Title: Is there a classical analogue of measurement-based quantum computation?

Date: Apr 29, 2008 02:00 PM

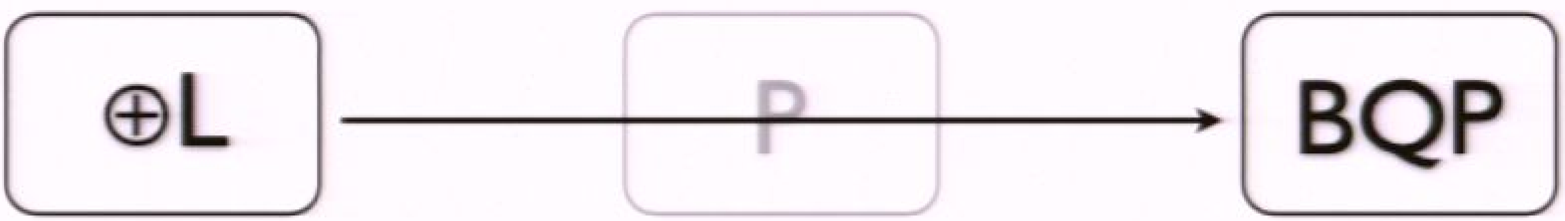
URL: http://pirsa.org/08040054

Abstract: Measurement-based quantum computation is unusual among quantum computational models in that it does not have an obvious classical analogue. In this talk, I shall describe some new results which shed some new light on this. In the one-way model [1], computation proceeds by adaptive single-qubit measurements on a multi-qubit entangled \'cluster state\'. The adaptive measurements require a classical computer, which processes the previous measurement outcomes to determine the correct bases for the following measurement. We shall describe a generalisation of the model where this classical \'side-computation\' plays a more central role. We shall show that this classical computer need not be classically universal, and can instead by performed by a limited power \'CNOT computer\' - a reversible classical computer whose generating gate set consists of CNOT and NOT. The CNOT computer is not universal for classical computation and is believed to be less powerful. Most notably in the context of quantum computation, it is the class of computer sufficient for the efficient simulation of Clifford group circuits [2] - a closely related result. This motivates the question of what resource states would be universal for classical computation, if the control computer is in the CNOT class. We shall answer this question with several examples. Leading from these examples, a natural question is thus, is \'classically universal measurement based computation\' possible with solely classical physics? By considering different settings, we shall answer this question both in the negative and positive, and draw some striking connections with some well-known techniques from models of generalised no-signalling theories. [1] R. Raussendorf and H.J. Briegel, Phys Rev Lett (2001) 86 5188 [2] S. Aaronson and D. Gottesman, Phys Rev A (2004) 70 052328 This is joint work with Janet Anders. We would like to acknowledge inspiring and fruitful discussions with Hans Briegel, Akimasa Miyake, Robin Blume Kohout and Debbie Leung.

# Measurement-Based Classical Computation:

## Classifying the computational power of entangled states

**Dan Browne**
University College London




Joint work with **Janet Anders**

# Measurement-Based Quantum Computation

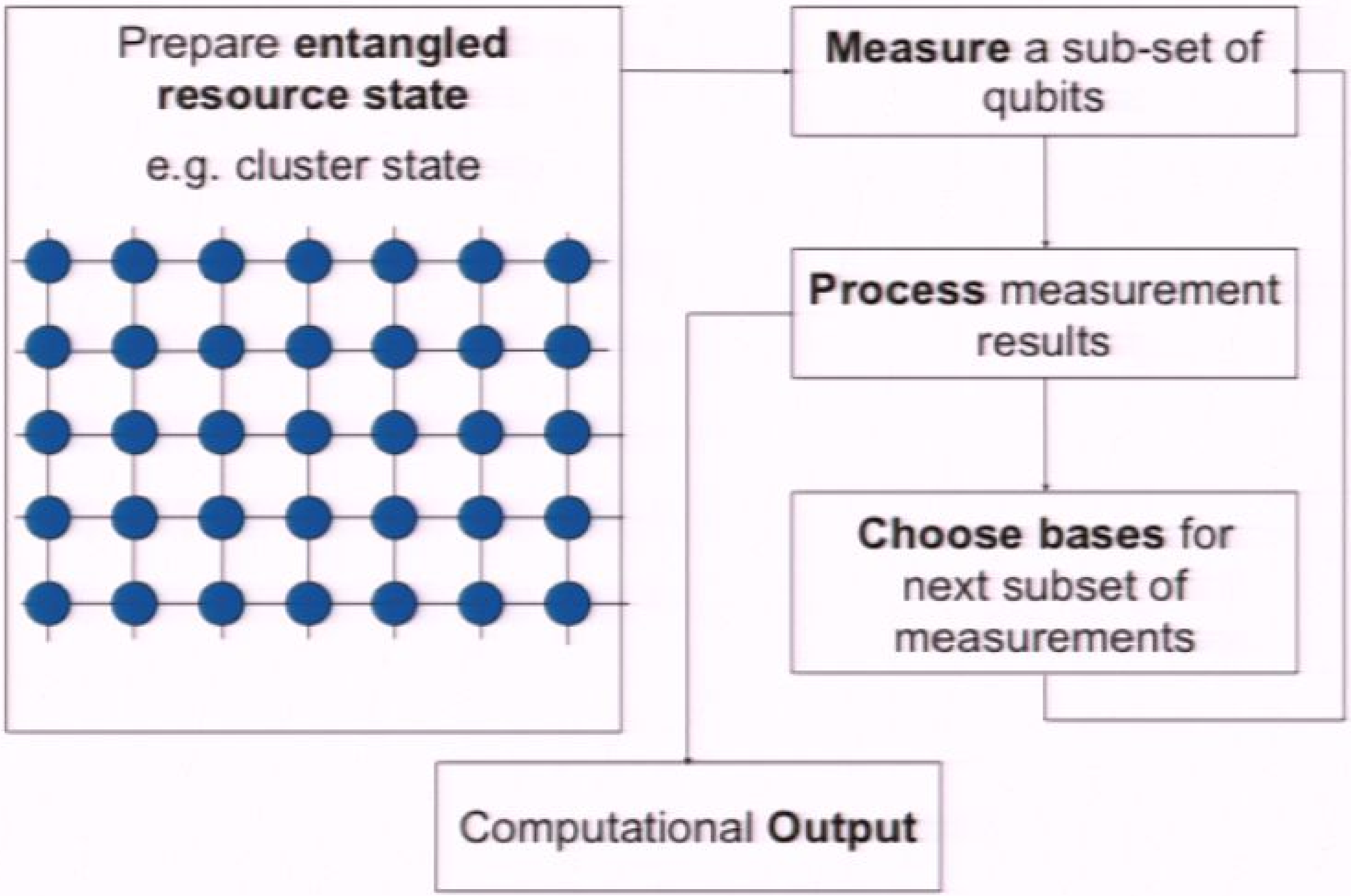
*Entanglement as a computational resource.*

**Resource state:**
Cluster State, Graph State etc.

**Single-qubit measurements**
(with classical processing, feedforward)

Desired state or computational **output**

# One-way Quantum Computation

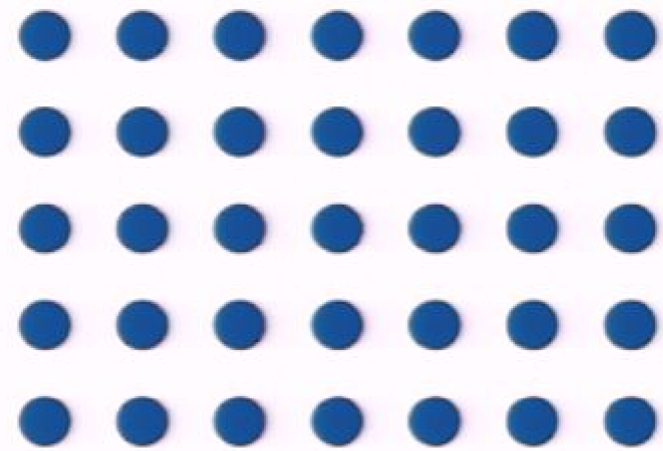



Raussendorf and Briegel, PRL 2001

# Cluster States

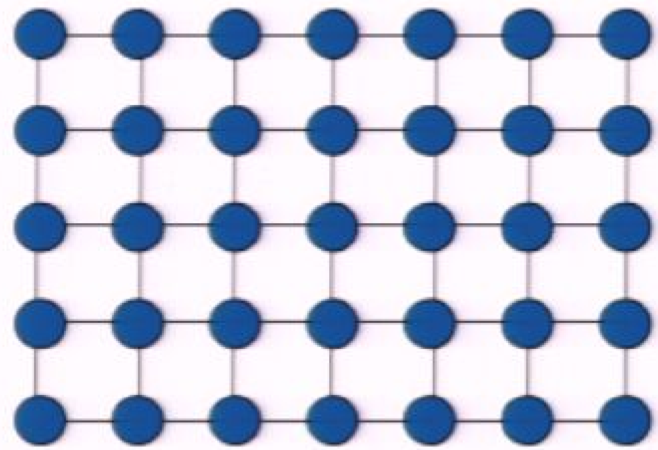
- Square lattice of qubits

- Each qubit prepared in state $|0\rangle + |1\rangle$.



# Cluster States

- Square lattice of qubits
- Each qubit prepared in state $|0\rangle + |1\rangle$.
- A controlled Z gate is applied between all neighbouring pairs.

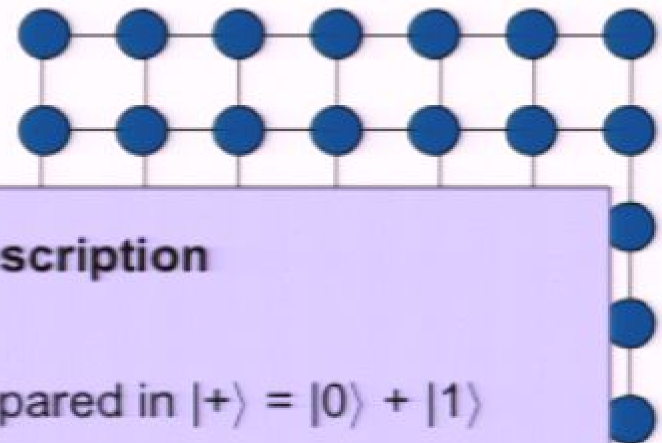


**Controlled-Z**
(CZ, CPHASE):

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

# Cluster States

- Square lattice of qubits



- Each qubit prepared in state

$|0\rangle +$

- A cont
betwe

**Controlle**
(CZ, CPH

Z

$$\begin{pmatrix} 1 & 0 & \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

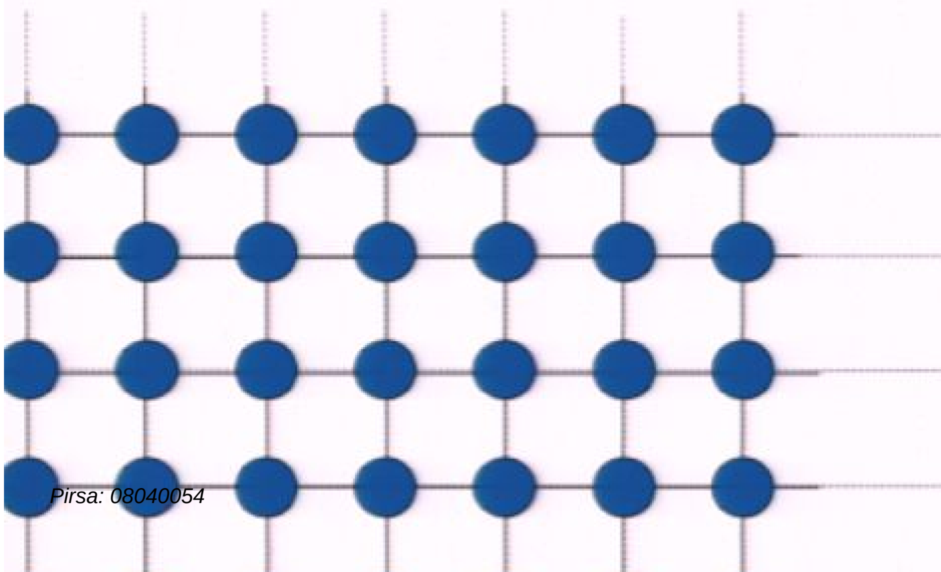
**The graphical state description**

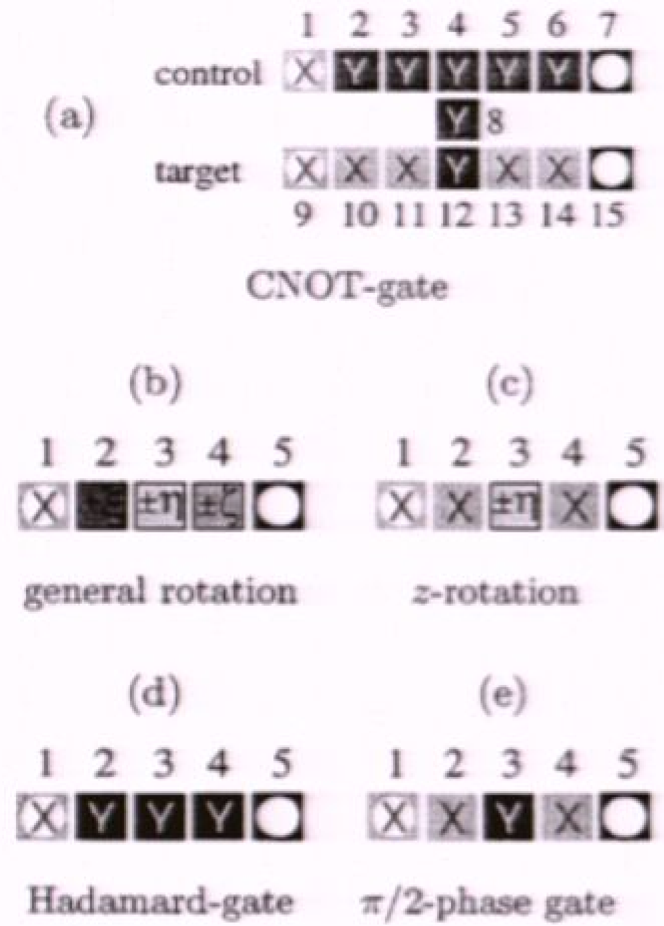
Node = Qubit – prepared in $|+\rangle = |0\rangle + |1\rangle$

Edge = Application of CZ gate between connected qubits

# Measurement Patterns

- The computation implemented is defined by the *measurement pattern.*
- Any quantum circuit can be efficiently achieved given suitable measurements.

