On the Significance of the Gottesman-Knill Theorem

Michael E. Cuffaro [1,2]

[1]Philosophy Department, The University of Western Ontario

[2]Munich Center for Mathematical Philosophy, Ludwig Maximilians Universität München

July 30, 2013

Foundations of Physics Conference, Munich, Germany

What is quantum computing?

Uses the resources of quantum mechanics to solve computational problems faster and more efficiently than is possible using (known) classical means.

In some cases, this 'quantum speedup' can be dramatic (exponential).

Example: factoring

- Much Internet security is based on the assumption that factoring arbitrary integers is a 'hard' problem:
    - No classical algorithm exists for efficiently (i.e. in polynomial time) factoring arbitrary numbers.

Example: factoring

- Much Internet security is based on the assumption that factoring arbitrary integers is a 'hard' problem:
  - No classical algorithm exists for efficiently (i.e. in polynomial time) factoring arbitrary numbers.
- Shor's algorithm: a provably efficient quantum algorithm for factoring.
  - Makes the factoring problem tractable.

What is the explanation for quantum speedup?

What is the explanation for quantum speedup?

Quantum Entanglement:

- Exponentially larger state space efficiently accessible to quantum (as opposed to classical) systems.
- Can be used as a resource to enable quantum speedup.

What role does entanglement play in quantum computation?

- Necessary for speedup?

- Sufficient for speedup?

What role does entanglement play in quantum computation?

- Necessary for speedup?
  - Even if possessing an entangled state is enough to enable speedup, there may be alternative ways to enable it.
- Sufficient for speedup?
  - Even if entanglement is required to enable speedup, it doesn't follow that nothing else is.

What role does entanglement play in quantum computation?

- Necessary for speedup?
    - Even if possessing an entangled state is enough to enable speedup, there may be alternative ways to enable it.
- Sufficient for speedup?
    - Even if entanglement is required to enable speedup, it doesn't follow that nothing else is.

What role does entanglement play in quantum computation?

- Necessary for speedup?
  - Even if possessing an entangled state is enough to enable speedup, there may be alternative ways to enable it.
- Sufficient for speedup?
  - Even if entanglement is required to enable speedup, it doesn't follow that nothing else is.
  - Is a pure entangled state sufficient to enable speedup?

What role does entanglement play in quantum computation?

- Necessary for speedup?
  - Even if possessing an entangled state is enough to enable speedup, there may be alternative ways to enable it.
- Sufficient for speedup?
  - Even if entanglement is required to enable speedup, it doesn't follow that nothing else is.
  - Is a pure entangled state sufficient to enable speedup?
  - Gottesman-Knill theorem: a counter-example?

Outline

1. Introduction.
2. The Gottesman-Knill theorem.
3. Analysis of the Gottesman-Knill operations.
    i. The CHSH inequality.
    ii. The GHZ argument.
4. Conclusion.

Outline

1. Introduction.
2. The Gottesman-Knill theorem.
3. Analysis of the Gottesman-Knill operations.
    i. The CHSH inequality.
    ii. The GHZ argument.
4. Conclusion.

The Gottesman-Knill theorem

Any algorithm using only these is efficiently simulable classically:

- State preparation of product states of qubits in the computational (i.e., $\{|0\rangle, |1\rangle\}$) basis
- Measurements of (products of) Pauli observables.
- "Clifford group" gates:
  - Pauli gates
  - Phase gates
  - CNOT gates
  - Hadamard gates
- Clifford group gates conditioned on classical bits

GK operations capable of generating entangled states

GK operations capable of generating entangled states

- State preparation of product states in the computational basis

$$|0\rangle|0\rangle$$

GK operations capable of generating entangled states

- State preparation of product states in the computational basis
- Hadamard gate: $|0\rangle \xrightarrow{H} \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|1\rangle \xrightarrow{H} \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

$$|0\rangle|0\rangle \quad \xrightarrow{H\otimes I} \frac{|0\rangle|0\rangle+|1\rangle|0\rangle}{\sqrt{2}}$$

GK operations capable of generating entangled states

- State preparation of product states in the computational basis
- Hadamard gate: $|0\rangle \xrightarrow{H} \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|1\rangle \xrightarrow{H} \frac{|0\rangle-|1\rangle}{\sqrt{2}}$
- CNOT gate

$$|0\rangle|0\rangle \quad \xrightarrow{H\otimes I} \frac{|0\rangle|0\rangle+|1\rangle|0\rangle}{\sqrt{2}} \quad \xrightarrow{CNOT} \frac{|0\rangle|0\rangle+|1\rangle|1\rangle}{\sqrt{2}} = |\Phi^+\rangle,$$

GK operations capable of generating entangled states

- State preparation of product states in the computational basis
- Hadamard gate: $|0\rangle \xrightarrow{H} \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|1\rangle \xrightarrow{H} \frac{|0\rangle-|1\rangle}{\sqrt{2}}$
- CNOT gate

$$
\begin{aligned}
|0\rangle|0\rangle &\xrightarrow{H\otimes I} \frac{|0\rangle|0\rangle + |1\rangle|0\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} = |\Phi^+\rangle, \\
|0\rangle|1\rangle &\xrightarrow{H\otimes I} \frac{|0\rangle|1\rangle + |1\rangle|1\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|0\rangle|1\rangle + |1\rangle|0\rangle}{\sqrt{2}} = |\Psi^+\rangle, \\
|1\rangle|0\rangle &\xrightarrow{H\otimes I} \frac{|0\rangle|0\rangle - |1\rangle|0\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|0\rangle|0\rangle - |1\rangle|1\rangle}{\sqrt{2}} = |\Phi^-\rangle, \\
|1\rangle|1\rangle &\xrightarrow{H\otimes I} \frac{|0\rangle|1\rangle - |1\rangle|1\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|0\rangle|1\rangle - |1\rangle|0\rangle}{\sqrt{2}} = |\Psi^-\rangle.
\end{aligned}
$$

Jozsa & Linden (2003) on the Gottesman-Knill theorem:

Recall that the significance of entanglement for pure-state computations is derived from the fact that unentangled pure states ... of n qubits have a description involving poly(n) parameters (in contrast to $O(2^n)$ parameters for a general pure state). But this special property of unentangled states (of having a 'small' descriptions [sic.]) is contingent on a particular mathematical description, as amplitudes in the computational basis. If we were to adopt some other choice of mathematical description for quantum states (and their evolution), then, although it will be mathematically equivalent to the amplitude description, there will be a different class of states which will now have a polynomially sized description; ...

Jozsa & Linden (2003) on the Gottesman-Knill theorem:

Recall that the significance of entanglement for pure-state computations is derived from the fact that unentangled pure states ... of n *qubits have a description involving poly(*n*) parameters (in contrast to* $O(2^n)$ *parameters for a general pure state). But this special property of unentangled states (of having a 'small' descriptions [sic.]) is contingent on a particular mathematical description, as amplitudes in the computational basis. If we were to adopt some other choice of mathematical description for quantum states (and their evolution), then, although it will be mathematically equivalent to the amplitude description, there will be a different class of states which will now have a polynomially sized description; ...*

Jozsa & Linden (2003) on the Gottesman-Knill theorem:

Recall that the significance of entanglement for pure-state computations is derived from the fact that unentangled pure states ... of n *qubits have a description involving poly(*n*) parameters (in contrast to* $O(2^n)$ *parameters for a general pure state). But this special property of unentangled states (of having a 'small' descriptions [sic.]) is contingent on a particular mathematical description, as amplitudes in the computational basis. If we were to adopt some other choice of mathematical description for quantum states (and their evolution), then, although it will be mathematically equivalent to the amplitude description, there will be a different class of states which will now have a polynomially sized description; ...*

Jozsa & Linden (2003) on the Gottesman-Knill theorem:

With this in mind we see that the significance of entanglement as a resource for quantum computation is not an intrinsic property of quantum physics itself, but is tied to a particular additional (arbitrary) choice of mathematical formalism for the theory. ... An explicit example of an alternative formalism and its implications for the power of quantum computation is provided by the so-called stabilizer formalism and the Gottesman-Knill theorem ... (Jozsa & Linden, 2003, 2029-2030).

