Title: Maximal noncontextuality; and qubit contextuality as a resource for Quantum Computation

Date: Jul 27, 2017 04:30 PM

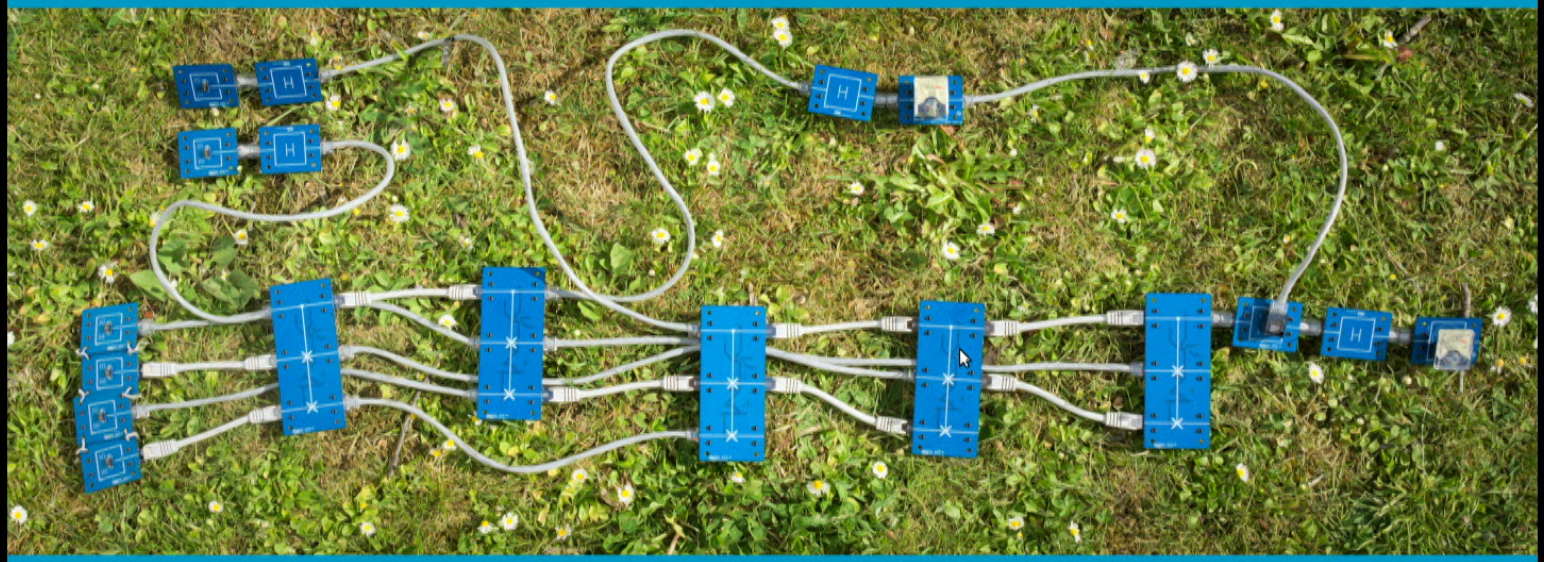
URL: http://pirsa.org/17070055

Abstract:

Maximal noncontextuality; and qubit contextuality as a resource for Quantum Computation

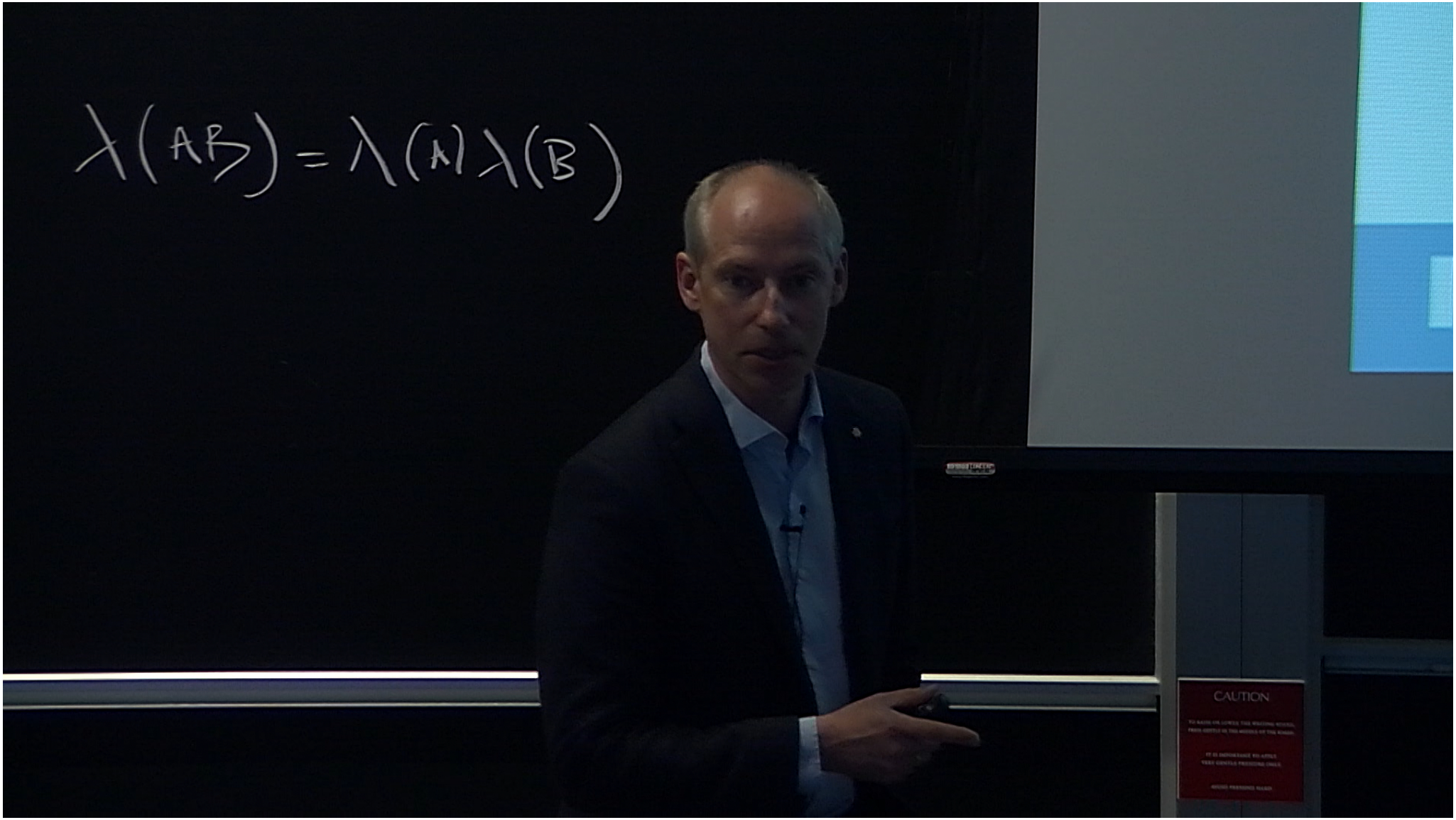
Jan-Åke Larsson
Linköping University, Linköping, Sweden

joint work with E. Dzhafarov, J. Kujala; O. Gühne, M. Kleinmann, J. R. Portillo, C. Budroni, A. Cabello; and N. Johansson, P. Harrysson



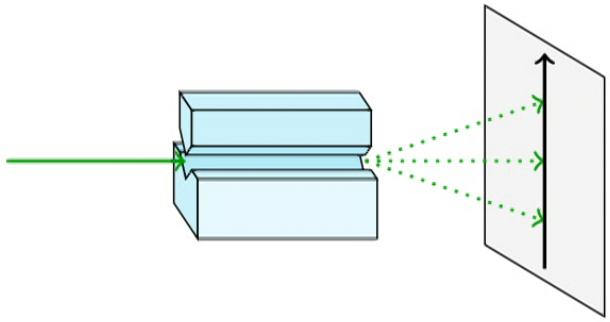
LINKÖPING UNIVERSITY

FQXi FOUNDATIONAL QUESTIONS INSTITUTE


λ(AB) = λ(A)λ(B)
CAUTION

Noncontextuality: outcome is independent of choice of compatible measurements

Spin measurement is measurement of magnetic dipole moment along a specified axis



Simultaneous spin measurement along several axes is not possible

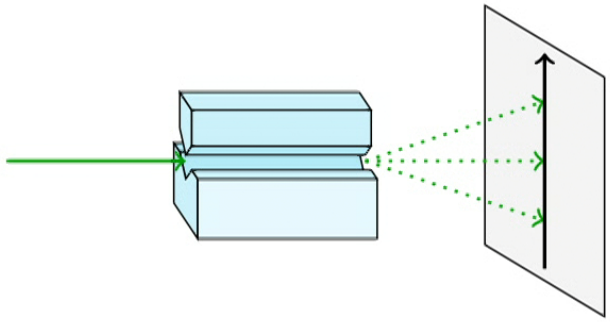
$$s_x = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},\ s_y = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & i & 0 \\ -i & 0 & i \\ 0 & -i & 0 \end{pmatrix},\ s_z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

But the spin-squared operators commute

$$s_x^2 = \frac{1}{2}\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix},\ s_y^2 = \frac{1}{2}\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 1 \end{pmatrix},\ s_z^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Noncontextuality: outcome is independent of choice of compatible measurements

Spin measurement is measurement of magnetic dipole moment along a specified axis



Simultaneous spin measurement along several axes is not possible

$$s_x = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},\ s_y = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & i & 0 \\ -i & 0 & i \\ 0 & -i & 0 \end{pmatrix},\ s_z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

But the spin-squared operators commute

$$s_x^2 = \frac{1}{2}\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix},\ s_y^2 = \frac{1}{2}\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 1 \end{pmatrix},\ s_z^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Noncontextuality: outcome is independent of choice of compatible measurements

The spin-squared operators can be simultaneously measured

$$s_x^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; s_y^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; s_z^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

This measurement answers the question: which direction has zero spin components?