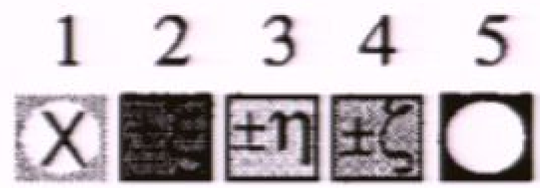





Raussendorf, Browne, Briegel, PRA 2003

# Measurement Patterns

- The computation implemented is defined by the *measurement pattern.*
- For each qubit
  - One of two bases:




$|0\rangle \pm e^{i\phi}|1\rangle$ or $|0\rangle \pm e^{-i\phi}|1\rangle$

general rotation

  - Angle predetermined
  - Sign a function of previous measurement outcomes
- Adaptivity ensures deterministic computation

# Universal Resource States

- Cluster states are not the only universal resources......

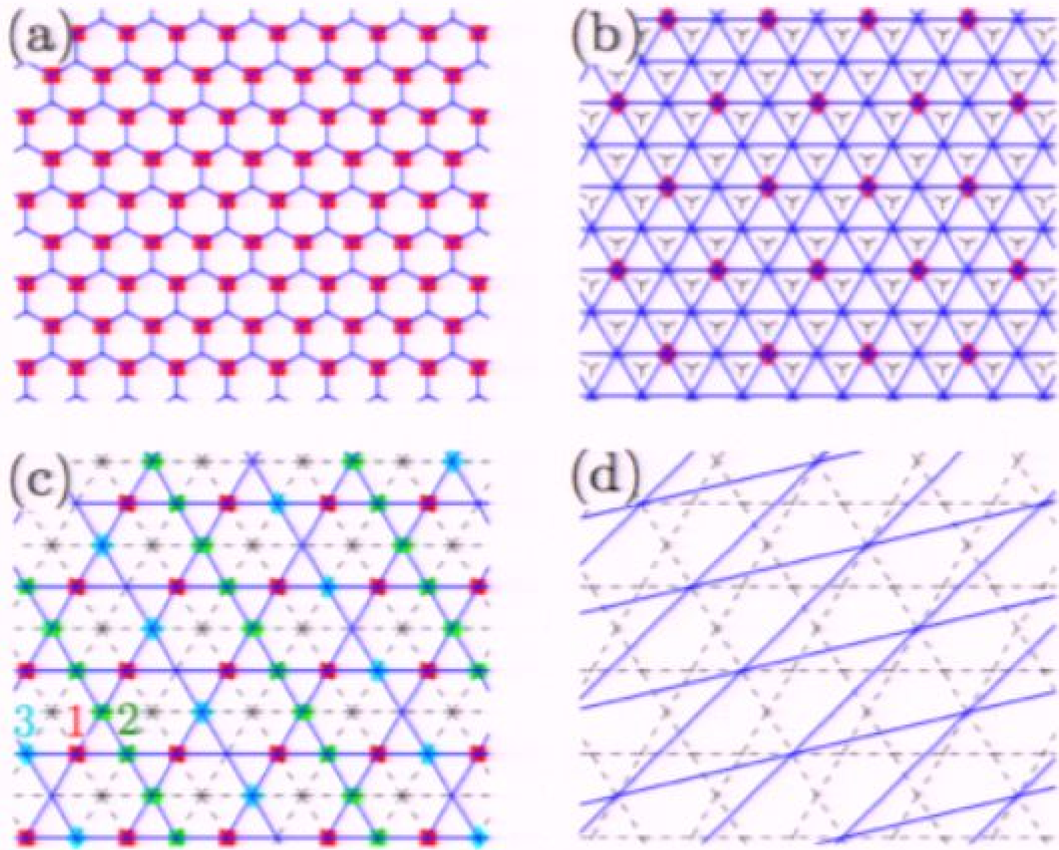
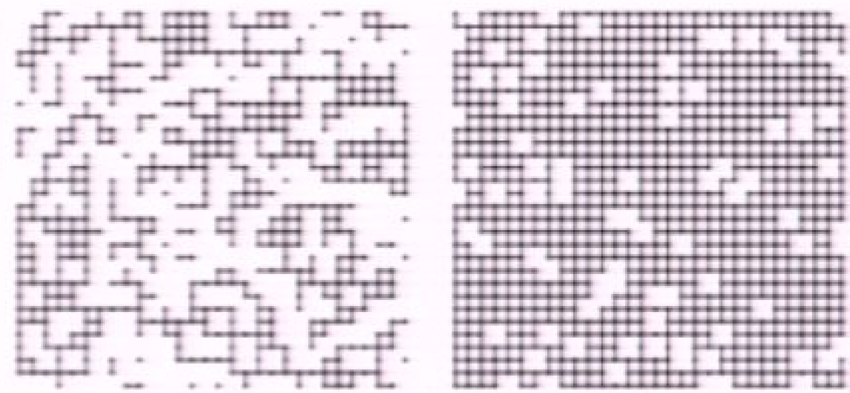



FIG. 1: Graph states corresponding to (a) hexagonal, (b) triangular and (c) Kagome lattices are universal for MQC.

M Van den Nest, A Miyake, W Dür, H Briegel, quant-ph/0604010

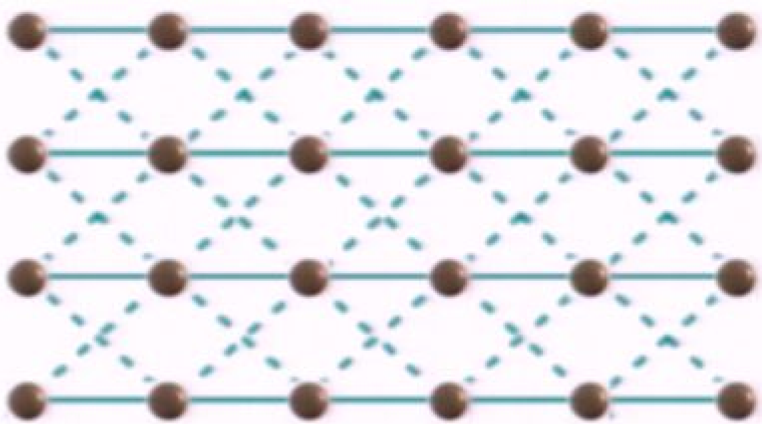


Percolation models above threshold

Kieling, Rudolph, Eisert, PRL 07; Browne, Elliot, Flammia, Miyake, Short, NJP 08

# Universal Resource States

- Computational Tensor Network states (CTN states)



D. Gross and J. Eisert, PRL 2007
D. Gross et al, PRA 07.

See talks by Jens Eisert and Katerina Mora

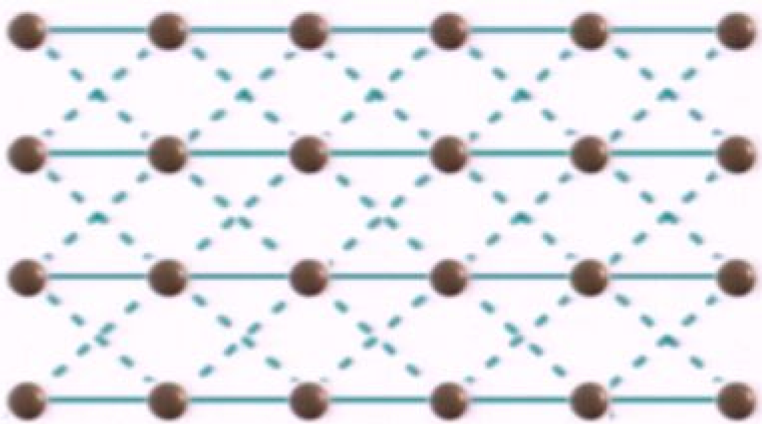
- Built upon Matrix Product State formalism
- Not (necessarily) graph states
- Different strategies to compensate for randomness

Robert's question:

*What is the essential quantum mechanical property that makes these states universal resources? Can it be quantified?*

# Universal Resource States

- Computational Tensor Network states (CTN states)



D. Gross and J. Eisert, PRL 2007
D. Gross et al, PRA 07.

See talks by Jens Eisert and Katerina Mora

- Built upon Matrix Product State formalism
- Not (necessarily) graph states
- Different strategies to compensate for randomness

Robert's question:

*What is the essential quantum mechanical property that makes these states universal resources? Can it be quantified?*

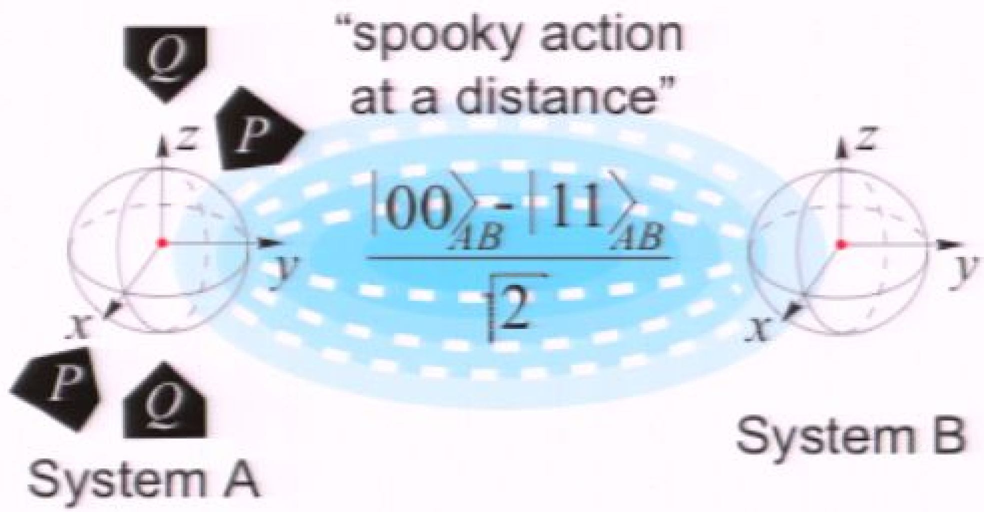
# EPR and Bell's theorem

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

**Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?**

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)




---

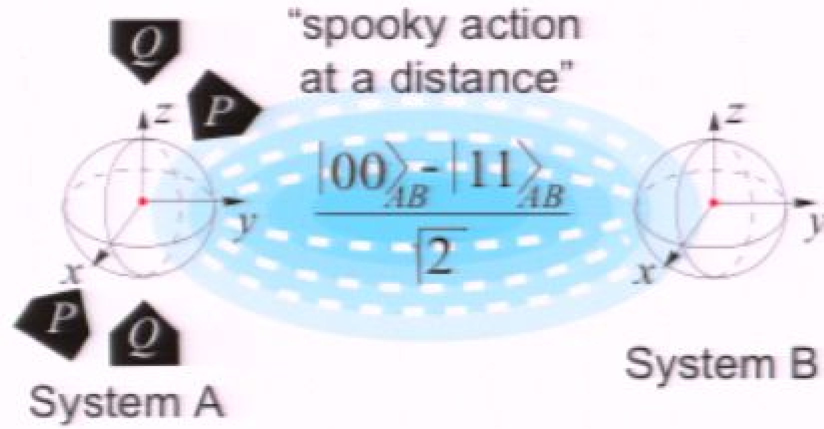
- EPR state $\Psi(x_A, x_B) = \int_{-\infty}^{\infty} e^{\frac{i}{\hbar}(x_A - x_B)p} dp \longrightarrow |\Psi\rangle = \frac{|00\rangle_{AB} - |11\rangle_{AB}}{\sqrt{2}}$ (Bohm).

