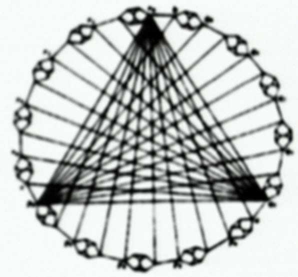
Title: Quantum codes â€“ from experimental realizations to quantum foundations

Date: Jul 15, 2014 11:30 AM

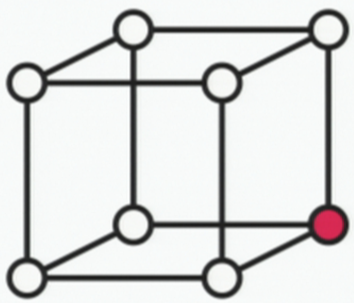
URL: http://pirsa.org/14070008

Abstract: <span>This talk is divided into two parts. In the first part, I discuss a scheme of fault-tolerant quantum computation for a web-like physical architecture of a quantum computer. Small logical units of a few qubits (realized in ion traps, for example) are linked via a photonic interconnect which provides probabilistic heralded Bell pairs [1]. Two time scales compete in this system, namely the characteristic decoherence time T_D and the typical time T_E it takes to provide a Bell pair. We show that, perhaps unexpectedly, this system can be used for fault-tolerant quantum computation for all values of the ratio T_D/T_E.<br><br>The second part of my talk is about something entirely different, namely the role of contextuality in quantum computation by magic state distillation. Recently, Howard et al. [2] have shown that contextuality is a necessary resource for such computation on qudits of odd prime dimension. Here we provide an analogous result for 2-level systems.<br>However, we require them to be rebits. [joint work with Jake Bian, Philippe Guerin and Nicolas Delfosse]<br><br>[1] C. Monroe, R. Raussendorf, A. Ruthven, K. R. Brown, P. Maunz4, L.-M.<br>Duan, and J. Kim, , Phys Rev A 89, 22317 (2014).<br><br>[2] Mark Howard, Joel Wallman, Victor Veitch & Joseph Emerson, Nature<br>doi:10.1038/nature13460 (2014).<br></span>



# Quantum codes

## From thresholds to foundations



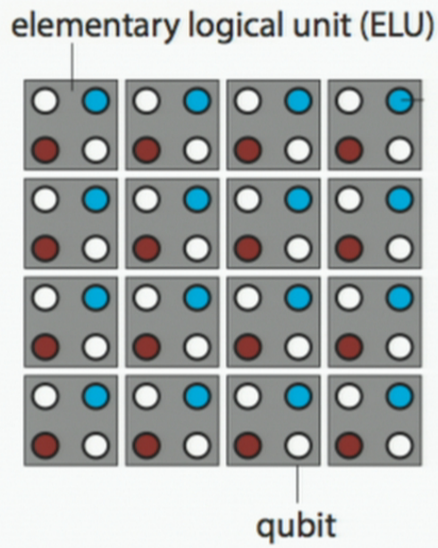
Robert Raussendorf (UBC), Perimeter Institute, July 2014

# Part I

# Fault-tolerance in sparse connectivity geometries

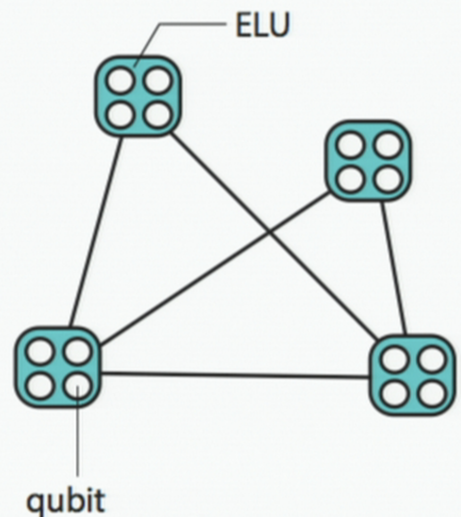
joint work with Chris Monroe, Jungsang Kim, Angela Ruthven and Ken Brown

## Planar architecture




error threshold = 1%
operational mult. overhead ~*log*$^3$(comp size)

## Interaction graph has bounded degree

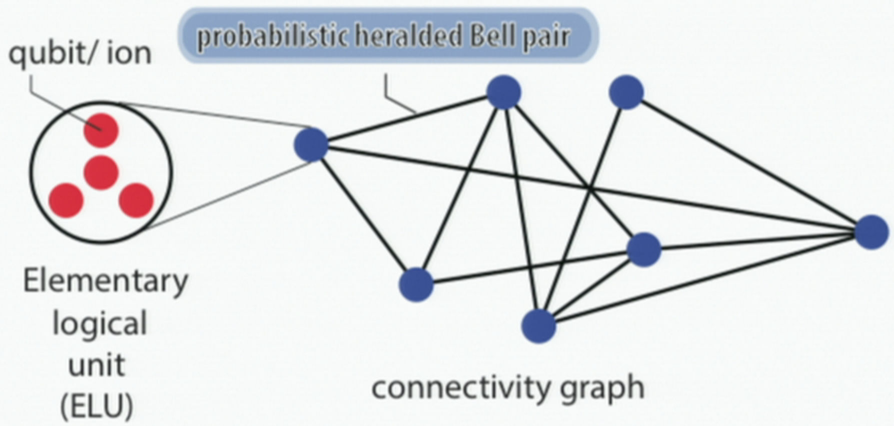



error threshold *???*
overhead *???*

*should be better than planar*


PI
INSTITUTE FOR

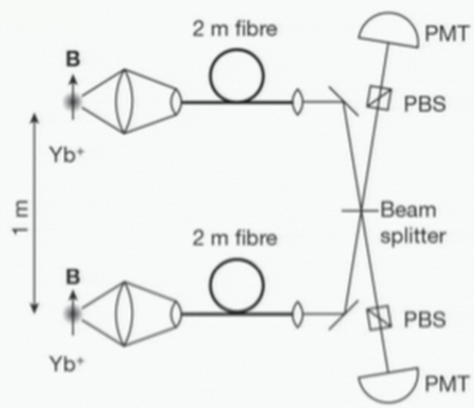
## Modular ion trap with photonic interconnects




Connectivity graph characterized by:

- Low (bounded) degree
- Potentially high dimensionality

# Modular ion trap with photonic interconnects



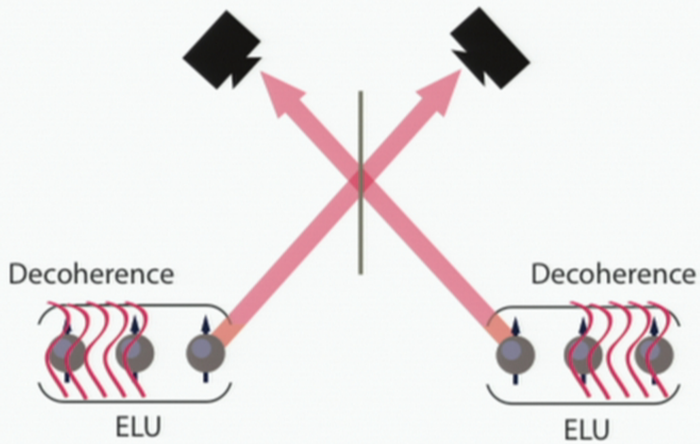

## Physical basis

Probabilistic heralded entanglement via photonic link

[1] D. L. Moehring *et al.*, Nature 449, 68 (2007).
[2] Architecture: C. Monroe *et al.*, Phys. Rev. A (2014).