This corresponds to a measurement of magnetic quadrupole moment, but that needs three directions as parameters, and the corresponding measurement operator is actually

$$\begin{pmatrix} \text{“}y\text{”} & 0 & 0 \\ 0 & \text{“}z\text{”} & 0 \\ 0 & 0 & \text{“}x\text{”} \end{pmatrix}$$

This is a single operator, that changes with the direction choices. Why would we expect a noncontextual model to work at all?

Noncontextuality: outcome is independent of choice of compatible measurements

The spin-squared operators can be simultaneously measured

$$s_x^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; s_y^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; s_z^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

This measurement answers the question: which direction has zero spin components?

This corresponds to a measurement of magnetic quadrupole moment, but that needs three directions as parameters, and the corresponding measurement operator is actually

$$\begin{pmatrix} \text{“}y\text{”} & 0 & 0 \\ 0 & \text{“}z\text{”} & 0 \\ 0 & 0 & \text{“}x\text{”} \end{pmatrix}$$

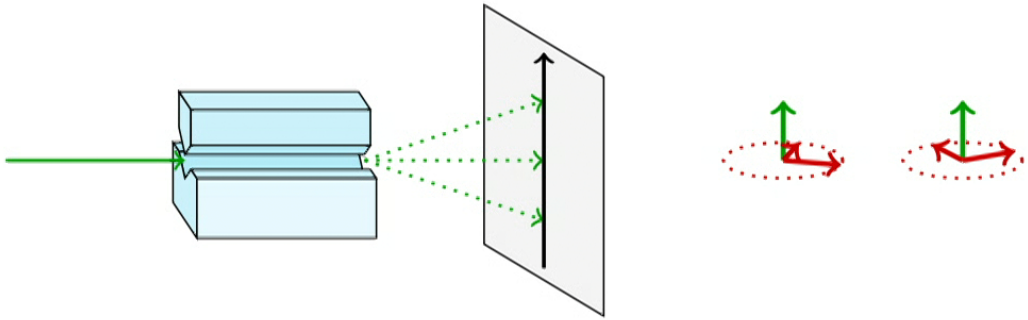
This is a single operator, that changes with the direction choices. Why would we expect a noncontextual model to work at all?

Noncontextuality of (parts of) a quadrupole moment measurement

We measure the direction of zero magnetic momentum. This will be one of the three axes chosen when we set up the measurement device

$$\begin{pmatrix} \text{“}y\text{”} & 0 & 0 \\ 0 & \text{“}z\text{”} & 0 \\ 0 & 0 & \text{“}x\text{”} \end{pmatrix}$$

This single operator changes with the direction choices. But we still expect the outcome along one axis to remain the same, independent of the choice of the other axes, because of the connection to the Stern-Gerlach measurement



Importantly, the spin measurement does not have a context. No additional directions are specified, or are even meaningful to discuss.

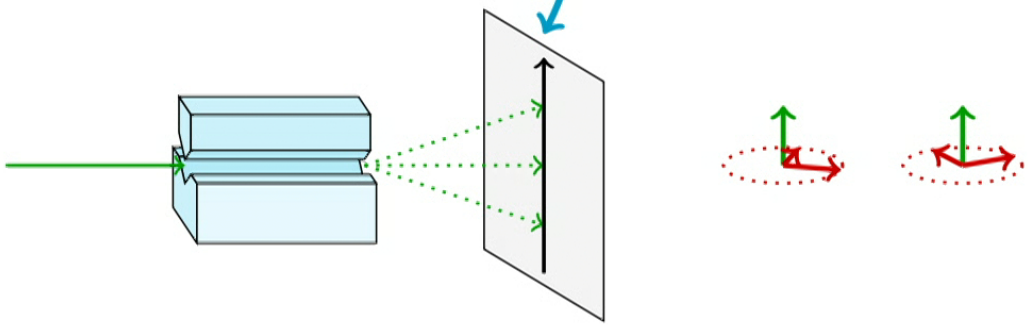
LINKÖPING UNIVERSITY

Noncontextuality of (parts of) a quadrupole moment measurement

We measure the direction of zero magnetic momentum. This will be one of the three axes chosen when we set up the measurement device

$$\begin{pmatrix} \text{“}y\text{”} & 0 & 0 \\ 0 & \text{“}z\text{”} & 0 \\ 0 & 0 & \text{“}x\text{”} \end{pmatrix}$$

This single operator changes with the direction choices. But we still expect the outcome along one axis to remain the same, independent of the choice of the other axes, because of the connection to the Stern-Gerlach measurement

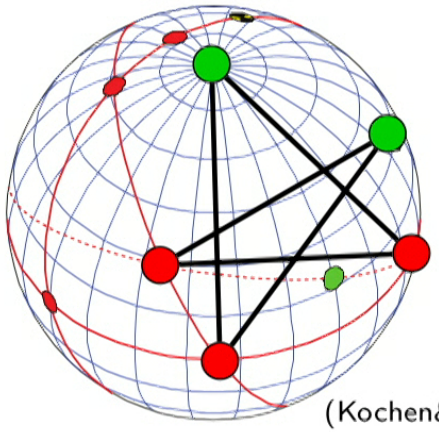


Importantly, the spin measurement does not have a context. No additional directions are specified, or are even meaningful to discuss.

There are no noncontextual models that give the same predictions as quantum mechanics

Theorem (Klyachko et al, 2008): For any noncontextual hidden-variable model,

$$E(A_1A_2) + E(A_2A_3) + E(A_3A_4) + E(A_4A_5) + E(A_5A_1) \geq -3$$



(Kochen&Specker)

There are quantum-mechanical states and measurements such that

$$\langle A_1A_2\rangle + \langle A_2A_3\rangle + \langle A_3A_4\rangle + \langle A_4A_5\rangle + \langle A_5A_1\rangle = 5 - 4\sqrt{5} \approx -3.94$$

Contextuality experiment (Lapkiewicz et al 2011)

$$E(A_1A_2) + E(A_2A_3) + E(A_3A_4) + E(A_4A_5) + E(A_5A_1) \geq -3$$

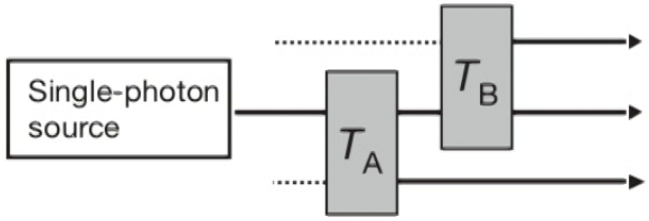


Table 1 | Collected experimental results

(a)	D_1		D_2		D_3		Calculated contribution	
	Condition	Value	Condition	Value	Condition	Value	Term	Value
	$P(A_1 = 1, A_2 = -1)$	0.471(3)	$P(A_1 = -1, A_2 = 1)$	0.432(3)	$P(A_1 = 1, A_2 = 1)$	0.097(1)	$\langle A_1A_2 \rangle$	−0.805(2)
	$P(A_2 = -1, A_3 = 1)$	0.473(4)	$P(A_2 = 1, A_3 = 1)$	0.098(2)	$P(A_2 = 1, A_3 = -1)$	0.429(4)	$\langle A_2A_3 \rangle$	−0.804(3)
	$P(A_3 = 1, A_4 = 1)$	0.146(2)	$P(A_3 = 1, A_4 = -1)$	0.429(2)	$P(A_3 = -1, A_4 = 1)$	0.426(2)	$\langle A_3A_4 \rangle$	−0.709(3)
	$P(A_4 = 1, A_5 = -1)$	0.466(2)	$P(A_4 = -1, A_5 = 1)$	0.439(2)	$P(A_4 = 1, A_5 = 1)$	0.095(1)	$\langle A_4A_5 \rangle$	−0.810(2)
	$P(A_5 = -1, A_1' = 1)$	0.469(2)	$P(A_5 = 1, A_1' = -1)$	0.414(2)	$P(A_5 = 1, A_1' = 1)$	0.117(2)	$\langle A_5A_1' \rangle$	−0.766(3)
							Sum	−3.893(6)

(b)	D_1	D_3	$D_1 + D_3$		D_2		Calculated contribution	
	Value	Value	Condition	Value	Condition	Value	Term	Value
	0.788(2)	0.196(2)	$P(A_1' = 1 \mid A_1 = 1)$	0.983(1)	$P(A_1' = -1 \mid A_1 = 1)$	0.017(1)	$-3 - \varepsilon$	−3.081(2)
	0.010(1)	0.062(2)	$P(A_1' = 1 \mid A_1 = -1)$	0.072(2)	$P(A_1' = -1 \mid A_1 = -1)$	0.928(2)		

Value indicates the measured probability corrected for relative efficiencies (Supplementary Information, section 3). Estimates of standard uncertainties (standard deviations of the means) are given in the brackets.

