Analogies and Disanalogies Between Classical and Quantum Physical Computation

Michael E. Cuffaro[†]

[†]Munich Center for Mathematical Philosophy, LMU Munich
Michael.Cuffaro@lmu.de

November 25, 2024

Politecnico di Milano, Milan, Italy

Powered by LaTeX

I. Introduction

What is quantum computing?

- Combines fundamental concepts from two separate sciences: (1) Computer science and (2) Physics.

What is quantum computing?

- Combines fundamental concepts from two separate sciences: (1) Computer science and (2) Physics.
- Quantum computing describes computational models which are specified using the abstract language associated with quantum mechanics (QM), as opposed to the abstract language associated with classical mechanics (CM).

What's so special about quantum computers?

What's so special about quantum computers?

- They give us insight into the differences between CM and QM.

What's so special about quantum computers?

- They give us insight into the differences between CM and QM.
- Quantum computers are (in principle) capable of easily carrying out tasks that are generally accepted to be hard for a classical computer.
  - E.g., factoring, unstructured search.

What's so special about quantum computers?

- They give us insight into the differences between CM and QM.
- Quantum computers are (in principle) capable of easily carrying out tasks that are generally accepted to be hard for a classical computer.
  - E.g., factoring, unstructured search.

Challenges

- Building scalable quantum computers requires that we deal with external "noise" which causes computational errors.

What's so special about quantum computers?

- They give us insight into the differences between CM and QM.
- Quantum computers are (in principle) capable of easily carrying out tasks that are generally accepted to be hard for a classical computer.
  - E.g., factoring, unstructured search.

Challenges

- Building scalable quantum computers requires that we deal with external "noise" which causes computational errors.
- Fault-tolerant computational models have been devised, but so far there has been relatively little progress in scaling them up.

What's so special about quantum computers?

- They give us insight into the differences between CM and QM.
- Quantum computers are (in principle) capable of easily carrying out tasks that are generally accepted to be hard for a classical computer.
  - E.g., factoring, unstructured search.

Challenges

- Building scalable quantum computers requires that we deal with external "noise" which causes computational errors.
- Fault-tolerant computational models have been devised, but so far there has been relatively little progress in scaling them up.

Noisy Intermediate-Scale Quantum computing (NISQ)

- NISQ is a near-term workaround that focuses on hardware components and problems that are inherently less sensitive to noise (e.g., simulation, sampling).

II. Computational complexity theory

Effective procedure (informal):

- Finite number of finite-length instructions

Effective procedure (informal):

- Finite number of finite-length instructions
- If followed exactly by a human being using nothing other than paper and pencil,

Effective procedure (informal):

- Finite number of finite-length instructions
- If followed exactly by a human being using nothing other than paper and pencil, guaranteed to produce a result in a finite number of steps.

p	q	$\sim(p \vee q) \rightarrow (\sim p \,\&\, \sim q)$
0	0	1
0	1	1
1	0	1
1	1	1

Effective procedure (informal):

- Finite number of finite-length instructions
- If followed exactly by a human being using nothing other than paper and pencil, guaranteed to produce a result in a finite number of steps.
  - Example: Truth-table method (in sentential logic)

p	q	$\sim(p \vee q) \rightarrow (\sim p \,\&\, \sim q)$
0	0	1
0	1	1
1	0	1
1	1	1

Effective procedure (informal):

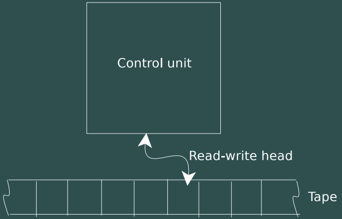
- Finite number of finite-length instructions
- If followed exactly by a human being using nothing other than paper and pencil, guaranteed to produce a result in a finite number of steps.
    - Example: Truth-table method (in sentential logic)
- Informal characterisation of human computation

Entscheidungsproblem (Decision problem):

- Give an effective procedure to decide whether an arbitrary expression in first-order logic is provable from the axioms (Hilbert & Ackermann, 1928, Pt. III).

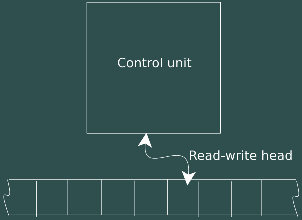
Entscheidungsproblem (Decision problem):

- Give an effective procedure to decide whether an arbitrary expression in first-order logic is provable from the axioms (Hilbert & Ackermann, 1928, Pt. III).
- Turing (1936-7) showed that there is no general solution.



Entscheidungsproblem (Decision problem):

- Give an effective procedure to decide whether an arbitrary expression in first-order logic is provable from the axioms (Hilbert & Ackermann, 1928, Pt. III).
- Turing (1936-7) showed that there is no general solution.
- Utilised Turing's thesis: any effectively calculable function can be computed by an automatic machine.



Entscheidungsproblem (Decision problem):

- Give an effective procedure to decide whether an arbitrary expression in first-order logic is provable from the axioms (Hilbert & Ackermann, 1928, Pt. III).
- Turing (1936-7) showed that there is no general solution.
- Utilised Turing's thesis: any effectively calculable function can be computed by an automatic machine.
- Turing machine: Captures what is essential about the process of human computation

Computability theory

- Concerns what can be computed in principle.
- Distinguishes between problems that can be computed and those that cannot.

Computability theory

- Concerns what can be computed in principle.
- Distinguishes between problems that can be computed and those that cannot.

Computational complexity theory

- Distinguishes computational problems on the basis of their resource costs (in time and space).

Computability theory

- Concerns what can be computed in principle.
- Distinguishes between problems that can be computed and those that cannot.

Computational complexity theory

- Distinguishes computational problems on the basis of their resource costs (in time and space).
- Cobham-Edmonds thesis: A decision problem is tractable if it is solvable in "polynomial time", intractable if it is not.

Computability theory

- Concerns what can be computed in principle.
- Distinguishes between problems that can be computed and those that cannot.

Computational complexity theory

- Distinguishes computational problems on the basis of their resource costs (in time and space).
- Cobham-Edmonds thesis: A decision problem is tractable if it is solvable in "polynomial time", intractable if it is not.
  - Example of a polynomial function: $5n^6 + 4n^2 + 3n + 2$.
  - Not a polynomial: $2^{n^k} + \ldots$ ("exponential")

Computability theory

- Concerns what can be computed in principle.
- Distinguishes between problems that can be computed and those that cannot.

Computational complexity theory

- Distinguishes computational problems on the basis of their resource costs (in time and space).
- Cobham-Edmonds thesis: A decision problem is tractable if it is solvable in "polynomial time", intractable if it is not.
  - Example of a polynomial function: $5n^6 + 4n^2 + 3n + 2$.
  - Not a polynomial: $2^{n^k} + \ldots$ ("exponential")

Decision problem (yes-or-no question):

Decision problem (yes-or-no question):

- Of the form: Given a (binary) string x, is it in the language L?