# Modular ion trap with photonic interconnects

*Obstacle:*




! While entanglement is attempted, everything decoheres.

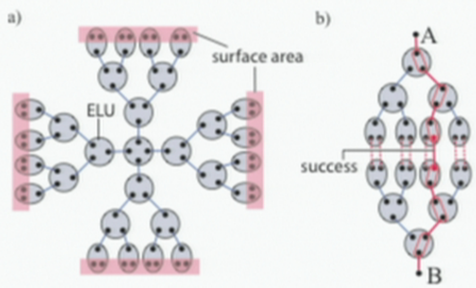
## Modular ion trap with photonic interconnects

- *Challenge:* Build a scalable fault-tolerant universal quantum computer.
- *Idea:* Probabilistic heralded entanglement generation between ion qubits using photons.
- *Obstacles:* Entangling time $\tau_{\mathcal{E}}$ may be long compared to the decoherence time $\tau_D$.

| |
|---|
| Early experiments: $\frac{\tau_{\mathcal{E}}}{\tau_D} = 10^3$, Now: $\frac{\tau_{\mathcal{E}}}{\tau_D} = 0.2$ |

Q: *Is there a maximal ratio $\tau_{\mathcal{E}}/\tau_D$ for fault-tolerance?*

# Modular ion trap with photonic interconnects

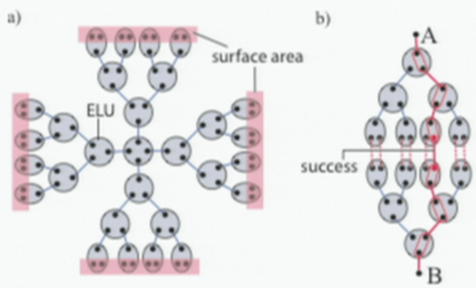



**Theorem 1** *For ELUs of size $n \geq 5$ and small gate error $\epsilon > 0$, efficient universal and fault-tolerant quantum computation is possible for any ratio $\tau_{\mathcal{E}}/\tau_D$.*

+ *There is no threshold $\tau_{\mathcal{E}}/\tau_D$ (!)*
+ Architecture has *constant* multiplicative overhead $c(\tau_{\mathcal{E}}/\tau_D)$.
− Flipside: $c(\tau_{\mathcal{E}}/\tau_D)$ increases exponentially in $\tau_{\mathcal{E}}/\tau_D$.

C. Monroe *et al.*, PRA (2014). Also see: Y. Li *et al.*, PRL 105, 250502 (2010), and K. Fujii and Y. Tokunaga, PRL 105, 250503 (2010).

## Modular ion trap with photonic interconnects



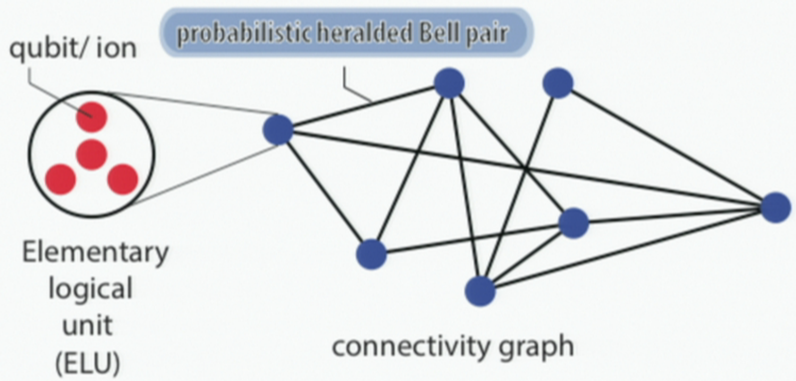

**Theorem 1** *For ELUs of size* $n \geq 5$ *and small gate error* $\epsilon > 0$, *efficient universal and fault-tolerant quantum computation is possible for any ratio* $\tau_{\mathcal{E}}/\tau_D$.

+ *There is no threshold* $\tau_{\mathcal{E}}/\tau_D$ *(!)*
+ Architecture has *constant* multiplicative overhead $c(\tau_{\mathcal{E}}/\tau_D)$.
− Flipside: $c(\tau_{\mathcal{E}}/\tau_D)$ increases exponentially in $\tau_{\mathcal{E}}/\tau_D$.

C. Monroe *et al.*, PRA (2014). Also see: Y. Li *et al.*, PRL 105, 250502 (2010), and K. Fujii and Y. Tokunaga, PRL 105, 250503 (2010).

## Summary

- *No practical solution yet, playing field wide open*

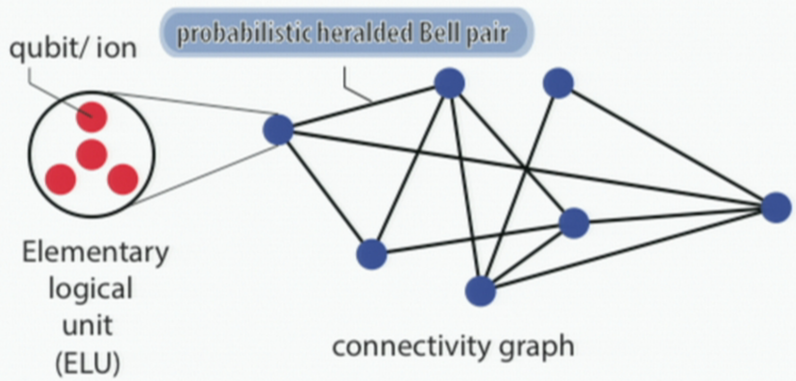



- Low (bounded) degree of the connectivity graph
- Potentially high-dimensional embedding

$\longrightarrow$ *Calls for LDPC codes*

## Summary

- *No practical solution yet, playing field wide open*




- Low (bounded) degree of the connectivity graph
- Potentially high-dimensional embedding

