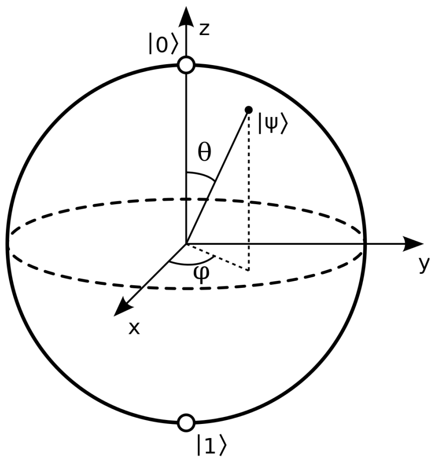


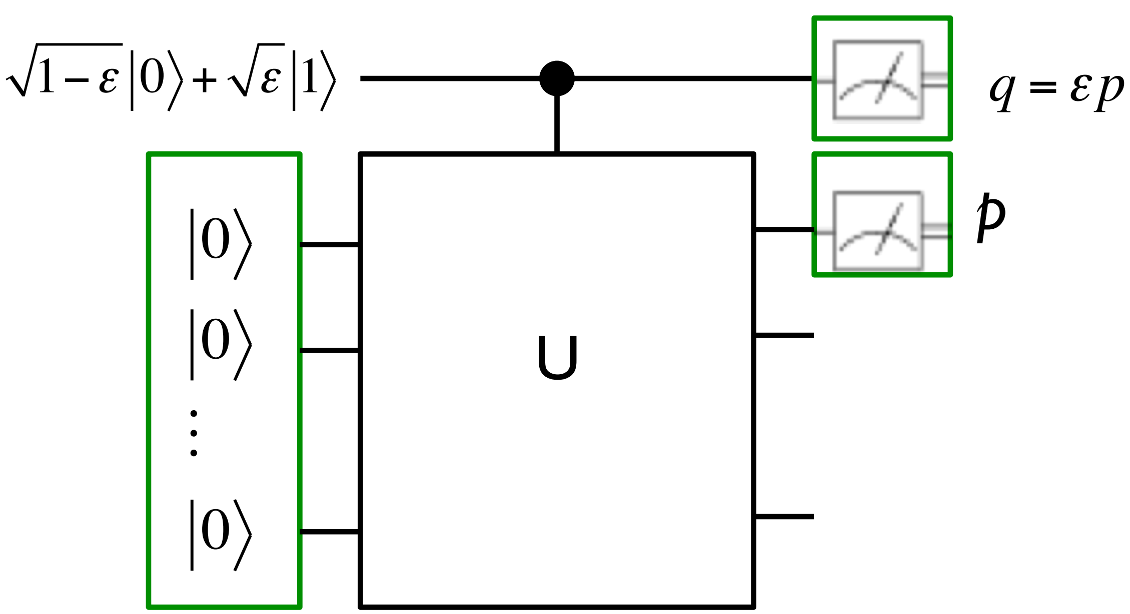
Introduction to quantum computation and simulability

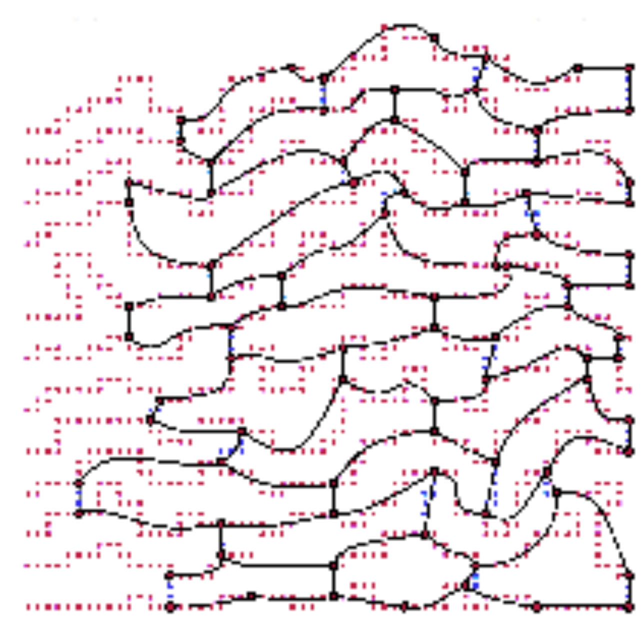
Daniel J. Brod (UFF)

Leandro Aolita (UFRJ/ICTP-SAIFR)

<u>Ernesto F. Galvão (UFF)</u>

Instituto de Física
Universidade Federal Fluminense





(f) deletion and contraction (Q.1 & Q.2)

ICTP-SAIFR – IFT/UNESP , October 15th-19th, 2018

Lecture 10 : Intermediate models of quantum computation

Outline:

- Intro: Intermediate models of quantum computation
- Postselected circuits and hardness of simulation
- IQP circuits are hard to simulate
- The one-clean-qubit (DQC-1) model and variations
- Entanglement as a resource in the circuit model
- Connections between different restricted QC models

- For slides and links to related material, see

Two notions of classical simulation

Given a quantum process (e.g. a circuit), input states and choice of output qubits to be measured, we can talk about two different notions of simulability:

1. Strong classical simulation:
   - compute probabilities of output outcomes.
2. Weak classical simulation:
   - output sample of output outcomes.

