Quantum information

Physical implementations

Quantum error correction

Quantum circuits

Quantum measurements

Quantum computation

Decoherence

Entanglement

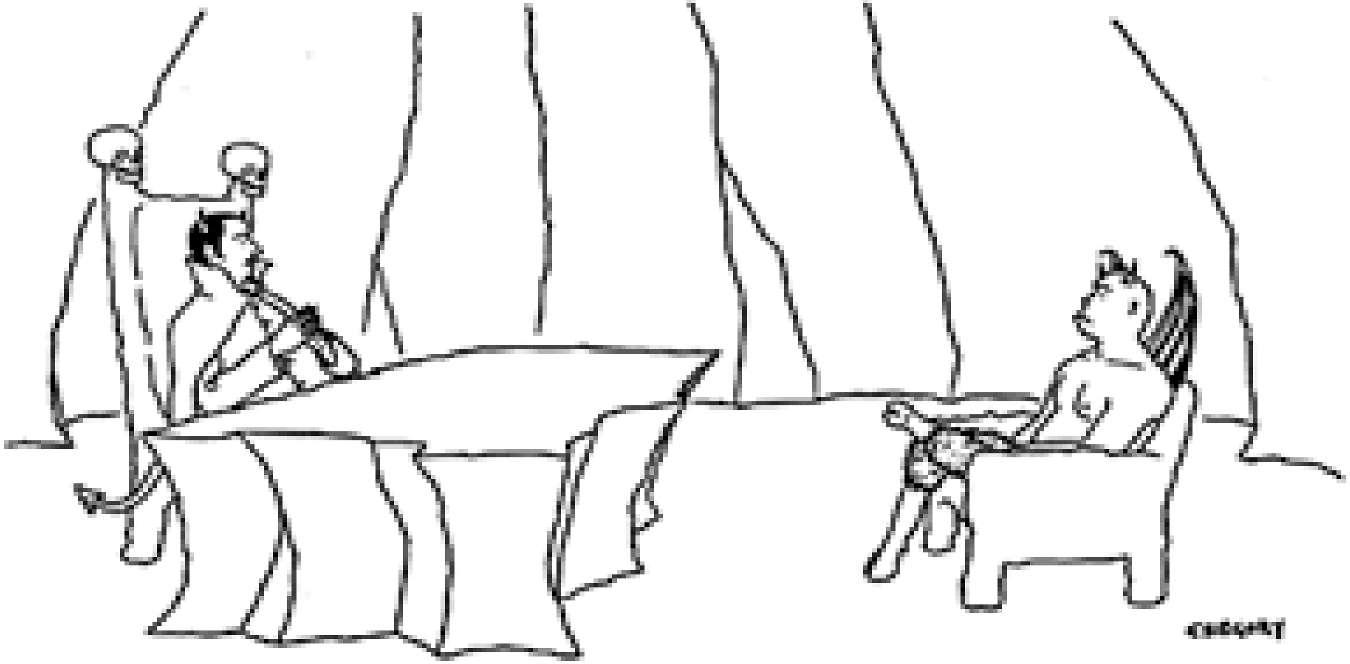
Quantum control

Quantum games

Quantum simulation

Quantum communication

Quantum algorithms



"I need someone well versed in the art of torture—do you know PowerPoint?"

Quantum information

Physical implementations

Quantum error correction

Quantum circuits

Quantum measurements

Quantum computation

Decoherence

Entanglement

Quantum control

Quantum games

Quantum simulation

Quantum communication

Quantum algorithms

Bird's-eye view of *one* aspect of quantum information

Entanglement

Quantum computation

Quantum information inside

Physical resources, entanglement, and the power of quantum computation

Physical resources, entanglement, and the power of quantum computation

What powers quantum computation?

I. Introduction

II. Physical-resource requirements

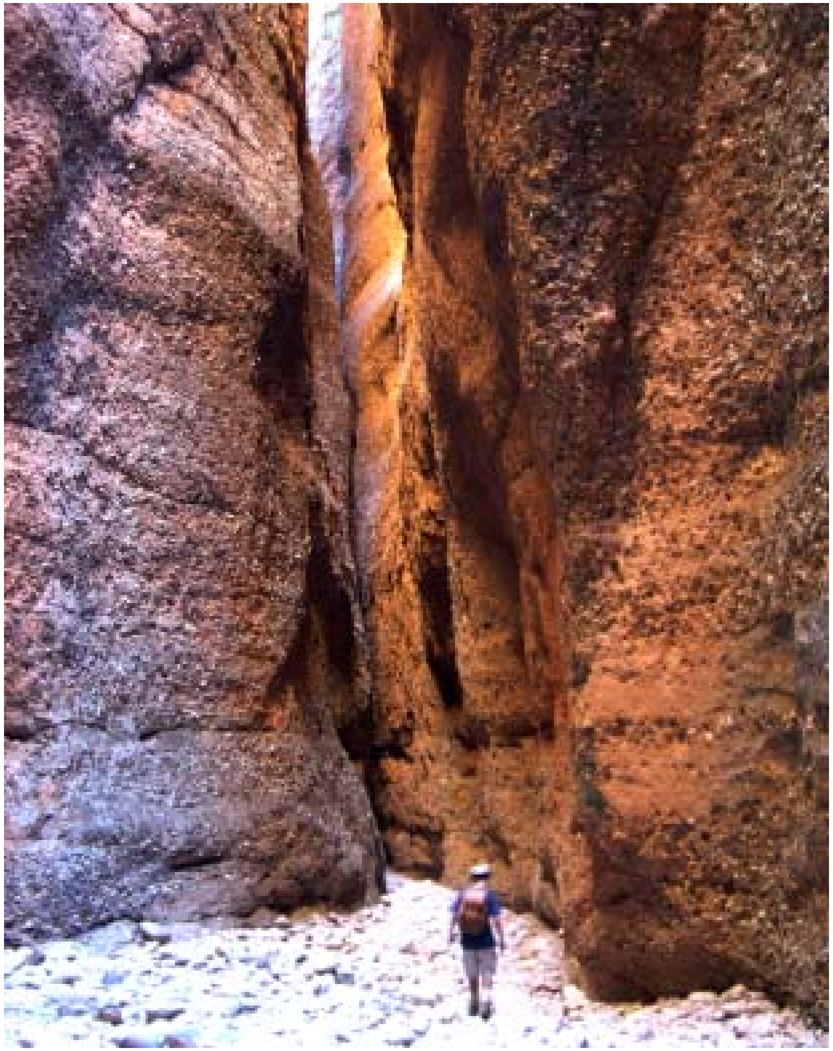
III. Role of entanglement

IV. Why we don't know all the answers

Carlton M. Caves
University of New Mexico
http://info.phys.unm.edu

SQuInT Summer Retreat
University of Southern California
2005 July 7

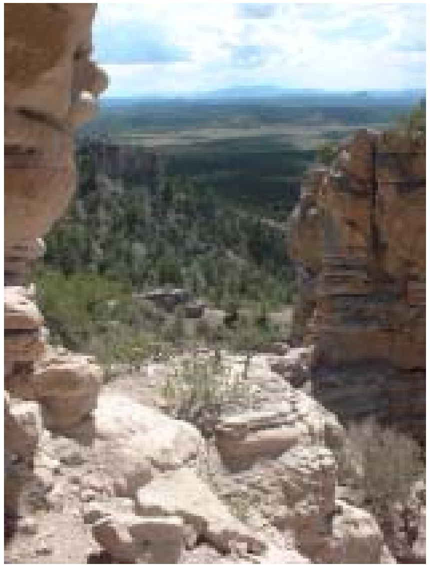
I. Introduction



Bungle Bungle Range, Purnululu National Park, The Kimberley, Western Australia

El Patio Cafe

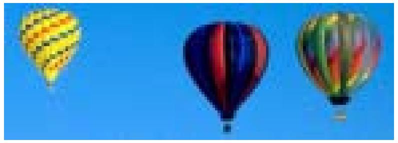
SERVER	TABLE	GUESTS	CHECK NUMBER
JC	D	3	31252



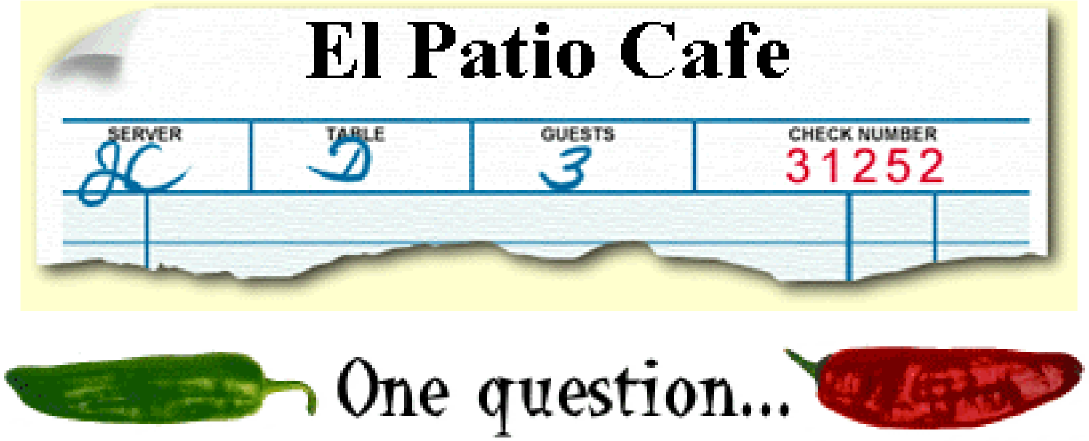
One question...

? **GREEN** or **RED**

Official state question of the state of New Mexico



Join us: *http://info.phys.unm.edu*



What makes a quantum computer tick?

Superpositions/interference?

Information-gain/disturbance tradeoff?
(wave-function collapse)

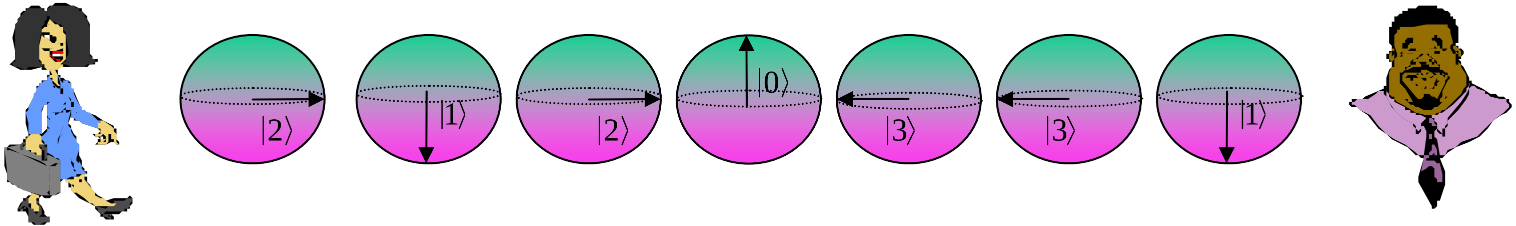
Universal set of quantum gates?

Entanglement?

Entangling unitaries?

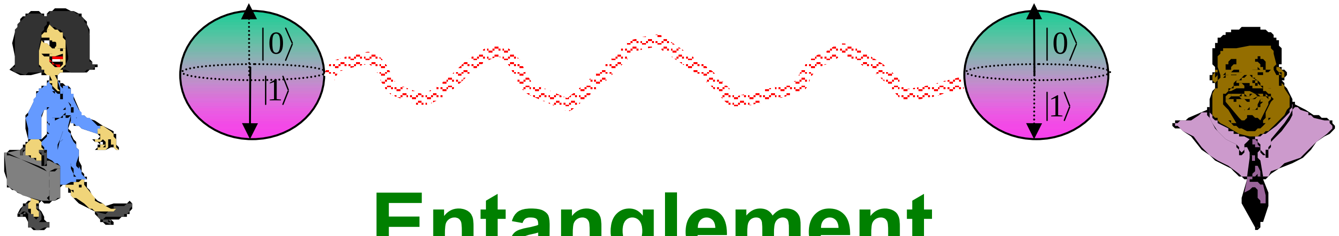
Other quantum information processing tasks

Quantum Key Distribution



Information/disturbance

Communication Complexity

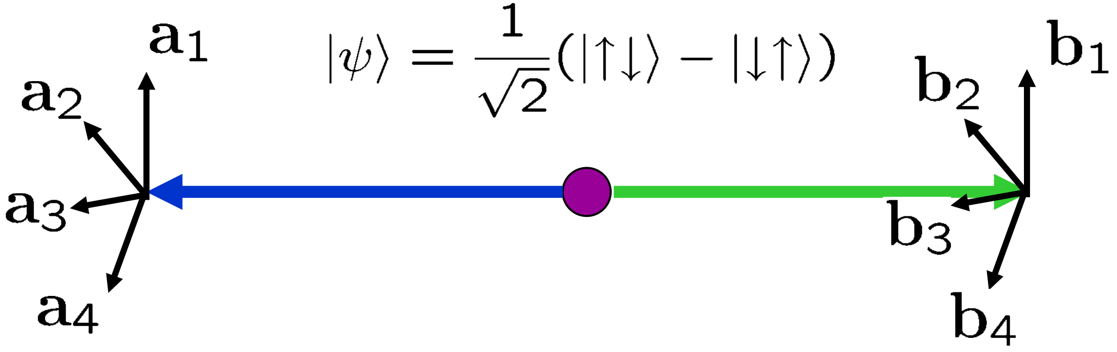


Entanglement

Quantum key distribution using entanglement

Theory: Ekert, PRL **67**, 661 (1991)
Experiment: Naik *et al.*, PRL **84**, 4733 (2000)
Tittel *et al.*, PRL **84**, 4737 (2000)
Jennewein *et al.*, PRL **84**, 4729
(2000)

Bell entangled state



$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$$

	b_1	b_2	b_3	b_4
a_1	**Qkey**	S	-	S
a_2	S'	**Qkey**	S'	-
a_3	-	S	**Qkey**	S
a_4	S'	-	S'	**Qkey**

LHV: $|S|, |S'| \leq 2$

QM: $S = S' = 2\sqrt{2}$

$$\begin{aligned} S &= C(\mathrm{a}_1,\mathrm{b}_2) + C(\mathrm{a}_3,\mathrm{b}_2) + C(\mathrm{a}_3,\mathrm{b}_4) - C(\mathrm{a}_1,\mathrm{b}_4) \\ S' &= C(\mathrm{a}_2,\mathrm{b}_1) + C(\mathrm{a}_2,\mathrm{b}_3) + C(\mathrm{a}_4,\mathrm{b}_3) - C(\mathrm{a}_4,\mathrm{b}_1) \end{aligned}$$

$$C(\mathbf{a},\mathbf{b}) = \langle \sigma_{\mathrm{a}} \sigma_{\mathrm{b}} \rangle$$

Detail

▶

Experiment

▶

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.

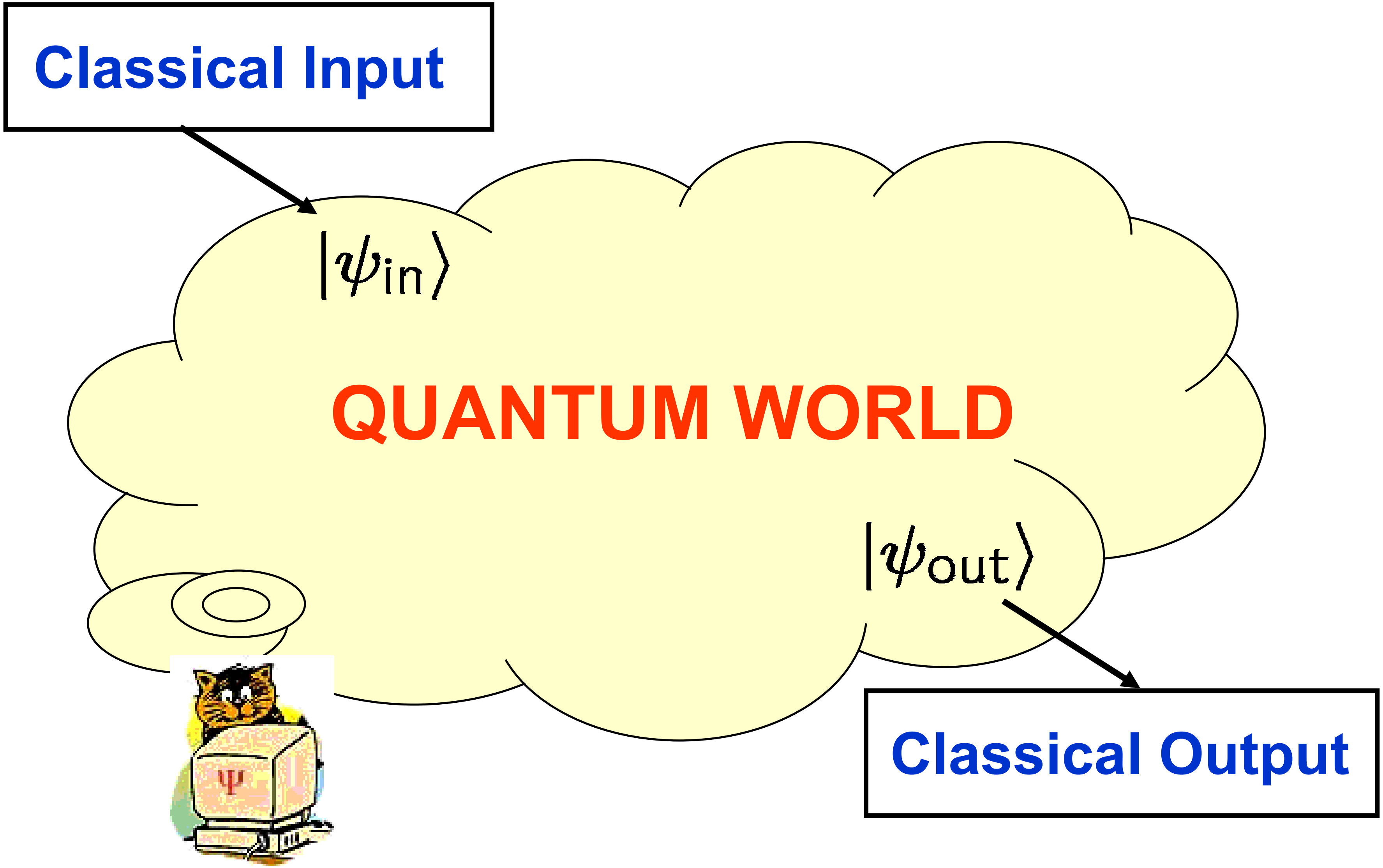
In a quantum computer the parts interact directly quantum mechanically. A classical simulation is realistic, but need not be local.

The number of systems entangled increases with problem size.