Jozsa & Linden (2003) on the Gottesman-Knill theorem:

With this in mind we see that the significance of entanglement as a resource for quantum computation is not an intrinsic property of quantum physics itself, but is tied to a particular additional (arbitrary) choice of mathematical formalism for the theory. ... An explicit example of an alternative formalism and its implications for the power of quantum computation is provided by the so-called stabilizer formalism and the Gottesman-Knill theorem ... (Jozsa & Linden, 2003, 2029-2030).

Jozsa & Linden (2003) on the Gottesman-Knill theorem:

With this in mind we see that the significance of entanglement as a resource for quantum computation is not an intrinsic property of quantum physics itself, but is tied to a particular additional (arbitrary) choice of mathematical formalism for the theory. ... An explicit example of an alternative formalism and its implications for the power of quantum computation is provided by the so-called stabilizer formalism and the Gottesman-Knill theorem ... (Jozsa & Linden, 2003, 2029-2030).

Differently sized descriptions

$$\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)_1(|0\rangle + |1\rangle)_2 \dots (|0\rangle + |1\rangle)_n \quad (1)$$

$$= \frac{1}{2^{n/2}}(|00\dots00\rangle + |00\dots01\rangle + \cdots + |11\dots10\rangle + |11\dots11\rangle. \quad (2)$$

· Eq. (1) is exponentially smaller than Eq. (2).

Differently sized descriptions

$$\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)_1(|0\rangle + |1\rangle)_2 \ldots (|0\rangle + |1\rangle)_n \tag{1}$$

$$= \frac{1}{2^{n/2}}(|00\ldots00\rangle + |00\ldots01\rangle + \cdots + |11\ldots10\rangle + |11\ldots11\rangle. \tag{2}$$

- Eq. (1) is exponentially smaller than Eq. (2).
- Even more compact expressions are possible. E.g.,

$$\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)^n \tag{3}$$

$$\frac{1}{2^{n/2}}\sum_x^{2^n-1}|x\rangle \tag{4}$$

Differently sized descriptions

$$\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)_1(|0\rangle + |1\rangle)_2 \ldots (|0\rangle + |1\rangle)_n \tag{1}$$

$$= \frac{1}{2^{n/2}}(|00\ldots00\rangle + |00\ldots01\rangle + \cdots + |11\ldots10\rangle + |11\ldots11\rangle. \tag{2}$$

- Eq. (1) is exponentially smaller than Eq. (2).
- Even more compact expressions are possible. E.g.,

$$\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)^n \tag{3}$$

$$\frac{1}{2^{n/2}}\sum_{x}^{2^n-1}|x\rangle \tag{4}$$

- No mystery: facts about the underlying system are what make these alternative descriptions possible.

Differently sized descriptions

$$\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)_1(|0\rangle + |1\rangle)_2 \ldots (|0\rangle + |1\rangle)_n \quad (1)$$

$$= \frac{1}{2^{n/2}}(|00\ldots00\rangle + |00\ldots01\rangle + \cdots + |11\ldots10\rangle + |11\ldots11\rangle. \quad (2)$$

- Eq. (1) is exponentially smaller than Eq. (2).
- Even more compact expressions are possible. E.g.,

$$\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)^n \quad (3) \qquad\qquad \frac{1}{2^{n/2}}\sum_{x}^{2^n-1}|x\rangle \quad (4)$$

- No mystery: facts about the underlying system are what make these alternative descriptions possible.
- No analogous "compression" is possible for entangled states

Differently sized descriptions

$$\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)_1(|0\rangle + |1\rangle)_2 \ldots (|0\rangle + |1\rangle)_n \qquad (1)$$

$$= \frac{1}{2^{n/2}}(|00\ldots00\rangle + |00\ldots01\rangle + \cdots + |11\ldots10\rangle + |11\ldots11\rangle. \qquad (2)$$

- Eq. (1) is exponentially smaller than Eq. (2).
- Even more compact expressions are possible. E.g.,

$$\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)^n \qquad (3) \qquad\qquad \frac{1}{2^{n/2}}\sum_x^{2^n-1}|x\rangle \qquad (4)$$

- No mystery: facts about the underlying system are what make these alternative descriptions possible.
- No analogous "compression" is possible for entangled states—and yet it is possible using the "stabiliser" formalism?

Differently sized descriptions

$$\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)_1(|0\rangle + |1\rangle)_2 \ldots (|0\rangle + |1\rangle)_n \quad (1)$$

$$= \frac{1}{2^{n/2}}(|00\ldots00\rangle + |00\ldots01\rangle + \cdots + |11\ldots10\rangle + |11\ldots11\rangle. \quad (2)$$

- Eq. (1) is exponentially smaller than Eq. (2).
- Even more compact expressions are possible. E.g.,

$$\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)^n \quad (3) \qquad \frac{1}{2^{n/2}}\sum_x^{2^n-1}|x\rangle \quad (4)$$

- No mystery: facts about the underlying system are what make these alternative descriptions possible.
- No analogous "compression" is possible for entangled states—and yet it is possible using the "stabiliser" formalism?
- Is there a physical reason?

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

- State preparation (single qubit):

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

- State preparation (single qubit): either $|0\rangle$ or $|1\rangle$, "stabilised" by Z, $-Z$ respectively (i.e., equivalent to $Z|0\rangle$, $-Z|1\rangle$).

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

- State preparation (single qubit): either $|0\rangle$ or $|1\rangle$, "stabilised" by Z, $-Z$ respectively (i.e., equivalent to $Z|0\rangle$, $-Z|1\rangle$).
- Pauli gates (X, Y, Z) applied to Z:

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

- State preparation (single qubit): either $|0\rangle$ or $|1\rangle$, "stabilised" by Z, $-\mathsf{Z}$ respectively (i.e., equivalent to $\mathsf{Z}|0\rangle$, $-\mathsf{Z}|1\rangle$).
- Pauli gates (X, Y, Z) applied to Z: $\mathsf{XZX}^\dagger = -\mathsf{Z}$, $\mathsf{YZY}^\dagger = -\mathsf{Z}$, $\mathsf{ZZZ}^\dagger = \mathsf{Z}$.