Contextuality experiment (Lapkiewicz et al 2011)

$$E(A_1A_2) + E(A_2A_3) + E(A_3A_4) + E(A_4A_5) + E(A_5A_1) \geq -3$$

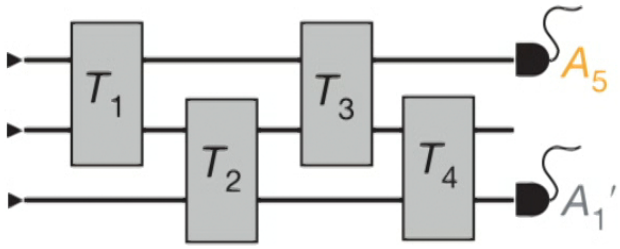


Table 1 | Collected experimental results

(a)	D_1		D_2		D_3		Calculated contribution	
	Condition	Value	Condition	Value	Condition	Value	Term	Value
	$P(A_1 = 1, A_2 = -1)$	0.471(3)	$P(A_1 = -1, A_2 = 1)$	0.432(3)	$P(A_1 = 1, A_2 = 1)$	0.097(1)	$\langle A_1A_2 \rangle$	−0.805(2)
	$P(A_2 = -1, A_3 = 1)$	0.473(4)	$P(A_2 = 1, A_3 = 1)$	0.098(2)	$P(A_2 = 1, A_3 = -1)$	0.429(4)	$\langle A_2A_3 \rangle$	−0.804(3)
	$P(A_3 = 1, A_4 = 1)$	0.146(2)	$P(A_3 = 1, A_4 = -1)$	0.429(2)	$P(A_3 = -1, A_4 = 1)$	0.426(2)	$\langle A_3A_4 \rangle$	−0.709(3)
	$P(A_4 = 1, A_5 = -1)$	0.466(2)	$P(A_4 = -1, A_5 = 1)$	0.439(2)	$P(A_4 = 1, A_5 = 1)$	0.095(1)	$\langle A_4A_5 \rangle$	−0.810(2)
	$P(A_5 = -1, A_1' = 1)$	0.469(2)	$P(A_5 = 1, A_1' = -1)$	0.414(2)	$P(A_5 = 1, A_1' = 1)$	0.117(2)	$\langle A_5A_1' \rangle$	−0.766(3)
							Sum	−3.893(6)

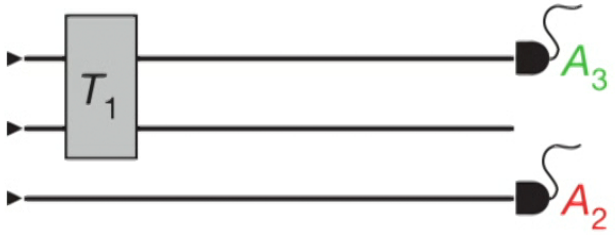
(b)	D_1	D_3	$D_1 + D_3$		D_2		Calculated contribution	
	Value	Value	Condition	Value	Condition	Value	Term	Value
	0.788(2)	0.196(2)	$P(A_1' = 1 \mid A_1 = 1)$	0.983(1)	$P(A_1' = -1 \mid A_1 = 1)$	0.017(1)	$-3 - \varepsilon$	−3.081(2)
	0.010(1)	0.062(2)	$P(A_1' = 1 \mid A_1 = -1)$	0.072(2)	$P(A_1' = -1 \mid A_1 = -1)$	0.928(2)		

Value indicates the measured probability corrected for relative efficiencies (Supplementary Information, section 3). Estimates of standard uncertainties (standard deviations of the means) are given in the brackets.

LINKÖPING UNIVERSITY

Problem: the transformations are not ideal

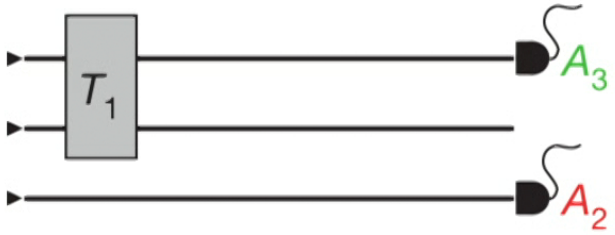
$$E(A_1A_2) + E(A_2A_3) + E(A_3A_4) + E(A_4A_5) + E(A_5A_1) \geq -3$$



- In a paper in EPL 2002 I propose to modify the inequality using a measure of precision ϵ, but do not specify how to link this measure to measurable quantities

Problem: the transformations are not ideal

$$E(A_1A_2) + E(A_2A_3) + E(A_3A_4) + E(A_4A_5) + E(A_5A_1) \geq -3$$



- In a paper in EPL 2002 I propose to modify the inequality using a measure of precision ϵ, but do not specify how to link this measure to measurable quantities
- Andreas Winter goes further, in JPA 2014, to link the measure to how close the actual quantum-mechanical effect (of the POVM) is to the desired projector in QM

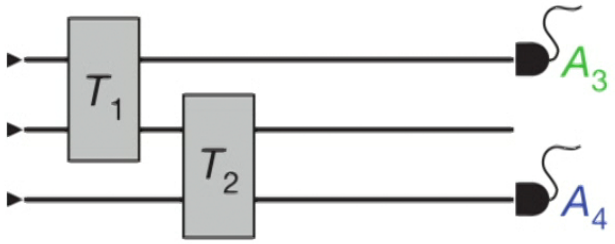
Problem: the transformations are not ideal

$$E(A_1A_2) + E(A_2A_3) + E(A_3A_4) + E(A_4A_5) + E(A_5A_1) \geq -3$$

- In a paper in EPL 2002 I propose to modify the inequality using a measure of precision ϵ, but do not specify how to link this measure to measurable quantities
- Andreas Winter goes further, in JPA 2014, to link the measure to how close the actual quantum-mechanical effect (of the POVM) is to the desired projector in QM
- However, the notion of noncontextuality and the contradictions and inequalities does not apply to QM. Why would the notion of QM distance between effect and projector be applicable?

Problem: the marginals are not equal

$$E(A_1A_2) + E(A_2A_3) + E(A_3A_4) + E(A_4A_5) + E(A_5A_1) \geq -3$$



Noncontextuality implies equal marginal expectations, i.e.,

$$P(A_4^3 = A_4^4) = 1 \quad \Rightarrow \quad \langle A_4^3 \rangle = \langle A_4^4 \rangle$$

while the experimental data give

$$\langle A_4^3 \rangle = 0.122(4); \qquad \langle A_4^4 \rangle = 0.142(4),$$

these are different at 1% significance

Proposed remedy

- With $T(A_4^3, A_4^4)$ as the trace distance (or the total variation distance), it is easy to prove that
$$P(A_4^3 \neq A_4^4) \geq T(A_4^3, A_4^4)$$
- A noncontextual model obeys
$$P(A_4^3 \neq A_4^4) = 0 = T(A_4^3, A_4^4)$$
- If $T(A_4^3, A_4^4) \neq 0$ we propose the term "maximal noncontextuality" for the case when
$$P(A_4^3 \neq A_4^4) = T(A_4^3, A_4^4)$$

LINKÖPING UNIVERSITY

A pentagon inequality for maximally noncontextual models (Kujala, Dzhafarov, JÅL, 2014)

Theorem: For a maximally noncontextual realist model,

$$E(A_1^1 A_2^1) + E(A_2^2 A_3^2) + E(A_3^3 A_4^3) + E(A_4^4 A_5^4) + E(A_5^5 A_1^5) + 2T(A_1^1, A_1^5) + 2T(A_2^1, A_2^2) + 2T(A_3^2, A_3^3) + 2T(A_4^3, A_4^4) + 2T(A_5^4, A_5^5) \geq -3$$

- The total variation distance makes estimating the left-hand side more difficult
- A conservative estimate gives a 99.99999999% confidence interval from the experimental data of Lapkiewicz et al (2011) as

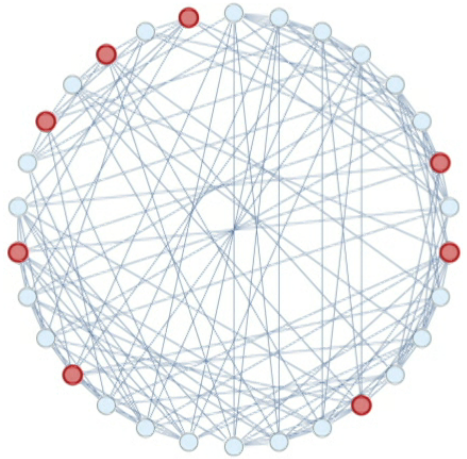
$$[-4.062, -3.127]$$

LINKÖPING UNIVERSITY

Contextuality supplies the "magic" for quantum computation

- Use stabilizer subtheory and inject magic states
- The magic states violate certain state-dependent NC inequalities

- The stabilizer subtheory is efficiently simulatable
- The stabilizer subtheory contains Peres-Mermin state-independent contextuality

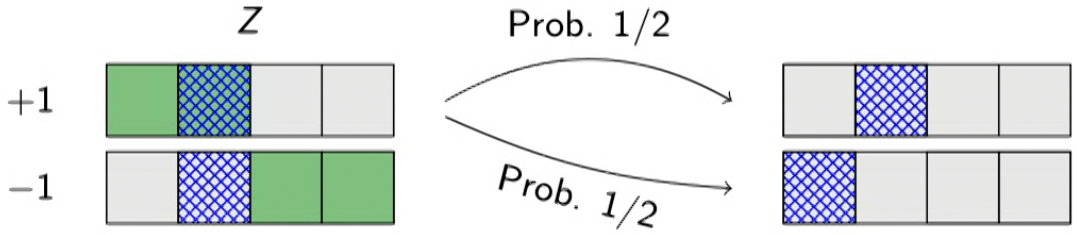


LINKÖPING UNIVERSITY

Another starting point is to use a simple noncontextual model, and add contextuality

Spekkens' toy model

- Each spin-1/2 system is associated with a two-bit "ontic state"
- Each spin-1/2 measurement outcome is associated with an "epistemic state"
- The "knowledge balance principle" ensures that maximal possible knowledge balances with the knowledge one lacks about the system
- This forces a random state change upon measurement, that gives you the uncertainty relation (and basically all the other properties present)