Quantum computing paradigms

Paradigm	Unitary Gates	Measurement (prior to readout)	Global Entanglement	Hilbert space
Standard Circuit Model	Yes	No	Yes	Yes
Nielsen 2003	No	Yes	Yes	Yes
Cluster-state computation	No	Yes	Yes/prior	Yes
KLM	Yes	Yes	Yes	Yes

Quantum computing



Classical Input

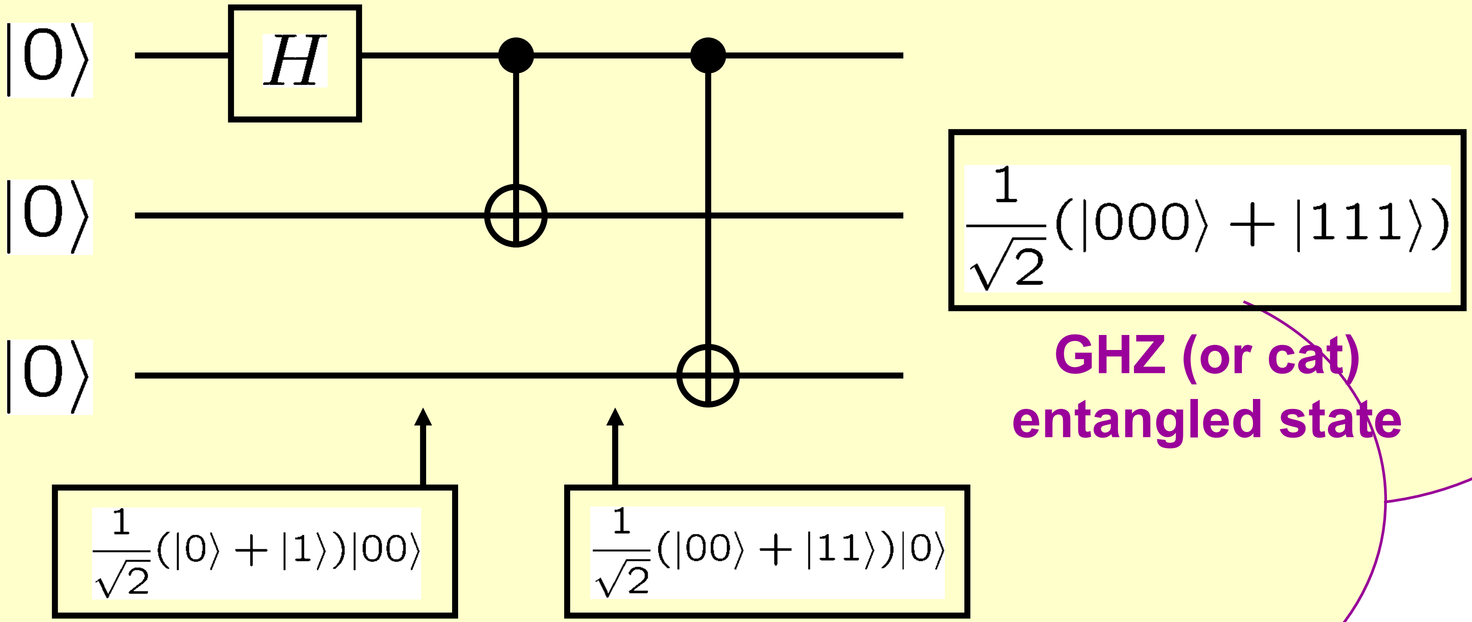
$|\psi_{\text{in}}\rangle$

QUANTUM WORLD

$|\psi_{\text{out}}\rangle$

Classical Output

QUANTUM WORLD



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

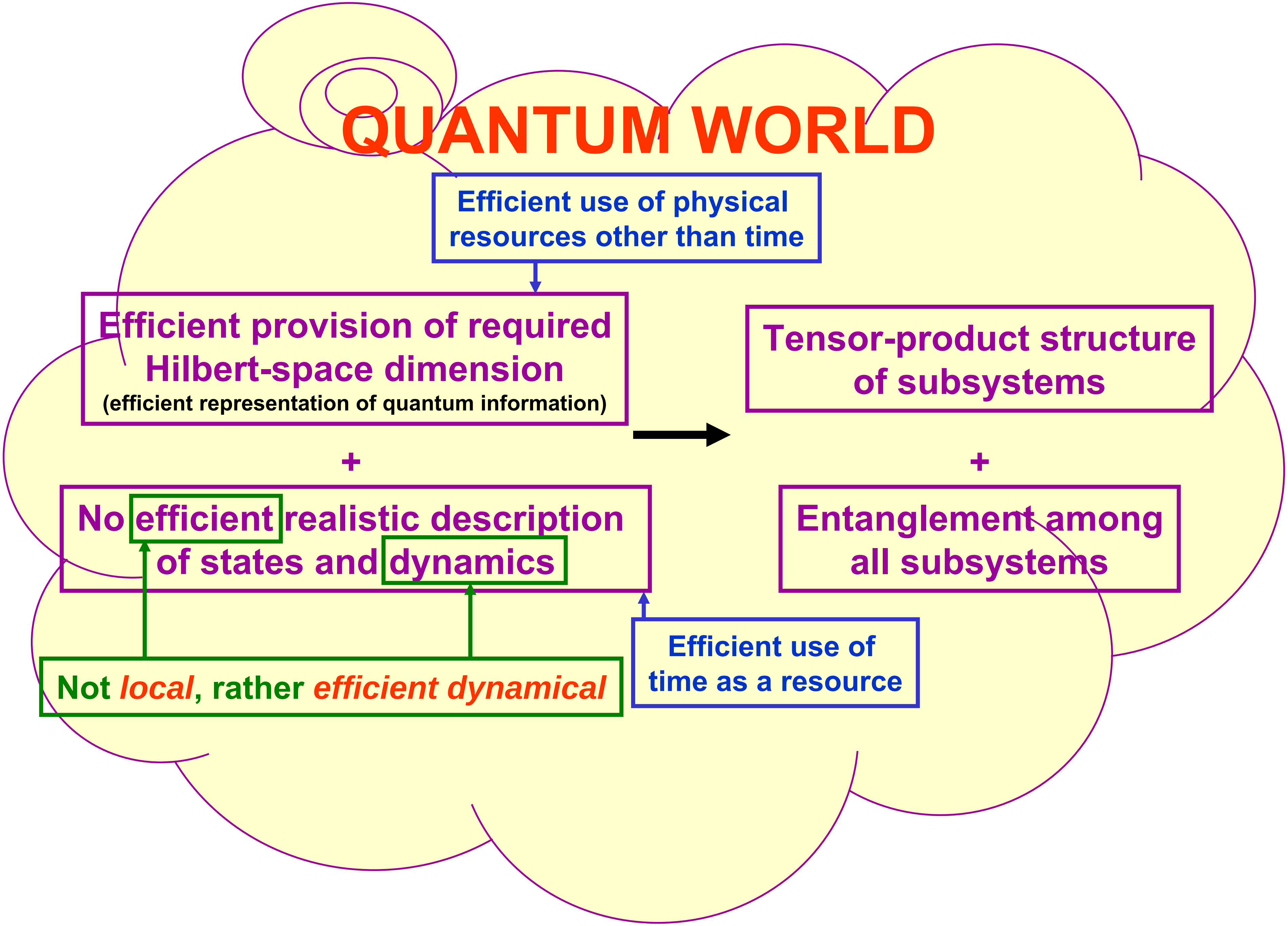
$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|0\rangle$$

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

GHZ (or cat) entangled state

Gates ▶

QUANTUM WORLD



Efficient use of physical resources other than time

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

+

No efficient realistic description of states and dynamics

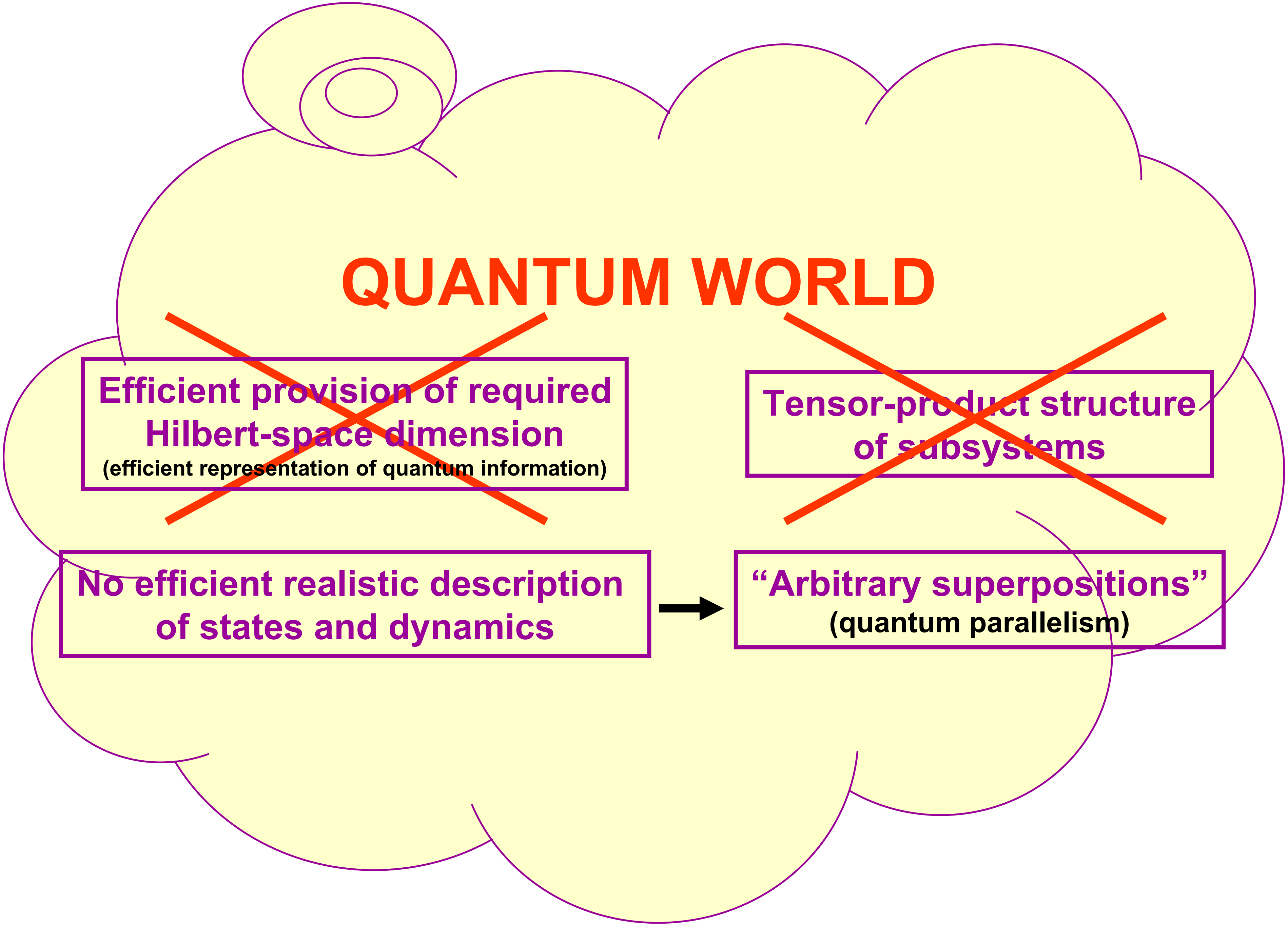
Not *local*, rather *efficient dynamical*

Efficient use of time as a resource

Tensor-product structure of subsystems

+

Entanglement among all subsystems

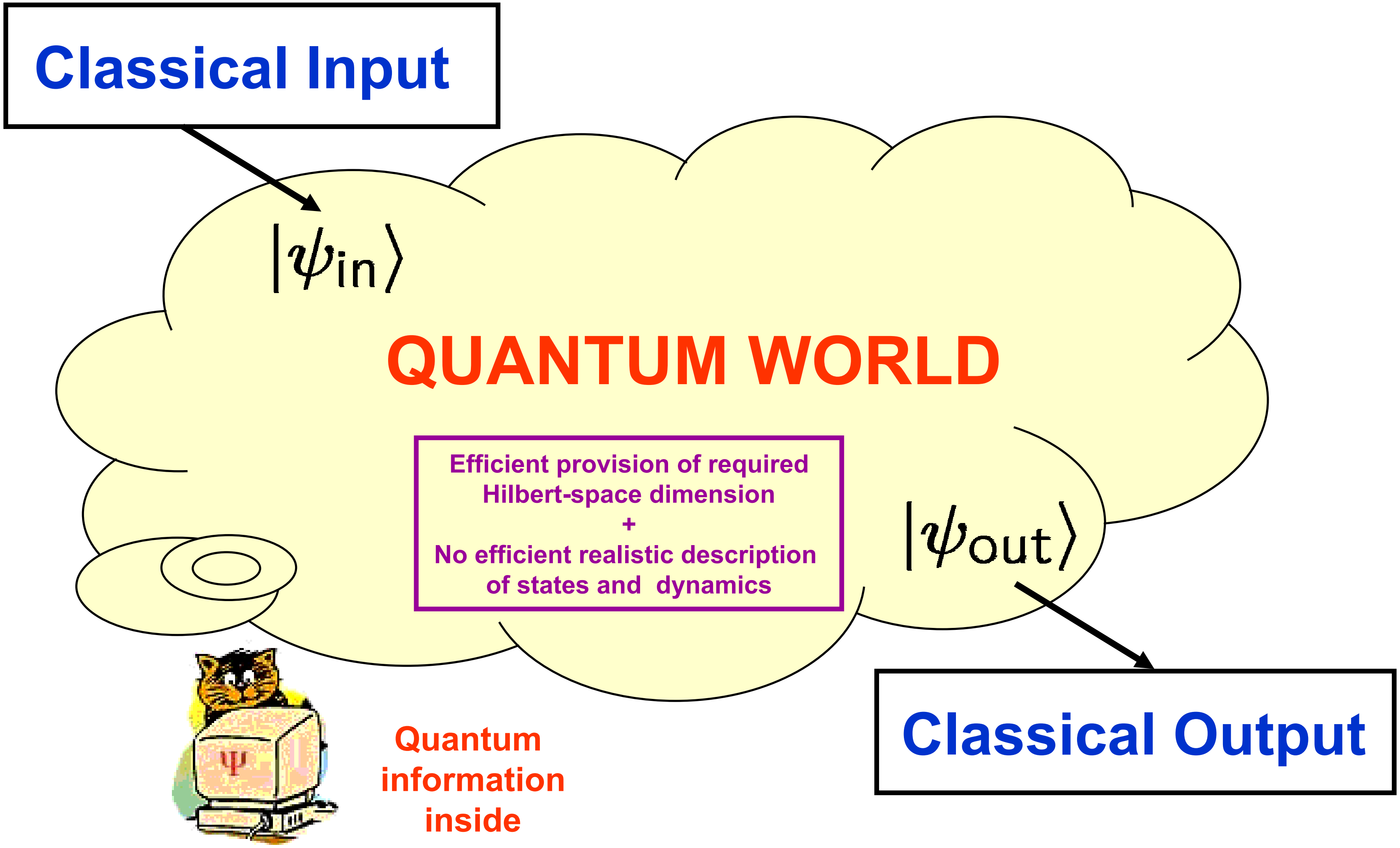


QUANTUM WORLD

~~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 → “Arbitrary superpositions”
(quantum parallelism)



Classical Input

$|\psi_{\text{in}}\rangle$

QUANTUM WORLD

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

$|\psi_{\text{out}}\rangle$

Classical Output

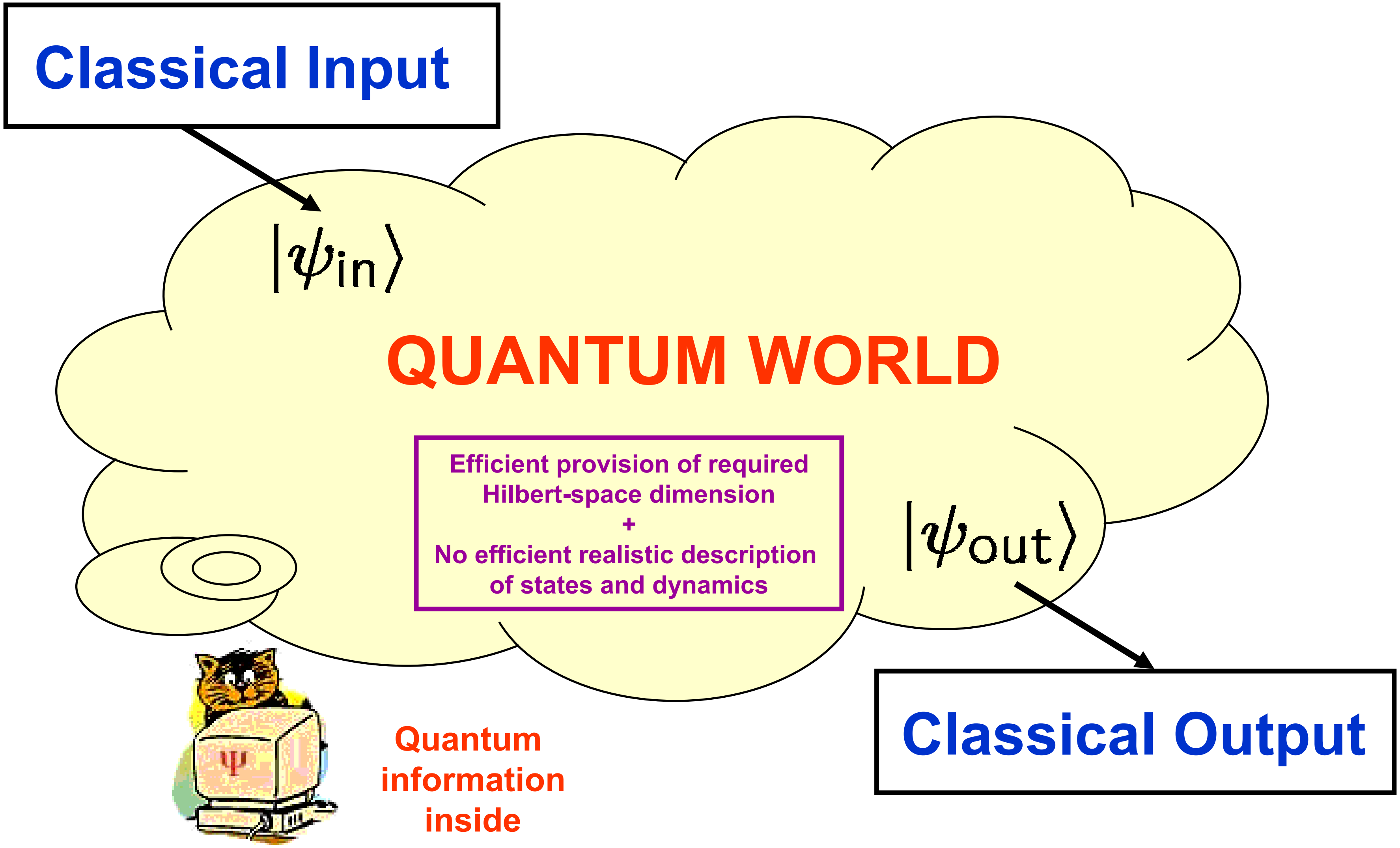
Quantum information inside

$$\left(\begin{array}{c}\text{Required Hilbert-space}\\ \text{dimension}\end{array}\right) = 2^N$$

Hilbert-space dimension measured in qubit units

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.

R. Blume-Kohout, I. H. Deutsch, and CMC, Found Phys **32**, 1641 (2002).



Classical Input

$|\psi_{\text{in}}\rangle$

QUANTUM WORLD

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

$|\psi_{\text{out}}\rangle$

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.

R. Jozsa and N. Linden, Proc. Roy. Soc. London A **459**, 2011 (2003).

II. Physical-resource requirements

In the Sawtooth range

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		Unary system
$\vert 0\rangle\otimes\vert 0\rangle$		$\vert 0\rangle$
$\vert 0\rangle\otimes\vert 1\rangle$		$\vert 1\rangle$
$\vert 1\rangle\otimes\vert 0\rangle$	↔	$\vert 2\rangle$
$\vert 1\rangle\otimes\vert 1\rangle$		$\vert 3\rangle$
$\vert x\rangle\otimes\vert y\rangle$		$\vert 2x+y\rangle$

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

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

We don’t live in Hilbert space

If this is news, see me after the talk.

