On Quantum Computation

Robert Raussendorf

University of British Columbia

TRIUMF Saturday Morning Lecture,

Jan 17, 2009


klassisch
O~exp(n)
quanten-
mechanisch
O~n^x
Problemgröße n

Part I:

The Physics of Computation

Computation and Physics

David Deutsch:

"It is not obvious a priori that any of the familiar recursive functions is in physical reality computable. The reason why we find it possible to construct, say, electronic calculators, and indeed why we can perform mental arithmetic, cannot be found in mathematics or logic. *The reason is that the laws of physics 'happen to' permit the existence of physical models for arithmetic* such as addition, subtraction and multiplication."

D. Deutsch, Proc. Roy. Soc. A **400**, 97 (1985).

The physics of quantum computation

... is Quantum Mechanics, which describes small objects such as atoms, electrons and photons.

Special about Quantum Mechanics:

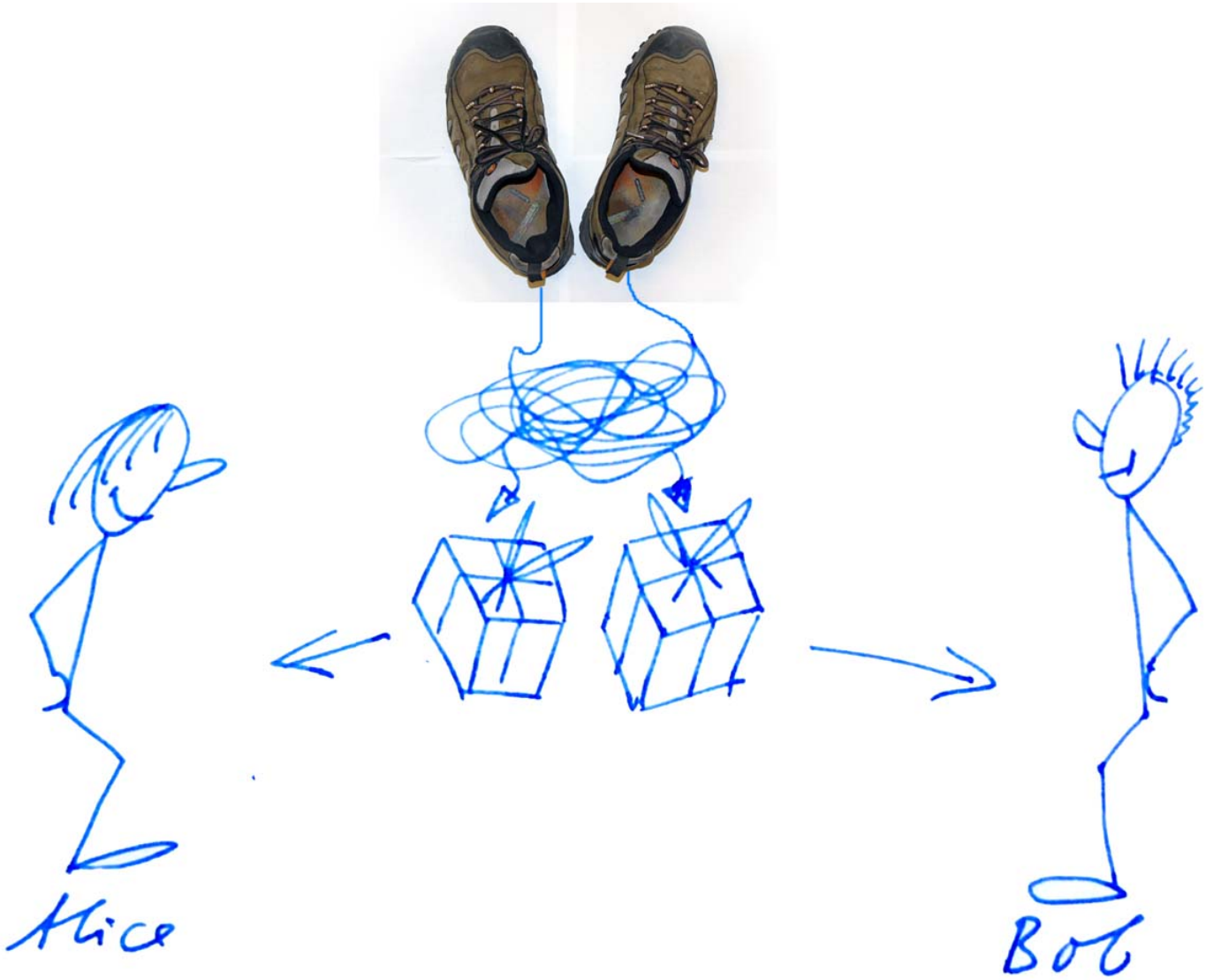
Entanglement • Superposition • Measurement

Entanglement

=

quantum correlation

Classical correlations



Classical correlations

- Alice's shoe randomly left or right.
- Bob holds *other* shoe with certainty.

Shoes held by Alice and Bob random but correlated.

