Quantum Shwantum

Michael A. Nielsen

University of Queensland

Goal: To explain all the things that got left out of my earlier lectures because I tried to stuff too much in.

The measurement postulate formulated in terms of "observables"

Our form: A measurement is described by a complete set of projectors P_j onto orthogonal subspaces. Outcome j occurs with probability

$$\Pr(j) = \langle\psi|P_j|\psi\rangle.$$

The corresponding post-measurement state is

$$\frac{P_j|\psi\rangle}{\sqrt{\langle\psi|P_j|\psi\rangle}}.$$

Old form: A measurement is described by an observable, a Hermitian operator M, with spectral decomposition

$$M = \sum_j \lambda_j P_j.$$

The possible measurement outcomes correspond to the eigenvalues λ_j, and the outcome λ_j occurs with probability

$$\Pr(\lambda_j) = \langle\psi|P_j|\psi\rangle.$$

The corresponding post-measurement state is

$$\frac{P_j|\psi\rangle}{\sqrt{\langle\psi|P_j|\psi\rangle}}.$$

An example of observables in action

Example: Suppose we "measure Z".

Z has spectral decomposition $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, so this is just like measuring in the computational basis, and calling the outcomes "1" and "-1", respectively, for 0 and 1.

Exercise: Find the spectral decomposition of $Z \otimes Z$. Show that measuring $Z \otimes Z$ corresponds to measuring the parity of two qubits, with the result +1 corresponding to even parity, and the result -1 corresponding to odd parity.

Hint: $Z \otimes Z = |00\rangle\langle 00| + |11\rangle\langle 11| - |10\rangle\langle 10| - |01\rangle\langle 01|$

Exercise: Suppose we measure the observable M for a state $|\psi\rangle$ which is an eigenstate of that observable. Show that, with certainty, the outcome of the measurement is the corresponding eigenvalue of the observable.

What can be measured in quantum mechanics?

Computer science can inspire fundamental questions about physics.

We may take an "informatic" approach to physics.

(Compare the physical approach to information.)

Problem: What measurements can be performed in quantum mechanics?

What can be measured in quantum mechanics?

"Traditional" approach to quantum measurements:
A quantum measurement is described by an *observable,* ***M***, that is, a Hermitian operator acting on the state space of the system.

Measuring a system prepared in an eigenstate of ***M*** gives the corresponding eigenvalue of ***M*** as the measurement outcome.

"The question now presents itself – Can every observable be measured? The answer theoretically is yes. In practice it may be very awkward, or perhaps even beyond the ingenuity of the experimenter, to devise an apparatus which could measure some particular observable, but the theory always allows one to imagine that the measurement could be made."

- Paul A. M. Dirac

The halting problem

Does program number x halt on input of x?

$$h(x) \equiv \begin{cases} 0 \text{ if program } x \text{ halts on input } x \\ 1 \text{ otherwise} \end{cases}$$

Is there an algorithm to solve the halting problem, that is, to compute $h(x)$?

~~Suppose such an algorithm exists.~~

Let T be the program number for TURING.

```
PROGRAM: TURING(x)

IF h(x) = 1 THEN
    HALT
ELSE
    loop forever
```

Contradiction!

$h(T) = 0$ ⟷ TURING(T) halts ⟷ $h(T) = 1$

The halting observable

Consider a quantum system with an infinite-dimensional state space with orthonormal basis $|0\rangle, |1\rangle, |2\rangle, \ldots$

$$M \equiv \sum_{x=0}^{\infty} h(x) |x\rangle\langle x|$$

Can we build a measuring device capable of measuring the halting observable?

Yes: Would give us a procedure to solve the halting problem.

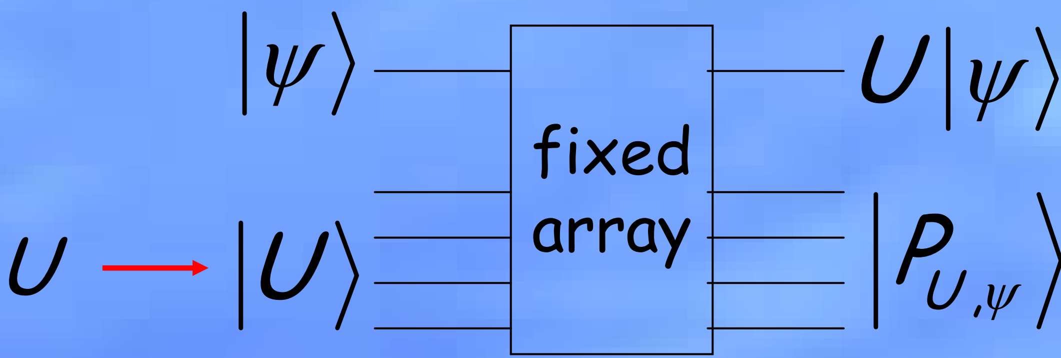
No: There is an interesting class of "superselection" rules controlling what observables may, in fact, be measured.