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

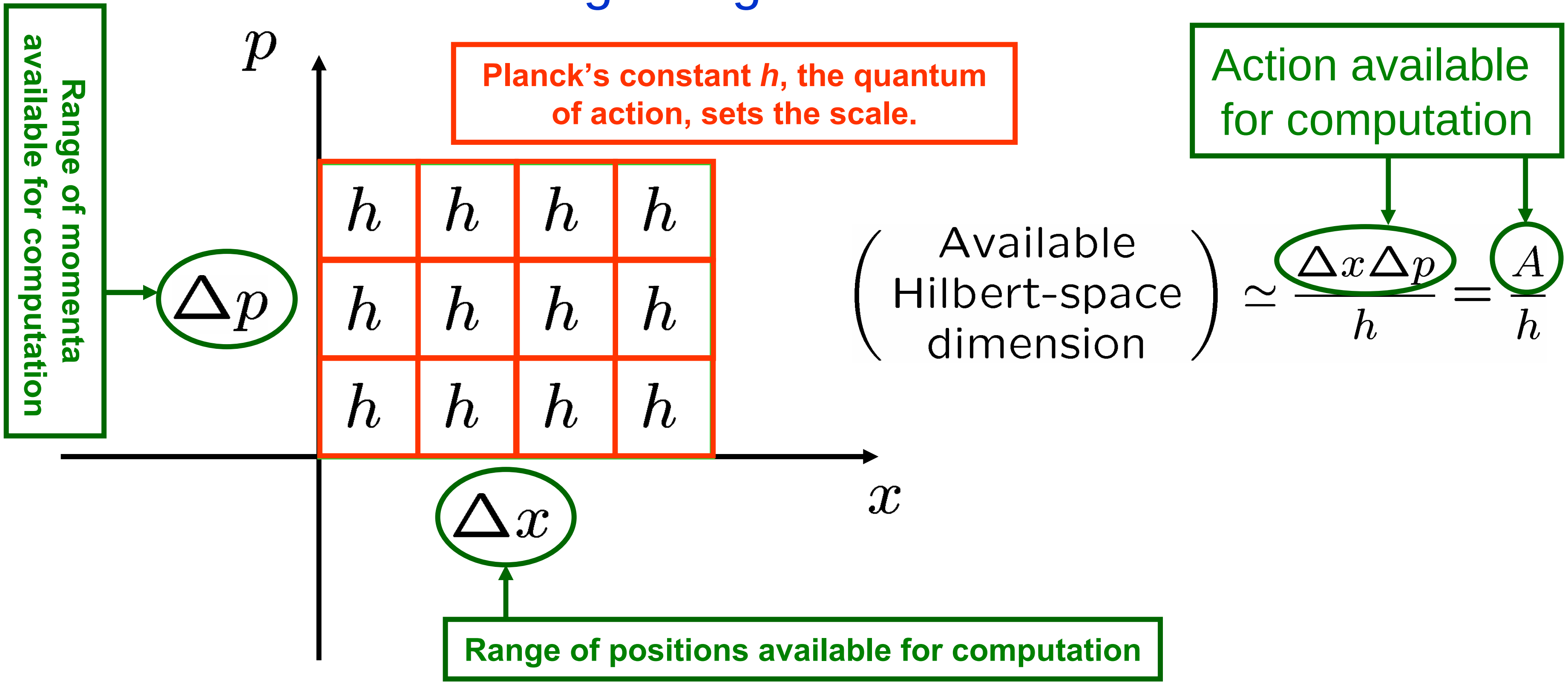
What physical resources are required to achieve a Hilbert-space dimension sufficient to carry out a given computation?

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



Range of momenta available for computation

Planck's constant *h*, the quantum of action, sets the scale.

Action available for computation

Range of positions available for computation

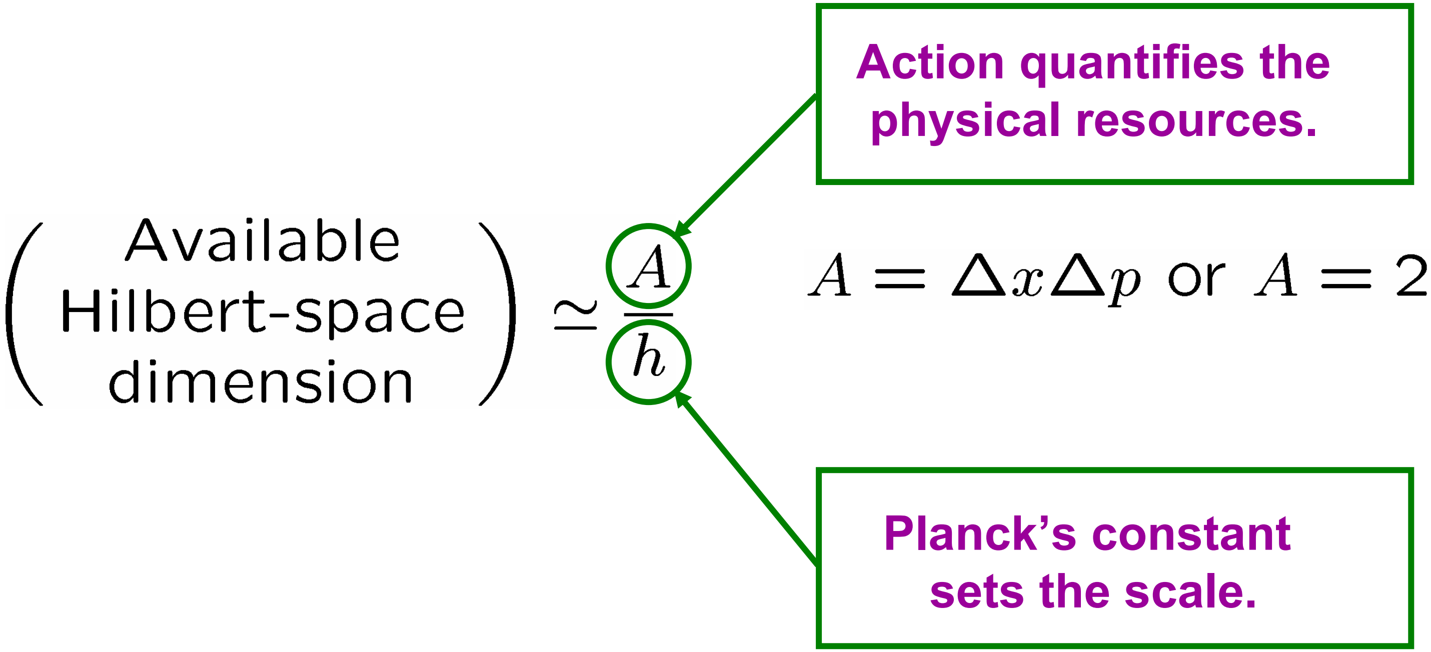
$$\left(\begin{array}{c}\text{Available}\\ \text{Hilbert-space}\\ \text{dimension}\end{array}\right) \simeq \frac{\Delta x\Delta p}{h} = \frac{A}{h}$$

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



$$\begin{pmatrix}\text{Available}\\ \text{Hilbert-space}\\ \text{dimension}\end{pmatrix} \simeq \frac{A}{h}$$

Action quantifies the physical resources.

$A = \Delta x \Delta p$ or $A = 2\pi \Delta J$

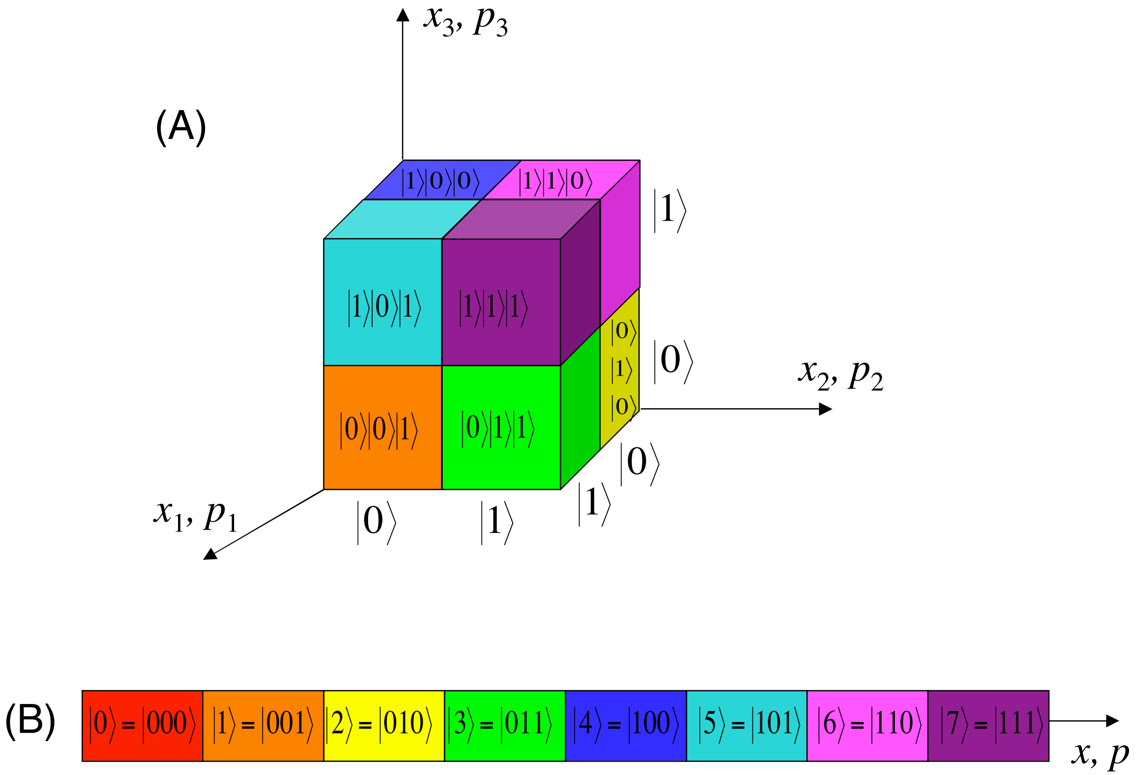
Planck’s constant sets the scale.

Hilbert space and physical resources

Primary resource is Hilbert-space dimension.

Hilbert-space dimension costs physical resources.

Many degrees of freedom



(A)
x_3, p_3
$|1\rangle|0\rangle|0\rangle$
$|1\rangle|1\rangle|0\rangle$
$|1\rangle$
$|1\rangle|0\rangle|1\rangle$
$|1\rangle|1\rangle|1\rangle$
$|0\rangle$
$|1\rangle$
$|0\rangle$
$|0\rangle$
x_2, p_2
$|0\rangle|0\rangle|1\rangle$
$|0\rangle|1\rangle|1\rangle$
$|0\rangle$
$|1\rangle$
x_1, p_1
$|0\rangle$
$|1\rangle$
(B)
$|0\rangle = |000\rangle$
$|1\rangle = |001\rangle$
$|2\rangle = |010\rangle$
$|3\rangle = |011\rangle$
$|4\rangle = |100\rangle$
$|5\rangle = |101\rangle$
$|6\rangle = |110\rangle$
$|7\rangle = |111\rangle$
x, p

Hilbert space and physical resources

Primary resource is Hilbert-space dimension.

Hilbert-space dimension costs physical resources.

Many degrees of freedom

$$2^N = \begin{pmatrix}\text{Available}\\ \text{Hilbert-space}\\ \text{dimension}\end{pmatrix} \simeq \frac{A_1\cdots A_T}{h^T} = \left(\frac{A}{h}\right)^{T}$$

Number of degrees of freedom

Hilbert-space dimension measured in qubit units.

Identical degrees of freedom

$$\boxed{\frac{A}{h} \sim 2^{N/T}}$$

quasilinear growth

Scalable resource requirement $\quad \dfrac{A}{h} \sim \mathrm{poly}(N) \qquad T \sim \dfrac{N}{\log\left(\mathrm{poly}(N)\right)}$

Strictly scalable resource requirement $\quad T \sim \dfrac{N}{\log D} \qquad \dfrac{A}{h} \sim D$ **qudits**

strictly linear growth

Example: Quantum computing in a harmonic oscillator

(field mode)

Characteristic scales are set by “oscillator units”

Length $\Delta x_c = \sqrt{\hbar/m\omega}$

Momentum $\Delta p_c = \sqrt{\hbar m\omega}$

Action $A_c = \Delta x_c \Delta p_c = \hbar$

Energy $E_c = \hbar\omega$

Quantization

$$A_n = n\hbar \qquad \Delta x_n = \sqrt{\frac{\hbar}{m\omega}}\sqrt{2n+1} \qquad \Delta p_n = \sqrt{\hbar m\omega}\sqrt{2n+1} \qquad E_n = \left(n+\frac{1}{2}\right)\hbar\omega$$

Poor scaling in this *physically unary* quantum computer

$$\Delta x_n \sim 2^{N/2}\sqrt{\frac{2\hbar}{m\omega}}$$

$$2^N = n+1 \qquad \Longrightarrow \qquad \Delta p_n \sim 2^{N/2}\sqrt{2\hbar m\omega}$$

$$E_n \sim 2^N\hbar\omega$$

▶ Phase space

Example: Quantum computing in a single atom

Experiment

Characteristic scales are set by “atomic units”

Length	Momentum	Action	Energy
$r_c = \frac{\hbar^2}{me^2} = a_0$	$p_c = \frac{me^2}{\hbar} = \frac{\hbar}{a_0}$	$L_c = r_c p_c = \hbar$	$E_c = \frac{e^2}{a_0} = \frac{p_c^2}{m}$

Bohr quantization

$$L_n = n\hbar \qquad r_n = n^2 a_0 \qquad p_n = \frac{1}{n}\frac{\hbar}{a_0} \qquad E_n = -\frac{1}{2n^2}\frac{e^2}{a_0}$$

Hilbert-space dimension up to *n*

$$2^N = \sum_{k=1}^{n} \sum_{l=0}^{k-1} (2l+1) \sim \frac{1}{3} n^3 \sim \left(\frac{L_n}{\hbar}\right)^3 = \left(\frac{r_n p_n}{\hbar}\right)^{③}$$

← 3 degrees of freedom

Example: Quantum computing in a single atom

Characteristic scales are set by “atomic units”

Length **Momentum** **Action** **Energy**

$$r_c = \frac{\hbar^2}{me^2} = a_0 \qquad p_c = \frac{me^2}{\hbar} = \frac{\hbar}{a_0} \qquad L_c = r_c p_c = \hbar \qquad E_c = \frac{e^2}{a_0} = \frac{p_c^2}{m}$$

Bohr quantization

$$L_n = n\hbar \qquad r_n = n^2 a_0 \qquad p_n = \frac{1}{n}\frac{\hbar}{a_0} \qquad E_n = -\frac{1}{2n^2}\frac{e^2}{a_0}$$

Poor scaling in this *physically unary* quantum computer

$$n \sim 2^{N/3} \quad \Longrightarrow \quad r_n \sim 2^{2N/3} a_0$$

$$N = 100 \text{ qubits} \Longrightarrow r_n \sim 10^{20} a_0 = 6 \times 10^6 \text{ km}$$

5 times the diameter of the Sun

Example: Quantum computing in a single atom

Characteristic scales are set by “atomic units”

Length	Momentum	Action	Energy
$r_c = \frac{\hbar^2}{me^2} = a_0$	$p_c = \frac{me^2}{\hbar} = \frac{\hbar}{a_0}$	$L_c = r_c p_c = \hbar$	$E_c = \frac{e^2}{a_0} = \frac{p_c^2}{m}$

Bohr quantization

$$L_n = n\hbar \qquad r_n = n^2 a_0 \qquad p_n = \frac{1}{n}\frac{\hbar}{a_0} \qquad E_n = -\frac{1}{2n^2}\frac{e^2}{a_0}$$

Poor scaling in this *physically unary* quantum computer

$$E_n \sim -2^{-2N/3}\frac{e^2}{2a_0} \qquad \Delta E \simeq \frac{e^2}{2a_0}$$

Though position range blows up exponentially, energy does not.

There are many ways not to skin a Schrödinger cat.

▶ Phase space

Quantum fields ▶

Example: Classical linear wave computing

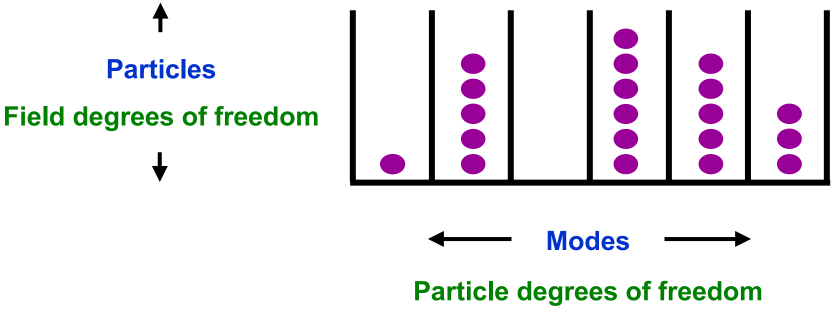
Grover's algorithm using classical waves: Bhattacharya, van den Heuvell, and Spreeuw, PRL **88**, 137901 (2002).

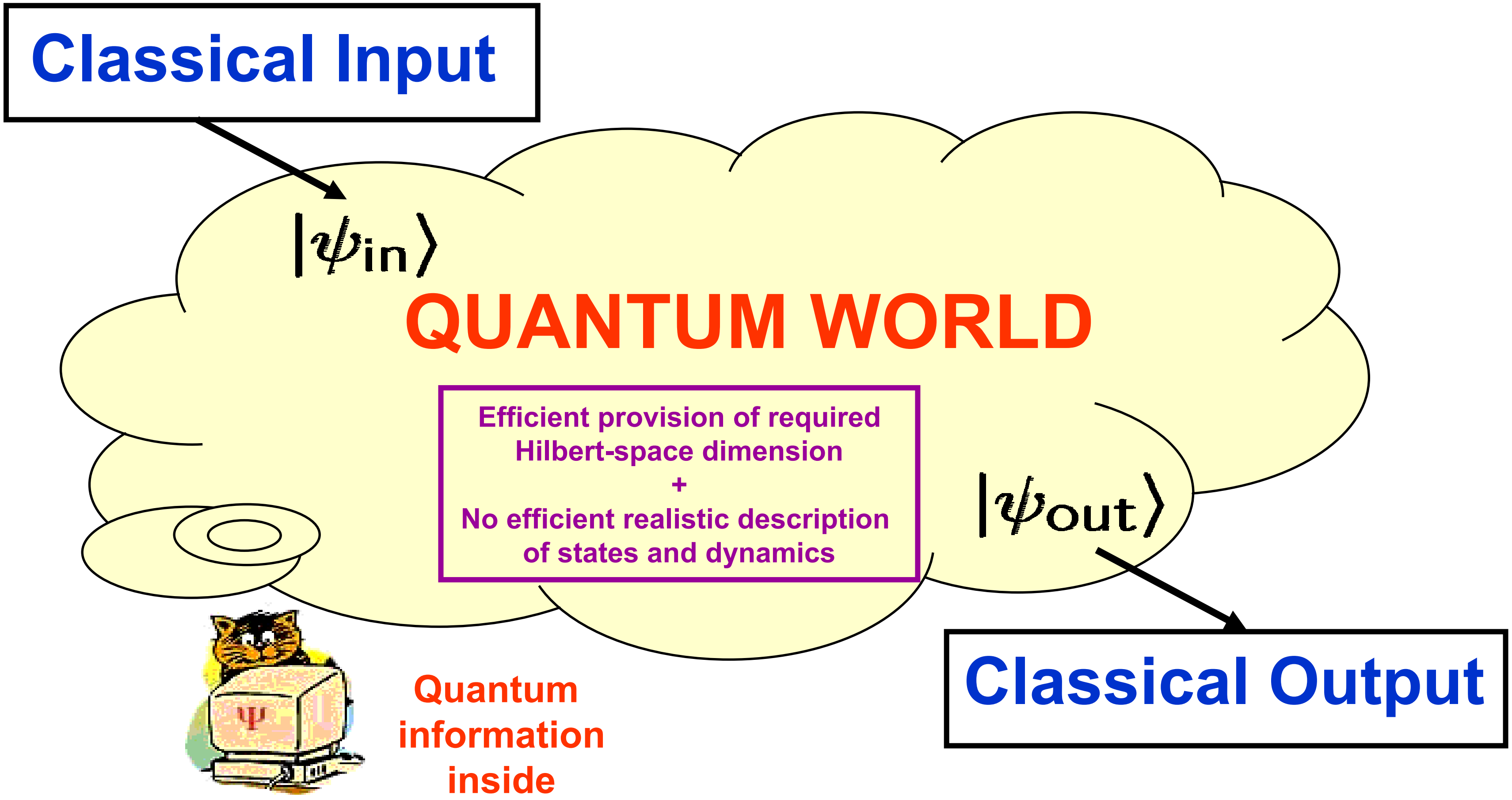
A single quantum making transitions among field modes is a physically unary system that requires an exponential number of modes.

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.





Classical Input

$|\psi_{\text{in}}\rangle$

QUANTUM WORLD

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

$|\psi_{\text{out}}\rangle$

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.

Physical resources: classical vs. quantum

A classical bit typically involves many degrees of freedom. The scaling analysis applies, but with a phase-space scale of arbitrary size. There being no fundamental scale, conclusions about resource scaling depend on a phase-space scale set by noise.

Classical bit

A few electrons on a capacitor

A pit on a compact disk

A 0 or 1 on the printed page

A smoke signal rising from a distant mesa

Quantum bit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

We still need to determine the consequences of quantum superposition.

Mr. Planck's constant sets the scale of irreducible resource requirements.

Other requirements for a scalable quantum computer

Avoiding an exponential demand for physical resources requires a quantum computer to have a scalable tensor-product structure. This is a *necessary*, but not *sufficient* requirement for a scalable quantum computer. There are certainly other requiremens.