← more reasonable than demanding strong simulation

Examples we've seen:

- computational basis input+measurement, Clifford circuit: strongly simulable
- separable input+measurement, Clifford circuit: not simulable at all (universal for QC)

Also important – how does the error scale? Assume n qubits, poly(n) repetitions

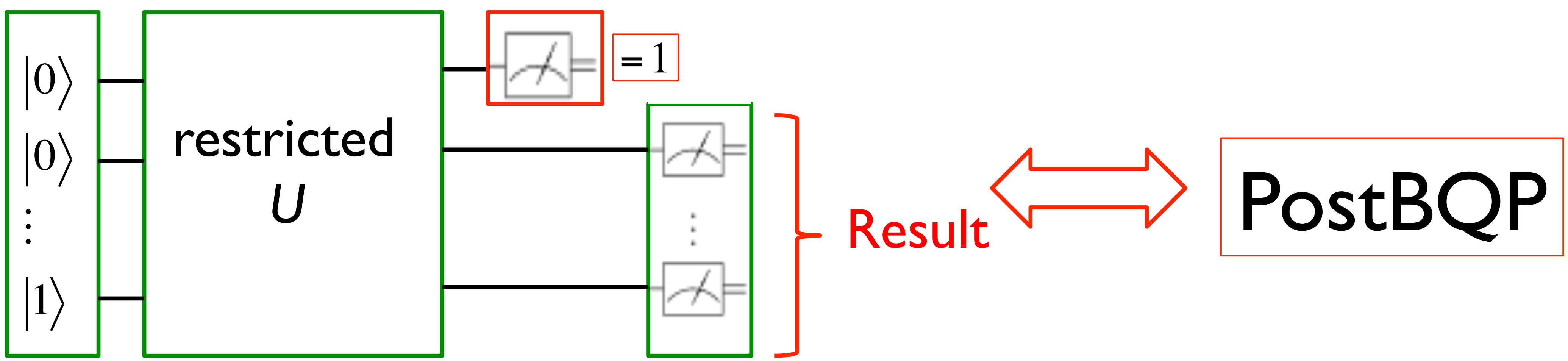
- Experimentally: estimates of probabilities with 1/poly(n) error
- Simulation: we'd like error to scale like the experimental one, i.e. 1/poly(n) error.

Post-selection and hardness of simulation

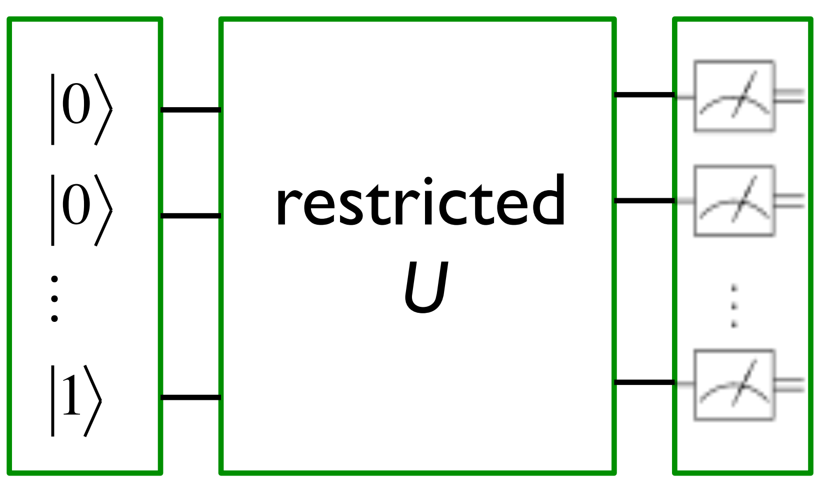
- Recalling Daniel's lecture:

If post-selected restricted model = PostBQP then restricted model can't be (weakly) simulated exactly, unless Polynomial Hierarchy collapses (considered highly unlikely)

If



then



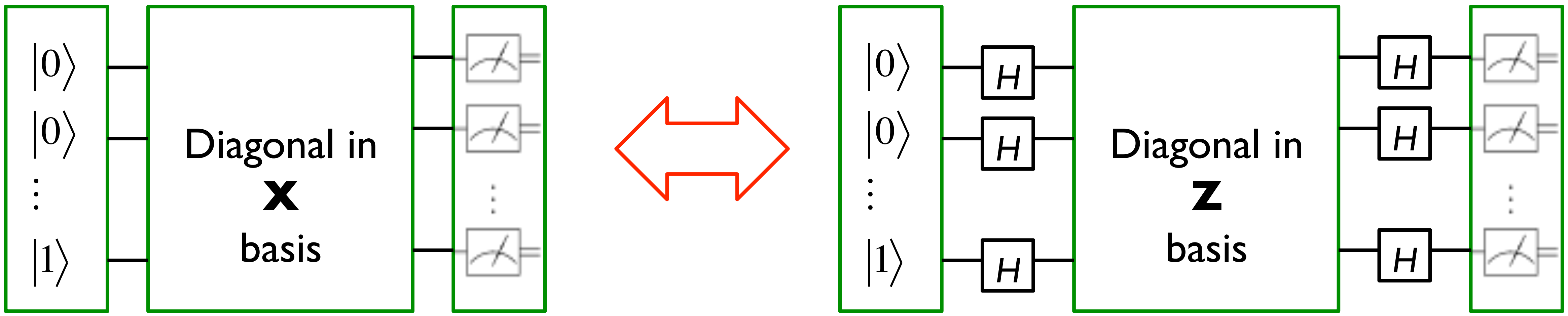
is hard to simulate exactly

Post-selection and hardness of simulation

If post-selected restricted model = PostBQP then restricted model can't be (weakly) simulated exactly, unless Polynomial Hierarchy collapses (considered highly unlikely)

