Foundations of quantum computing and complexity

Richard Jozsa

DAMTP University of Cambridge
Why quantum computing? - physics and computation

A key question: what is computation... fundamentally?
What makes it work? What determines its limitations?...

Information storage
bits 0,1 -- not abstract Boolean values but two distinguishable states of a physical system

"Information is physical!" "No information without representation!"

Information processing: updating information
A physical evolution of the information-carrying physical system

Hence (Deutsch 1985): Possibilities and limitations of information storage / processing / communication must all depend on the Laws of Physics and cannot be determined from mathematics alone!
Conventional computation (bits / Boolean operations etc.) based on structures from classical physics.

But classical physics has been superseded by quantum physics ...
Current very high interest in Quantum Computing

“Quantum supremacy”
expectation of imminent availability of a QC device that can perform some (albeit maybe not at all useful..) computational task beyond the capability of all currently existing classical computers.

More generally: many other applications of quantum computing and quantum information ideas:
Novel possibilities for
information security (quantum cryptography), communication (teleportation, quantum channels), ultra-high precision sensing, etc;

and with larger QC devices:
“useful” computational tasks (quantum algorithms offering significant benefits over possibilities of classical computing) such as:
Factoring and discrete logs evaluation;
Simulation of quantum systems: design of large molecules (quantum chemistry)
for new nano-materials, drugs etc.
Some kinds of optimisation tasks (semi-definite programming etc), search problems.

Currently: we’re on the cusp of a “quantum revolution in technology”.
**Novel quantum effects for computation and complexity**

Quantum entanglement;
Superposition/interference;
Quantum measurement.

Quantum processes cannot compute anything that’s not computable classically. But still have many benefits of complexity – Possible exponential reduction in complexity / cost of a computation.
Novel quantum effects for computation and complexity
Quantum entanglement;
Superposition/interference;
Quantum measurement.

Quantum processes cannot compute anything that’s not computable classically. But still have many benefits of complexity –
Possible exponential reduction in complexity / cost of a computation.

Basic notion of computational (time) complexity
Computational task has input: a bit string $i_1i_2\ldots i_n$ length $n =$ input size.
Computational process: sequence of elementary steps
each requiring constant (indep. of $n$) amount of resources to implement.
(e.g. classically, Boolean gates on 1 or 2 bits).
**Time complexity** \( T(n) = \text{number of steps as function of input size } n \)

(max over all inputs of size \( n \))

Key question: can the task be computed by a process that runs in polynomial time \( T(n) = O(\text{poly}(n)) \) (rather than say exponential time \( 2^{O(n)} \))? 

Poly time algorithms: called efficient; computation that’s “feasible in practice”.
Exponential (super-poly) time: viewed as effectively “uncomputable in practice”.

**Example:** Factoring \( N = i_1 \ldots i_n \) (n binary digits)

Best known classical algorithm \( T(n) = e^{O(n^{1/3} \log n^{2/3})} \) not poly time!
Shor’s quantum factoring algorithm \( T(n) = O(n^3) \)

Also: probabilistic algorithms – have access to random bits;
and want final answer to be correct with suitably high probability e.g. >2/3
Quantum entanglement

State space of any quantum physical system A always (unit vectors in) a Hilbert space $\mathcal{H}_A$ (for us finite dimensional)
Qubit: 2 dimensional space with orthonormal basis $\{|0\rangle, |1\rangle\}$ labelled by bit values 0 and 1.

Composite systems (AB) state space:
Quantum: tensor(!) product of individual state spaces $\mathcal{H}_A \otimes \mathcal{H}_B$
Classical: cartesian product of individual state spaces $S_A \times S_B$

So n qubits have $2^n$ (exponential in n) dimensional state space

Generally: composite of n instances of a system A has mathematical description:
Quantum: exponential number of parameters in n
Classical: linear number of parameters in n

\{ systems of same physical size in the two theories!

Entangled state of composite system: cannot be written as tensor product of individual subsystem states.
Product state: not entangled i.e. each subsystem has well defined separate state.
Quantum superposition / interference

Recall classical probabilistic computation - configurations of computer updated by sequence of (suitably local) probabilistic transitions.

"Sum over paths" rule:
- $P(c)$ final probability of $c$ -
- multip. along paths, then sum overall paths arriving at $c$.

Algebra:
- column vector $\mathbf{v} = (p_1, p_2, \ldots, p_N)$
- $p_i$ = prob of config $c_i$
- $\mathbf{v} = p_1 [00 \ldots] + p_2 [00 \ldots] + \ldots$
- Transitions: stochastic matrices $\mathbf{v} \rightarrow S \mathbf{v}$
- columns are transition probs for pure configurations.

