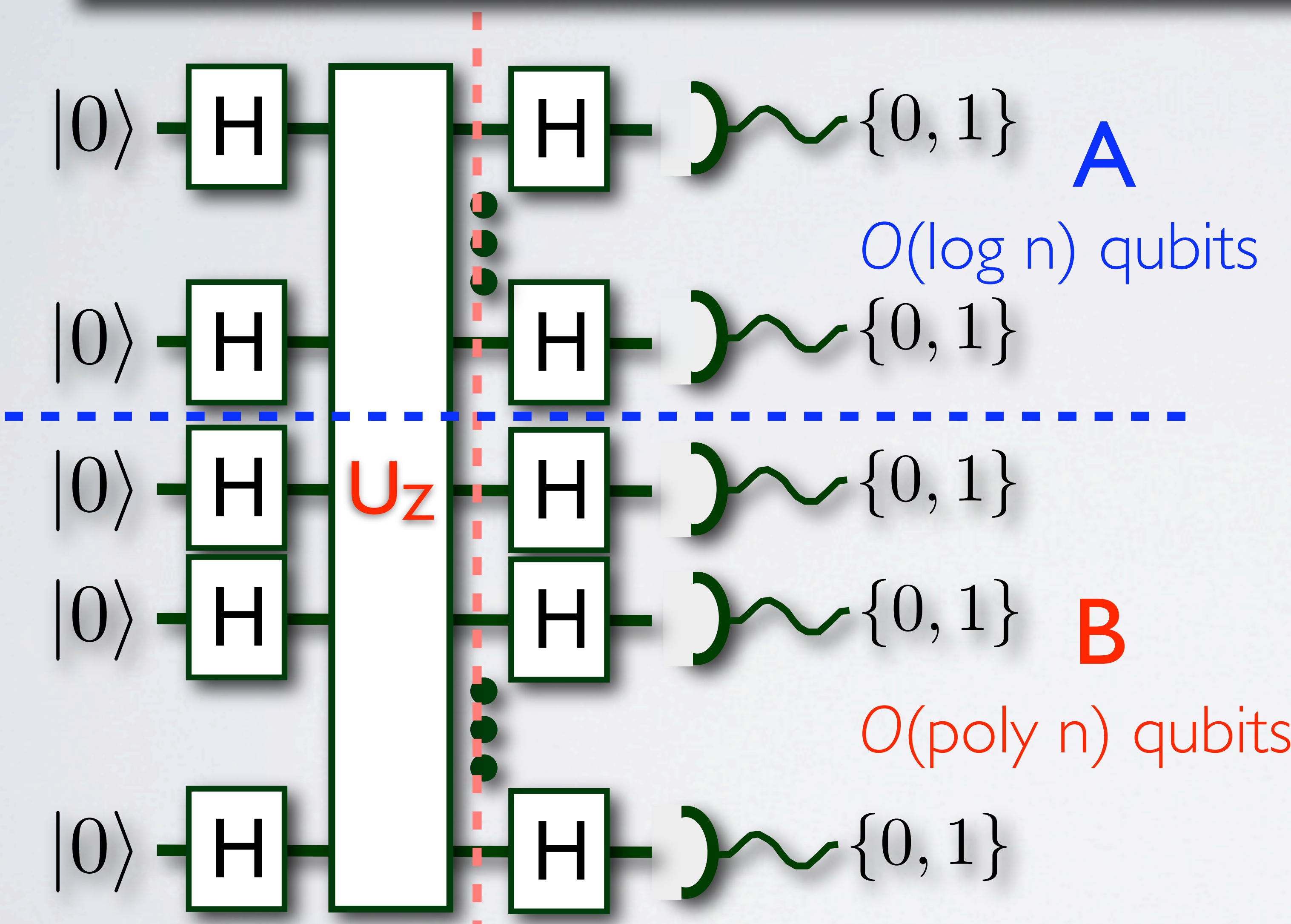
IQP is easy theorem: If the output of uniform (poly-time/size) IQP circuits is restricted to O(log n) may be sampled (without approximation) by a classical randomized process that runs in time O(poly n).



