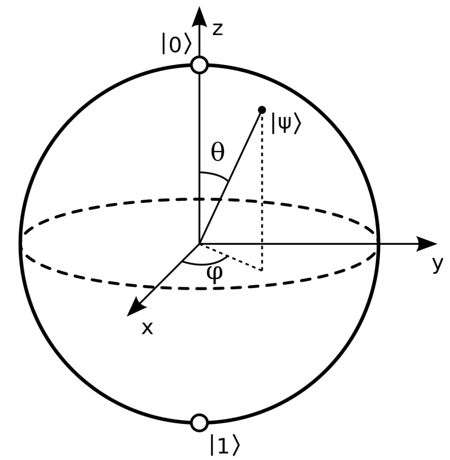


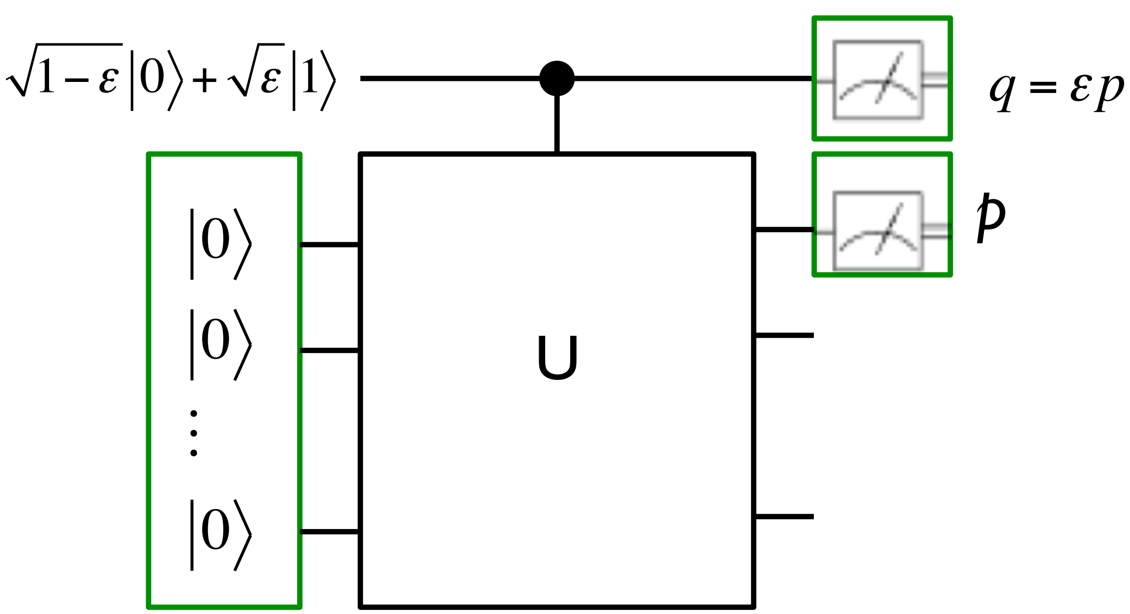
Introduction to quantum computation and simulability

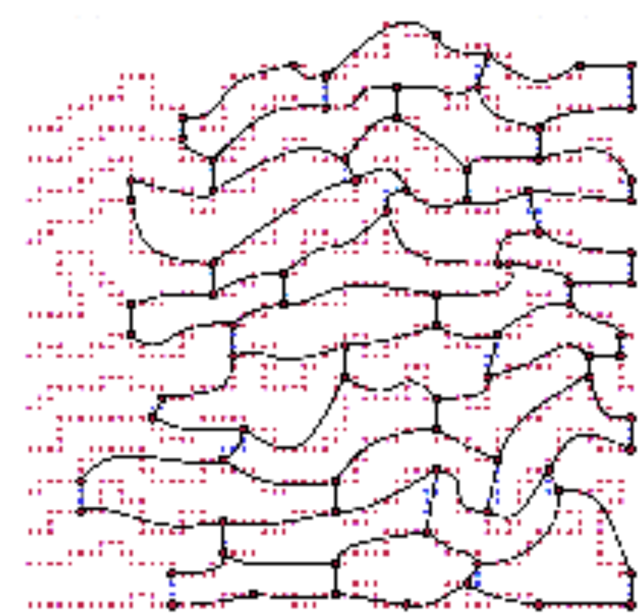
Ernesto F. Galvão

Instituto de Física, Universidade Federal Fluminense

(Niterói, Brazil)