# EPR and Bell's theorem

- CHSH correlation

$$C = |E_{00} + E_{10} + E_{01} - E_{11}|$$

$E_{ab}$ Expectation of the product of measurement outcomes $\pm 1$.




- Local hidden variable model: $C \leq 2$
- Violated by quantum mechanics up to Tsirolsen's bound: $C \leq 2\sqrt{2}$

# GHZ "paradox"

**Quantum mysteries revisited**

N. David Mermin
*Laboratory of Atomic and Solid State Physics, Cornell University, Ithaca, New York 14853-2501*

(Received 30 March 1990; accepted for publication 28 April 1990)

$$|\psi\rangle = |001\rangle + |110\rangle$$

(uniquely) satisfies:

$$X \otimes X \otimes X|\psi\rangle = |\psi\rangle$$
$$X \otimes Y \otimes Y|\psi\rangle = |\psi\rangle$$
$$Y \otimes X \otimes Y|\psi\rangle = |\psi\rangle$$

which also imply:

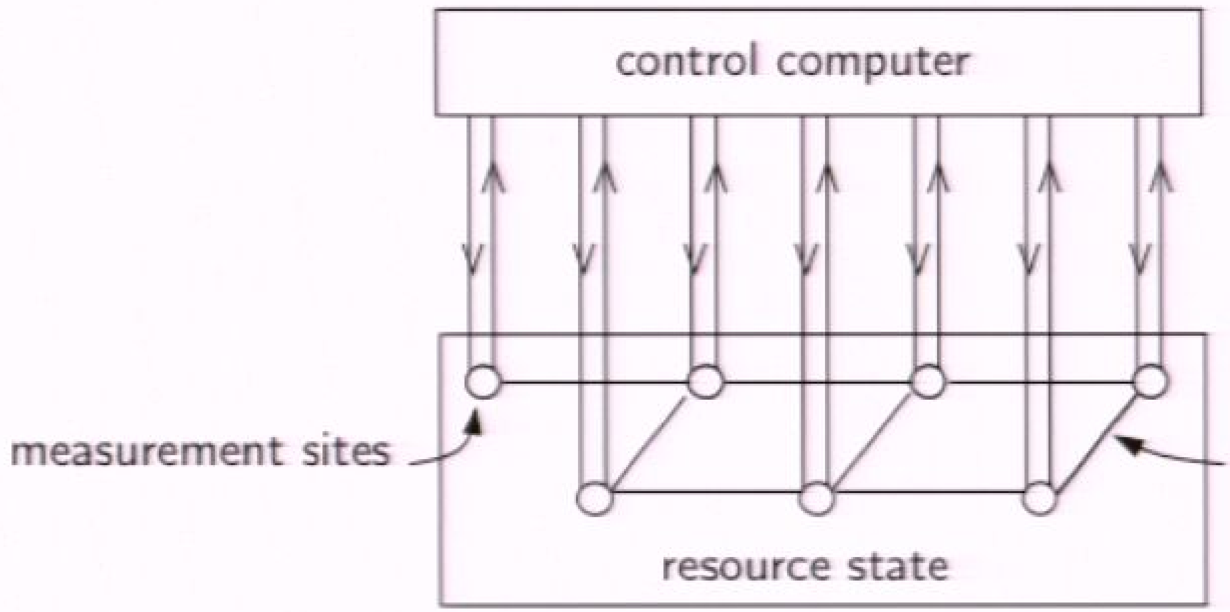
$$Y \otimes Y \otimes X|\psi\rangle = -|\psi\rangle$$

no classical assignment of *X*, *Y* can satisfy these.

# This talk

- Motivation
  - Better understand the necessary properties of entangled states which lead to computational resource power.
  - Understand the physics behind this.
- Tool
  - Focus on computational power of the classical computer controlling the adaptive measurements...

# The classical computer in charge....




- records measurement outcomes
- calculates the dependancy function for each qubit in turn
- is the *only* active computational element in the model.

# The control computer

- Just by exchanging messages with the measurement sites, its power is promoted

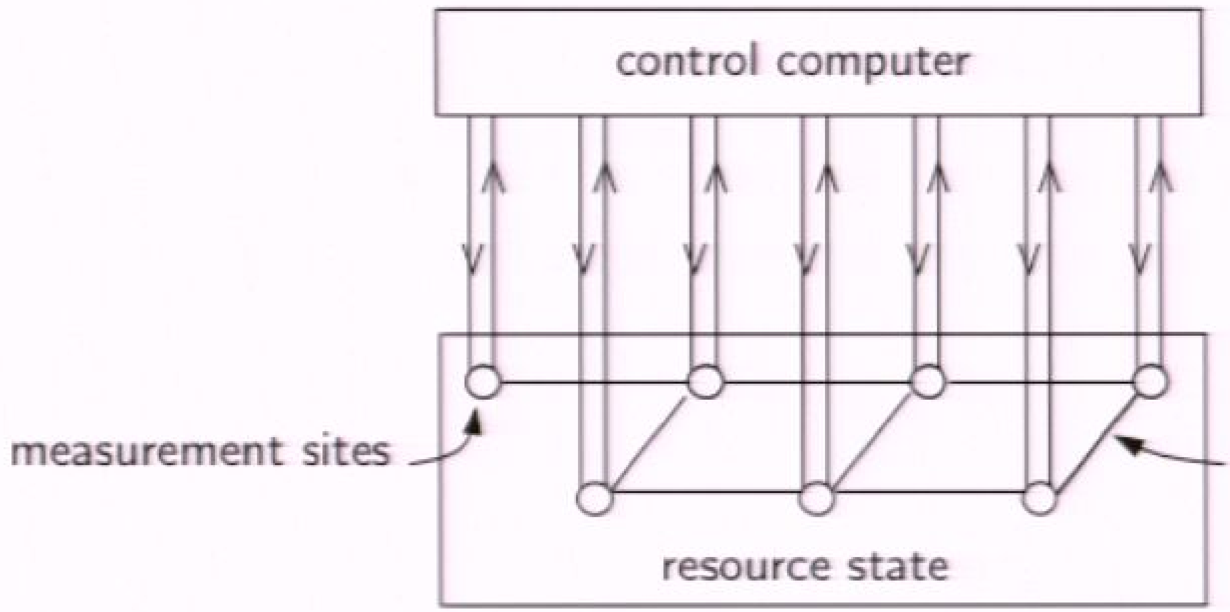
**P** — Power of a (polynomial) universal **classical** computer

↓ Exchange of bits with measurement devices on cluster state

**BQP** — Power of a (polynomial) universal **quantum** computer

- Interpretation: intrinsic computational power of the cluster state.

# The classical computer in charge....




- records measurement outcomes
- calculates the dependancy function for each qubit in turn
- is the *only* active computational element in the model.

# The control computer

- Just by exchanging messages with the measurement sites, its power is promoted

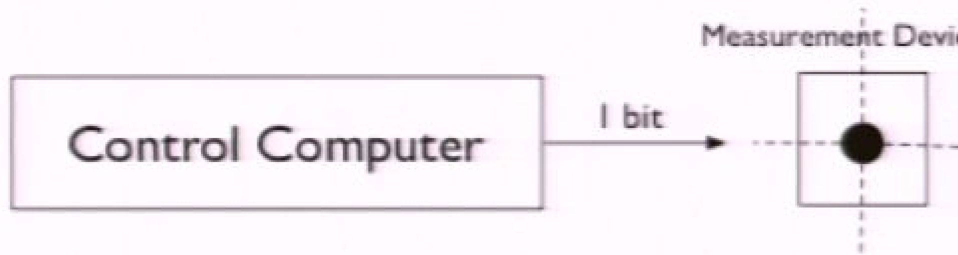
**P** — Power of a (polynomial) universal **classical** computer

↓ Exchange of bits with measurement devices on cluster state

**BQP** — Power of a (polynomial) universal **quantum** computer

- Interpretation: intrinsic computational power of the cluster state.

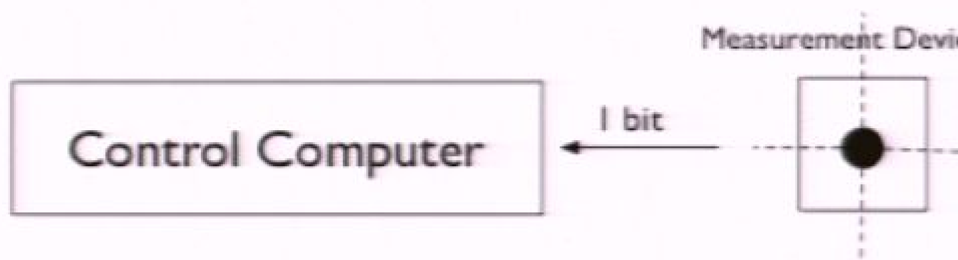
# Role of the control computer




$|0\rangle \pm e^{i\phi}|1\rangle$

$|0\rangle \pm e^{-i\phi}|1\rangle$

- Before each qubit is measured it must
  - Calculate sign of measurement basis
  - This is a function of previous measurement outcomes



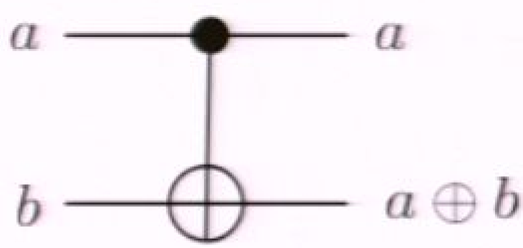

- The control computer receives measurement outcome and stores it in memory.

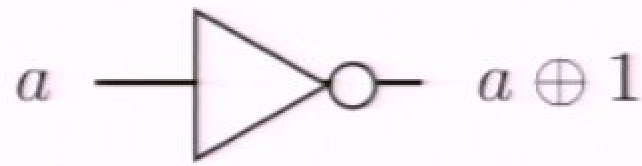
# Easy as parity

- **What do these dependency functions look like?**
  - The control computer has to keep track of all the measurement outcomes, and choose a sign for the measurement basis accordingly.
  - In cluster state MBQC, these functions reduce to calculating the **parity** of subsets of measured bits. $X^a X^b = X^{a \oplus b}$
- **Parity calculations do not require a universal classical computer.**

# Parity computer

- Consider a classical computer which can implements circuits of gates from {NOT, CNOT}.




- This is *not* a universal set.
- This is still a valid computational model and has an associated polynomial-time complexity class - "Parity L".

$\oplus$L

# Power of the CNOT computer

- Believed to be weaker than a universal classical computer (class P).

$\oplus L$

- There are problems which a CNOT computer *can* efficiently solve:
  - Parity of an *n*-bit string.
  - Simulating deterministic Clifford group circuits (CNOT, H, Pi/4 gates).
  - Matrix inversion over GF(2).

# Power of the CNOT computer

- Believed to be weaker than a universal classical computer (class P).

$\oplus$L

- There are problems which a CNOT computer *can* efficiently solve:
  - Parity of an *n*-bit string.
  - Simulating deterministic Clifford group circuits (CNOT, H, Pi/4 gates).
  - Matrix inversion over GF(2).

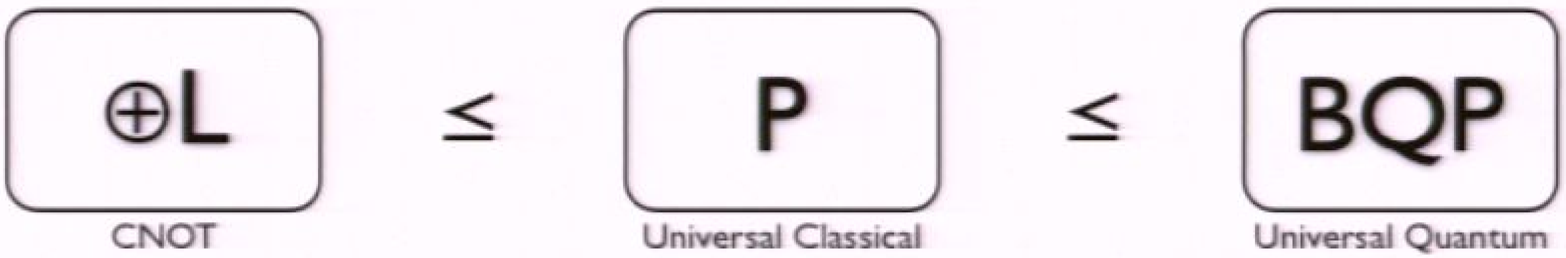
# Power of the CNOT computer

- Believed to be weaker than a universal classical computer (class P).