$$|\phi\rangle = \frac{1}{\sqrt{2^{M+N}}} \sum_{x,y} e^{if(x,y)} |x, y\rangle$$

WHY IQP? (CSISH)

IQP is easy theorem: If the output of uniform (poly-time/size) IQP circuits is restricted to O(log n) may be sampled (without approximation) by a classical randomized process that runs in time O(poly n).



$$|\phi\rangle = \frac{1}{\sqrt{2^{M+N}}} \sum_{x,y} e^{if(x,y)} |x, y\rangle$$

Algorithm:

1. Choose random bit string y_0.
2. Calculate:

$$|\phi_{y_0}\rangle = \frac{1}{\sqrt{2^M}} \sum_x e^{if(x,y_0)} |x\rangle$$

3. Strongly simulate remaining operations on A - possible as now only O(log n) qubits.
4. Repeat.

WHY IQP? (CSISH+)

$$T_{\mathcal{M}}(x,y) = \sum_{X \subseteq E} (x-1)^{\rho_{\mathcal{M}}(E)-\rho_{\mathcal{M}}(X)}.(y-1)^{|X|-\rho_{\mathcal{M}}(X)}$$

WHY IQP? (CSISH+)

$$T_{\mathcal{M}}(x,y) = \sum_{X \subseteq E} (x-1)^{\rho_{\mathcal{M}}(E)-\rho_{\mathcal{M}}(X)}.(y-1)^{|X|-\rho_{\mathcal{M}}(X)}$$

- Exact evaluation of Tutte polynomials is #P-hard.
  [Jaeger, Vertigan, Welsh 90]

WHY IQP? (CSISH+)

$$T_{\mathcal{M}}(x,y) = \sum_{X \subseteq E} (x-1)^{\rho_{\mathcal{M}}(E)-\rho_{\mathcal{M}}(X)}.(y-1)^{|X|-\rho_{\mathcal{M}}(X)}$$

- Exact evaluation of Tutte polynomials is #P-hard.
  [Jaeger, Vertigan, Welsh 90]
- If (x-1)(y-1)=q=2 an FPRAS exists for y>1. [Jerrum and Sinclair 93]

WHY IQP? (CSISH+)

$$T_{\mathcal{M}}(x,y) = \sum_{X \subseteq E} (x-1)^{\rho_{\mathcal{M}}(E)-\rho_{\mathcal{M}}(X)}.(y-1)^{|X|-\rho_{\mathcal{M}}(X)}$$

- Exact evaluation of Tutte polynomials is #P-hard.
  [Jaeger, Vertigan, Welsh 90]
- If (x-1)(y-1)=q=2 an FPRAS exists for y>1. [Jerrum and Sinclair 93]
- Additive approximations to Jones polynomials are BQP-complete.
  [Freedman, Larsen, Wang 01 and Aharanov, Jones, Landau 05]

WHY IQP? (CSISH+)

$$T_{\mathcal{M}}(x,y) = \sum_{X \subseteq E} (x-1)^{\rho_{\mathcal{M}}(E)-\rho_{\mathcal{M}}(X)}.(y-1)^{|X|-\rho_{\mathcal{M}}(X)}$$

- Exact evaluation of Tutte polynomials is #P-hard.
  [Jaeger, Vertigan, Welsh 90]
- If (x-1)(y-1)=q=2 an FPRAS exists for y>1. [Jerrum and Sinclair 93]
- Additive approximations to Jones polynomials are BQP-complete.
  [Freedman, Larsen, Wang 01 and Aharanov, Jones, Landau 05]
- Additive approximations of the Potts model is BQP-hard.
  [Aharanov et al 07]

