

# Physical resources, entanglement, and the power of quantum computation

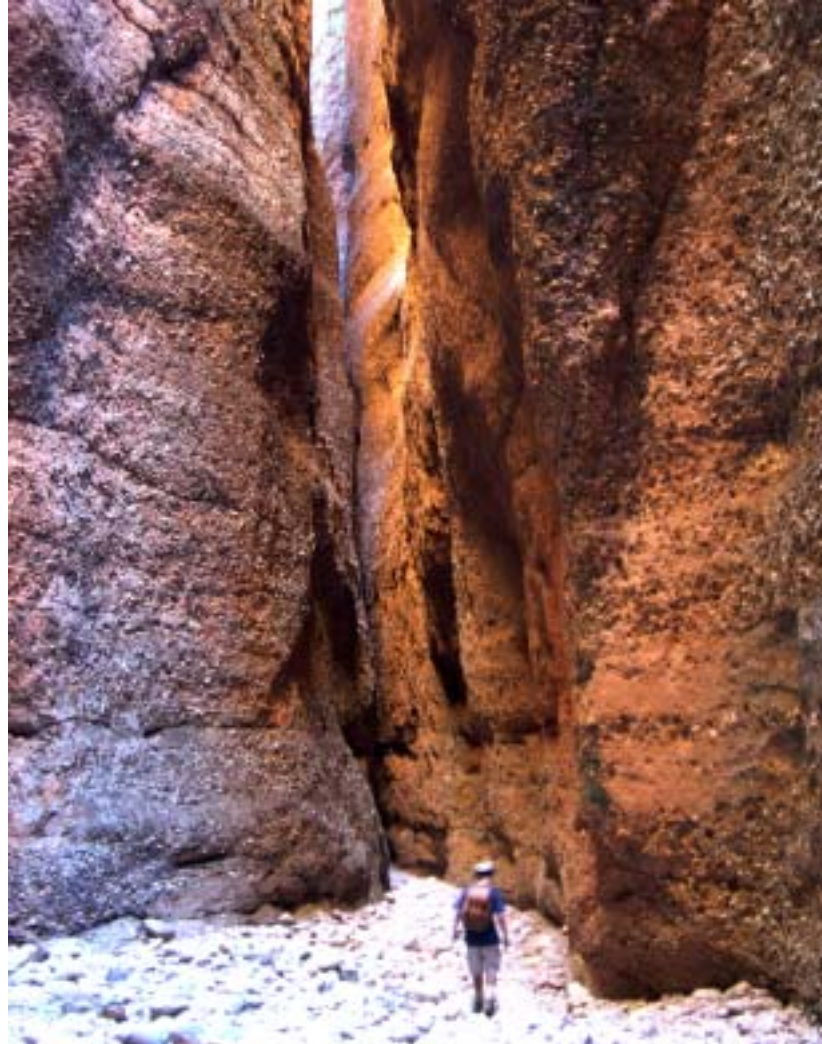
What powers quantum computation?

- I. Introduction
- II. Physical-resource requirements
- III. Role of entanglement
- IV. Why we don't know all the answers

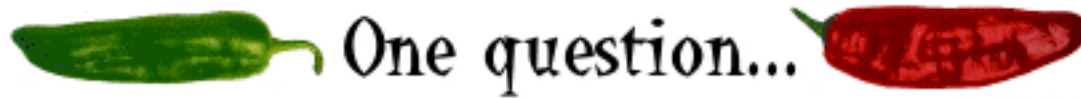
*Carlton M. Caves*  
*University of New Mexico*  
<http://info.phys.unm.edu/~caves>

**GDEST Workshop on Quantum Information and Coherence**  
**Max Planck Society, Munich**  
**2005 December 8**

# I. Introduction



**Bungle Bungle Range, Purnulu National Park, The Kimberley, Western Australia**



**What makes a quantum computer tick?**

**Superpositions/interference?**

**Information-gain/disturbance tradeoff?**

(wave-function collapse)

**Universal set of quantum gates?**

**Entanglement?**

**Entangling unitaries?**

# Quantum computing

**Classical Input**

$|\psi_{in}\rangle$

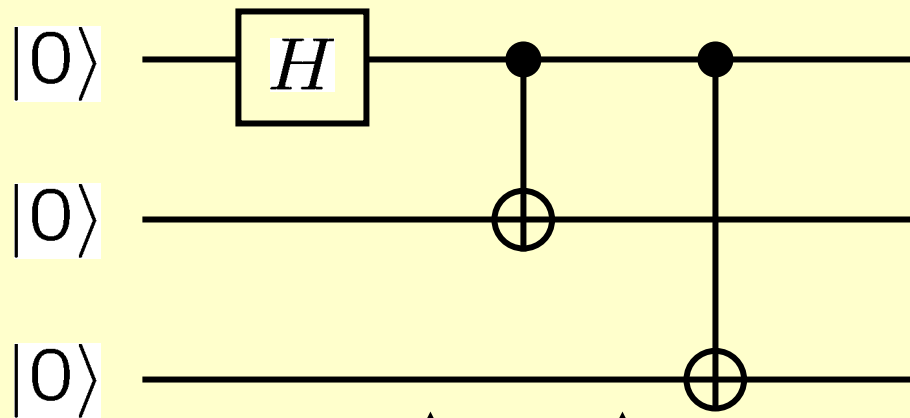
**QUANTUM WORLD**

$|\psi_{out}\rangle$

**Classical Output**



# QUANTUM WORLD



$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

**GHZ (or cat)  
entangled state**

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle$$

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|0\rangle$$

**Bell  
entangled  
state**

# Entanglement as a resource

Quantum key distribution

Teleportation

Quantum repeaters

Clock synchronization

Quantum communication complexity

Distributed computing

Separate parties perform operations locally and communicate classically. Classical resources are realistic and local. Shared entanglement is an additional resource not available classically.