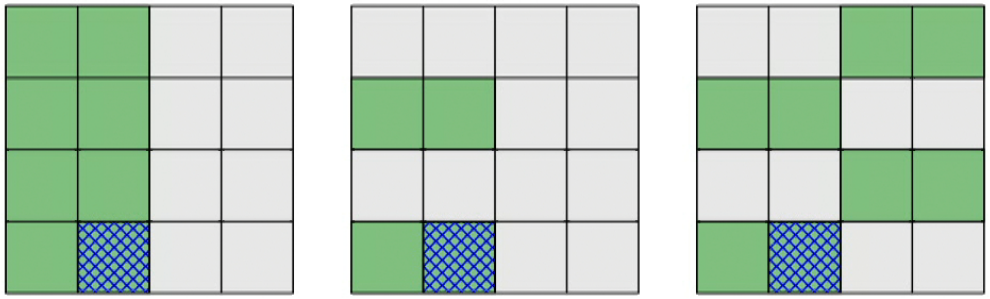


LINKÖPING UNIVERSITY

Spekkens' toy model for composite systems

- This can now be extended to two toy bits, mimicking two qubits

$Z_1 = +1$ $\quad$ $Z_1 = +1, X_2 = +1$ $\quad$ $Z_1 X_2 = +1$

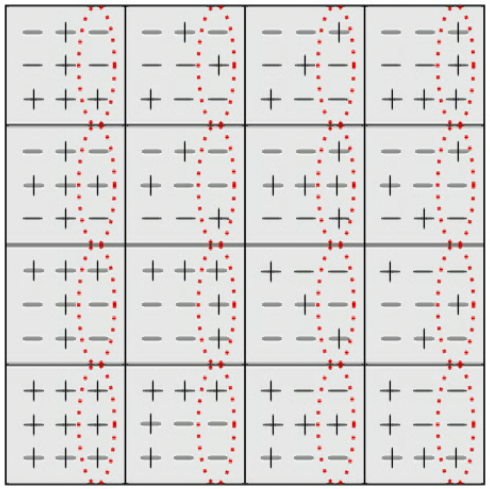


- It is simple to see that the model is noncontextual
- For this particular ontic state,

$$\begin{bmatrix} Z_1 & Z_2 & Z_1 Z_2 \\ X_2 & X_1 & X_1 X_2 \\ Z_1 X_2 & X_1 Z_2 & Y_1 Y_2 \end{bmatrix} = \begin{bmatrix} +1 & +1 & +1 \\ +1 & -1 & -1 \\ +1 & -1 & -1 \end{bmatrix}.$$

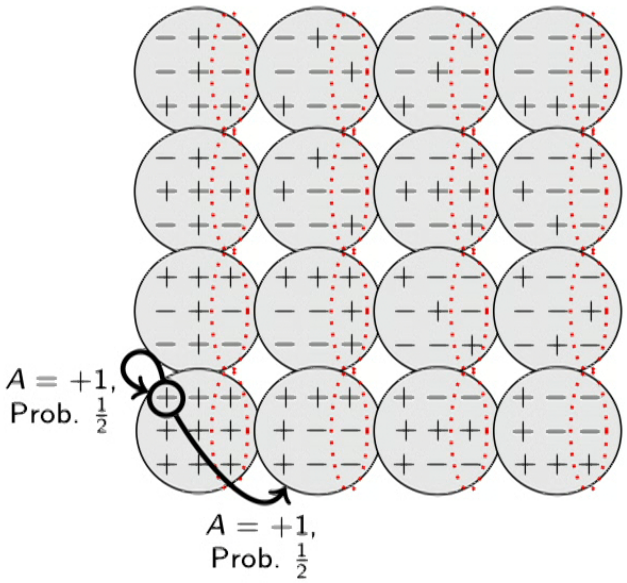
Spekkens' toy model and the Peres-Mermin square

- Writing out the signs contained in the PM square for each of the ontic states results in



Spekkens' toy model and the Peres-Mermin square

- The toy model is a stochastic Mealy machine



The toy model reproduces many of the quantum predictions

In the toy model

- Noncommuting measurements
- Uncertainty
- Interference
- Remote steering
- No cloning
- No broadcasting
- Mutually Unbiased Partitions
- Superdense coding
- Entanglement monogamy
- Teleportation
- Positive Operator Valued Measures
- ...

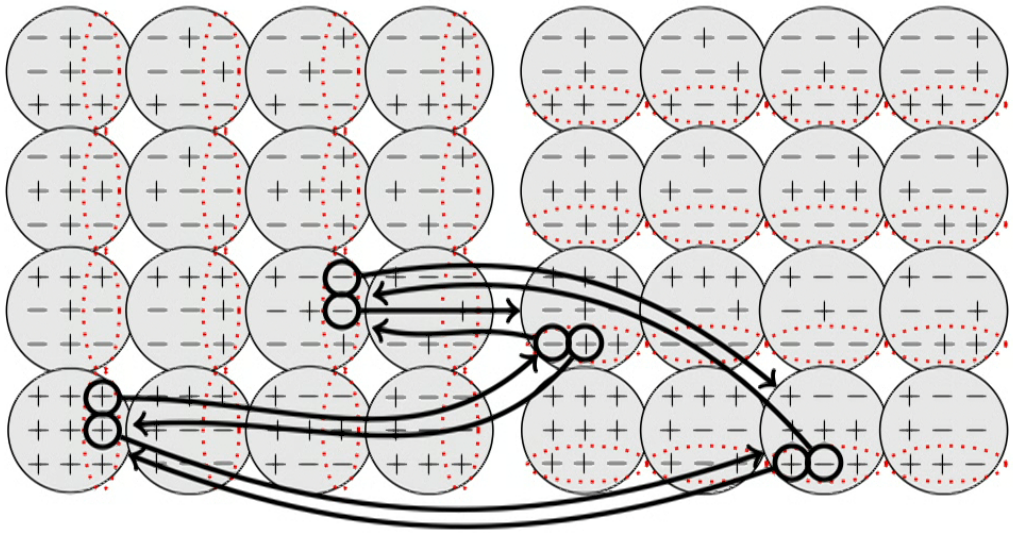
Not in the toy model

- Contextuality
- Nonlocality
- Quantum-computational speedup
- Continuum of states
- ...

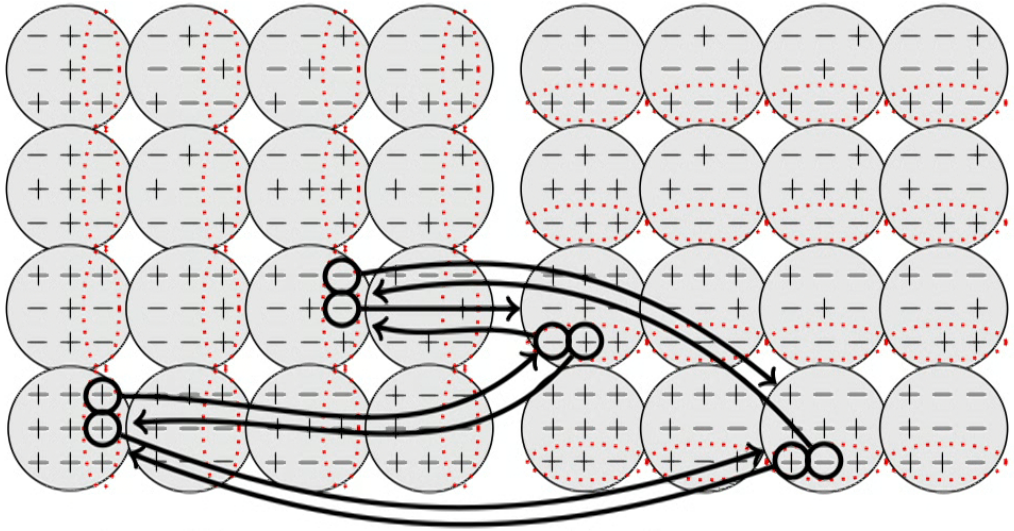
LINKÖPING UNIVERSITY

Memory requirements for reproducing the QM predictions for the PM square (Kleinmann, Gühne, Portillo, JÅL, Cabello, 2011)

- Extends the Mealy machine to include contextuality
- This extends the state space, and needs more complicated state change structure



Memory requirements for reproducing the QM predictions for the PM square (Kleinmann, Gühne, Portillo, JÅL, Cabello, 2011)



- Requires at least 32 states, or one more bit of memory
- With all 10 PM squares, depending on your demands on the model, between 60 and 768 states are sufficient (P Harrysson, 2016)
- The knowledge balance principle becomes a knowledge imbalance principle, because there is always more knowledge one lacks than one has

The toy model reproduces many of the quantum predictions

In the toy model

- Noncommuting measurements
- Uncertainty
- Interference
- Remote steering
- No cloning
- No broadcasting
- Mutually Unbiased Partitions
- Superdense coding
- Entanglement monogamy
- Teleportation
- Positive Operator Valued Measures

\+ Contextuality

\+ Nonlocality

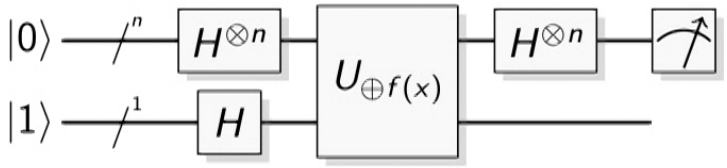
- ...

Not in the toy model

- ~~Contextuality~~
- ~~Nonlocality~~
- Quantum-computational speedup?
- Continuum of states
- ...

LINKÖPING UNIVERSITY

How much contextuality do you need to do Deutsch-Jozsa for three-bit inputs?



