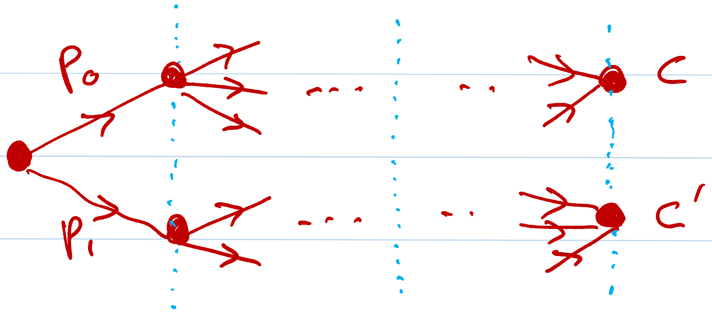
Comparing classical and quantum complexity

Richard Jozsa
DAMTP, University of Cambridge
UK

What is quantum computing?

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 –
mult. along paths, then
sum over all paths arriving at c.

Algebra: column vector $\underline{v} = (p_1, p_2, \ldots p_N)$ $\quad p_i$ = prob of config c_i

$$\underline{v} = p_1 [00..0] + p_2 [00..1] + \ldots$$

transitions: stochastic matrices $\underline{v} \to S\underline{v}$ ← preserves L^1 norm

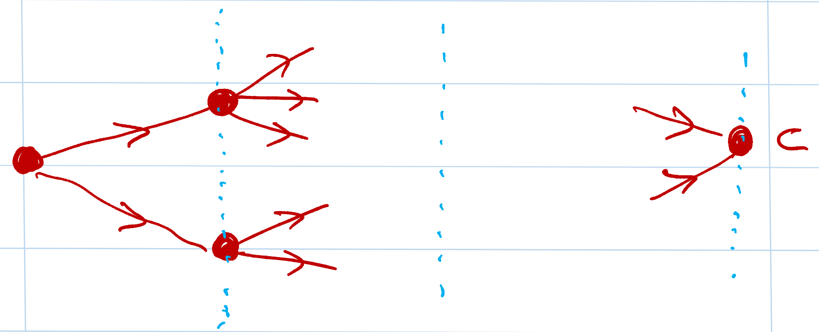
columns are transition probs. for pure configurations.

"sum over paths" rule $\equiv$ matrix multiplication of transition matrices.

Quantum computing: probabilities $p_i \rightsquigarrow$ probability amplitudes a_i

real +ve $\Sigma p_i = 1$ complex $\Sigma |a_i|^2 = 1$

L^1 norm $= 1$ L^2 norm $= 1$



"Sum over paths" rule:

$A(c)$ 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 $|v\rangle \to U|v\rangle$, preserves L^2 norm

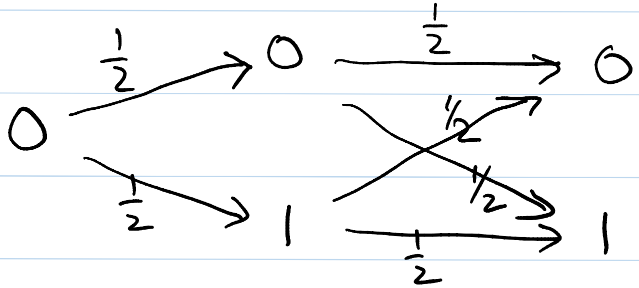
So also columns are orthonormal vectors!

At any stage for $c_i \neq c_j$ have $Uc_i \perp Uc_j$

no analogous compatability condition for L^1!

Example: classical bit

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



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

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

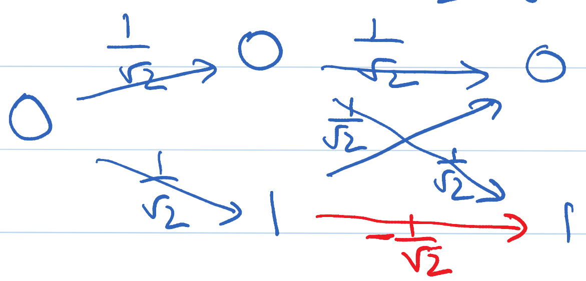
vectors: $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} \rightsquigarrow \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$

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

So can <u>efficiently</u> simulate exponentially big (poly depth) trees!