⟶ *Calls for LDPC codes*

PHYSICAL REVIEW A VOLUME 55, NUMBER 6 JUNE 1997

# Quantum code words contradict local realism

David P. DiVincenzo
*IBM Research Division, IBM T. J. Watson Research Center, Yorktown Heights, New York 10598*

Asher Peres*
*Institute for Theoretical Physics, University of California, Santa Barbara, California 93106*
(Received 8 November 1996)

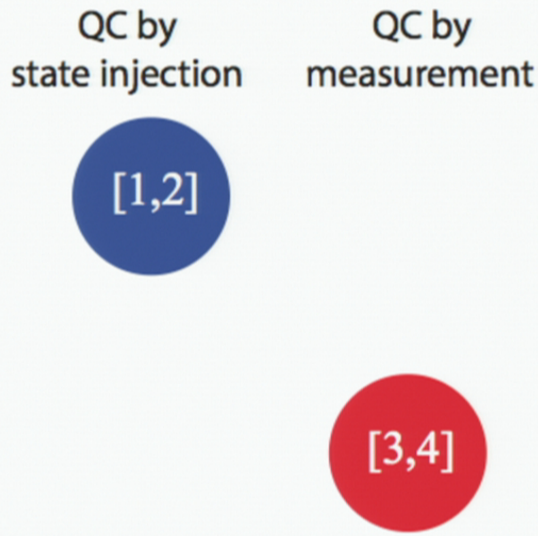
Quantum code words are highly entangled combinations of two-state systems. The standard assumptions of local realism lead to logical contradictions similar to those found by Bell, Kochen, and Specker, Greenberger, Horne and Zeilinger, and Mermin. The new contradictions have some noteworthy features that did not appear in the older ones. [S1050-2947(97)00306-5]

PACS number(s): 03.65.Bz, 89.80.+h, 89.70.+c

Quantum code words are highly entangled combinations of two-state quantum systems (qubits). They are structured in such a way that if one (or sometimes more) of the qubits is perturbed, there remains enough quantum information encoded in the remaining qubits for restoring the original code word unambiguously [1–4]. In this article, we investigate some properties of the five-qubit code words invented by Bennett *et al.* [5] (which are equivalent, up to a change of bases of the individual qubits, to the five-qubit code words of Laflamme *et al.* [2]). The logical 0 is represented by the

$$\sigma_{xzuzx}, \quad \sigma_{yxuxy}, \quad \sigma_{zyuyz}, \quad \mp\sigma_{uxzxu},$$
$$\mp\sigma_{yuzuy}, \quad \pm\sigma_{xyzyx}, \tag{3}$$

and their cyclic permutations. The upper and lower signs refer to $|0_L\rangle$ and $|1_L\rangle$, respectively, (this convention will be followed throughout this article). These 32 operators (with either choice of sign) form an Abelian group; those that are unsigned in Eq. (3) form an invariant subgroup. The existence of such a group associated with this type of quantum



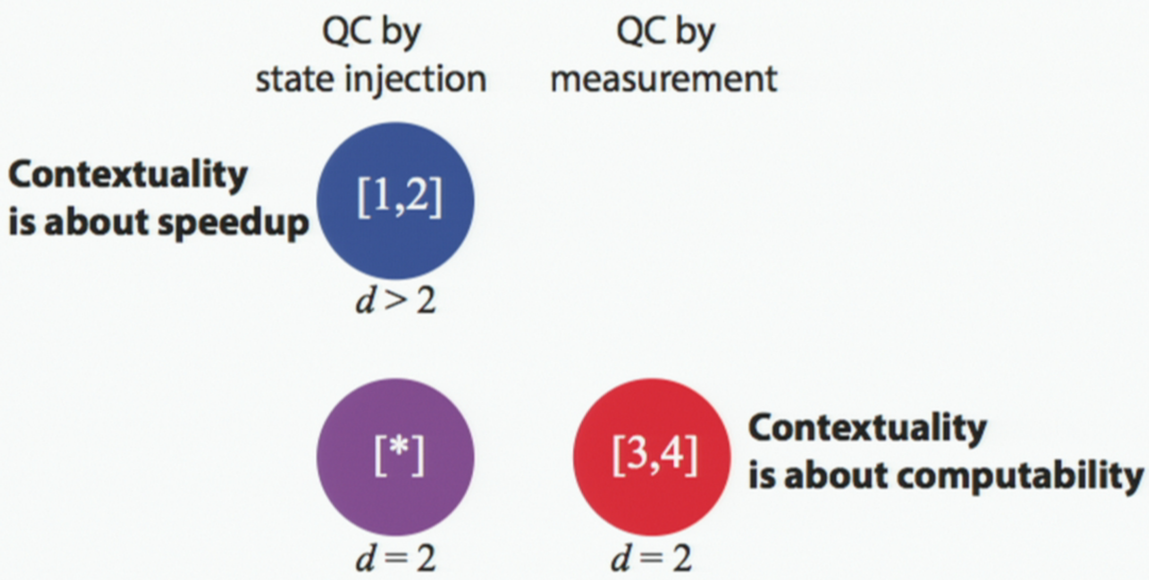

[1] V. Veitch *et al.*, New J. Phys. 14, 113011 (2012).

[2] M. Howard *et al.*, Nature (2014), arXiv:1401.4174.

[3] J. Anders and D. Browne, PRL 2009.

[4] R. Raussendorf, PRA 2013.

[*] joint work w. Jake Bian, Philippe Guerin, Nicolas Delfosse; on arXiv soon.




[1] V. Veitch *et al.*, New J. Phys. 14, 113011 (2012).

[2] M. Howard *et al.*, Nature (2014), arXiv:1401.4174.

[3] J. Anders and D. Browne, PRL 2009.

[4] R. Raussendorf, PRA 2013.

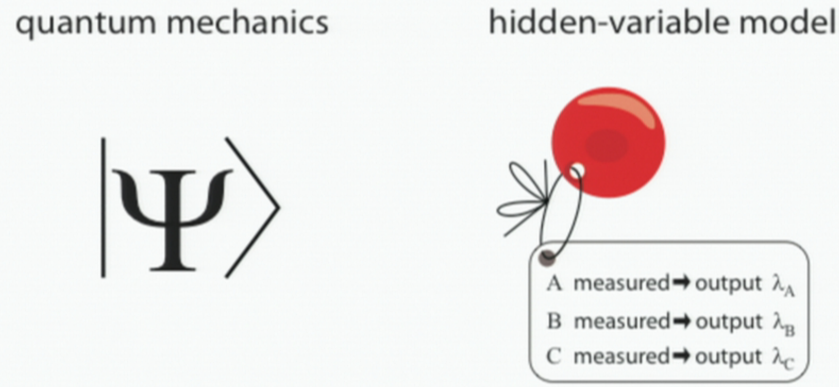
[*] joint work w. Jake Bian, Philippe Guerin, Nicolas Delfosse; on arXiv soon.

