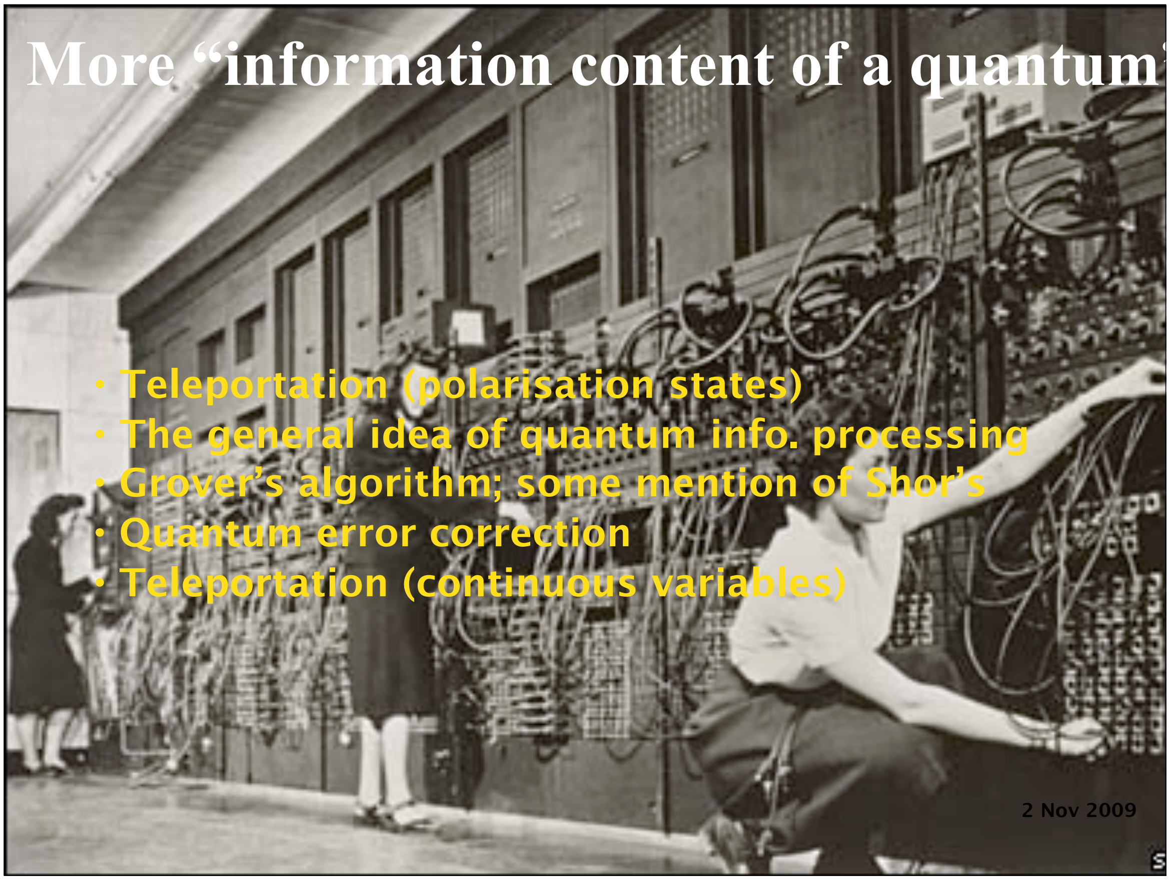
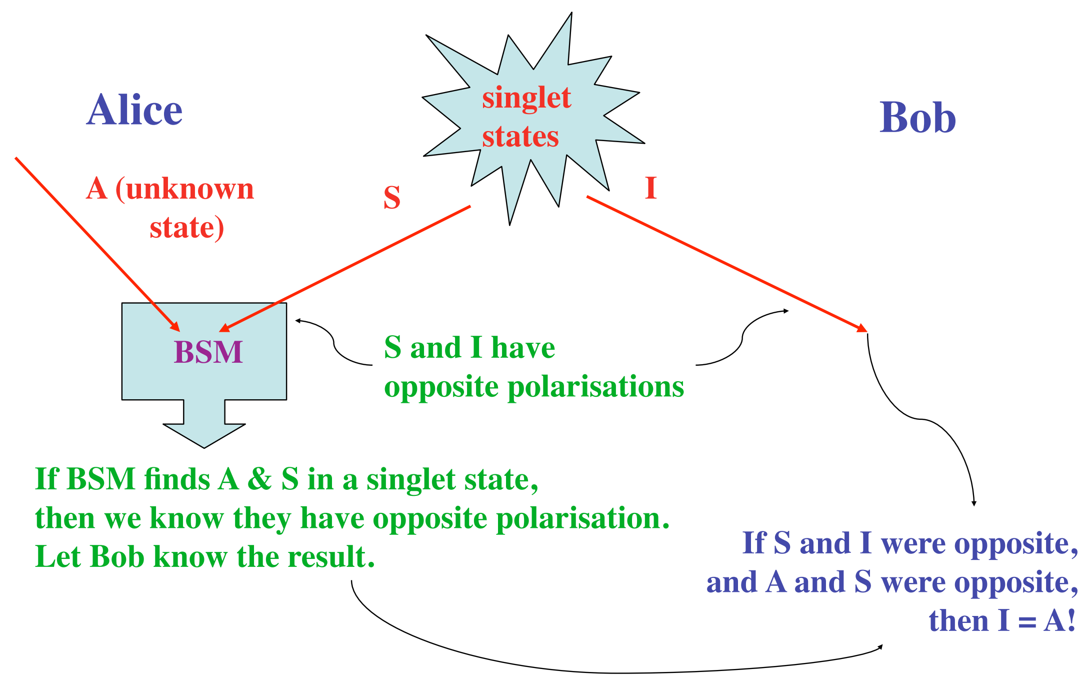