WHY IQP? (CSISH+)

$$T_{\mathcal{M}}(x,y) = \sum_{X \subseteq E} (x-1)^{\rho_{\mathcal{M}}(E)-\rho_{\mathcal{M}}(X)}.(y-1)^{|X|-\rho_{\mathcal{M}}(X)}$$

- Exact evaluation of Tutte polynomials is #P-hard.
  [Jaeger, Vertigan, Welsh 90]
- If (x-1)(y-1)=q=2 an FPRAS exists for y>1. [Jerrum and Sinclair 93]
- Additive approximations to Jones polynomials are BQP-complete.
  [Freedman, Larsen, Wang 01 and Aharanov, Jones, Landau 05]
- Additive approximations of the Potts model is BQP-hard.
  [Aharanov et al 07]
- Multiplicative approximations to the 2-state Potts model is #P-hard for q ≥ 4 and x,y<0 (except x,y=-1).
  [Kuperberg 10]

WHY IQP? (CSISH+)

$$T_{\mathcal{M}}(x,y) = \sum_{X \subseteq E} (x-1)^{\rho_{\mathcal{M}}(E)-\rho_{\mathcal{M}}(X)}.(y-1)^{|X|-\rho_{\mathcal{M}}(X)}$$

- Exact evaluation of Tutte polynomials is #P-hard. [Jaeger, Vertigan, Welsh 90]
- If (x-1)(y-1)=q=2 an FPRAS exists for y>1. [Jerrum and Sinclair 93]
- Additive approximations to Jones polynomials are BQP-complete. [Freedman, Larsen, Wang 01 and Aharanov, Jones, Landau 05]
- Additive approximations of the Potts model is BQP-hard. [Aharanov et al 07]
- Multiplicative approximations to the 2-state Potts model is #P-hard for q ≥ 4 and x,y<0 (except x,y=-1). [Kuperberg 10]
- Beginnings of a complete characterization of the rational Tutte plane. [Goldberg, Jerrum since 08]

WHY IQP? (CSISH+)

$$T_{\mathcal{M}}(x,y) = \sum_{X \subseteq E} (x-1)^{\rho_{\mathcal{M}}(E)-\rho_{\mathcal{M}}(X)}.(y-1)^{|X|-\rho_{\mathcal{M}}(X)}$$