"Sum over paths" rule = matrix multiplication of transition matrices.
Quantum computing: probabilities $p_i \rightarrow$ probability amplitudes $a_i$

real non-negative $\sum p_i = 1$

$L'$ norm = 1

complex $\sum |a_i|^2 = 1$

$L^2$ norm = 1

"sum over paths" rule:

$c A(c)$ final amplitude of $c$—multiply along paths, then sum over all paths arriving at $c$

But prob $P(c) = |A(c)|^2$ !

Algebra: column vector $|v\rangle = (a_1, \ldots, a_N)$ $a_i =$ amplitude of config $c_i$

$|v\rangle = a_1 |00, 0\rangle + a_2 |00, 1\rangle + \ldots$

Transitions: unitary matrices $|v\rangle \rightarrow U |v\rangle$, preserves $L^2$ norm

So also columns are orthonormal vectors!

At any stage for $c_i \neq c_j$:

have $U |c_i\rangle \perp U |c_j\rangle$
Example: classical bit

Stochastic $T = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$, two transitions

\[
\begin{array}{ccc}
\frac{1}{2} & \rightarrow & 0 \\
0 & \rightarrow & \frac{1}{2} \\
\frac{1}{2} & \rightarrow & 1 \\
0 & \rightarrow & 0 \\
\end{array}
\]

Pr(0) = $\frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}$

Pr(1) = $\frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}$

Vectors:

\[
\begin{pmatrix} 0 \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} \rightarrow \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}
\]

Can simulate process by probabilistic choice of a single path through the tree.

So can efficiently simulate exponentially big (poly-depth) trees!
Example: "quantum" bit - qubit

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

Transitions:

\[ 0 \xrightarrow{\frac{1}{2}} 0 \]
\[ 0 \xrightarrow{\frac{1}{2}} 1 \]
\[ 1 \xrightarrow{-\frac{1}{2}} 0 \]
\[ 1 \xrightarrow{-\frac{1}{2}} 1 \]

\[ \psi(0) = \left| \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \right|^2 = 1 \]

\[ \psi(1) = \left| \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} (-\frac{1}{\sqrt{2}}) \right|^2 = 0 \]

Vectors:

\[ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \]

- non-zero paths 0 \rightarrow 1 but transition forbidden!
- at intermediate stage both 0 & 1 need to be "present"
  "in superposition" to interfere destructively at end.
- So cannot simulate process by a choice of single path through tree! Some kind of weighted non-deterministic computation?

\[ \]
Quantum measurement – readout of final classical answer

For the state $|\psi\rangle = \sum a_i |i_i..i_n\rangle$

If measure all qubits, see $i_i..i_n$ with prob $|a_i..a_n|^2$

and after mnt, state “collapses” to see $|i_i..i_n\rangle$!

(even though all “present” before – cf classical: sample and look again, will always see same result again, but only one was present initally!)

If measure only first (say) qubit:

write $|\psi\rangle = |0\rangle |\psi_0\rangle + |1\rangle |\psi_1\rangle$

Then see $i$ with prob $p(i) = |\langle 0 |\psi_i \rangle|^2$

and after mnt, state collapses to see $|i\rangle |\psi_i\rangle$, renormalised to length 1.

Same holds for intermediate measurement – destroys presence of all paths except those consistent with seen outcome!

Intuition. $|\psi\rangle$ can encode $2^n$ configurations in superposition for unitary processing, but have very little access to encoded info for read-outs!
Fundamental example

If $f: n$-bits $\rightarrow 1$-bit is efficiently computable boolean function, can efficiently make

$$|v\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle |f(i)\rangle$$

encodes all $2^n f$-values!

- From $|v\rangle$ can get small amount of “global” information about all $f$-values that’s hard to get classically!

“Pattern recognition” e.g. $f$ constant vs. $f$ balanced; and
Periodicity determination (Shor’s efficient factoring algorithm)

Satisfiability? just 1 bit of info! but alas “wrong kind of info…”

Grover’s quantum searching algorithm: if $f$ used as black box then

$O(\sqrt{2^n})$ queries are necessary and sufficient for a quantum algorithm
to decide SAT.
Classical simulation of a quantum circuit $C$

Given: (description of $C$, its input, output lines)
- list of gates (usually many, often one (decision problem))
- lines of action

Let $N =$ circuit size $=$ number of gates in $C$ (usually $\text{poly}(n)$)

Weak simulation: a sample of its output distribution (by classical means)
Strong simulation: calculate any output prob. or marginal

Weak efficient simulation: as above, in classical $\text{poly}(n)$ time
Strong efficient simulation: calculate any prob. or marginal to $K$ digits in $\text{poly}(K, N)$ time.
Remarks

Quantum process $C$ itself gives only a sample of output distribution and strong simulation is asking for much more. Weak efficient classical simulation of $C$ means: “no quantum computational benefit over classical”.