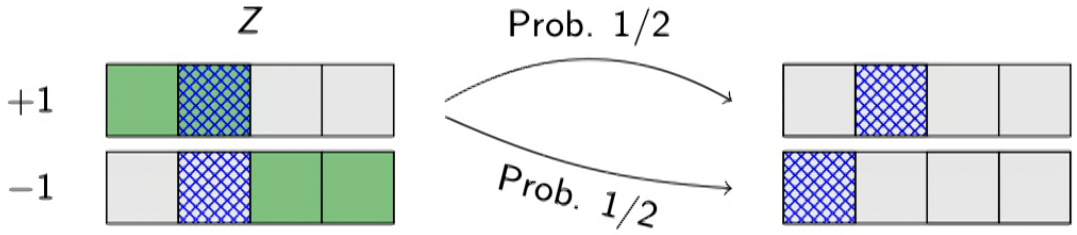
- Determine if f is balanced or constant
- One- or two-bit input function oracles are in the Clifford group, and also in the toy model
- Three-bit input or larger function oracles are not

LINKÖPING UNIVERSITY

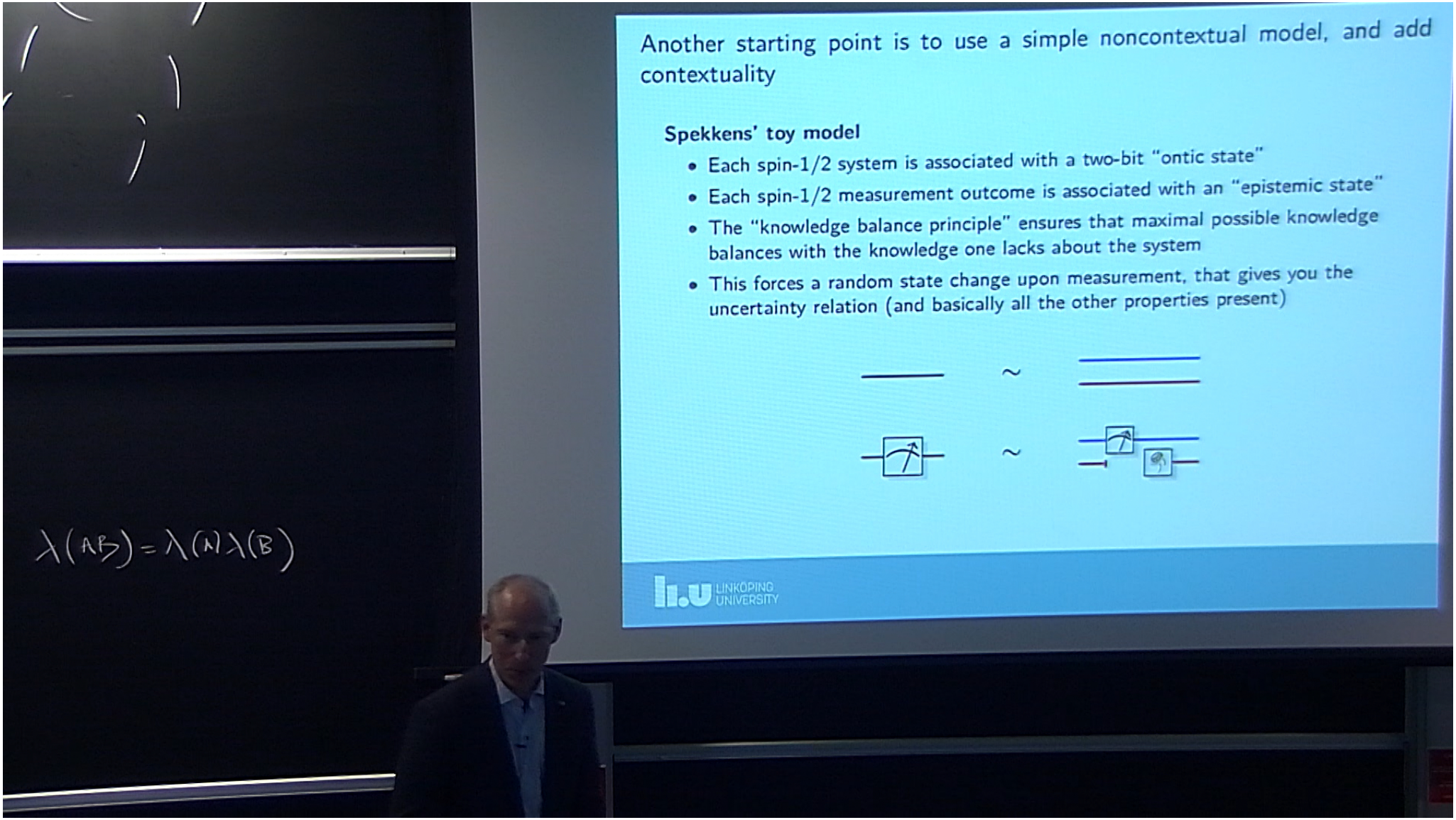
Another starting point is to use a simple noncontextual model, and add contextuality

Spekkens' toy model

- Each spin-1/2 system is associated with a two-bit "ontic state"
- Each spin-1/2 measurement outcome is associated with an "epistemic state"
- The "knowledge balance principle" ensures that maximal possible knowledge balances with the knowledge one lacks about the system
- This forces a random state change upon measurement, that gives you the uncertainty relation (and basically all the other properties present)



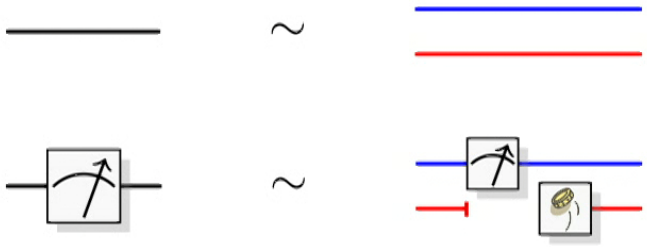
LINKÖPING UNIVERSITY


$\lambda(AB) = \lambda(A)\lambda(B)$
Another starting point is to use a simple noncontextual model, and add contextuality
Spekkens' toy model
• Each spin-1/2 system is associated with a two-bit "ontic state"
• Each spin-1/2 measurement outcome is associated with an "epistemic state"
• The "knowledge balance principle" ensures that maximal possible knowledge balances with the knowledge one lacks about the system
• This forces a random state change upon measurement, that gives you the uncertainty relation (and basically all the other properties present)
LINKÖPING UNIVERSITY

Another starting point is to use a simple noncontextual model, and add contextuality

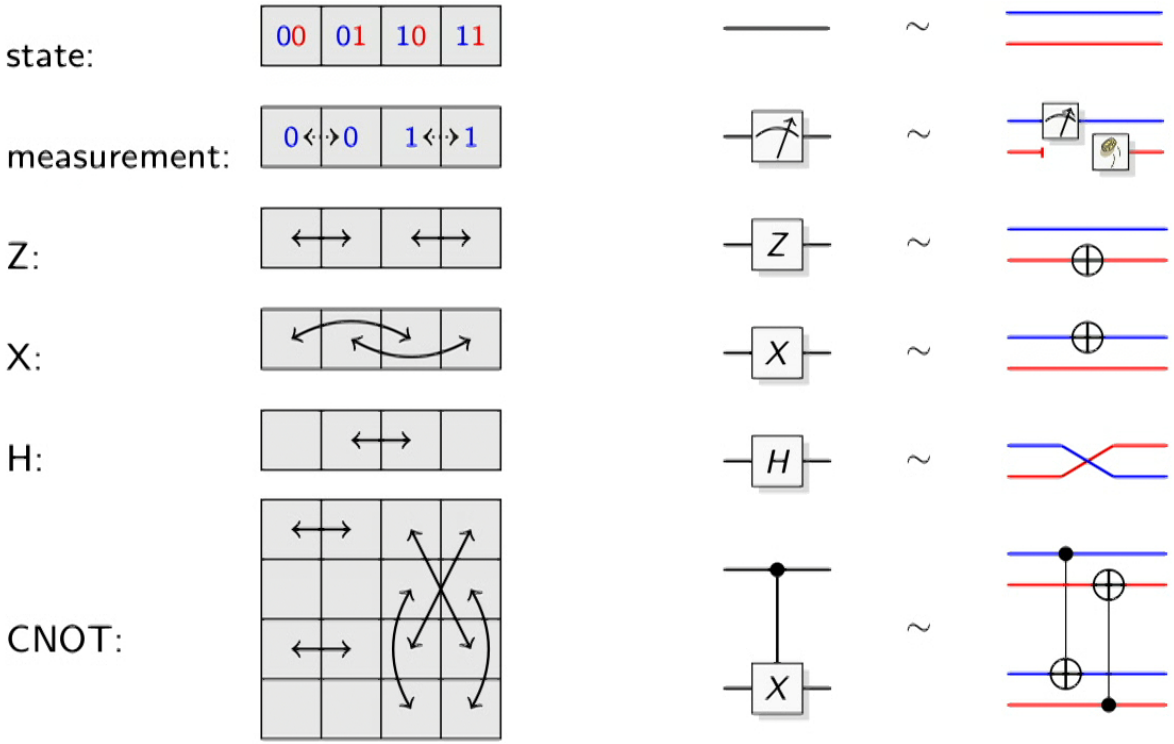
Spekkens' toy model

- Each spin-1/2 system is associated with a two-bit "ontic state"
- Each spin-1/2 measurement outcome is associated with an "epistemic state"
- The "knowledge balance principle" ensures that maximal possible knowledge balances with the knowledge one lacks about the system
- This forces a random state change upon measurement, that gives you the uncertainty relation (and basically all the other properties present)

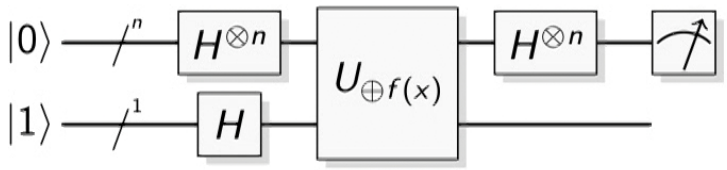


LINKÖPING UNIVERSITY

Gates can now be represented in a more direct way



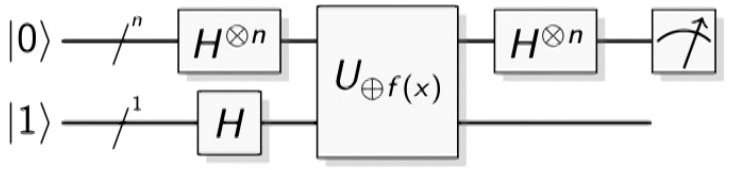
How much contextuality do you need to do Deutsch-Jozsa for three-bit inputs?