For bigger tasks you don't entangle more systems; instead you use more copies of a basic entangled resource.

In a quantum computer the parts interact directly quantum mechanically. A classical simulation is realistic, but need not be local.

The number of systems entangled increases with problem size.

# QUANTUM WORLD

Efficient use of physical resources other than time

Efficient provision of required Hilbert-space dimension  
(efficient representation of quantum information)

Tensor-product structure of subsystems

+

+

No efficient realistic description of states and dynamics

Entanglement among all subsystems

Not *local*, rather *efficient dynamical*

Efficient use of time as a resource

**Classical Input**

$|\psi_{in}\rangle$

# QUANTUM WORLD

Efficient provision of required  
Hilbert-space dimension  
+  
No efficient realistic description  
of states and dynamics

$|\psi_{out}\rangle$

**Classical Output**



**Quantum  
information  
inside**

**(The primary resource for quantum computation is Hilbert space dimension. Efficient provision of the required dimension implies that the computer must be made of subsystems.)**

$$\equiv 2^n$$

**Hilbert space dimension measured in qubit units**

**Classical Input**

$|\psi_{in}\rangle$

**QUANTUM WORLD**

Efficient provision of required  
Hilbert-space dimension  
+  
No efficient realistic description  
of states and dynamics

$|\psi_{out}\rangle$

**Classical Output**



**Quantum  
information  
inside**

**No efficient realistic description of the states and dynamics implies that the subsystems must become globally entangled in the course of the computation.**

# II. Physical-resource requirements



**In the Sawtooth range, central New Mexico**

# Hilbert spaces are *fungible*

ADJECTIVE: 1. *Law*. Returnable or negotiable in kind or by substitution, as a quantity of grain for an equal amount of the same kind of grain. 2. Interchangeable.  
 ETYMOLOGY: Medieval Latin *fungibilis*, from Latin *fung* (*vice*), to perform (in place of).

## Hilbert-space dimension $D = 4$

### Subsystem division

#### 2 qubits

$$|0\rangle \otimes |0\rangle$$

$$|0\rangle \otimes |1\rangle$$

$$|1\rangle \otimes |0\rangle$$

$$|1\rangle \otimes |1\rangle$$

$$|x\rangle \otimes |y\rangle$$

### Unary system

$$|0\rangle$$

$$|1\rangle$$

$$|2\rangle$$

$$|3\rangle$$

$$|2x + y\rangle$$



$$|\psi\rangle = \sum_{x,y} c_{x,y} |x\rangle \otimes |y\rangle$$

$$|\psi\rangle = \sum_{x,y} c_{x,y} |2x + y\rangle$$

$$\hat{A} = \sum_{x,x',y,y'} A_{x,x';y,y'} |x\rangle \langle x'| \otimes |y\rangle \langle y'|$$

$$\hat{A} = \sum_{x,x',y,y'} A_{x,x';y,y'} |2x + y\rangle \langle 2x' + y'|$$

# We don't live in Hilbert space

A Hilbert space is endowed with structure by the *physical system* described by it, not vice versa.

The structure comes from observables associated with spacetime symmetries that anchor Hilbert space to the external world. These observables provide the “handles” that allow us to grab hold of a physical system and manipulate it.

Hilbert-space dimension is determined by physics. The dimension available for a quantum computation is a physical quantity that costs physical resources.

## Key Question

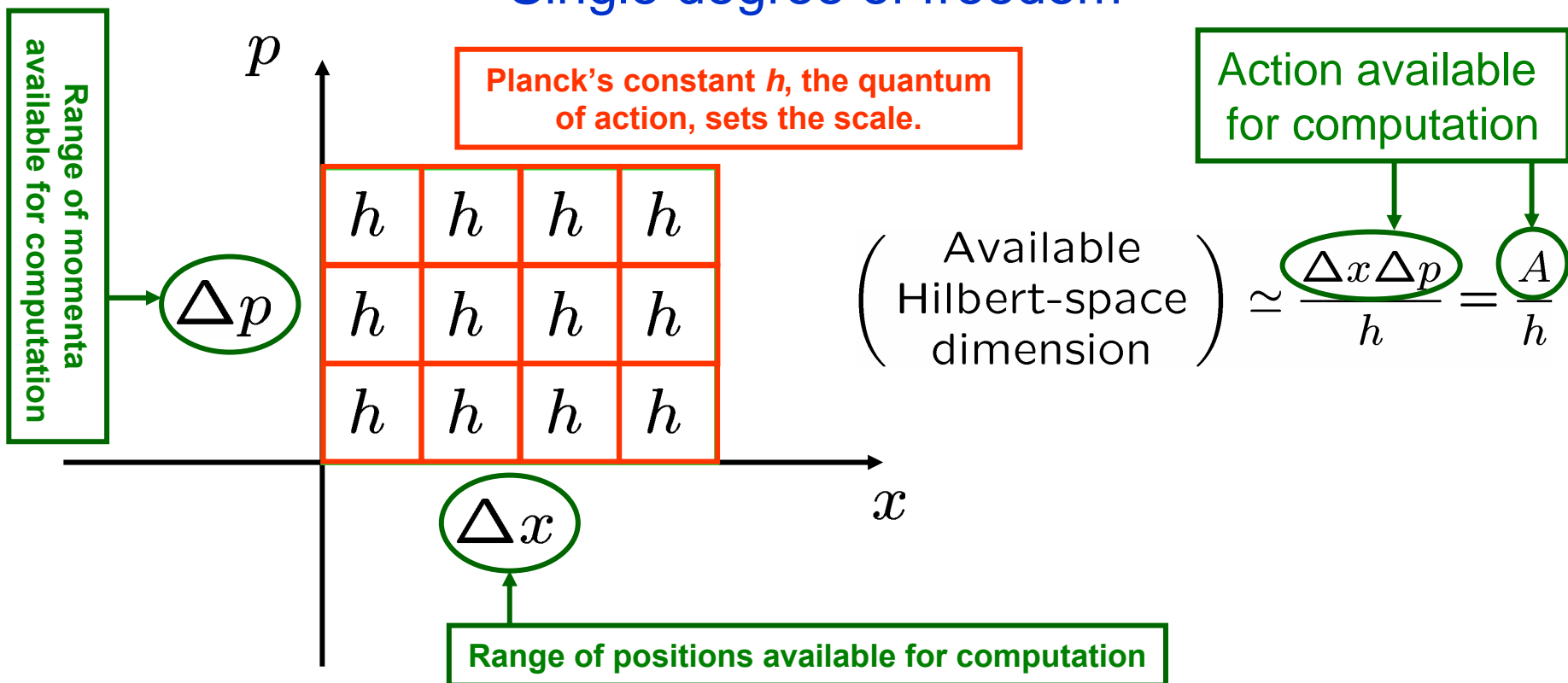
**What physical resources are required to achieve a Hilbert-space dimension sufficient to carry out a given computation?**

