Computation & Entanglement

Richard Jozsa
Univ. Bristol, U.K.

mostly joint work with
Noah Linden (Bristol)

Why is entanglement good for computation?

(in contrast to communication)

Representing information:

- information stored in identity of a physical state
- information content of a physical system
  ~ number of parameters needed to describe system.

Then:

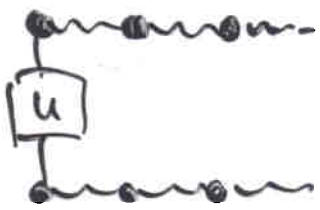
Quantum: n qubits $O(2^n)$ parameters (exponential in n)

Classical: n bits $O(n)$ parameters (linear in n)

(or any given physical system, n times over.)

Processing Information (= changing the state identity)

Simplest scenario:



$$|\psi\rangle = \sum_{i_1, i_2 \ldots i_n} a_{i_1 i_2 \ldots i_n} |i_1\rangle \ldots |i_n\rangle$$

$$|\psi'\rangle = \sum_{i_1 \ldots i_n} a'_{i_1 \ldots i_n} |i_1\rangle \ldots |i_n\rangle$$

$$a'_{i_1 i_2 \ldots i_n} = \sum_{j_1=0}^{1} U_{i_1 j_1} a_{j_1 i_2 \ldots i_n}$$

One step of quantum computation but exponentially many steps for direct classical calculation!

Unless:

unentangled state:

$$a_{i_1 i_2 \ldots i_n} = a^{(1)}_{i_1} \cdot a^{(2)}_{i_2} \cdots a^{(n)}_{i_n}$$

so $$a'_{i_1 \ldots i_n} = \left(\sum_{j_1} U_{i_1 j_1} a^{(1)}_{j_1} \right) a^{(2)}_{i_2} \ldots a^{(n)}_{i_n}$$

now only a constant sized calculation!

Using this, can show:

"no entanglement" $\Rightarrow$ "no computational benefit" !

(for pure states)

Quantum Computational Process - Toy model

- start with input

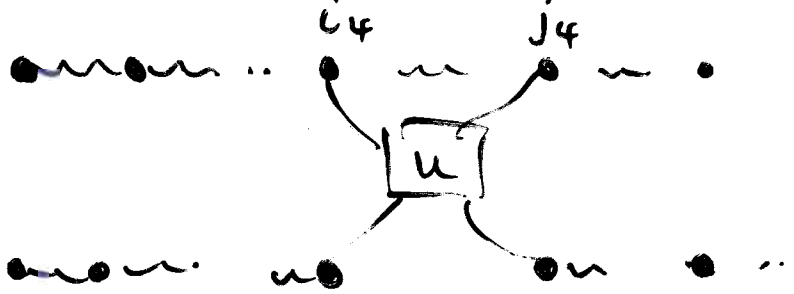
$$|i_1\rangle|i_2\rangle \ldots |i_n\rangle |0\rangle|0\rangle \ldots |0\rangle \ldots$$

($|i_1\rangle|i_2\rangle \ldots |i_n\rangle$: input size n)

- For each input size n, have a prescribed sequence of: n 2-qubit gates & which pairs of qubits to apply them to. ("the program")

step k: apply chosen U to qubits (i_k, j_k) & replace.

eg step 4



- After n steps, measure first qubit for 0 vs 1.

Classical simulation requirement:

given the prescription of the program, want to sample final probability distribution (once) in $\text{poly}(n)$ time using a classical process i.e. a classical computer with random choices!

(... instead of measuring the quantum state ...)

One classical simulation method:

1. Just calculate the state at each step
   (simple linear algebra)
2. Compute final probability distribution
3. Toss a weighted coin.