Decision problem (yes-or-no question):

- Of the form: Given a (binary) string x, is it in the language L?

- E.g., "does x represent a prime number?"
  $\rightarrow$ "is x in the set: $L_{\mathrm{PRIMES}} \equiv \{10, 11, 101, 111, 1011, 1101, 10001, 10011, \ldots\}$?"

Decision problem (yes-or-no question):

- Of the form: Given a (binary) string x, is it in the language L?
- E.g., "does x represent a prime number?"
  $\rightarrow$ "is x in the set: $L_{\mathrm{PRIMES}} \equiv \{10, 11, 101, 111, 1011, 1101, 10001, 10011, \ldots\}$?"
- $L \subseteq \mathrm{DTIME}(T(n))$ iff there is a (deterministic) Turing machine that will come to a decision, in "on the order of $T(n)$" steps, as to whether a given string x of length n is in L.

Decision problem (yes-or-no question):

- Of the form: Given a (binary) string x, is it in the language L?

- E.g., "does x represent a prime number?"
  $\rightarrow$ "is x in the set: $L_{\text{PRIMES}} \equiv \{10, 11, 101, 111, 1011, 1101, 10001, 10011, \ldots\}$?"

- $L \subseteq \mathsf{DTIME}(T(n))$ iff there is a (deterministic) Turing machine that will come to a decision, in "on the order of $T(n)$" steps, as to whether a given string x of length n is in L.
  - "On the order of $T(n)$": $t(n)$ is $O(T(n))$ iff for every sufficiently large n, $t(n) \leq k \cdot T(n)$ for some constant k.
  - E.g., $5n^4 + 3n^2 + 4n + 1$ is $O(n^4)$

Decision problem (yes-or-no question):

- Of the form: Given a (binary) string x, is it in the language L?
- E.g., "does x represent a prime number?"
  $\rightarrow$ "is x in the set: $L_{\text{PRIMES}} \equiv \{10, 11, 101, 111, 1011, 1101, 10001, 10011, \ldots\}$?"
- $L \subseteq \text{DTIME}(T(n))$ iff there is a (deterministic) Turing machine that will come to a decision, in "on the order of $T(n)$" steps, as to whether a given string x of length n is in L.
  - "On the order of $T(n)$": $t(n)$ is $O(T(n))$ iff for every sufficiently large n, $t(n) \leq k \cdot T(n)$ for some constant k.
  - E.g., $5n^4 + 3n^2 + 4n + 1$ is $O(n^4)$

$$P = \bigcup_{k \geq 1} \text{DTIME}(n^k).$$

Deterministic Turing machine (DTM)

Deterministic Turing machine (DTM)

- initial state $+$ input $\Rightarrow$ final state

Deterministic Turing machine (DTM)

- initial state $+$ input $\Rightarrow$ final state
- Unique instruction set (transition function)

Deterministic Turing machine (DTM)

- initial state $+$ input $\Rightarrow$ final state
- Unique instruction set (transition function)

Nondeterministic Turing Machine (NTM)

- Multiple transition functions; choices are made by an external operator (i.e., not explicitly modeled).

Deterministic Turing machine (DTM)

- initial state + input $\Rightarrow$ final state
- Unique instruction set (transition function)
- A DTM accepts x (outputs "yes") if following its instruction set, given the input x, results in its being in an "accept state," and rejects x (answers "no") otherwise.

Nondeterministic Turing Machine (NTM)

- Multiple transition functions; choices are made by an external operator (i.e., not explicitly modeled).

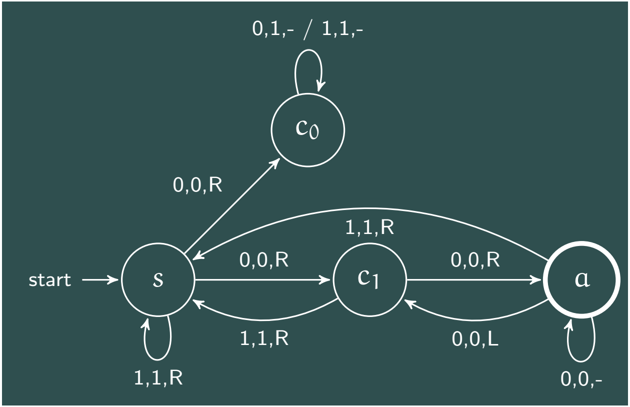
Deterministic Turing machine (DTM)

- initial state + input $\Rightarrow$ final state
- Unique instruction set (transition function)
- A DTM accepts x (outputs "yes") if following its instruction set, given the input x, results in its being in an "accept state," and rejects x (answers "no") otherwise.

Nondeterministic Turing Machine (NTM)

- Multiple transition functions; choices are made by an external operator (i.e., not explicitly modeled).
- An NTM accepts x if there exists a path through its state space, given x, that results in its being in an "accept state," and it rejects x otherwise.

Example of a Nondeterministic Turing Machine (NTM)



Accepts: $*00$.

$L \subseteq$ DTIME($T(n)$) iff there is a deterministic Turing machine that will produce a correct answer, in $O(T(n))$ steps, to the question of whether a given string x of length n is in L (Arora & Barak, 2009, p. 25).

$L \subseteq \mathrm{DTIME}(T(n))$ iff there is a deterministic Turing machine that will produce a correct answer, in $O(T(n))$ steps, to the question of whether a given string x of length n is in L (Arora & Barak, 2009, p. 25).

$L \subseteq \mathrm{NTIME}(T(n))$ iff there is a nondeterministic Turing machine that can answer "yes", in $O(T(n))$ steps, whenever a given string x of length n is in L (Arora & Barak, 2009, p. 41).

$L \subseteq \mathrm{DTIME}(T(n))$ iff there is a deterministic Turing machine that will produce a correct answer, in $O(T(n))$ steps, to the question of whether a given string x of length n is in L (Arora & Barak, 2009, p. 25).

$L \subseteq \mathrm{NTIME}(T(n))$ iff there is a nondeterministic Turing machine that can answer “yes”, in $O(T(n))$ steps, whenever a given string x of length n is in L (Arora & Barak, 2009, p. 41).

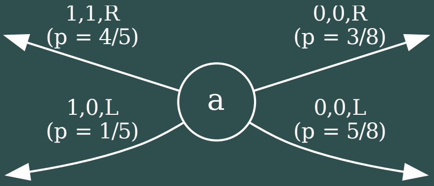
$$\mathrm{NP} =_{df} \bigcup_{k \geq 1} \mathrm{NTIME}(n^k).$$

Deterministic Turing machine (DTM)

- initial state + input $\Rightarrow$ final state
- Unique instruction set (transition function)
- A DTM accepts x (outputs "yes") if following its instruction set, given the input x, results in its being in an "accept state," and rejects x (answers "no") otherwise.