# Hilbert space and physical resources

The primary resource for quantum computation is Hilbert-space dimension.

Hilbert spaces of the same dimension are fungible, but the available Hilbert-space dimension is a physical quantity that costs physical resources.

## Single degree of freedom



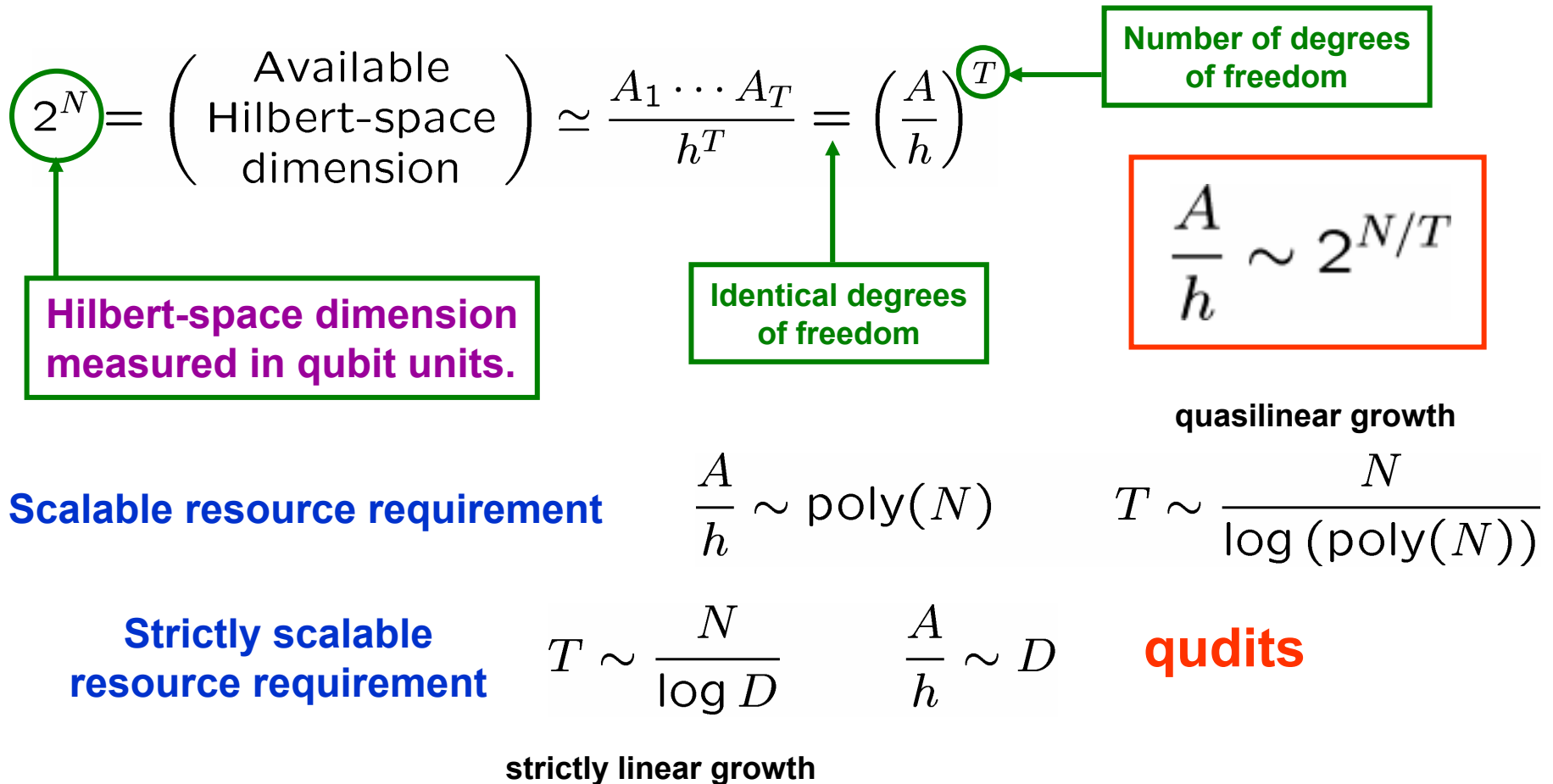


# Hilbert space and physical resources

Primary resource is Hilbert-space dimension.

Hilbert-space dimension costs physical resources.

Many degrees of freedom



**Classical Input**

$|\psi_{in}\rangle$

**QUANTUM WORLD**

Efficient provision of required  
Hilbert-space dimension  
+  
No efficient realistic description  
of states and dynamics

$|\psi_{out}\rangle$

**Classical Output**



**Quantum  
information  
inside**

The primary resource for quantum computation is Hilbert-space dimension. Efficient provision of the required dimension implies that the computer must be made of subsystems.



No efficient realistic description of the states and dynamics implies that the subsystems must become globally entangled in the course of the computation.