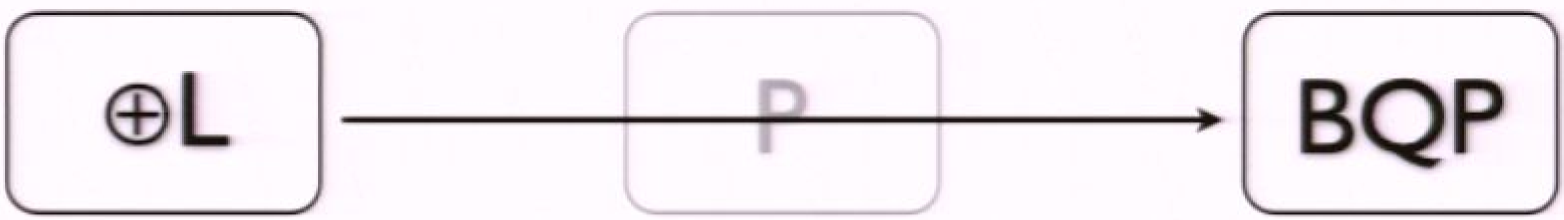
$\oplus L$

- There are problems which a CNOT computer *can* efficiently solve:
  - Parity of an *n*-bit string.
  - Simulating deterministic Clifford group circuits (CNOT, H, Pi/4 gates).
  - Control of adaptive measurements in measurement-based quantum computing.

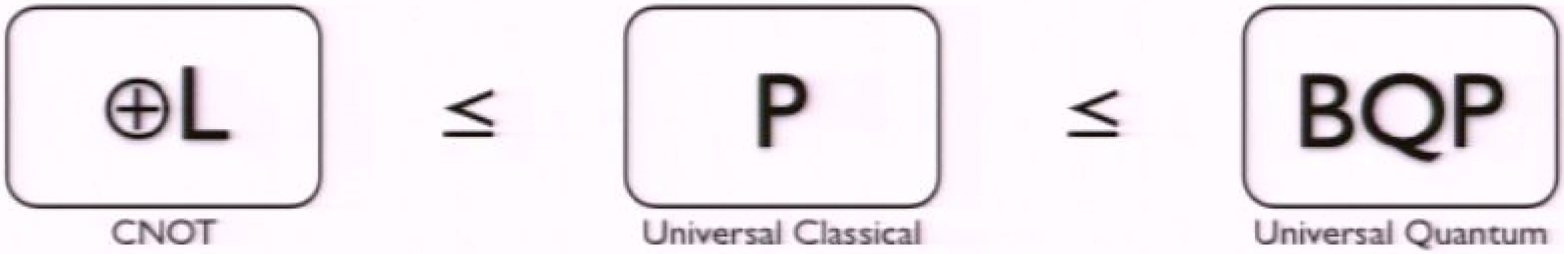
# Computational Resource Classes



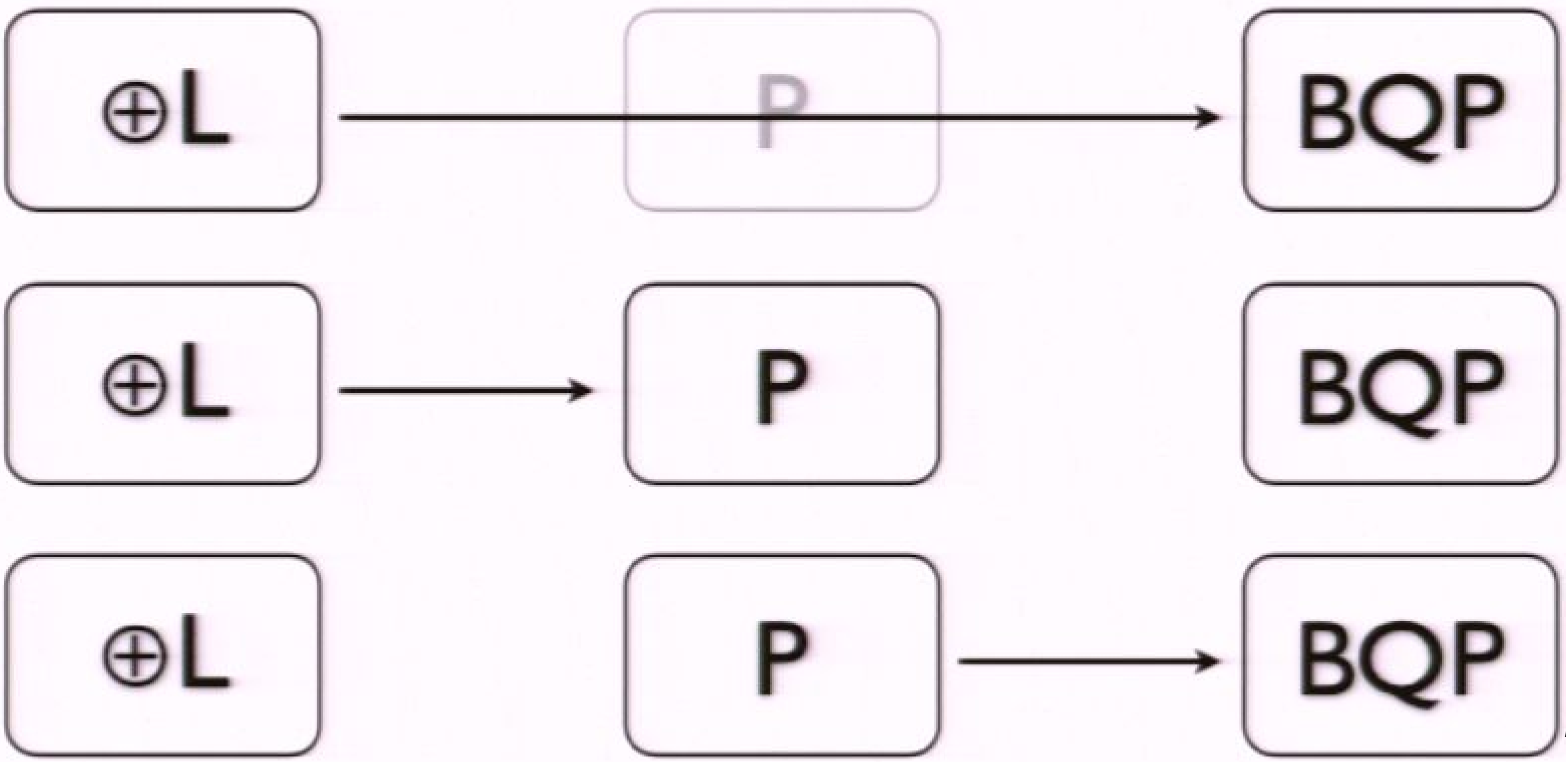

- The computational power of the cluster state is thus greater than previously described.



# Computational Resource Classes




- Three classes of computational resource



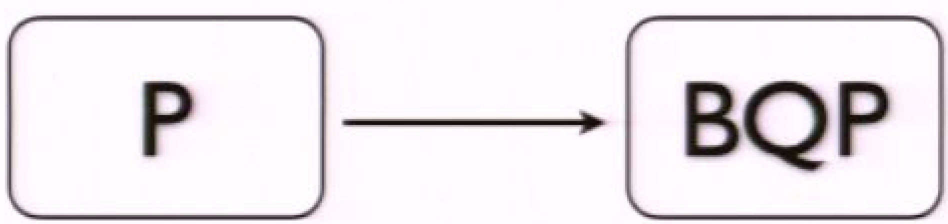
# Fast-forward to ~~Friday~~ Wednesday

PRL 98, 220503 (2007) PHYSICAL REVIEW LETTERS week ending 1 JUNE 2007

**Novel Schemes for Measurement-Based Quantum Computation**

D. Gross and J. Eisert
*Blackett Laboratory, Imperial College London, Prince Consort Road, London SW7 2BW, United Kingdom*
*Institute for Mathematical Sciences, Imperial College London, Exhibition Rd, London SW7 2BW, United Kingdom*
(Received 2 November 2006; revised manuscript received 29 January 2007; published 31 May 2007)

- In this paper, a new approach for MBQC is introduced with new states (CTN states).
- Instead of parity, the control computer in their model requires counting Mod(n).
- This requires a full universal classical computer.

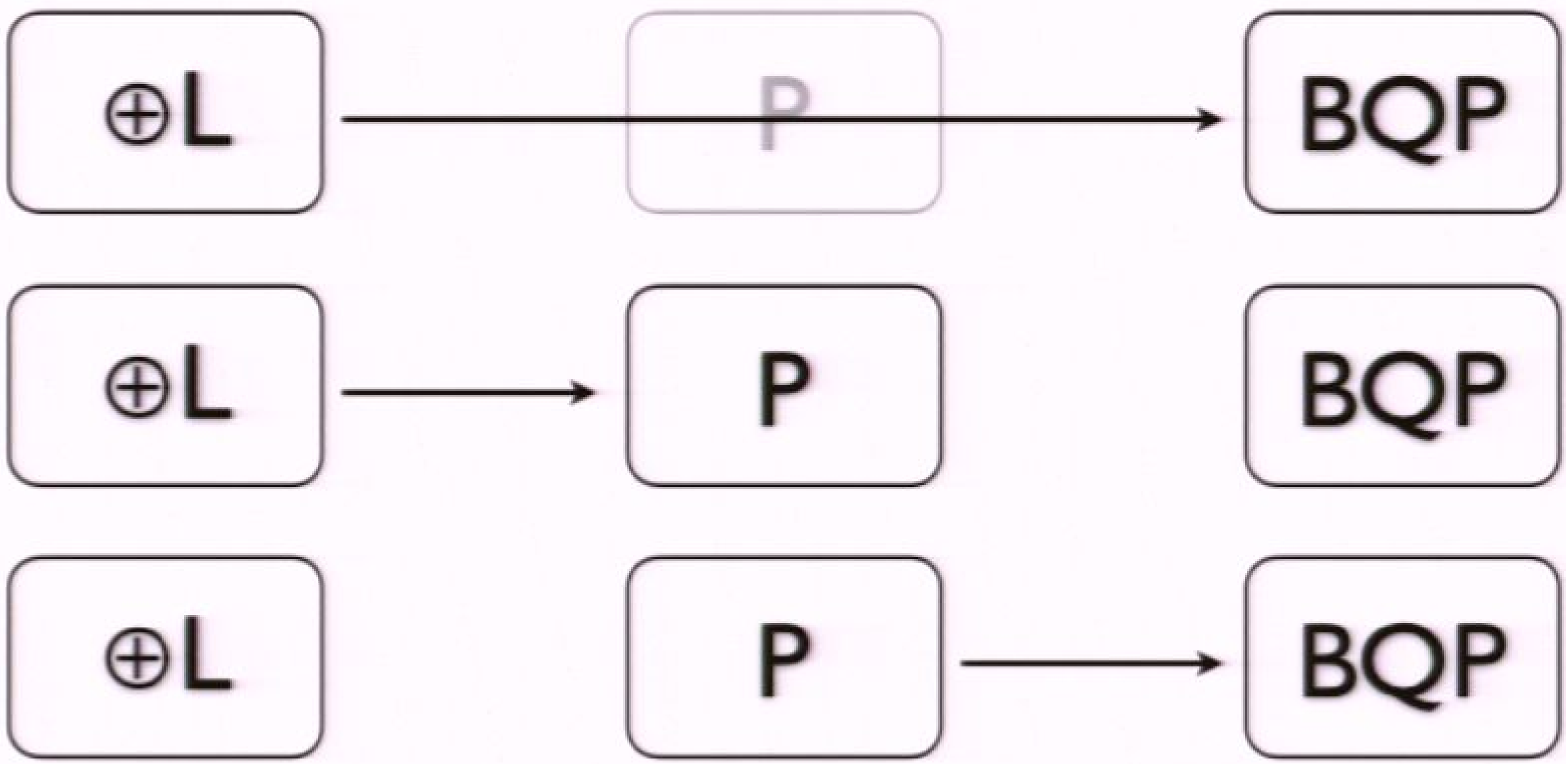


# Computational Resource Classes

$\oplus L \leq P \leq BQP$

CNOT — Universal Classical — Universal Quantum

- Three classes of computational resource



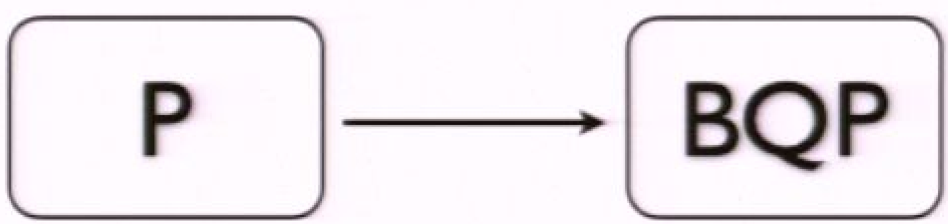
# Fast-forward to ~~Friday~~ Wednesday

PRL 98, 220503 (2007) PHYSICAL REVIEW LETTERS week ending 1 JUNE 2007

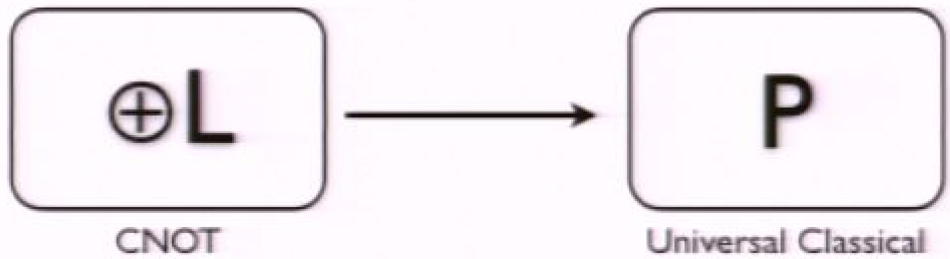
**Novel Schemes for Measurement-Based Quantum Computation**

D. Gross and J. Eisert
*Blackett Laboratory, Imperial College London, Prince Consort Road, London SW7 2BW, United Kingdom*
*Institute for Mathematical Sciences, Imperial College London, Exhibition Rd, London SW7 2BW, United Kingdom*
(Received 2 November 2006; revised manuscript received 29 January 2007; published 31 May 2007)

- In this paper, a new approach for MBQC is introduced with new states (CTN states).
- Instead of parity, the control computer in their model requires counting Mod(n).
- This requires a full universal classical computer.