Can show:
Strong implies weak simulation (need marginals for this).
If weak implies strong, then $P = NP$.

Direct strong simulation:
Circuit is just simple linear algebra! (matrix multiplications), so just calculate evolving state etc.
Difficulty - each extra qubit doubles the dimension so typically get exponentially growing calculational effort with number of steps.
But – if all states remain product states throughout then all updates can be computed in poly time.
Hence – presence of entanglement is necessary for quantum computational benefit (but not sufficient...
More generally: using theory of tensor network contractions

Theorem (Markov and Shi 2005, RJ 2006)
Any log depth circuit of bounded range gates (with input any product state) can be classically strongly efficiently simulated.

Proof idea

Quantum rules ⇒ probe \( p = V_{a b} W_{c d} x a \cdots z b \)

are contractions of tensors corresponding to gates in circuit.

Want: contraction ordering so that intermediate tensors never accumulate more than \( O(n \log n) \) indices, so stay poly-sized.

\( T_{b_1, \ldots, b_k} \) has \( O(2^{2k}) \) components.

Fact (Cleve & Watrous 2000): Shor’s quantum factoring algorithm can be presented as a log depth circuit but gates are not of bounded range!
Pauli and Clifford operations

Pauli matrices (1-qubit operations; both unitary and hermitian)

\[
I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}
\]

1-qubit Pauli group \( \mathcal{P}_1 \) generated by \( I, X, Y, Z \) \( = \{ \pm P, \pm iP : P \text{ Pauli} \} \)

n-qubit Pauli group \( \mathcal{P}_n = \mathcal{P}_1 \otimes \ldots \otimes \mathcal{P}_1 \subseteq U(2^n) \)

Clifford group \( \mathcal{C} \) : normaliser of \( \mathcal{P}_n \) in \( U(2^n) \)

i.e. \( \mathcal{C} \in U(2^n) \) is Clifford iff for all \( P_1, \ldots, P_n \) there are \( P'_1, \ldots, P'_n \) with

\[
\mathcal{C} (P_1 \otimes \ldots \otimes P_n) C^\dagger = k (P'_1 \otimes \ldots \otimes P'_n) \quad k = \pm 1, \pm i
\]
Theorem

**C is Clifford iff** C is a circuit of

\[
H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} 
\]  
(Hadamard gate)

1-qubit gates:

\[
S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} 
\]  
(\(\frac{\pi}{2}\) phase gate)

And the 2-qubit gate: \(CX\) controlled-X gate \(|k\rangle|l\rangle \to |k\rangle X^k |l\rangle\) \(k, l = 0, 1\)

(so in particular get all Pauli’s \(SS = Z\) \(HZH = X\) etc.)

Note: Clifford circuits can generate entanglement e.g.

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

And similarly for any number of qubits.
Gottesman-Knill theorem (variant)
Consider any Clifford circuit $C$ on $n$ lines (comprising $N=\text{poly}(n)$ H, S, CX gates) with
(i) any product input state $\ket{\psi} = \ket{a_1}\ket{a_2} \ldots \ket{a_n}$
(ii) single line output.
Then it can be classically efficiently strongly simulated.

Proof outline
$C\ket{\psi} = C_N \ldots C_1 \ket{\psi}$
Measure say first line. Get probabilities $p_0, p_1$. Then by quantum rules:
\[
p_0 - p_1 = \bra{\psi} C_N^\dagger \ldots C_1^\dagger Z_1 C_1 \ldots C_N \ket{\psi} \quad Z_1 = Z \otimes I \otimes \ldots \otimes I \in \mathcal{P}_n
\]
So \[
C_N^\dagger \ldots C_1^\dagger Z_1 C_1 \ldots C_N = P_1 \otimes \ldots \otimes P_n \quad \text{for some Pauli's } P_i
\]
which can be determined in $\text{poly}(N) = \text{poly}(n)$ time by $N$ successive conjugations on 1 or 2 lines each. So:
\[
p_0 - p_1 = \bra{a_n} \ldots \bra{a_1} (P_1 \otimes \ldots \otimes P_n) \ket{a_1} \ldots \ket{a_n} = \prod_{i=1}^{n} \bra{a_i} P_i \ket{a_i}
\]
i.e. 2X2 matrix multiplications, $n$ of them, so computable in $\text{poly}(n)$ time, so output probabilities computable in $\text{poly}(n)$ time too.
A further ingredient
Now allow also intermediate 1-qubit measurements (in $\{|0\rangle, |1\rangle\}$ basis) within the Clifford circuit.