# Example: Classical linear wave computing

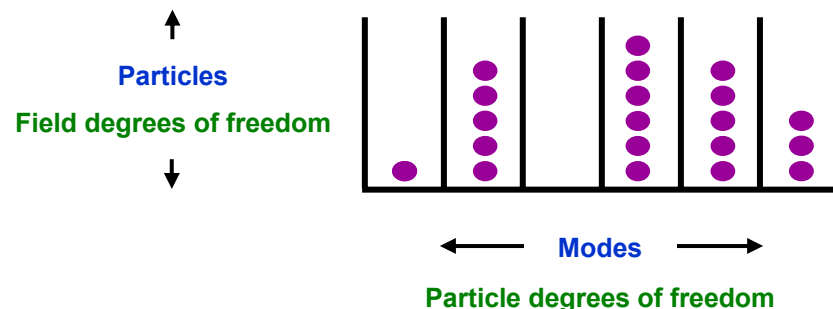
Grover's algorithm using classical waves: Bhattacharya, van den Heuvel, and Spreuw, PRL **88**, 137901 (2002).

A single quantum making transitions among field modes is a **physically unary** system that requires an exponential number of modes.

Classical (realistic) linear wave (coherent-state) *field amplitudes* undergo the same transformations as do the single-quantum *quantum amplitudes* in the unary single-quantum computer.

Classical linear waves inherit a demand for an exponential number of modes from the underlying unary structure.

Classical linear waves make an additional demand for exponential field strength if the waves are to be truly classical throughout the computation.



# III. Role of entanglement



**Albuquerque International Balloon Fiesta**

# Realistic description and entanglement

$$T = N / \log D \text{ qudits}$$

Computer's state:  $|\Psi\rangle = \sum_{j_1, \dots, j_T} c_{j_1 \dots j_T} |j_1\rangle \otimes \dots \otimes |j_T\rangle$

A realistic description could be a classical-computer simulation of the evolving quantum amplitudes.

$$(\# \text{ of amplitudes}) = D^T = 2^N$$

exponential in problem size

One-qudit operations:  $|\Psi'\rangle = U^{(j)}|\Psi\rangle$

$D^{T-1}$  applications of  $D \times D$  unitary matrix

exponential in problem size

Two-qudit operations:  $|\Psi'\rangle = U^{(j,k)}|\Psi\rangle$

$D^{T-2}$  applications of  $D^2 \times D^2$  unitary matrix

# Realistic description and entanglement

$$T = N / \log D \text{ qudits}$$

Suppose the computer's state is a product state throughout the computation.  
There are  $T$  local qudit processors with no entanglement between them.

$$|\Psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_T\rangle = \sum_{j_1, \dots, j_T} c_{j_1} \cdots c_{j_T} |j_1\rangle \otimes \cdots \otimes |j_T\rangle$$

$$(\# \text{ of amplitudes}) = DT = DN / \log D$$

One-qudit operations:

$$|\psi'_j\rangle = U^{(j)} |\psi_j\rangle$$

1 application of  $D \times D$  unitary matrix

polynomial in  
problem size

polynomial in  
problem size

Efficient realistic description

Readout: Determine  $DT = DN / \log D$  amplitudes.

# QUANTUM WORLD

Efficient provision of required  
Hilbert-space dimension  
(efficient representation of quantum information)

Scalable tensor-product  
structure of subsystems

Assume subsystems are qubits.

+

+

No efficient realistic description  
of states and dynamics

Entanglement not restricted  
to blocks of fixed size

Efficient realistic description  
of states and dynamics

Entanglement restricted to  
blocks of  $p$  qubits,  
independent of problem size.

Computer's state at all times is  $p$ -blocked.

$$|\Psi\rangle = \begin{array}{c} \boxed{|\Psi_1\rangle} \\ \uparrow \\ \boxed{\text{Block 1}} \\ \text{(} p \text{ qubits)} \end{array} \otimes \begin{array}{c} \boxed{|\Psi_2\rangle} \\ \uparrow \\ \boxed{\text{Block 2}} \\ \text{(} p \text{ qubits)} \end{array} \otimes \dots \otimes \begin{array}{c} \boxed{|\Psi_M\rangle} \\ \uparrow \\ \boxed{\text{Block } M} \\ \text{(} p \text{ qubits)} \end{array}$$

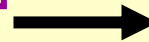
$N = pM$  qubits

# QUANTUM WORLD

Efficient provision of required  
Hilbert-space dimension  
(efficient representation of quantum information)

Tensor-product structure  
of subsystems

+



+

No efficient realistic description  
of states and dynamics

Entanglement among  
all subsystems

Global entanglement  
is the *resource* that allows  
a quantum computer to  
economize on resources.



# BUT

wait just one minute.

**Well, I'll take whatever's left.**

# Blue Latitudes: Boldly Going Where Captain Cook Has Gone Before by Tony Horwitz

On his first Pacific voyage, Captain Cook “loaded the *Endeavor* with experimental antiscorbutics such as malt wort (a drink), sauerkraut, and ‘portable soup,’ a decoction of ‘vegetables mixed with liver, kidney, heart, and other offal boiled to a pulp.’ Hardened into slabs, it was dissolved into oatmeal or ‘pease,’ a pudding of boiled peas.” (p. 34)

Cook might report to his superiors in London that “these experimental antiscorbutics are the essential resource that prevents scurvy,” but we know now that the soup was indeed awful, but only the sauerkraut was of any value in preventing scurvy.

When we report that “global entanglement is the essential resource for quantum computation,” are we making a logically similar statement?

# IV. Why we don't know all the answers

Gottesman-Knill theorem  
Mixed-state quantum computation



**Aspens in the Sangre de Cristo Range**

Global entanglement

No efficient classical description

Gottesman-Knill  
theorem

Mixed-state quantum  
computation?