# Outline

1. Review
   (a) Hidden variable models & contextuality
   (b) Contextuality in measurement-based quantum computation
   (c) Contextuality, Wigner function negativity in QC with magic states; *What goes wrong for qubits*
2. Quantum computation with magic states on rebits
   (a) Computational scheme
   (b) Matching Wigner function
   (c) Matching notion of contextuality
   (d) Results and comparison with qudits

# Contextuality of QM

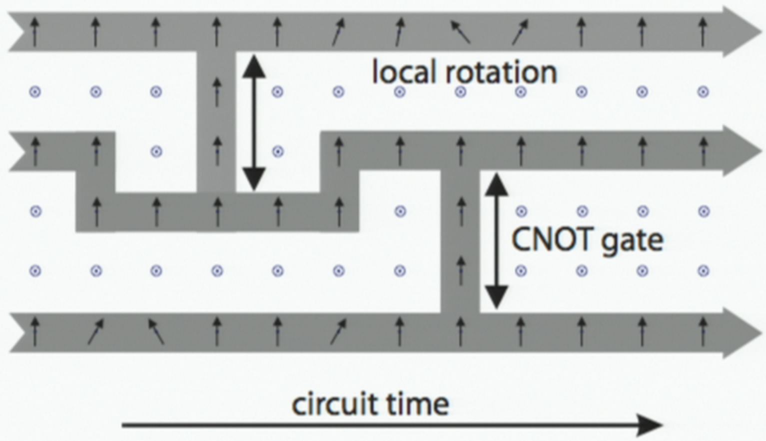
*What is a non-contextual hidden-variable model?*




Noncontextuality: Given observables $A$,$B$,$C$: $[A, B] = [A, C] = 0$:
$\lambda_A$ is *independent* of whether $A$ is measured jointly with $B$ or $C$.

**Theorem** [Kochen, Specker]: For $\dim(\mathcal{H}) \geq 3$, quantum-mechanics cannot be reproduced by a non-contextual hidden-variable model.

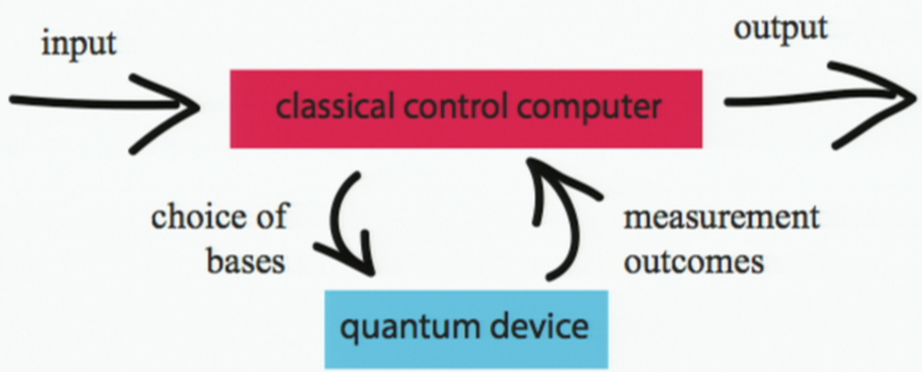
# Quantum computation by measurement




- Information written onto a cluster state, processed and read out by one-qubit measurements only.
- The resulting computational scheme is *universal*.