Quantum Teleportation

Bennett *et al*., Phys. Rev. Lett. 70, 1895 (1993)



(And the other three results just leave Bob with a unitary operation to do)

Teleportation as projections

$$|\psi_A\rangle = a|H\rangle + b|V\rangle$$

$$|\psi_{SI}\rangle = |HV\rangle - |VH\rangle$$

$$|\psi\rangle_{ASI} = a|HHV\rangle \underline{+b|VHV\rangle} - \underline{a|HVH\rangle} - b|VVH\rangle$$

$$\{\langle HV|_{AS} - \langle VH|_{AS}\}|\psi\rangle = -a|H\rangle - b|V\rangle \sim |\psi_A\rangle_i$$

$$\{\langle HV| + \langle VH|\}|\psi\rangle = -a|H\rangle + b|V\rangle \sim \sigma_z|\psi_A\rangle_i$$

Teleportation as projections

$$|\psi_A\rangle = a|H\rangle + b|V\rangle$$

$$|\psi_{SI}\rangle = |HV\rangle - |VH\rangle$$

$$|\psi\rangle_{ASI} = \underline{a|HHV\rangle} + b|VHV\rangle - a|HVH\rangle \underline{-b|VVH\rangle}$$

$$\{\langle HV|_{AS} - \langle VH|_{AS}\}|\psi\rangle = -a|H\rangle - b|V\rangle \sim |\psi_A\rangle_i$$

$$\{\langle HV| + \langle VH|\}|\psi\rangle = -a|H\rangle + b|V\rangle \sim \sigma_z|\psi_A\rangle_i$$