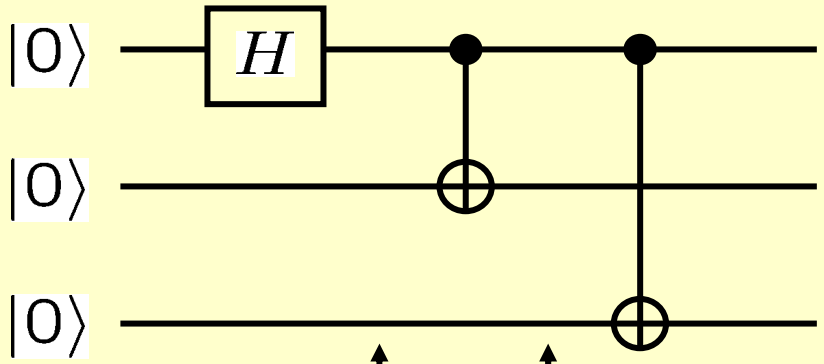
Mixed



Measure  $XYX$ ,  $YXY$ , and  $YYX$ : All yield result -1.  
*Local* realism implies  $XXX=-1$ .  
 Quantum mechanics says  $XXX=+1$ .

# QUANTUM WORLD

$ZII$   
 $IZI$   
 $IIZ$



$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

GHZ entangled state

$XXX, ZZI, ZIZ$

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle$$

$XII, IZI, IIZ$

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|0\rangle$$

$XXI, ZZI, IIZ$

$$S = \left\{ \begin{array}{l} III, ZZI, ZIZ, IZZ, \\ XXX, -XYY, -YXY, -YYX \end{array} \right\}$$

**Efficient (nonlocal) realistic description of states, dynamics, and measurements in terms of the stabilizer generators.**

# Gottesman-Knill theorem

- $N$  qubits in an initial product state in  $Z$  basis
- Allowed gates: Pauli operators  $X$ ,  $Y$ , and  $Z$ , plus Hadamard  $H$ , phase gate  $S$ , and C-NOT
- Allowed measurements: Products of Pauli operators

## Global entanglement

but

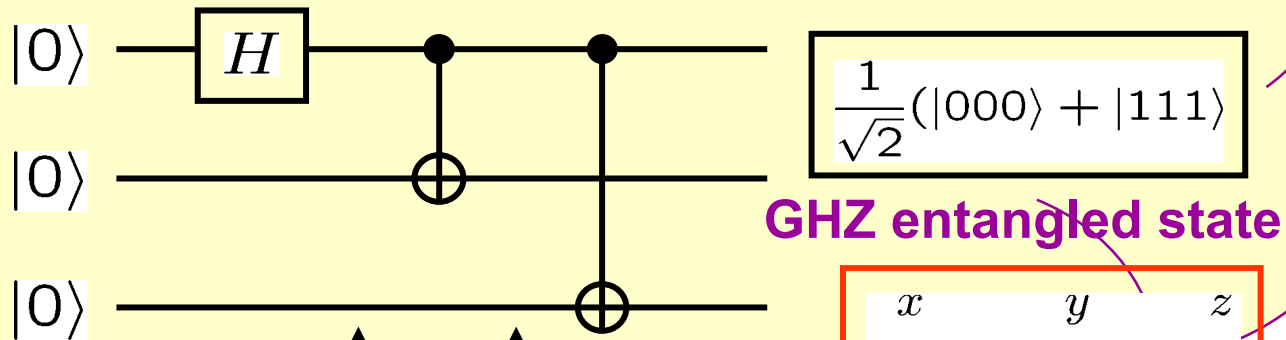
Efficient (nonlocal) realistic description of states, dynamics, and measurements in terms of the stabilizer generators

This kind of global entanglement, when measurements are restricted to the Pauli group, is, like the relation of Captain Cook's portable soup to scurvy, not "the essential resource for quantum computation."

$ZZI = ZIZ = IZZ = XXX = +1$ ;  $XYY = YXY = YYX = -1$ .

To get correlations right requires 1 bit of classical communication: party 2 tells party 1 whether  $Y$  is measured on qubit 2; party 1 flips her result if  $Y$  is measured on either 1 or 2.

# QUANTUM WORLD



$x$	$y$	$z$
$r_1$	$-r_1$	1
$r_2$	$r_2$	1
$r_3$	$r_3$	1

$x$	$y$	$z$
$r_2 r_3$	$r_1 r_2 r_3$	$r_1$
$r_2$	$r_1 r_2$	$r_1$
$r_3$	$r_1 r_3$	$r_1$

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle$$

$x$	$y$	$z$
1	$r_1$	$r_1$
$r_2$	$r_2$	1
$r_3$	$r_3$	1

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|0\rangle$$

$x$	$y$	$z$
$r_2$	$r_1 r_2$	$r_1$
$r_2$	$r_1 r_2$	$r_1$
$r_3$	$r_3$	1

For  $N$ -qubit GHZ states, this same procedure gives a *local realistic* description, aided by  $N-2$  bits of *classical communication* (provably minimal), of *states, dynamics, and measurements*.

# Gottesman-Knill circuits

- $N$  qubits in an initial product state in  $Z$  basis
- Allowed gates: Pauli operators  $X$ ,  $Y$ , and  $Z$ , plus  $H$ ,  $S$ , and C-NOT
- Allowed measurements: Products of Pauli operators