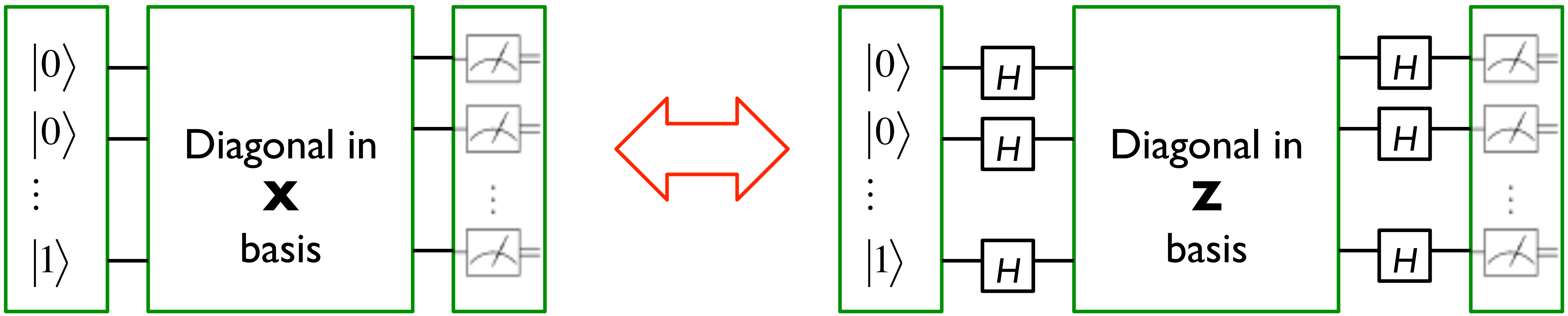
- Restricted models shown to be hard to simulate using this recipe:
  - Quantum circuits of depth 3 [Terhal, DiVincenzo, quant-ph/020513]
  - IQP (commuting quantum circuits)
  - version of DQC1
  - Boson Sampling

IQP: commuting gates



IQP: circuits with commuting gates

- The complexity class IQP was initially studied by Shepherd, Bremner, and Jozsa
- Initialization and measurement in computational basis, but only commuting gates (in X basis)
    - Temporal order of gates irrelevant; strong restriction on computational power



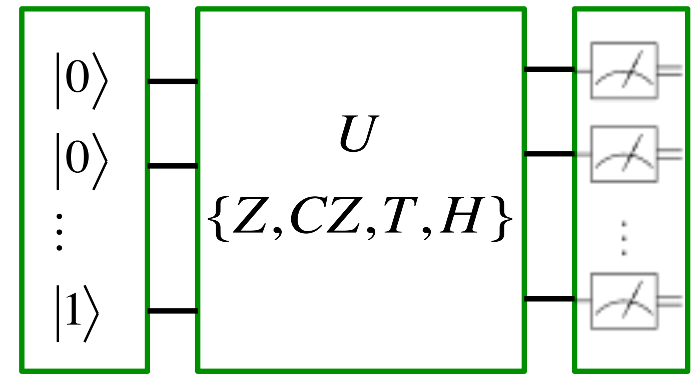
- Proving IQP circuits are hard to simulate…

[Shepherd, Bremner, Proc. R. Soc. London A 465, 1413 (2009)]
[Bremner, Jozsa, Shepherd, Proc. R. Soc. London A 467, 459 (2011)]