R. Raussendorf and H.-J. Briegel, PRL 86, 5188 (2001).

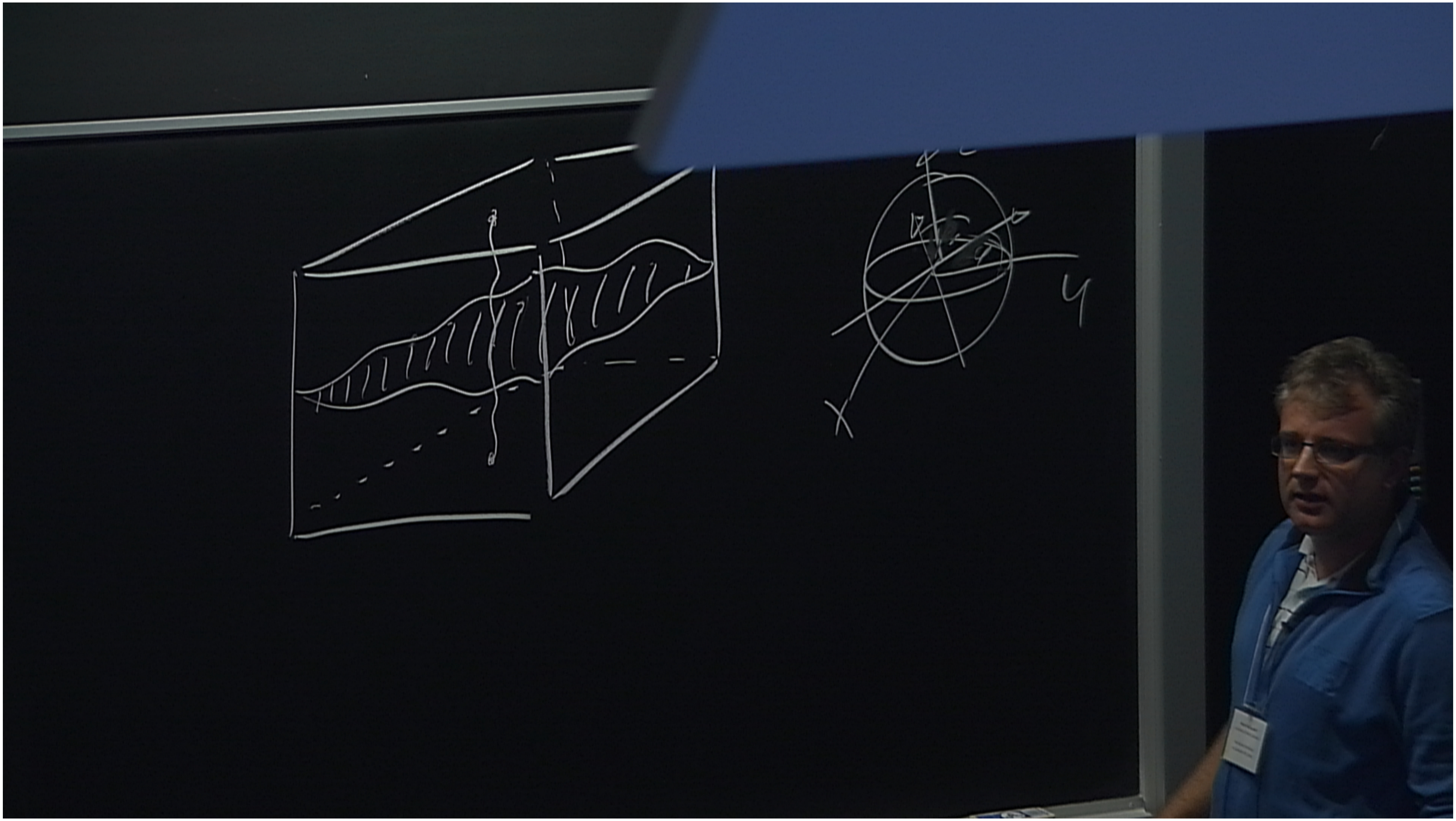
## Classical processing relations




All classical processing is *mod-2 linear!*

- Linear functions are for free.
- Non-linear functions are of value

*What resources are needed to evaluate non-linear functions?*



## An extension of Theorem 1

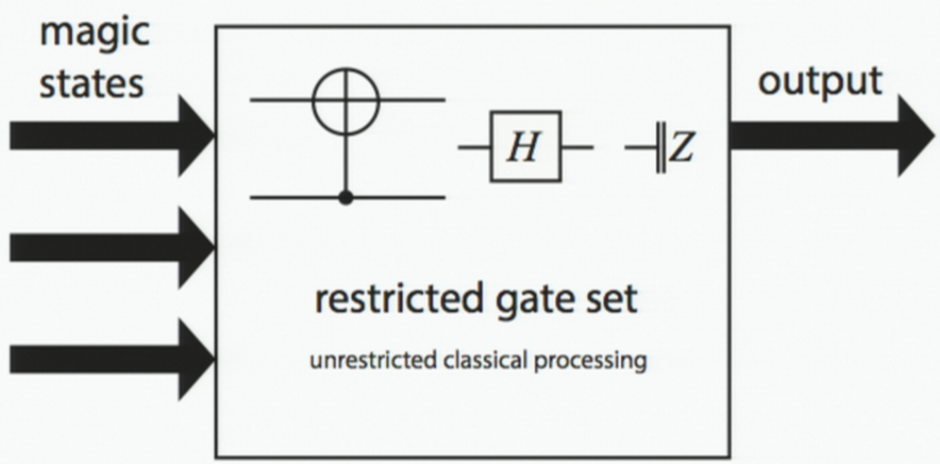
*Can the condition of determinism be relaxed?*

**Theorem 2:** Be $M_{p_s}$ an MBQC on qubits that probabilistically evaluates a non-linear Boolean function on $m$ bits of input, with success probability $p_S$. If $\boxed{p_S > 1 - \frac{1}{2^m}}$ then $M_{p_S}$ is contextual.

**Theorem 3:** Be $M_{p_S}$ an MBQC on qubits that evaluates with success probability $p_S$ a bent function on $m$ bits. Then $M_{p_S}$ is contextual if $\boxed{p_S > \frac{1}{2} + \left(\frac{1}{2}\right)^{m/2+1}}$.

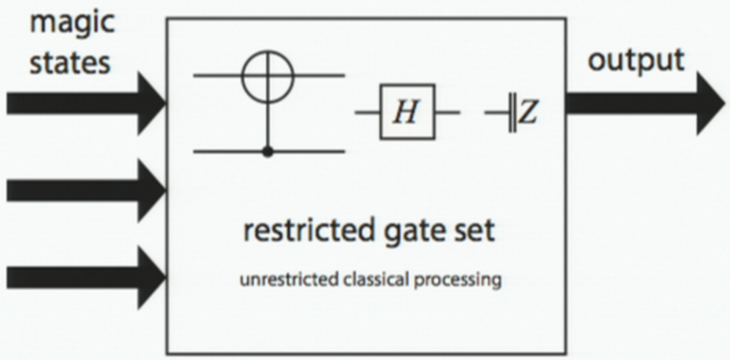
*An MBQC can be contextual even if its output is almost completely random.*

# Different model: QC by state injection




- Non-universal restricted gate set: *e.g. Clifford gates.*
- Universality reached through injection of *magic states.*
- *As of now, leading scheme for fault-tolerant QC.*

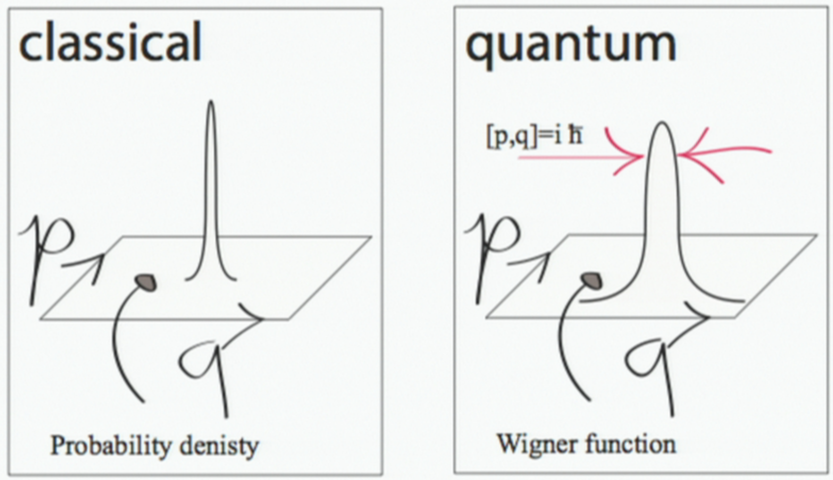
# QC by state injection




*Which properties must the magic states have to enable universality?*

A: Wigner function negativity, contextuality

## [quantum] mechanics in phase space

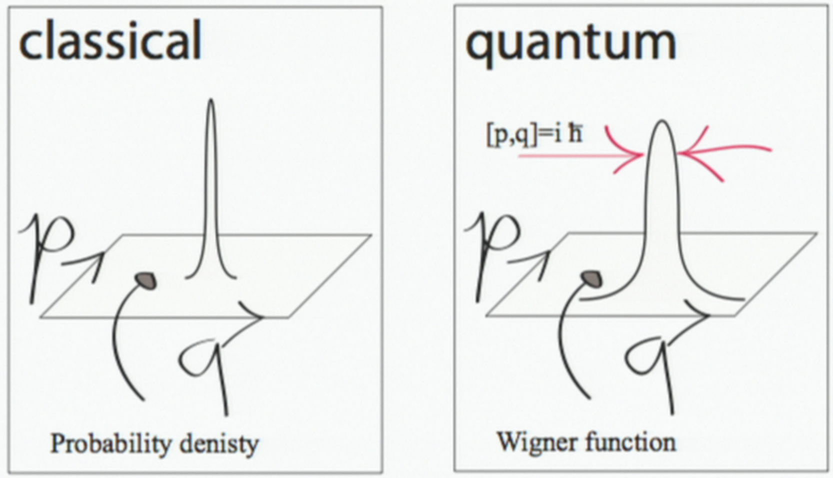



- The Wigner function

$$W_\psi(p,q) = \frac{1}{\pi}\int d\xi\, e^{-2\pi i\xi p}\psi^\dagger(q-\xi/2)\psi(q+\xi/2).$$

is a quasi-probability distribution.