Global entanglement

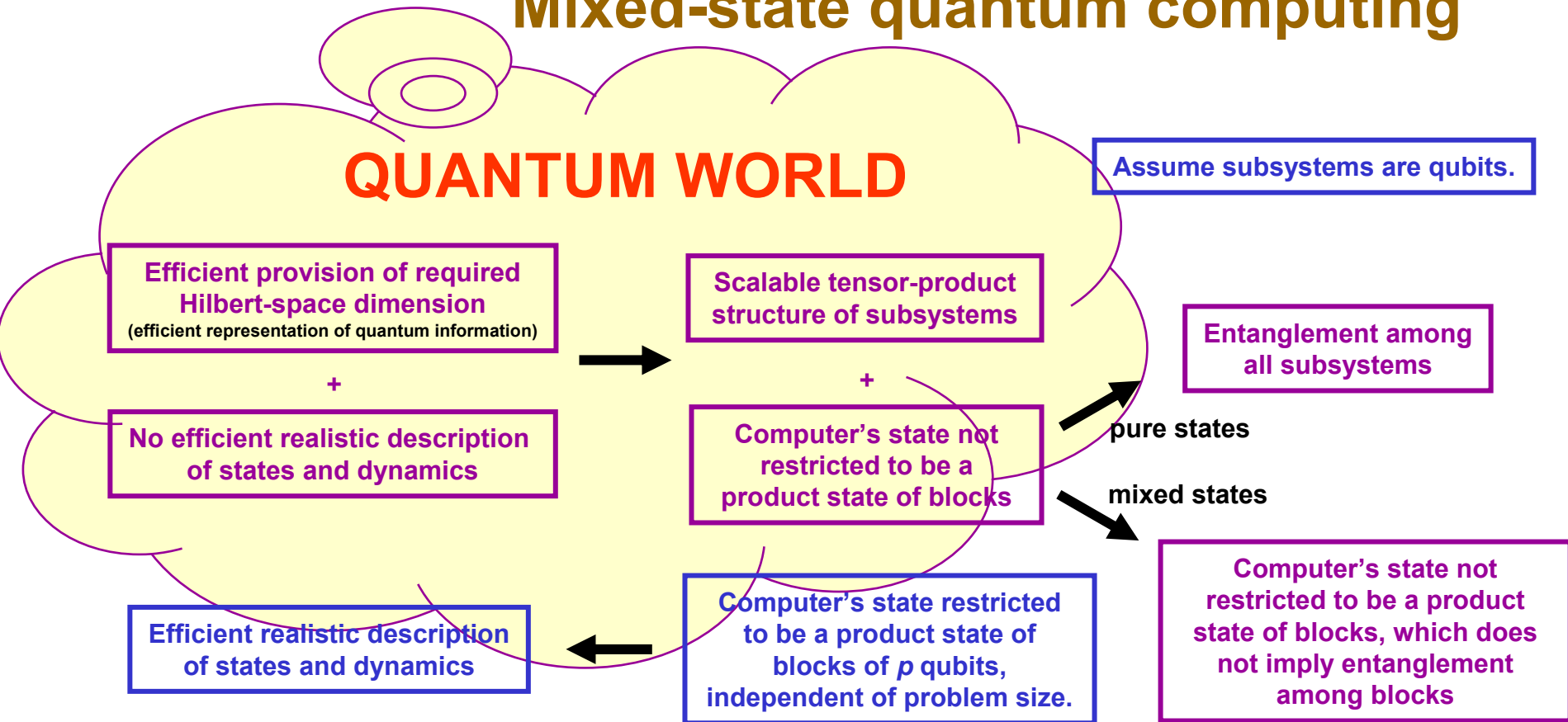
but

Efficient (nonlocal) realistic  
description of states, dynamics,  
and measurements

This kind of global entanglement,  
when measurements are  
restricted to the Pauli group, is  
not “the essential resource for  
quantum computation” because it  
can be simulated efficiently by  
local variables assisted by  
classical communication.



# Mixed-state quantum computing



$\rho$  not entangled (separable)

$$\rho = \left( \begin{array}{c} \text{mixture of} \\ \text{product states} \end{array} \right) = \sum_j p_j \rho_j^{(1)} \otimes \cdots \otimes \rho_j^{(M)}$$

# Power of one qubit

## Problem

Let  $U$  be a unitary operator on  $N$  qubits, which can be implemented efficiently in terms of a universal set of quantum gates. Find  $\text{tr}(U)/2^N$  to a fixed accuracy.