# Measurement-Based Classical Computation

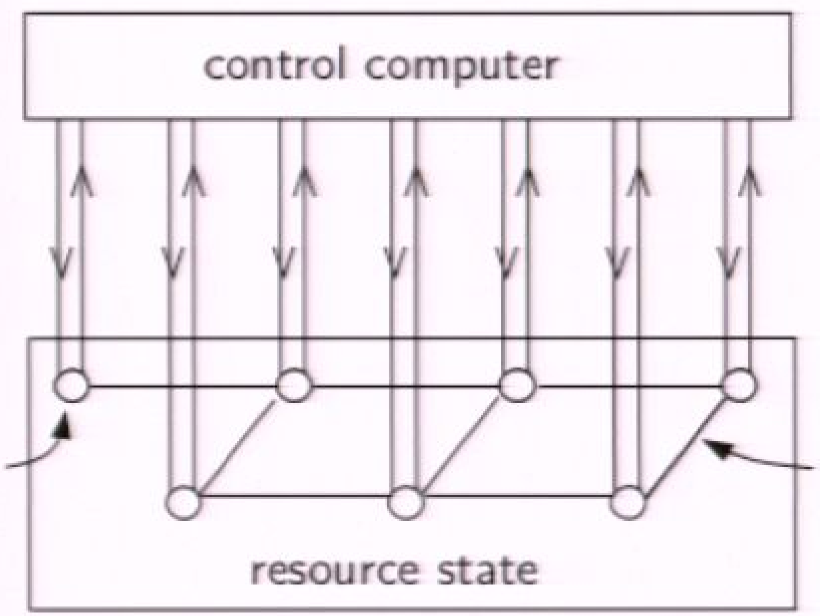



- This is measurement-based *classical* computation.
  - Universal classical computation is achieved by a non-universal machine with access to a resource state.
- What examples can we find of such a resource (which does not also enable universal quantum computation)?

# Enabling universal classical computation

- (Classical) Universal Gate Sets

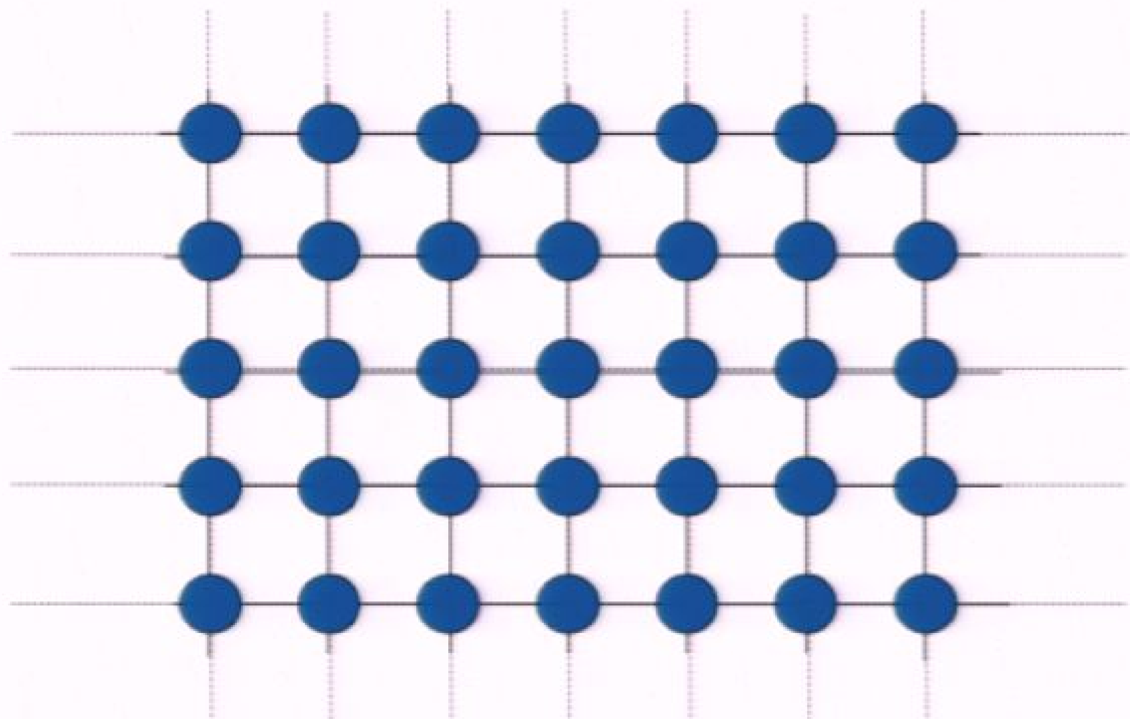
{NOT, CNOT} + AND / NAND / OR / TOFFOLI / etc.




- The ability to *repeatedly efficiently* simulate any one of these gates will enable universal classical computation.

# A simple example

- For universal quantum computation cluster states of unbounded size must be available.



$\oplus L \longrightarrow P$

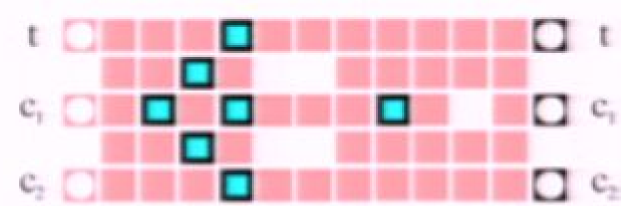
- Consider a supply of cluster states
  - big enough to support the measurement pattern of a **universal classical** gate
  - but no larger (not quantum universal)
- This will be a resource of class

$\oplus L$ $P$

but not

$\oplus L \longrightarrow BQP$

E.g. A Toffolli gate




Raussendorf, Browne, Briegel, PRA 2003



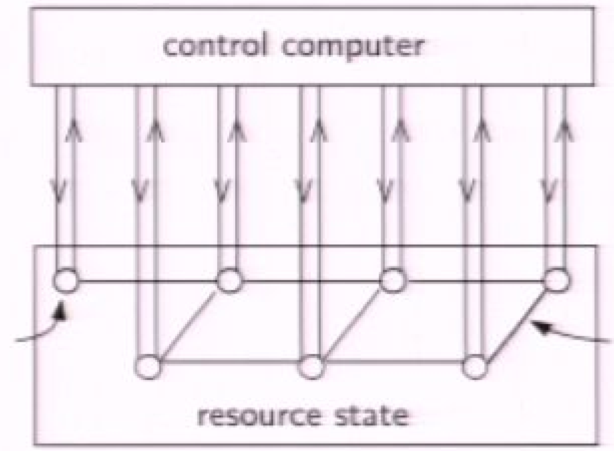
See also independent work by Blume-Kohout, Miyake, Leung (unpublished)

# Computational Resources from First Principles

- The bounded-size clusters are an example of a $\oplus L \rightarrow P$ resource, but what do they teach us?
- Is there a "simpler" resource which enables measurement based classical computation?
- Will this illuminate the necessary features of such a resource?
- Let's take a *first principles* approach...

# The model

- **We demand following properties of one-way model retained.**
  - Only **1bit** sent and **1bit** received at each site.
  - No signalling between sites.
  - Site may share entanglement, private correlations




- **Other than this, we make no restrictions on the properties of the sites.**

- The above restrictions avoid "trivial" solutions, i.e. hiding a NAND gate in a measurement site.

# Enabling universal classical computation

- Recall, to promote the power of our parity computer to full classical universality:

- We add a gate to the gate set

| | | |
|---|---|---|
| {NOT, CNOT} | + | AND<br>NAND<br>OR<br>TOFFOLI<br>etc. |

- The ability to *repeatedly efficiently* simulate any one of these gates will enable universal classical computation.

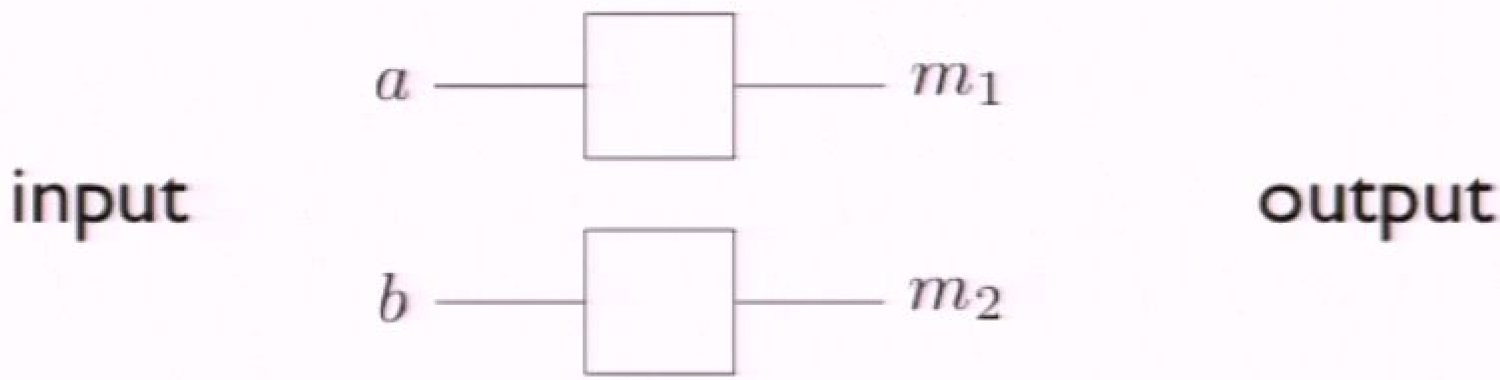
# AND from first principles

- AND: 2 bit inputs (a,b) → 1 bit output
- Restrictions of our framework lead to:


- Want $f(m_1, m_2) = a \text{ AND } b$
  - such that $f(m_1, m_2)$ can be evaluated by the parity computer

# AND from first principles

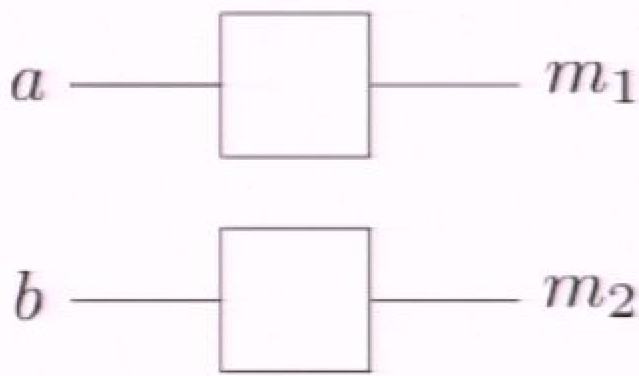
- AND: 2 bit inputs (a,b) → 1 bit output
- Restrictions of our framework lead to:




- Want $f(m_1, m_2) = a \text{ AND } b$
  - such that $f(m_1, m_2)$ can be evaluated by the parity computer
- No signalling implies $m_1 \oplus m_2 = a \text{ AND } b$