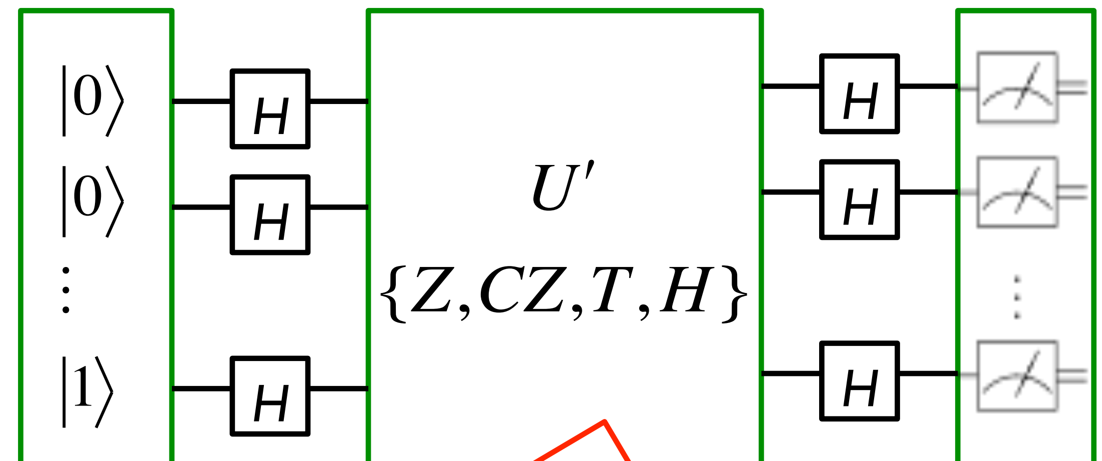
IQP is hard to simulate

- Take general circuit using universal gate-set

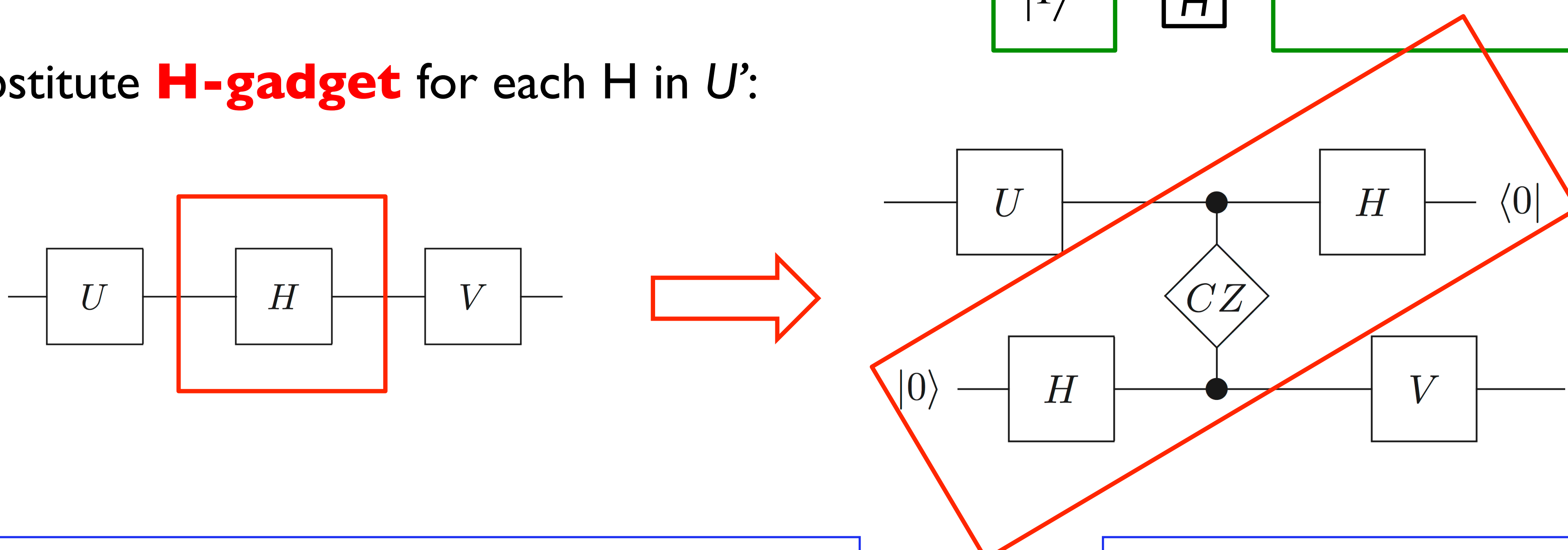
$$\{H, Z, CZ, T\}$$



- Add identities HH=I so that circuit is in the form:



- Substitute **H-gadget** for each H in *U'*:



Resulting circuit is in IQP format, and with post-selection does PostBQP

IQP must be hard to simulate classically

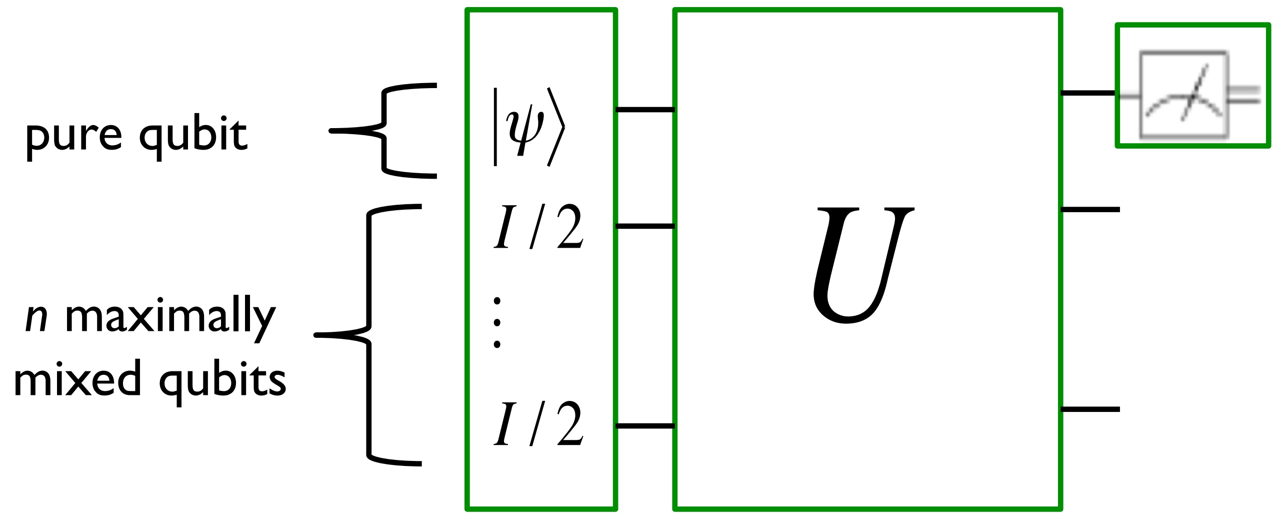
[Bremner, Jozsa, Shepherd, Proc. R. Soc. London A 467, 459 (2011)]

IQP is hard to simulate

- Even approximate weak simulation unlikely, due to connection of IQP circuits with two other problems which are considered hard:
  - Calculation of partition functions of random instances of the Ising model
  - Approximation of gap of degree-3 polynomials over F_2

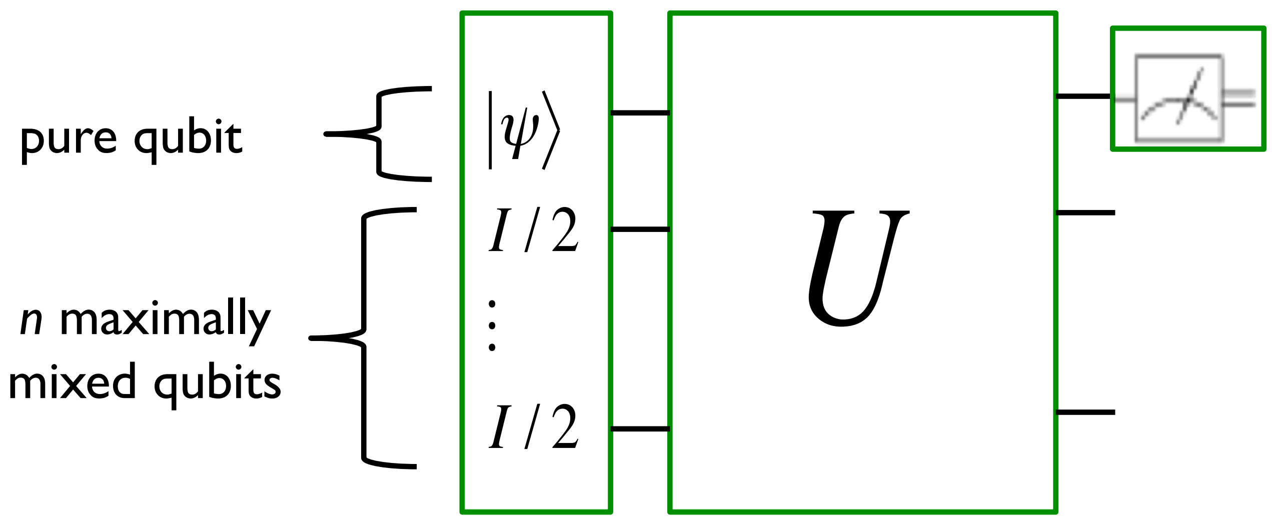
[Bremner, Montanaro, Shepherd, arXiv:1504.07999]