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

- State preparation (single qubit): either $|0\rangle$ or $|1\rangle$, "stabilised" by Z, $-Z$ respectively (i.e., equivalent to $Z|0\rangle$, $-Z|1\rangle$).
- Pauli gates (X, Y, Z) applied to Z: $XZX^\dagger = -Z$, $YZY^\dagger = -Z$, $ZZZ^\dagger = Z$.
- Pauli gates applied to X and Y:

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

- State preparation (single qubit): either $|0\rangle$ or $|1\rangle$, "stabilised" by Z, $-\mathsf{Z}$ respectively (i.e., equivalent to $\mathsf{Z}|0\rangle$, $-\mathsf{Z}|1\rangle$).
- Pauli gates (X, Y, Z) applied to Z: $\mathsf{XZX}^\dagger = -\mathsf{Z}$, $\mathsf{YZY}^\dagger = -\mathsf{Z}$, $\mathsf{ZZZ}^\dagger = \mathsf{Z}$.
- Pauli gates applied to X and Y: $\mathsf{XXX}^\dagger = \mathsf{X}$, $\mathsf{YXY}^\dagger = -\mathsf{X}$, $\mathsf{ZXZ}^\dagger = -\mathsf{X}$, $\mathsf{XYX}^\dagger = -\mathsf{Y}$, $\mathsf{YYY}^\dagger = \mathsf{Y}$, $\mathsf{ZYZ}^\dagger = -\mathsf{Y}$.

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

- State preparation (single qubit): either $|0\rangle$ or $|1\rangle$, "stabilised" by Z, $-Z$ respectively (i.e., equivalent to $Z|0\rangle$, $-Z|1\rangle$).
- Pauli gates (X, Y, Z) applied to Z: $XZX^\dagger = -Z$, $YZY^\dagger = -Z$, $ZZZ^\dagger = Z$.
- Pauli gates applied to X and Y: $XXX^\dagger = X$, $YXY^\dagger = -X$, $ZXZ^\dagger = -X$, $XYX^\dagger = -Y$, $YYY^\dagger = Y$, $ZYZ^\dagger = -Y$.
- Hadamard gate (H):

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

- State preparation (single qubit): either $|0\rangle$ or $|1\rangle$, "stabilised" by Z, $-Z$ respectively (i.e., equivalent to $Z|0\rangle$, $-Z|1\rangle$).
- Pauli gates (X, Y, Z) applied to Z: $XZX^\dagger = -Z$, $YZY^\dagger = -Z$, $ZZZ^\dagger = Z$.
- Pauli gates applied to X and Y: $XXX^\dagger = X$, $YXY^\dagger = -X$, $ZXZ^\dagger = -X$, $XYX^\dagger = -Y$, $YYY^\dagger = Y$, $ZYZ^\dagger = -Y$.
- Hadamard gate (H): $HXH^\dagger = Z$, $HYH^\dagger = -Y$, and $HZH^\dagger = X$.

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

- State preparation (single qubit): either $|0\rangle$ or $|1\rangle$, "stabilised" by Z, $-Z$ respectively (i.e., equivalent to $Z|0\rangle$, $-Z|1\rangle$).
- Pauli gates (X, Y, Z) applied to Z: $XZX^\dagger = -Z$, $YZY^\dagger = -Z$, $ZZZ^\dagger = Z$.
- Pauli gates applied to X and Y: $XXX^\dagger = X$, $YXY^\dagger = -X$, $ZXZ^\dagger = -X$, $XYX^\dagger = -Y$, $YYY^\dagger = Y$, $ZYZ^\dagger = -Y$.
- Hadamard gate (H): $HXH^\dagger = Z$, $HYH^\dagger = -Y$, and $HZH^\dagger = X$.
- Phase gate (R):

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

- State preparation (single qubit): either $|0\rangle$ or $|1\rangle$, "stabilised" by Z, $-Z$ respectively (i.e., equivalent to $Z|0\rangle$, $-Z|1\rangle$).
- Pauli gates (X, Y, Z) applied to Z: $XZX^\dagger = -Z$, $YZY^\dagger = -Z$, $ZZZ^\dagger = Z$.
- Pauli gates applied to X and Y: $XXX^\dagger = X$, $YXY^\dagger = -X$, $ZXZ^\dagger = -X$, $XYX^\dagger = -Y$, $YYY^\dagger = Y$, $ZYZ^\dagger = -Y$.
- Hadamard gate (H): $HXH^\dagger = Z$, $HYH^\dagger = -Y$, and $HZH^\dagger = X$.
- Phase gate (R): $RXR^\dagger = Y$, $RYR^\dagger = X$, $RZR^\dagger = Z$.

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

- State preparation (single qubit): either $|0\rangle$ or $|1\rangle$, "stabilised" by Z, $-Z$ respectively (i.e., equivalent to $Z|0\rangle$, $-Z|1\rangle$).
- Pauli gates (X, Y, Z) applied to Z: $XZX^\dagger = -Z$, $YZY^\dagger = -Z$, $ZZZ^\dagger = Z$.
- Pauli gates applied to X and Y: $XXX^\dagger = X$, $YXY^\dagger = -X$, $ZXZ^\dagger = -X$, $XYX^\dagger = -Y$, $YYY^\dagger = Y$, $ZYZ^\dagger = -Y$.
- Hadamard gate (H): $HXH^\dagger = Z$, $HYH^\dagger = -Y$, and $HZH^\dagger = X$.
- Phase gate (R): $RXR^\dagger = Y$, $RYR^\dagger = X$, $RZR^\dagger = Z$.
- CNOT:

Analysis of the Gottesman-Knill operations

What do the GK operations have in common?

- State preparation (single qubit): either $|0\rangle$ or $|1\rangle$, "stabilised" by Z, $-Z$ respectively (i.e., equivalent to $Z|0\rangle$, $-Z|1\rangle$).
- Pauli gates (X, Y, Z) applied to Z: $XZX^\dagger = -Z$, $YZY^\dagger = -Z$, $ZZZ^\dagger = Z$.
- Pauli gates applied to X and Y: $XXX^\dagger = X$, $YXY^\dagger = -X$, $ZXZ^\dagger = -X$, $XYX^\dagger = -Y$, $YYY^\dagger = Y$, $ZYZ^\dagger = -Y$.
- Hadamard gate (H): $HXH^\dagger = Z$, $HYH^\dagger = -Y$, and $HZH^\dagger = X$.
- Phase gate (R): $RXR^\dagger = Y$, $RYR^\dagger = X$, $RZR^\dagger = Z$.
- CNOT: produces correlations, but is basically a controlled-X gate on the target qubit.

Analysis of the Gottesman-Knill operations

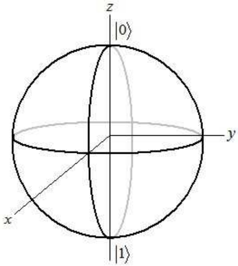
What do the GK operations have in common?

- State preparation (single qubit): either $|0\rangle$ or $|1\rangle$, "stabilised" by Z, $-Z$ respectively (i.e., equivalent to $Z|0\rangle$, $-Z|1\rangle$).
- Pauli gates (X, Y, Z) applied to Z: $XZX^\dagger = -Z$, $YZY^\dagger = -Z$, $ZZZ^\dagger = Z$.
- Pauli gates applied to X and Y: $XXX^\dagger = X$, $YXY^\dagger = -X$, $ZXZ^\dagger = -X$, $XYX^\dagger = -Y$, $YYY^\dagger = Y$, $ZYZ^\dagger = -Y$.
- Hadamard gate (H): $HXH^\dagger = Z$, $HYH^\dagger = -Y$, and $HZH^\dagger = X$.
- Phase gate (R): $RXR^\dagger = Y$, $RYR^\dagger = X$, $RZR^\dagger = Z$.
- CNOT: produces correlations, but is basically a controlled-X gate on the target qubit.

Combined effect of any sequence of only GK operations is equivalent to the measurement of one of the Pauli observables: $\pm X$, $\pm Y$, $\pm Z$ on either $|0\rangle$ or $|1\rangle$.