Quantum correlations

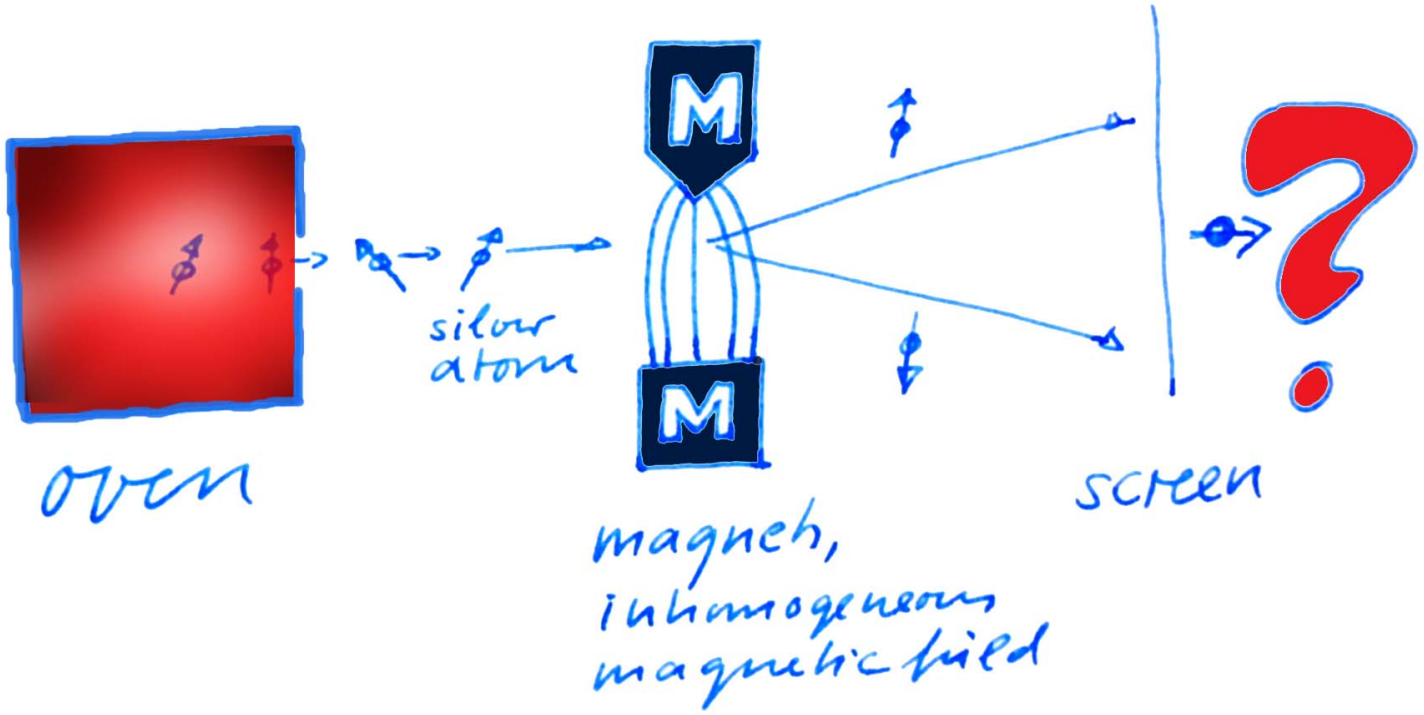
... are stronger than classical ones!

First discuss:

- Superposition
- Measurement

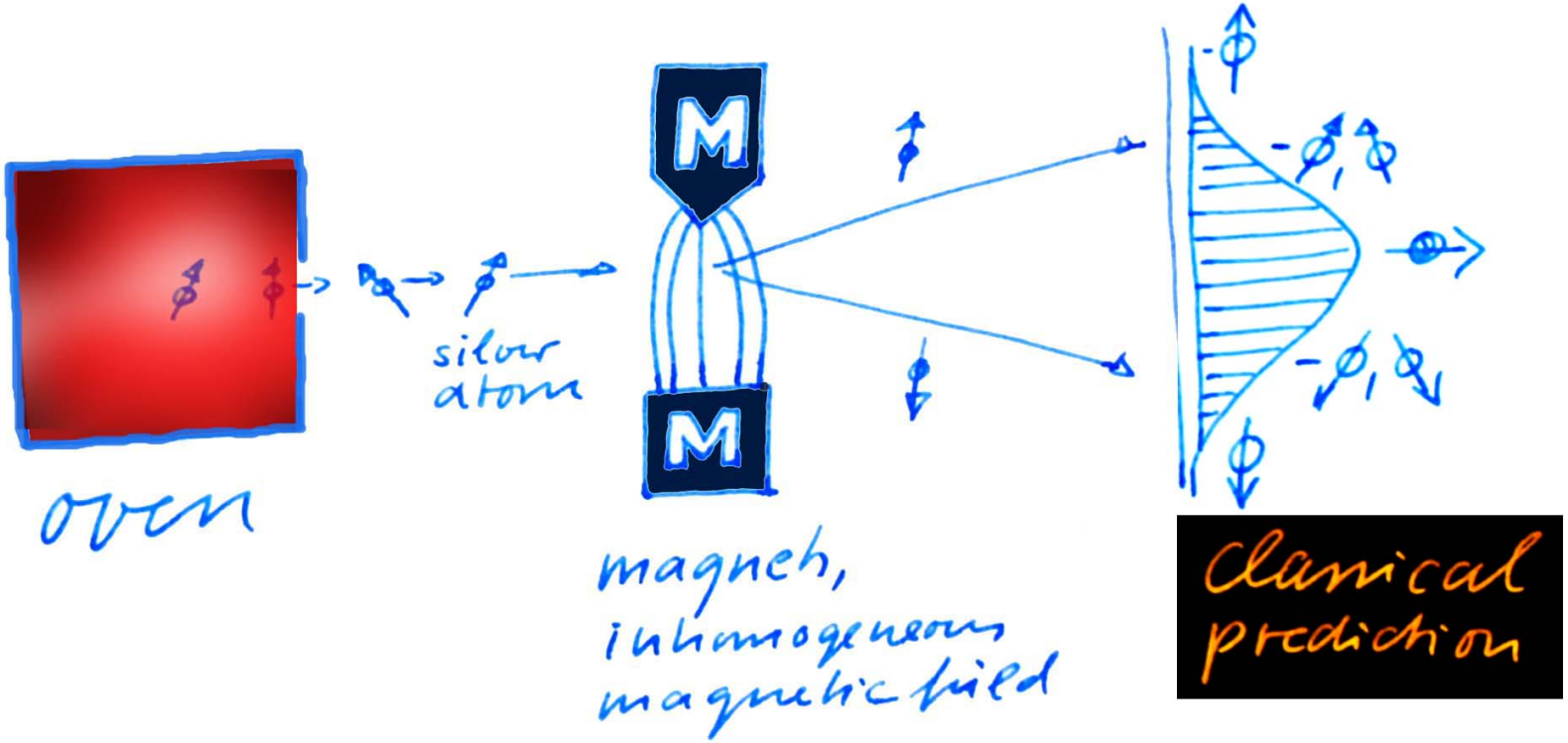
... This leads us to the Stern-Gerlach experiment.