DQC1
AKA "one-clean-qubit" model



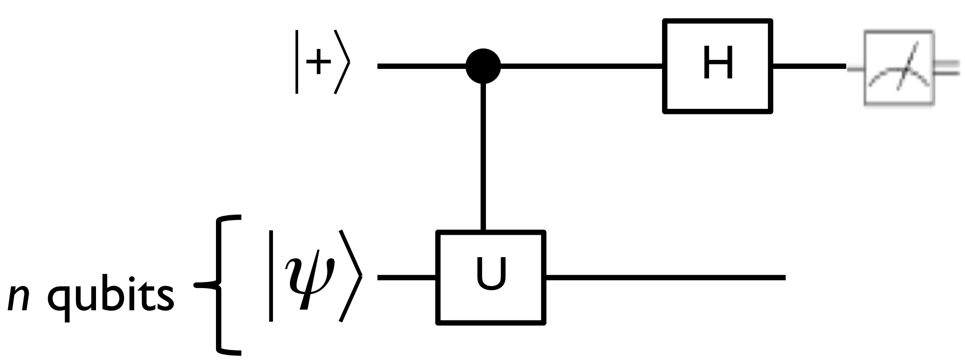
DQC1, or "one-clean-qubit" model

- Inspired by NMR QC, Knill and Laflamme proposed the "one-clean-qubit model", by changing the input of a general circuit: [Knill, Laflamme, PRL 81, 5672 (1998)]



- Problem is encoded in U's gate decomposition – measurements must reveal some property of U
- DQC1 = class of problems solvable in poly(n) time, with high probability

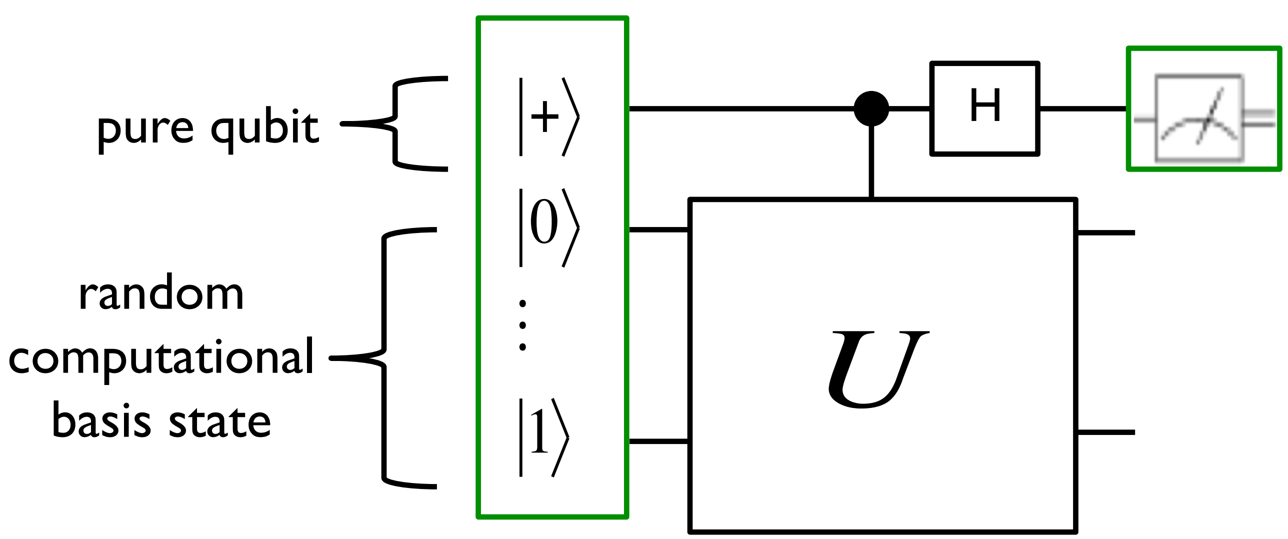
- DQC1 circuits are good for estimating traces of unitaries. This is done via the Hadamard test:



$$p_0 = \frac{1 + \mathrm{Re}\left(\langle\psi|U|\psi\rangle\right)}{2}$$

- $O(1/\varepsilon^2)$ measurements estimate $\mathrm{Re}\left(\langle\psi|U|\psi\rangle\right)$
- similar scheme estimates $\mathrm{Im}\left(\langle\psi|U|\psi\rangle\right)$