DiVincenzo's criteria

DiVincenzo, Fortschr. Phys. **48**, 771 (2000)

1. ***Scalability:*** A scalable physical system with well characterized parts, usually qubits. ✓

2. ***Initialization:*** The ability to initialize the system in a simple fiducial state. ✓

3. ***Control:*** The ability to control the state of the computer using sequences of elementary universal gates. ✓

4. ***Stability:*** Decoherence times much longer than gate times, together with the ability to suppress decoherence through error correction and fault-tolerant computation.

5. ***Measurement:*** The ability to read out the state of the computer in a convenient product basis. ✓

III. Role of entanglement

Oljedo Wash, southern Utah

Realistic description and entanglement

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

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

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

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

exponential in problem size

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

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

exponential in problem size

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

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

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.

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

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

polynomial in problem size

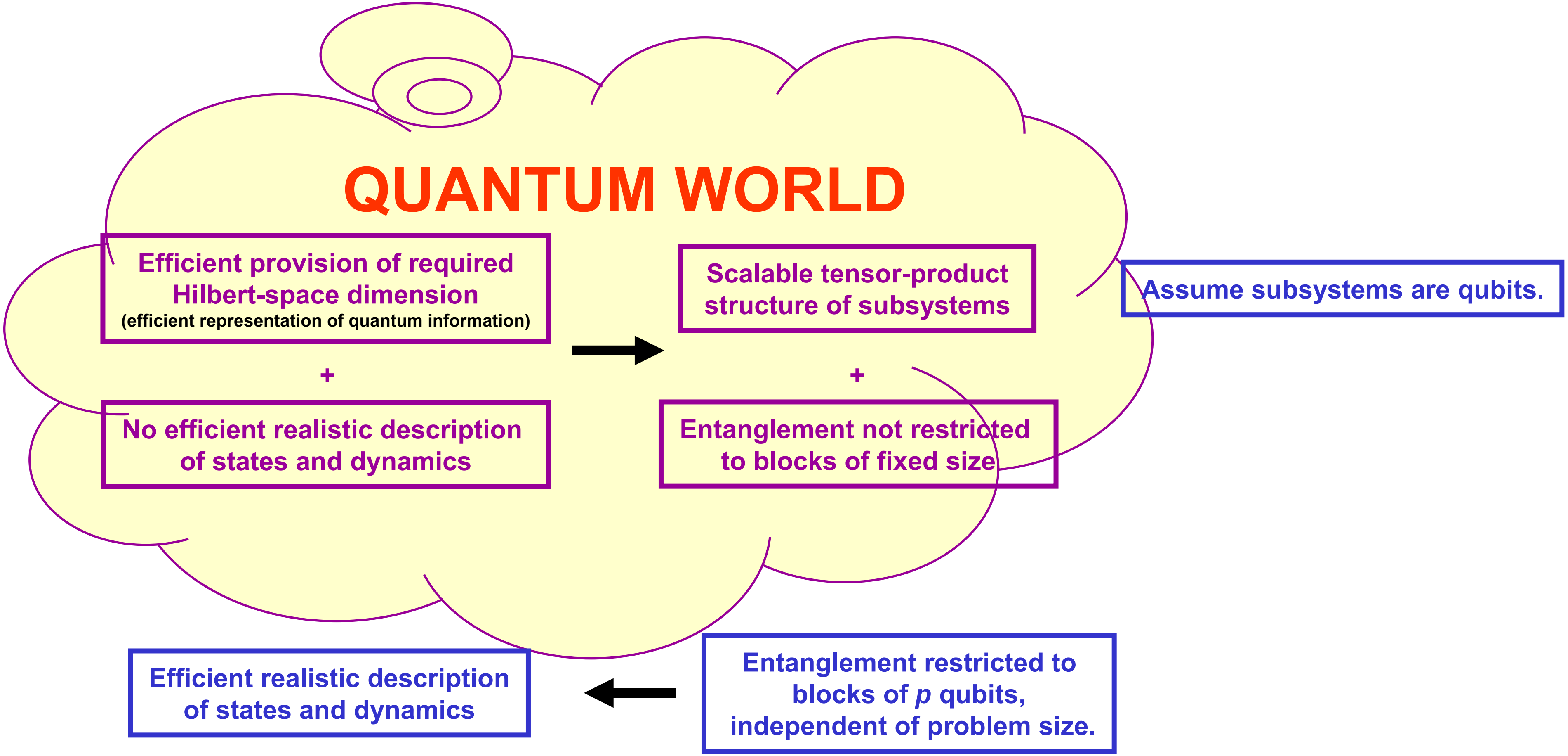
One-qudit operations: $|\psi_j'\rangle = U^{(j)}|\psi_j\rangle$

$\boxed{1}$ application of $D \times D$ unitary matrix

polynomial in problem size

Efficient realistic description

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



QUANTUM WORLD

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

+

No efficient realistic description of states and dynamics

Scalable tensor-product structure of subsystems

+

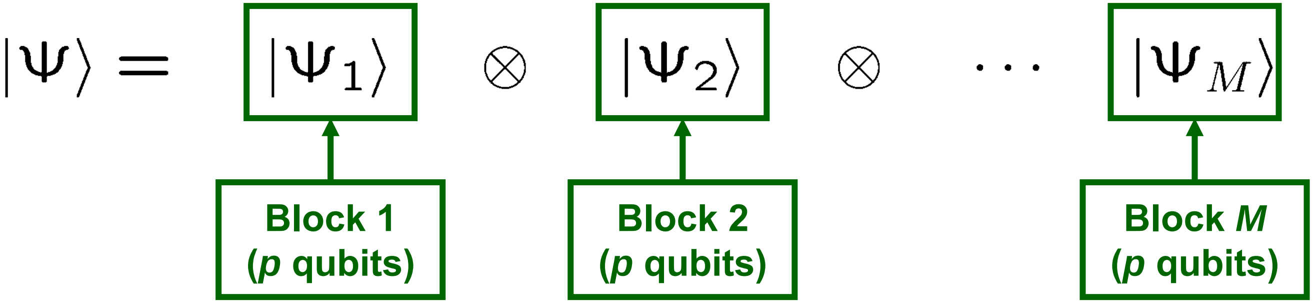
Entanglement not restricted to blocks of fixed size

Assume subsystems are qubits.

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*.



$$|\Psi\rangle = \boxed{|\Psi_1\rangle} \otimes \boxed{|\Psi_2\rangle} \otimes \cdots \boxed{|\Psi_M\rangle}$$

Block 1
(*p* qubits)

Block 2
(*p* qubits)

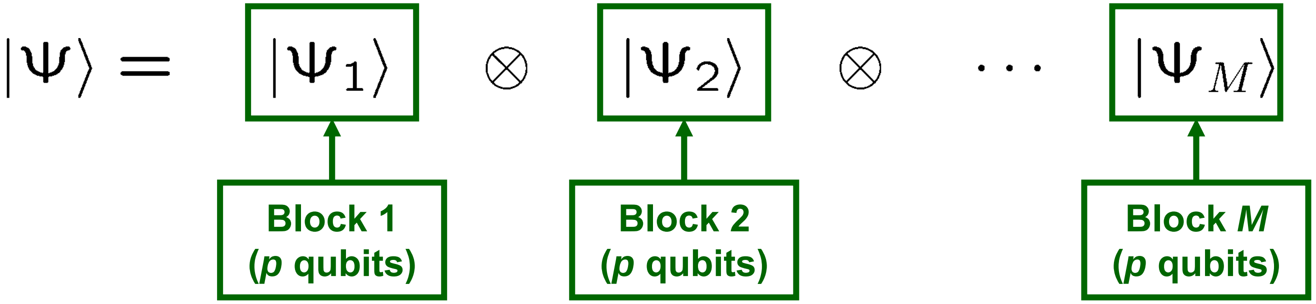
Block *M*
(*p* qubits)

***N* = *pM* qubits**

Gate set of 1- and 2-qubit gates

Realistic description and entanglement

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



$$|\Psi\rangle = \boxed{|\Psi_1\rangle} \otimes \boxed{|\Psi_2\rangle} \otimes \cdots \boxed{|\Psi_M\rangle}$$

***N* = *pM* qubits**

Gate set of 1- and 2-qubit gates

R. Jozsa and N. Linden, Proc. Roy. Soc. London A **459**, 2011 (2003).

How many quantum amplitudes need to be simulated?

How many arithmetic operations does it take to simulate 1- and 2-qubit quantum gates?

How many operations are required for readout?

The hard part of the Jozsa-Linden proof is showing that the complex arithmetic of quantum amplitudes and unitary matrices can be carried out efficiently using a sufficiently good rational approximation. By ignoring this hard aspect, we reduce the proof to a counting argument.

Realistic description and entanglement

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

$$|\Psi\rangle = \underset{\substack{\uparrow \\ \textbf{Block 1} \\ \textbf{(}\textbf{\textit{p}}\textbf{ qudits)}}}{\boxed{|\Psi_1\rangle}} \otimes \underset{\substack{\uparrow \\ \textbf{Block 2} \\ \textbf{(}\textbf{\textit{p}}\textbf{ qudits)}}}{\boxed{|\Psi_2\rangle}} \otimes \cdots \underset{\substack{\uparrow \\ \textbf{Block } \textbf{\textit{M}} \\ \textbf{(}\textbf{\textit{p}}\textbf{ qudits)}}}{\boxed{|\Psi_M\rangle}}$$

***N* = *pM* qubits**

Gate set of 1- and 2-qubit gates

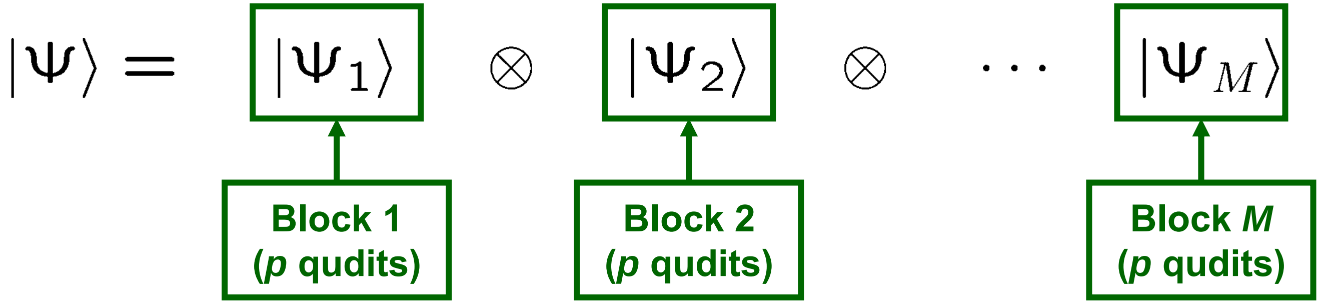
How many quantum amplitudes need to be simulated?

How many operations are required for readout?

$$(\#\text{ of amplitudes}) = 2^p M = \underset{\substack{\uparrow \\ \textbf{polynomial in} \\ \textbf{problem size}}}{\boxed{\frac{2^p}{p} N}}$$

Realistic description and entanglement

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



$$|\Psi\rangle = \boxed{|\Psi_1\rangle} \otimes \boxed{|\Psi_2\rangle} \otimes \cdots \boxed{|\Psi_M\rangle}$$

Block 1 (*p* qudits)

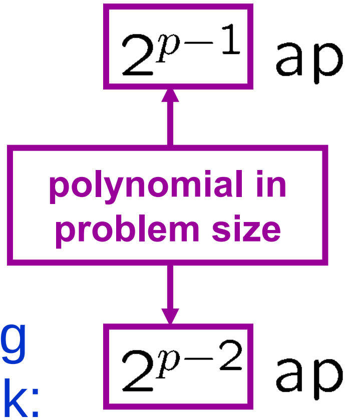
Block 2 (*p* qudits)

Block *M* (*p* qudits)

***N* = *pM* qubits**

Gate set of 1- and 2-qubit gates

How many arithmetic operations does it take to simulate 1- and 2-qubit quantum gates?



One-qubit operations: $\boxed{2^{p-1}}$ applications of 2×2 matrix

polynomial in problem size

Two-qubit operations acting on two qubits in same block: $\boxed{2^{p-2}}$ applications of 4×4 matrix

Realistic description and entanglement

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

$$|\Psi\rangle = \underset{\substack{\uparrow \\ \boxed{\substack{\textbf{Block 1} \\ \textbf{(}\boldsymbol{p}\textbf{ qudits)}}}}}{\boxed{|\Psi_1\rangle}} \otimes \underset{\substack{\uparrow \\ \boxed{\substack{\textbf{Block 2} \\ \textbf{(}\boldsymbol{p}\textbf{ qudits)}}}}}{\boxed{|\Psi_2\rangle}} \otimes \cdots \underset{\substack{\uparrow \\ \boxed{\substack{\textbf{Block }\boldsymbol{M} \\ \textbf{(}\boldsymbol{p}\textbf{ qudits)}}}}}{\boxed{|\Psi_M\rangle}}$$

***N* = *pM* qubits**

Gate set of 1- and 2-qubit gates

How many arithmetic operations does it take to simulate 1- and 2-qubit quantum gates?

Two-qubit operations acting on two qubits in different blocks:

$\boxed{2^{2p-2}}$ applications of 4×4 matrix

$\boxed{\binom{2p}{p}}$ checks to determine new p-blocks

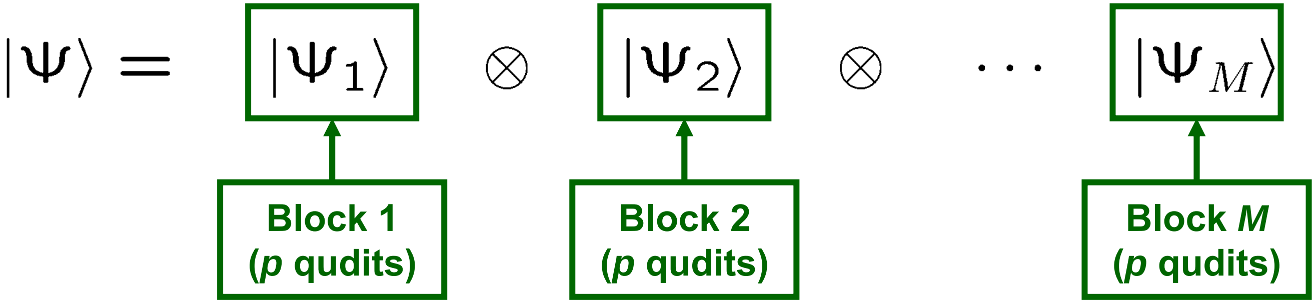
$\uparrow$

polynomial in problem size

In the absence of this reblocking, we have *M* local qudit processors.

Realistic description and entanglement

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



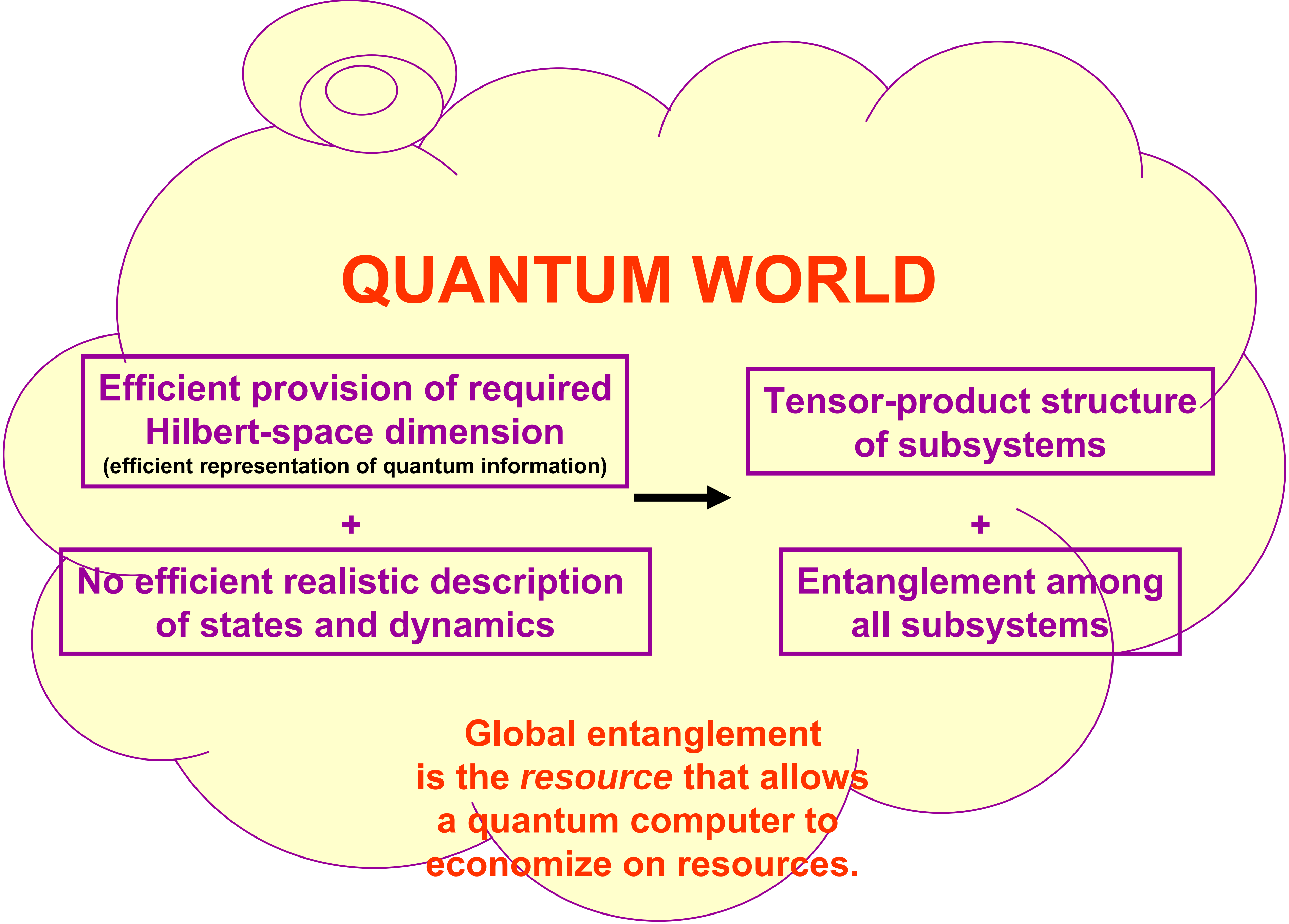
$$|\Psi\rangle = \boxed{|\Psi_1\rangle} \otimes \boxed{|\Psi_2\rangle} \otimes \quad \cdots \quad \boxed{|\Psi_M\rangle}$$

***N* = *pM* qubits**

Gate set of 1- and 2-qubit gates

_p_-blocked entanglement → **Efficient realistic description**

No efficient realistic description → **Global entanglement**



QUANTUM WORLD

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

+

No efficient realistic description of states and dynamics

→

Tensor-product structure of subsystems

+

Entanglement among all subsystems

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

BUT

wait just one minute.

Well, gimme 30.

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 although the soup was indeed awful, only the sauerkraut was of any value in preventing scurvy.

