Quantum computation for computer scientists

Richard Jozsa
University of Bristol UK
What is quantum computation?

Recall usual TM: head states $Q$, tape alphabet $\Gamma$
    run time $t = t(n)$ (here $= \text{poly}(n)$)
Set of configurations $\mathcal{C}$, size $C = 2^{O(n)}$
Initial config. $c_I$ • Accepting config. $c_A$ (assume unique)

DTM, NDTM: transition matrix $T$, size $C \times C$

$$T(c',c) = \begin{cases} 0 & \text{if transition } c \rightarrow c' \text{ not allowed in 1 step} \\ 1 & \text{allowed} \end{cases}$$

$T^r(c',c)$ is number of paths $c$-to-$c'$ of length $r$
TM accepts iff $T^t(c_A, c_I)$ not zero.

Transition matrix $T$ comes from transition function

$$\delta: (Q \times \Gamma) \times (Q \times \Gamma) \times \{L,R\} \rightarrow A = \{0,1\}$$

Values of $\delta$ determine entries of $T$ in usual way.

$T^r(c',c) = \text{sum over all length-r paths } c\text{-to-}c' \text{ of products of values of } \delta \text{ along the path.}$
**Probabilistic TM**: simply modify \( \delta \) to have values in \( A = \{0, 1\} \) \([0,1]\) “\( \delta \) values are now probabilities of transitions”

And extra restriction –

For each separate \((q,a)\):

\[
\sum_{q',a',d} \delta (q,a,q',a',d) = 1 \quad (\times)
\]

Stages of machine \( \sim \) column vectors of length \( C \) listing probs. of configs.

\( T^r(c, c_r) \) = prob. of config \( c \) after \( r \) steps from \( c_r \).

\( T \) is a **stochastic** matrix (columns sum to 1 and have non-negative entries).

(guaranteed simply if \( \delta \) satisfies \((\times)\) – a “local” condition).

\( T \) preserves \( L^1 \) norm of stage vectors

\[
|v|_1 = \sum_i |v_i| = \sum v_i \quad \text{here} = 1
\]
Quantum TM: just modify $\delta$ to have values in $A = \{0, 1\}$ (or $\{0, \pm 1, \pm \sqrt{3}/2\}$, or $\{0, \pm 1, \pm \sqrt{2}\}$ suffice).

And extra restriction –
$T$ preserves $L^2$ norm $\|v\|_2 = \sqrt{\sum |v_i|^2} = 1$ (**)
i.e. “$T$ is a unitary matrix”

Define! : $|T^r(c, c_\perp)|^2 = \text{probability to go from } c_\perp \text{ to } c \text{ in } r \text{ steps.}$

Looks like mild generalisation!.... but note:
conditions on $\delta$ to ensure (**)? ‘Global’ now:
Cannot have separate transition condition for each (q,a) individually.
Need to consider collisions of target configs (q’,a’) coming from different sources – add transition $v_i$‘s before squaring in $L^2$ norm.
Transitions can “interfere destructively” and in that case, must be enhanced somewhere else!
Unitary matrix: columns orthonormal so now have global constraint on all columns.
Complexity classes

**BPP** class of languages $L$ such that there is poly-time PTM with

$x \in L \Rightarrow T^\epsilon (c_A, c_x) \geq \frac{2}{3}

x \notin L \Rightarrow T^\epsilon (c_A, c_x) \leq \frac{1}{3}$

**BQP** (quantum polynomial time)

class of languages $L$ such that there is poly-time QTM with

$x \in L \Rightarrow |T^\epsilon (c_A, c_x)|^2 \geq \frac{2}{3}

x \notin L \Rightarrow |T^\epsilon (c_A, c_x)|^2 \leq \frac{1}{3}$

Above characterisations ~ *formal* properties like $BPP \subseteq BQP \subseteq PP \subseteq PSPACE$

**But** how to exploit QTM model for *algorithm design*??...

And where’s the physics??...

Seek more informative model description:

**Circuit model** –

Notions of qubits, quantum measurements, entanglement, unitary quantum gates....
**Bits and quantum bits (qubits)**

**Classical Information**

*bit*: 0 or 1  
Two distinguishable states of a physical system

**Quantum Information**

*Single qubit*: simplest quantum physical system  
with two distinguishable states  
“Classical” values $|0\rangle$ and $|1\rangle$  
and general complex superpositions $a|0\rangle + b|1\rangle$  
$s|a|^2 + |b|^2 = 1$

*Two qubits:*

$a|0\rangle|0\rangle + b|0\rangle|1\rangle + c|1\rangle|0\rangle + d|1\rangle|1\rangle$

(normalised); similarly for more qubits.