INSTITUTO DE FÍSICA
Universidade Federal Fluminense





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

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

Lecture 8 : Measurement-based QC (MBQC) II

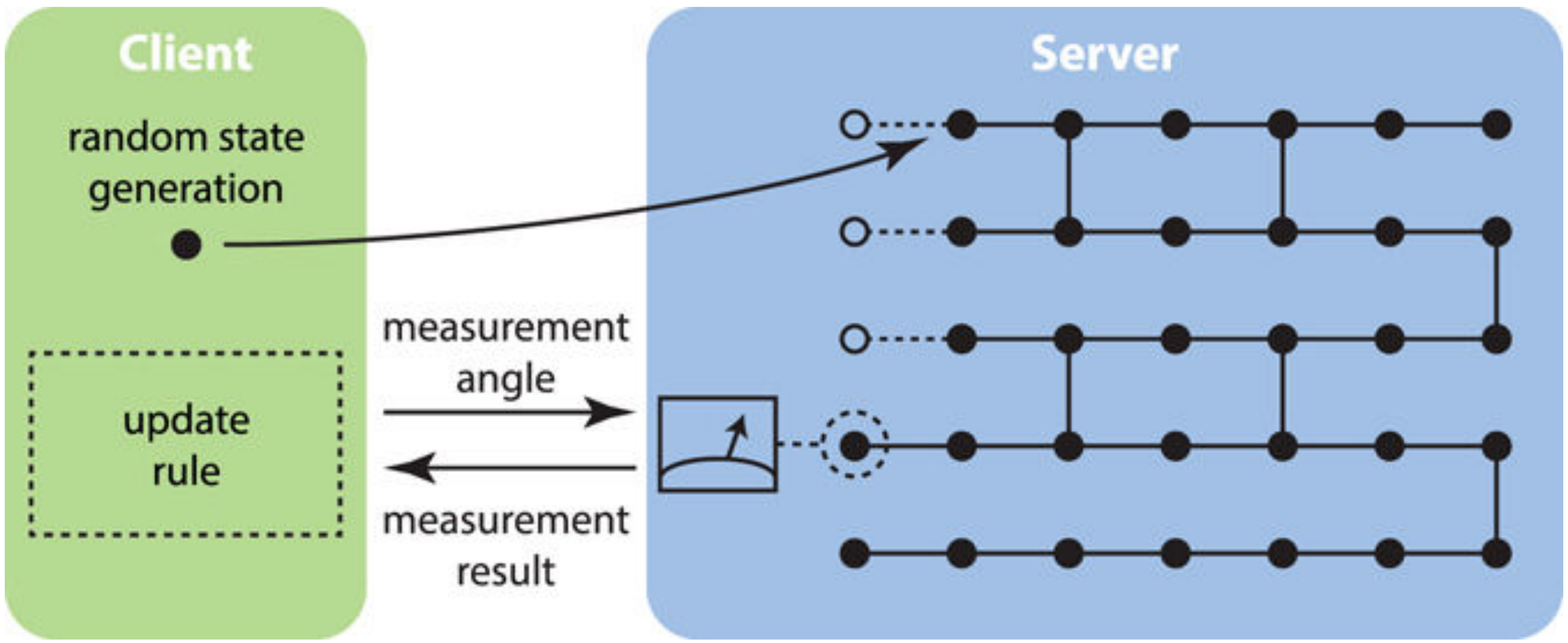
Outline:

- Applications of MBQC:
  - models for quantum spacetime
  - blind quantum computation
- Time-ordering in MBQC
- MBQC without adaptativity:
  - Clifford circuits
  - IQP circuits
- Introduction to quantum contextuality
- Contextuality as a computational resource
  - in magic state distillation
  - in MBQC

- For slides and links to related material, see

Application: blind quantum computation

- Classical/quantum separation in MBQC allow for implementation of novel protocols – such as blind quantum computation
- Here, client has limited quantum capabilities, and uses a server to do computation for her.
- Blind = server doesn't know what's being computed.



Broadbent, Fitzsimons, Kashefi, axiv:0807.4154 [quant-ph]

Application: model for quantum spacetime

- MBQC can serve as a discrete toy model for quantum spacetime:

quantum space-time	**MBQC**
quantum substrate	graph states
events	measurements
principle establishing global space-time structure	determinism requirement for computations

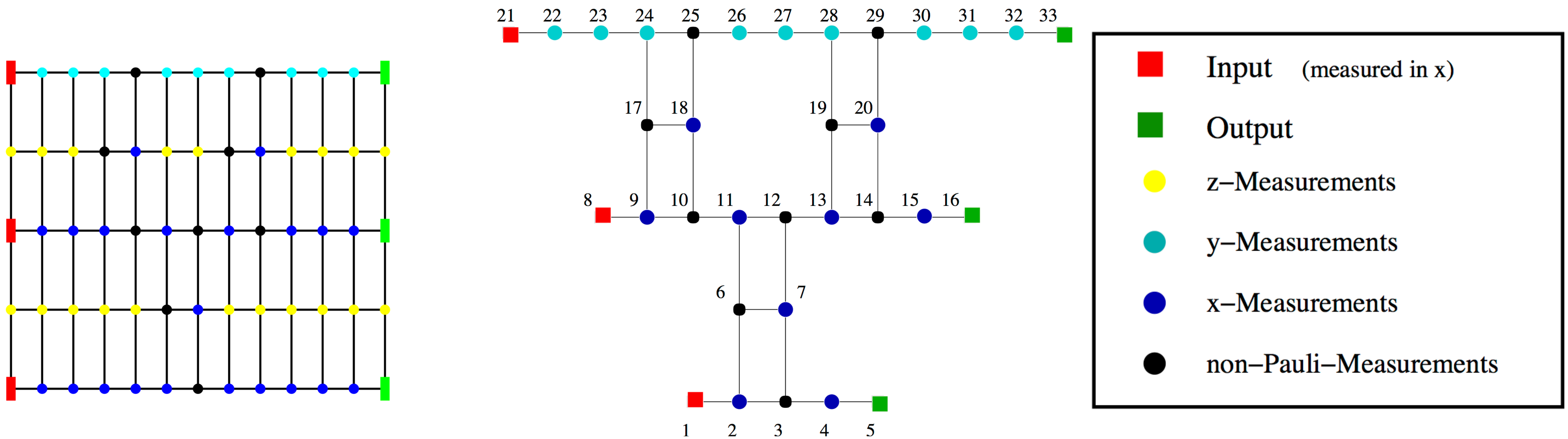
[Raussendorf *et al.*, arxiv:1108.5774]

- Even closed timelike curves (= time travel) have analogues in MBQC!

[Dias da Silva, Kashefi, Galvão PRA 83, 012316 (2011)]

Time-ordering in MBQC

M. HEIN, W. DÜR, J. EISERT, R. RAUSSENDORF, M. VAN DEN NEST and H.-J. BRIEGEL

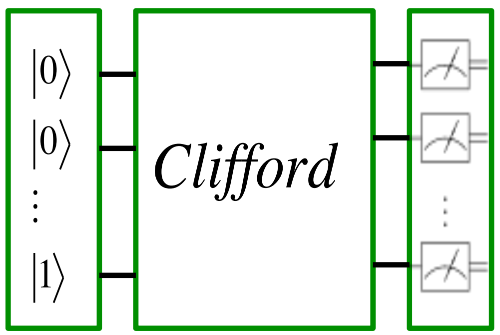


from: Proc. Int. School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos", Varenna, Italy (2005)