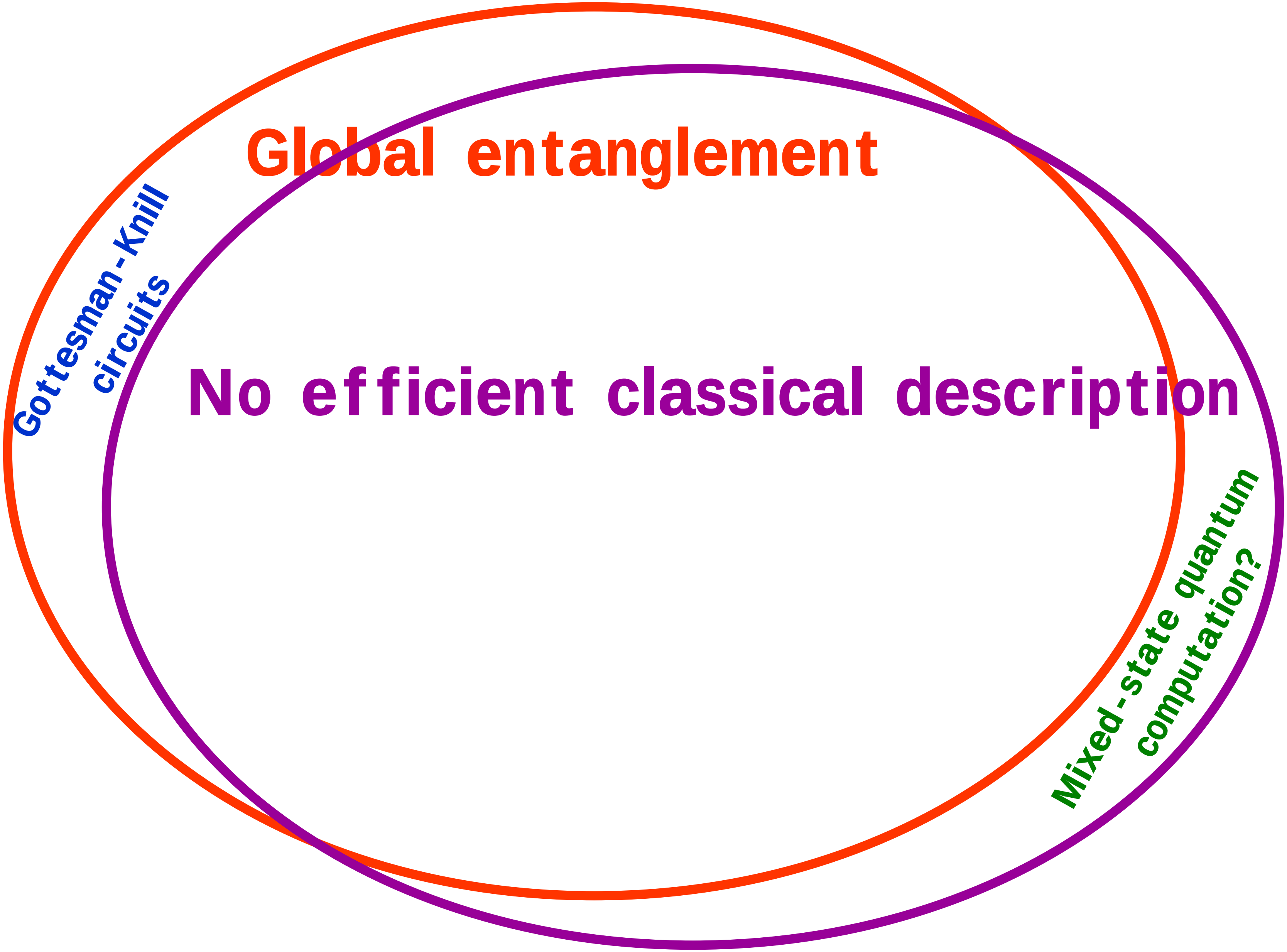
When we report that “global entanglement is the essential resource for quantum computation,” are we making a logically similar statement?

IV. Why we don't know all the answers

Gottesman-Knill circuits

Mixed-state quantum computation

Aspens in the Sangre de Cristo Range



Global entanglement

No efficient classical description

Gottesman-Knill circuits

Mixed-state quantum computation?

Mixed

Gottesman-Knill circuits

- N qubits in an initial product state in the 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

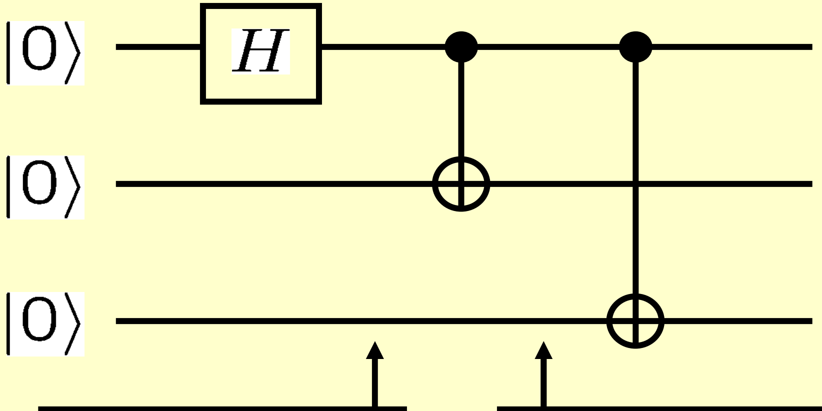
Efficient (nonlocal) realistic description of states, dynamics, and measurements

Details ▶

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

QUANTUM WORLD

ZII
IZI
IIZ



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

XII, IZI, IIZ

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

XXI, ZZI, IIZ

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

GHZ entangled state

XXX, ZZI, ZIZ

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

Efficient (nonlocal) realistic description 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

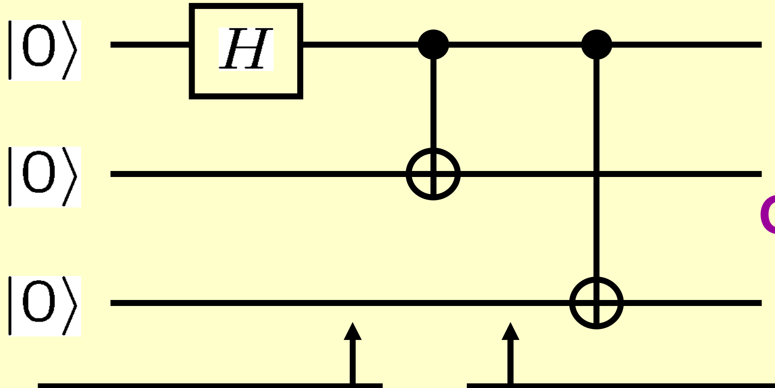
Efficient (nonlocal) realistic description of states, dynamics, and measurements

This kind of global entanglement, when measurements are restricted to the Pauli group, is, 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



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

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_1r_2	r_1
r_2	r_1r_2	r_1
r_3	r_3	1

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

GHZ entangled state

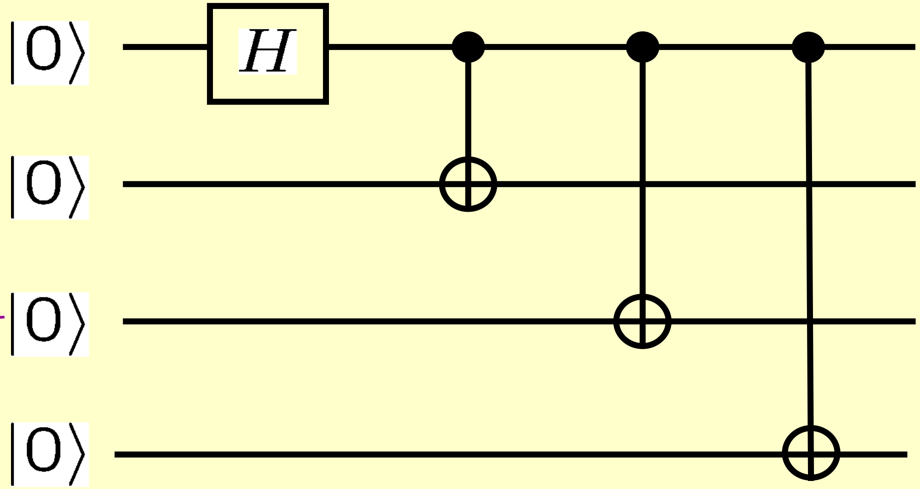
x	y	z
r_2r_3	$r_1r_2r_3$	r_1
r_2	r_1r_2	r_1
r_3	r_1r_3	r_1

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.*

Assume 1 bit of communication between qubits 1 and 2.
Letting *S*=*XX* and *T*=*XY*, we have *SYY*=*TXY*=*TYX*=-1.
Local realism implies *SXX*=-1.
Quantum mechanics says *SXX*=+1.

QUANTUM WORLD

$$\begin{array}{c} ZIII \\ IZII \\ IIZI \\ IIIZ \end{array}$$



$$\boxed{\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)}$$

4-qubit GHZ entangled state

$$XXXX, ZZII, ZIZI, ZIIZ$$

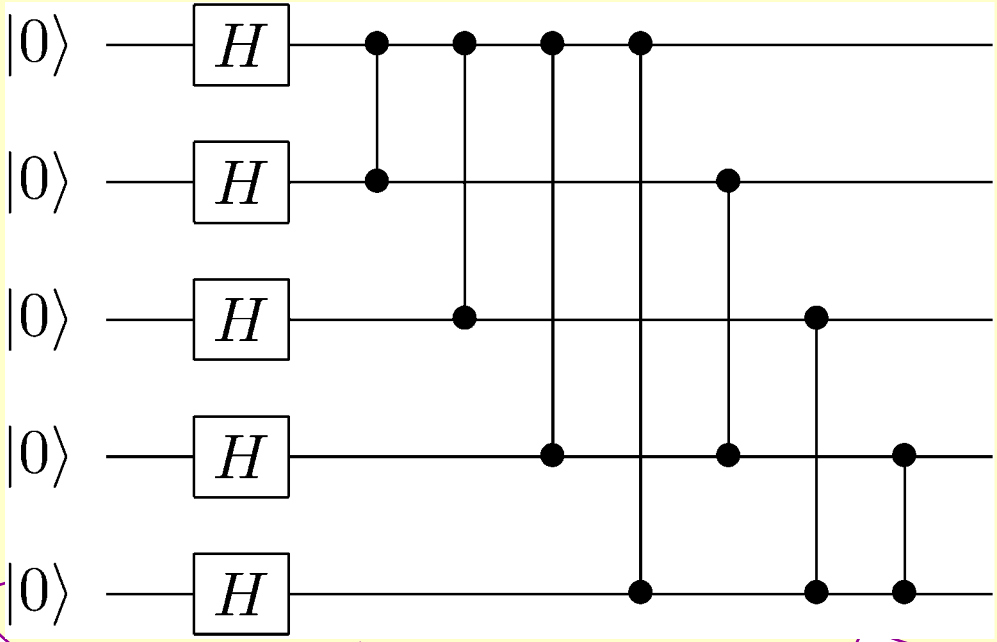
$$S = \left\{ \begin{array}{c} IIII, ZZII, ZIZI, ZIIZ, IZZI, IZIZ, IIZZ \\ XXXX, -XXYY, -XYXY, -XYYX, \\ -YXXY, -YXYX, -YYXX, YYYY \end{array} \right\}$$

For *N*-qubit GHZ states, a simple extension of this argument shows that *N-2* bits of *classical communication* is the minimum required to mimic the predictions of quantum mechanics.

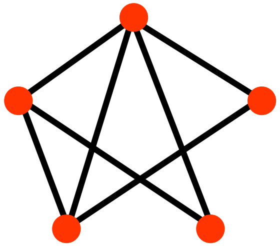
All GK states are related to graph states by *Z*, Hadamard, and S gates. All graph states have a communication-assisted LHV model of the sort used for GHZ states.

QUANTUM WORLD

$ZIIII$
$IZIII$
$IIZII$
$IIIZI$
$IIIIZ$



$XZZZZ$
$ZXIZI$
$ZIXIZ$
$ZZIXZ$
$ZIZZX$



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

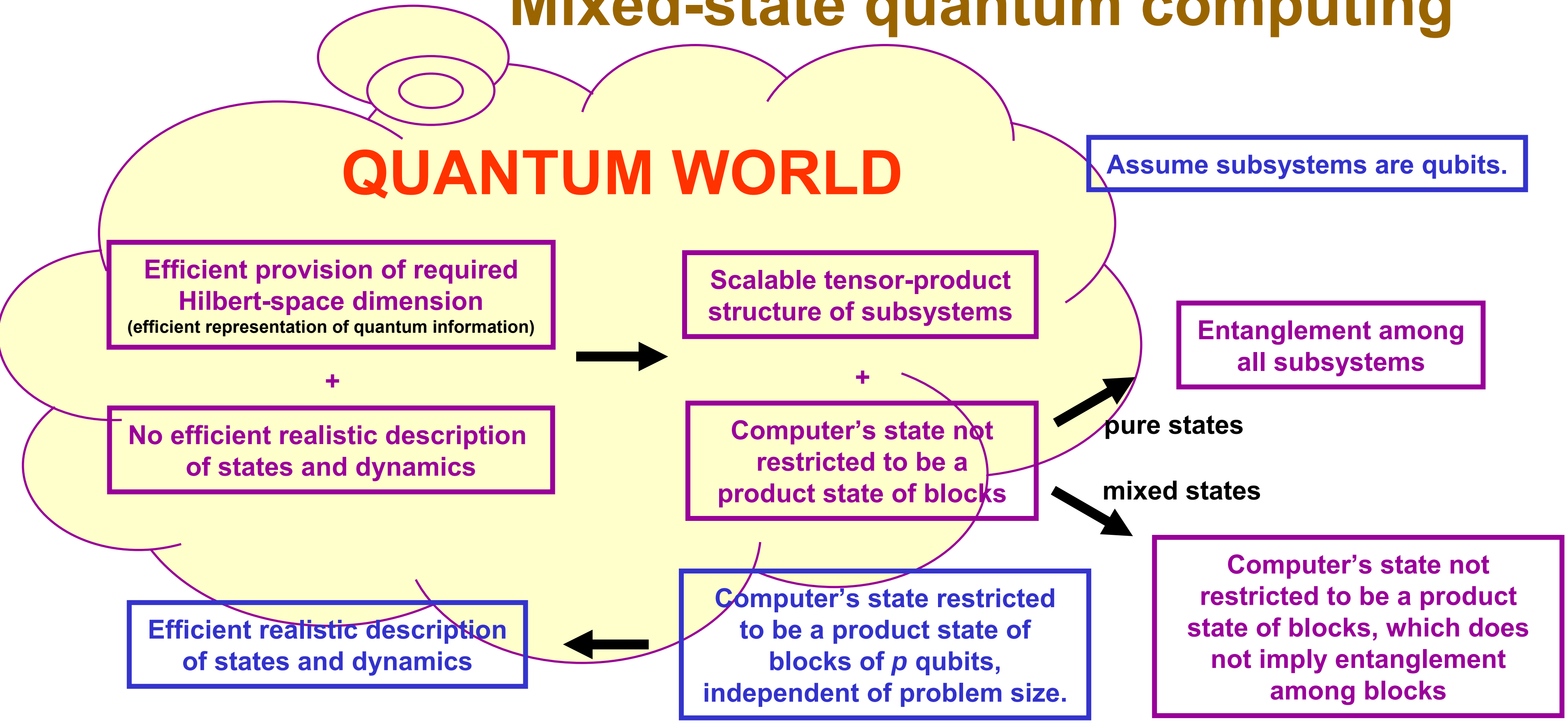
Efficient (nonlocal) realistic description of states, dynamics, and measurements

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.

Conclusion

▶

Mixed-state quantum computing



QUANTUM WORLD

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

+

No efficient realistic description of states and dynamics

Scalable tensor-product structure of subsystems

+

Computer's state not restricted to be a product state of blocks

Assume subsystems are qubits.

pure states

Entanglement among all subsystems

mixed states

Computer's state not restricted to be a product state of blocks, which does not imply entanglement among blocks

Computer's state restricted to be a product state of blocks of *p* qubits, independent of problem size.

Efficient realistic description of states and dynamics

ρ not entangled (separable)

$$\rho = \begin{pmatrix} \textit{mixture of} \\ \text{product states} \end{pmatrix} = \sum_j p_j \rho_j^{(1)} \otimes \cdots \otimes \rho_j^{(M)}$$

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 $\mathrm{tr}(U)/2^N$ to a fixed accuracy.

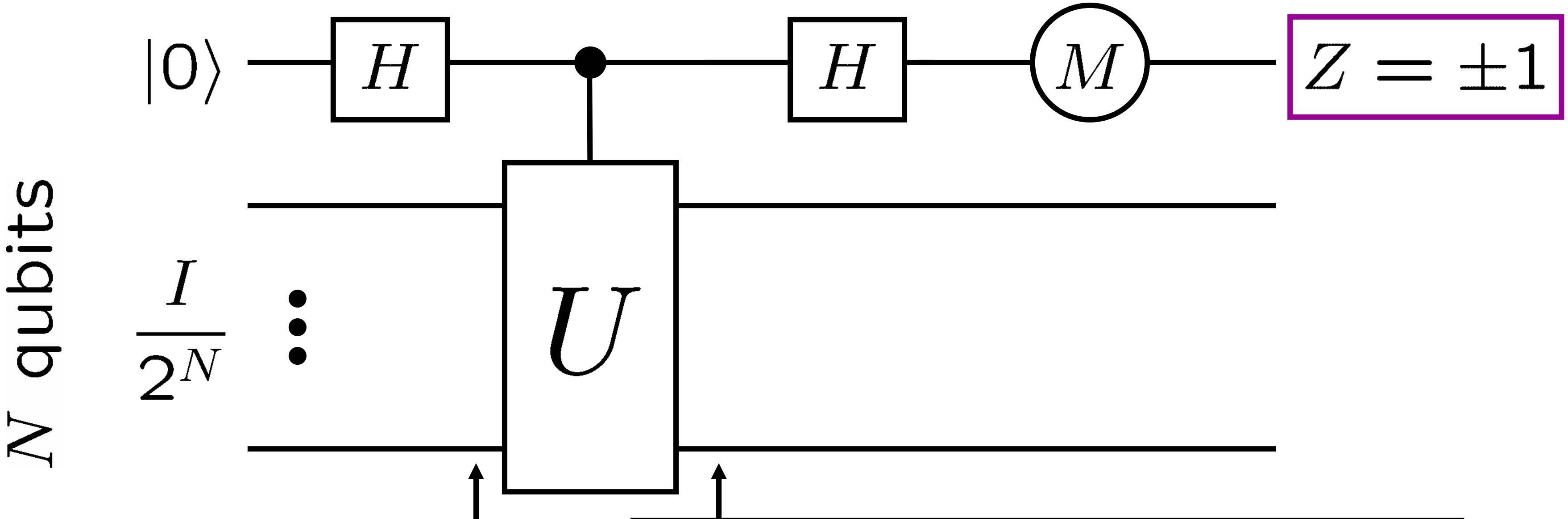
Power of one qubit

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, PRL **92**, 177906 (2004).

Power of one qubit

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

Many repetitions



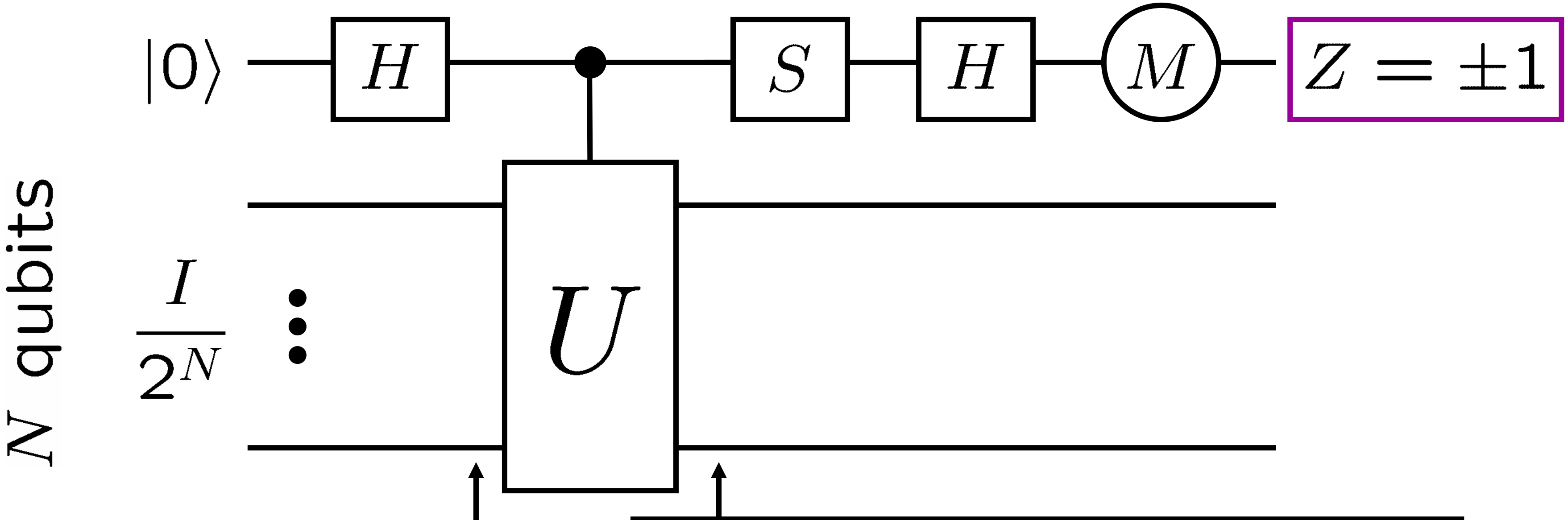
$$\frac{1}{2^{N+1}}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\Big)\otimes I$$

$$\begin{aligned}\rho &= \frac{1}{2^{N+1}}\Big(|0\rangle\langle 0|\otimes I + |0\rangle\langle 1|\otimes U^\dagger \\ &\qquad + |1\rangle\langle 0|\otimes U + |1\rangle\langle 1|\otimes I\Big) \\ &= \frac{1}{2^{N+1}}\Big(I\otimes I + |0\rangle\langle 1|\otimes U^\dagger + |1\rangle\langle 0|\otimes U\Big)\end{aligned}$$

Power of one pure qubit

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

Many repetitions



$$\frac{1}{2^{N+1}}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\Big)\otimes I$$

$$\begin{aligned}\rho &= \frac{1}{2^{N+1}}\Big(|0\rangle\langle 0|\otimes I + |0\rangle\langle 1|\otimes U^\dagger + |1\rangle\langle 0|\otimes U + |1\rangle\langle 1|\otimes I\Big)\\ &= \frac{1}{2^{N+1}}\Big(I\otimes I + |0\rangle\langle 1|\otimes U^\dagger + |1\rangle\langle 0|\otimes U\Big)\end{aligned}$$

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 $\mathrm{tr}(U)/2^N$ to a fixed accuracy.