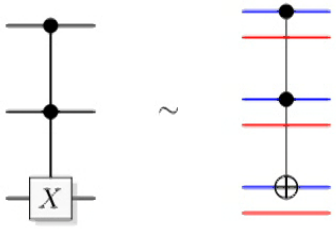
- Determine if f is balanced or constant
- One- or two-bit input function oracles are in the Clifford group, and also in the toy model
- Three-bit input or larger function oracles are not

LINKÖPING UNIVERSITY

How much contextuality do you need to do Deutsch-Jozsa for three-bit inputs?

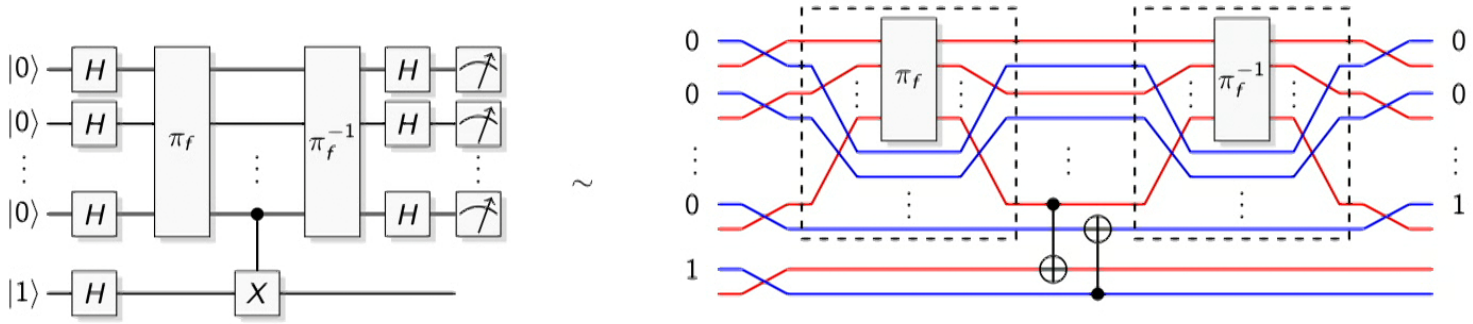


- Determine if f is balanced or constant
- One- or two-bit input function oracles are in the Clifford group, and also in the toy model
- Three-bit input or larger function oracles are not
- Nonetheless, three-bit input oracles can be realized



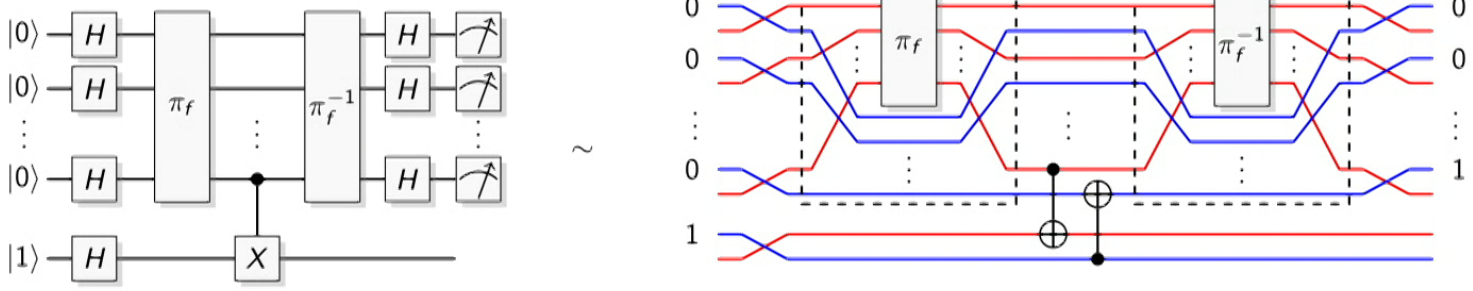
LINKÖPING UNIVERSITY

Deutsch-Jozsa in our framework



- A balanced oracle has the center CNOT, a constant oracle has not
- Measurement after the final Hadamards will reveal whether it is balanced or constant
- The overhead is constant, a factor 2

Common questions about Deutsch-Jozsa in our framework



- Surely this is impossible, there are theorems that state that exponentially many function calls are needed in a classical computer?
- Your oracle is too simple, isn't optical inspection enough to determine if it is a balanced function or not?
- For a quantum oracle, it is enough to generate the function map, but that cannot be sufficient here?

LINKÖPING UNIVERSITY

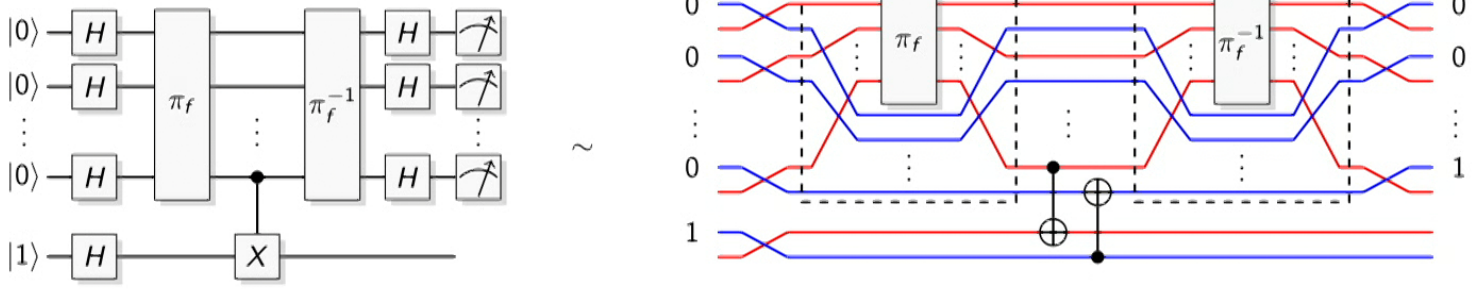
Surely this is impossible, there are theorems!

Theorem (Simon, 1997)

Let O be an oracle constructed as follows: for each n, a random n-bit string $s(n)$ and a random bit $b(n)$ are uniformly chosen from $\{0,1\}^n$ and $\{0,1\}$, respectively. If $b(n) = 0$, then the function $f_n : \{0,1\}^n \to \{0,1\}^n$ chosen for O to compute on n-bit queries is a random function uniformly distributed over permutations on $\{0,1\}^n$; otherwise, it is a random function uniformly distributed over two-to-one functions such that $f_n(x) = f_n\big(x \oplus s(n)\big)$ for all x, where $\oplus$ denotes bitwise exclusive-or. Then any PTM that queries O no more than $2^{n/4}$ times cannot correctly guess $b(n)$ with probability greater than $(1/2) + 2^{-n/2}$, over choices made in the construction of O.

The important detail here is that $f_n : \{0,1\}^n \to \{0,1\}^n$, which is not the case in quantum computation. Nor is it the case in our framework.

Common questions about Deutsch-Jozsa in our framework



- Surely this is impossible, there are theorems that state that exponentially many function calls are needed in a classical computer?
- Your oracle is too simple, isn't optical inspection enough to determine if it is a balanced function or not?
- For a quantum oracle, it is enough to generate the function map, but that cannot be sufficient here?

LINKÖPING UNIVERSITY

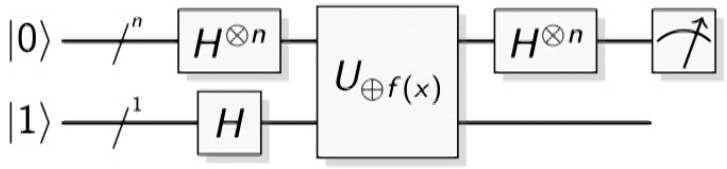
Surely this is impossible, there are theorems!

Theorem (Simon, 1997)

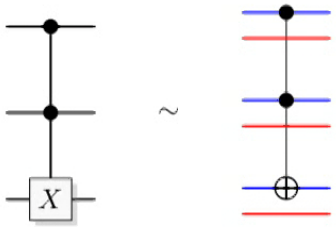
Let O be an oracle constructed as follows: for each n, a random n-bit string $s(n)$ and a random bit $b(n)$ are uniformly chosen from $\{0,1\}^n$ and $\{0,1\}$, respectively. If $b(n) = 0$, then the function $f_n : \{0,1\}^n \to \{0,1\}^n$ chosen for O to compute on n-bit queries is a random function uniformly distributed over permutations on $\{0,1\}^n$; otherwise, it is a random function uniformly distributed over two-to-one functions such that $f_n(x) = f_n\big(x \oplus s(n)\big)$ for all x, where $\oplus$ denotes bitwise exclusive-or. Then any PTM that queries O no more than $2^{n/4}$ times cannot correctly guess $b(n)$ with probability greater than $(1/2) + 2^{-n/2}$, over choices made in the construction of O.

The important detail here is that $f_n : \{0,1\}^n \to \{0,1\}^n$, which is not the case in quantum computation. Nor is it the case in our framework.

How much contextuality do you need to do Deutsch-Jozsa for large inputs?