But: exp. time (and exp space, but can reduce to poly-space)

Note: Get far too much information!
- the full identity of the final state

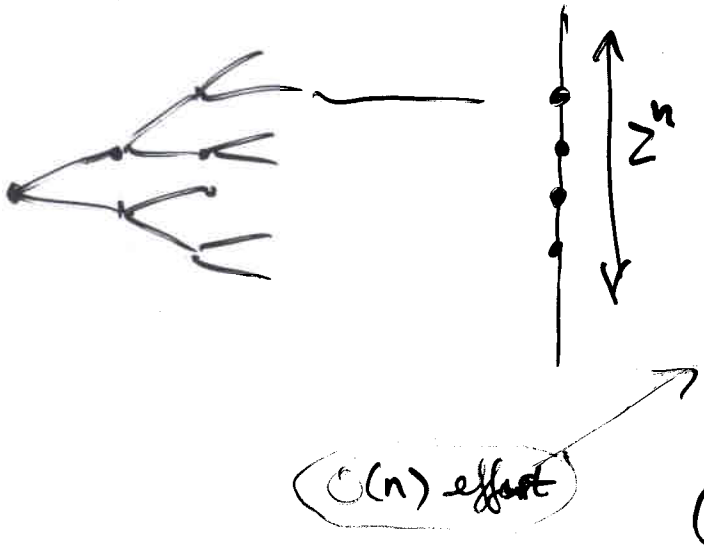
(Running the quantum process itself will not yield this!)

A further simulation method:

Classical probabilistic process

- also has exp large branching tree for full state description

e.g. toss a coin n times $\rightsquigarrow 2^n$ outcomes exp large!

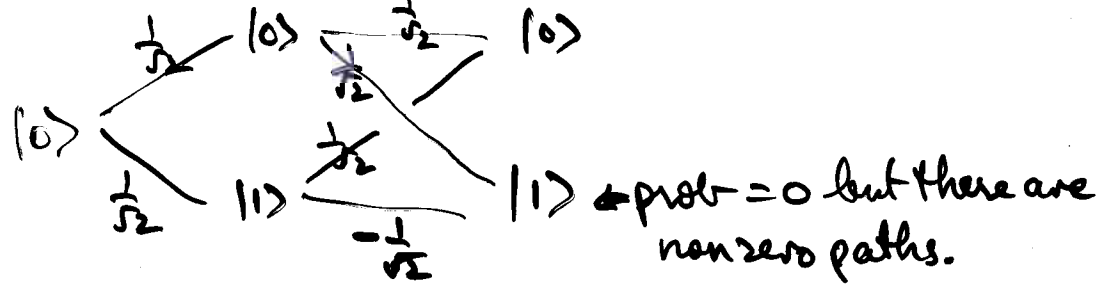


but can sample final prob. distribution once by probabilistic choices
→ follow one path through the tree, chosen with correct branching probs.
(and not compute whole distribution)

Doesn't work for tree of amplitudes?:

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

e.g. H.H on $|0\rangle$:



← prob = 0 but there are non-zero paths.

"final probs depend "globally" on whole tree?.."

More subtle use of probabilistic choice to simulate the quantum branching tree??
Feynman — discrete Wigner function → negative probabilities!
still "global"!!

Entanglement & simulation by classical calculation:

For p (fixed) & n (varying) a pure state of n qubits is called <u>p-blocked</u> if no $(p+1)$ qubits are entangled together.

(N. Linden & R.J. (quant-ph/0201143))

e.g. 3-blocked: at most 3 qubits entg together

Theorem: Consider any quantum computational process on pure states (with increasing input sizes n)
Suppose there is a p such that the states are p-blocked at every stage.
Then the computation can be efficiently classically simulated.

- Hence to see an exp speedup in a quantum algorithm, increasing input sizes <u>must</u> use increasing <u>multi</u>-party entanglement (e.g. more bi-partite entg is not sufficient)

  ↑ locate it in, say, Shor's algorithm!..

- p-blocking $\Rightarrow$ n-qubit state has poly(n) sized description

  $\frac{n}{p}$ blocks, 2^p parameters each, list of n numbers giving block number of each qubit $\Rightarrow O(n)$ parameters

Theorem (quant-ph/0201143)

Quantum computational process, input size n, runtime $T = \text{poly}(n)$.

Let α_j = state at step j. β = final output probability distribution.

Suppose α_j are not exactly p-blocked but there exists a sequence of p-blocked states β_j (identities generally unknown) such that

$$\| \alpha_j - \beta_j \| \leq \epsilon$$

Then for any $\eta > 0$

if $\epsilon \leq \frac{\eta}{4} c^T$ $\left(\text{for } c = \frac{1}{2p+4}\right)$

we can classically sample a distribution β' with $\| \beta - \beta' \| \leq \eta$ using $\text{poly}(T, \log 1/\eta)$ steps.