Example: "quantum" bit — qubit

Unitary $H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$, two transitions



$$pr(0) = \left| \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \right|^2 = 1$$

$$pr(1) = \left| \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \left(-\frac{1}{\sqrt{2}}\right) \right|^2 = 0 \ !$$

Vectors: $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \longrightarrow \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \longrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

- non-zero paths $0 \rightsquigarrow 1$ but transition is 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 a single path through tree! ← a kind of "weighted non-deterministic" computation? ...

Circuit model of computation

Classical $\underline{v} = p_0\,[00..0] + p_1\,[00..1] + \ldots$

updated by circuit of local stochastic Boolean gates.

To sample final distribution, suffices to sample individual dist^{ns} of steps sequentially, carrying along only a single bit string.

Quantum $|v\rangle = a_0\,|00..0\rangle + a_1\,|00..1\rangle + \ldots$

updated by local unitary gates.

To sample final distribution cannot do it by sequentially returning single/small description - need to generally carry full exponentially growing description of $|v\rangle$!

n-qubit state: $|v\rangle = \sum_{i_1..i_n=0}^{1} a_{i_1..i_n}\,|i_1..i_n\rangle$

Quantum measurement - readout of classical answers

For the state $|v\rangle = \sum a_{i_1 \dots i_n} |i_1 \dots i_n\rangle$

if we measure all qubits, see $i_1 \dots i_n$ with prob $|a_{i_1 \dots i_n}|^2$

and after mmt, state "collapses" to seen $|i_1 \dots i_n\rangle$!

(even though all "present" before - cf classical: sample and look again, will always see same result again, but only one was present initially!)

If measure only first (say) qubit:

write $|v\rangle = |0\rangle|v_0\rangle + |1\rangle|v_1\rangle$

then see i with $\text{prob}(i) = \| |v_i\rangle \|^2$

and after mmt, state collapses to seen $|i\rangle|v_i\rangle$ re-normalised to length 1.

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

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

Iconic Example

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

$$|v\rangle = \frac{1}{\sqrt{2^n}} \sum_{\text{all } \underline{i}} |\underline{i}\rangle |f(\underline{i})\rangle$$

encodes all 2^n f-values!

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

$\downarrow H \otimes \cdots \otimes H$

$\frac{1}{\sqrt{2^n}} \sum_{\underline{i}} |\underline{i}\rangle$

- from $|v\rangle$ can get small amount of "global" information about all f-values, that's hard to get classically!

sometimes even with prob 1

! Satisfiability? just 1 bit of info! but alas "wrong kind of info..."

Grover's quantum searching algorithm (1996): if f used as black box then $O(\sqrt{2^n})$ queries are necessary and sufficient for a quantum algorithm to decide SAT.

How can we find new quantum algorithms?

- different from finding new classical algorithms!?

Use: serendipitous coincidences between well known pure math constructs and the math formalism of quantum physics (expressed in various ways...)

Example: discrete Fourier transform in C19 maths is linear & unitary!
- hence candidate for a quantum gate/evolution.

Shor (1994) –

Problem of factoring $\xrightarrow[\text{(Legendre c. 1800)}]{\text{old number theory}}$ Periodicity of efficiently comp. $f : \mathbb{N} \to \mathbb{N}$ $\xrightarrow[\text{of FT}]{\text{quantum use}}$ efficient period extraction & hence factoring.

In contrast: how to find new classical factoring algorithm?
- study latest research in number theory... i.e. new maths!