## [quantum] mechanics in phase space

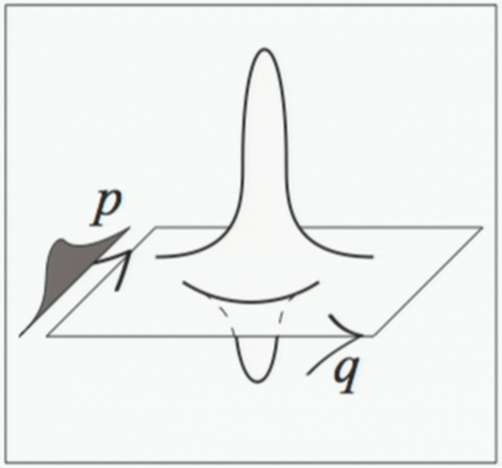



- The Wigner function

$$W_\psi(p,q) = \frac{1}{\pi}\int d\xi\, e^{-2\pi i \xi p}\psi^\dagger(q-\xi/2)\psi(q+\xi/2).$$

is a quasi-probability distribution.

## [quantum] mechanics in phase space




- Wigner function can go negative
- Marginals must be non-negative

Wigner function negativity is an indicator of quantumess

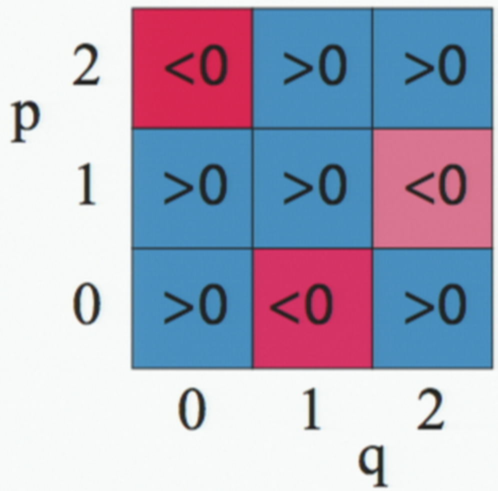
*Which states have positive/ negative Wigner function?*

## Hudson's theorem

*Which states have positive/ negative Wigner function?*

> **Theorem.** A pure state $\psi$ has a non-negative Wigner function if and only if and only if $\psi$ is Gaussian, i.e. $\psi(q) \sim e^{2\pi i(q\theta q + xq)}$.

# Wigner functions for qudits




Possible Wigner function for a qutrit

Wigner functions can be adapted to finite-dimensional state spaces.

## Wigner functions for $n$ qudits – Definition

- $W$ is built from qudit Pauli operators $T_{\mathbf{a}} = Z(\mathbf{a}_Z)X(\mathbf{a}_X)$:

$$W_\rho(\mathbf{v}) = \frac{1}{d^n}\text{Tr}(A_{\mathbf{v}}\rho), \quad \forall \mathbf{v} \in \mathbb{Z}_d{}^n \times \mathbb{Z}_d{}^n, \qquad (1)$$

where

$$A_{\mathbf{v}} = T_{\mathbf{v}} A_0 T_{\mathbf{v}}^\dagger, \qquad (2)$$

and

$$A_0 = \frac{1}{d^n}\sum_{\mathbf{v}} \omega^{\mathbf{a}_Z\cdot\mathbf{a}_X/2 \text{ mod } d} T_{\mathbf{v}}. \qquad (3)$$

| | | |
|---|---|---|
| $A_{(2,0)}$ | $A_{(2,1)}$ | $A_{(2,2)}$ |
| $A_{(1,0)}$ | $A_{(1,1)}$ | $A_{(1,2)}$ |
| $A_{(0,0)}$ | $A_{(0,1)}$ | $A_{(0,2)}$ |

*: In Eq. (3), replace $\omega^{\mathbf{a}_z\cdot\mathbf{a}_x/2 \text{ mod } d}$ by $i^{\mathbf{a}_z\cdot\mathbf{a}_x \text{ mod } 4}$ for $d = 2$.

## Wigner functions for qudits – Properties

Elementary properties

- $W$ is linear in $\rho$.
- The marginals of $W$ are probability distributions.
- $W$ is informationally complete.

## Wigner functions for qudits – Properties

If the dimension $d$ is a power of an odd prime, then

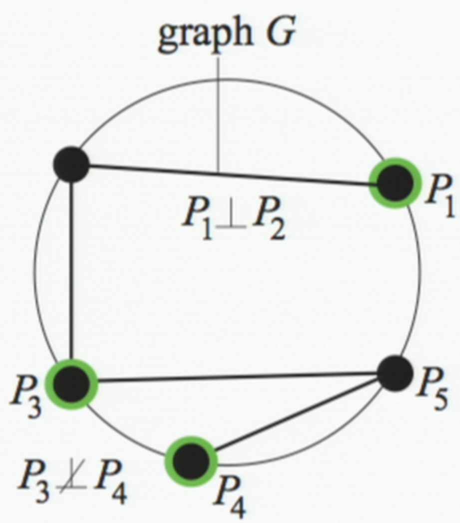
> **Theorem.*** [extended Gottesman-Knill theorem] The evolution of states $\rho$ with positive Wigner function under Clifford gates and Pauli measurements can be efficiently classically simulated.

**Consequence:**

- Wigner function negativity is *necessary* for a quantum speedup

*: V. Veitch *et al.*, NJP 2012.