Complications (see quant-ph/0201143)

* block structure can change - need to keep track of this.
* precision of arithmetical calculations?
  e.g. if exactly p-blocked process requires infinite precision parameters: approximate by "rational" gates, but then not p-blocked states!

  But show: can simulate process classically efficiently to within an accuracy (ϵ) if states are not exactly p-blocked, but suitably near to (unknown) p-blocked states.

Some consequences of the theorem:

For exponential benefit of quantum over classical computation, on pure states:

* any amount of just bi partite entanglement is no use! (cf communication).
* it's not enough that every qubit is entangled with every other, at some stage
* distributed quantum computing: many local bounded-size quantum processors in only classical communication — no use!

Another view of this result:

Our classical computational simulation of quantum algorithm is tied to choice of mathematical representation of states.

i.e. description via amplitudes in computational basis
(just one possible such choice)

For this choice

absence of entanglement $\Rightarrow$ polynomial sized descriptions $\Rightarrow$ efficient classical simulation is possible for processes with no entanglement

Hence "entanglement is "necessary resource" for computational benefit."

But: other descriptions (which are mathematically equivalent) have different conditions guaranteeing poly-sized descriptions!

For any description $\mathcal{D}$ have "property" $P(\mathcal{D})$ such that:

absence of $P(\mathcal{D})$ in n qubit states $\Rightarrow$ polynomial sized $\mathcal{D}$-description of the state

So absence of $P(\mathcal{D}) \Rightarrow$ efficient classical simulation by calculating in the $\mathcal{D}$ description

i.e. for any $\mathcal{D}$, $P(\mathcal{D})$ is "necessary resource" for q. comp. benefit.

e.g. $\mathcal{D}$ = amplitude description $P(\mathcal{D})$ = entanglement

but this $\mathcal{D}$ has no special significance!

i.e. entanglement $\Rightarrow$ computation relation depends not on physics alone but also on choice of math. formalism for physical theory.

Example: (Knill-Gottesman theorem)

State description given by **stabiliser formalism**:

Special states $|\psi\rangle$ of n-qubits stabilised by subgroup H_ψ of Pauli group on n qubits

(generated by I, X, Y, Z on each qubit.)

H_ψ generated by n elements $g_1, \ldots, g_n \in$ Pauli group.

* Description of $|\psi\rangle$ is $\{g_1, \ldots, g_n\}$ ← (poly-sized)

e.g. $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \rightsquigarrow \{X \otimes X, Z \otimes Z\}$

Facts:

① all computational basis states have poly-size description

② The gates: $\pi/2$ phase $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, H, X, Y, Z, CNOT
all preserve the simple $\{g_1, \ldots g_n\}$ description and have simple update rules.

③ Measurement probabilities in computational basis are easily determined from $\{g_1, \ldots g_n\}$ description.

④ Application of other gates (like Toffoli etc) can cause the stabiliser description to grow exp.

Hence

Knill Gottesman theorem:

Any quantum computation that starts with a computational basis state & uses only the gates in (2) above — can be efficiently simulated classically.

Note: can generate large entangled states using C-NOT, H etc.

Hence these computations can have exp. growing descriptions in the amplitude description.

" non-polynomial stabiliser description
→ 'generalised entanglement' "

Other examples?

Valiant; Terhal, DiVincenzo quant-ph/0108010
~ fermionic operator formalism.... ?

Computational power of pure states:

entanglement ≡ exp growth of state description

so no entg ⇒ poly. sized description ⇒ classical simulation by direct calculation is efficient.

But now: mixed states?

p-blocked : product of mixtures $\rho = \rho_1 \otimes \rho_2 \otimes .. \otimes \rho_n$

(of p qubits each)

Previous theorem still holds (ρ has poly-sized description for fixed p)

But:

Definition : ρ is unentangled (separable) if ρ can be expressed as a mixture of product states

$$\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$$

(many possible decompositions)

"there exists a representation that involves no entanglement".

---

p-blocked "product of mixtures" $\Longrightarrow$ separable "mixture of products"

↑ extra classical correlations between the p-block states

Theorem: the n-qubit state

$$\rho = (1-\epsilon)\, I/2^n + \epsilon\, \xi$$

is separable for all mixed states ξ if $\epsilon < \frac{1}{4^n - 1}$.