Power of one qubit

E. Knill and R. Laflamme, PRL **81**, 5672 (1998).

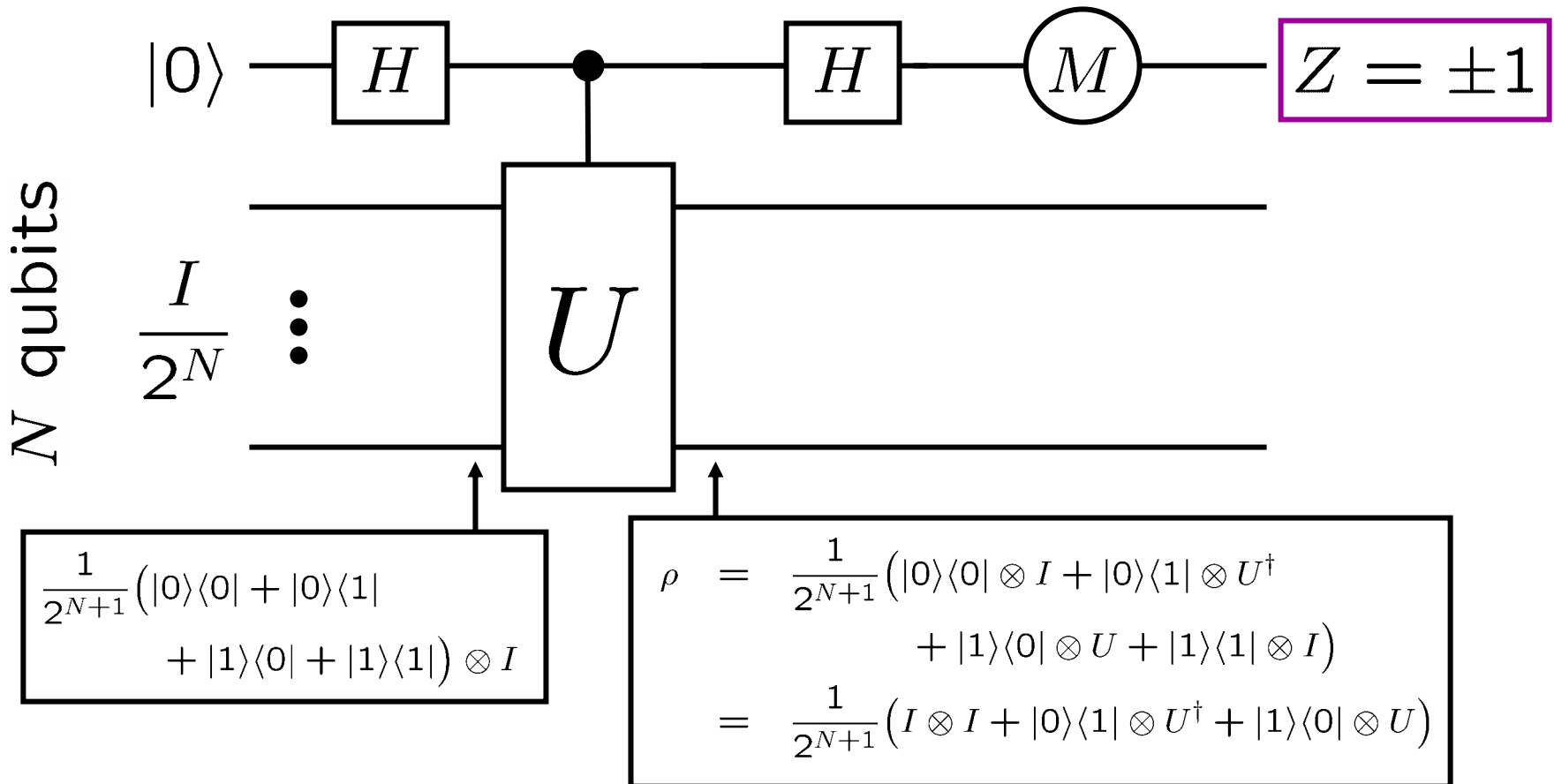
R. Laflamme, D. G. Cory, C. Negrevergne, and L. Viola, Quant. Inf. Comp. **2**, 166 (2002).

D. Poulin, R. Blume-Kohout, R. Laflamme, and H. Ollivier, quant-ph/0310038.

# Power of one qubit

$$\langle Z \rangle = \text{tr}(ZH\rho H) = \text{tr}(\underbrace{HZH}_= X \rho) = \frac{1}{2^{N+1}} \text{tr}(U^\dagger + U) = \frac{\text{Re}(\text{tr}(U))}{2^N}$$