Pauli observables

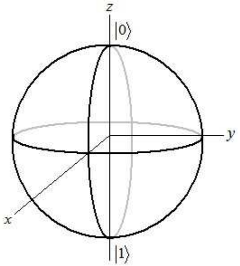
X, Y, Z: π rotations of the Bloch sphere about the x, y, and z axes respectively.

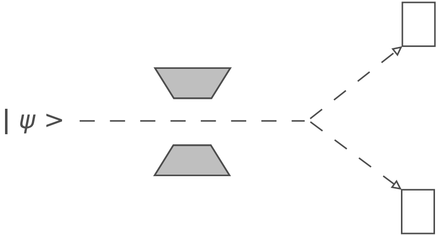


Pauli observables

X, Y, Z: π rotations of the Bloch sphere about the x, y, and z axes respectively.

Difference in orientations of different ends of a measurement apparatus: angle always proportional to $\pi/2$.



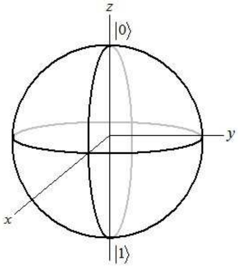


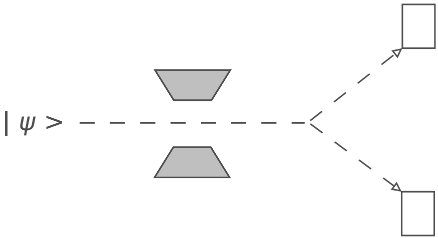
Pauli observables

X, Y, Z: π rotations of the Bloch sphere about the x, y, and z axes respectively.

Difference in orientations of different ends of a measurement apparatus: angle always proportional to $\pi/2$.

Precisely the orientations for which it is possible to provide a LHVT to reproduce the statistics associated with a Bell state.





Bell's theorem (CHSH inequality)

Assume outcomes of local experiments depend only on the local setup and on the value of a hidden variable λ assigned at state preparation (i.e. are described by a LHVT).

Bell's theorem (CHSH inequality)

Assume outcomes of local experiments depend only on the local setup and on the value of a hidden variable λ assigned at state preparation (i.e. are described by a LHVT). Then:

$$|\langle \sigma_m \otimes \sigma_n \rangle + \langle \sigma_m \otimes \sigma_{n'} \rangle| + |\langle \sigma_{m'} \otimes \sigma_n \rangle - \langle \sigma_{m'} \otimes \sigma_{n'} \rangle| \leq 2.$$

Bell's theorem (CHSH inequality)

Assume outcomes of local experiments depend only on the local setup and on the value of a hidden variable λ assigned at state preparation (i.e. are described by a LHVT). Then:

$$|\langle \sigma_m \otimes \sigma_n \rangle + \langle \sigma_m \otimes \sigma_{n'} \rangle| + |\langle \sigma_{m'} \otimes \sigma_n \rangle - \langle \sigma_{m'} \otimes \sigma_{n'} \rangle| \leq 2.$$

Violated by quantum mechanical statistics in general.

Bell's theorem (CHSH inequality)

Assume outcomes of local experiments depend only on the local setup and on the value of a hidden variable λ assigned at state preparation (i.e. are described by a LHVT). Then:

$$|\langle\sigma_m \otimes \sigma_n\rangle + \langle\sigma_m \otimes \sigma_{n'}\rangle| + |\langle\sigma_{m'} \otimes \sigma_n\rangle - \langle\sigma_{m'} \otimes \sigma_{n'}\rangle| \leq 2.$$

Violated by quantum mechanical statistics in general.

But <u>no conflict</u> when $\hat{m}$ and $\hat{n}$, $\hat{m}$ and $\hat{n}'$, $\hat{m}'$ and $\hat{n}$, and $\hat{m}'$ and $\hat{n}'$ are all oriented at angles $\propto \pi/2$.

Physical motivation for the GK theorem

- Measurement statistics on systems subjected to only GK operations are recoverable by a LHVT.
- But joint experiments in an LHVT can be described using product states, hence “compressible”.
- So unsurprising that these operations are efficiently simulable with a classical computer.

The GHZ argument

Cf. Greenberger, Horne, & Zeilenger (1989); Greenberger, Horne, Shimony, & Zeilenger (1990); Mermin (1990); Clifton, Redhead, & Butterfield (1991)

Demonstrates an incompatibility between the predictions of certain LHVTs and QM predictions.

- uses measurements of Pauli observables exclusively,

The GHZ argument

Consider three spatially separated (in the same plane) spin-1/2 systems a, b, c are in the state:

$$|\mathrm{GHZ}\rangle_3 = \frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b|0\rangle_c + |1\rangle_a|1\rangle_b|1\rangle_c).$$

The GHZ argument

Consider three spatially separated (in the same plane) spin-1/2 systems a, b, c are in the state:

$$|\mathrm{GHZ}\rangle_3 = \frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b|0\rangle_c + |1\rangle_a|1\rangle_b|1\rangle_c).$$

Show that a LHVT predicts that

$$v(X^a \otimes X^b \otimes X^c) = v(X^a) \cdot v(X^b) \cdot v(X^c) = -1.$$

The GHZ argument

Consider three spatially separated (in the same plane) spin-1/2 systems a, b, c are in the state:

$$|\mathrm{GHZ}\rangle_3 = \frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b|0\rangle_c + |1\rangle_a|1\rangle_b|1\rangle_c).$$

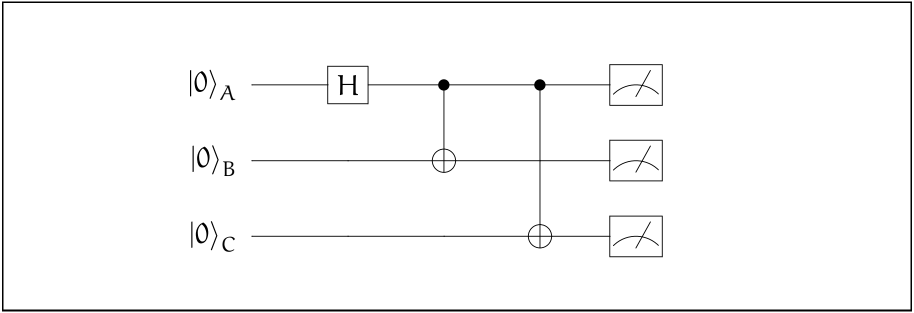
Show that a LHVT predicts that

$$v(X^a \otimes X^b \otimes X^c) = v(X^a) \cdot v(X^b) \cdot v(X^c) = -1.$$

Point out that this contradicts quantum mechanical prediction of:

$$v(X^a \otimes X^b \otimes X^c) = 1.$$

Quantum circuit diagram representation of the GHZ argument



Implements:

$$\text{CNOT}_{13}\text{CNOT}_{12}\text{H}_1|0\rangle|0\rangle|0\rangle.$$

All of these (including subsequent X, Y measurements) are allowed GK operations.

Physical motivation for the GK theorem??

- Measurement statistics on systems subjected to only GK operations are recoverable by a LHVT??

HVT to recover GHZ_3 predictions (Tessier, 2004; Tessier et al., 2005)

	q_A	q_B	q_C
X	R_2R_3	R_2	R_3
Y	$iR_1R_2R_3$	iR_1R_2	iR_1R_3
Z	R_1	R_1	R_1
I	1	1	1

- q_A, q_B, and q_C: qubits for Alice, Bob, Chris.
- R_k: random variables; take a value of ± 1 with equal probability (interpreted epistemically).
- $R_k^2 = (\pm 1)^2 = 1$.