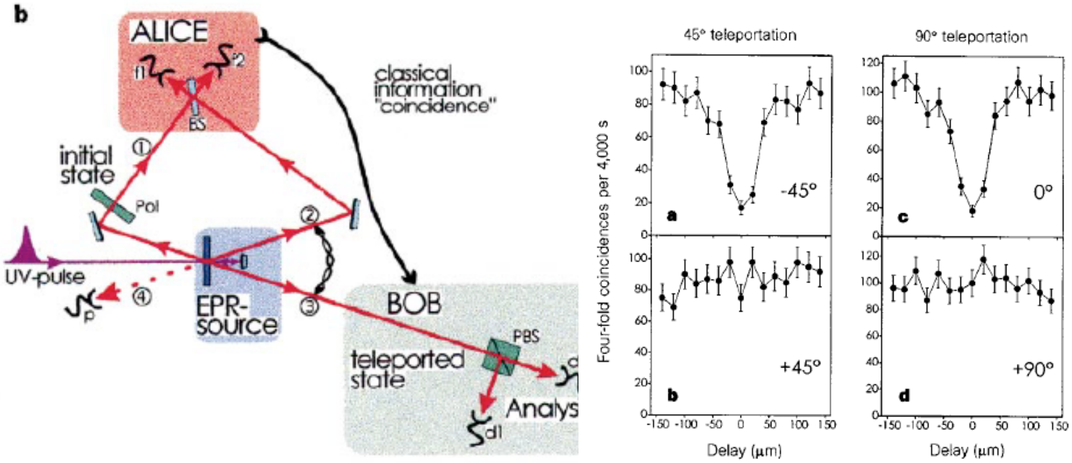
$$\{\langle HH| - \langle VV|\}|\psi\rangle = a|V\rangle + b|H\rangle \sim \sigma_x|\psi_A\rangle_i$$

$$\{\langle HH| + \langle VV|\}|\psi\rangle = a|V\rangle - b|H\rangle$$

$$\sim \sigma_z\sigma_x|\psi_A\rangle_i$$

$$\sim \sigma_y|\psi_A\rangle_i$$

Quantum Teleportation (expt)



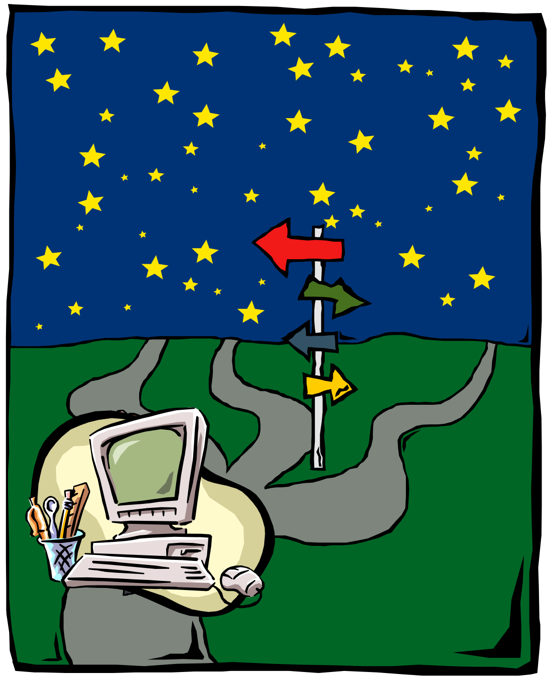
Bouwmeester *et al*., Nature 390, 575 (1997)

One striking aspect of teleportation

- **Alice's photon and Bob's have no initial relationship – Bob's could be in any of an infinite positions on the Poincaré sphere.**
- **The Bell-state measurement collapses photon S (and hence Bob's photon I) into one of four particular states – states with well-defined relationships to Alice's initial photon.**
- **Thus this measurement transforms a continuous, infinite range of possibilities (which we couldn't detect, let alone communicate to Bob) into a small discrete set.**
- ***All* possible states can be teleported, by projecting the continuum onto this complete set.**

Quantum Information

What's so great about it?



What makes a computer quantum?

(One partial answer...)

If a quantum "bit" is described by two numbers:

$$|\Psi\rangle = c_0|0\rangle + c_1|1\rangle,$$

then n quantum bits are described by 2^n coeff's:

$$|\Psi\rangle = c_{00..0}|00..0\rangle + c_{00..1}|00..1\rangle + ... c_{11..1}|11..1\rangle;$$

this is exponentially more information than the 2n coefficients it would take to describe n independent (e.g., classical) bits.

Quantum Information

What's so great about it?

If a classical computer takes input |n> to output |f(n)>, an analogous quantum computer takes a state |n>|0> and maps it to |n>|f(n)> (unitary, reversible).