~1998
- Zyczkowski, P. Horodecki, Lewenstein, Sanpera
- Vidal, Tarrach
- Braunstein, Caves, J, Linden, Popescu, Schack.

Hence: separable states have non zero volume in space of all states

i.e. require same number of parameters as general (entangled) mixed states!
So potentially same info. content.

ie. absence of entg $\not\Rightarrow$ exponential reduction of complexity of state description.

Problem:
If a quantum computation has a separable state at each stage, can it be classically simulated efficiently?
(Unsolved)

Power of computing with mixed states ??

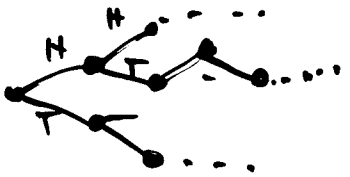
(a) separable state = classical prob. mixture of product states ✓

(b) can simulate processing of pure product states ✓

(c) can make classical prob. choices in our simulations ✓

So why not just combine (b) & (c) to simulate separable processes?

Compare: classical process of tossing a coin n times



exponentially big branching tree
Final distribution expon. big
(2^n possibilities!)

But: can just make prob. choices along the way
→ "local passage through the tree.

Doesn't work quantumly!

- separable mixture <u>changes</u> at each step &
  new separable mixture is a 'global' property
  of whole mixed state (i.e. need to know
  <u>all</u> paths of the tree).

Example 2 qubits

50/50 mixture of $\boxed{(|0\rangle+|1\rangle)|1\rangle \;,\; (|0\rangle-|1\rangle)|1\rangle}$ separable

$\Downarrow$ CNOT operation

50/50 mixture $\boxed{|0\rangle|1\rangle + |1\rangle|0\rangle \;,\; |0\rangle|1\rangle - |1\rangle|0\rangle}$

↑ entangled components but still separable:

equivalent to 50/50 mixture of

$\boxed{|0\rangle|1\rangle \;,\; |1\rangle|0\rangle}$

New product states ↗ depend on all component states in mixture, not just some one, chosen probabilistically!

Exploring computational benefits of very noisy states?

e.g. Knill-Laflamme "power of 1 clean qubit"

— more? . .

So

neither coherence nor entanglement seem (??) to be necessary for quantum computational power!

(But: special kinds of noise?

can this occur naturally in physical systems?)

Entanglement & Precision of parameters in quantum gates

(quantum computation vs classical analog computation)

Recall: quantum computational process ≡ application of N 2-qubit gates

$U_1, U_2, \ldots U_N$ to $|0\rangle|0\rangle \ldots |0\rangle$

Final state $= |\psi_N\rangle$

Bernstein-Vazirani thm: Consider the corresponding process with $U_1', U_2', \ldots U_N'$ "nearby" approximate gates satisfying

$$\| U_i - U_i' \| \leq \epsilon/N$$

Then $\| |\psi_N\rangle - |\psi_N'\rangle \| \leq \epsilon$.

operator norm

$$\|A\| = \max_{\|v\|=1} \|Av\|$$

Proof idea: each successive U_i' is unitary, so preserves any existing error, but also introduces a new error of $\leq \epsilon/N$. Hence error accumulates linearly to $(\frac{\epsilon}{N})N = \epsilon$. //

Relate $\|U - U'\|$ to precision:

Lemma: Operator $A = [a_{ij}]$ in d dimensions

Suppose $|a_{ij}| \leq \eta$ all i,j.

Then $\|A\| \leq d\eta$.

Furthermore the bound on $\|A\|$ is tight (can be realised for suitable A's.)