HVT to recover GHZ_3 predictions (Tessier, 2004; Tessier et al., 2005)

	q_A	q_B	q_C
X	R_2R_3	R_2	R_3
Y	$iR_1R_2R_3$	iR_1R_2	iR_1R_3
Z	R_1	R_1	R_1
I	1	1	1

Determining measurement outcomes:

- $v(XXX) = R_2R_3R_2R_3 = 1$
- $v(XYY) = R_2R_3iR_1R_2iR_1R_3 = i^2 = -1$
- $v(YYX) = iR_1R_2R_3iR_1R_2R_3 = i^2 = -1$
- $v(XYI) = R_2R_3iR_1R_2 = \pm i \Rightarrow \pm 1$
- etc.

HVT to recover GHZ_3 predictions (Tessier, 2004; Tessier et al., 2005)

	q_A	q_B	q_C
X	R_2R_3	R_2	R_3
Y	$iR_1R_2R_3$	iR_1R_2	iR_1R_3
Z	R_1	R_1	R_1
I	1	1	1

Determining measurement outcomes:

- $v(XXX) = R_2R_3R_2R_3 = 1$
- $v(XYY) = R_2R_3iR_1R_2iR_1R_3 = i^2 = -1$
- $v(YYX) = iR_1R_2R_3iR_1R_2R_3 = i^2 = -1$
- $v(XYI) = R_2R_3iR_1R_2 = \pm i \Rightarrow \pm 1$
- etc.

Recovers all of the predictions of quantum mechanics for any product of Pauli experiments on the GHZ_3 state.

HVT to recover GHZ_3 predictions (Tessier, 2004; Tessier et al., 2005)

	q_A	q_B	q_C
X	R_2R_3	R_2	R_3
Y	$iR_1R_2R_3$	iR_1R_2	iR_1R_3
Z	R_1	R_1	R_1
I	1	1	1

Problem: outcomes are inconsistent with one another.

E.g.,

$$\begin{aligned} v(XYY) &= R_2R_3iR_1R_2iR_1R_3 = -1 \\ &\neq v(XII) \times v(IYI) \times v(IIY) = (R_2R_3)(R_1R_2)(R_1R_3) = 1 \end{aligned}$$

HVT to recover GHZ_3 predictions (Tessier, 2004; Tessier et al., 2005)

	q_A	q_B	q_C
X	$R_2 R_3$	R_2	R_3
Y	$iR_1 R_2 R_3$	$iR_1 R_2$	$iR_1 R_3$
Z	R_1	R_1	R_1
I	1	1	1

Solution: add a wee bit of signalling.

- Bob agrees to send a single classical bit to Alice: 0 if Bob measured Y or 1 otherwise.
- Alice flips the sign of her local outcome if one of she or Bob measure Y.

HVT to recover GHZ_3 predictions (Tessier, 2004; Tessier et al., 2005)

	q_A	q_B	q_C
X	R_2R_3	R_2	R_3
Y	$iR_1R_2R_3$	iR_1R_2	iR_1R_3
Z	R_1	R_1	R_1
I	1	1	1

Solution: add a wee bit of signalling.

- Bob agrees to send a single classical bit to Alice: 0 if Bob measured Y or 1 otherwise.
- Alice flips the sign of her local outcome if one of she or Bob measure Y.
- $XII \times IYI \times IIY = (R_2R_3)(R_1R_2)(R_1R_3) = 1.$

HVT to recover GHZ_3 predictions (Tessier, 2004; Tessier et al., 2005)

	q_A	q_B	q_C
X	R_2R_3	R_2	R_3
Y	$iR_1R_2R_3$	iR_1R_2	iR_1R_3
Z	R_1	R_1	R_1
I	1	1	1

Solution: add a wee bit of signalling.

- Bob agrees to send a single classical bit to Alice: 0 if Bob measured Y or 1 otherwise.
- Alice flips the sign of her local outcome if one of she or Bob measure Y.
- $XII \times IYI \times IIY = (-R_2R_3)(R_1R_2)(R_1R_3) = -1$.
- Consistent both with outcome of XYY and with outcomes for XII, IYI, and IIY.

HVT to recover GHZ_3 predictions (Tessier, 2004; Tessier et al., 2005)

	q_A	q_B	q_C
X	R_2R_3	R_2	R_3
Y	$iR_1R_2R_3$	iR_1R_2	iR_1R_3
Z	R_1	R_1	R_1
I	1	1	1

Solution: add a wee bit of signalling.

- Bob agrees to send a single classical bit to Alice: 0 if Bob measured Y or 1 otherwise.
- Alice flips the sign of her local outcome if one of she or Bob measure Y.
- $XII \times IYI \times IIY = (-R_2R_3)(R_1R_2)(R_1R_3) = -1$.
- Consistent both with outcome of XYY and with outcomes for XII, IYI, and IIY.
- All measurement outcomes can be made consistent in this way.

Recovering GHZ_n predictions

Scheme generalises:

Recovering GHZ_n predictions

Scheme generalises:

$$\frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} \pm |1\rangle^{\otimes n}),$$

- For n-qubit GHZ state $n - 2$ bits of classical communication required to accurately model the statistics associated with measurements of Pauli observables.

Recovering Gottesman-Knill predictions

Scheme generalises:

$$\frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} \pm |1\rangle^{\otimes n}),$$

- For n-qubit GHZ state $n - 2$ bits of classical communication required to accurately model the statistics associated with measurements of Pauli observables.
- Also true for any circuit consisting exclusively of Gottesman-Knill operations (details given in Tessier 2004).

Recovering Gottesman-Knill predictions

Scheme generalises:

$$\frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} \pm |1\rangle^{\otimes n}),$$

- For n-qubit GHZ state $n-2$ bits of classical communication required to accurately model the statistics associated with measurements of Pauli observables.
- Also true for any circuit consisting exclusively of Gottesman-Knill operations (details given in Tessier 2004).
- Scheme no longer works for non-GK operations. Amount of classical communication conjectured to grow exponentially (Tessier, 2004).

Tessier (2004) on the significance of the GK theorem

Our results yield an alternative perspective on the GK theorem, and demonstrate that we may replace the nonlocal hidden variables represented by the stabilizer generators with LHVs and an amount of classical communication that scales efficiently with the size of the problem. This is a general feature of quantum circuits obeying the constraints of the GK theorem since, as our model illustrates, such circuits do not utilize the full capabilities of the available entanglement in the probability distributions that they generate (Tessier, 2004, 103).

Tessier (2004) on the significance of the GK theorem

The success of our simulation provides strong evidence that the power of quantum computation arises not directly from entanglement, but rather from the nonexistence of an efficient, local realistic description of the computation, even when supplemented by an efficient amount of nonlocal, but classical communication (Tessier, 2004, 117).

Tessier (2004) on the significance of the GK theorem

The success of our simulation provides strong evidence that the power of quantum computation arises not directly from entanglement, but rather from the nonexistence of an efficient, local realistic description of the computation, even when supplemented by an efficient amount of nonlocal, but classical communication (Tessier, 2004, 117).

Tessier (2004) on the significance of the GK theorem

Our results yield an alternative perspective on the GK theorem, and demonstrate that we may replace the nonlocal hidden variables represented by the stabilizer generators with LHVs and an amount of classical communication that scales efficiently with the size of the problem. This is a general feature of quantum circuits obeying the constraints of the GK theorem since, as our model illustrates, such circuits do not utilize the full capabilities of the available entanglement in the probability distributions that they generate (Tessier, 2004, 103).