Nondeterministic Turing Machine (NTM)

- Multiple transition functions; choices are made by an external operator (i.e., not explicitly modeled).
- An NTM accepts x if there exists a path through its state space, given x, that results in its being in an "accept state," and it rejects x otherwise.



Probabilistic Turing machine (PTM)

- Probabilities are associated with transitions.

BPP (bounded-error probabilistic polynomial time)

- Class of languages such that there exists a PTM that will produce an answer to the question of whether or not a given string x is in L ...

BPP (bounded-error probabilistic polynomial time)

- Class of languages such that there exists a PTM that will produce an answer to the question of whether or not a given string x is in L in polynomial time ...

BPP (bounded-error probabilistic polynomial time)

- Class of languages such that there exists a PTM that will produce an answer to the question of whether or not a given string x is in L in polynomial time with the probability that it is correct, $p \geq 2/3$.

BPP (bounded-error probabilistic polynomial time)

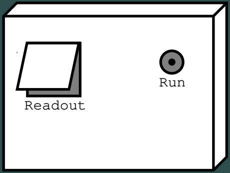
- Class of languages such that there exists a PTM that will produce an answer to the question of whether or not a given string x is in L in polynomial time with the probability that it is correct, $p \geq 2/3$.
    - (actually, p can be as low as: $1/2 + n^{-k}$)

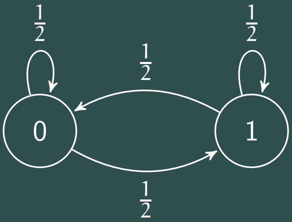
BPP (bounded-error probabilistic polynomial time)

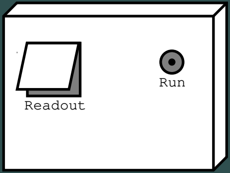
- Class of languages such that there exists a PTM that will produce an answer to the question of whether or not a given string x is in L in polynomial time with the probability that it is correct, $p \geq 2/3$.
  - (actually, p can be as low as: $1/2 + n^{-k}$)

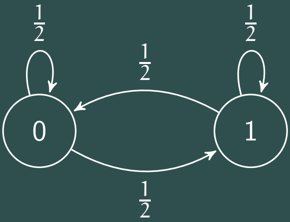
BQP (quantum bounded-error probabilistic polynomial time)

- Class of languages such that there exists a Quantum-probabilistic Turing machine that will produce an answer to the question of whether or not a given string x is in L in polynomial time, with the probability that it is correct, $p \geq 2/3$.

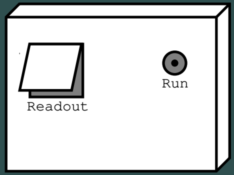

Readout
Run

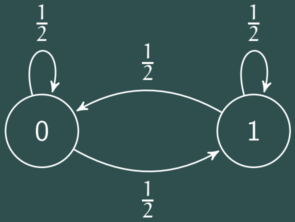

1/2
1/2
1/2
1/2
0
1



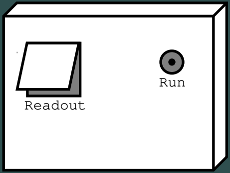


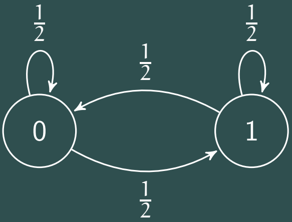
$\Pr(C0 \to 0)$





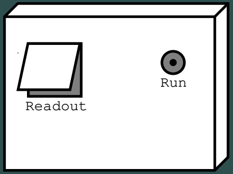
$$\Pr(C0 \to 0) = \Pr(C0 \to 1) = \Pr(C1 \to 0) = \Pr(C1 \to 1) = \tfrac{1}{2}$$

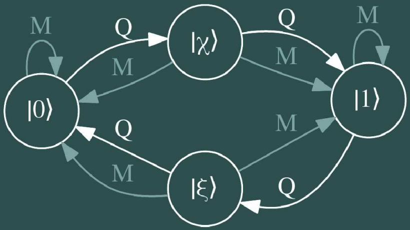




$$\Pr(C0 \to 0) = \Pr(C0 \to 1) = \Pr(C1 \to 0) = \Pr(C1 \to 1) = \tfrac{1}{2}$$

$$\begin{aligned} \Pr(C^2 0 \to 0) \;=\;& \Pr(C0 \to 0) \times \Pr(C0 \to 0) \\ &+ \Pr(C0 \to 1) \times \Pr(C1 \to 0) = \tfrac{1}{2} \end{aligned}$$





$$|0\rangle \xrightarrow{Q} \underbrace{\frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle}_{|\chi\rangle} \xrightarrow{Q} |1\rangle$$

$$|1\rangle \xrightarrow{Q} \underbrace{\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle}_{|\xi\rangle} \xrightarrow{Q} |0\rangle$$

$$\Pr(C0 \to 0) = \tfrac{1}{2} \qquad \Pr(Q|0\rangle \xrightarrow{meas} 0) = \tfrac{1}{2}$$

$$\Pr(C0 \to 1) = \tfrac{1}{2} \qquad \Pr(Q|0\rangle \xrightarrow{meas} 1) = \tfrac{1}{2}$$

$$\Pr(C1 \to 0) = \tfrac{1}{2} \qquad \Pr(Q|1\rangle \xrightarrow{meas} 0) = \tfrac{1}{2}$$

$$\Pr(C1 \to 1) = \tfrac{1}{2} \qquad \Pr(Q|1\rangle \xrightarrow{meas} 1) = \tfrac{1}{2}$$

$$\Pr(C0 \to 0) = \tfrac{1}{2} \qquad \Pr(Q|0\rangle \xrightarrow{meas} 0) = \tfrac{1}{2}$$

$$\Pr(C0 \to 1) = \tfrac{1}{2} \qquad \Pr(Q|0\rangle \xrightarrow{meas} 1) = \tfrac{1}{2}$$

$$\Pr(C1 \to 0) = \tfrac{1}{2} \qquad \Pr(Q|1\rangle \xrightarrow{meas} 0) = \tfrac{1}{2}$$

$$\Pr(C1 \to 1) = \tfrac{1}{2} \qquad \Pr(Q|1\rangle \xrightarrow{meas} 1) = \tfrac{1}{2}$$

$$\Pr(C^2 0 \to 0) = \tfrac{1}{2} \qquad \Pr(Q^2|0\rangle \xrightarrow{meas} 0) = 0$$

$$\Pr(C^2 0 \to 1) = \tfrac{1}{2} \qquad \Pr(Q^2|0\rangle \xrightarrow{meas} 1) = 1$$

$$\Pr(C^2 1 \to 0) = \tfrac{1}{2} \qquad \Pr(Q^2|1\rangle \xrightarrow{meas} 0) = 1$$

$$\Pr(C^2 1 \to 1) = \tfrac{1}{2} \qquad \Pr(Q^2|1\rangle \xrightarrow{meas} 1) = 0$$

$\mathsf{BPP} \subseteq \mathsf{BQP}$

$$\mathrm{BPP} \subseteq \mathrm{BQP}$$

$$\mathrm{BPP} \subsetneq \mathrm{BQP}?$$

$\Rightarrow$ Do problems exist that are tractable for a quantum computer but (provably) intractable for a PTM?