The Stern-Gerlach Experiment

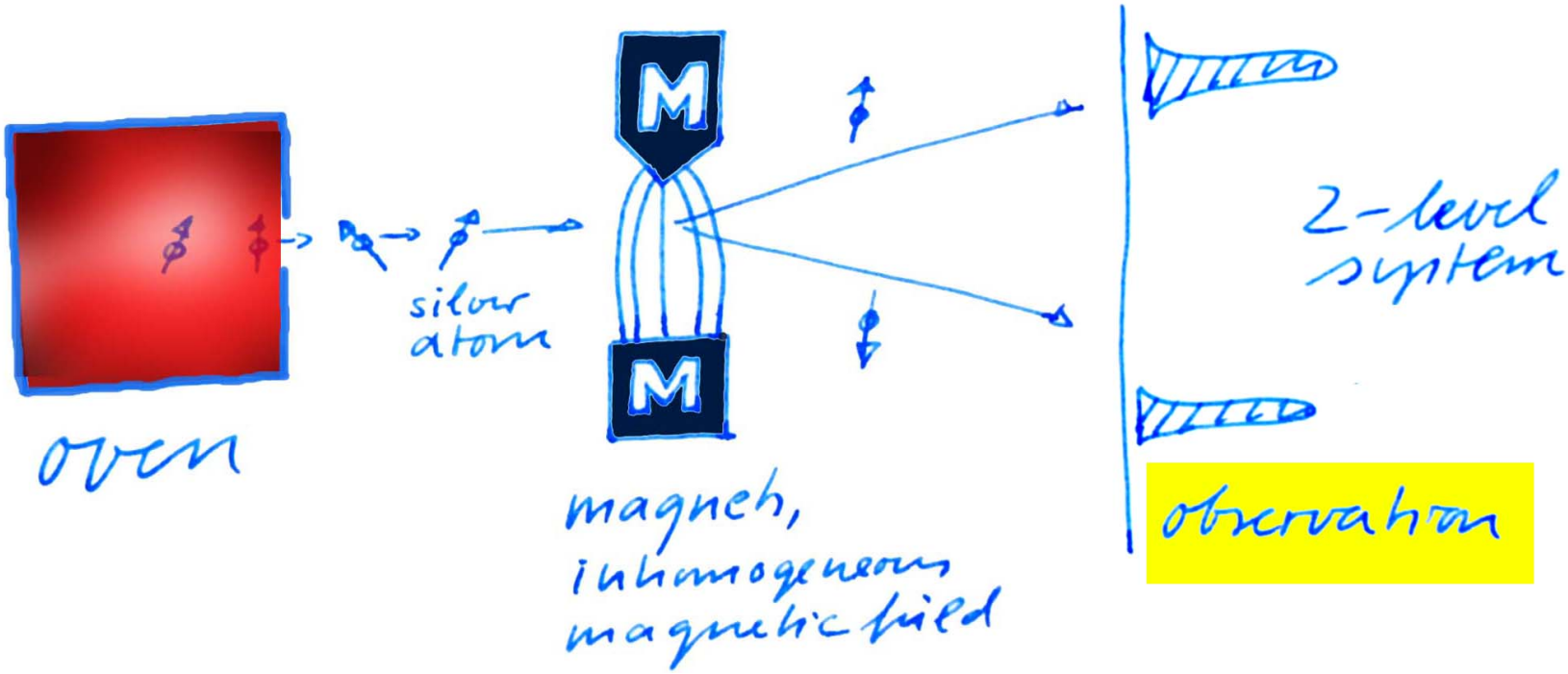


- A silver atom has a "spin" $= \frac{1}{2}\hbar$.
- Spin $\approx$ spinning charge.
- Spin reacts to magnetic field.

The Stern-Gerlach Experiment

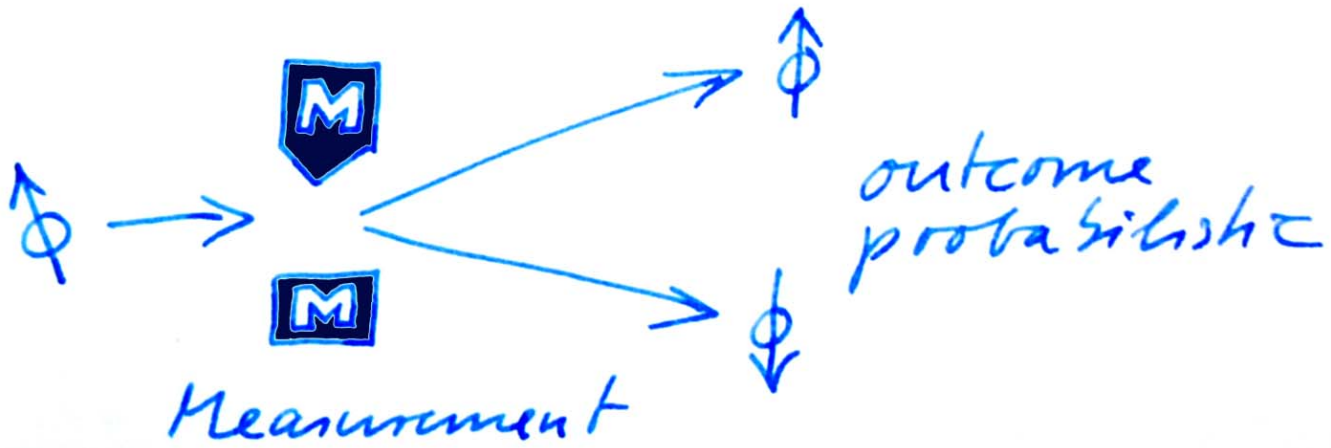


The Stern-Gerlach Experiment

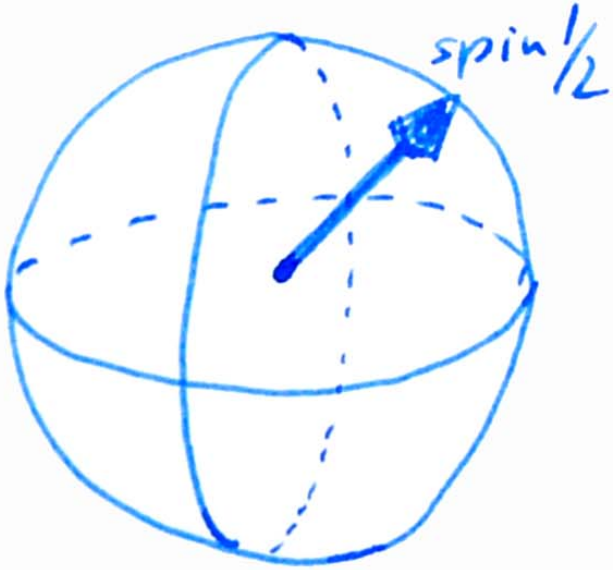


This experiment was performed by O. Stern and W. Gerlach in 1922 in Frankfurt, Germany.

Lesson: Measurement changes the quantum state!