Notable feature of many quantum benefits –

For FT (and other quantum gates) data generally needs to be encoded in "quantum" form as amplitudes – exponentially smaller physical system than classical representation!

e.g. values of Boolean $f: n\text{-bits} \to 1\text{-bit}$ represented classically as bit string of length 2^n (v. long!)

quantumly as amplitudes of n (or $n+1$) qubit state (expon. smaller!)

Exponential number of parameters in

$$|v\rangle = \sum a_{i_1 \ldots i_n} |i_1 \ldots i_n\rangle \quad \sim \text{"entanglement"}$$

vs. product state $|v\rangle = \left(\sum_{i_1} a_{i_1} |i_1\rangle\right)\left(\sum_{i_2} a_{i_2} |i_2\rangle\right) \ldots \left(\sum_{i_n} a_{i_n} |i_n\rangle\right)$

i.e. $a_{i_1 \ldots i_n}$ factorises as $a_{i_1} a_{i_2} \ldots a_{i_n}$.

having each qubit in separate pure state and only $O(n)$ parameters.

Classical physics: composite systems always in such a product state of each subsystem, having only $O(n)$ growth of param's with system size!

Classical simulation of a quantum circuit C

Given: (description of C, its input, output lines)

↗ list of gates and lines of action

↗ usually $|i_1 .. i_n\rangle$ or $|\alpha_1\rangle|\alpha_2\rangle .. |\alpha_n\rangle$

↗ often one (decision problem) but maybe more

Let N = circuit size = number of gates in C (usually 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 poly(N) time.

Strong efficient simulation: calculate any prob. or marginal to K digits in poly (K, N) time.

Remarks

- can show strong $\Rightarrow$ weak (need calc. of marginals!)
  weak $\not\Rightarrow$ strong (unless $P = NP = \#P$)
- weak efficient simulation of $C \Rightarrow$
  "no quantum comp. benefit over classical computing"

Henceforth write weak/strong for efficient weak/strong

Issues to explore:

① find classes A of quantum circuits that are classically efficiently simulatable ("computationally lame" but interesting...)

② given a class A as in ①, what extra feature suffices to re-gain full universal quantum computing power?
~ candidates for the "mystery quantum resource"...

Direct strong simulation

Circuit = just simple linear algebra! (matrix multiplication)

So calculate components of evolving state?

Problem: each extra qubit ⇝ doubles dim & # components

⇝ typically exponential calc. effort with # steps!

e.g. n qubit $|\psi\rangle = \sum c_{i_1 \ldots i_n} |i_1 \ldots i_n\rangle$

Apply V on qubits 1&2 : $V|\psi\rangle = \sum c'_{i_1 \ldots i_n} |i_1 \ldots i_n\rangle$

$$c'_{i_1 \ldots i_n} = V^{j_1 j_2}_{i_1 i_2} \, c_{j_1 j_2 \underbrace{i_3 \ldots i_n}}$$

2^{n-2} strings!

But if all states are product states $c_{i_1 \ldots i_n} = a_{i_1} b_{i_2} c_{i_3} \ldots$

then $a'_{i_1} b'_{i_2} \ldots = \left(V^{j_1 j_2}_{i_1 i_2} a_{j_1} b_{j_2} \right) \left(c_{i_3} \ldots \right)$

update can be computed in poly(n) time!

Hence: presence of entanglement is necessary for quantum computational benefit (but it is not sufficient! ...)

Using theory of tensor network contractions:

Theorem (Markov & Shi 2005, R.J. 2006)

Any log depth circuit of bounded range gates (with input any product state) can be classically strongly simulated. □

Proof idea

Quantum rules ⇒ probs $p = V^{cd}_{ab} \, W^{\cdot\cdot}_{c\cdot\cdot} \, X^{a\cdot\cdot}_{d\cdot\cdot} \, Z^{b}_{\cdot\cdot}$

are contractions of tensors corresponding to gates in circuit.