III. The Physics of Classical and Quantum Computers

Classical computers

Classical computers

- Manipulate bits

Classical computers

- Manipulate bits: abstractly, binary digits

Classical computers

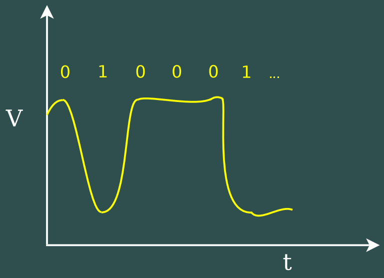
- Manipulate bits: abstractly, binary digits
- Physically realised in a 2-level system

Classical computers

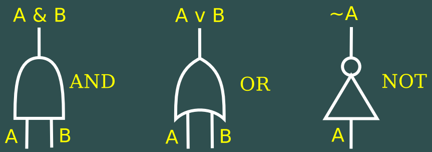
- Manipulate bits: abstractly, binary digits
- Physically realised in a 2-level system, e.g., light switch, magnet, …

Classical computers

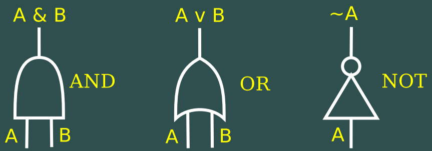
- Manipulate bits: abstractly, binary digits
- Physically realised in a 2-level system, e.g., light switch, magnet, or any physical process in which we can distinguish two physical states, e.g.,



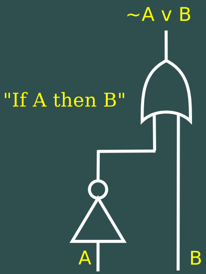
Classical logic gates



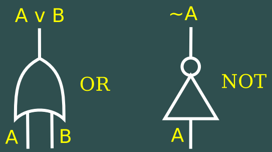
Classical logic gates



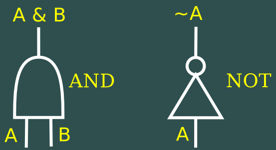
Classical circuit



Universal set:

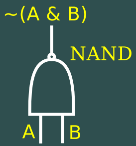


Another universal set:

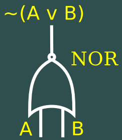


Given a universal set of logic gates, we can exactly simulate the output of any arbitrary logic gate.

Another universal set:



Another universal set:



Given a universal set of logic gates, we can exactly simulate the output of any arbitrary logic gate.

Quantum computers

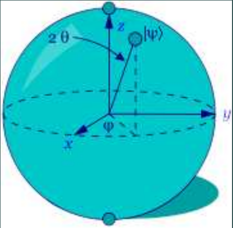
- Manipulate quantum bits (qubits),

Quantum computers

- Manipulate quantum bits (qubits), abstractly: unit vectors in a 2-dimensional complex Hilbert space.

Quantum computers

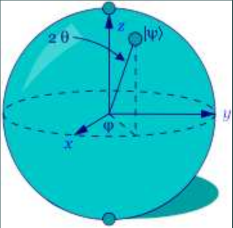
- Manipulate quantum bits (qubits), abstractly: unit vectors in a 2-dimensional complex Hilbert space.
- Physically realised by a 2-level quantum system, e.g., the spin of an electron in a particular direction.



Quantum computers

- Manipulate quantum bits (qubits), abstractly: unit vectors in a 2-dimensional complex Hilbert space.
- Physically realised by a 2-level quantum system, e.g., the spin of an electron in a particular direction.

$|0\rangle$



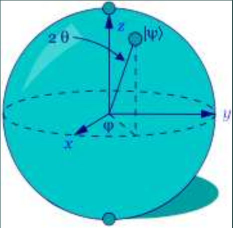
$|1\rangle$

- Typically initialized in one of the "computational basis" states, i.e., the eigenstates, $\{|0\rangle, |1\rangle\}$, of the Pauli Z operator.

Quantum computers

- Manipulate quantum bits (qubits), abstractly: unit vectors in a 2-dimensional complex Hilbert space.
- Physically realised by a 2-level quantum system, e.g., the spin of an electron in a particular direction.

$|0\rangle$



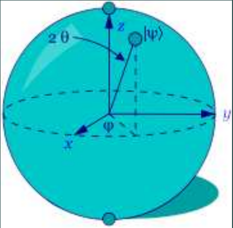
$|1\rangle$

- Typically initialized in one of the "computational basis" states, i.e., the eigenstates, $\{|0\rangle, |1\rangle\}$, of the Pauli Z operator.
- General form for a qubit's state (in the z-basis): $\alpha|0\rangle + \beta|1\rangle$

Quantum computers

- Manipulate quantum bits (qubits), abstractly: unit vectors in a 2-dimensional complex Hilbert space.
- Physically realised by a 2-level quantum system, e.g., the spin of an electron in a particular direction.

$|0\rangle$



$|1\rangle$

- Typically initialized in one of the "computational basis" states, i.e., the eigenstates, $\{|0\rangle, |1\rangle\}$, of the Pauli Z operator.
- General form for a qubit's state (in any basis): $c_1|b_1\rangle + c_2|b_2\rangle$

Quantum logic gates

- Described by unitary transformations (reversible, norm preserving), $UU^{\dagger} = U^{\dagger}U = I$, on unit vectors

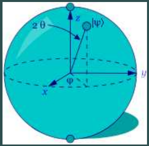
Quantum logic gates

- Described by unitary transformations (reversible, norm preserving), $UU^\dagger = U^\dagger U = I$, on unit vectors

$$|0\rangle \;—\boxed{X}—\; |1\rangle$$

$$|1\rangle \;—\boxed{X}—\; |0\rangle$$

π-rotation about x-axis



$$X|0\rangle \;=\; |1\rangle \qquad\qquad X|1\rangle \;=\; |0\rangle$$

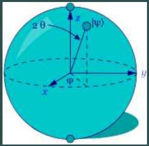
Quantum logic gates

- Described by unitary transformations (reversible, norm preserving), $UU^\dagger = U^\dagger U = I$, on unit vectors

$$|0\rangle \;—\!\!\!—\boxed{Y}—\!\!\!—\; i|1\rangle$$

$$|1\rangle \;—\!\!\!—\boxed{Y}—\!\!\!—\; -i|0\rangle$$

π-rotation about y-axis



$$Y|0\rangle \;=\; i|1\rangle \qquad\qquad Y|1\rangle \;=\; -i|0\rangle$$

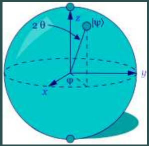
Quantum logic gates

- Described by unitary transformations (reversible, norm preserving), $UU^\dagger = U^\dagger U = I$, on unit vectors

$$|0\rangle \;—\boxed{Z}—\; |0\rangle$$

$$|1\rangle \;—\boxed{Z}—\; -|1\rangle$$

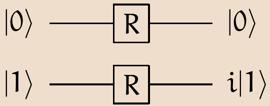
π-rotation about z-axis



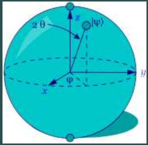
$$Z|0\rangle \;=\; |0\rangle \qquad\qquad Z|1\rangle \;=\; -|1\rangle$$