# AND from first principles

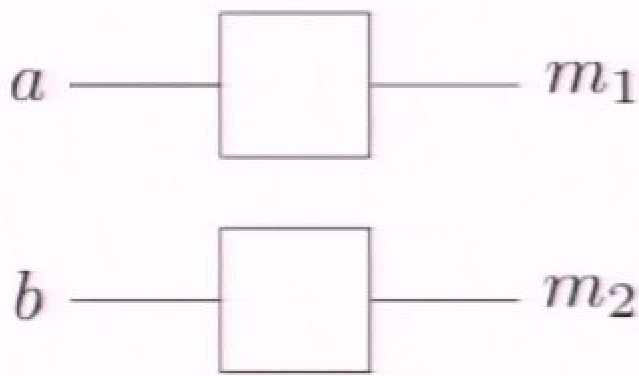
- To find our computational resource, need to find a state which delivers the correlations:




$$m_1 \oplus m_2 = a \text{ AND } b$$

# AND from first principles

- To find our computational resource, need to find a state which delivers the correlations:



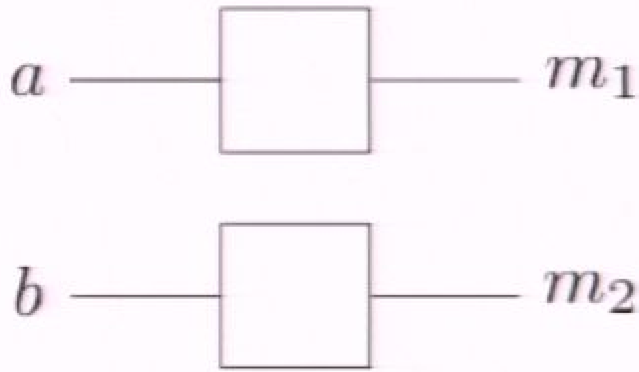

$$m_1 \oplus m_2 = a \text{ AND } b$$

- Sanity check: CHSH inequality

$$C = |E_{00} + E_{10} + E_{01} - E_{11}| = 4$$

# AND from first principles

- To find our computational resource, need to find a state which delivers the correlations:




$$m_1 \oplus m_2 = a \text{ AND } b$$

- Sanity check: CHSH inequality

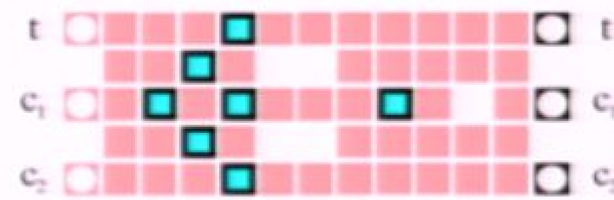
$$C = |E_{00} + E_{10} + E_{01} - E_{11}| = 4$$

- Tsirolsen's bound is violated...

- This is a Popescu-Rohrlich non-local box!

# Smallest AND resource?

- Know that:
  - Toffoli gate achievable with large-ish bounded size clusters




  - 2-bit resource forbidden (violates Tsirolsen's bound) $C > 2\sqrt{2}$

- What is smallest (fewest site) resource which enables AND?

# GHZ correlations revisited

$$X \otimes X \otimes X|\psi\rangle = |\psi\rangle$$
$$X \otimes Y \otimes Y|\psi\rangle = |\psi\rangle$$
$$Y \otimes X \otimes Y|\psi\rangle = |\psi\rangle$$
$$Y \otimes Y \otimes X|\psi\rangle = -|\psi\rangle$$

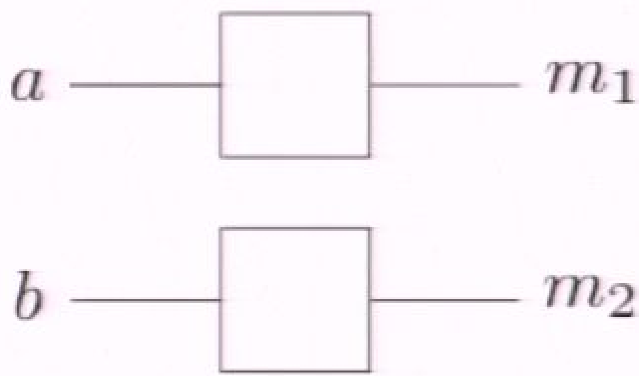
- Label the measurements $M_0 = X$ $M_1 = Y$
  - and rewrite equations in compact form

$$M_a \otimes M_b \otimes M_{a \oplus b}|\psi\rangle = (-1)^{a\,\mathrm{AND}\,b}|\psi\rangle \qquad \forall a, b \in \{0, 1\}$$

- If we associate measured eigenvalues ±1 with bit-values {0,1} we can write this.....

# AND from first principles

- To find our computational resource, need to find a state which delivers the correlations:




$$m_1 \oplus m_2 = a \text{ AND } b$$

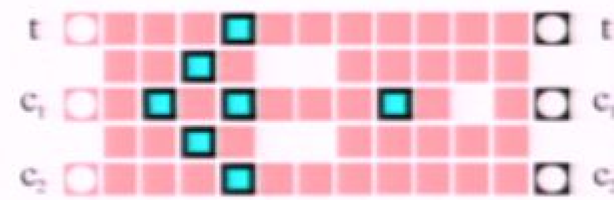
- Sanity check: CHSH inequality

$$C = |E_{00} + E_{10} + E_{01} - E_{11}| = 4$$

- Tsirolsen's bound is violated...
- This is a Popescu-Rohrlich non-local box!

# Smallest AND resource?

- Know that:
  - Toffoli gate achievable with large-ish bounded size clusters




  - 2-bit resource forbidden (violates Tsirolsen's bound) $C > 2\sqrt{2}$

- What is smallest (fewest site) resource which enables AND?

# GHZ correlations revisited

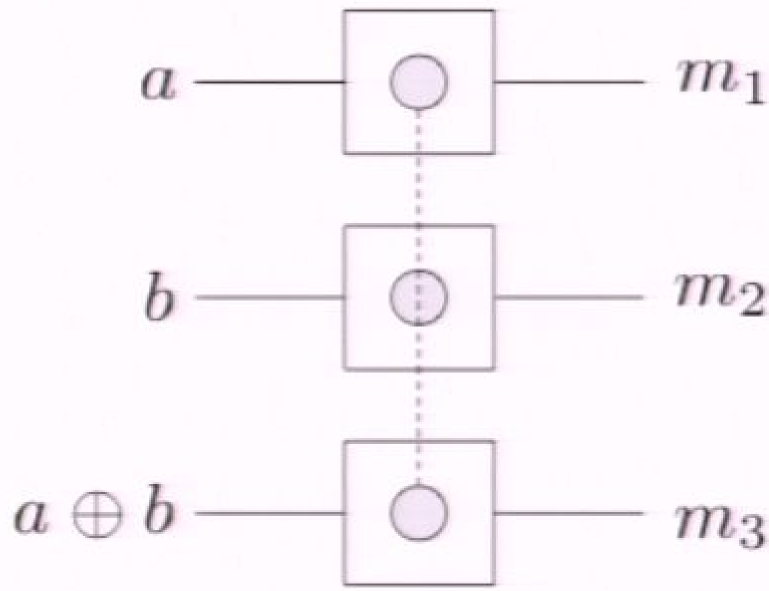
$$X \otimes X \otimes X|\psi\rangle = |\psi\rangle$$
$$X \otimes Y \otimes Y|\psi\rangle = |\psi\rangle$$
$$Y \otimes X \otimes Y|\psi\rangle = |\psi\rangle$$
$$Y \otimes Y \otimes X|\psi\rangle = -|\psi\rangle$$

- Label the measurements $M_0 = X \qquad M_1 = Y$
  - and rewrite equations in compact form

$$M_a \otimes M_b \otimes M_{a\oplus b}|\psi\rangle = (-1)^{a \,\mathrm{AND}\, b}|\psi\rangle \qquad \forall a, b \in \{0, 1\}$$

- If we associate measured eigenvalues ±1 with bit-values {0,1} we can write this.....

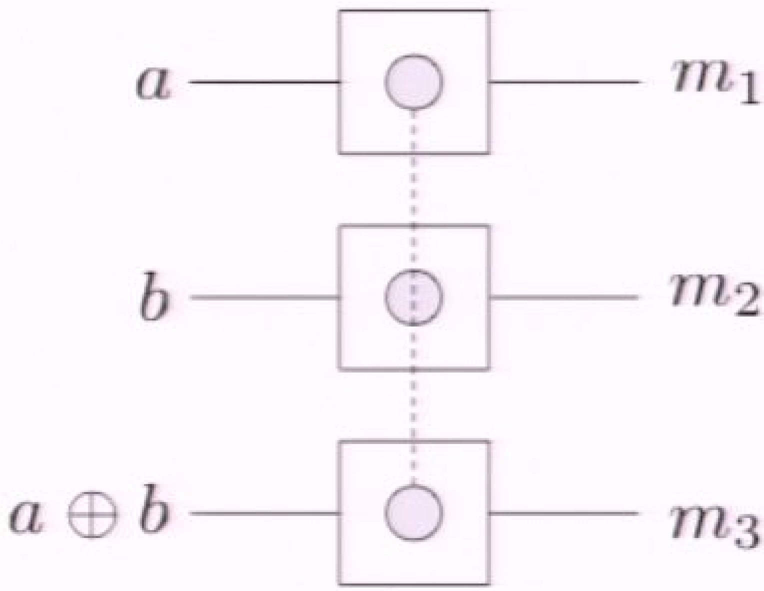
# GHZ correlations revisited




$$m_1 \oplus m_2 \oplus m_3 = a \text{ AND } b$$

- The correlations of Mermin-GHZ allow the parity computer to achieve the AND gate!
- It is the fewest site correlation which achieves this (within quantum physics).

# GHZ correlations revisited

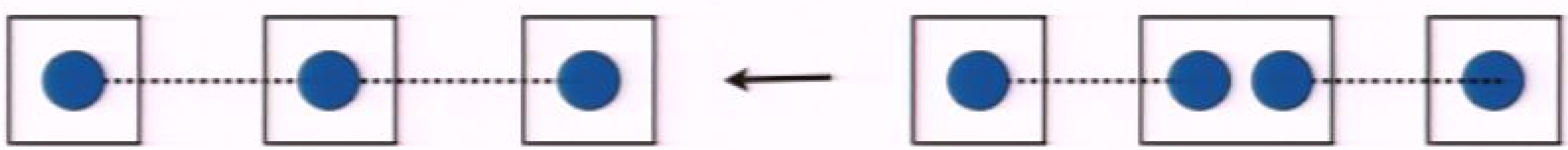



$$m_1 \oplus m_2 \oplus m_3 = a \text{ AND } b$$

- The correlations of Mermin-GHZ allow the parity computer to achieve the AND gate!
- It is the fewest site correlation which achieves this (within quantum physics).

# GHZ correlations revisited

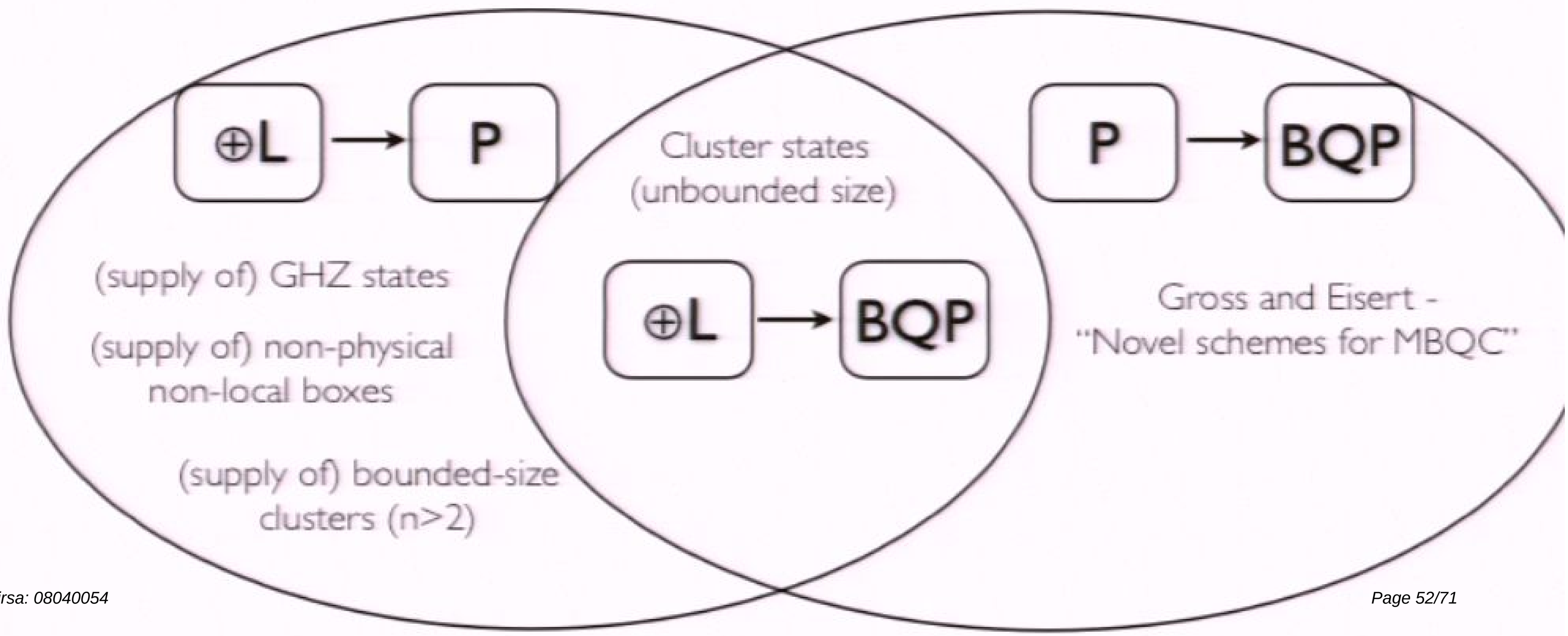
- The GHZ correlations are the fewest site resource for implementing AND.
- Why does nature allow three-qubit deterministic resource states but not two bit?
    - NB: bi-partite entanglement is all that's required.