How to represent $|\phi\rangle$ in quantum mechanics?



$$|\phi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$$

superposition state

spin $\frac{1}{2}$ = 2-level system

Entangled states

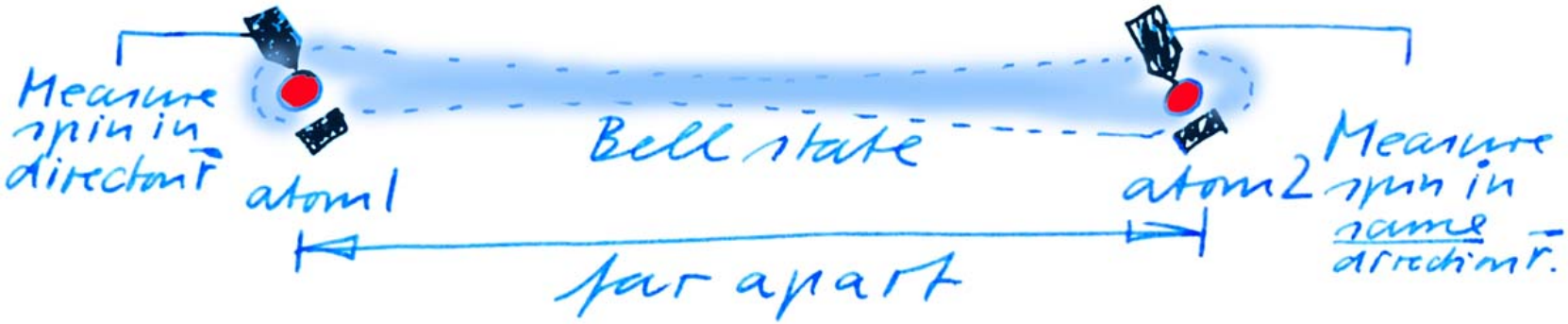
Example: the Bell* state (of two atoms)

$$|\Psi\rangle_{12} = |\uparrow_1 \downarrow_2\rangle - |\downarrow_1 \uparrow_2\rangle$$

- The Bell state is a prototypical entangled state.

*: After John Bell (1928 - 1990).

Properties of the Bell state



- For *any* direction $\vec{r}$, the measurement outcome for spin 1 is completely random, $+\frac{1}{2}\hbar$ or $-\frac{1}{2}\hbar$.
- Whatever the measurement direction, the measurement outcomes on spin 1 and 2 are *always* opposite.

A. Einstein: "Spooky action at a distance".

In quantum information:

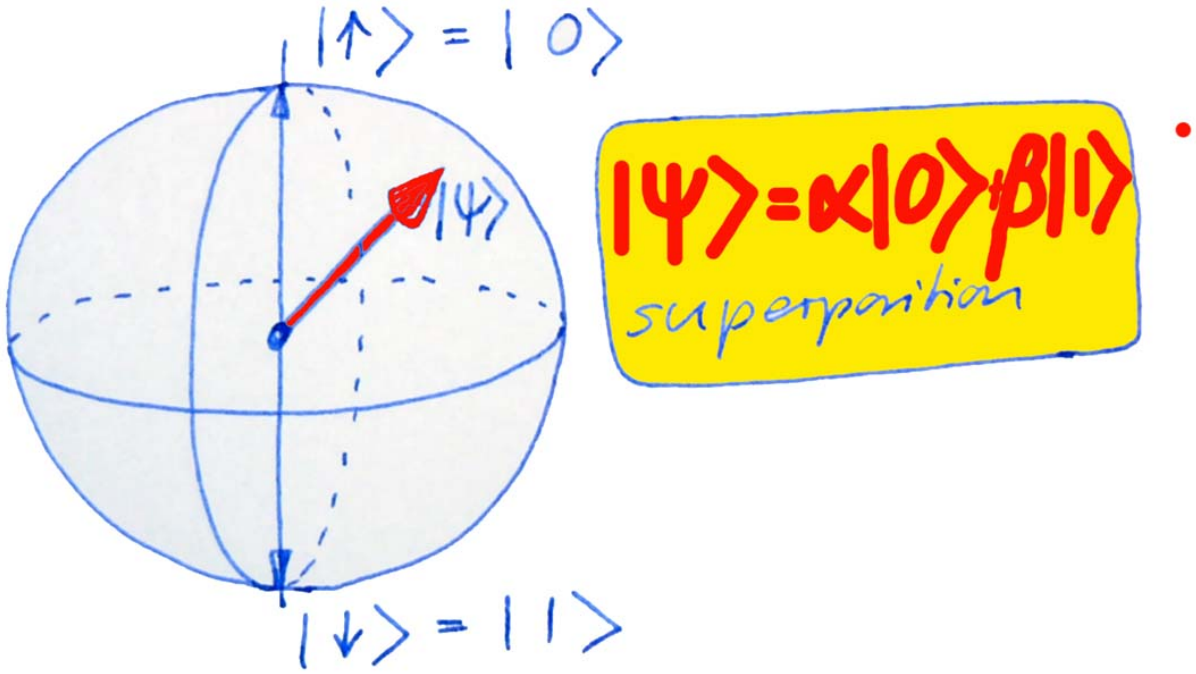
Entanglement is a resource.

It makes quantum computation work.

Part II:

The building blocks of quantum computation

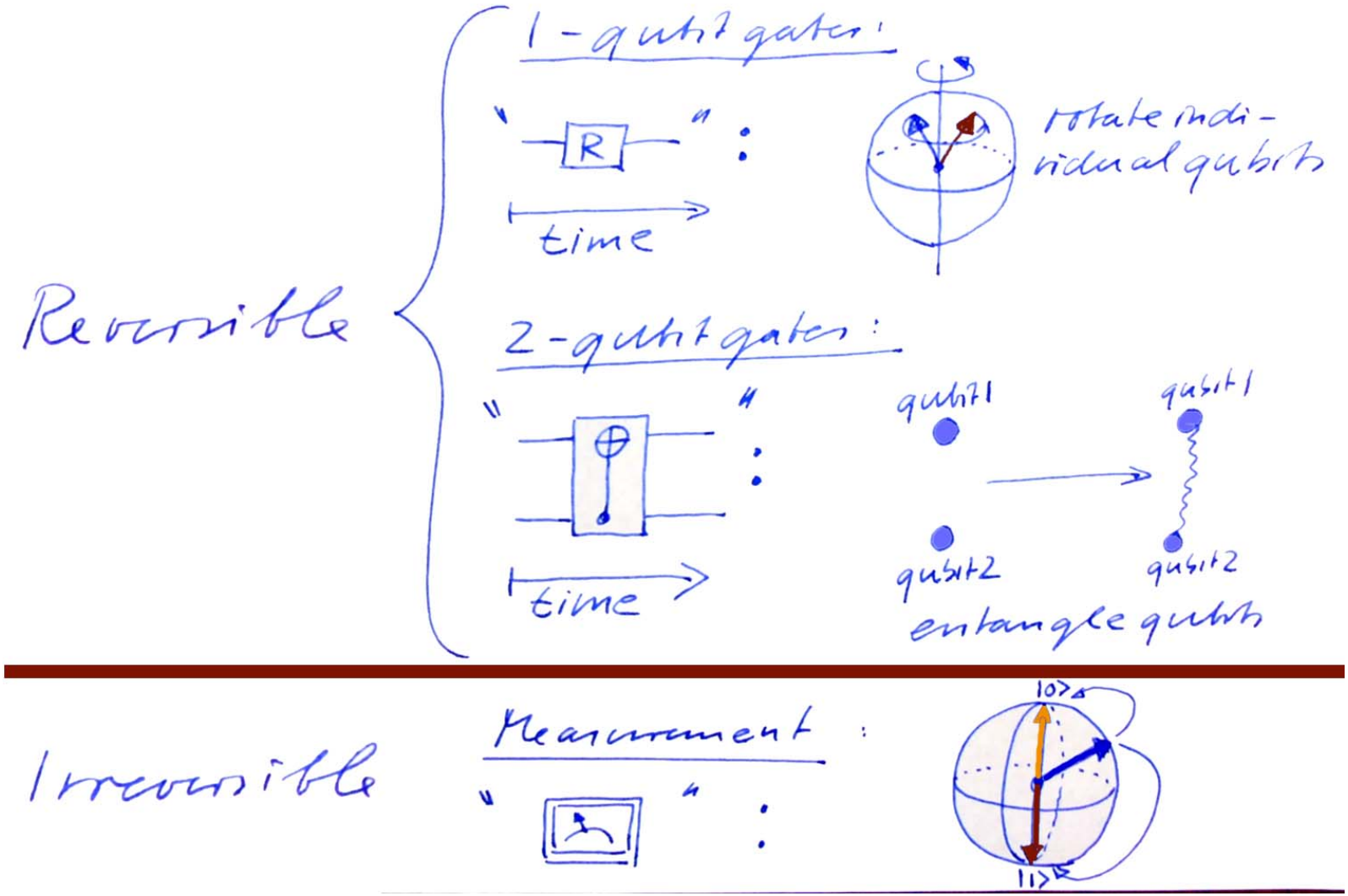
Unit of quantum information: the qubit

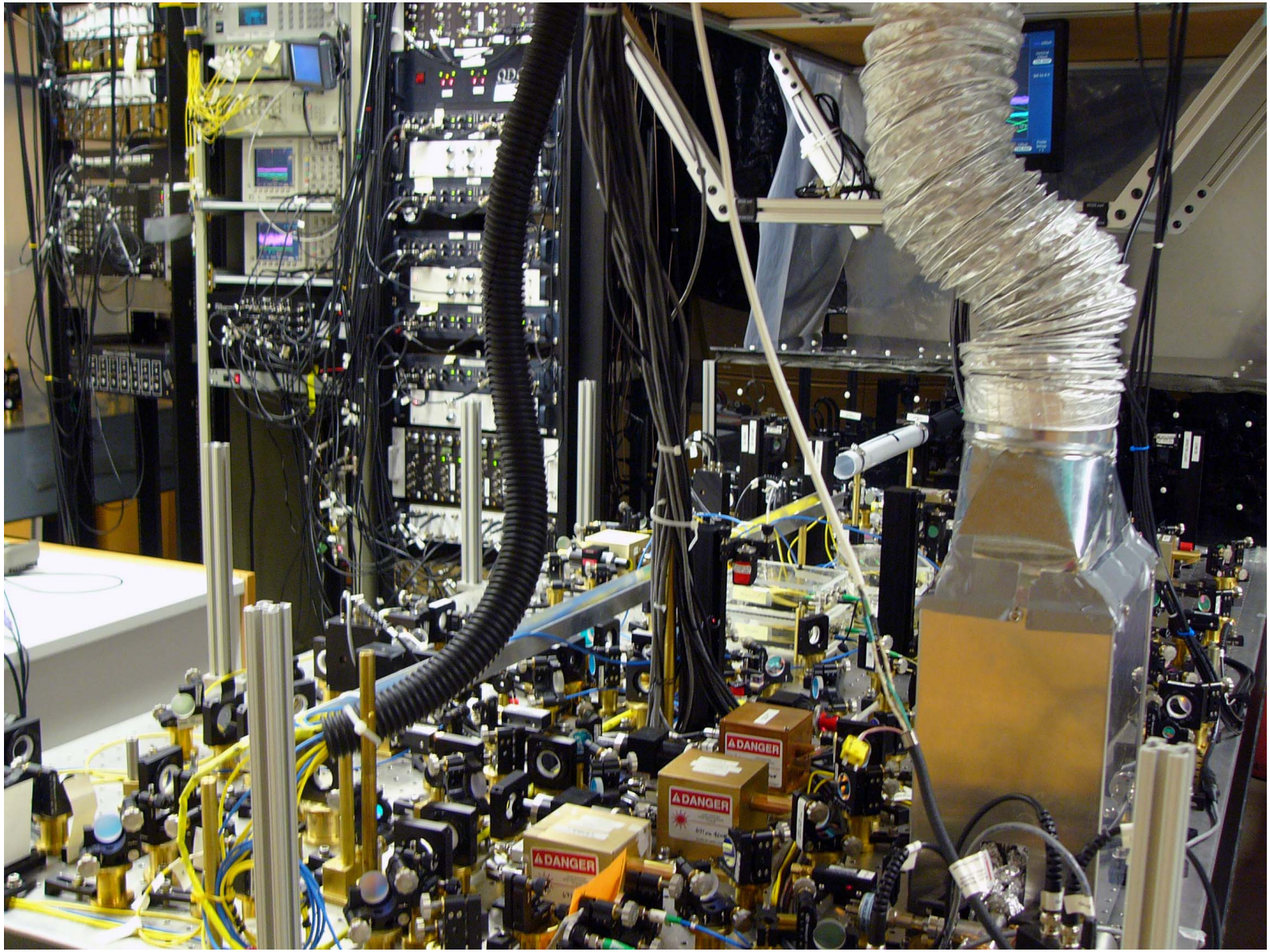


Qubit inherits

- Logical states "**0**" and "**1**" from classical bit,
- Superposition from quantum mechanics.