Hence argue (!?..) —

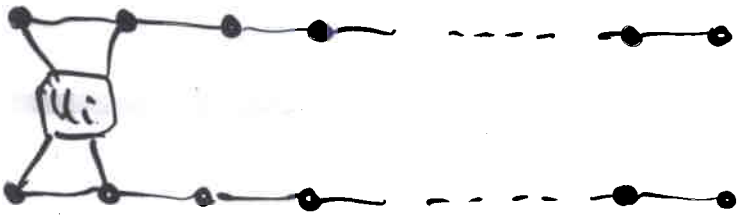
Suppose entries of 2 qubit gates U_i have been specified only to tolerance $\eta = \epsilon/dN = \epsilon/4N$ i.e. $O(\log N)$ bits of precision, resulting in approximate gates U_i':

(so $\|U_i' - U_i\| \leq \frac{\epsilon}{N}$)

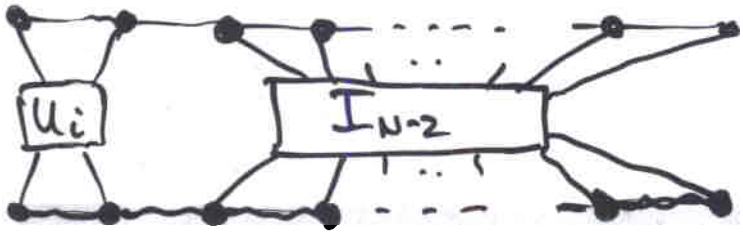
Then get final constant error ϵ (indep of N) in final state, and algorithm is still OK.

* Extra stability of q. computation parameters compared to classical analog computation " given by unitarity? ..... or? ...

However: typical computational step is NOT



BUT PHYSICALLY (i.e. "REALLY") IS



I_{N-2} is on same footing as other gates like U_i!

Computational step is $U_i \otimes I_{N-2}$
– exponentially many parameters in $d = 2^N$ dims!

So U_i' is in 2^N dims and $O(\log N)$ bits of precision, (i.e. accuracy ϵ/N):

$$\| U_i' - U_i \otimes I_{N-2} \| \leq \epsilon/N$$

Can have

$$\| |\psi_N'\rangle - |\psi_N\rangle \| \sim \left(\frac{\epsilon}{N}\right) N d = \epsilon 2^N$$

arbitrarily large!

STILL ALL UNITARY!

* Now need exponential precision of parameters ($O(N)$ bits) to guarantee $\| |\psi_N\rangle - |\psi_N'\rangle \| \leq \epsilon$

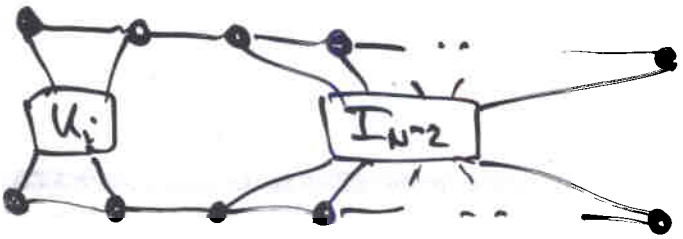
...looks bad! ... but...

ENTANGLEMENT: 2^N parameters vs $O(N)$ local parameters in N qubit state

$\Rightarrow$ many degrees of freedom are nonlocal

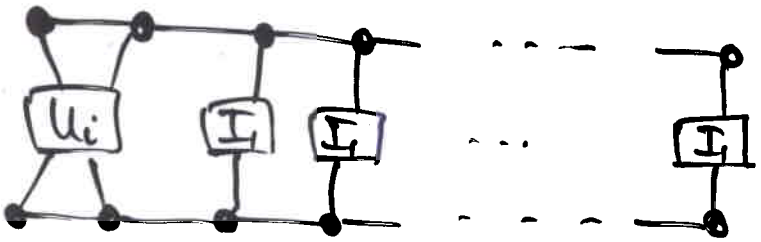
$\Rightarrow$ possibility of local access to global info content of state when component qubits are widely separated.

So can replace



exp(N) many parameters

BY (widely separate the qubits):



now only poly(N) parameters
~ local independent errors

and then BV stability applies.

Conclusion: BV stability result relies not only on unitarity but on properties of entanglement in an essential way.

~ spatial locality
c.f. communication benefits

Concluding Remarks

- Increasing multi-partite entanglement is necessary in pure state quantum algorithms if we are to have exponential speedup over classical computation.

- Relation of computational speedup $\Leftrightarrow$ entanglement depends on a further choice of mathematical formalism for representing quantum theory. Hence role of entanglement (necessary but not sufficient) is probably not fundamental from a conceptual point of view.

- Computational power of unentangled (separable) mixed states ? — unsolved !

- Further role of entanglement in stability of physically implementing quantum computation (cf also quantum error correcting codes)