In general: states of quantum system are  
normalised complex vectors, with a notion of inner product.

**Two new features:**

Quantum measurement  
Quantum entanglement
Quantum entanglement: states of composite systems

Classical information
n bits: 010…0 n similar systems
Number of parameters grows linearly for a composite of n similar systems.
Total state space is cartesian product of subsystem spaces

Quantum information
n qubits: superposition of $2^n$ “classical” possibilities
$$\sum a_{i_1 i_2 \ldots i_n} |i_1\rangle |i_2\rangle \ldots |i_n\rangle$$
Total state space is tensor product of subsystem spaces
Number of parameters grows exponentially with n.

Entanglement
Individual qubits do not have separate pure states of the form $a|0\rangle + b|1\rangle$. The qubits are “entangled”.

Example:
$$\frac{1}{\sqrt{2}}(|0\rangle |0\rangle + |1\rangle |1\rangle) \neq (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$$ for any values of a,b,c,d.
Measurement for multi-qubit states

Measure 0 vs. 1 on the first qubit of a 2-qubit state

\[ a |0\rangle |0\rangle + b |0\rangle |1\rangle + c |1\rangle |0\rangle + d |1\rangle |1\rangle \]

\[ = |0\rangle (a |0\rangle + b |1\rangle) + |1\rangle (c |0\rangle + d |1\rangle) \]

Outcome of measurement is probabilistic

<table>
<thead>
<tr>
<th>See:</th>
<th>0</th>
<th>or</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability:</td>
<td>$</td>
<td>a</td>
<td>^2 +</td>
</tr>
<tr>
<td>Final state:</td>
<td>$</td>
<td>0\rangle (a</td>
<td>0\rangle + b</td>
</tr>
</tbody>
</table>

Irreversible “collapse” of state:
Information of initial state identity significantly lost.
Full information of physical state identity is not available!
Further measurement examples

1-qubit state: \( a|0\rangle + b|1\rangle \)
Can sample \( \{ |a|^2, |b|^2 \} \) distribution once.

n-qubit state: \( \sum_i a_{i_1 i_2 \ldots i_n} |i_1\rangle |i_2\rangle \ldots |i_n\rangle \)

Measuring all qubits allows one sampling of \( \{ |a_{i_1 \ldots i_n}|^2 \} \) distribution and then state is totally destroyed.

General n-qubit state: exponentially many components physically present for interference and physical state identity but mostly not accessible as information output!

In a more formal information theoretic setting:
“at most n bits of mutual information about the state identity can be obtained from a single copy of the state”.
Computational steps in circuit model: quantum gates

**Classical:** Boolean gate acting locally on a bit string

**Quantum:** unitary operations on vector space of states (states of qubit strings)

**Examples of quantum gates**

**NOT gate**  \[ a|0\rangle + b|1\rangle \rightarrow a|1\rangle + b|0\rangle \]

**NOT**:  \[ a|0\rangle + b|1\rangle + c|10\rangle \rightarrow a|10\rangle + b|11\rangle + c|11\rangle \]

**Hadamard gate**

\[ H|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \]
\[ H|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \]

\[ H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \]

**CNOT gate**

\[ \text{CNOT}: \begin{array}{c|c}
|00\rangle & |00\rangle \\
|01\rangle & |01\rangle \\
|10\rangle & |11\rangle \\
|11\rangle & |10\rangle \\
\end{array} \]

\[ \text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
\end{bmatrix} \]
Example of two H’s and interfering paths

\[ |0\rangle \xrightarrow{\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)} H \xrightarrow{\frac{1}{\sqrt{2}} \left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)} = |0\rangle \]

Thinking in terms of transitions and computational paths:

Since total prob = 1
If one outcome suppressed by destructive interference
Then some other outcome must be enhanced.
Computation by quantum parallelism

Can get exponentially large “parallelism” in polynomial time

\[ |0\rangle \ldots |0\rangle \]
\[ \downarrow H \ldots \downarrow H \quad \text{(n operations)} \]
\[ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \ldots \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \]
\[ = \frac{1}{\sqrt{2^n}} \sum_{\text{all } x} |x\rangle \]

Suppose we have a computational process that computes a function

\[ f : n-\text{bits} \rightarrow 1-\text{bit} \quad |x\rangle |0\rangle \rightarrow |x\rangle |f(x)\rangle \]

Then by linearity of the process:

\[ \sum_{\text{all } x} |x\rangle |0\rangle \rightarrow |f\rangle = \sum_{\text{all } x} |x\rangle |f(x)\rangle \]

|f\rangle encodes all values of f. But

Restrictions of quantum measurement -
What kind of information about f can we get from |f\rangle ?
Some computational tasks

**Deutsch-Jozsa problem (1992)**

*Given* a black box that computes \( f : n\text{-bits} \rightarrow 1\text{-bit} \)

*Promise:* \( f \) is either (a) a constant function (all values 0 or all 1),

or (b) a balanced function (50/50 values are 0/1).