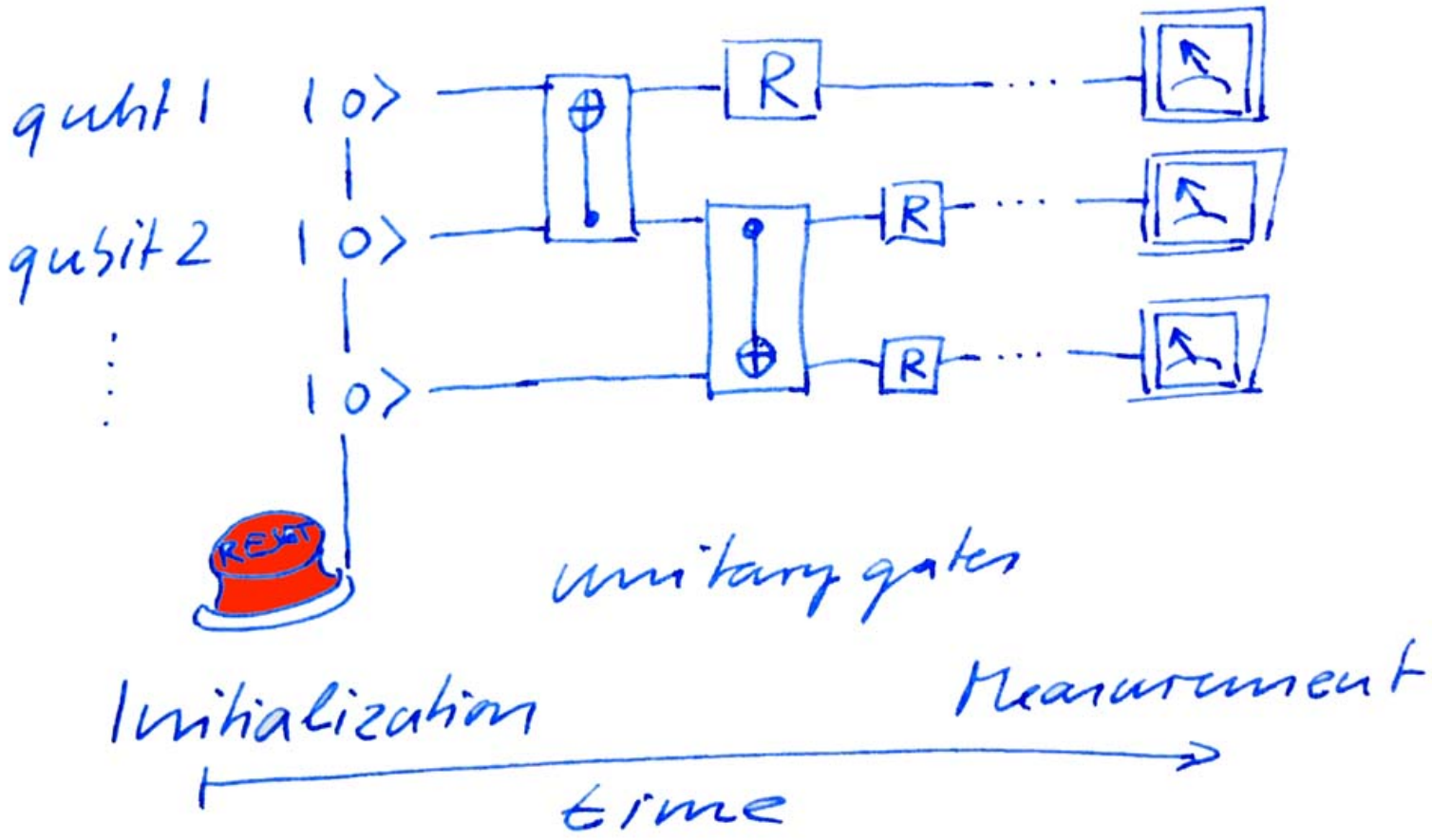
Unit of quantum processing: the quantum gate





Kirk Madison's lab @ UBC.

Quantum circuits



Part III:

Shor's algorithm

Shor's factoring algorithm

What it does:

Given an integer number q,

$$q \;=\; m \times n,$$

Returns m, n.

Shor's factoring algorithm

Why care?

- Shor's algorithm breaks the RSA crypto-system

Shor's factoring algorithm

How can that be?

- Multiplication of two numbers $m, n \longrightarrow q = m \times n$ is simple.
- The reverse operation, i.e. computing the prime factors m, n of $q = m \times n$ is *hard* for classical computation,

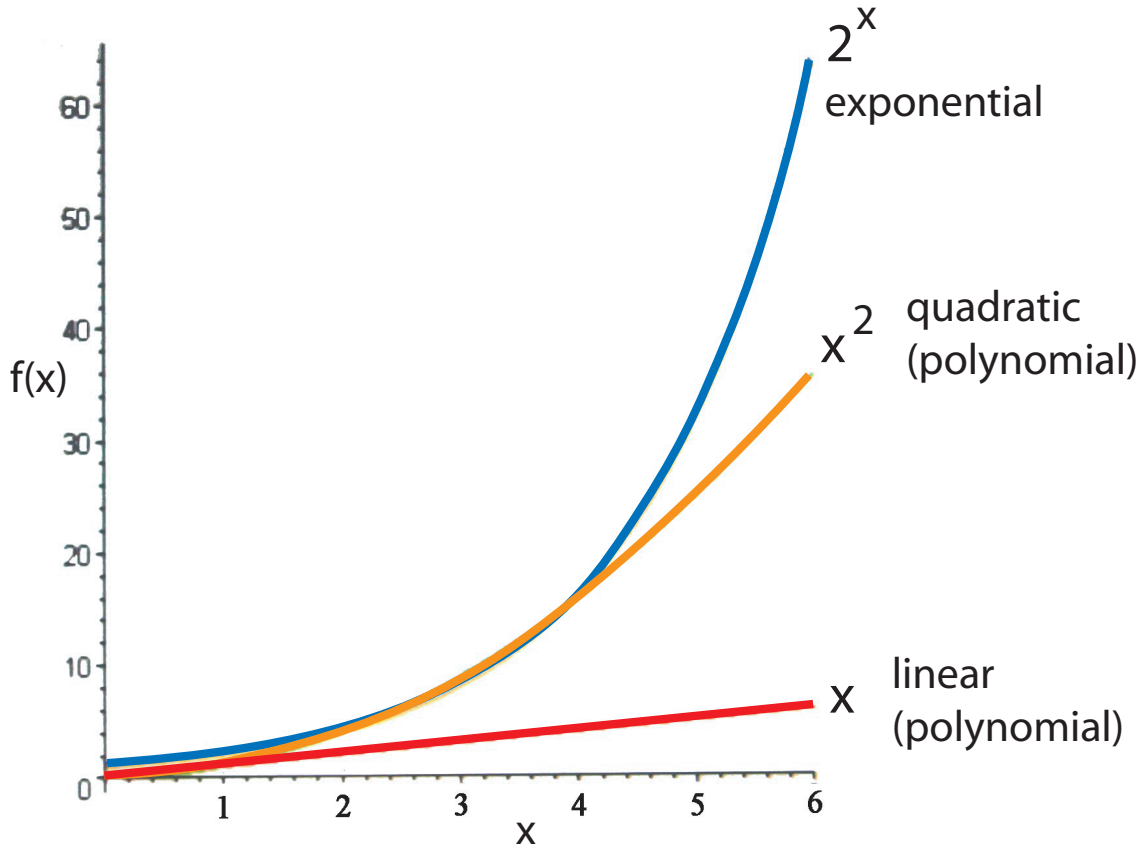
$$\text{runtime}_{classical} = \underbrace{2^{\#\text{digits of } q}}_{exponential}. \tag{1}$$