Quantum logic gates

- Described by unitary transformations (reversible, norm preserving), $UU^\dagger = U^\dagger U = I$, on unit vectors



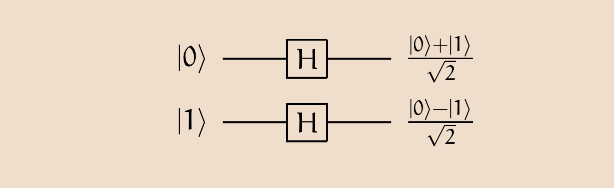
$\pi/2$-rotation about z-axis



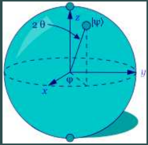
$$R|0\rangle = |0\rangle \qquad R|1\rangle = i|1\rangle$$

Quantum logic gates

- Described by unitary transformations (reversible, norm preserving), $UU^\dagger = U^\dagger U = I$, on unit vectors



(1) $\pi/2$-rotation about y-axis +
(2) π-rotation about x



$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Controlled-Not (CNOT) gate (a.k.a. Controlled-X gate)

$$C_{10}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$$

Controlled-Not (CNOT) gate (a.k.a. Controlled-X gate)

$$C_{10}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$$

$C_{10}|00\rangle = |00\rangle$,

Controlled-Not (CNOT) gate (a.k.a. Controlled-X gate)

$$C_{10}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$$

$C_{10}|00\rangle = |00\rangle, \quad C_{10}|01\rangle = |01\rangle,$

Controlled-Not (CNOT) gate (a.k.a. Controlled-X gate)

$$C_{10}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$$

$$C_{10}|00\rangle = |00\rangle, \quad C_{10}|01\rangle = |01\rangle, \quad C_{10}|10\rangle = |11\rangle,$$

Controlled-Not (CNOT) gate (a.k.a. Controlled-X gate)

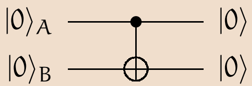
$$C_{10}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$$

$$C_{10}|00\rangle = |00\rangle, \quad C_{10}|01\rangle = |01\rangle, \quad C_{10}|10\rangle = |11\rangle, \quad C_{10}|11\rangle = |10\rangle.$$

Controlled-Not (CNOT) gate (a.k.a. Controlled-X gate)

$$C_{10}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$$

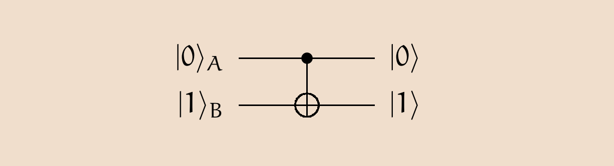
$$C_{10}|00\rangle = |00\rangle, \quad C_{10}|01\rangle = |01\rangle, \quad C_{10}|10\rangle = |11\rangle, \quad C_{10}|11\rangle = |10\rangle.$$



Controlled-Not (CNOT) gate (a.k.a. Controlled-X gate)

$$C_{10}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$$

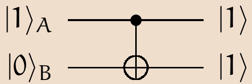
$$C_{10}|00\rangle = |00\rangle, \quad C_{10}|01\rangle = |01\rangle, \quad C_{10}|10\rangle = |11\rangle, \quad C_{10}|11\rangle = |10\rangle.$$



Controlled-Not (CNOT) gate (a.k.a. Controlled-X gate)

$$C_{10}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$$

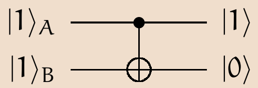
$$C_{10}|00\rangle = |00\rangle, \quad C_{10}|01\rangle = |01\rangle, \quad C_{10}|10\rangle = |11\rangle, \quad C_{10}|11\rangle = |10\rangle.$$



Controlled-Not (CNOT) gate (a.k.a. Controlled-X gate)

$$C_{10}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$$

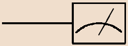
$$C_{10}|00\rangle = |00\rangle, \quad C_{10}|01\rangle = |01\rangle, \quad C_{10}|10\rangle = |11\rangle, \quad C_{10}|11\rangle = |10\rangle.$$



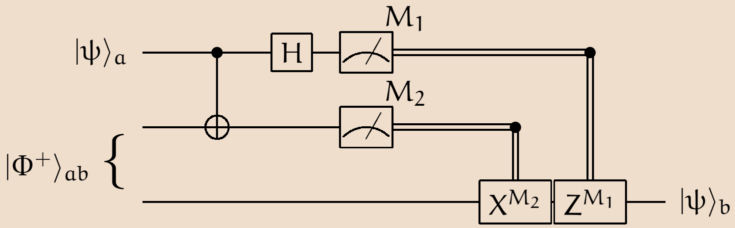
Measurement gate

Implemented by a projective measurement in a given basis.

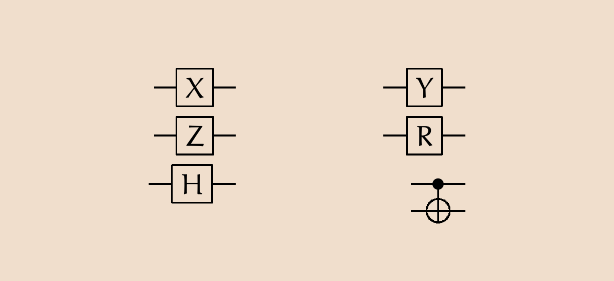
- Probabilistic transition
- Given $\alpha|0\rangle + \beta|1\rangle$, measurement in the z-basis yields $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$.

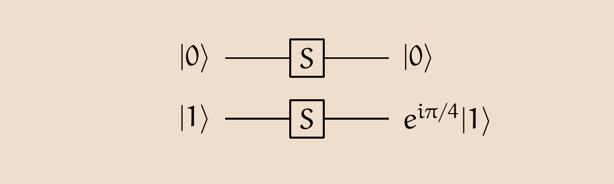


Circuits



Universal set of quantum logic gates:





Can simulate any quantum gate to arbitrary accuracy

IV. Deeper Analogies and Disanalogies

Consider the operator:

$$\hat{S} \equiv \hat{S}_a + \hat{S}_b + \hat{S}_c$$

- In QM we can assign a value to a sum without assigning values to the summands.