- $O(1/\epsilon^2)$ repetitions are needed to determine $\langle Z \rangle$ and, hence, $\mathrm{tr}(U)/2^N$ with accuracy ϵ.

- If the special qubit has an initial polarization δ, the output expectation value is reduced by a factor of δ. 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?

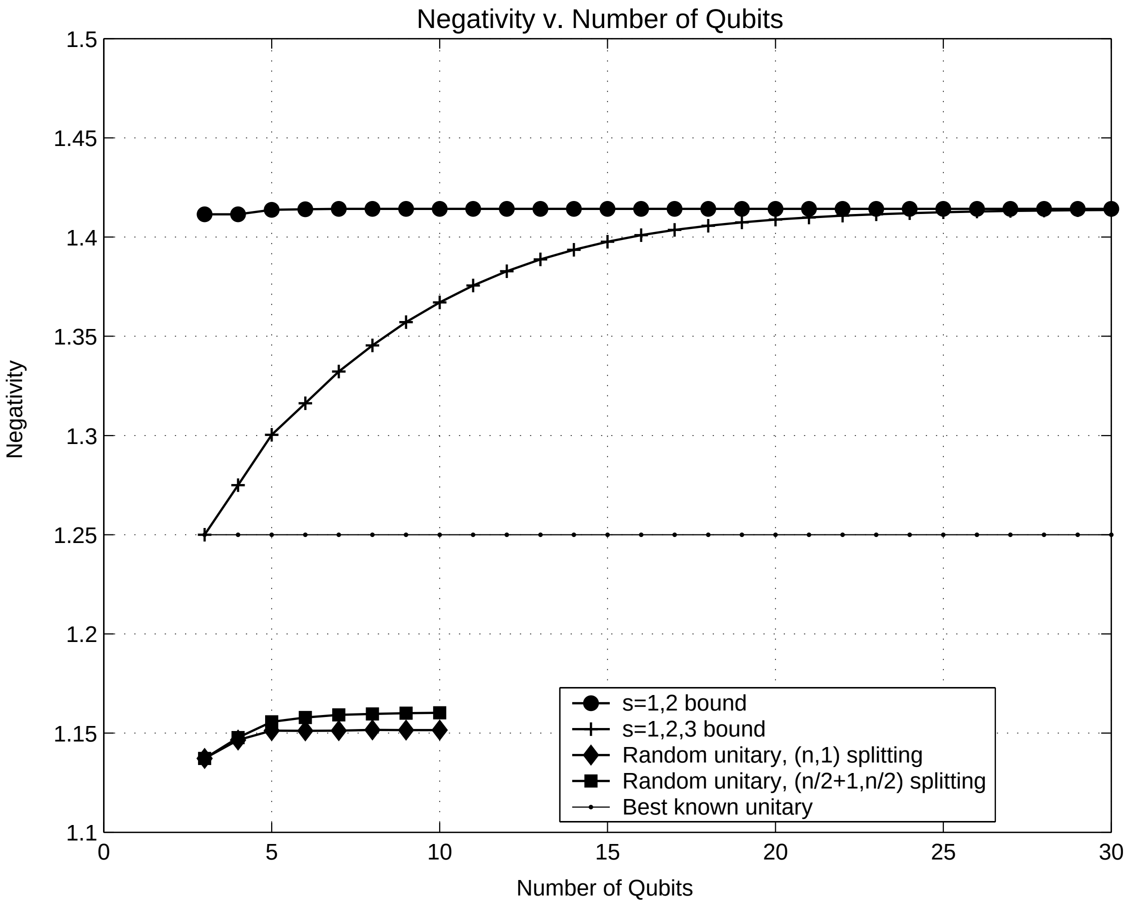
- **Given a unitary operator *U* on *N* qubits, which can be implemented efficiently in terms of a universal set of quantum gates, is there a classical algorithm for finding tr(*U*)/2^N to a fixed accuracy?**

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

Mixed-state quantum computing

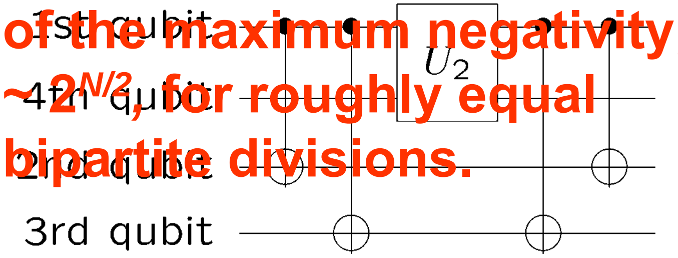
Power of one qubit

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



$$U_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

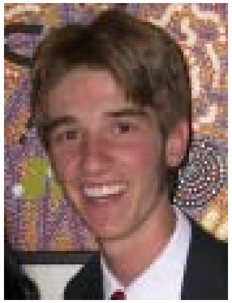
The achievable negativity is a vanishingly small fraction of the maximum negativity, ~$2^{N/2}$, for roughly equal bipartite divisions.



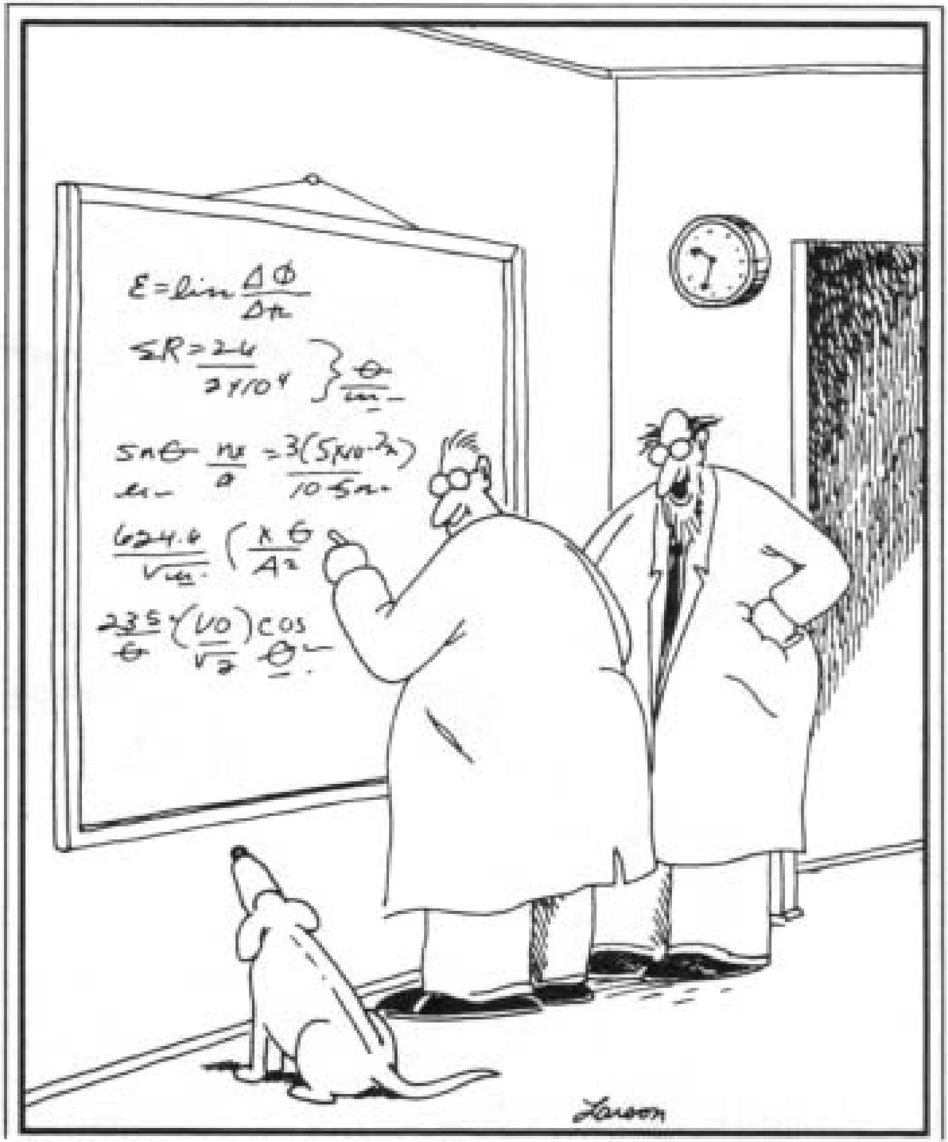
Planck’s constant did appear.

Alice

Alice and Bob did not.



Bob



“Ohhhhhh…Look at that, Schuster…Dogs are so cute when they try to comprehend quantum mechanics.”

Before getting too proud of ourselves, can we say we really *comprehend* quantum mechanics? Or do we just know how to use the formalism?

Is quantum mechanics a “law of thought” or a “law of physics” or some combination of the two? We need to disentangle the epistemology from the ontology.

Can there be a better route to understanding than studying how to use quantum phenomena to accomplish information-processing tasks that are impossible in a classical world?

Quantum information science is the place.

Quantum fields

L **particles**

M **single-particle states (modes)**

K **spatial modes**

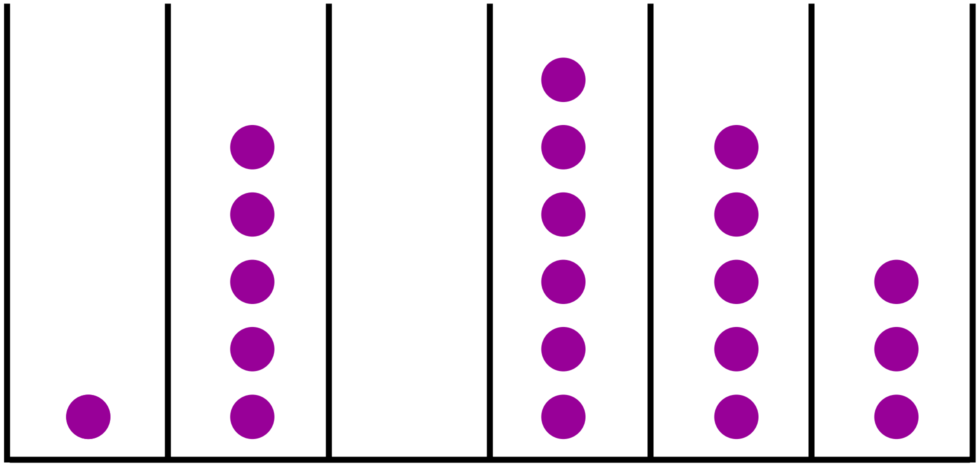
D **internal states**

M* = *KD

Particles

Field degrees of freedom

$\Delta E \Delta B$



Modes

Particle degrees of freedom

$\Delta x \Delta p$

Bose ▶ Fermi ▶ Distinguishable ▶

Quantum fields

L particles

M single-particle states (modes)

K spatial modes

D internal states

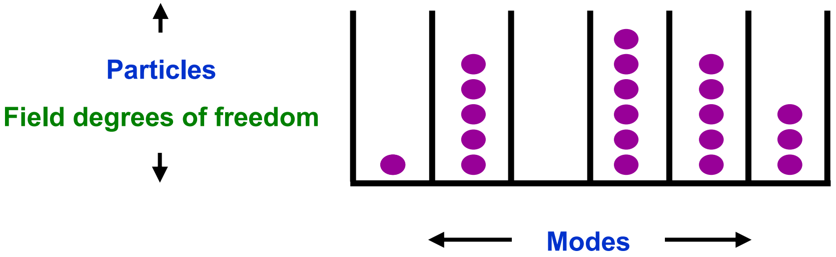
M = *KD*

Bose systems

$$2^N = \Omega_B = \frac{(L+M-1)!}{(M-1)!\,L!}$$

Particle-mode symmetry

$$L \leftrightarrow M-1$$



Particles

Field degrees of freedom

Modes

Particle degrees of freedom

Quantum fields

L_{max} **particles**

$$L = 0, 1, \ldots, L_{\text{max}}$$

$$(L \to L_{\text{max}},\ M \to M + 1)$$

***M* single-particle states (modes)**

***K* spatial modes**

***D* internal states**

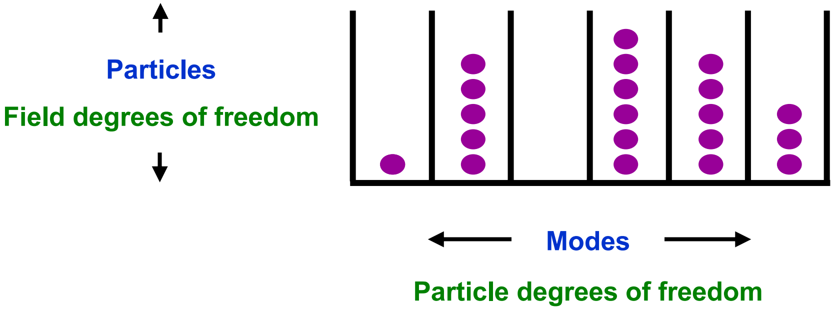
M = KD

Bose systems

$$2^N = \Omega'_B = \frac{(L_{\text{max}} + M)!}{M!\, L_{\text{max}}!}$$

Particle-mode symmetry

$$L_{\text{max}} \leftrightarrow M$$



Scaling of bose systems. I

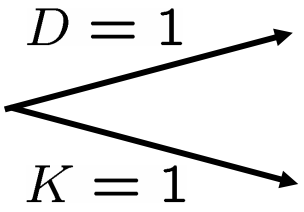
Asymptotics of $2^N = \Omega_B = \dfrac{(L+M-1)!}{(M-1)!\,L!}$

***L* fixed, *M* grows:** $\cancel{2^N = \Omega_B \sim \dfrac{M^L}{L!}}$ ***M* grows exponentially**

***M* fixed, L_{max} grows:** $\cancel{2^N = \Omega_B \sim \dfrac{L_{\text{max}}^M}{M!}}$ **L_{max} grows exponentially**

Physically unary systems

***L* = 1:** $2^N = \Omega_B = M$



$D = 1$ **Single-photon optics**

$K = 1$ **Single atom or molecule**

***M* = 1:** $2^N = \Omega'_B = L_{\text{max}}$ **Single optical mode (harmonic oscillator)**

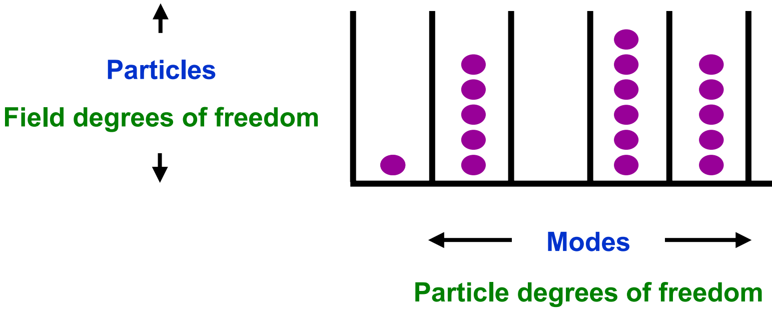
Classical linear wave computing

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

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



Particles

Field degrees of freedom

Modes

Particle degrees of freedom

Scaling of bose systems. II

Asymptotics of $2^N = \Omega_B = \dfrac{(L+M-1)!}{(M-1)!\,L!}$

***L* and *M* both grow:** $2^N = \Omega_B \sim \underbrace{\left(1+\frac{L}{M}\right)^M}_{\text{field d.o.f.}} \underbrace{\left(1+\frac{M}{L}\right)^L}_{\text{particle d.o.f.}}$

Scalable resource requirement

$$\frac{M}{L} \sim \text{poly}(N) \qquad L \sim \frac{N}{\log(\text{poly}(N))} \qquad M \sim \frac{N\text{poly}(N)}{\log(\text{poly}(N)}$$

or

$$\frac{L}{M} \sim \text{poly}(N) \qquad M \sim \frac{N}{\log(\text{poly}(N))} \qquad L \sim \frac{N\text{poly}(N)}{\log(\text{poly}(N)}$$

Scaling of bose systems. II

***L* and *M* both grow:** $\dfrac{L}{M} = \mu = \text{constant}$

$$2^N = \Omega_B \sim \underbrace{(1+\mu)^M}_{\substack{\text{field}\\ \text{d.o.f.}}} \underbrace{(1+\mu^{-1})^L}_{\substack{\text{particle}\\ \text{d.o.f.}}} = 2^{MS(\mu)} = 2^{LS(1/\mu)}$$

Entropy of a field mode that has *L/M* particles on average

Strictly scalable resource requirement

$$M \sim \frac{N}{S(\mu)} \qquad L \sim \frac{N}{S(1/\mu)} = \frac{\mu N}{S(\mu)}$$

$\mu \gg 1$: $2^N = \Omega_B \sim \mu^M = (\text{particles/mode})^M$

$M \sim N/\log\mu$

Field d.o.f. predominate

$\mu \ll 1$: $2^N = \Omega_B \sim (1/\mu)^L = (\text{modes/particle})^L$

$L \sim N/\log(1/\mu)$

Particle d.o.f. predominate

Quantum fields

L **particles**

M **single-particle states (modes)**

K **spatial modes**

D **internal states**

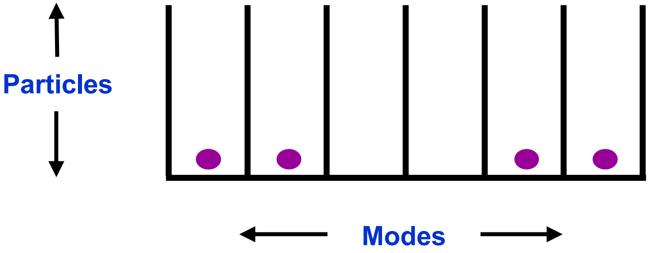
M = KD

Fermi systems

$$2^N = \Omega_F = \frac{M!}{L!\,(M-L)!}$$

Particle-hole symmetry

$$L \to M - L$$



Particle degrees of freedom

Scaling of fermi systems. I

Asymptotics of $$2^N = \Omega_F = \frac{M!}{L!\,(M-L)!}$$

***L* fixed, *M* grows:** $$\cancel{2^N = \Omega_F \sim \frac{M^L}{L!}}$$ ***M* grows exponentially**

***L* and *M* both grow:**

$$2^N = \Omega_F \sim \underbrace{\left(\frac{1}{1-L/M}\right)^{M-L}}_{\text{hole d.o.f.}} \underbrace{\left(\frac{M}{L}\right)^{L}}_{\text{particle d.o.f.}}, \qquad L \leq M$$

Scalable resource requirement

$$\frac{M}{L} \sim \text{poly}(N) \qquad L \sim \frac{N}{\log(\text{poly}(N))} \qquad M \sim \frac{N\text{poly}(N)}{\log(\text{poly}(N))}$$

Scaling of fermi systems. II

***L* and *M* both grow:** $\dfrac{L}{M} = \mu\,, \qquad \mu \le 1$

$$2^N = \Omega_F \sim \underbrace{(1-\mu)^{-(1-\mu)M}}_{\substack{\text{hole}\\ \text{d.o.f.}}} \; \underbrace{\mu^{-\mu M}}_{\substack{\text{particle}\\ \text{d.o.f.}}} = 2^{MH(\mu)}$$

binary Shannon entropy for fraction *L/M*

Strictly scalable resource requirement

$$M \sim \frac{N}{H(\mu)} \qquad\qquad L \sim \frac{\mu N}{H(\mu)}$$

$$\mu \ll 1 \;: \qquad 2^N = \Omega_F \sim (1/\mu)^L = (\text{modes/particle})^L$$

$$L \sim N/\log(1/\mu)$$

Particle d.o.f. predominate

$$1-\mu \gg 1 \;: \qquad 2^N = \Omega_F \sim [1/(1-\mu)]^{M-L} = (\text{modes/hole})^{M-L}$$

$$M - L \sim N/\log[1/(1-\mu)]$$

Hole d.o.f. predominate

Quantum fields

L particles

Only one particle per spatial mode (external state). Spatial label makes particles effectively distinguishable.