- On a quantum computer, computing the prime factors m, n of $q = m \times n$ again is simple,

$$\text{runtime}_{quantum} = \underbrace{(\#\text{digits of } q)^2}_{polynomial}. \tag{2}$$

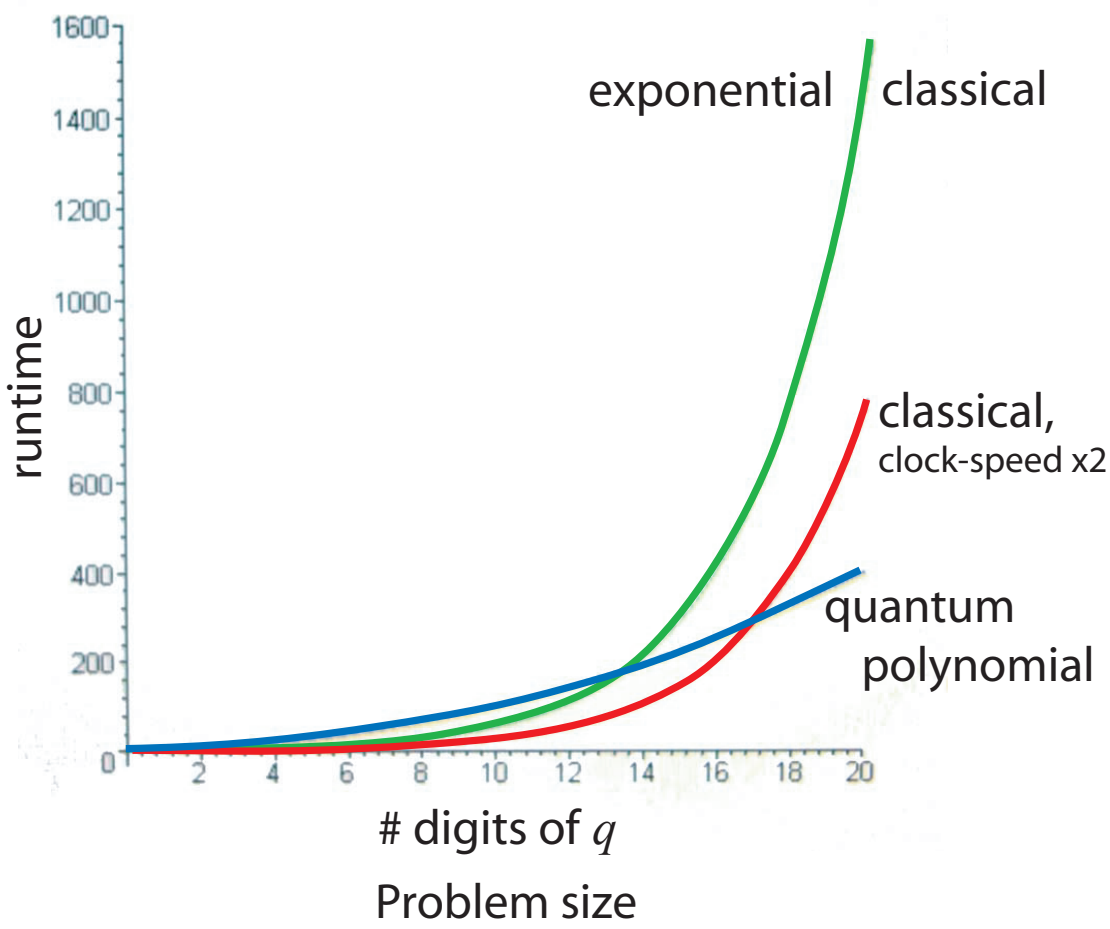
‘Polynomial’ vs. ‘Exponential’

$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$
$2^7 = 128$
$2^8 = 256$
$2^9 = 512$
$2^{10} = 1024$
$2^{20} = 1048576$
$2^{30} = 1073741824$
$2^{40} = 1099511627776$



- An exponential function increases faster than *any* polynomial function.

Scaling of computation time



- The quantum speedup is not a matter of clock-speed, its a matter of *scaling*.

Constructing quantum algorithms

Richard Feynman:

> *"One feels like Cavalieri must have felt calculating the volume of a pyramid before the invention of calculus."*

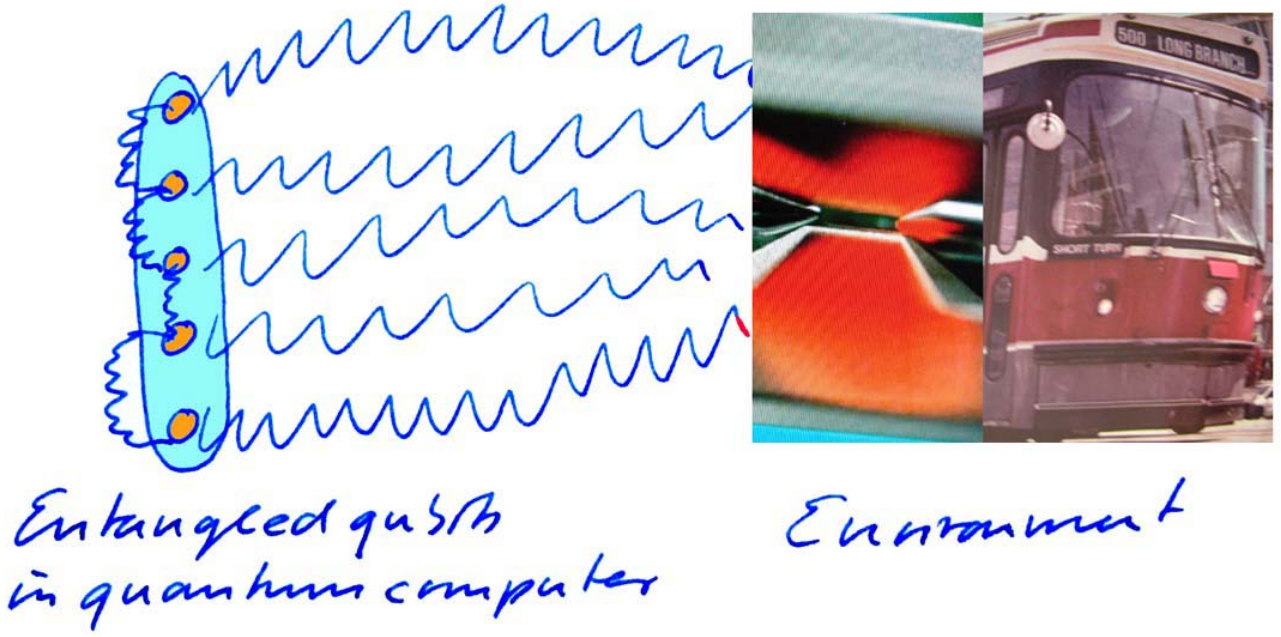
R.P. Feynman, on developing the path integral formalism, taken from: M. Kaku, Quantum Field Theory, Oxford University Press (1993).