By superposition, such a computer takes Σ_n |n>|0> to Σ_n |n>|f(n)>; it calculates f(n) for every possible input simultaneously.

A clever measurement may determine some global property of f(n) even though the computer has only run once...

A not-clever measurement "collapses" n to some random value, and yields f(that value).

The rub: any interaction with the environment leads to "decoherence," which can be thought of as continual unintentional measurement of n.

One simple example of a quantum speedup...

dj

Page 5 of 6 - Nov 29,

Grover's search

Suppose $U|i\rangle = \begin{cases} -|i\rangle & \text{if } i=n \\ |i\rangle & \text{if } i\neq n \end{cases}$

n is some "marked element"

How many runs to tell which i is marked?

If i runs $1 \to N$, then $\frac{N}{2}$ on average.

(Like searching a phone book in reverse)

Suppose $N=4$ and we input $|\psi_{in}\rangle = \sum_{i=1}^{4} \frac{1}{2}|i\rangle$

Phase-flip the state $|\psi_{in}\rangle$:

$$U = I - 2|\psi_{in}\rangle\langle\psi_{in}|$$

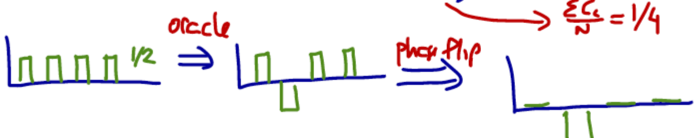
st $|\psi_{in}\rangle \to -|\psi_{in}\rangle$

any $|\psi_{orth}\rangle \to +|\psi_{orth}\rangle$

$$U\sum c_M|M\rangle = \sum_M c_M|M\rangle - 2\frac{\sum_i|i\rangle}{\sqrt{N}}\frac{\sum_j\langle j|}{\sqrt{N}}\sum c_M|M\rangle$$

$$= \sum_M c_M|M\rangle - \left(2\sum \frac{c_M}{\sqrt{N}}\right)\sum_i \frac{|i\rangle}{\sqrt{N}}$$

$$= \sum_M \left(c_M - 2\frac{\sum c_i}{N}\right)|M\rangle \longrightarrow \frac{\sum c_i}{N} = 1/4$$



Measure *i*, and Bob's your uncle! A single trial.
More general, sqrt{N} trials to search N elements... still pretty cool.

Shor's algorithm: factor products of primes in poly time (break RSA?) -> $$$

Quantum Error Correction

In classical computers, small errors are continuously corrected – built-in dissipation pulls everything back towards a "1" or a "0".

Recall that quantum computers must avoid dissipation and irreversibility.

How, then, can errors be avoided?

> **A bit could be anywhere on the Poincaré sphere – and an error could in principle move it anywhere else. Can we use measurement to reduce the error symptoms to a discrete set, à la teleportation?**

Yes: if you measure whether or not a bit flipped, you get either a "YES" or a "NO", and can correct it in the case of "YES".
As in dense coding, the phase degree of freedom is also important, but you can similary measure whether or not the phase was flipped, and then correct that.
Any possible error can be collapsed onto a "YES" or "NO" for each of these.

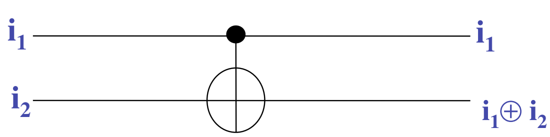
The four linearly independent errors

Identity	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$I\|a\rangle = \|a\rangle$
Bit Flip	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$X\|a\rangle = \|a \oplus 1\rangle$
Phase Flip	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$Z\|a\rangle = (-1)^a\|a\rangle$
Bit & Phase	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = iXZ$	$Y\|a\rangle = i(-1)^a\|a \oplus 1\rangle$