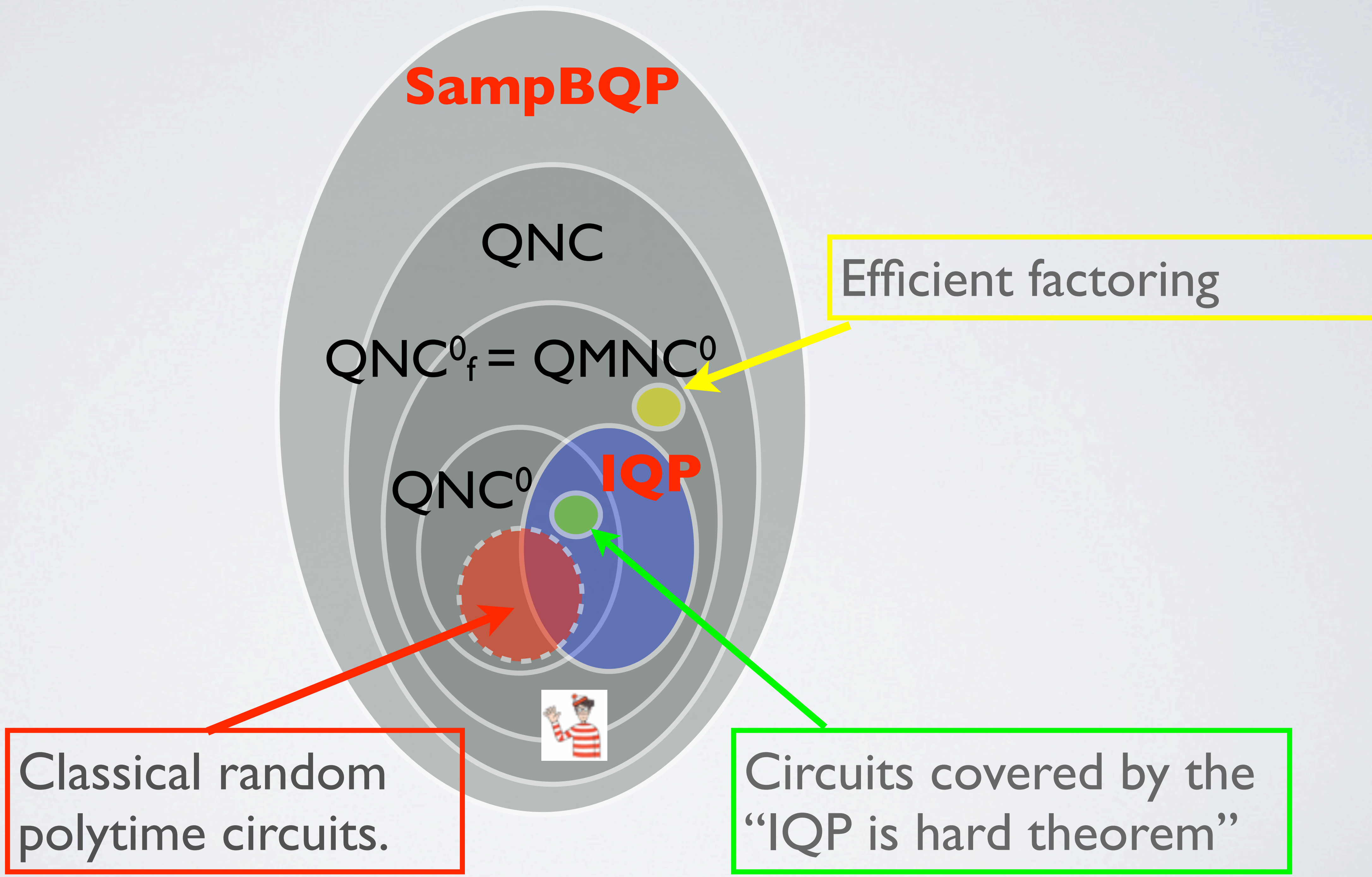
Strong simulation of constant-weight IQP distributions is equivalent to evaluating the 2-state Potts model at x=-i tan(ϴ), y=e^{iϴ}. [Shepherd 10]

- Exact evaluation of Tutte polynomials is #P-hard. [Jaeger, Vertigan, Welsh 90]
- If (x-1)(y-1)=q=2 an FPRAS exists for y>1. [Jerrum and Sinclair 93]
- Additive approximations to Jones polynomials are BQP-complete. [Freedman, Larsen, Wang 01 and Aharanov, Jones, Landau 05]
- Additive approximations of the Potts model is BQP-hard. [Aharanov et al 07]
- Multiplicative approximations to the 2-state Potts model is #P-hard for q ≥ 4 and x,y<0 (except x,y=-1). [Kuperberg 10]
- Beginnings of a complete characterization of the rational Tutte plane. [Goldberg, Jerrum since 08]

WHAT IS LEFT TO DO?

- Additive version of the IQP is hard theorem!
- Can the relationship between binary matroids and non-universal gate sets be used to enlarge the set of Tutte polynomials that do not have an FPRAS?
- Can any form of error protection be performed in IQP?
- Can we use the these results to design experiments that aren't classically simulable?
- Is BPP^{IQP} more powerful than BPP? Can it do anything interesting?
- Can we find anything simpler than IQP that probably can't be classically simulated?
- Look at Aaronson and Arkhipov's list of open problems in arXiv:011.3245 and try to answer them!!!

WHERE IS IQP?


SampBQP
QNC
$QNC^0_f = QMNC^0$
QNC^0
IQP
Efficient factoring
Classical random polytime circuits.
Circuits covered by the "IQP is hard theorem"