Correlations between R_k arise from local interactions

$|000\rangle$

Correlations between R_k arise from local interactions

	q_A	q_B	q_C
X	R_1	R_2	R_3
Y	$-iR_1$	iR_2	iR_3
Z	1	1	1
I	1	1	1

$|000\rangle$

Correlations between R_k arise from local interactions

	q_A	q_B	q_C
X	R_1	R_2	R_3
Y	$-iR_1$	iR_2	iR_3
Z	1	1	1
I	1	1	1

$\xrightarrow{H_A}$

	q_A	q_B	q_C
X	1	R_2	R_3
Y	iR_1	iR_2	iR_3
Z	R_1	1	1
I	1	1	1

$$|000\rangle \xrightarrow{H_A} \frac{(|0\rangle + |1\rangle)|00\rangle}{\sqrt{2}}$$

Correlations between R_k arise from local interactions

	q_A	q_B	q_C
X	R_1	R_2	R_3
Y	$-iR_1$	iR_2	iR_3
Z	1	1	1
I	1	1	1

$\xrightarrow{H_A}$

	q_A	q_B	q_C
X	1	R_2	R_3
Y	iR_1	iR_2	iR_3
Z	R_1	1	1
I	1	1	1

$\xrightarrow{CNOT_{AB}}$

	q_A	q_B	q_C
X	R_2	R_2	R_3
Y	iR_1R_2	iR_1R_2	iR_3
Z	R_1	R_1	1
I	1	1	1

$$|000\rangle \xrightarrow{H_A} \frac{(|0\rangle + |1\rangle)|00\rangle}{\sqrt{2}} \xrightarrow{CNOT_{AB}} \frac{(|00\rangle + |11\rangle)|0\rangle}{\sqrt{2}}$$

Correlations between R_k arise from local interactions

	q_A	q_B	q_C
X	R_1	R_2	R_3
Y	$-iR_1$	iR_2	iR_3
Z	1	1	1
I	1	1	1

$\xrightarrow{H_A}$

	q_A	q_B	q_C
X	1	R_2	R_3
Y	iR_1	iR_2	iR_3
Z	R_1	1	1
I	1	1	1

$\xrightarrow{CNOT_{AB}}$

	q_A	q_B	q_C
X	R_2	R_2	R_3
Y	iR_1R_2	iR_1R_2	iR_3
Z	R_1	R_1	1
I	1	1	1

$\xrightarrow{CNOT_{AC}}$

	q_A	q_B	q_C
X	R_2R_3	R_2	R_3
Y	$iR_1R_2R_3$	iR_1R_2	iR_1R_3
Z	R_1	R_1	R_1
I	1	1	1

$$|000\rangle \xrightarrow{H_A} \frac{(|0\rangle + |1\rangle)|00\rangle}{\sqrt{2}} \xrightarrow{CNOT_{AB}} \frac{(|00\rangle + |11\rangle)|0\rangle}{\sqrt{2}}$$
$$\xrightarrow{CNOT_{AC}} \frac{(|000\rangle + |111\rangle)}{\sqrt{2}}.$$

Outcomes completely determined by R_k

R_1	R_2	R_3	"XYY" $R_2R_3iR_1R_2iR_1R_3$	"YXY" $iR_1R_2R_3R_2iR_1R_3$	"YYX" $iR_1R_2R_3iR_1R_2R_3$	"XXX" $R_2R_3R_2R_3$
+1	+1	+1	−1	−1	−1	+1
+1	+1	−1	−1	−1	−1	+1
+1	−1	+1	−1	−1	−1	+1
+1	−1	−1	−1	−1	−1	+1
−1	+1	+1	−1	−1	−1	+1
−1	+1	−1	−1	−1	−1	+1
−1	−1	+1	−1	−1	−1	+1
−1	−1	−1	−1	−1	−1	+1

R_1	R_2	R_3	"XII" R_2R_3	"IYI" iR_1R_2	"IIY" iR_1R_3	...
+1	+1	+1	+1	+1	+1	
+1	+1	−1	−1	+1	−1	
+1	−1	+1	−1	−1	+1	
+1	−1	−1	+1	−1	−1	
−1	+1	+1	+1	−1	−1	
−1	+1	−1	−1	−1	+1	
−1	−1	+1	−1	+1	−1	
−1	−1	−1	+1	+1	+1	

Outcomes not completely determined by R_k

			"XYY"	"YXY"	"YYX"	"XXX"
R_1	R_2	R_3	$R_2R_3iR_1R_2iR_1R_3$	$iR_1R_2R_3R_2iR_1R_3$	$iR_1R_2R_3iR_1R_2R_3$	$R_2R_3R_2R_3$
$+1$	$+1$	$+1$	-1	-1	-1	$+1$
$+1$	$+1$	-1	-1	-1	-1	$+1$
$+1$	-1	$+1$	-1	-1	-1	$+1$
$+1$	-1	-1	-1	-1	-1	$+1$
-1	$+1$	$+1$	-1	-1	-1	$+1$
-1	$+1$	-1	-1	-1	-1	$+1$
-1	-1	$+1$	-1	-1	-1	$+1$
-1	-1	-1	-1	-1	-1	$+1$

			"XII"	"IYI"	"IIY"	…
R_1	R_2	R_3	R_2R_3	iR_1R_2	iR_1R_3	
$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	
$+1$	$+1$	-1	-1	$+1$	-1	
$+1$	-1	$+1$	-1	-1	$+1$	
$+1$	-1	-1	$+1$	-1	-1	
-1	$+1$	$+1$	$+1$	-1	-1	
-1	$+1$	-1	-1	-1	$+1$	
-1	-1	$+1$	-1	$+1$	-1	
-1	-1	-1	$+1$	$+1$	$+1$	

Outcomes not completely determined by R_k

"Local hidden variables [(R_k)] and an amount of classical communication that scales efficiently with the size of the problem."

- Not true. The i terms interfere nonlocally.

Outcomes not completely determined by $\mathsf{R_k}$

"Local hidden variables [$(\mathsf{R_k})$] and an amount of classical communication that scales efficiently with the size of the problem."

- Not true. The i terms interfere nonlocally.
- True only if every joint measurement is interpreted as "really" just a product measurement. E.g., "XYY" $=_{\mathsf{df}}$ XII · IYI · IIY.

Outcomes not completely determined by R_k

R_1	R_2	R_3	"XYY" $R_2R_3iR_1R_2iR_1R_3$	"YXY" $iR_1R_2R_3R_2iR_1R_3$	"YYX" $iR_1R_2R_3iR_1R_2R_3$	"XXX" $R_2R_3R_2R_3$
+1	+1	+1	−1	−1	−1	+1
+1	+1	−1	−1	−1	−1	+1
+1	−1	+1	−1	−1	−1	+1
+1	−1	−1	−1	−1	−1	+1
−1	+1	+1	−1	−1	−1	+1
−1	+1	−1	−1	−1	−1	+1
−1	−1	+1	−1	−1	−1	+1
−1	−1	−1	−1	−1	−1	+1

R_1	R_2	R_3	"XII" R_2R_3	"IYI" iR_1R_2	"IIY" iR_1R_3	…
+1	+1	+1	+1	+1	+1	
+1	+1	−1	−1	+1	−1	
+1	−1	+1	−1	−1	+1	
+1	−1	−1	+1	−1	−1	
−1	+1	+1	+1	−1	−1	
−1	+1	−1	−1	−1	+1	
−1	−1	+1	−1	+1	−1	
−1	−1	−1	+1	+1	+1	

Outcomes <u>not</u> completely determined by $\mathsf{R_k}$

"Local hidden variables [($\mathsf{R_k}$)] and an amount of classical communication that scales efficiently with the size of the problem."