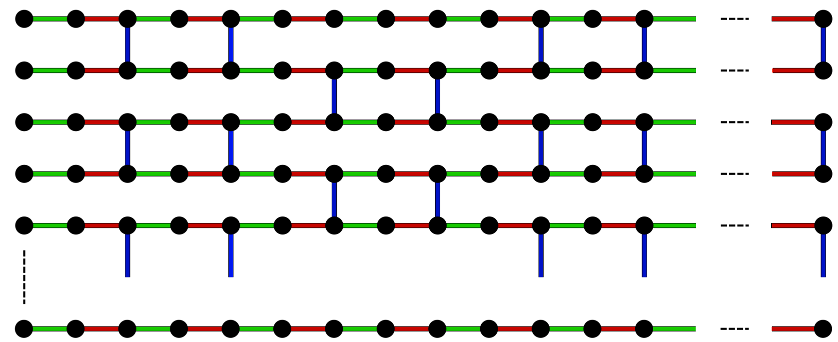
- Note that some measurements are **not adaptive**, but in fixed bases. These can be performed at once at beginning of computation
- Parts of protocol corresponding to Clifford gates are non-adaptive
- MBQC neatly separates Clifford (non-adaptive) from non-Clifford (adaptive) parts of the computation
- Back-and-forth translations between models reveal possible circuit optimizations

Circuit optimization: example

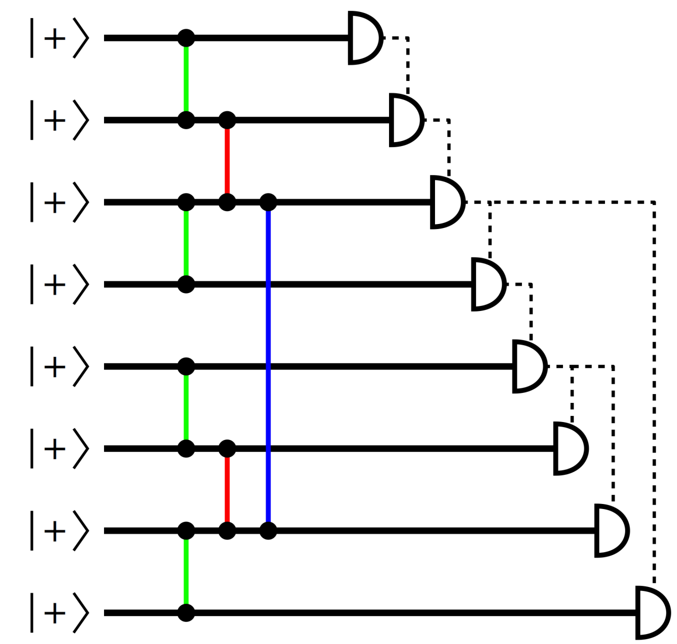
- We've seen that MBQC allows for implementation of Clifford operations in constant time. Back-translating to the circuit model we obtain circuits which implement all the Clifford part in constant time:



Clifford circuit



MBQC on universal graph state



Circuit translation of MBQC protocol

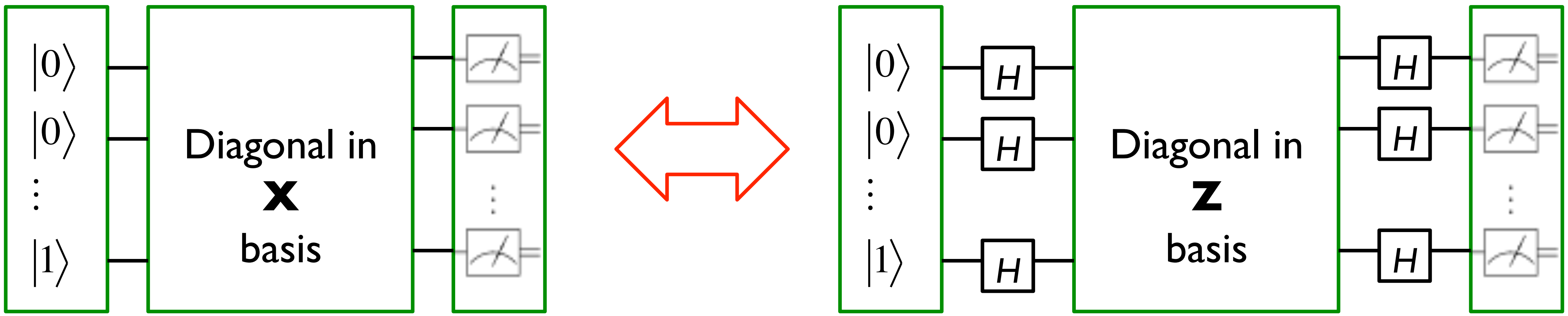
- No adaptativity in Clifford MBQC -> no adaptativity in circuit.
- Depth is 4 (3 CZs and 1 single-qubit unitary for measurement)

- **Trade-off**: depth becomes constant, at cost of increasing number of qubits

- For non-Clifford circuits, depth increases by the number of layers of non-Clifford 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

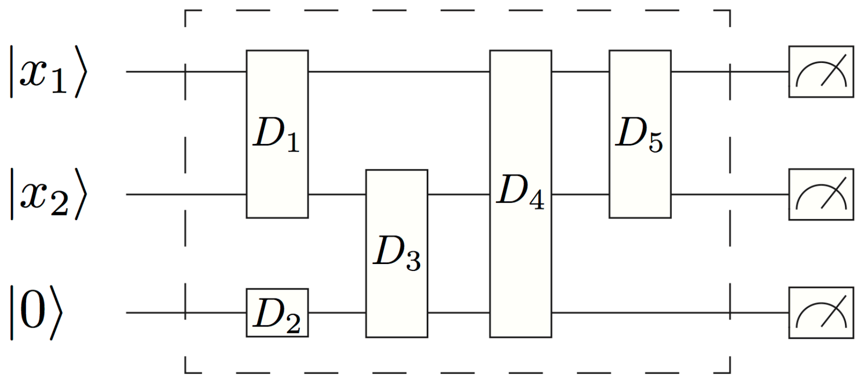


[Shepherd, Bremner, Proc. R. Soc. London A 465, 1413 (2009)]
[Bremner, Jozsa, Shepherd, Proc. R. Soc. London A 467, 459 (2011)]