M single-particle states (modes)

K spatial modes

D internal states

$M = KD$

"Distinguishable" particles

$$L \le K$$

$$2^N = \Omega_D = \frac{K!}{L!\,(K-L)!} D^{L}$$

D = 1 reduces to the fermi case.

For truly distinguishable particles, the *L*! is absent.

L = *K* reduces to the simple d.o.f. analysis.

K plays the role of the number of d.o.f., *T*, in the simple d.o.f. analysis, and *D* plays the role of *A*/*h*, but note that *D* is raised not to the power *K*, as in the simple analysis, but to the power *L*, because not all the external states are occupied.

Scaling of “distinguishable” particles. I

Asymptotics of $2^N = \Omega_E = \dfrac{K!}{L!\,(K-L)!} D^L$

***L* fixed, *K* grows:** $\cancel{2^N = \Omega_D \sim \dfrac{(KD)^L}{L!}}$ ***K* grows exponentially**

***L* and *K* both grow:**

$$2^N = \Omega_D \sim \left(\frac{1}{1-L/K}\right)^{K-L} \left(\frac{KD}{L}\right)^L , \qquad L \le K$$

Scalable resource requirement

$$\frac{K}{L} \sim \frac{1}{D}\mathrm{poly}(N) \qquad L \sim \frac{N}{\log(\mathrm{poly}(N))} \qquad K \sim \frac{1}{D}\frac{N\mathrm{poly}(N)}{\log(\mathrm{poly}(N))}$$

Scaling of “distinguishable” particles. II

L **and** ***K*** **both grow:** $\dfrac{L}{K} = \mu\,, \qquad \mu \leq 1$

$$2^N = \Omega_D \sim (1-\mu)^{-(1-\mu)K}\mu^{-\mu K}D^L = 2^{K[H(\mu)+\mu\log D]}$$

binary Shannon entropy for fraction *L/K*

Strictly scalable resource requirement

$$K \sim \frac{N}{H(\mu)+\mu\log D} \qquad\qquad L \sim \frac{\mu N}{H(\mu)+\mu\log D}$$

Quantum fields. Summary

L particles

M single-particle states (modes)

K spatial modes

D internal states

$M = KD$

Scalability requires that the number of particles or the number of modes, whichever (or both) acts as the effective number of degrees of freedom, must grow quasilinearly with the equivalent number of qubits, *N*; if the effective number of degrees of freedom grows more slowly than quasilinearly in *N*, the complementary resource set demands an exponential supply of physical resources.

◀

Quantum key distribution using entanglement

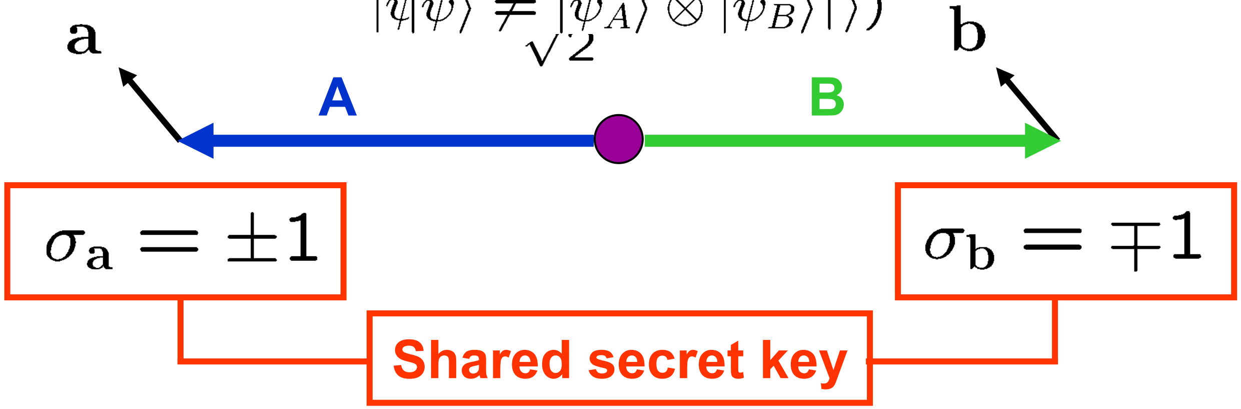
Entangled state

(quantum correlations)

Bell entangled state

$$|\psi\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(\ldots |\uparrow\rangle \rangle \right)$$



$\sigma_{\mathrm{a}} = \pm 1$

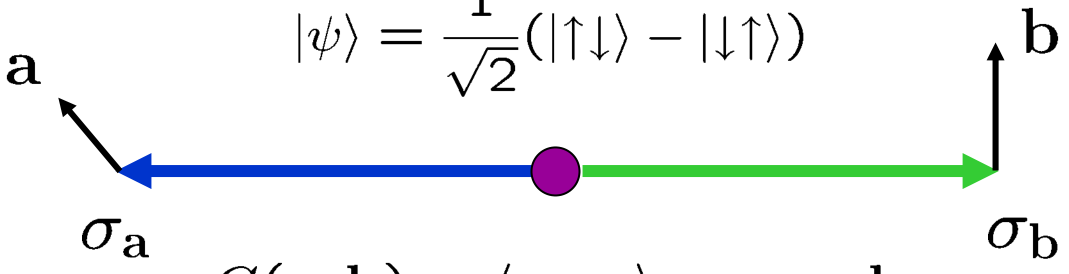
$\sigma_{\mathrm{b}} = \mp 1$

Shared secret key

Quantum key distribution using entanglement

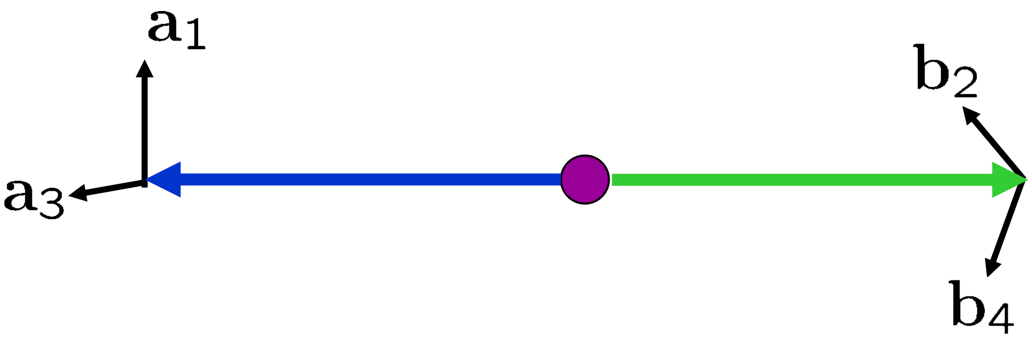
Bell entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$$



$$C(\mathbf{a},\mathbf{b}) \equiv \langle \sigma_{\mathbf{a}} \sigma_{\mathbf{b}} \rangle = -\mathbf{a}\cdot\mathbf{b}$$

Local hidden variables (LHV) and Bell inequalities



LHV: $|S| \leq 2$

QM: $S = 2\sqrt{2}$

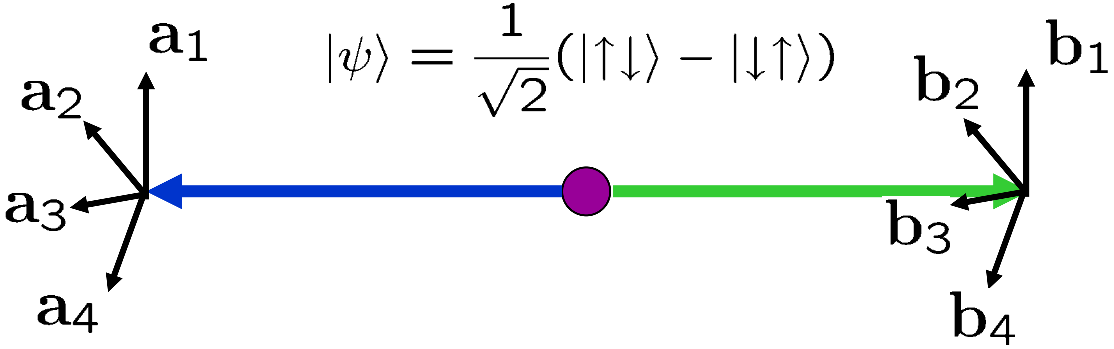
$$\begin{aligned} S &= C(\mathbf{a}_1,\mathbf{b}_2) + C(\mathbf{a}_3,\mathbf{b}_2) + C(\mathbf{a}_3,\mathbf{b}_4) - C(\mathbf{a}_1,\mathbf{b}_4) \\ &= \sigma_{\mathbf{a}_1}(\sigma_{\mathbf{b}_2} - \sigma_{\mathbf{b}_4}) + \sigma_{\mathbf{a}_3}(\sigma_{\mathbf{b}_2} + \sigma_{\mathbf{b}_4}) = \pm 2 \end{aligned}$$

Quantum key distribution using entanglement

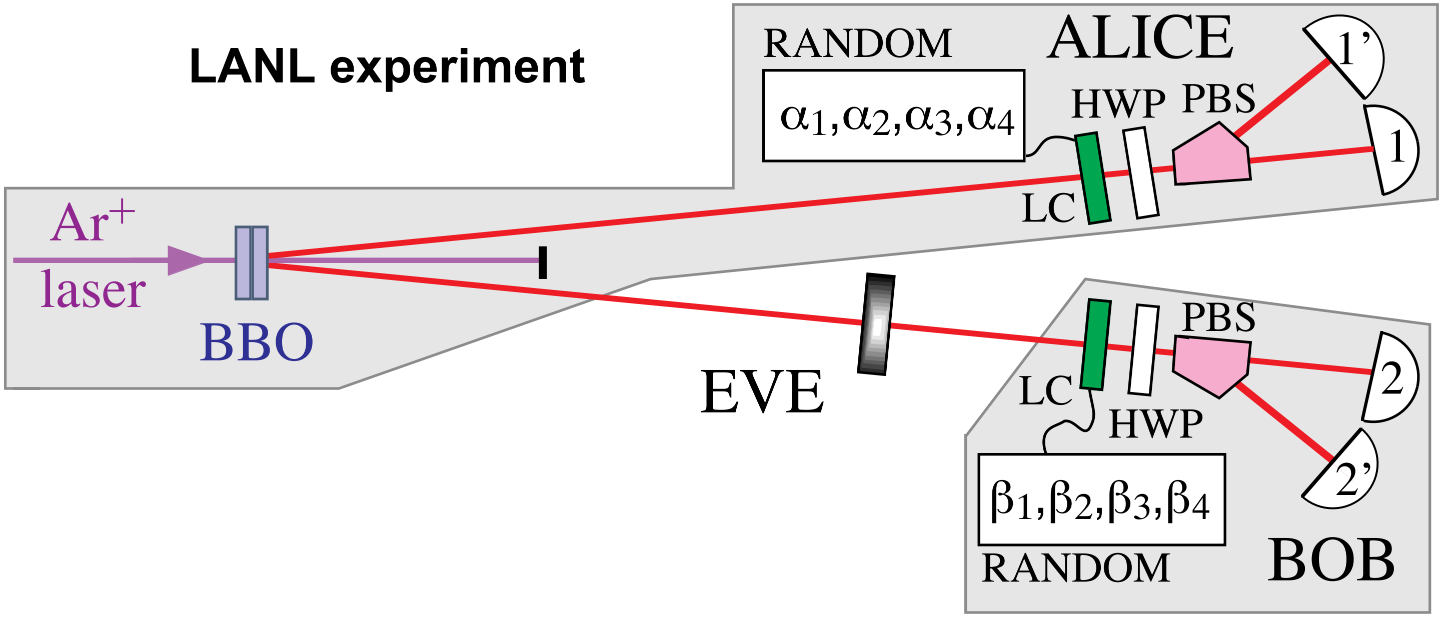
Theory: Ekert, PRL **67**, 661 (1991)
Experiment: Naik *et al.*, PRL **84**, 4733 (2000)
Tittel *et al.*, PRL **84**, 4737 (2000)
Jennewein *et al.*, PRL **84**, 4729 (2000)

Bell entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$$



LANL experiment


RANDOM
ALICE
$\alpha_1,\alpha_2,\alpha_3,\alpha_4$
HWP
PBS
1'
1
LC
Ar$^+$
laser
BBO
EVE
LC
HWP
PBS
2
2'
$\beta_1,\beta_2,\beta_3,\beta_4$
RANDOM
BOB

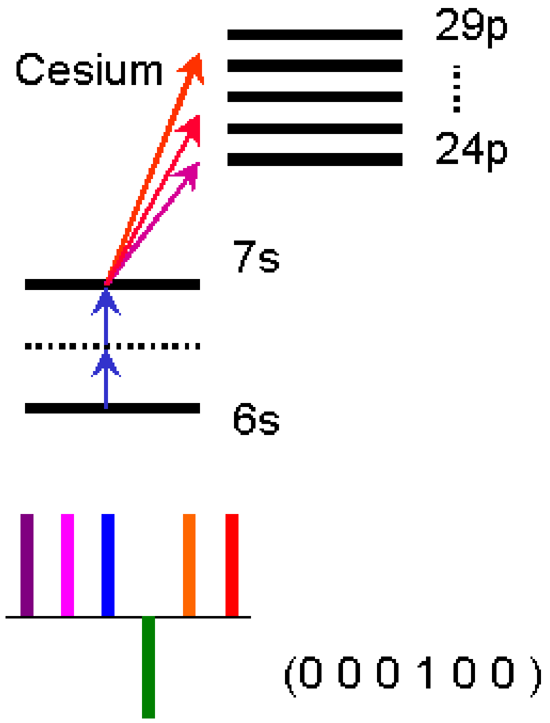
Example: Rydberg atom

http://gomez.physics.lsa.umich.edu/~phil/qcomp.html

Grover's database search algorithm

Data register: Rydberg wave packet

Read-in: phase information

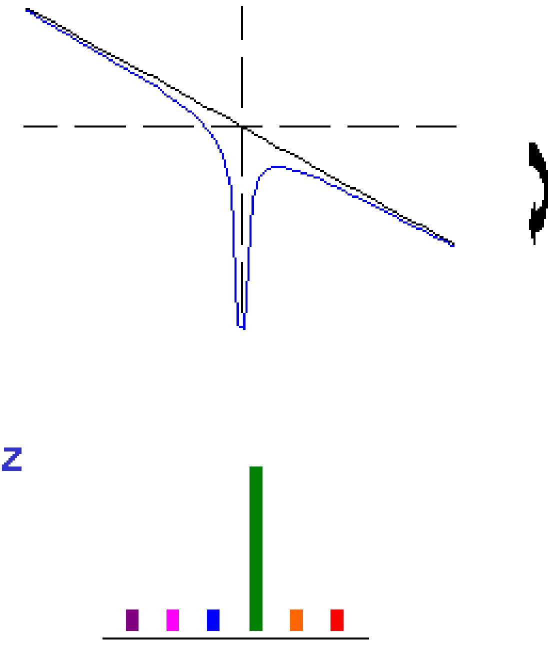


Optical Short Pulse (A)

Decoding pulse

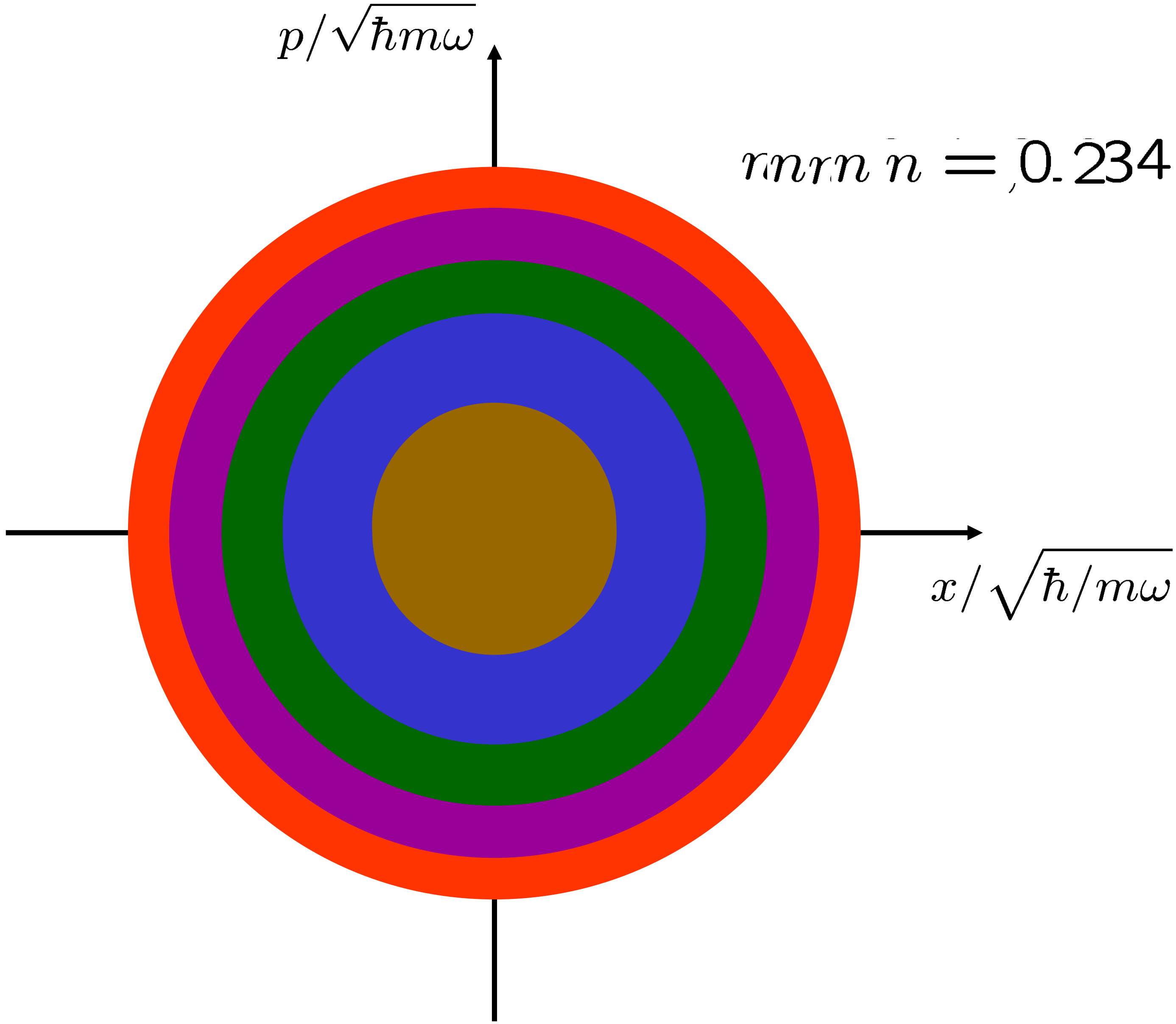
Optical pulse or terahertz Half-cycle Pulse (B)