- Not true. The i terms interfere nonlocally.
- True only if every joint measurement is interpreted as "really" just a product measurement. E.g., "XYY" $=_{\mathsf{df}}$ XII · IYI · IIY.
- But then the i terms are never used and have no place in the model (classical communication is their replacement).

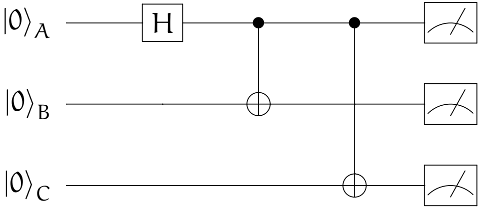
Outcomes <u>not</u> completely determined by $\mathsf{R_k}$

"Local hidden variables [($\mathsf{R_k}$)] and an amount of classical communication that scales efficiently with the size of the problem."

- Not true. The $\mathfrak{i}$ terms interfere nonlocally.
- True only if every joint measurement is interpreted as "really" just a product measurement. E.g., "XYY" $=_{\mathsf{df}}$ $\mathsf{XII} \cdot \mathsf{IYI} \cdot \mathsf{IIY}$.
- But then the $\mathfrak{i}$ terms are never used and have no place in the model (classical communication is their replacement).

Is there a better, more illuminating, way to understand the significance of this model?

Received interpretation of the model



$R_2 R_3$	"XII"
$i R_1 R_2$	"IYI"
$i R_1 R_3$	"IIY"

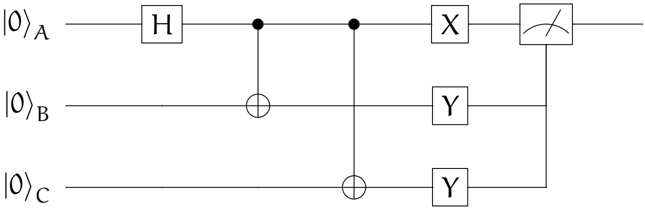
Interfering i terms represent a nonlocal influence.

- Yield contextual measurement outcomes:

$$\begin{aligned} \nu(XYY) &= R_2 R_3 i R_1 R_2 i R_1 R_3 = -1 \\ &\neq \nu(XII) \times \nu(IYI) \times \nu(IIY) = (R_2 R_3)(R_1 R_2)(R_1 R_3) = 1 \end{aligned}$$

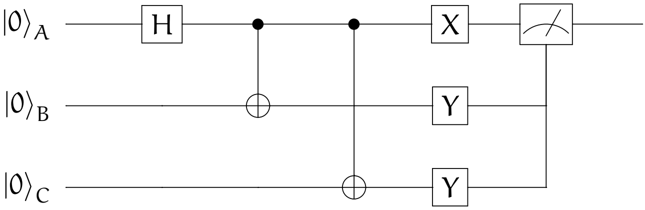
- Contextuality is eliminated using efficient classical communication $\Rightarrow$ failure of parameter independence.

Reinterpreting the model



Actually observing the results of a joint measurement involves combining the individual measurement outcomes.

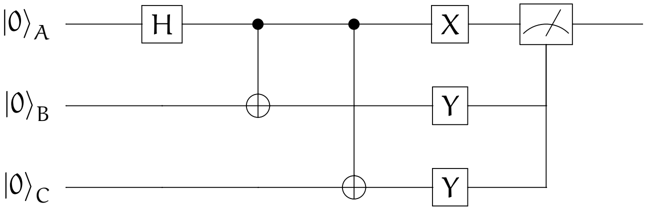
Reinterpreting the model



Actually observing the results of a joint measurement involves combining the individual measurement outcomes.

- Classical communication occurs at some point during the past light cone of this measurement event.

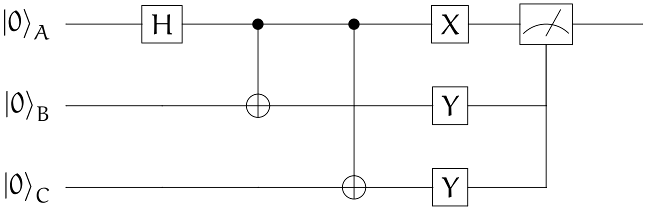
Reinterpreting the model



Actually observing the results of a joint measurement involves combining the individual measurement outcomes.

- Classical communication occurs at some point during the past light cone of this measurement event.
- From this point of view, mutual influences on measurement outcomes are no longer nonlocal.

Reinterpreting the model



Actually observing the results of a joint measurement involves combining the individual measurement outcomes.

- Classical communication occurs at some point during the past light cone of this measurement event.
- From this point of view, mutual influences on measurement outcomes are no longer nonlocal.
- Interpreted this way the model is a LHVT.

Objections

- This LHVT is ad hoc.

Objections

- This LHVT is ad hoc. **Yes.**

Objections

- This LHVT is ad hoc. **Yes.**
- This LHVT is conspiratorial.

Objections

- This LHVT is ad hoc. **Yes.**
- This LHVT is conspiratorial. **Yes.**

Objections

- This LHVT is ad hoc. **Yes.**
- This LHVT is conspiratorial. **Yes.**
- This LHVT doesn't faithfully represent the situation according to quantum mechanics.

Objections

- This LHVT is ad hoc. **Yes.**
- This LHVT is conspiratorial. **Yes.**
- This LHVT doesn't faithfully represent the situation according to quantum mechanics. **True.**

Explicating the notion of a local hidden variables theory

What question are we answering with a LHVT?

Explicating the notion of a local hidden variables theory

- Theoretical question: does QM approximate some deeper underlying theory of the world? (and if so, what is that theory?)

Explicating the notion of a local hidden variables theory

- Theoretical question: does QM approximate some deeper underlying theory of the world? (and if so, what is that theory?)
  - Answers to this question must be very serious.

Explicating the notion of a local hidden variables theory

- Theoretical question: does QM approximate some deeper underlying theory of the world? (and if so, what is that theory?)
  - Answers to this question must be very serious.
  - Must satisfy plausibility constraints: E.g., consistency with our other physical theories (or at least a plausible reason why those should be modified).

Explicating the notion of a local hidden variables theory

- Theoretical question: does QM approximate some deeper underlying theory of the world? (and if so, what is that theory?)
  - Answers to this question must be very serious.
  - Must satisfy plausibility constraints: E.g., consistency with our other physical theories (or at least a plausible reason why those should be modified).
  - Most "loopholes" to the Aspect et al. (1981, 1982a,b) experiments do not satisfy these plausibility constraints and are ruled out of consideration on these grounds.

Explicating the notion of a local hidden variables theory

- Theoretical question: does QM approximate some deeper underlying theory of the world? (and if so, what is that theory?)
  - Answers to this question must be very serious.
  - Must satisfy plausibility constraints: E.g., consistency with our other physical theories (or at least a plausible reason why those should be modified).
  - Most "loopholes" to the Aspect et al. (1981, 1982a,b) experiments do not satisfy these plausibility constraints and are ruled out of consideration on these grounds.
- Purely conceptual question: what is logically possible and still consistent with the predictions of quantum mechanics?
  - Toy theories: no plausibility constraints whatsoever.
  - Useful for making conceptual points; e.g., outcome independence $\neq$ separability (Maudlin, 2011).