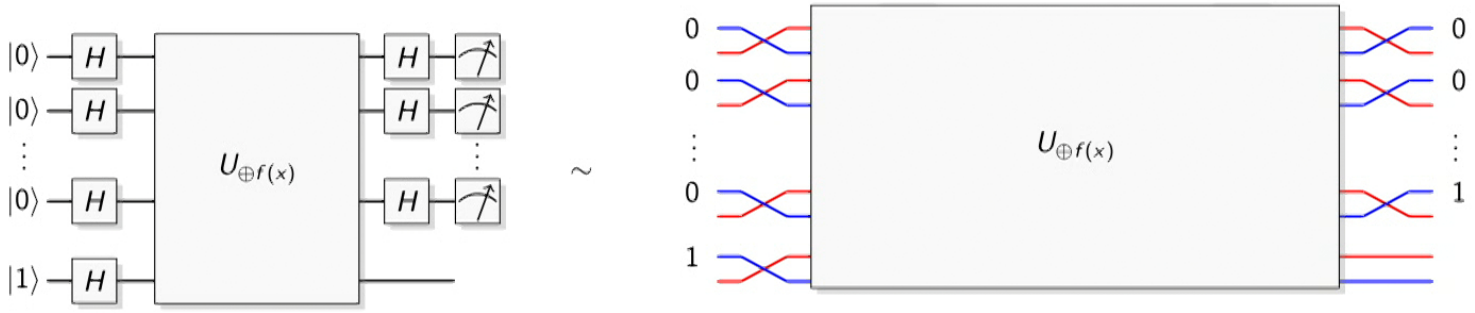


- Determine if f is balanced or constant
- One- or two-bit input function oracles are in the Clifford group, and also in the toy model
- Three-bit input or larger function oracles are not
- Nonetheless, *n*-bit input oracles can be realized



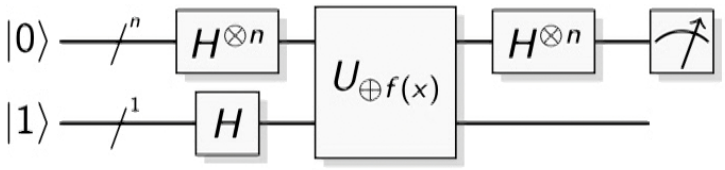
LINKÖPING UNIVERSITY

Your oracle is too simple, just look!



The important detail here is that the algorithm is to solve the oracle problem: given an oracle with one of two promised properties, determine which using only the function inputs and outputs.

For a quantum oracle, it is enough to generate the function map!



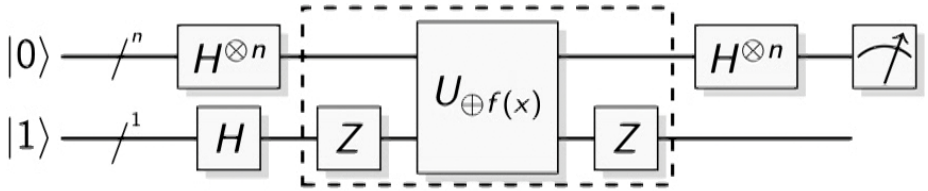
Some presentations tell you the unitary map (only) needs to make sure that

$$|x, y\rangle \mapsto |x, y \oplus f(x)\rangle$$

but the real difficulty in quantum computation is to ensure that

$$\sum_{x,y} c_{x,y} |x, y\rangle \mapsto \sum_{x,y} c_{x,y} |x, y \oplus f(x)\rangle$$

For a quantum oracle, it is enough to generate the function map!



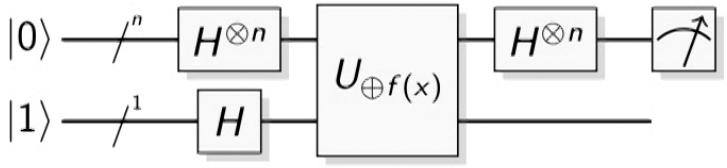
The real difficulty in quantum computation is to ensure that

$$\sum_{x,y} c_{x,y} |x, y\rangle \mapsto \sum_{x,y} c_{x,y} |x, y \oplus f(x)\rangle$$

instead of, say,

$$\sum_{x,y} c_{x,y} |x, y\rangle \mapsto \sum_{x,y} c_{x,y} (-1)^{f(x)} |x, y \oplus f(x)\rangle$$

For a quantum oracle, it is enough to generate the function map!

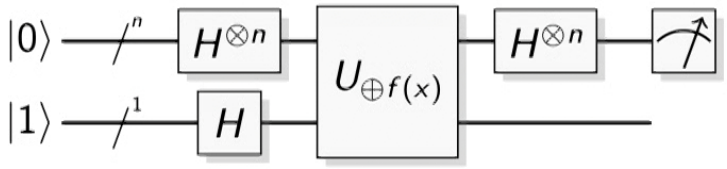


In fact, the "phase kick-back" of the Deutsch-Jozsa algorithm requires

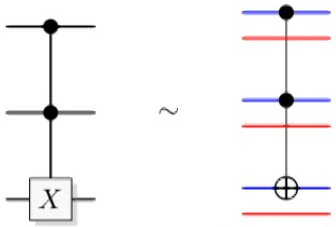
$$\sum_{x,y} c_{x,y} \, |x, y\rangle \mapsto \sum_{x,y} c_{x,y} \, |x, y \oplus f(x)\rangle$$

. . . and phase kick-back is what forces the oracle (internal) structure in our framework

How much contextuality do you need to do Deutsch-Jozsa for large inputs?

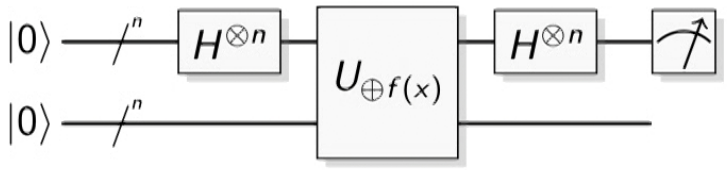


- Determine if f is balanced or constant
- One- or two-bit input function oracles are in the Clifford group, and also in the toy model
- Three-bit input or larger function oracles are not
- Nonetheless, *n*-bit input oracles can be realized

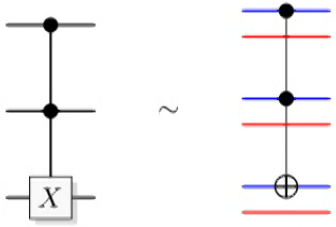


LINKÖPING UNIVERSITY

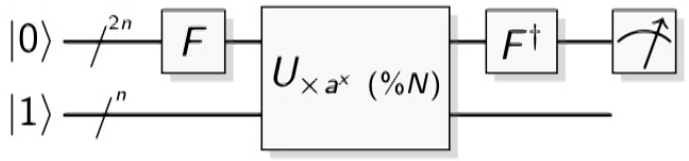
Simon's algorithm, that finds the generator of a hidden order-two group, can also be efficiently realized



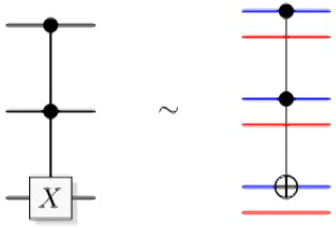
- The function is such that $f(x) = f(y)$ iff $x = y \oplus s$ for a secret s
- Determine if s is nonzero (or find s)
- Needs an exponential number of classical function calls, but only $O(n)$ quantum oracle calls
- Our framework also finds s in $O(n)$ oracle calls



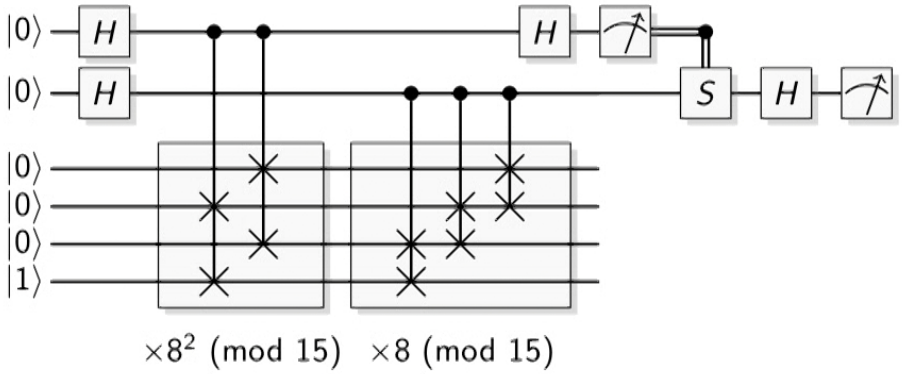
What about Shor's algorithm?



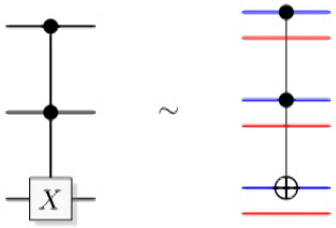
- Find period of a^x mod N
- If you do not "compile" the circuitry, even factoring 15 is outside the Clifford group



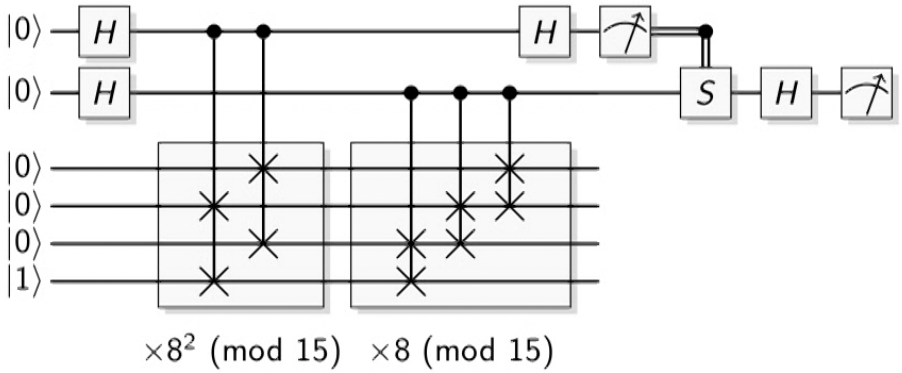
What about Shor's algorithm?