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

$\left(T^{a_1 \ldots a_k}_{b_1 \ldots b_k} \text{ has } O(2^{2k}) \text{ components} \right)$

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

Clifford circuits

Clifford gates: $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$, CNOT

$|0\rangle|b\rangle \to |0\rangle|b\rangle$
$|1\rangle|b\rangle \to |1\rangle|\text{NOT } b\rangle$

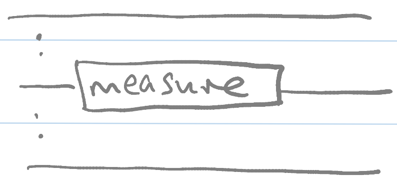
Further possible ingredients (cf. RJ & M. van den Nest 2014 - for more too)

(A) Input states: allow general product states $|\alpha_1\rangle \ldots |\alpha_n\rangle$

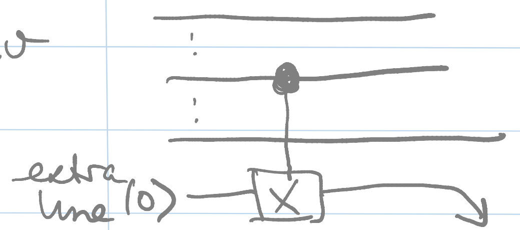
(B) Allow measurements (in standard basis $|0\rangle, |1\rangle$ only) in body of circuit with either

(i) non-adaptive: } choice of { can not } depend on earlier
or (ii) adaptive: } later gates { can } mmt outcomes.

Easy to see: circuits with non-adaptive mmts
$\equiv$ Clifford circuits with <u>no</u> intermediate mmts.



equiv to



(and CX is Clifford.)

Theorem For Clifford circuits with product state inputs, intermediate mmts, single bit final output:

(a) (Gottesman-Knill variant)
If mmts non-adaptive then classically strongly simulatable.

(b) If mmt adaptive then strong simulation is #P-hard and weak simulation is "QC-hard"
i.e. can do universal quantum computing with such circuits.

Remark: for (a) –

- contraction ordering method does not work for proof.
- can generate lots of entanglement.
- proof relies on special algebraic & group theoretic properties of Clifford gates (relation to Pauli group $P_n < U(2^n)$ whose elements are described by only poly(n) bits ...)

So we have: for Clifford circuits with product state inputs, single line outputs, & allowing intermediate mmts —

(a) non adaptive – is classically simulatable (even strongly)

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

i.e. for Clifford C_k's, $M(i,y) \equiv$ "measure line i, get result $y = 0$ or 1"

(a): $C_0 \; M(i_1, y_1) \; C_1 \; M(i_2, y_2) \; C_2 \ldots$

(b) $C_0 \; M(i_1, y_1) \; C_1(y_1) \; M(i_2, y_2) \; C_2(y_1, y_2) \ldots$

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) !

Quantum matchgate computations

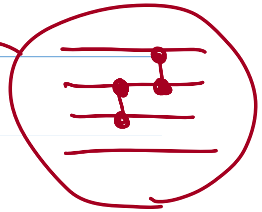
Matchgate (2-qubit gate)
$$G(A,B) = \begin{bmatrix} p & 0 & 0 & q \\ 0 & a & b & 0 \\ 0 & c & d & 0 \\ r & 0 & 0 & s \end{bmatrix} \qquad A = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \qquad B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

with A, B both in $SU(2)$ (or $U(2)$ with same determinant)

Theorem (Valiant 2000; Knill, Terhal & diVincenzo 2001; RJ & A. Miyake 2008)

Consider any circuit of matchgates such that:

- $G(A,B)$'s act on nearest-neighbour (n.n.) lines only
- output is measurement on any single line.



Then output can be classically efficiently simulated. □

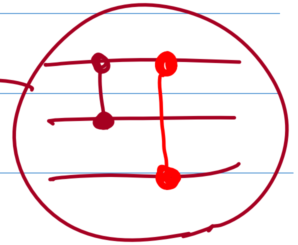
Remark: actually equivalent to known simulation of non-interacting fermions in quantum many-body physics (~1980's)

Valiant: special case of his theory of (classical) 'holographic algorithms' relations to computing perfect matching sums in weighted graphs.