Circuit can be either

- **non-adaptive**
  - choice of later gates
  - can *not* depend on earlier

- **adaptive**
  - measurement outcomes

Then have **Theorem:**

Non-adaptive Clifford circuits remain classically efficiently strongly simulatable; Adaptive Clifford circuits are universal for quantum computation!
So we have: for Clifford circuits with product-state inputs, single line outputs, & allowing intermediate units—
(a) non-adaptive - is classically simulatable (even strongly)

(b) adaptive - has full universal quantum computing power.

i.e. for Clifford C_k's, M(i,y) = "measure line i, get result y = 0 or 1"
(a): C_0 M(i_1,y_1) C_1 M(i_2,y_2) C_2 ...
(b): C_0 M(i_1,y_1) C_1(y_1) M(i_2,y_2) C_2(y_1,y_2) ...

Purely classical ingredient viz adaptive choice of gates is resource that gives full quantum computing power from classically limited power!

Experimentally: no difference between (a) & (b)! —
no new quantum processes in (b) that do not occur in (a)!

- experimenter being instructed on sequence of operations
  cannot tell if instructor is using (a) or (b)!
Is there a fundamental complexity principle for physics?

For example: central significance of P vs. NP issue in complexity theory may(?) suggest:

“No physical process should be able to compute an NP-complete problem with poly-resources”.

Appears to be true of both classical and quantum physics

despite the fact that

both theories appear to involve massive computing power
(well sufficient for NP) but both limit our access to it! (in different ways).
(cf. in similar vein - quantum non-locality yet no-signalling!...)

*Modifications of quantum mechanics generally have immense computing power - above principle appears to be very restrictive for form of physical laws.*
Classical physics

Physical evolution updates real numbers – infinite information content!
e.g. N-bit input $i_1i_2..i_N$ can be encoded as $x = 0.i_1i_2..i_N$
Computational step $x' = f(x)$ needs $N$ bits of precision in implementation
(analog computation) to preserve the information.

But – instability of analog computation:
Higher order digits become “exponentially fragile” -
to control evolution of parameters to $n$ digits of accuracy we need to
invest $O(\exp(n))$ physical resources (error tolerance of $1/\exp(n)$)

Remedy:
For $n$ digits of information,
instead of single parameter/system with $n$ digits ($\exp(n)$ cost)
use
$O(n)$ parameters/systems to const number of digits each –
now only linear($n$) cost!
i.e. digital computation, stable but at expense of losing
many-digit (i.e. $O(n)$) processing per single step!
Quantum physics

Entanglement
Composite of n similar systems – $O(\exp(n))$ parameters; can all be updated efficiently by just local actions.
(Classically no entanglement; only $O(n)$ parameters here!)

\[ \frac{1}{\sqrt{2^n}} \sum_{x} |x \rangle |f(x)\rangle \]

Can be produced in linear time + 1 application of $f$.
State identity contains information of SAT problem.
Quantum physics (cont.)

Quantum computing also uses continuous (analog) parameters but it is not subject to instabilities of classical analog computation!
- deep rooted linearity and unitarity in quantum principles avoids exponential sensitivity to perturbations.
- there is a fault tolerance threshold theorem for quantum computing (but not for classical analog computing).
  so (unlike classical analog computing) we can “process exponentially much information” with poly effort.

But now quantum measurement theory limits access to full state identity!
Its destructive effects are remarkably finely balanced against exponential computational benefits of entanglement.
So
Both classical (analog) and quantum evolution implicitly contain computing power sufficient to solve NP complete problems. But both theories impose an exponential cost to our access to the processed information, in seemingly different ways.

Interesting point is not so much power of quantum computing as lack of power of quantum computing — a consequence of the laws of quantum (measurement) theory.

*Can we understand origin of quantum laws (measurement rules etc.) from computational complexity principles? Can a physical quantum computing device help explore such foundational issues? Test the validity of quantum theory? hmm...*