*Problem:* decide (with certainty) which it is, with least number of queries to the box.

**Classically:** need \( \frac{2^n}{2} + 1 \) queries

**Quantumly:** one query suffices (plus \( O(n) \) overhead)

---

**What about NP complete problems?** –

*e.g.* SAT asks for only one bit of information about \( f : n\text{-bits} \rightarrow 1\text{-bit} \)

But “wrong kind” of information!

**Theorem (Grover’s quantum searching algorithm):**

*Given* \( f \) as a black box, to solve SAT

*(with high probability) we need* \( O(\sqrt{2^n}) \) *queries*

*(and this suffices).*

---

**So:** What “kind” of information is available from a multi-qubit state \( |\psi\rangle \)?
Important example: “pattern recognition”

$|\psi\rangle$ encodes many values of a periodic function $f$
(all computed in superposition with a single evaluation of $f$)
We can read out only a few selected values but alternatively
we can read out the single value of the period.
Classically need many explicit values of $f$ (a lot of computation)

**Shor’s quantum factoring algorithm**

Problem of number theory \[\xrightarrow{\text{Legendre \sim 1800}}\] Problem of determining a period

To factorise $N$ need period of $f : \mathbb{Z} \rightarrow \mathbb{Z}_N$ where $f(n) = c^n \mod N$ for $c < N$ coprime to $N$.

Then use a quantum period finding algorithm

Quantum factoring of $n$ digit number: $O(n^3)$ time

Best classical algorithm: $\exp(O(n^{\frac{1}{3}}(\log n)^{\frac{2}{3}}))$ time
Quantum Fourier transform

QFT on n qubits: usual discrete FT mod $2^n$

Matrix $[QFT]_{ab} = \frac{1}{\sqrt{2^n}} e^{\frac{2\pi i ab}{2^n}}$ is a unitary $2^n \times 2^n$ matrix

Many mathematical applications.
As a quantum operation, can be implemented by a quantum circuit of poly size $O(n^2)$.

Applying QFT to periodic states of the form $\frac{1}{\sqrt{A}} \left( |x_0\rangle + e^{2\pi i \frac{r}{A}} |x_0 + r\rangle + e^{2\pi i \frac{2r}{A}} |x_0 + 2r\rangle + \ldots + e^{2\pi i \frac{(A-1)r}{A}} |x_0 + (A-1)r\rangle \right)$

Allows us to efficiently extract the period value $r$. 

$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^k} \end{bmatrix}$
Further quantum algorithms based on FT -- One example:

**Pell’s equation**
Given integer $d$ find smallest integers $(x,y)$ solving $x^2 - dy^2 = 1$
Want poly(log $d$) time algorithm.
Fact: smallest solution can have exp(log $d$) digits!

Examples -- $d = 5$ has $x=9$ $y=4$.
$d = 6009$ has $x = 131634010632725315892594469510599473884013975$
$y = 1698114661157803451688949237883146576681664$

Ask instead for $R = \log(x + \sqrt{dy})$ (now log $d$ digits) to $n$ decimal places in poly (log $d$, $n$) time.

**Classical complexity:**
Best time: $\exp(\sqrt{\log d})$ assuming unproven GRH
(or $\exp(\frac{1}{4} \log d)$ without GRH).

**Hallgren (2002):**
Poly time quantum algorithm.
Some algebraic number theory – reduce solving Pell to periodicity of a function on real numbers, period = $R$.
Then use quantum FT techniques.
How can we find new quantum algorithms?
(identify problems that are “hard” for classical comp. but “easy” for quantum comp.)

1) Recast problems in a mathematical form that overlaps the math formalism of quantum theory (e.g. applications of FT in maths).

2) Develop other models of quantum computation (or alternative mathematical formalisms for quantum theory) which can suggest new algorithmic applications – quantum walks, quantum adiabatic algorithms, measurement-based quantum computation (hybrid classical-quantum) etc…

3) Concoct problems of simulation/properties of a quantum physical process - use a quantum computer to mimic the actual process itself!