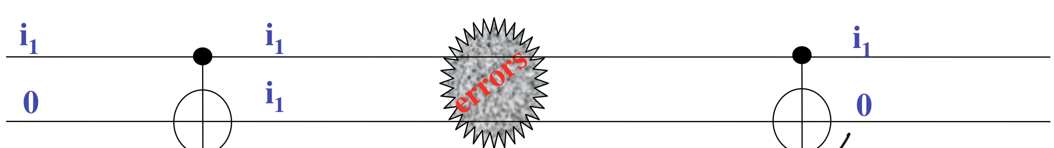
TABLE 1. The Pauli matrices

Encoding & decoding

Notation - the controlled NOT (CNOT):



In (ct)	Out (ct)
00	00
01	01
10	11
11	10



$(a|0\rangle + b|1\rangle)|0\rangle$ $a|00\rangle + b|11\rangle$ $(a|0\rangle + b|1\rangle)|0\rangle$

or 1 if one of the bits flipped!

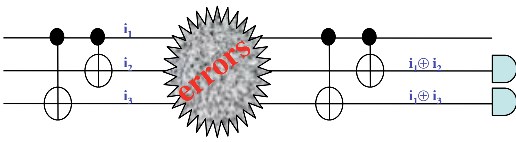
Error *detection*!

Q. error correction: Shor's 3-bit code

In case of bit flips, use redundancy – it's unlikely that more than 1 bit will flip at once, so we can use "majority rule"...

BUT: we must not actually measure the value of the bits!

Encode: a|0> + b|1> ⇒ a|000> + b|111>



Symptom	State	$i_1 \oplus i_2$	$i_1 \oplus i_3$
Nothing happens	a|000> + b|111>	0	0
i_1 flips	a|100> + b|011>	1	1
i_2 flips	a|010> + b|101>	1	0
i_3 flips	a|001> + b|110>	0	1

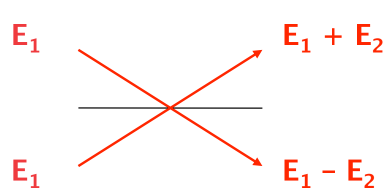
And now just flip i_1 back if you found that it was flipped – note that when you measure which of these four error syndromes occurred, you exhaust all the information in the two extra bits, and no record is left of the value of i_1!

NOTE: you could have phase errors as well as bit flips; more copies required.

How to measure the continuous analog of Bell states ?

We wish to learn about the “relative” state of two systems,

without measuring the exact state of either...



$X_1 + X_2$;

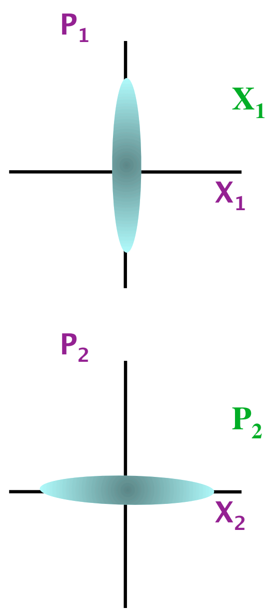
$P_1 + P_2$

$X_1 – X_2$;

$P_1 – P_2$

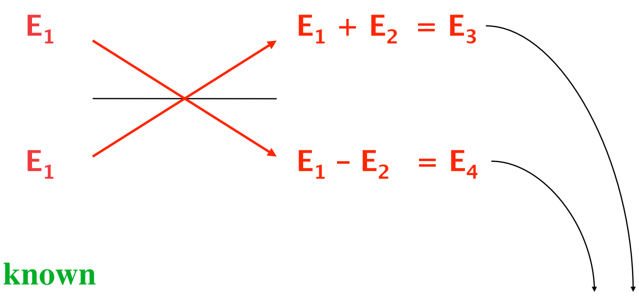
Do homodyne measurement on the outcomes, to measure differences or sums of the chosen quadratures.
(At best, one difference and one sum.)

How to generate the continuous analog of Bell pairs?