Part IV:

Quantum computation and the real world

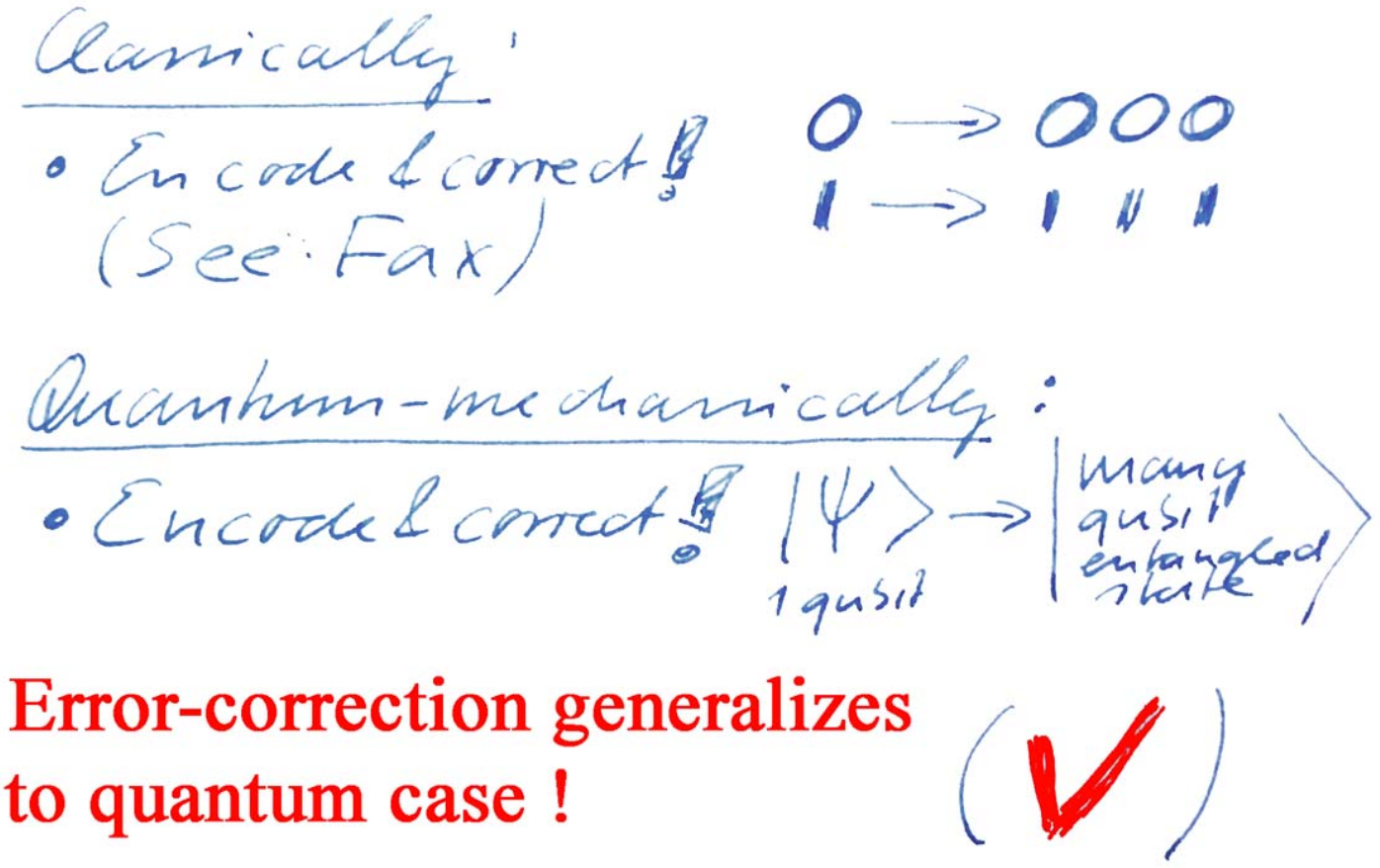
Decoherence • Experiments

Entanglement - friend and foe



- Unavoidably, the quantum computer becomes entangled with its environment.
- Leads to 'quantum noise' = decoherence
- Decoherence disturbs quantum computation.

To protect against noise ...



Error-correction generalizes to quantum case ! ✓

Experiment

Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance

Lieven M. K. Vandersypen*†, Matthias Steffen*†, Gregory Breyta*, Costantino S. Yannoni*, Mark H. Sherwood* & Isaac L. Chuang*†

* *IBM Almaden Research Center, San Jose, California 95120, USA*
† *Solid State and Photonics Laboratory, Stanford University, Stanford, California 94305-4075, USA*

Factored: $15 = 5 \times 3$.

L. Vandersypen et *al.*, Nature **414**, 883 (2001).

F.C. Williams on the first successful run of the 'baby' in 1948:

*"A program was laboriously inserted and the start switch pressed. Immediately the spots on the display tube entered a mad dance. In early trials it was a dance of death leading to no useful result, and what was even worse, without yielding any clue as to what was wrong. But one day it stopped, and there, shining brightly in the expected place, was the expected answer. It was a moment to remember. This was in June 1948, and nothing was ever the same again."**

... a long way to go for quantum computation

*: taken from http://www.computer50.org/mark1/new.baby.html