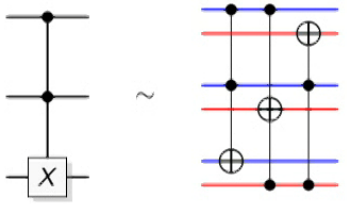
- Find period of a^x mod N
- If you do not "compile" the circuitry, even factoring 15 is outside the Clifford group



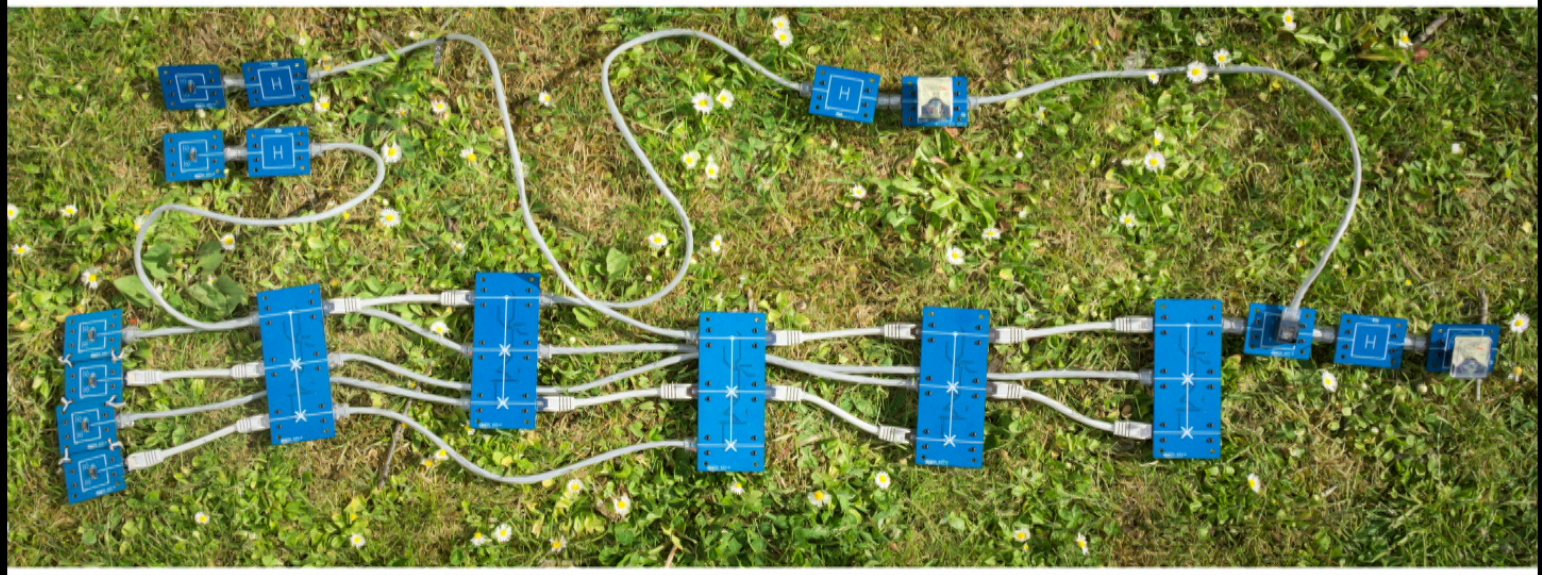
What about Shor's algorithm?



- Find period of a^x mod N
- If you do not "compile" the circuitry, even factoring 15 is outside the Clifford group
- The simple Toffoli does not work, but a better Toffoli does

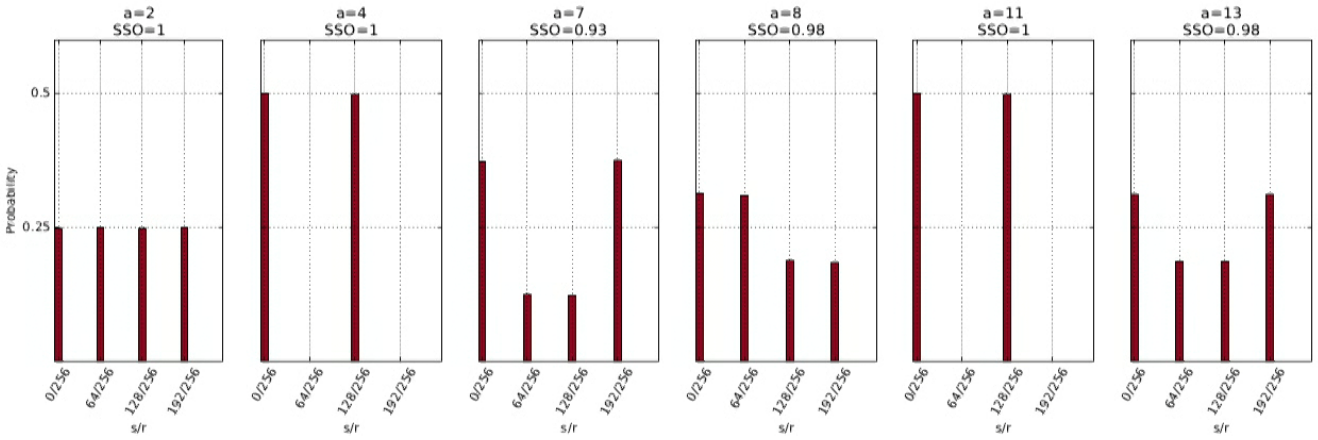


Shor's algorithm in complementary pass-transistor logic



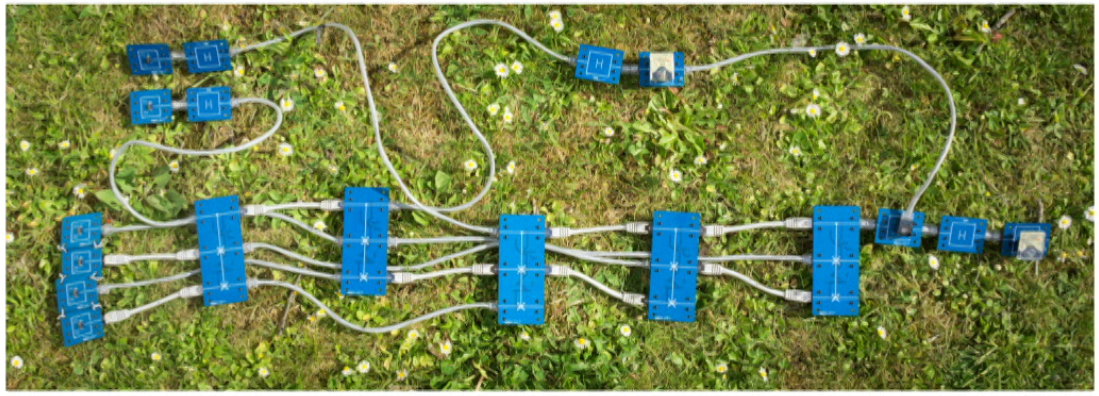
LINKÖPING UNIVERSITY

Shor's algorithm in complementary pass-transistor logic



- There are systematic errors
- (. . . but they are smaller than in any other state-of-the-art experiment)

This device runs the quantum algorithms better than any other state-of-the-art quantum computer



- If I had sold you this, you would have become very suspicious — because it seems too good to be true
- Contains the toy model (noncommuting measurements, uncertainty, interference, remote steering, Mutually Unbiased Partitions, dense coding, teleportation, Positive Operator Valued Measures, . . . ; sans the Toffoli, you also have no cloning, no broadcasting, entanglement monogamy, QKD, . . .)
- The Deutsch-Jozsa and Simon's algorithms can be run efficiently, with zero error
- Shor's algorithm can be run efficiently with lower error than any other state-of-the-art quantum computer

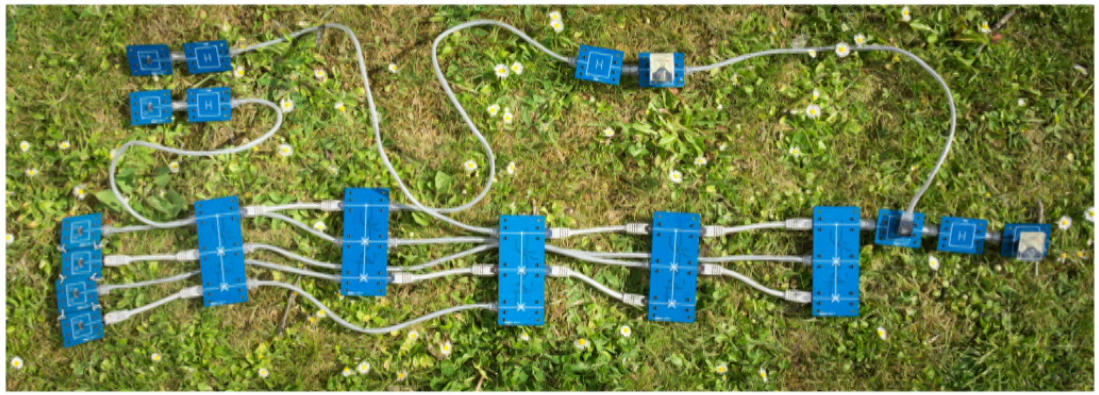
LINKÖPING UNIVERSITY

Conclusions

- Noncontextuality experiments are limited by statistical and systematic errors
- A relaxed notion of noncontextuality can be used to restore the usefulness of the bounds

$$E(A_1^1 A_2^1) + E(A_2^2 A_3^2) + E(A_3^3 A_4^3) + E(A_4^4 A_5^4) + E(A_5^5 A_1^5) + 2T(A_1^1, A_1^5) + 2T(A_2^1, A_2^2) + 2T(A_3^2, A_3^3) + 2T(A_4^3, A_4^4) + 2T(A_5^4, A_5^5) \geq -3$$

- The toy model can be extended to be contextual
- But there is not a strong link to the quantum speedup
- Better to extend with something close to a quantum Toffoli



LINKÖPING UNIVERSITY