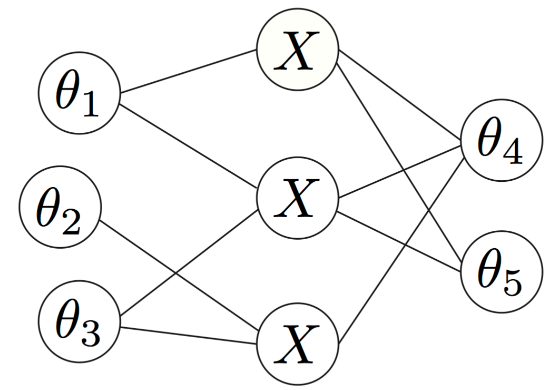
IQP circuits in MBQC

- IQP circuits can be implemented in the MBQC model – the translation is curious

[Browne, Briegel, quant-ph/0603226]



translation



Commuting gates in X basis

non-adaptive MBQC

- [Hoban *et al.* PRL 112, 140505 (2014)] define a suitable subclass IQP* of IQP circuits, and prove that:

IQP* hardness of simulation

translation

Hardness of simulating non-adaptive MBQC

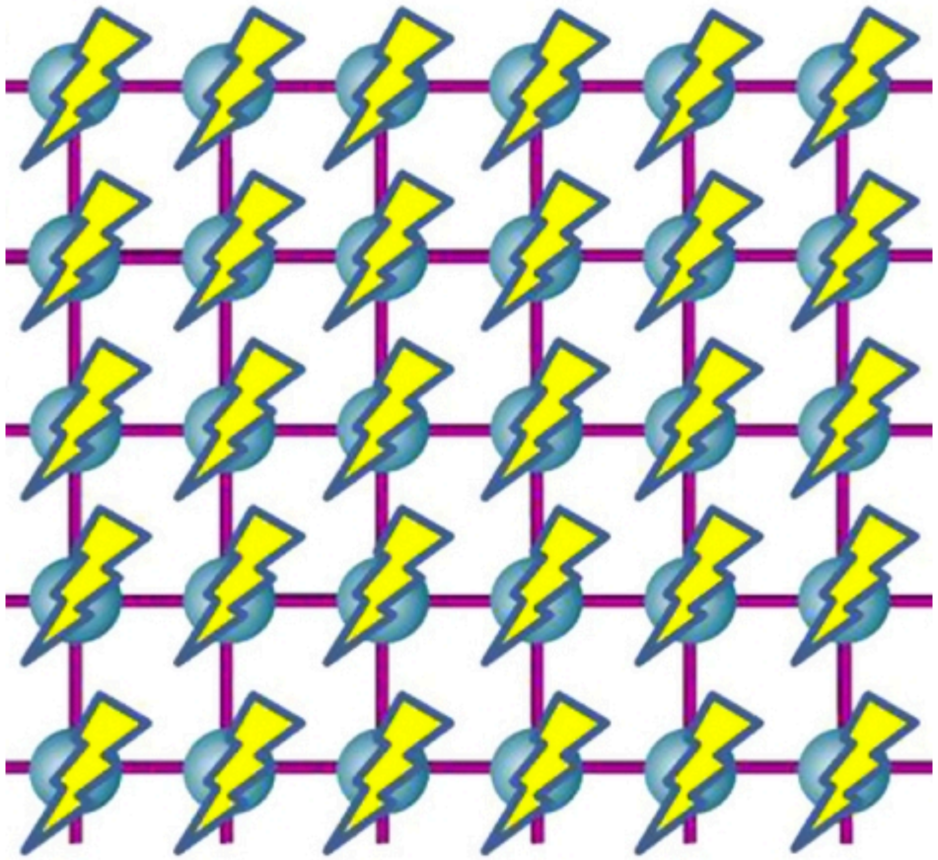
- Now: prior to measurement, decohere each qubit in its measurement eigenbasis. This doesn't change statistics, but results in states which are **separable** and **discord-free**.

this "Classical" MBQC is hard to simulate exactly

Where's the quantum ingredient there?

Which resource gives MBQC its power?

- Clearly, the correlations in the resource state.



- Analysis of MBQC protocols in terms of Bell inequalities:
  - Anders/Browne PRL 102, 050502 (2009)
  - Hoban et al., New J. Phys. 13, 023014 (2011)

- …but measurements are usually not space-like separated:

  ⇨ quantum contextuality

  - Raussendorf, PRA 88, 022322 (2013)

Quantum contextuality

- Context of an observable A = set of commuting observables measured together with A
- Non-contextuality hypothesis: outcomes of observables are context-independent
- Violated by quantum mechanics!

- Famously proved by Kochen and Specker (1967). Let's see a proof by Mermin (1990).

$\mathbb{1} \otimes \sigma_z$	$\sigma_z \otimes \mathbb{1}$	$\sigma_z \otimes \sigma_z$
$\sigma_x \otimes \mathbb{1}$	$\mathbb{1} \otimes \sigma_x$	$\sigma_x \otimes \sigma_x$
$\sigma_x \otimes \sigma_z$	$\sigma_z \otimes \sigma_x$	$\sigma_y \otimes \sigma_y$

- Operators in each row and column commute;

Moreover, they are the product of the other two in same row/column

- EXCEPTION: third column:

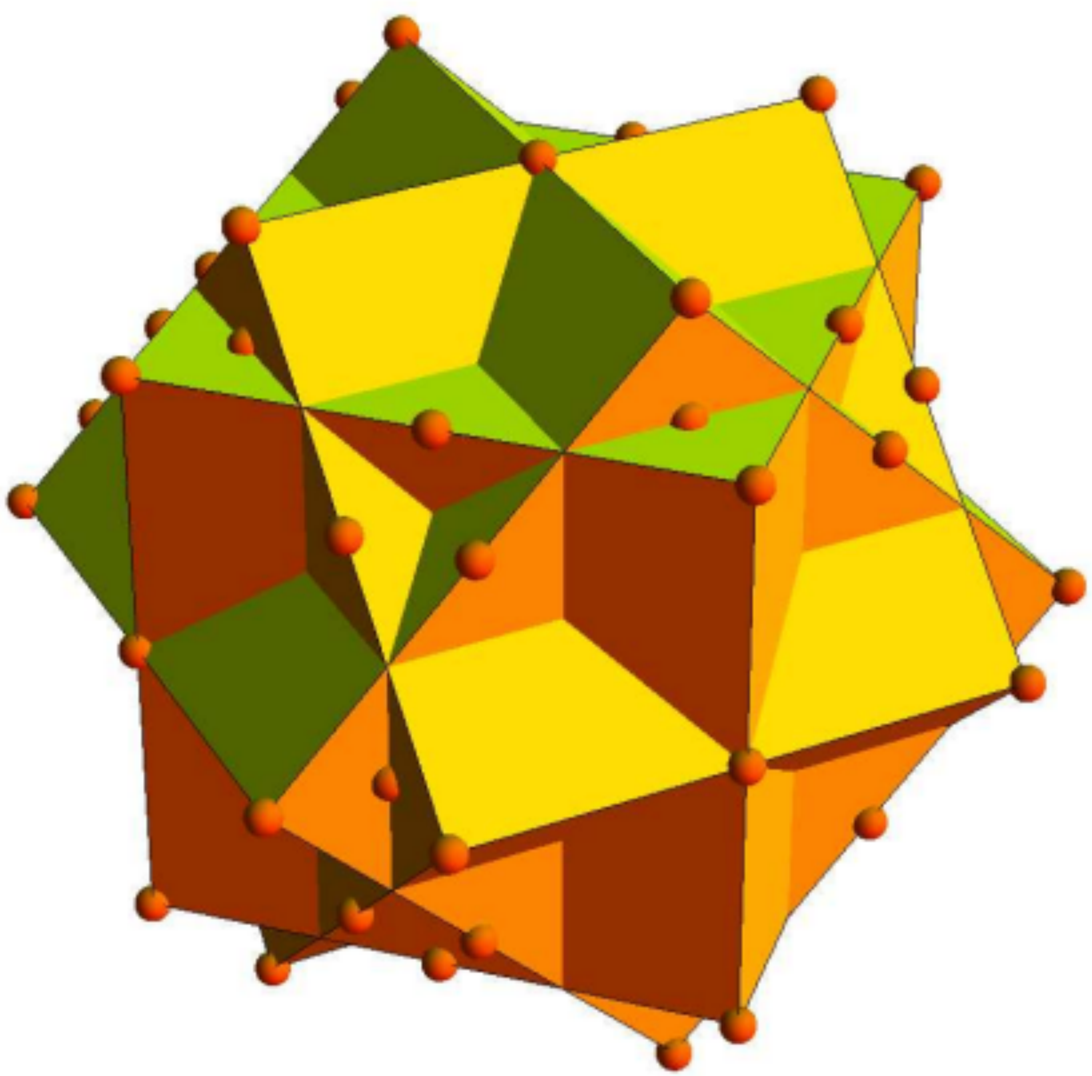
$$\sigma_y \otimes \sigma_y = -\sigma_z \otimes \sigma_z \cdot \sigma_x \otimes \sigma_x$$

- So it's impossible to assign +1 or -1 values to each observable in a context-independent way.

  $\Rightarrow$ QM is contextual.

Proof by Peres (1991) – Kochen and Specker flavour

- Consider 57 states in 3-dimensional Hilbert space, real amplitudes.
  - Orthogonal triads must be colored black, white, white.
  - Some of the triads above have vectors in common.
  - One can show that there's no possible coloring satisfying the orthogonality relations.



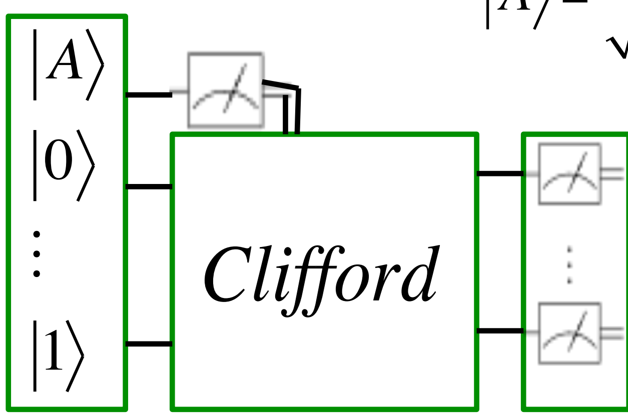
Contextuality is necessary for magic state distillation

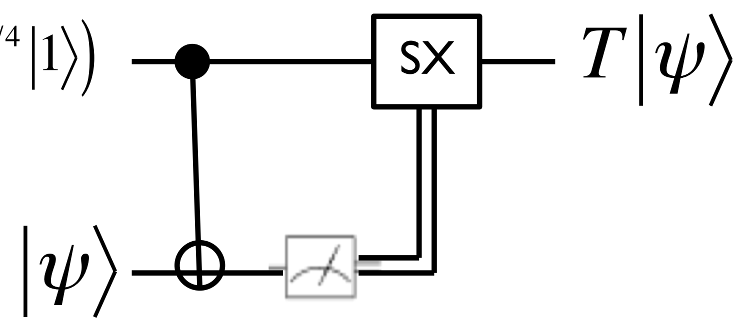
Howard et al., Nature 310, 351 (2014)