- Can bi-partite entanglement be directly exploited?

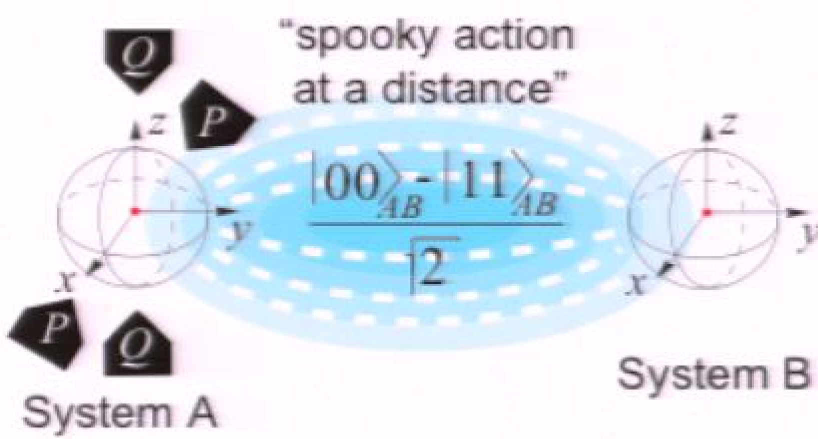
# Summary of results so far

- We have seen how the computational power of resource states for MBQC can be classified.



# Non-Deterministic Gates

- We have shown GHZ entanglement is the smallest entanglement resource for **deterministic** classically universal gate.
- What if non-deterministic gates are allowed?
- Can bi-partite entanglement be useful?



# Non-Deterministic Gates

- Re-write the CHSH quantity:

$$C = E_{00} + E_{10} + E_{01} - E_{11}$$

using: $E_{ab} = [p(m_1 \oplus m_2 = 0) - p(m_1 \oplus m_2 = 1)]_{ab}$

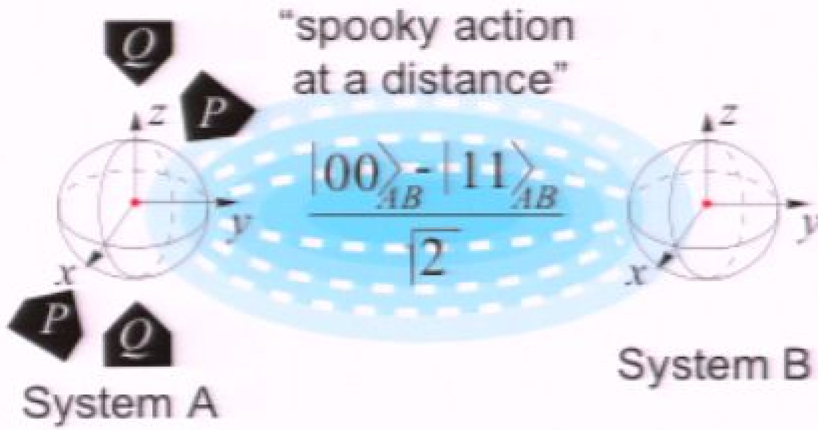
$$C = 8\frac{\sum_{a,b} p(m_1 \oplus m_2 = a \text{ AND } b)}{4} - 4$$

To give bounds on the mean success probability $\bar{p}$ of the AND gate.

| Classical (LHV) | Quantum (Tsirolsen) |
|---|---|
| $\bar{p} \leq 0.75$ | $\bar{p} \leq \frac{2+\sqrt{2}}{4} \approx 0.85$ |

# Non-Deterministic Gates

- Can the extra success probability available in the quantum case be computationally useful in our model?
- Can the CNOT computer error correct and lever this probability arbitrarily close to one?

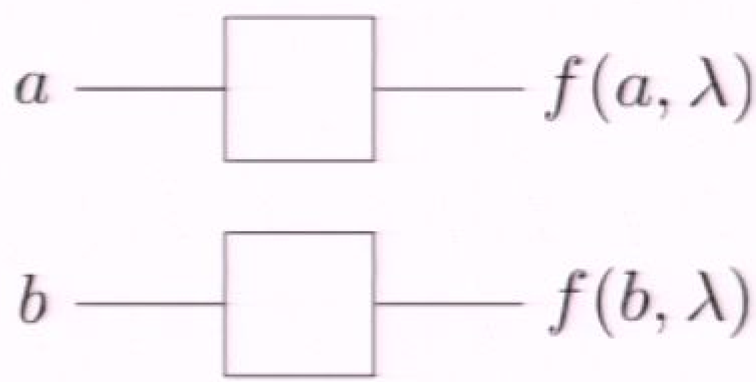



$$\frac{|00\rangle_{AB} - |11\rangle_{AB}}{\sqrt{2}}$$

- **This is an open question.**

# Separable states and classical randomness

- Can separable states be computationally useful?
  - Perhaps, but not much, no more than classical channels and randomness sources.....
- Signalling requirement means:




$\lambda$ :shared classical data

# Parallelizing power of generalised no-signalling theories?

- Write down correlations for any Boolean function

$$\bigoplus_{i=1}^{n} m_i = f(a, b, c, \ldots)$$

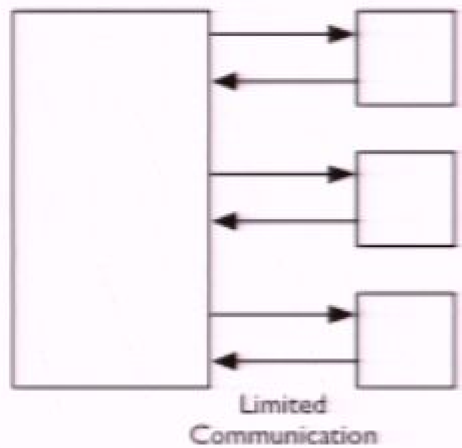
  - This is still a no-signalling resource.
  - The computational depth of the parity calculation is logarithmic.
- **Thus** (ignoring preparation complexity - this might be cheating)
  - **All n-bit functions can be evaluated in log n depth.**

# Aside: Interactive Proof systems

## Interactive Proof System

Verifier Provers

Limited computational power



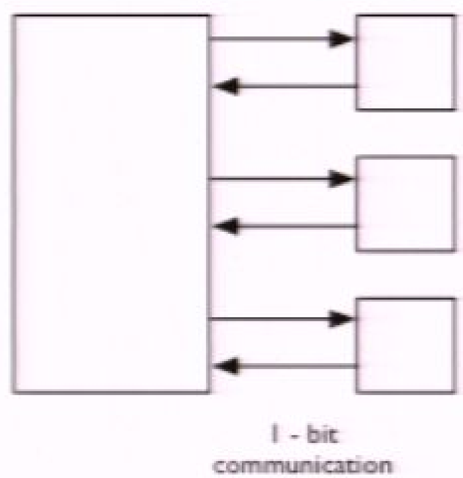

Unconstrained computational power

No inter-prover signalling

## Measurement-Based Computation

Control Measurement sites

Limited computational power




Unconstrained computational power

No inter-site signalling

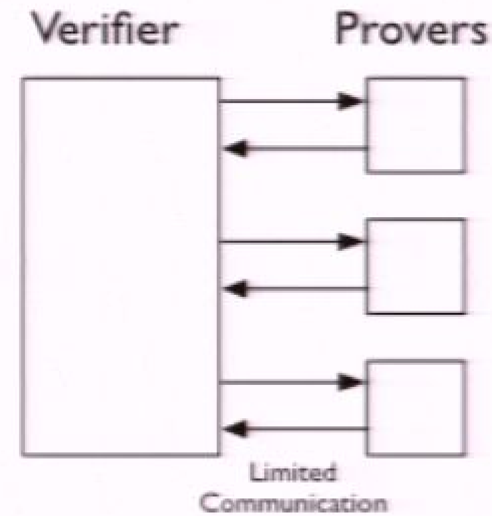
# Discussion

- **We have classified the computational power of resource states for MBQC.**
  - New classes of resource states for MB classical C.
- **Surprising connections between computer science, quantum computation and the study of quantum non-locality.**
  - A new (and unified) way of formulating GHZ, and CHSH "paradoxes".
  - New language, meaning for "pseudo-telepathy games"

# Aside: Interactive Proof systems

## Interactive Proof System

Limited computational power

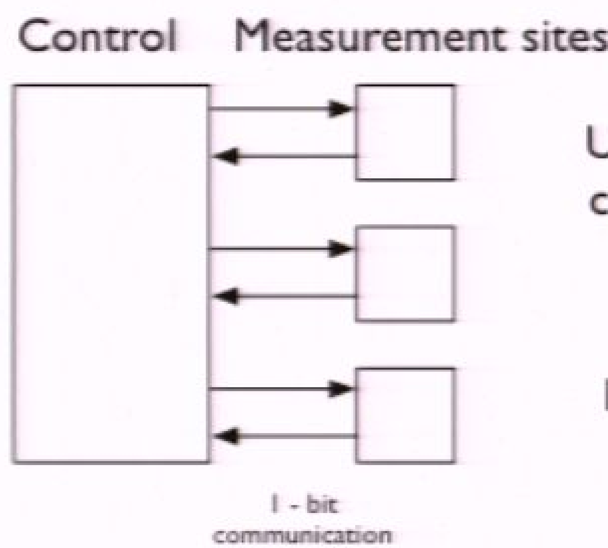



Unconstrained computational power

No inter-prover signalling

## Measurement-Based Computation

Limited computational power




Unconstrained computational power

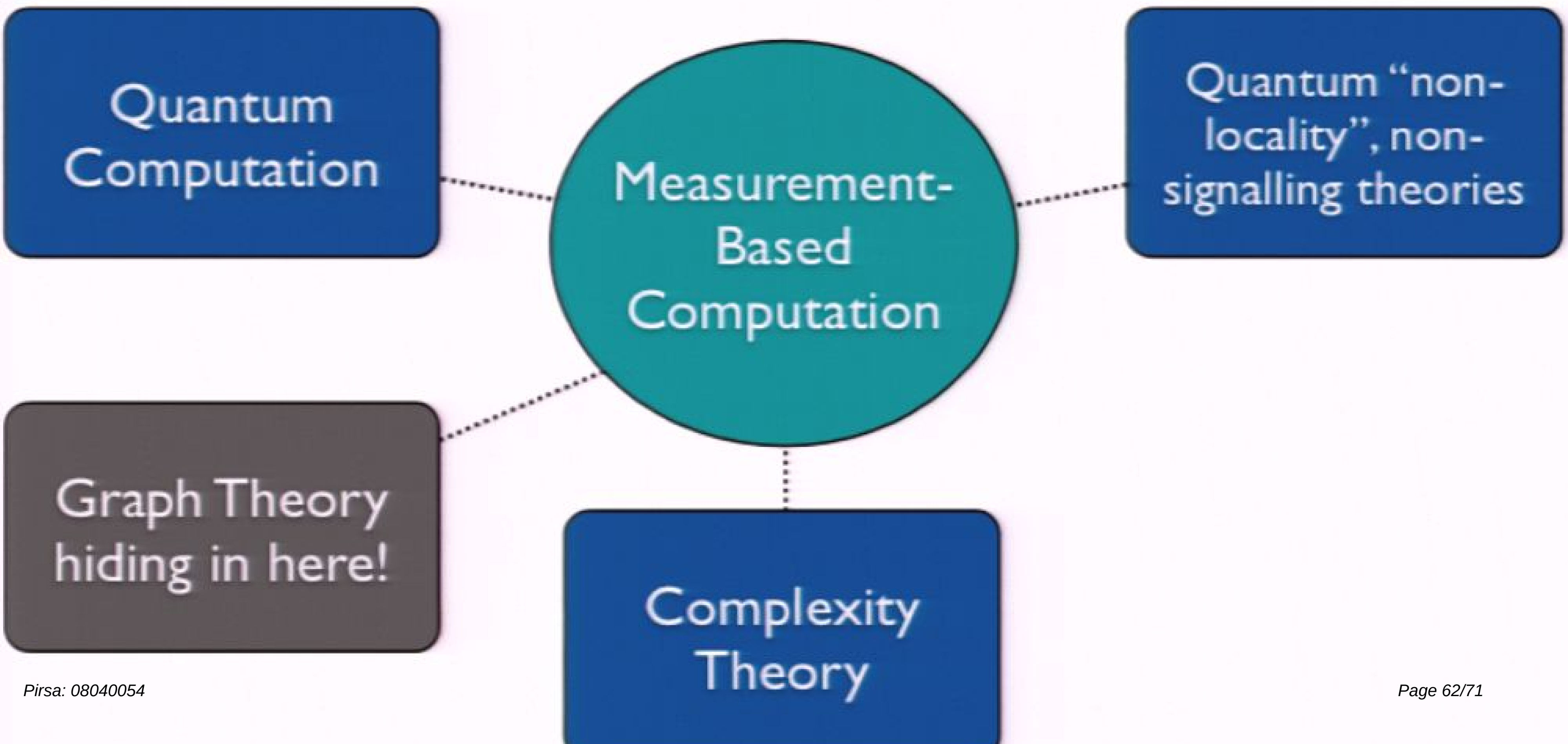
No inter-site signalling

# Discussion

- **We have classified the computational power of resource states for MBQC.**
  - New classes of resource states for MB classical C.
- **Surprising connections between computer science, quantum computation and the study of quantum non-locality.**
  - A new (and unified) way of formulating GHZ, and CHSH "paradoxes".
  - New language, meaning for "pseudo-telepathy games"