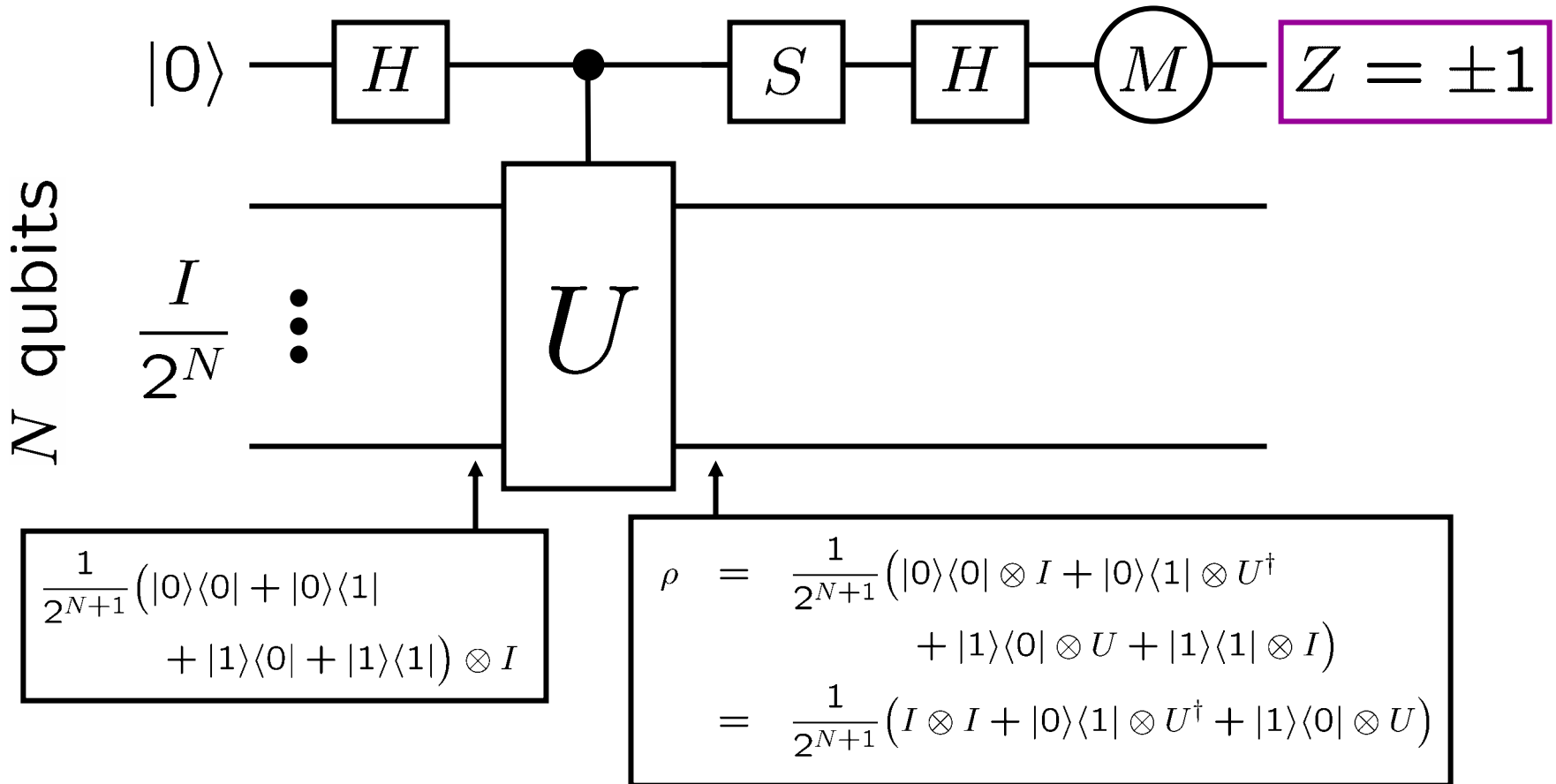
Many repetitions



# Power of one pure qubit

$$\langle Z \rangle = \text{tr}(ZHS\rho S^\dagger H) = \text{tr}(\underbrace{S^\dagger HZHS}_{=-Y}\rho) = \frac{i}{2^{N+1}} \text{tr}(-U^\dagger + U) = -\frac{\text{Im}(\text{tr}(U))}{2^N}$$

Many repetitions



# Power of one qubit

## Problem

Let  $U$  be a unitary operator on  $N$  qubits, which can be implemented efficiently in terms of a universal set of quantum gates. Find  $\text{tr}(U)/2^N$  to a fixed accuracy.

- $O(1/\epsilon^2)$  repetitions are needed to determine  $\langle Z \rangle$  and, hence,  $\text{tr}(U)/2^N$  with accuracy  $\epsilon$ .
- If the special qubit has an initial polarization  $\delta$ , the output expectation value is reduced by a factor of  $\delta$ . The only effect is to increase the required number of repetitions to  $O(1/\delta^2\epsilon^2)$ .
- The special qubit is not entangled with the other  $N$  qubits at any point during the computation, nor are the other  $N$  qubits entangled among themselves.

# Mixed-state quantum computing

## Power of one qubit

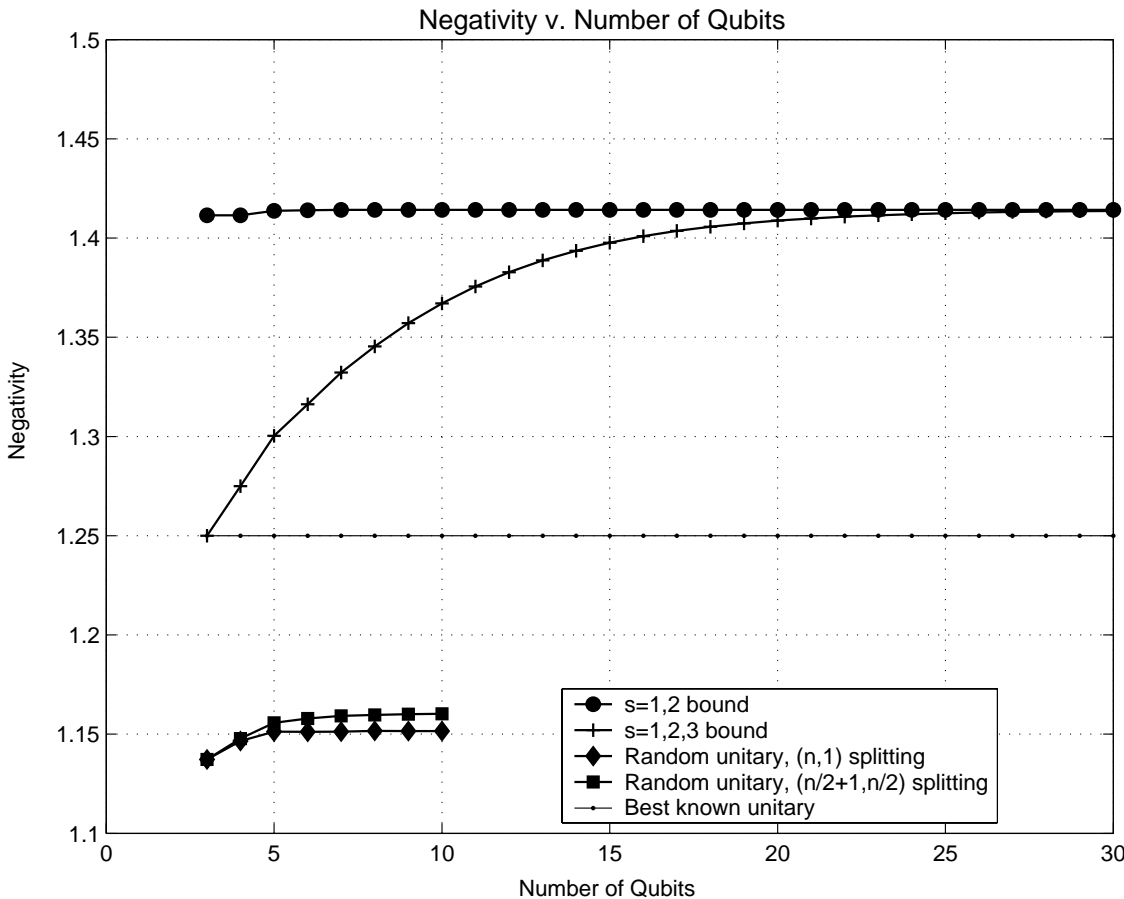
What should we make of this?

- Given a unitary operator  $U$  on  $N$  qubits, which can be implemented efficiently in terms of a universal set of quantum gates, is there a classical algorithm for finding  $\text{tr}(U)/2^N$  to a fixed accuracy?
- Is the overall state entangled during the course of the computation, and if so, how much?

# Mixed-state quantum computing

## Power of one qubit

- Is the overall state entangled during the course of the computation, and if so, how much?



$$U_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$
 The achievable negativity is a vanishingly small fraction of the maximum negativity,  $\sim 2^{-N/2}$ , for roughly equal bipartite divisions.



**Planck's constant did appear.**



Alice

**Alice and Bob did not.**



Bob