Matchgates (cont.)

<u>Theorem</u> (R.J. & A. Miyake 2008)

If we allow $G(A,B)$'s to act on n.n. lines and just next-n.n. lines then we regain full universal quantum computing!



! Significance of $SWAP = G(I, X)$

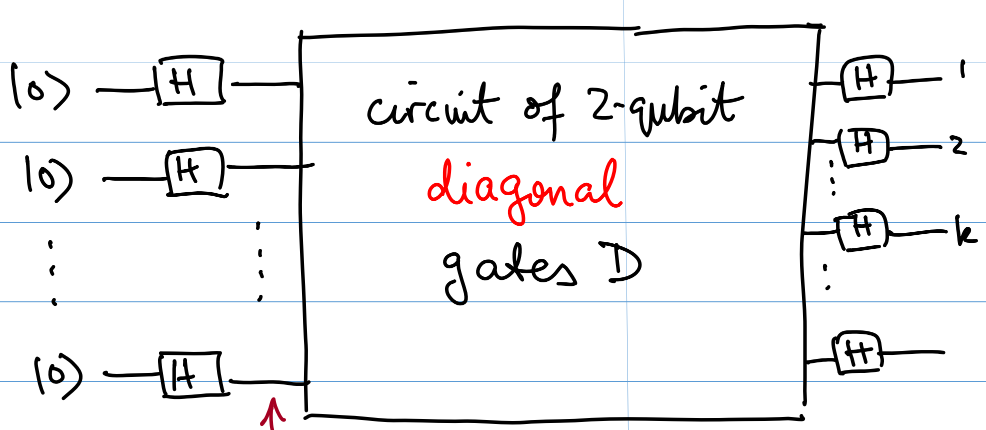
↳ not a valid matchgate as $\det I = 1$ & $\det X = -1$.

Suggests that relation between classical & quantum computing power may be "delicate"?

but...

"Instantaneous" quantum computation

Circuits of commuting gates!



measure any choice of k lines. Get $i_1 \ldots i_k$ with prob$(i_1 \ldots i_k)$.

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

state here is $\frac{1}{\sqrt{2^n}} \sum_{\text{all } i_1 \ldots i_n} |i_1 i_2 \ldots i_n\rangle$

$$D = \begin{bmatrix} e^{i\theta_1} & & & \\ & e^{i\theta_2} & & 0 \\ & 0 & e^{i\theta_3} & \\ & & & e^{i\theta_4} \end{bmatrix}$$

and suffices for θ's to all be multiples of $\pi/8$.

IQC (cont.)

<u>Theorem</u> (M. Bremner, R.J., D. Shepherd 2010)

(a) If $k = O(\log n)$ (i.e. small vs n) then can classically efficiently simulate output.

(b) If $k = O(n)$ then classical efficient simulation (even up to a generous multiplicative error) implies collapse of infinite tower of complexity classes called the polynomial hierarchy (PH) to its third level. $\square$

implausible like P=NP

Hence: even such (very simple) quantum processes are likely to exceed the power of efficient classical computation!

Is there a fundamental complexity principle for physics?

"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).

Modifications of quantum mechanics often have immense computing power.

Classical physics

Physical evolution updates real numbers – infinite information content!
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
high precision processing per single step!

Quantum physics

Entanglement

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

e.g. for Boolean function f

$$\frac{1}{\sqrt{2^n}} \sum_{\text{all } x} |x\rangle |f(x)\rangle$$

can be produced in linear time + 1 application of f.
State identity contains information of SAT problem.

But now **quantum measurement theory** limits access to full state identity!
Its destructive effects finely balanced against exponential benefits of entanglement.

All suggestive of a fundamental significance for computational complexity theory in the foundations of physics?