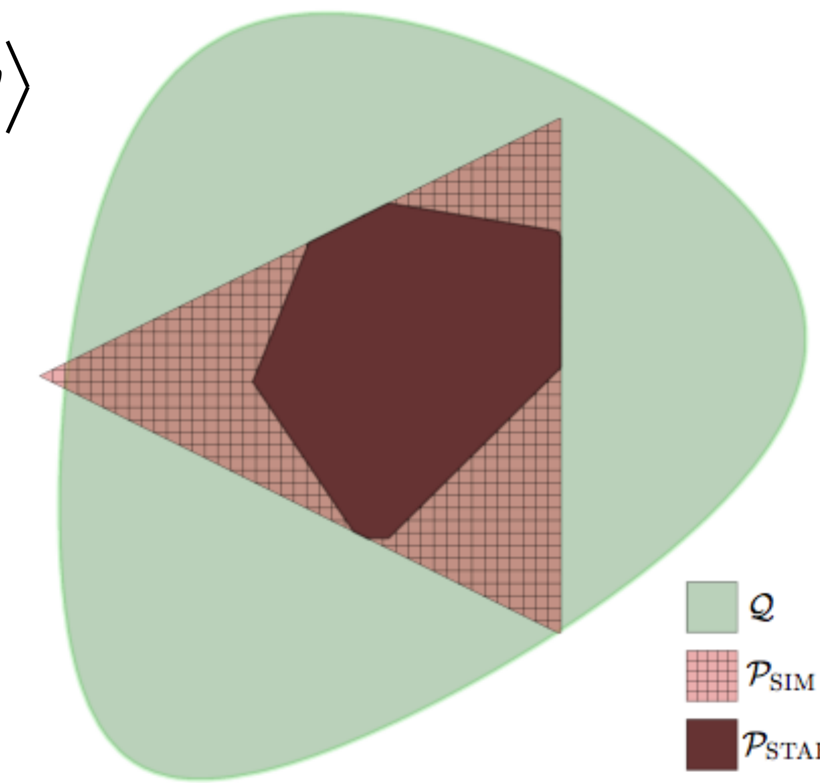
- The Mermin square proof of quantum contextuality is state-independent – any state violates the non-contextuality hypothesis.
- For Hilbert space dimension d>2, all contextuality proofs are *state-dependent.*
- So what’s special about states revealing contextuality?

- Howard et al. (2014) looked at that problem in the QC model of Clifford computer + magic states:

$$|A\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}|1\rangle\right)$$





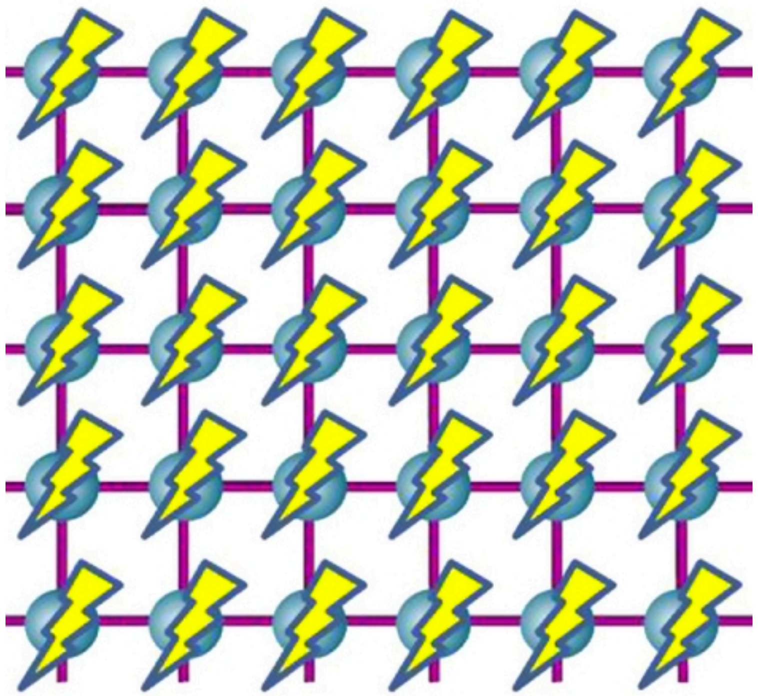


from Howard et al., Nature 310, 351 (2014)

- Result: any state out of PSIM violates a state-dependent non-contextuality inequality, using stabilizer measurements. States in PSIM are non-contextual.

contextuality is necessary
for magic-state computation

PSIM = simulable under stabilizer measurements
PSTAB = stabilizer states
Q = general quantum states



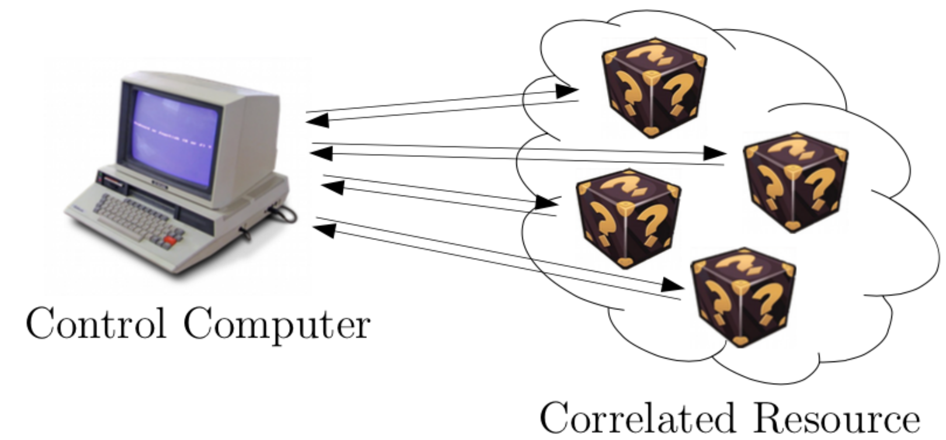
Contextuality in MBQC:
evaluating non-linear Boolean functions