Consider the operator:

$$\hat{S} \equiv \hat{S}_a + \hat{S}_b + \hat{S}_c$$

- In QM we can assign a value to a sum without assigning values to the summands.
- Not possible in classical theory.

Consider the operator:

$$\hat{S} \equiv \hat{S}_a + \hat{S}_b + \hat{S}_c$$

- In QM we can assign a value to a sum without assigning values to the summands.
- Not possible in classical theory.
- The kinematics of QM are less restrictive.

Consider the operator:

$$\hat{S} \equiv \hat{S}_a + \hat{S}_b + \hat{S}_c$$

- In QM we can assign a value to a sum without assigning values to the summands.
- Not possible in classical theory.
- The kinematics of QM are less restrictive.

Kinematical constraints (broad sense; see Janssen 2009):

- Constraints imposed by a theoretical framework on our physical description of a system independently of the specifics of its dynamics.

Comparing the kinematics of CM and QM

Classical mechanics:

- An observable A is represented by $f_A(\omega)$ acting on the phase space of a system.

Quantum mechanics:

Comparing the kinematics of CM and QM

Classical mechanics:

- An observable A is represented by $f_A(\omega)$ acting on the phase space of a system.

Quantum mechanics:

- An observable A is represented by $\hat{A}$ acting on the Hilbert space of a system.

Comparing the kinematics of CM and QM

Classical mechanics:

- An observable A is represented by $f_A(\omega)$ acting on the phase space of a system.
- With f_A we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.

Quantum mechanics:

- An observable A is represented by $\hat{A}$ acting on the Hilbert space of a system.

Comparing the kinematics of CM and QM

Classical mechanics:

- An observable A is represented by $f_A(\omega)$ acting on the phase space of a system.
- With f_A we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.

Quantum mechanics:

- An observable A is represented by $\hat{A}$ acting on the Hilbert space of a system.
- With $\hat{A}$ we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.

Comparing the kinematics of CM and QM

Classical mechanics:

- An observable A is represented by $f_A(\omega)$ acting on the phase space of a system.
- With f_A we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.
- Points in phase space are "truthmakers"

Quantum mechanics:

- An observable A is represented by $\hat{A}$ acting on the Hilbert space of a system.
- With $\hat{A}$ we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.

Comparing the kinematics of CM and QM

Classical mechanics:

- An observable A is represented by $f_A(\omega)$ acting on the phase space of a system.
- With f_A we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.
- Points in phase space are "truthmakers" in the sense that
  - Fixing ω fixes the values for *every* observable.

Quantum mechanics:

- An observable A is represented by $\hat{A}$ acting on the Hilbert space of a system.
- With $\hat{A}$ we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.

Comparing the kinematics of CM and QM

Classical mechanics:

- An observable A is represented by $f_A(\omega)$ acting on the phase space of a system.
- With f_A we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.
- Points in phase space are "truthmakers" in the sense that
  - Fixing ω fixes the values for *every* observable.
  - $\mathfrak{A}, \mathfrak{B}, \ldots$ embeddable into a global Boolean algebra.

Quantum mechanics:

- An observable A is represented by $\hat{A}$ acting on the Hilbert space of a system.
- With $\hat{A}$ we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.

Comparing the kinematics of CM and QM

Classical mechanics:

- An observable A is represented by $f_A(\omega)$ acting on the phase space of a system.
- With f_A we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.
- Points in phase space are "truthmakers" in the sense that
  - Fixing ω fixes the values for *every* observable.
  - $\mathfrak{A}, \mathfrak{B}, \ldots$ embeddable into a global Boolean algebra.

Quantum mechanics:

- An observable A is represented by $\hat{A}$ acting on the Hilbert space of a system.
- With $\hat{A}$ we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.
- Vectors in Hilbert space *not* "truthmakers"

Comparing the kinematics of CM and QM

Classical mechanics:

- An observable A is represented by $f_A(\omega)$ acting on the phase space of a system.
- With f_A we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.
- Points in phase space are "truthmakers" in the sense that
  - Fixing ω fixes the values for *every* observable.
  - $\mathfrak{A}, \mathfrak{B}, \ldots$ embeddable into a global Boolean algebra.

Quantum mechanics:

- An observable A is represented by $\hat{A}$ acting on the Hilbert space of a system.
- With $\hat{A}$ we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.
- Vectors in Hilbert space *not* "truthmakers" in the sense that
  - Fixing $|\psi\rangle$ only fixes $\Pr(v_A|A)$, $\Pr(v_B|B), \ldots$

Comparing the kinematics of CM and QM

Classical mechanics:

- An observable A is represented by $f_A(\omega)$ acting on the phase space of a system.
- With f_A we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.
- Points in phase space are "truthmakers" in the sense that
  - Fixing ω fixes the values for *every* observable.
  - $\mathfrak{A}, \mathfrak{B}, \ldots$ embeddable into a global Boolean algebra.

Quantum mechanics:

- An observable A is represented by $\hat{A}$ acting on the Hilbert space of a system.
- With $\hat{A}$ we can associate a Boolean algebra $\mathfrak{A}$ of yes-or-no questions concerning A.
- Vectors in Hilbert space *not* "truthmakers" in the sense that
  - Fixing $|\psi\rangle$ only fixes $\Pr(\nu_A|A),\ \Pr(\nu_B|B), \ldots$
  - $\mathfrak{A}, \mathfrak{B}, \ldots$ not embeddable into global Boolean algebra.

Conditional probability distribution:

- Informal gloss: "What to expect whenever I measure X"

Conditional probability distribution:

- Informal gloss: "What to expect whenever I measure X"

Classical mechanics:

- Specifying that I have chosen to measure the observable A (as opposed to B) adds no information regarding what probabilities to expect, over the possible outcomes of A, that is not already given to us via the state description, ω (Hughes, 1989, p. 61).

Conditional probability distribution:

- Informal gloss: "What to expect whenever I measure X"

Classical mechanics:

- Specifying that I have chosen to measure the observable A (as opposed to B) adds no information regarding what probabilities to expect, over the possible outcomes of A, that is not already given to us via the state description, ω (Hughes, 1989, p. 61).

Quantum mechanics:

- This is not the case.

Conditional probability distribution:

- Informal gloss: "What to expect whenever I measure X"

Classical mechanics:

- Specifying that I have chosen to measure the observable A (as opposed to B) adds no information regarding what probabilities to expect, over the possible outcomes of A, that is not already given to us via the state description, ω (Hughes, 1989, p. 61).