Example. If \( H \) is a Hermitian matrix then \( U = e^{iHt} \) is unitary for all \( t \).
It can represent the time evolution of a quantum system.
Then \( H \sim \) energy of the system; eigenvalues of \( H \) are the possible energy values.
\( H \) is also called the Hamiltonian of the system.
Hence suitable mathematical questions about Hermitian matrices (and eigenvalues) can be translated into properties of quantum physical systems and investigated by quantum computation.
Identifying likely-hard problems for classical and quantum computation

**BQP complete problems** (complete relative to classical poly-time reductions)
These will be hard for classical computation if quantum computing has any extra power.

**Much recent work; producing examples:**

**Input:** a knot.
**Problem:** approximate evaluation of the Jones polynomial of the knot at fifth root of unity. (Freedman, Larsen, Wang 2002)

**Input:** real symmetric nxn matrix $A$ with poly-log nonzero entries in any row and integer $m=polylog(n)$ and integer $j$ between 1 and $n$.
**Problem:** estimate diagonal entry $[A^m]_{jj}$ to $1/polylog(n)$ accuracy. (Janzing, Wocjan 2006)

Also other hamiltonian problems.....
Problems hard for quantum computers
(e.g. for crypto secure against quantum attacks?...)

**QMA** – quantum generalisation of MA.
(Recall MA – probabilistic generalisation of NP as defined by
decision poly-time verifier and certificates).

“certificates of membership are quantum states and
the verifier is a quantum process”
Verifier V is now a quantum poly-time computation
acting on $|w>|c>$ such that:

**Completeness:**
if $w$ in $L$ then $\text{Prob}[V(|w>|c>=1] > 2/3$ for some quantum state $|c>$

**Soundness:**
if $w$ not in $L$ then $\text{Prob}[ V(|w>|c>)=1] < 1/3$ for all quantum states $|c>$

**QMA completeness:** relative to usual poly-time (classical) reductions.
5-local hamiltonian problem

**Given:** a 5-local hamiltonian $H$ on $n$ qubits
i.e. $H = H_1 + \ldots + H_r$ such that:
Each $H_i$ acts on at most 5 qubits;
r is $O(poly(n))$;
All $|\text{eigenvalues}|$ of $H_i$ are $\leq 1$;
Entries of each $H_i$ are given with $\text{poly}(n)$ bits;
Also given: constants $a$ and $b$ with $a < b$.

Let $L(H)$ be smallest eigenvalue of $H$
**Promise:** $L(H)$ is either smaller than $a$ or larger than $b$.
**Problem:** Is $L(H)$ smaller than $a$?

**Kitaev’s theorem:**
5-local hamiltonian problem is QMA complete.
(Subsequent improvements (Kempe, Regev, Kitaev) 5-local to 3-local to 2-local)
(Lack of) power of quantum computing
(and quantum computing vs. classical analog computing)

Quantum computation can efficiently process exponentially much information in the identity of an n-qubit state

$$\sum a_{i_1i_2...i_n} |i_1\rangle |i_2\rangle ... |i_n\rangle$$

But - classical analog computation: classical physics has even greater information processing power – real numbers are updated by physical evolution.

Fact: quantum formalism is based on continuous parameters too.
Question: Does power of quantum computing require (unreasonably) high precision of parameters?

$O(\log n)$ bits of precision in gates suffices to have

$$\sum |\Delta a_{i_1...i_n}|^2 \leq \epsilon \text{ (const)}$$
Classical analog computation

N bits \(i_1i_2\ldots i_N\) coded as digits of a real number \(x = 0.\overline{i_1i_2\ldots i_N}\).
Computational step \(x' = f(x)\) needs \(N\) bits of precision to develop all (high order) bits.

Seemingly reasonable assumption:
Effort required to operate with finer precision grows exponentially with number of bits of precision.
Is this necessary? Why not just poly effort?
Appears to fail in quantum theory…

Better classical way to store/process \(N\) bits:
Use \(O(N)\) real numbers with constant precision (1 or 2 bits each)
Then effort grows linearly with \(N\).
This is just classical digital computation.

But then processing possibilities more limited – local gates vs.
global processing of full information all at a single site.
Physical significance of computational complexity?

Both classical and quantum physics embody great computing power. But both theories limit our ability to harness it.

<table>
<thead>
<tr>
<th>Classical physics</th>
<th>Quantum physics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase of precision in devices</td>
<td>Restrictions of quantum measurement</td>
</tr>
<tr>
<td>requires exponential effort</td>
<td>~ inaccessibility of high precision</td>
</tr>
<tr>
<td></td>
<td>information content of a quantum state</td>
</tr>
</tbody>
</table>

Both classical and quantum physics appear to be unable to provide efficient solution of NPC problems.

-- non-typical of “toy” physical theories!

Elevate to a “computational physical principle”? “No physical theory should allow efficient solution of NPC problem”

-- very limiting restriction on form of future physical laws…