DQC1, or "one-clean-qubit" model

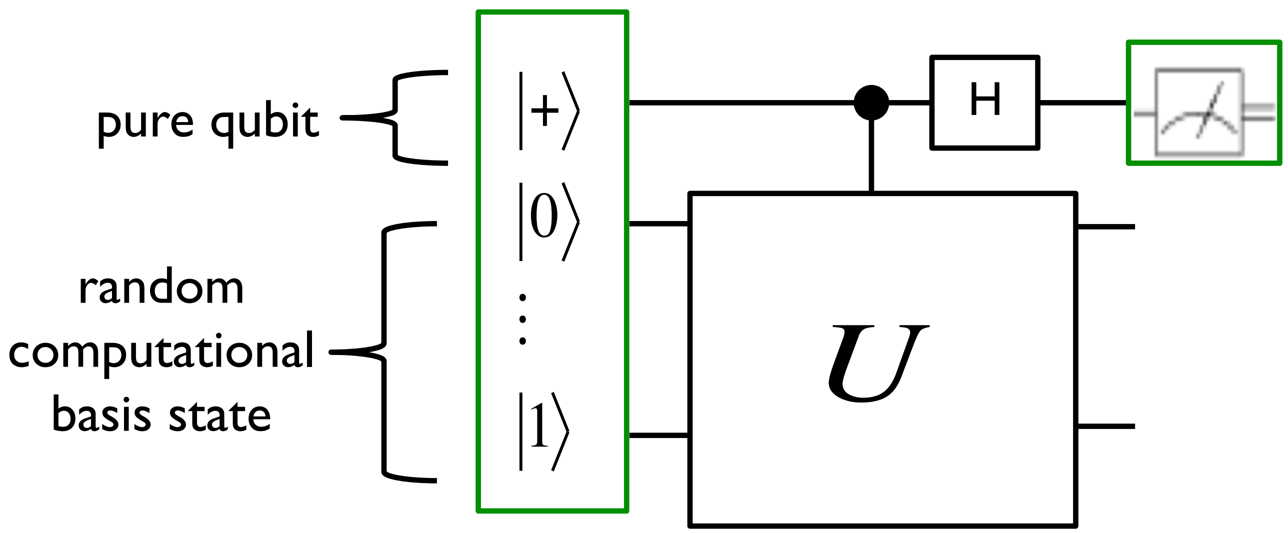


$$p_0 = \frac{1}{2^n}\sum_x \frac{1+\mathrm{Re}\left(\langle x|U|x\rangle\right)}{2} = \frac{1}{2} + \frac{\mathrm{Re}(TrU)}{2^{n+1}}$$

- random input in computational basis state = picking input $\frac{I}{2^n}$

- U is exp(n)-size – hence difficulty in estimating trace on a classical computer
- A "collapse of PH" argument shows DQC1 can't be simulated exactly (under this plausible assumption) [Fujii et al., arxiv:1409.6777]
- What's DQC1 good for?
  - Knot theory: estimating Jones polynomials [Shor, Jordan, QIC 8, 681 (2008)]
  - Testing for integrability of U [Poulin *et al.*, PRA 68, 22302 (2003)]
  - Average fidelity decay [Poulin *et al.*, PRL 92, 177906 (2004)]

DQC1, or “one-clean-qubit” model

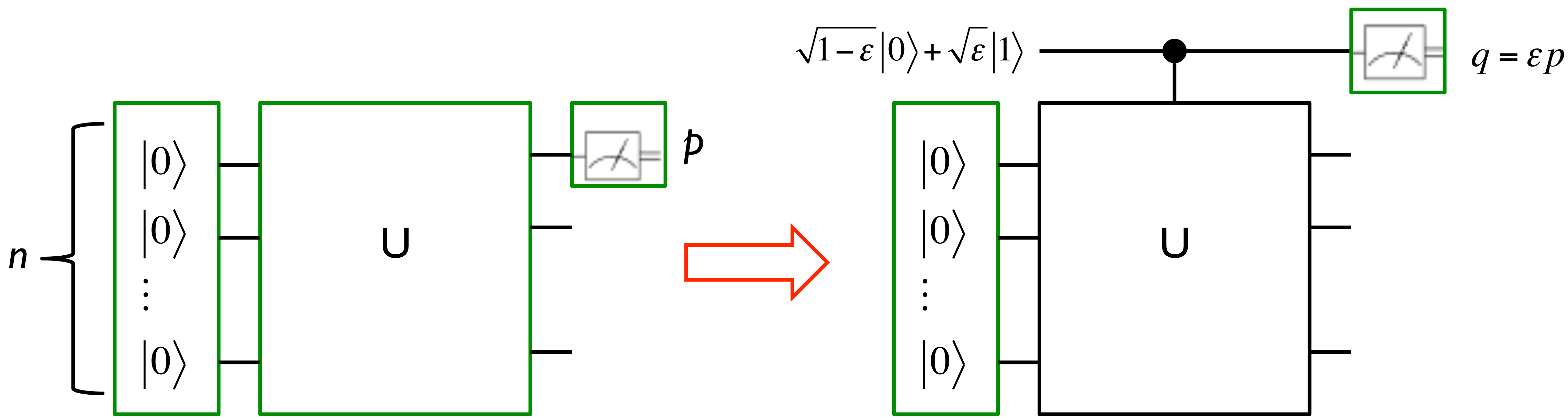


- Where does the quantum advantage come from?
    - Partitions reveal small amount of entanglement (doesn’t increase with *n*)
    - Little entanglement but large Schmidt rank – simulation not possible with MPS scheme
    - Role of quantum discord in model?

How much entanglement is necessary?

- Some entanglement is necessary in pure-state quantum computation
  [Jozsa, Linden, Proc. R. Soc. London A 459,(2036), 2011 (2003)]

- But how much? Very small entropy of entanglement across all bipartitions is sufficient:
  [Van den Nest, PRL 110, 060504 (2013)]