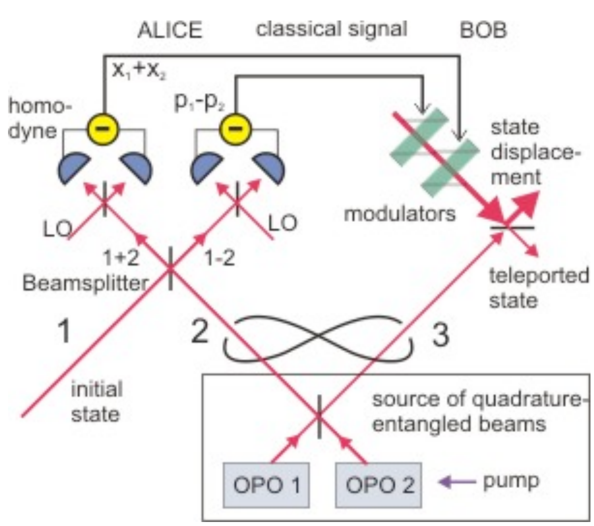
X_1 is well known

P_2 is well known



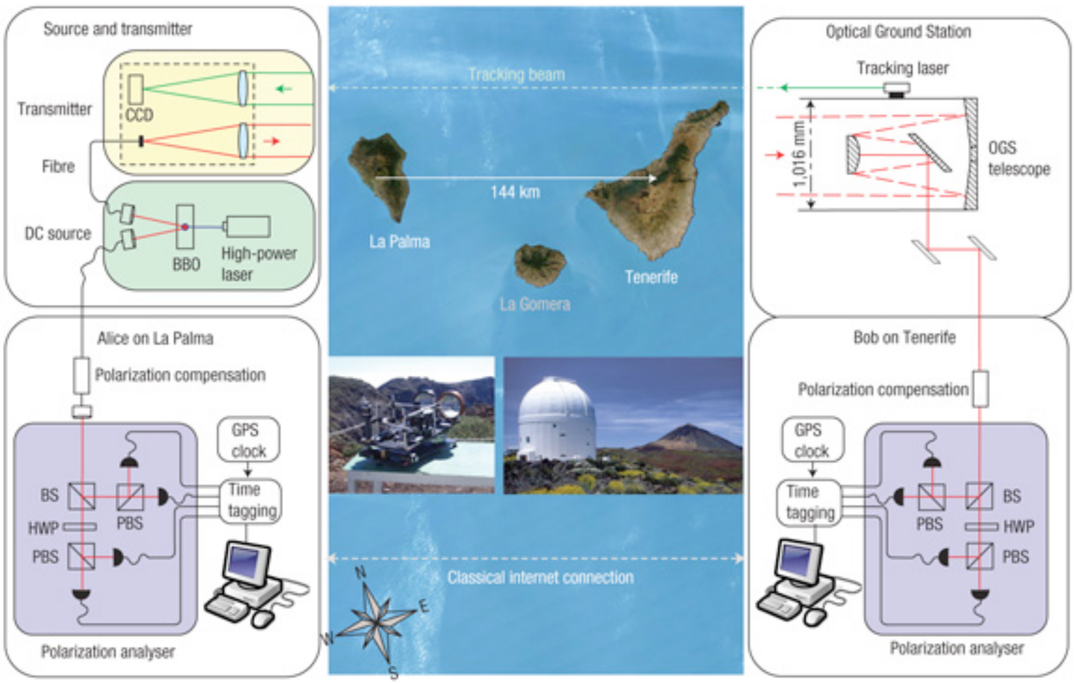
$X_3 + X_4 = X_1$ is well known.
$P_3 - P_4 = P_2$ is well known.

Continuous-variable teleportation



"Unconditional quantum teleportation," A. Furusawa, J. Sorensen, S. L. Braunstein, C. Fuchs, H. J. Kimble, and E. S. Polzik, Science **282**, 706 (1998).

A good excuse for a junket! (light teleported over 144 km)



Some more references (incomplete!)