Explicating the notion of a local hidden variables theory

- Practical question:

Explicating the notion of a local hidden variables theory

- Practical question: what can we do in order to reproduce the predictions of quantum mechanics.

Explicating the notion of a local hidden variables theory

- Practical question: what can we do in order to reproduce the predictions of quantum mechanics.
  - Plausibility constraints: must be Turing computable.

Explicating the notion of a local hidden variables theory

- Practical question: what can we do in order to reproduce the predictions of quantum mechanics.
  - Plausibility constraints: must be efficiently Turing computable.

Explicating the notion of a local hidden variables theory

- Practical question: what can we do in order to reproduce the predictions of quantum mechanics.
  - Plausibility constraints: must be efficiently Turing computable.
  - We aim to capture the observables, not the beables.

Objections

- But is this LHVT really efficient? In what sense?

Objections

- But is this LHVT really efficient? In what sense?
  - **Yes it is.** A system described by this LHVT will produce the same actually observed (Pauli) measurement statistics as a quantum mechanical one with a number of additional resources that is polynomial (indeed, linear!) in n.

Objections

- But is this LHVT really efficient? In what sense?
  - **Yes it is.** A system described by this LHVT will produce the same actually observed (Pauli) measurement statistics as a quantum mechanical one with a number of additional resources that is polynomial (indeed, linear!) in n.
  - I.e. it is no harder for this LHVT than it is for a quantum system.

The GHZ argument

Consider three spatially separated (in the same plane) spin-1/2 systems a, b, c are in the state:

$$|\text{GHZ}\rangle_3 = \frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b|0\rangle_c + |1\rangle_a|1\rangle_b|1\rangle_c).$$

Show that a LHVT predicts that

$$v(X^a \otimes X^b \otimes X^c) = v(X^a) \cdot v(X^b) \cdot v(X^c) = -1.$$

Point out that this contradicts quantum mechanical prediction of:

$$v(X^a \otimes X^b \otimes X^c) = 1.$$

The significance of the GHZ argument

This is an altogether more powerful refutation of the existence of elements of reality than the one provided by Bell's theorem for the two-particle EPR experiment. Bell showed that the elements of reality inferred from one group of measurements are incompatible with the statistics produced by a second group of measurements. Such a refutation cannot be accomplished in a single run, but is built up with increasing confidence as the number of runs increases [...] In the GHZ experiment, on the other hand, the elements of reality require a class of outcomes to occur all of the time, while quantum mechanics never allows them to occur. [...] I recently declared in writing that no set of experiments, real or gedanken, was known that could produce such an all-or-nothing demolition of the elements of reality. With a bow of admiration to Greenberger, Horne and Zeilinger, I hereby recant (Mermin, 1990).

The significance of the GHZ argument

Is GHZ's argument more powerful than Bell's (in Mermin's sense)?

The significance of the GHZ argument

Is GHZ's argument more powerful than Bell's (in Mermin's sense)?

- From a theoretical point of view:

- From a practical point of view?

The significance of the GHZ argument

Is GHZ's argument more powerful than Bell's (in Mermin's sense)?

- From a theoretical point of view:
  - Perhaps (though see Clifton et al. 1991).
- From a practical point of view?

The significance of the GHZ argument

Is GHZ's argument more powerful than Bell's (in Mermin's sense)?

- From a theoretical point of view:
  - Perhaps (though see Clifton et al. 1991).
- From a practical point of view?
  - No. It is less powerful. (at least in its original form).

The significance of the GHZ argument

Is GHZ's argument more powerful than Bell's (in Mermin's sense)?

- From a theoretical point of view:
  - Perhaps (though see Clifton et al. 1991).
- From a practical point of view?
  - No. It is less powerful. (at least in its original form).
  - Real contradiction arises only for general measurements (i.e., those outside the group of Pauli measurements). These can't be reproduced efficiently.

The significance of the GHZ argument

Is GHZ's argument more powerful than Bell's (in Mermin's sense)?

- From a theoretical point of view:
  - Perhaps (though see Clifton et al. 1991).
- From a practical point of view?
  - No. It is less powerful. (at least in its original form).
  - Real contradiction arises only for general measurements (i.e., those outside the group of Pauli measurements). These can't be reproduced efficiently.
  - But this contradiction is only statistical, so GHZ's argument is no more powerful than Bell's argument.

Two senses of sufficiency

1. Simply possessing an entangled state is sufficient for speedup.

2. Entanglement is sufficient as a resource to enable speedup

.

Two senses of sufficiency

1. Simply possessing an entangled state is sufficient for speedup. False.

2. Entanglement is sufficient as a resource to enable speedup

.

Two senses of sufficiency

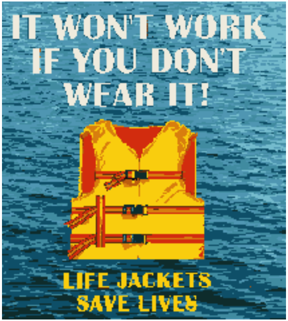
1. Simply possessing an entangled state is sufficient for speedup. False.

2. Entanglement is sufficient as a resource to enable speedup (denied by Jozsa & Linden).

Two senses of sufficiency

1. Simply possessing an entangled state is sufficient for speedup. False.

2. Entanglement is sufficient as a resource to enable speedup (denied by Jozsa & Linden). True.



Outline

1. Introduction.
2. The Gottesman-Knill theorem.
3. Analysis of the Gottesman-Knill operations.
   i. The CHSH inequality.
   ii. The GHZ argument.
4. Conclusion.

Works Cited I

Aspect, A., Dalibard, J., & Roger, G. (1982a). Experimental test of Bell's inequalities using time-varying analyzers. Physical Review Letters, 49, 1804–1807.

Aspect, A., Grangier, P., & Roger, G. (1981). Experimental tests of realistic local theories via Bell's theorem. Physical Review Letters, 47, 460–463.

Aspect, A., Grangier, P., & Roger, G. (1982b). Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment : A new violation of Bell's inequalities. Physical Review Letters, 49, 91–94.

Clifton, R. K., Redhead, M. L. G., & Butterfield, J. N. (1991). Generalization of the greenberger-horne-zeilinger algebraic proof of nonlocality. Foundations of Physics, 21, 149–184.

Greenberger, D. M., Horne, M. A., Shimony, A., & Zeilenger, A. (1990). Bell's theorem without inequalities. American Journal of Physics, 58, 1131–1143.

Greenberger, D. M., Horne, M. A., & Zeilenger, A. (1989). Going beyond Bell's theorem. In M. Kafatos (Ed.) Bell's Theorem, Quantum Theory and Conceptions of the Universe, (pp. 69–72). Dordrecht: Kluwer Academic Publishers.

Jozsa, R., & Linden, N. (2003). On the role of entanglement in quantum-computational speed-up. Proceedings of the Royal Society of London. Series A. Mathematical, Physical and Engineering Sciences, 459, 2011–2032.

Maudlin, T. (2011). Quantum Non-Locality and Relativity. Cambridge, MA: Wiley-Blackwell, third ed.

Works Cited II

Mermin, N. D. (1990). What's wrong with these elements of reality? Physics Today, 43, 9–11.

Tessier, T. E. (2004). Complementarity and Entanglement in Quantum Information Theory. Ph.D. thesis, The University of New Mexico, Albuquerque, New Mexico.

Tessier, T. E., Caves, C. M., Deutsch, I. H., & Eastin, B. (2005). Optimal classical-communication-assisted local model of n-qubit greenberger-horne-zeilinger correlations. Physical Review A, 72, 032305.