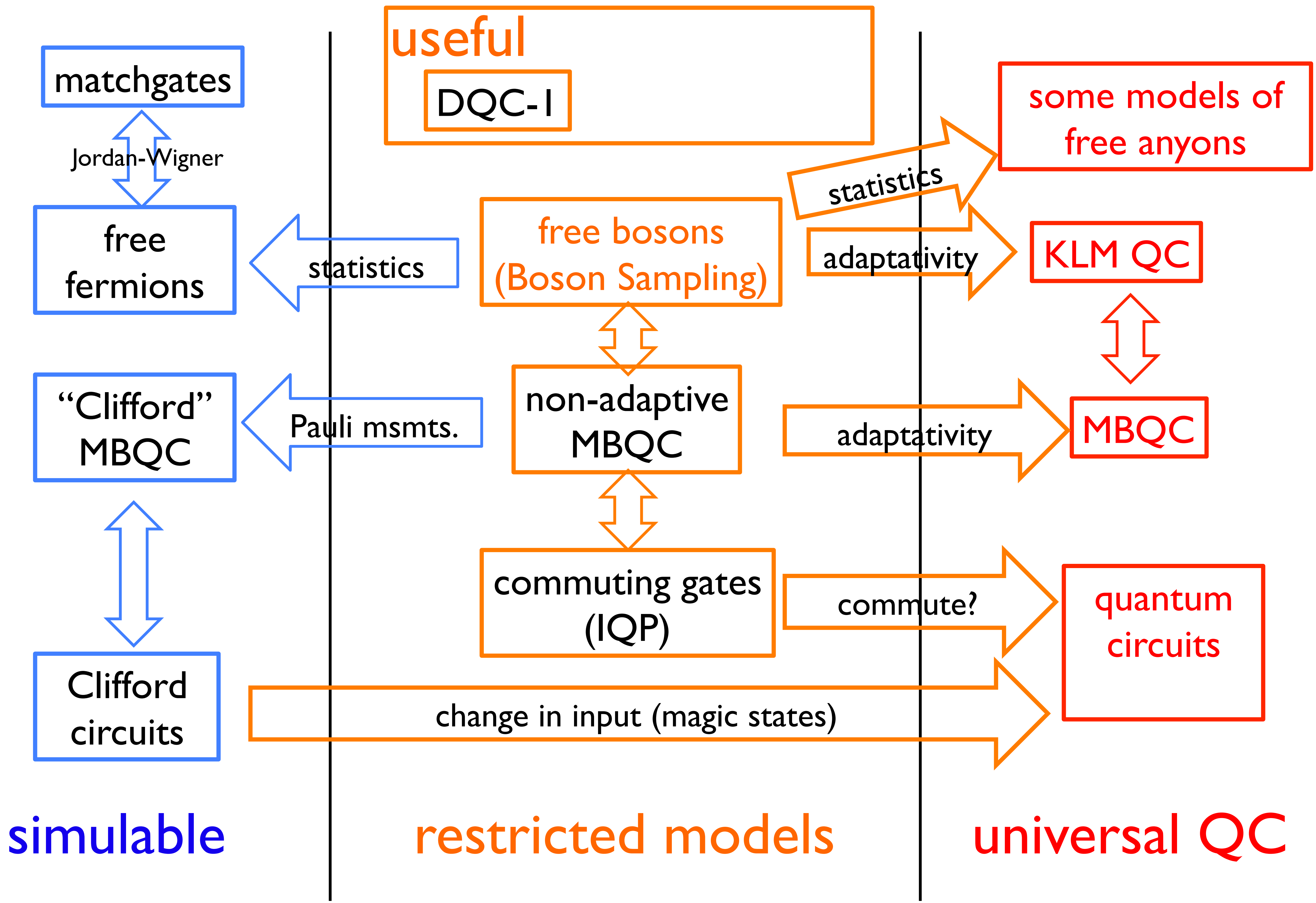
- After t gates of (controlled) U: $|\psi_t\rangle = \sqrt{1-\varepsilon}\,|0\rangle^n \otimes |0\rangle + \sqrt{\varepsilon}\left(U_t|0\rangle^n\right)\otimes|1\rangle$
- State always close to $|0\rangle^n \otimes |0\rangle$, but q (and p) can be estimated with poly(n) runs
- By continuity of entropy of entanglement, 1/poly(n) amount of entanglement at each run
- Large "integrated" entanglement over all runs, however, seems to be necessary

So what is necessary/sufficient for quantum speed-up?

- Entanglement:
    - not sufficient (e.g. Clifford circuits)
    - some is necessary (Jozsa, Linden)
    - but not much is necessary (DQC1, Van den Nest's scheme for general BQP)
    - depends on which measure (entropy of entanglement versus Schmidt rank)

- Dynamics / input states / measurements
    - a combination of dynamics, input states and measurements defines the computational capacity of model.
    - some resource trade-offs possible (e.g. Clifford + magic states)

Restricted models for QC: connections



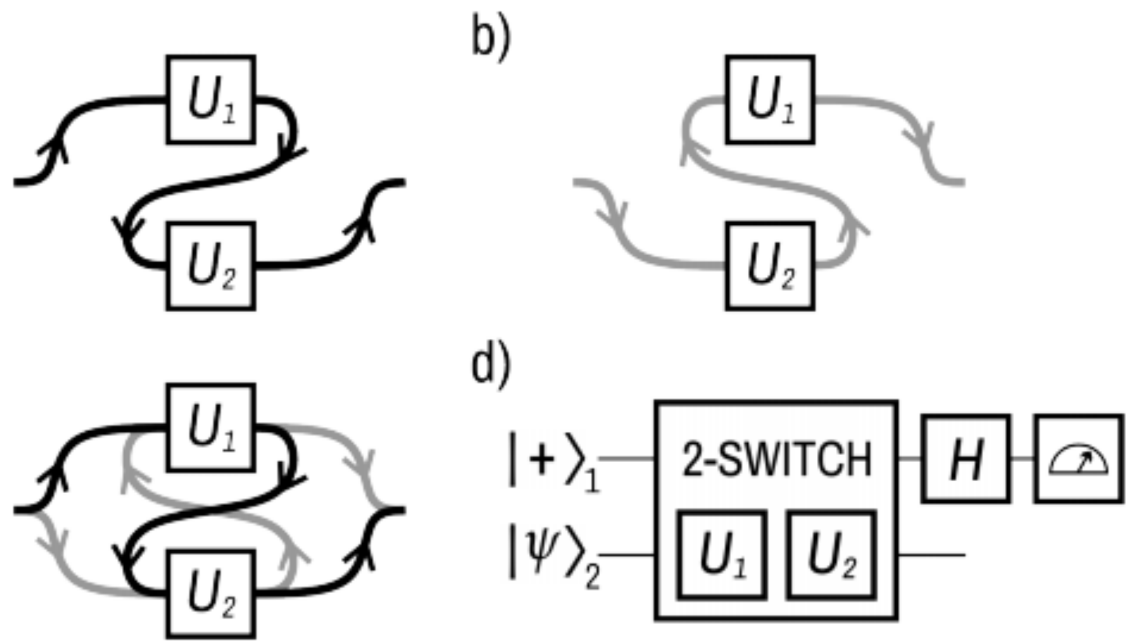
Time ordering in quantum computation:

- superposition of causal orders

- simulated closed time-like curves

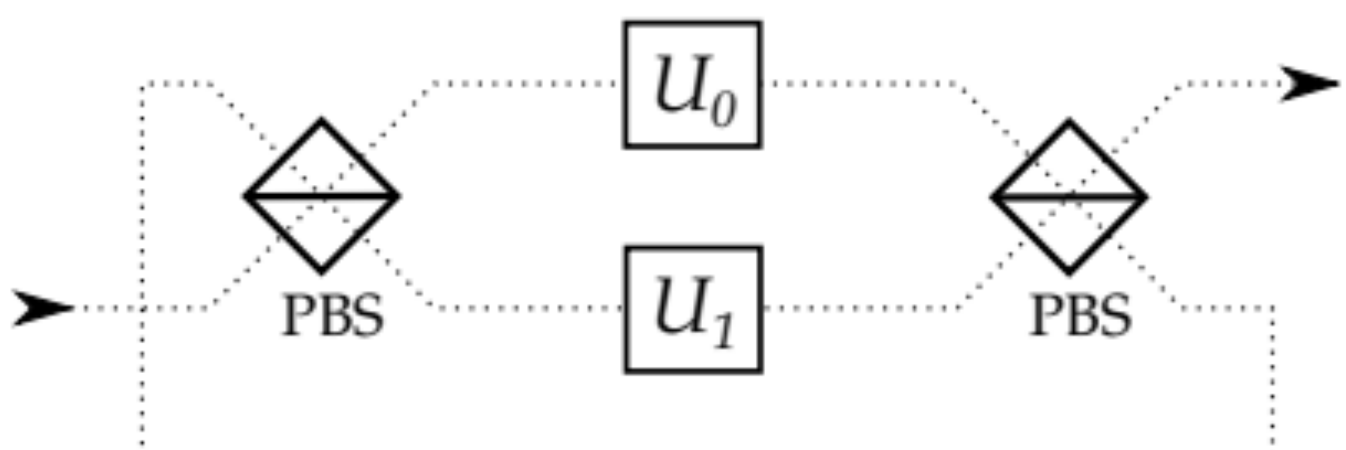
Computational resource: superposition of causal orders

- It’s possible to imagine superposing different orders of operations:



Procopio et al., arXiv:1412.4006

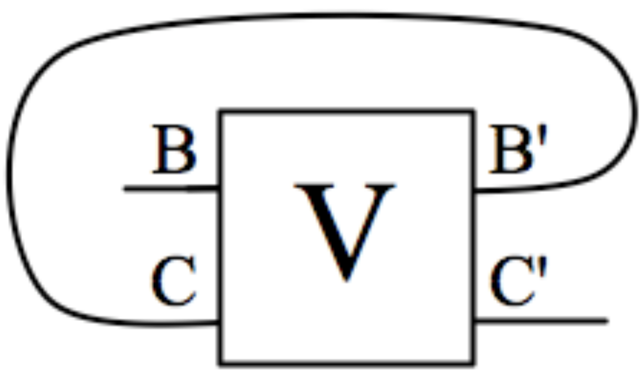
- This can be achieved using an interferometer (but not a circuit):



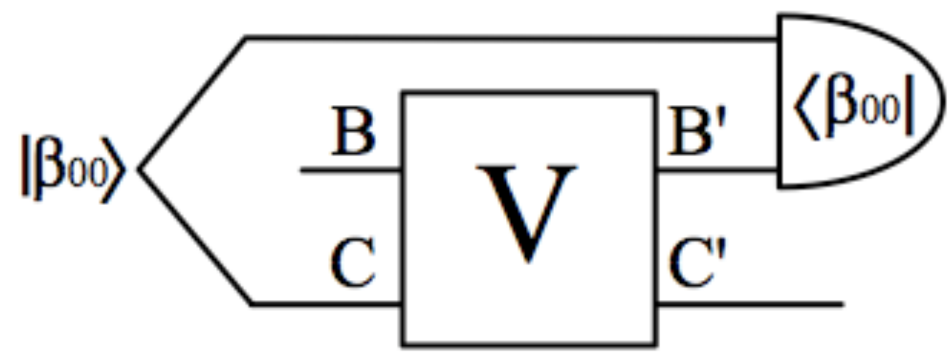
- Based on theoretical work by Chiribella (2012).

PCTCs: a model based on teleportation and post-selection

- Bennett and Schumacher, unpublished (2002) – see seminar http://bit.ly/crs8Lb
- Rediscovered independently by Svetlichny (2009) - arXiv:0902.4898v1
  - Related work on black holes by Horowitz/Maldacena (2004), Preskill/Gottesman (2004)



CTC



$$|\beta_{00}\rangle \equiv \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Simulation using teleportation and post-selection: B’=C

- We post-select projections onto $|\beta_{00}\rangle$
  - Postselection successful: state B’ is teleported back in time (state C = state B’)
  - Simulation works only when post-selection happens -> finite probability of success.