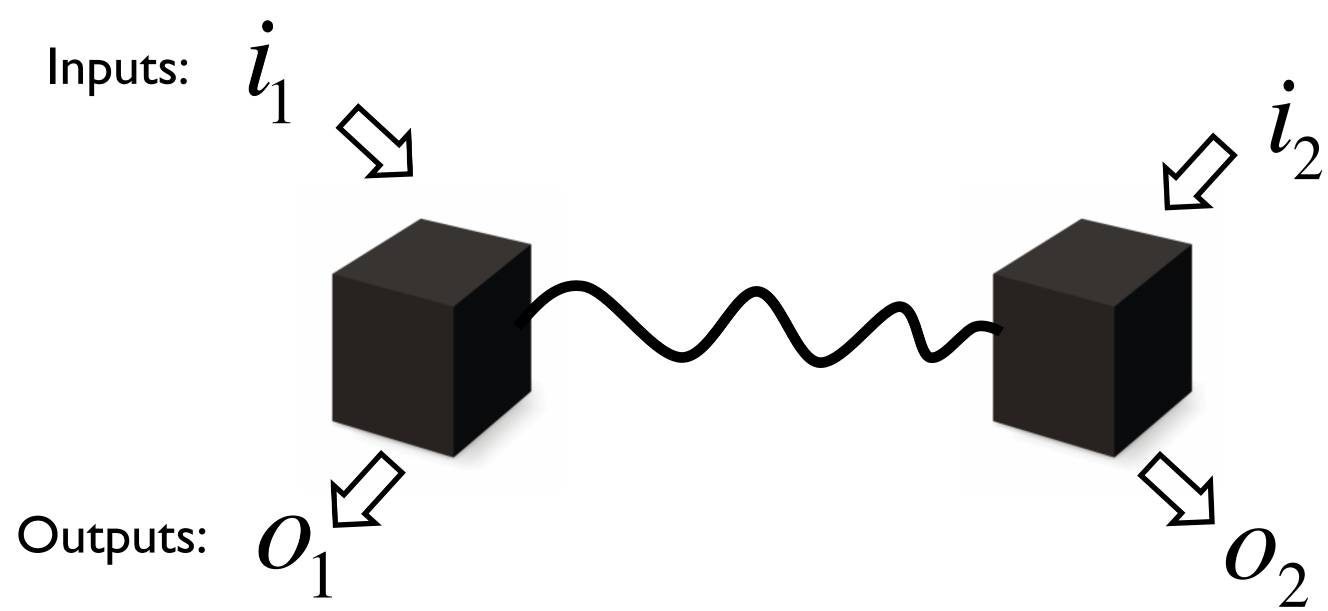
Computation using correlations

Anders, Browne, *PRL* 102, 050502 (2009)

- Measurement-based quantum computation (MBQC) computes with correlations
  - what properties of the correlations enable computation in MBQC?

- Anders and Browne modelled MBQC with:
  - *N* boxes, 1-bit inputs, 1-bit outputs
  - auxiliary pre- and post-computation restricted to sums modulo-2





- Popescu-Rohrlich correlations: deterministic evaluation of i_1 *AND* i_2

$$p(o_1, o_2 \mid i_1, i_2) = \frac{1}{2}\delta_{o_1 \oplus o_2, i_1 AND i_2}$$

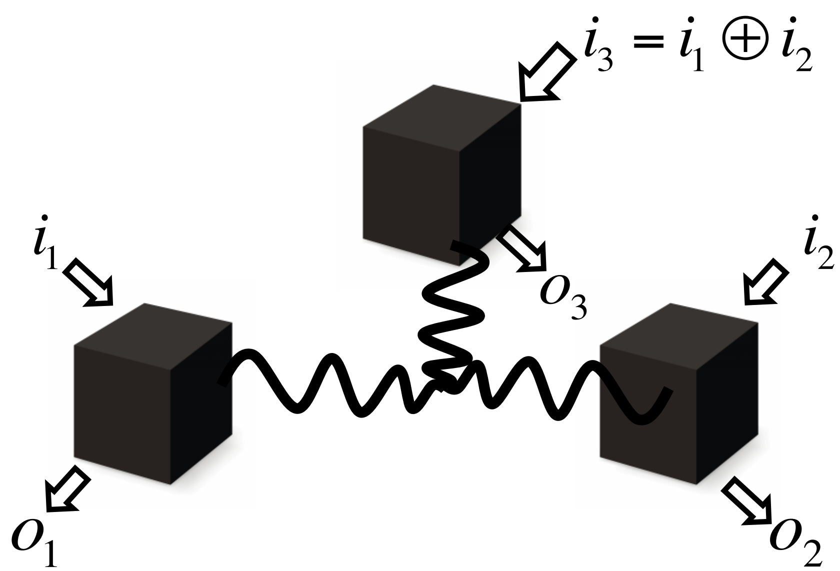
- Quantum correlations result in input-independent error $e = \sin^2(\pi/8) \cong 0.15$
- Non-contextual correlations necessarily result in larger error $e^{NC} \geq 1/4$

(Tsirelson bound)

Deterministic OR from 3-qubit GHZ correlations

Anders, Browne, *PRL* 102, 050502 (2009)

- Stabilizers of 3-qubit GHZ state enable deterministic evaluation of AND gate:



$$\begin{cases} i_j = 0 \Rightarrow \text{Measure X} \\ i_j = 1 \Rightarrow \text{Measure Y} \end{cases}$$

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$$

$$\begin{cases} \text{outcome} = +1 \Rightarrow O_j = 0 \\ \text{outcome} = \text{-}1 \Rightarrow O_j = 1 \end{cases}$$

- GHZ stabilizers: $\{X_1X_2X_3, -X_1Y_2Y_3, -Y_1X_2Y_3, -Y_1Y_2X_3\}$

$$\Rightarrow O_1 \oplus O_2 \oplus O_3 = i_1 \text{ OR } i_2$$

- NOT is free and NOR is universal, so this is sufficient for universal classical computation

- Motivation: is GHZ non-contextuality required for classical computation? Is the quantum AND gate with e=0.15 useless?

2 Theorems by Raussendorf

Raussendorf, *PRA* 88, 022322 (2013)

- Thm. 1: Non-linear Boolean functions require strong contextuality for deterministic MBQC evaluation.