Read-out: amplitude information

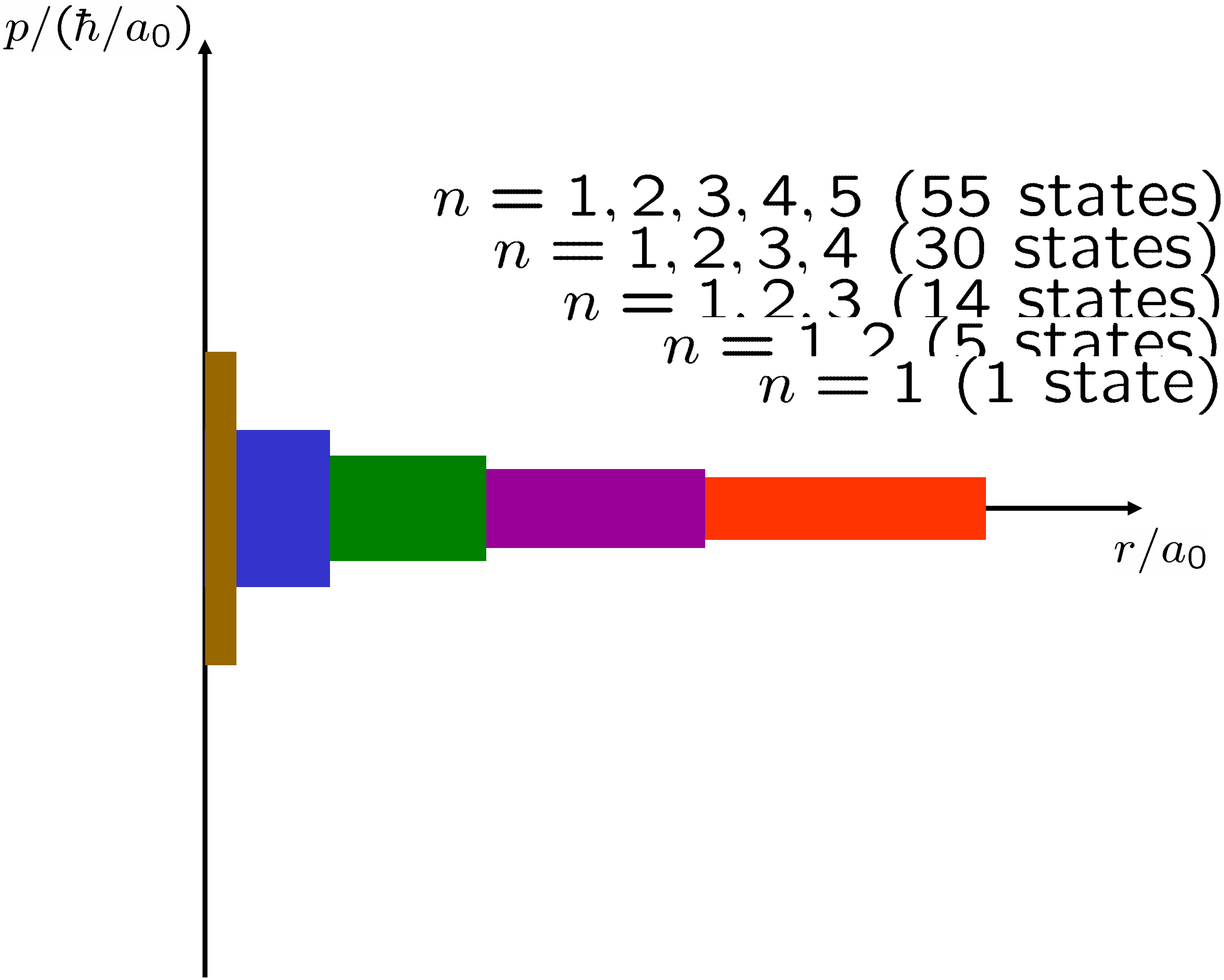


State-selective field ionization signal

Harmonic-oscillator phase space



Single-atom phase space



$n = 1, 2, 3, 4, 5$ (55 states)

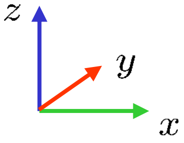
$n = 1, 2, 3, 4$ (30 states)

$n = 1, 2, 3$ (14 states)

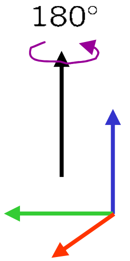
$n = 1, 2$ (5 states)

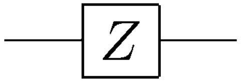
$n = 1$ (1 state)

Single-qubit gates

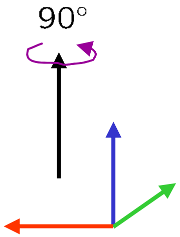


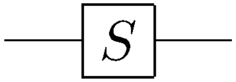
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = S^2$$



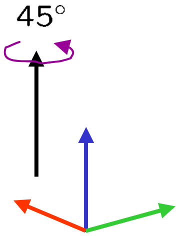


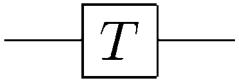
$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = T^2$$



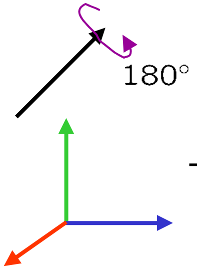


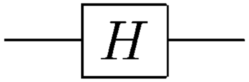
$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$





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





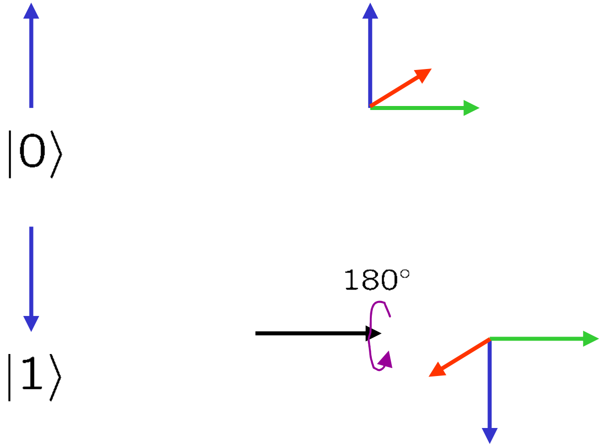
Hadamard

Two-qubit gate

$$\text{C-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

Control **Target**

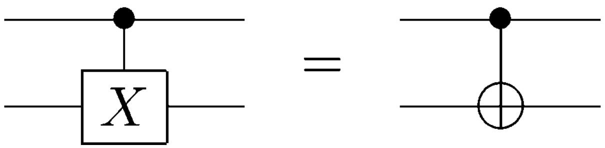


Intro ◀

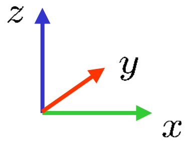
Stabilizer ◀

Control

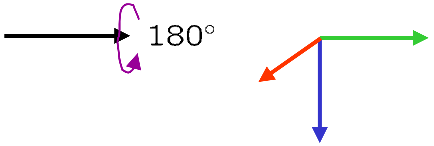
Target



More single-qubit gates

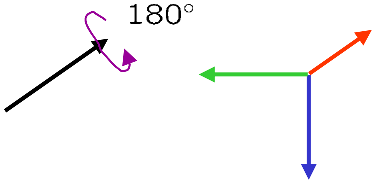


$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = HZH$$



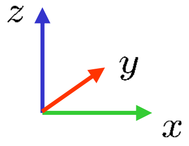
$$\boxed{X} \quad = \quad \boxed{H}\,\boxed{Z}\,\boxed{H}$$

$$iY = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = ZX$$

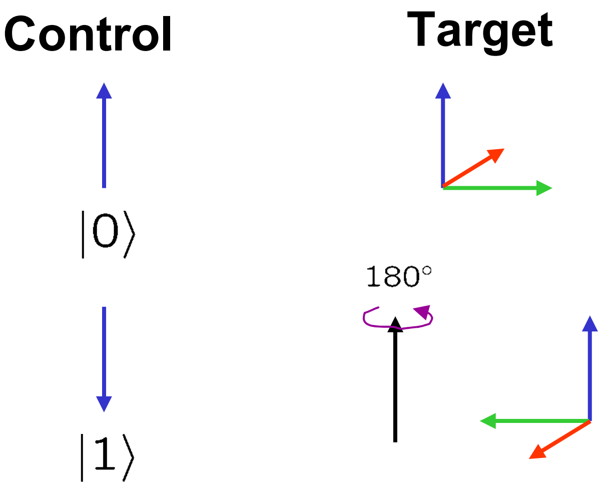


$$\boxed{iY} \quad = \quad \boxed{X}\,\boxed{Z} \quad = \quad \boxed{H}\,\boxed{Z}\,\boxed{H}\,\boxed{Z}$$

Another two-qubit gate



$$\text{C-PHASE} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$



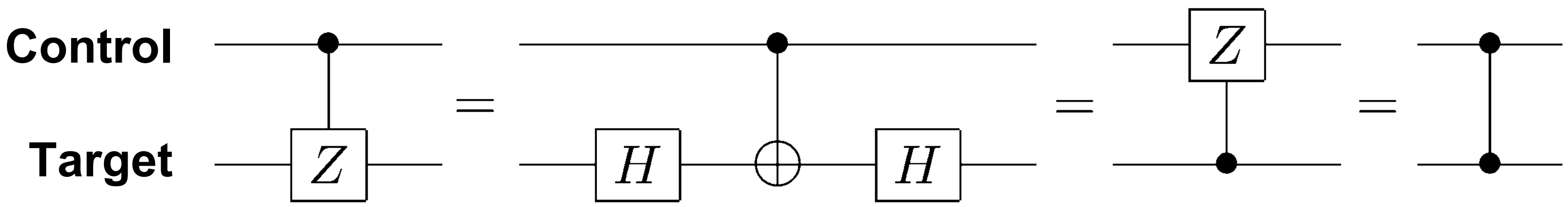
Control

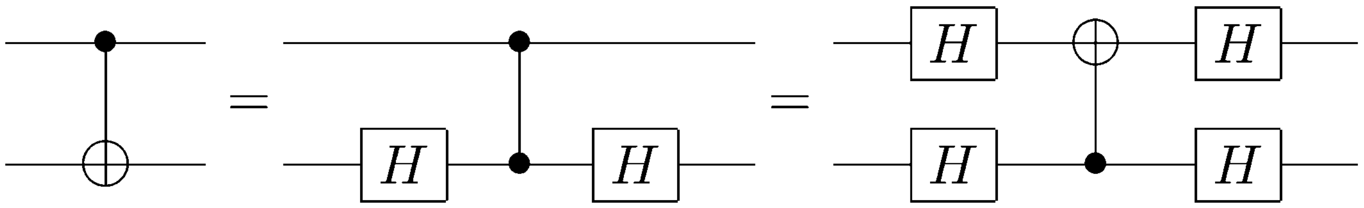
Target

$|0\rangle$

180°

$|1\rangle$





Intro

Stabilizer

Stabilizer formalism. States

$$\begin{aligned}\sigma_0 &= I\\ \sigma_1 &= X\\ \sigma_2 &= Y\\ \sigma_3 &= Z\end{aligned}$$

Pauli group for *N* qubits: $G_N = \left\{ \begin{pmatrix} \pm 1 \\ \pm i \end{pmatrix} \sigma_{\alpha_1} \otimes \cdots \otimes \sigma_{\alpha_N} \right\}$

$$\begin{array}{lcccccc} & g^2 = I & \Leftrightarrow & g = \pm\sigma_{\alpha_1} \otimes \cdots \otimes \sigma_{\alpha_N} & \Leftrightarrow & g = g^\dagger \text{ has eigenvalues } \pm 1 \\ \text{or} & g^2 = -I & \Leftrightarrow & g = \pm i\sigma_{\alpha_1} \otimes \cdots \otimes \sigma_{\alpha_N} & \Leftrightarrow & g = -g^\dagger \end{array}$$

Elements of G_N are unitary and either commute or anticommute.

Stabilizer: $S = \begin{pmatrix} \text{subgroup of } G_N \text{ with } 2^N \\ \text{elements and } -I \notin S \end{pmatrix}$

Elements of S commute, square to I, and if $g \in S$, $-g \notin S$.

State stabilized by S: $g|\psi\rangle = |\psi\rangle$ for all $g \in S$

$$|\psi\rangle\langle\psi| = \frac{1}{2^N} \sum_{g \in S} g$$

Stabilizer formalism. States

Pauli group for *N* qubits: $G_N = \left\{ \begin{pmatrix} \pm 1 \\ \pm i \end{pmatrix} \sigma_{\alpha_1} \otimes \cdots \otimes \sigma_{\alpha_N} \right\}$

Stabilizer: $S = \left(\begin{matrix} \text{subgroup of } G_N \text{ with } 2^N \\ \text{elements and } -I \notin S \end{matrix} \right)$

Stabilized state: $g|\psi\rangle = |\psi\rangle$ for all $g \in S$, $|\psi\rangle\langle\psi| = \frac{1}{2^N} \sum_{g \in S} g$

Examples

1 qubit: $S = \{I, X\}$, $|\psi\rangle\langle\psi| = \frac{1}{2}(I + X)$, $|\psi\rangle = \frac{e^{i\phi}}{\sqrt{2}}(|0\rangle + |1\rangle)$

2 qubits: $S = \{II, XX, ZZ, -YY\}$, $|\psi\rangle\langle\psi| = \frac{1}{4}(II + XX + ZZ - YY)$

$$|\psi\rangle = \frac{e^{i\phi}}{\sqrt{2}}(|00\rangle + |11\rangle)$$

3 qubits:

$$S = \{III, XXX, -XYY, -YXY, -YYX, IZZ, ZIZ, ZZI\}$$

$$|\psi\rangle\langle\psi| = \frac{1}{8}(III + XXX - XYY - YXY - YYX + IZZ + ZIZ + ZZI)$$

$$|\psi\rangle = \frac{e^{i\phi}}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Stabilizer formalism. States

Stabilizer generators: $g_1, \ldots, g_N$

$S = \langle g_1, \ldots, g_N \rangle$: Generators commute, square to I, are independent

Complete set of commuting observables that generate *S*

Stabilized state: $g_j|\psi\rangle = |\psi\rangle,\ j = 1, \ldots, N,\quad |\psi\rangle\langle\psi| = \prod_{j=1}^{N} \frac{1}{2}(I + g_j)$

Examples

1 qubit: $S = \langle X \rangle = \{I, X\}\ ,\quad |\psi\rangle\langle\psi| = \frac{1}{2}(I + X)\ ,$

2 qubits: $S = \langle XX, ZZ \rangle = \{II, XX, ZZ, -YY\}$

$$|\psi\rangle\langle\psi| = \frac{1}{4}(II + XX)(II + ZZ) = \frac{1}{4}(II + XX + ZZ - YY)$$

3 qubits:

$$S = \langle XXX, ZZI, ZIZ \rangle = \{III, XXX, -XYY, -YXY, -YYX, IZZ, ZIZ, ZZI\}$$

$$|\psi\rangle\langle\psi| = \frac{1}{8}(III + XXX)(III + ZZI)(III + ZIZ)$$

$$= \frac{1}{8}(III + XXX - XYY - YXY - YYX + IZZ + ZIZ + ZZI)$$

Stabilizer formalism. States

$$\underbrace{\boxed{g}}_{2N+1 \text{ bits}} = \overbrace{\boxed{\pm}}^{1 \text{ bit}} \underbrace{\boxed{\sigma_{\alpha_1}}}_{2 \text{ bits}} \otimes \cdots \otimes \underbrace{\boxed{\sigma_{\alpha_N}}}_{2 \text{ bits}}$$

N stabilizer generators $\underbrace{\boxed{g_1, \ldots, g_N}}_{N(2N+1) \text{ bits}}$

Efficient realistic, but highly nonlocal description of stabilized state

$$|\psi\rangle\langle\psi| = \prod_{j=1}^{N} \frac{1}{2}(I + g_j)$$

Stabilizer formalism. Dynamics

$$S = \langle g_1, \ldots, g_N \rangle \quad \xrightarrow[U]{} \quad USU^\dagger = \langle U g_1 U^\dagger, \ldots, U g_N U^\dagger \rangle$$

$$(U g_j U^\dagger) U |\psi\rangle = U g_j |\psi\rangle = U|\psi\rangle$$

Normalizer: $\mathcal{N}(G_N) = \{U \mid U G_N U^\dagger = G_N\}$

Single-qubit gates

$U = X$ $\quad UXU^\dagger = X$, $\quad UZU^\dagger = -Z$

$U = Y$ $\quad UXU^\dagger = -X$, $\quad UZU^\dagger = -Z$

$U = Z$ $\quad UXU^\dagger = -X$, $\quad UZU^\dagger = Z$

$\boxed{U = H}$ $\quad UXU^\dagger = Z$, $\quad UZU^\dagger = X$

$\boxed{U = S}$ $\quad UXU^\dagger = Y$, $\quad UZU^\dagger = Z$

$U = T$ $\quad UXU^\dagger = \boxed{\frac{1}{\sqrt{2}}(X + Y)}$, $\quad UZU^\dagger = -Z$

The culprit

Two-qubit gates

$U = \text{C-NOT}$

$$UX \otimes IU^\dagger = X \otimes X$$
$$UI \otimes XU^\dagger = I \otimes X$$
$$UZ \otimes IU^\dagger = Z \otimes I$$
$$UI \otimes ZU^\dagger = Z \otimes Z$$

Normalizer generators

$U = \text{C-PHASE}$

$$UX \otimes IU^\dagger = X \otimes Z$$
$$UI \otimes XU^\dagger = Z \otimes X$$
$$UZ \otimes IU^\dagger = Z \otimes I$$
$$UI \otimes ZU^\dagger = I \otimes Z$$

What's missing from a universal gate set?

Gates

Stabilizer formalism. Dynamics

Single-qubit $U \in \mathcal{N}(G_N)$

- Action of U is described by a rule that requires $\leq 4 \times (1+2) =$ 12 bits

- To update N generators requires N applications of rule

Two-qubit $U \in \mathcal{N}(G_N)$

- Action of U is described by a rule that requires $\leq 16 \times (1+4) =$ 80 bits

- To update N generators requires N applications of rule

Efficient realistic description of dynamics

Stabilizer formalism. Measurements

$$S = \langle \underbrace{g_1\,,\,\ldots\,,\,g_N}_{\text{stabilizer generators}} \rangle \text{ stabilizes } |\psi\rangle$$

Allowed measurements: Products of Pauli operators

Observables $g \in G_N$ such that $g^2 = I$, i.e., $g = \pm\sigma_{\alpha_1} \otimes \cdots \otimes \sigma_{\alpha_N}$

$$g_j g|\psi\rangle = \begin{cases} +gg_j|\psi\rangle = +g|\psi\rangle\,, & \text{if } g \text{ commutes with } g_j \\ -gg_j|\psi\rangle = -g|\psi\rangle\,, & \text{if } g \text{ anticommutes with } g_j \end{cases}$$

$g|\psi\rangle$ is a $\begin{matrix}+1\\-1\end{matrix}$ eigenstate of g_j if it $\begin{matrix}\text{commutes}\\\text{anticommutes}\end{matrix}$ with g_j

Stabilizer formalism. Measurements

$g|\psi\rangle$ is a $\begin{matrix}+1\\-1\end{matrix}$ eigenstate of g_j if it $\begin{matrix}\text{commutes}\\\text{anticommutes}\end{matrix}$ with g_j

- g commutes with all generators $\Rightarrow$ $p_{+1} = 1$ or $p_{-1} = 1$ and post-measurement state is $|\psi\rangle$

  $g|\psi\rangle = \pm|\psi\rangle \Leftrightarrow \pm g \in S \Rightarrow \pm g = g_1^{a_1} \cdots g_N^{a_N}$

  The powers $a_1, \ldots, a_N$ can be determined by solving N linear equations [$O(N^3)$ operations] and then the product $g_1^{a_1} \cdots g_N^{a_N}$ can be computed [$O(N^2)$ operations] to determine which result is predictable.

$O(N^2)$ operations

- g anticommutes with one or more generators (relabel generators so that g anticommutes with $g_1, \ldots, g_l$ and commutes with $g_{l+1}, \ldots, g_N$)

$\Rightarrow \underbrace{p_{+1} = p_{-1} = \frac{1}{2}}_{\text{coin flip}}$ and post-measurement state $\frac{1}{2}(I \pm g)|\psi\rangle$ is stabilized by $g, g_1 g_2, \ldots, g_1 g_l, g_{l+1}, \ldots, g_N$ [computable in $O(N^2)$ operations]

$$\langle\psi|g|\psi\rangle = \langle\psi|g g_1|\psi\rangle = -\langle\psi|g_1 g|\psi\rangle = -\langle\psi|g|\psi\rangle \Rightarrow \langle\psi|g|\psi\rangle = 0$$