Dense coding and teleportation:
Bennett & Wiesner, PRL 69, 2881 (1992)
Mattle et al., PRL 76, 4656 (1996)
Benett et al., PRL 70, 1895 (1993)
Bouwmeester et al., Nature 390, 575 (1997)
Furusawa et al., Science 282, 706 (1998)

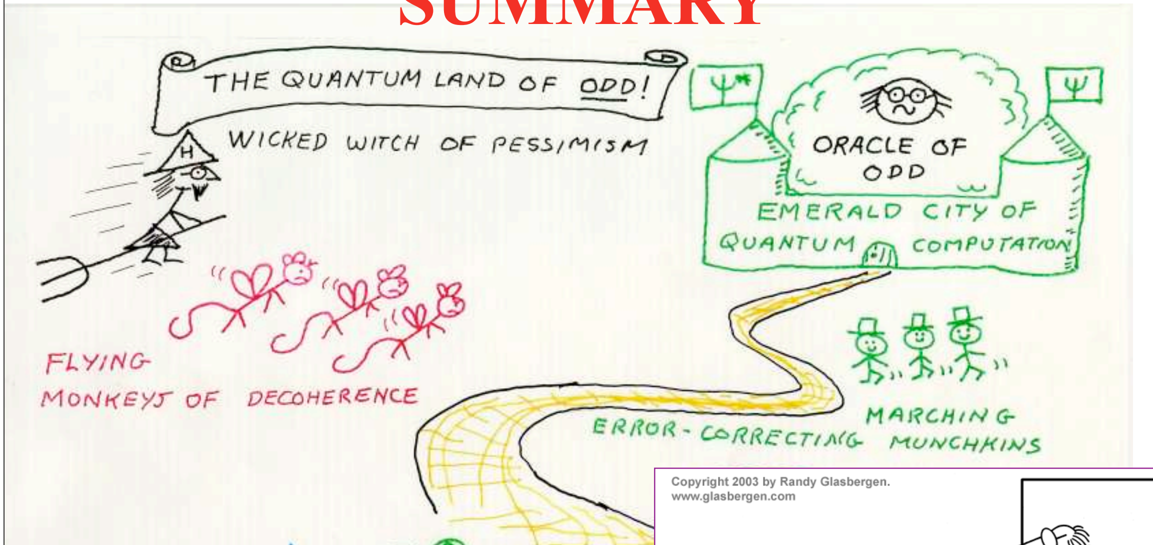
Error-correcting codes:
Steane, Proc. Roy. Soc. Lond. A 452, 2551 (1996)
Shor, PRA 52, 2493 (1995)
Knill et al, quant-ph/020717

Linear-optics quantum computation:
Knill, Laflamme, & Milburn, Nature 409, 46 (2001)
Gottesmann & Chuang, Nature 402, 390 (1999)
Ralph, Langford, Bell, & White, PRA 65, 062324 (2002)
O'Brien, Pryde, White, Ralph, & Branning, Nature 426, 264 (2003)
Langford et al., PRL 95, 210504 (2005)

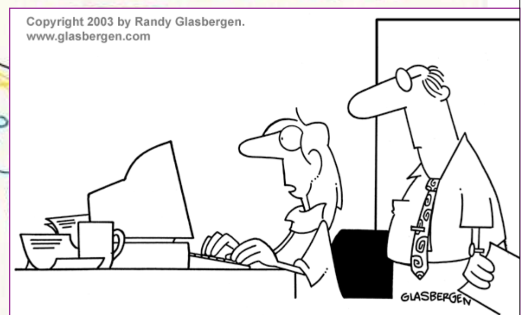
Cluster-state quantum computation:
Nielsen, "Universal quantum computation using only...", quant-ph/0108020
Raussendorf & Briegel, "A one-way quantum computer", PRL 86, 5188 (2001)
Raussendorf & Briegel, PRA 68, 022312 (2003)
Aliferis & Leung, "Computation by measurements: a unifying picture", quant-ph/0404082
Nielsen, "Cluster-state Quantum Computation", quant-ph/0504097
Walther et al, Nature 434, 169 (2005)

Weak-nonlinearity optical quantum computation:
Nemoto & Munro, PRL 93, 250502 (04)

SUMMARY



(Cartoon stolen from Jonathan Dowling)



"We don't need to worry about information security or message encryption. Most of our communications are impossible to understand in the first place."