## Contextuaity




$P_i$: projector on stabilizer state

$\max\langle\sum_i P_i\rangle_{\text{class}} =: \alpha(G)$

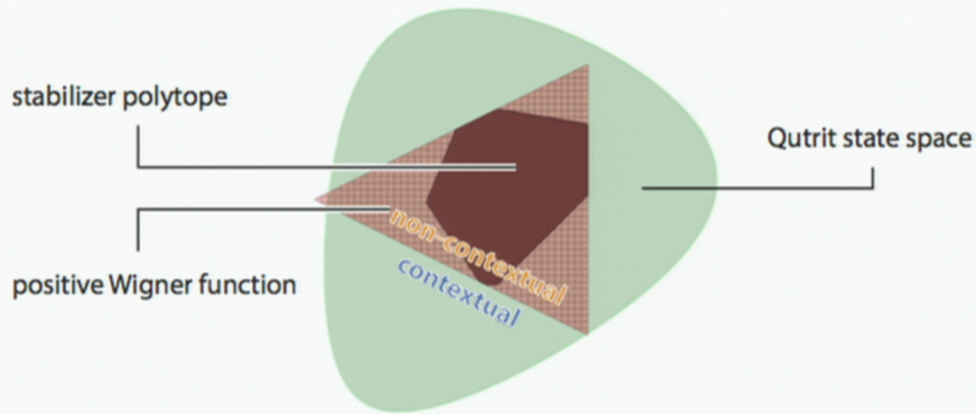
$\max\langle\sum_i P_i\rangle_{\text{QM}} =: \theta(G)$

$\theta(G) > \alpha(G) \implies$ setting contextual [1]

$\boxed{\langle\Psi|\sum P_i|\Psi\rangle > \alpha(G) \implies |\Psi\rangle \text{ contextual}}$ [2]


[1] Cabello, Severini and Winter, PRL 2014.
[2] M. Howard *et al.*, Nature 2014.

# Qudit state space




- All positive pure states are stabilizer states [Gross].
- Clifford ops on positive states efficiently simulatable [Veitch et al.]
- Set of positive states = set of non-contextual states [Howard et al.]

| Contextuality, Wigner negativity: necessary resources for QC. |
|---|

*** end of review ***

Contextuality and Wigner negativity

in QC by state injection

on rebits

## QC by state injection with rebits

- *We devise a universal scheme of quantum computation by state injection for rebits.*

For this scheme, the following properties of $d > 2$ are restored:

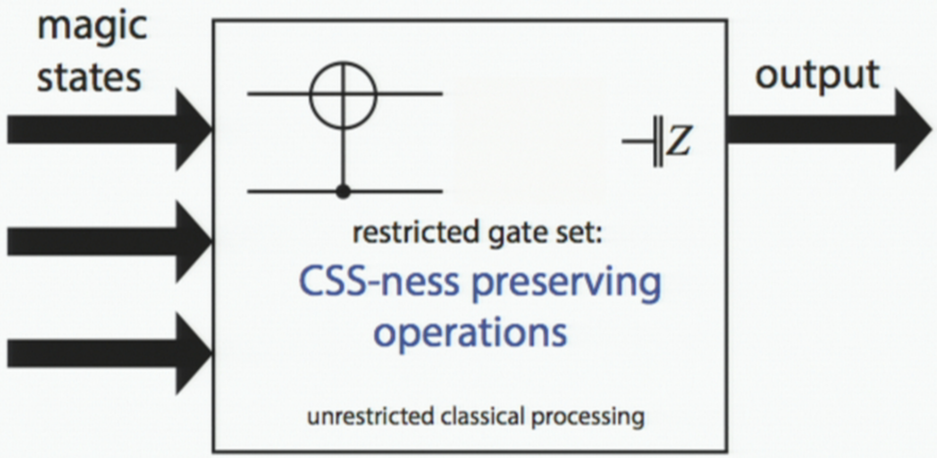
- [discrete Hudson's thm] A state is pure if and only if it is a CSS state.
- The rebit Wigner function is covariant under all CSS-ness preserving operations.
- [extended Gottesman-Knill theorem] CSS-ness preserving operations on positive states are efficiently simulatable .
- $W_\rho$ is positive $\Longrightarrow$ $\rho$ is non-contextual.

| Contextuality, Wigner negativity: necessary resources for QC |
|---|

## Tasks

1. Devise universal scheme of quantum computation by state injection on rebits
2. Construct matching Wigner function
3. Find matching notion of state-dependent contextuality

## QC by state injection on rebits




- Non-universal gate set: *CSS-ness preserving Clifford gates.*
- Universality reached through injection of *magic states.*

## 1. Computational scheme

- Use encoding of $n$ qubits in $n+1$ rebits*:

$$|\Psi\rangle \longrightarrow \mathcal{R}(|\Psi\rangle) \otimes |R\rangle_{n+1} + \mathcal{I}(|\Psi\rangle) \otimes |I\rangle_{n+1}.$$

- Restricted gate set: CSS-ness preserving operations

$CNOTs$, $H_{\text{all}}$, Pauli flips, measurements of $Z_i, X_i$.

- Use magic states

$$\begin{aligned} |A\rangle &= \frac{|0\rangle|0\rangle}{\sqrt{2}} + |1\rangle\frac{|0\rangle+|1\rangle}{2} \\ |B\rangle &= \frac{|0\rangle|+\rangle+|1\rangle|-\rangle}{\sqrt{2}} \end{aligned}.$$

[*] T. Rudolph and L. Grover, *Encoded universality using rebits*, quant-ph/02

## 1. Computational scheme

- Use encoding of $n$ qubits in $n+1$ rebits*:

$$|\Psi\rangle \longrightarrow \mathcal{R}(|\Psi\rangle) \otimes |R\rangle_{n+1} + \mathcal{I}(|\Psi\rangle) \otimes |I\rangle_{n+1}.$$

- Restricted gate set: CSS-ness preserving operations

$CNOTs$, $H_{\text{all}}$, Pauli flips, measurements of $Z_i, X_i$.

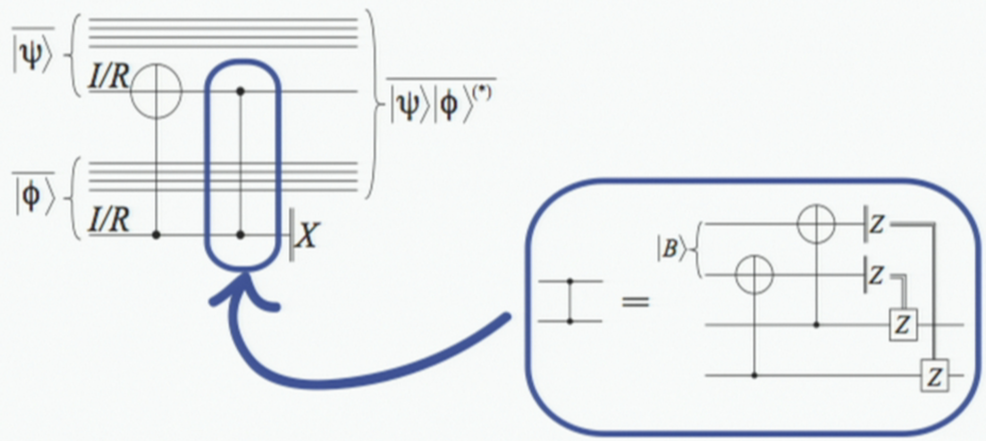
- Use magic states

$$\begin{aligned} |A\rangle &= \frac{|0\rangle|0\rangle}{\sqrt{2}} + |1\rangle\frac{|0\rangle+|1\rangle}{2} \\ |B\rangle &= \frac{|0\rangle|+\rangle+|1\rangle|-\rangle}{\sqrt{2}} \end{aligned}.$$

[*] T. Rudolph and L. Grover, *Encoded universality using rebits*, quant-ph/02

# 1. Computational scheme

- Devise circuits for the various encoded gates.