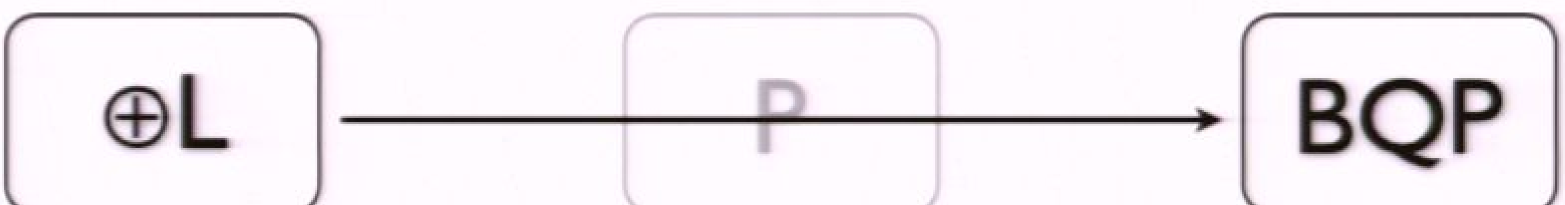
# Outlook

- In what new ways can these connections be exploited?



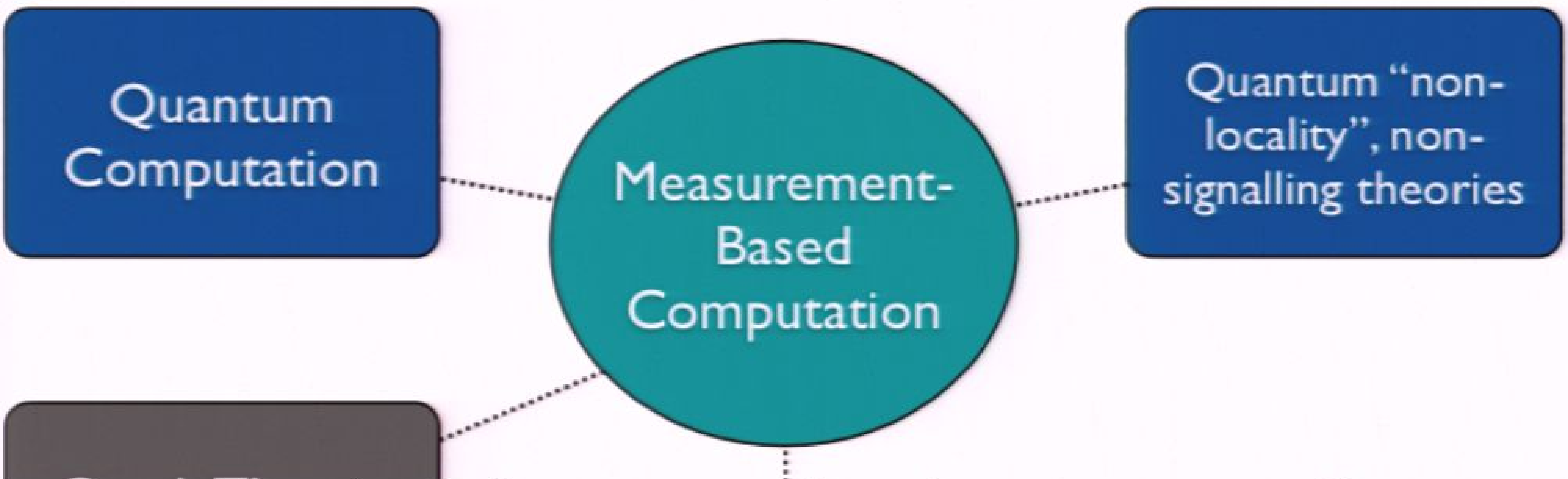
# Acknowledgements and reference


- **Joint work with Janet Anders (UCL)**
- Funded by **QIPIRC**
  - **Reference:** J. Anders and D. E. Browne (in preparation)
- Thanks to: Hans Briegel, Robin Blume-Kohout, Akimasa Miyake, Joe Fitzsimons, Debbie Leung, Howard Wiseman, Elham Kashefi, Simon Perdrix, Barry Sanders

# Outlook

- In what new ways can these connections be exploited?




GHZ, and CHSH "paradoxes".

- New language, meaning for "pseudo-telepathy games"

# Non-Deterministic Gates

- Re-write the CHSH quantity:

$$C = E_{00} + E_{10} + E_{01} - E_{11}$$

using: $E_{ab} = [p(m_1 \oplus m_2 = 0) - p(m_1 \oplus m_2 = 1)]_{ab}$

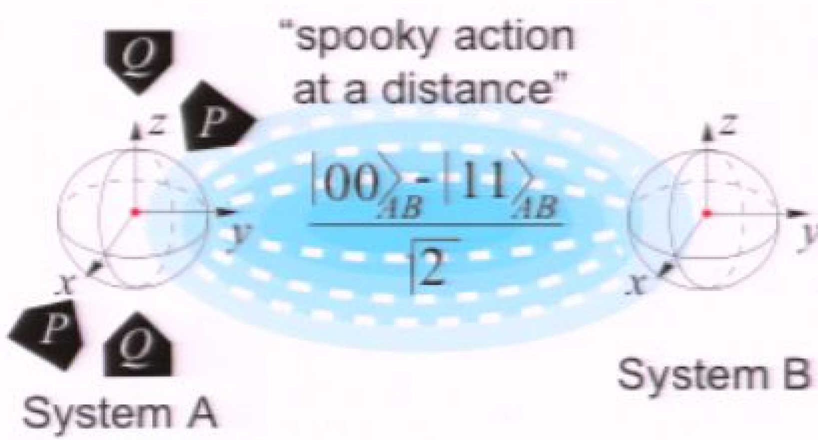
$$C = 8\frac{\sum_{a,b} p(m_1 \oplus m_2 = a \text{ AND } b)}{4} - 4$$

To give bounds on the mean success probability $\bar{p}$ of the AND gate.

| Classical (LHV) | Quantum (Tsirolsen) |
| --- | --- |
| $\bar{p} \leq 0.75$ | $\bar{p} \leq \frac{2+\sqrt{2}}{4} \approx 0.85$ |

# Non-Deterministic Gates

- Can the extra success probability available in the quantum case be computationally useful in our model?
- Can the CNOT computer error correct and lever this probability arbitrarily close to one?




- **This is an open question.**

# Non-Deterministic Gates

- Re-write the CHSH quantity:

$$C = E_{00} + E_{10} + E_{01} - E_{11}$$

using: $E_{ab} = [p(m_1 \oplus m_2 = 0) - p(m_1 \oplus m_2 = 1)]_{ab}$

$$C = 8\frac{\sum_{a,b} p(m_1 \oplus m_2 = a \text{ AND } b)}{4} - 4$$

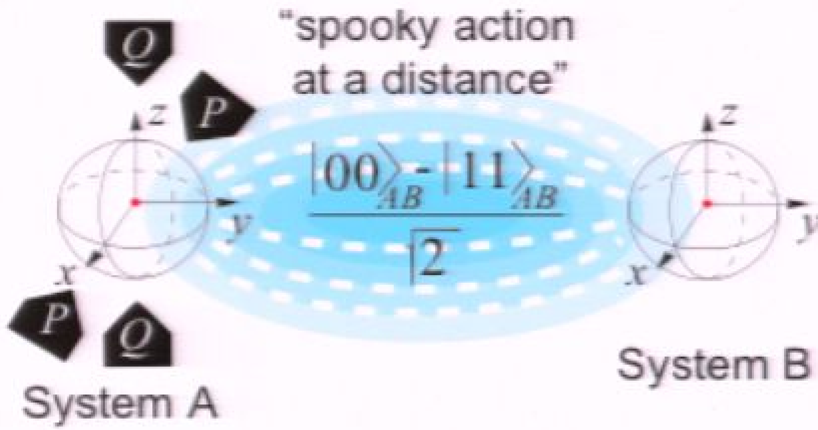
To give bounds on the mean success probability $\bar{p}$ of the AND gate.

| Classical (LHV) | Quantum (Tsirolsen) |
| --- | --- |
| $\bar{p} \leq 0.75$ | $\bar{p} \leq \frac{2+\sqrt{2}}{4} \approx 0.85$ |

# Non-Deterministic Gates

- Can the extra success probability available in the quantum case be computationally useful in our model?

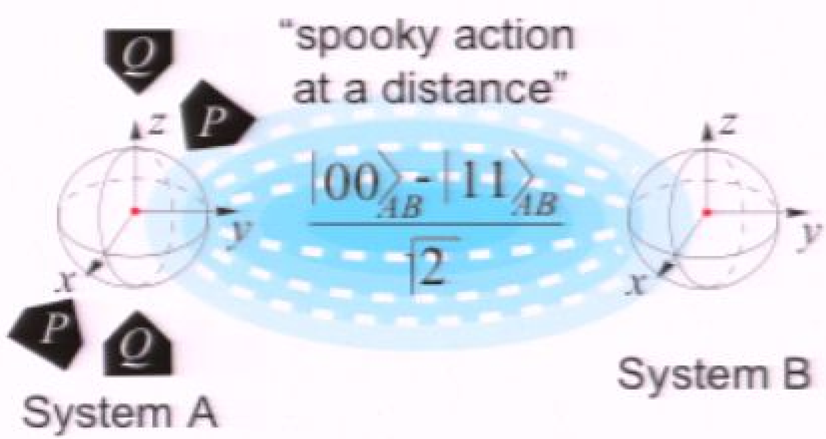
- Can the CNOT computer error correct and lever this probability arbitrarily close to one?




- **This is an open question.**

# Non-Deterministic Gates

- We have shown GHZ entanglement is the smallest entanglement resource for **deterministic** classically universal gate.
- What if non-deterministic gates are allowed?
- Can bi-partite entanglement be useful?



# Enabling universal classical computation

- Recall, to promote the power of our parity computer to full classical universality:

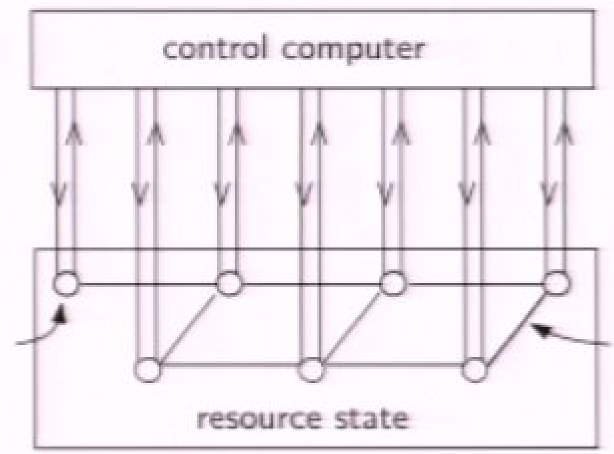
- We add a gate to the gate set

{NOT, CNOT} + AND / NAND / OR / TOFFOLI / etc.

- The ability to *repeatedly efficiently* simulate any one of these gates will enable universal classical computation.

# The model

- **We demand following properties of one-way model retained.**
  - Only **1bit** sent and **1bit** received at each site.
  - No signalling between sites.
  - Site may share entanglement, private correlations




- **Other than this, we make no restrictions on the properties of the sites.**

- The above restrictions avoid "trivial" solutions, i.e. hiding a NAND gate in a measurement site.