- Thm. 2: MBQC evaluation of arbitrary, *k*-bit Boolean function *f* using non-contextual resources results in average error

$$e_f^{NC} \geq \frac{\nu_f}{2^k}$$

$$\nu_f = \text{ non-linearity of } f = \min_{\text{linear g}} \text{ [no. outputs s.t. } g(i) \neq f(i)]$$

- Example: of i_1 *AND* i_2 = $i_1 i_2$ is nonlinear. Its closest linear approximation is e.g. the constant function 0:

i_1	i_2	$i_1 AND i_2$	0
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	$\cancel{0}$

$\nu_f = 1$

$i_0 i_1$	0	i_1	i_2	$i_1 \oplus i_2 \oplus 1$
00	0	0	0	$\cancel{1}$
01	0	0	$\cancel{1}$	0
10	0	$\cancel{1}$	0	0
11	$\cancel{0}$	1	1	1

Average error of closest linear approximation is ¼.

2 Theorems by Raussendorf

Raussendorf, *PRA* 88, 022322 (2013)

- Thm. 1: Non-linear Boolean functions require strong contextuality for deterministic MBQC evaluation.

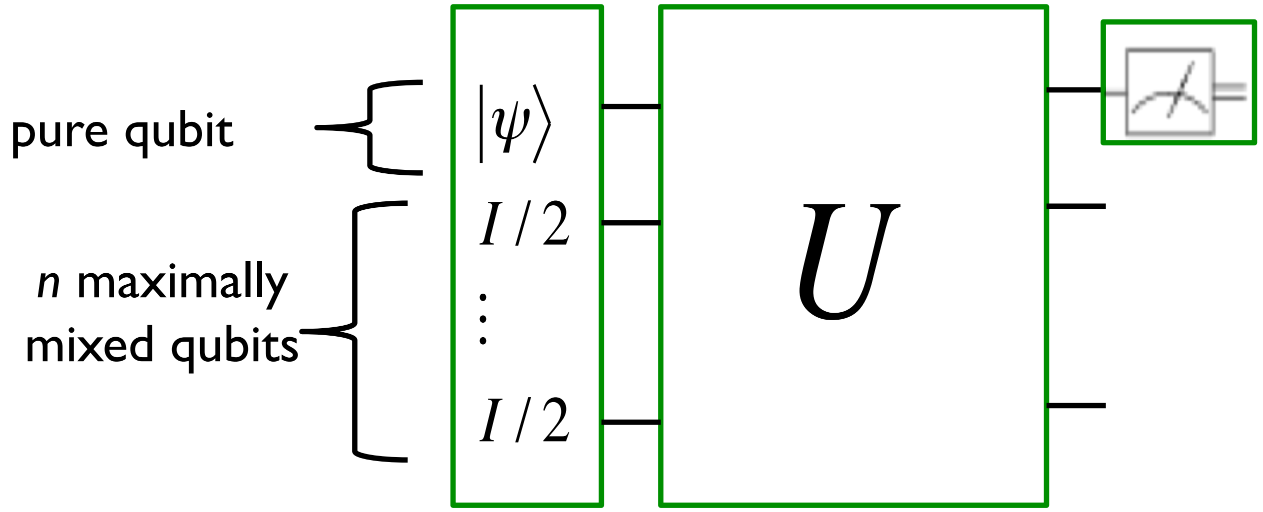
- Thm. 2: MBQC evaluation of arbitrary, k-bit Boolean function f using non-contextual resources results in average error

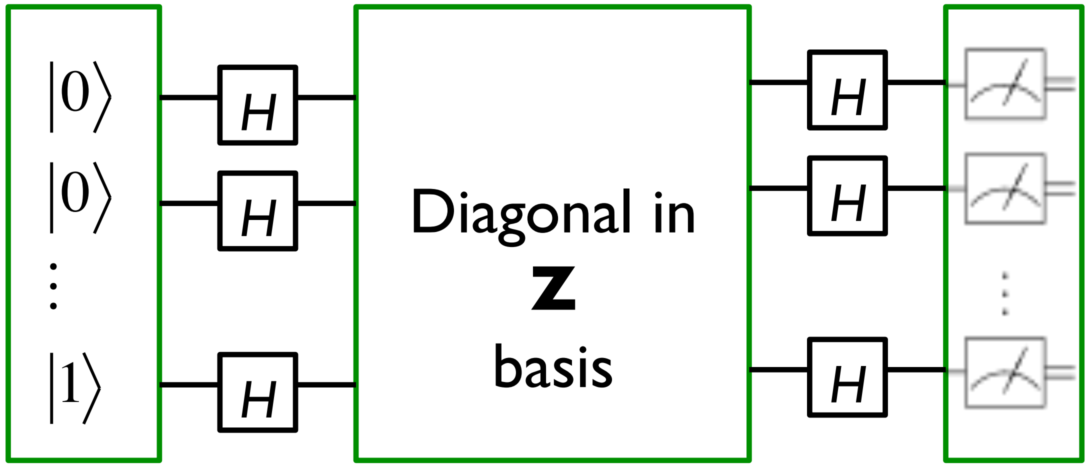
$$e_f^{NC} \geq \frac{\nu_f}{2^k}$$

How much contextuality is sufficient for bounded bias evaluation of any Boolean function?
[Oestereich, E.F.G., PRA 96, 062305 (2017)]

- Arbitrarily small violation of non-contextuality inequality $e_f^{NC} \geq \frac{\nu_f}{2^k}$ is sufficient.

Restricted models
of quantum computation





Restricted models of quantum computation

- Restrictions allow us to:

  - Identify regimes in which <u>quantum computers are simulable</u>
    Clifford circuits
    matchgates
    MBQC on a 1D chain

  - Find new intermediate models which may be <u>useful</u>, even if not universal
    DQC1 or "one-clean-qubit" model by Knill/Laflamme
    Permutational quantum computation (Jordan)

  - Eliminate <u>or minimize resource use</u>, with a view to feasible experiments
    Boson Sampling – Aaronson and Arkhipov
    Non-adaptive MBQC

- Translations between models is particularly interesting, as resource trade-offs are possible