Example: circuit for code merging

Purpose: Merge separately encoded ancillas into one code block.

## 2. Rebit Wigner function $W_\rho$

- $W$ is a quasi-probability distribution.
- Built from Pauli/ translation operators $T_{\mathbf{a}} = Z(\mathbf{a}_Z)X(\mathbf{a}_X)$:

$$W_\rho(\mathbf{v}) = \frac{1}{2^n}\mathrm{Tr} A_{\mathbf{v}}\rho, \quad \forall \mathbf{v} \in {\mathbb{Z}_2}^n \times {\mathbb{Z}_2}^n, \tag{4}$$

where

$$A_{\mathbf{v}} = T_{\mathbf{v}} A_0 T_{\mathbf{v}}^\dagger, \tag{5}$$

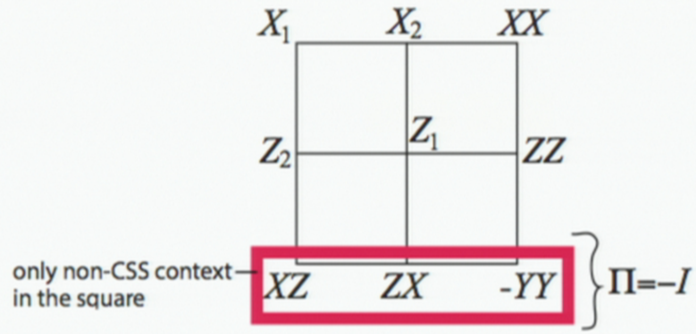
and

$$A_0 = \frac{1}{2^n} \sum_{\mathbf{v}|\, \mathbf{v}_Z \cdot \mathbf{v}_X = 0} 1\, T_{\mathbf{v}}. \tag{6}$$

Page 45 of 50

# 2. Rebit Wigner function $W_\rho$

Illustration:
Positivity of CSS-states.




- The joint eigenstates of $XZ$, $ZX$, $-YY$ are non-CSS and have negative Wigner function
- The joint eigenstates of the observables in all other contexts are CSS and have positive Wigner function.
- Consequence of $\prod_{O\in\text{context}} O = \pm I$.

## 2. Rebit Wigner function $W_\rho$

- $W$ is a quasi-probability distribution.
- Built from Pauli/ translation operators $T_{\mathbf{a}} = Z(\mathbf{a}_Z)X(\mathbf{a}_X)$:

$$W_\rho(\mathbf{v}) = \frac{1}{2^n}\mathrm{Tr} A_{\mathbf{v}}\rho, \quad \forall \mathbf{v} \in \mathbb{Z}_2{}^n \times \mathbb{Z}_2{}^n, \tag{4}$$

where

$$A_{\mathbf{v}} = T_{\mathbf{v}} A_0 T_{\mathbf{v}}^\dagger, \tag{5}$$

and

$$A_0 = \frac{1}{2^n} \sum_{\mathbf{v}|\, \mathbf{v}_Z \cdot \mathbf{v}_X = 0} 1\, T_{\mathbf{v}}. \tag{6}$$

## 3. Contextuality & Wigner functions

**Lemma.** $W_\rho \geq 0 \longrightarrow$ CSS-measurements on $\rho$ are described by a non-contextual HVM.

*Proof sketch:* A positive Wigner function *is* a non-contextual HVM.

Consider a POVM with elements $E_a$. The probability of outcome $a$ is

$$p_a = \sum_{\mathbf{u}\in\mathbb{Z}_2^{2n}} W_{E_a}(\mathbf{u}) W_\rho(\mathbf{u}).$$

For the allowed measurements, all $W_{E_a} \geq 0$. Therefore may identify

$$\begin{aligned} \{\mathbf{u} \in \mathbb{Z}_2^{2n}\} &: \text{ set of states} \\ W_\rho(\mathbf{u}) &: \text{ probability of state } \mathbf{u} \\ W_{E_a} &: \text{ conditional probability of outcome } a \text{ given } \mathbf{u}. \end{aligned}$$

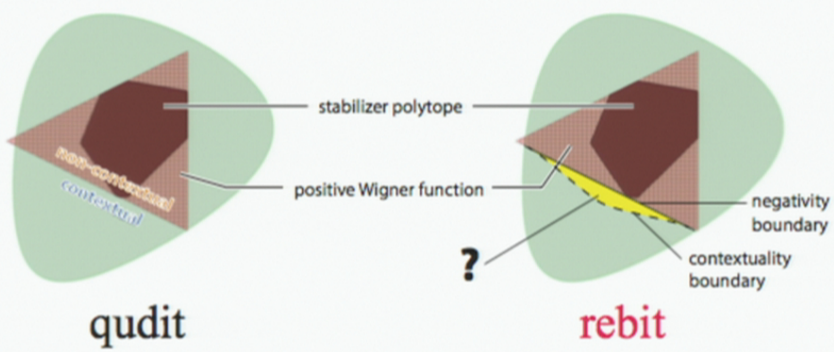
Need to check that the conditional probability distributions $\{p_a(E)\}$ are compatible under taking marginals. $\Rightarrow$ Works! Have a non-contextual HVM. $\square$

Wigner function negativity is necessary for contextuality.

# Result

**Theorem.** In quantum computation by state injection on rebits, Wigner negativity of the magic states is necessary for the hardness of classical simulation.

**Theorem.** In quantum computation by state injection on rebits, contextuality and Wigner negativity of the magic states are necessary for computational universality.



## Open questions

- *Why does contextuality play different roles in QC with magic states and MBQC?*
- *Covariance is an important property of Wigner functions. Does covariance play any role in MBQC?*

## Questions Re fault-tolerance

- *For which restricted gate sets does quantum computation by state injection work?*
- *Is there any favourable alternative to Clifford gates as the restricted gate set?*
- *Is there any favourable alternative to magic state distillation?*