Quantum mechanics:

- This is not the case.
- The case in which a state description is always "complete" (in the classical sense) is a special case of the more general framework described by QM.

Conditional probability distribution:

- Informal gloss: "What to expect whenever I measure X"

Classical mechanics:

- Specifying that I have chosen to measure the observable A (as opposed to B) adds no information regarding what probabilities to expect, over the possible outcomes of A, that is not already given to us via the state description, ω (Hughes, 1989, p. 61).

Quantum mechanics:

- This is not the case.
- The case in which a state description is always "complete" (in the classical sense) is a special case of the more general framework described by QM.
- Result: exponentially more possible state descriptions for a given n-dimensional system in QM. I.e., QM allows for entangled states.
- From a computational point of view: Exponentially more resources available – allows for "shortcuts" through a system's state space.

Illustration: General constraint on the correlations between three balanced random variables (Janas, MEC, & Janssen 2022):

$$1 - \chi_{ab}^2 - \chi_{ac}^2 - \chi_{bc}^2 + 2\chi_{ab}\chi_{ac}\chi_{bc} \geq 0$$

Illustration: General constraint on the correlations between three balanced random variables (Janas, MEC, & Janssen 2022):

$$1 - \chi_{ab}^2 - \chi_{ac}^2 - \chi_{bc}^2 + 2\chi_{ab}\chi_{ac}\chi_{bc} \geq 0$$

Quantum elliptope:

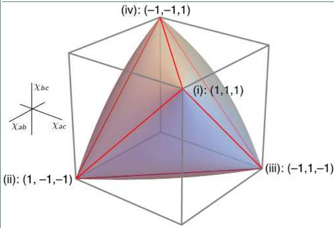
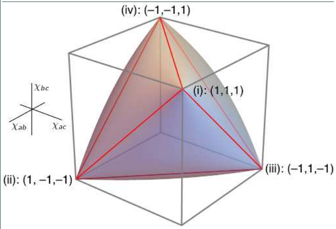


Illustration: General constraint on the correlations between three balanced random variables (Janas, MEC, & Janssen 2022):

$$1 - \chi_{ab}^2 - \chi_{ac}^2 - \chi_{bc}^2 + 2\chi_{ab}\chi_{ac}\chi_{bc} \geq 0$$

Quantum elliptope:



Classical tetrahedron:

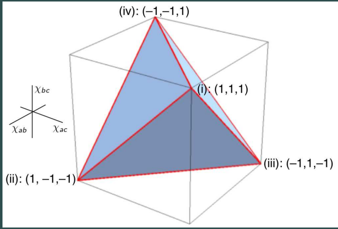
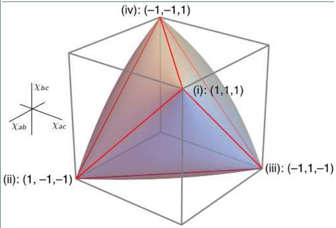


Illustration: General constraint on the correlations between three balanced random variables (Janas, MEC, & Janssen 2022):

$$1 - \chi_{ab}^2 - \chi_{ac}^2 - \chi_{bc}^2 + 2\chi_{ab}\chi_{ac}\chi_{bc} \geq 0$$

Higher values of spin?

Quantum elliptope:



Classical tetrahedron:

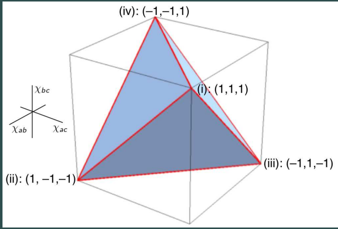
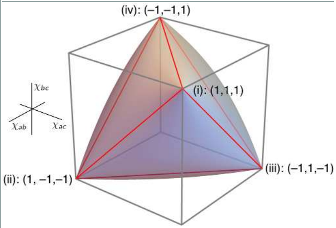


Illustration: General constraint on the correlations between three balanced random variables (Janas, MEC, & Janssen 2022):

$$1 - \chi_{ab}^2 - \chi_{ac}^2 - \chi_{bc}^2 + 2\chi_{ab}\chi_{ac}\chi_{bc} \geq 0$$

Higher values of spin? Result: M. Janas

Quantum elliptope:



Classical polytope (spin 1):

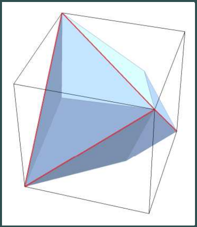
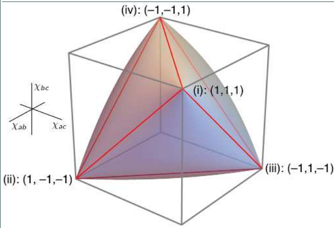


Illustration: General constraint on the correlations between three balanced random variables (Janas, MEC, & Janssen 2022):

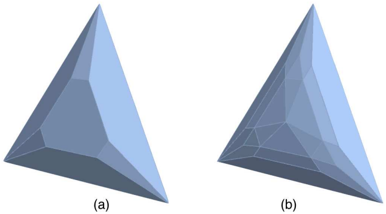
$$1 - \chi_{ab}^2 - \chi_{ac}^2 - \chi_{bc}^2 + 2\chi_{ab}\chi_{ac}\chi_{bc} \geq 0$$

Higher values of spin? Result: M. Janas

Quantum elliptope:



Classical polytope (spin $\frac{3}{2}$ and 2):



Kinematical constraints (broad sense; see Janssen 2009):

- Constraints imposed by a theoretical framework on our physical description of a system independently of the specifics of its dynamics.
- Kinematics of QM are less restrictive.

Kinematical constraints (broad sense; see Janssen 2009):

- Constraints imposed by a theoretical framework on our physical description of a system independently of the specifics of its dynamics.
- Kinematics of QM are less restrictive.

Independent of the specifics $\neq$ independent of the dynamics per se.

Kinematical constraints (broad sense; see Janssen 2009):

- Constraints imposed by a theoretical framework on our physical description of a system independently of the specifics of its dynamics.
- Kinematics of QM are less restrictive.

Independent of the specifics $\neq$ independent of the dynamics per se.

Gottesman-Knill Theorem:

- Merely possessing an entangled state isn't enough to yield a speedup over classical computation.

Kinematical constraints (broad sense; see Janssen 2009):

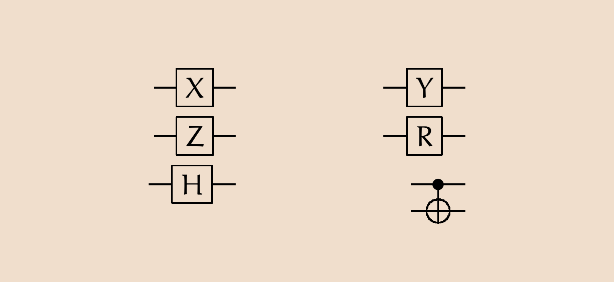
- Constraints imposed by a theoretical framework on our physical description of a system independently of the specifics of its dynamics.
- Kinematics of QM are less restrictive.

Independent of the specifics $\neq$ independent of the dynamics per se.

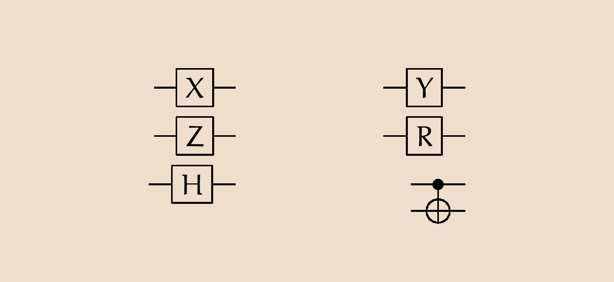
Gottesman-Knill Theorem:

- Merely possessing an entangled state isn't enough to yield a speedup over classical computation.
- The Clifford group of operations alone are sufficient to generate an entangled state.
- However: You also need to use it effectively

Clifford group of quantum logic gates:

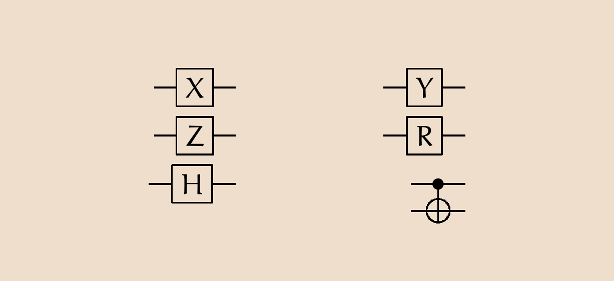


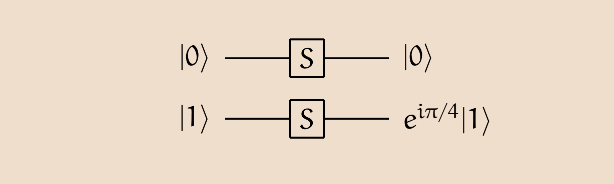
Clifford group of quantum logic gates:



Not universal

Universal set of quantum logic gates:





Can simulate any quantum gate to arbitrary accuracy

Analogy: CHSH inequality (MEC 2017)

Assuming that outcomes of local experiments depend only on the local setup and on the value of a hidden variable λ assigned to the combined system at state preparation, then:

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

Analogy: CHSH inequality (MEC 2017)

Assuming that outcomes of local experiments depend only on the local setup and on the value of a hidden variable λ assigned to the combined system at state preparation, 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.

Analogy: CHSH inequality (MEC 2017)

Assuming that outcomes of local experiments depend only on the local setup and on the value of a hidden variable λ assigned to the combined system at state preparation, 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. E.g., let $\hat{m}, \hat{m}', \hat{n}, \hat{n}'$ lie in the same plane with respective orientations of: $0, \pi/2, \pi/4, -\pi/4$.

Analogy: CHSH inequality (MEC 2017)

Assuming that outcomes of local experiments depend only on the local setup and on the value of a hidden variable λ assigned to the combined system at state preparation, 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. E.g., let $\hat{m}, \hat{m}', \hat{n}, \hat{n}'$ lie in the same plane with respective orientations of: $0, \pi/2, \pi/4, -\pi/4$. Then for the singlet state, since:
$\langle \sigma_m \otimes \sigma_n \rangle = -\hat{m} \cdot \hat{n} = -\cos\theta$,

Analogy: CHSH inequality (MEC 2017)

Assuming that outcomes of local experiments depend only on the local setup and on the value of a hidden variable λ assigned to the combined system at state preparation, 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. E.g., let $\hat{m}, \hat{m}', \hat{n}, \hat{n}'$ lie in the same plane with respective orientations of: $0, \pi/2, \pi/4, -\pi/4$. Then for the singlet state, since:
$\langle \sigma_m \otimes \sigma_n \rangle = -\hat{m} \cdot \hat{n} = -\cos\theta$,

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

Analogy: CHSH inequality (MEC 2017)

Assuming that outcomes of local experiments depend only on the local setup and on the value of a hidden variable λ assigned to the combined system at state preparation, 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. E.g., let $\hat{m}, \hat{m}', \hat{n}, \hat{n}'$ lie in the same plane with respective orientations of: $0, \pi/2, \pi/4, -\pi/4$. Then for the singlet state, since:
$\langle \sigma_m \otimes \sigma_n \rangle = -\hat{m} \cdot \hat{n} = -\cos\theta$,

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

But no conflict 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 $\propto \pi/2$.

$\Rightarrow$ The Pauli measurements (Clifford group).

Kinematical constraints (broad sense; see Janssen 2009):

- Constraints imposed by a theoretical framework on our physical description of a system independently of the specifics of its dynamics.
- Kinematics of QM are less restrictive.

Independent of the specifics $\neq$ independent of the dynamics per se.

Gottesman-Knill Theorem:

- Merely possessing an entangled state isn't enough to yield a speedup over classical computation.
- The Clifford group of operations alone are sufficient to generate an entangled state.
- However: You also need to use it effectively

Kinematical constraints (broad sense; see Janssen 2009):

- Constraints imposed by a theoretical framework on our physical description of a system independently of the specifics of its dynamics.
- Kinematics of QM are less restrictive.

Independent of the specifics $\neq$ independent of the dynamics per se.

Gottesman-Knill Theorem:

- Merely possessing an entangled state isn't enough to yield a speedup over classical computation.
- The Clifford group of operations alone are sufficient to generate an entangled state.
- However: You also need to use it effectively
- I.e., you need to perform the right operations (duh!)

Thanks!

Works Cited I

Arora, S., & Barak, B. (2009). *Computational Complexity: A Modern Approach*. Cambridge: Cambridge University Press.

Cuffaro, M. E. (2017). On the significance of the Gottesman-Knill theorem. *The British Journal for the Philosophy of Science*, *68*, 91–121.

Hilbert, D., & Ackermann, W. (1928). *Principles of Mathematical Logic*. Berlin: Springer-Verlag.

Hughes, R. I. G. (1989). *The Structure and Interpretation of Quantum Mechanics*. Cambridge, MA.: Harvard University Press.

Janas, M., Cuffaro, M. E., & Janssen, M. (2022). *Understanding Quantum Raffles: Quantum Mechanics on an Informational Approach: Structure and Interpretation*. Cham: Springer-Verlag. Foreword by Jeffrey Bub.

Janssen, M. (2009). Drawing the line between kinematics and dynamics in special relativity. *Studies in History and Philosophy of Modern Physics*, *40*, 26–52.

Turing, A. M. (1936-7). On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society. Second Series*, *s2-42*, 230–265.