Research problem: Is the halting observable really measurable? If so, how? If not, why not?

Quantum computation via measurement alone

A quantum computation can be done simply by a sequence of two-qubit measurements. (No unitary dynamics required, except quantum memory!)

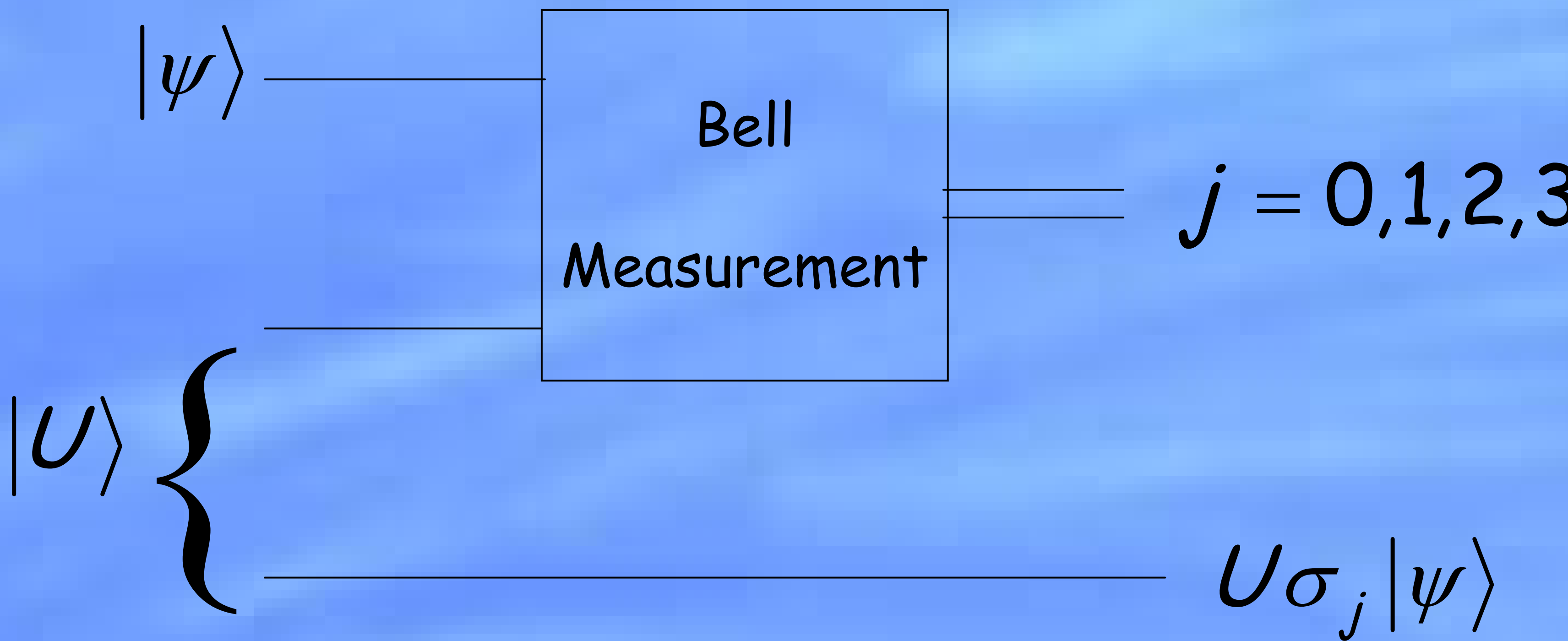
Can we build a programmable quantum computer?



No-programming theorem: Unitary operators $U_1,\ldots,U_n$ which are distinct, even up to global phase factors, require orthogonal programs $|U_1\rangle,\ldots,|U_n\rangle$.

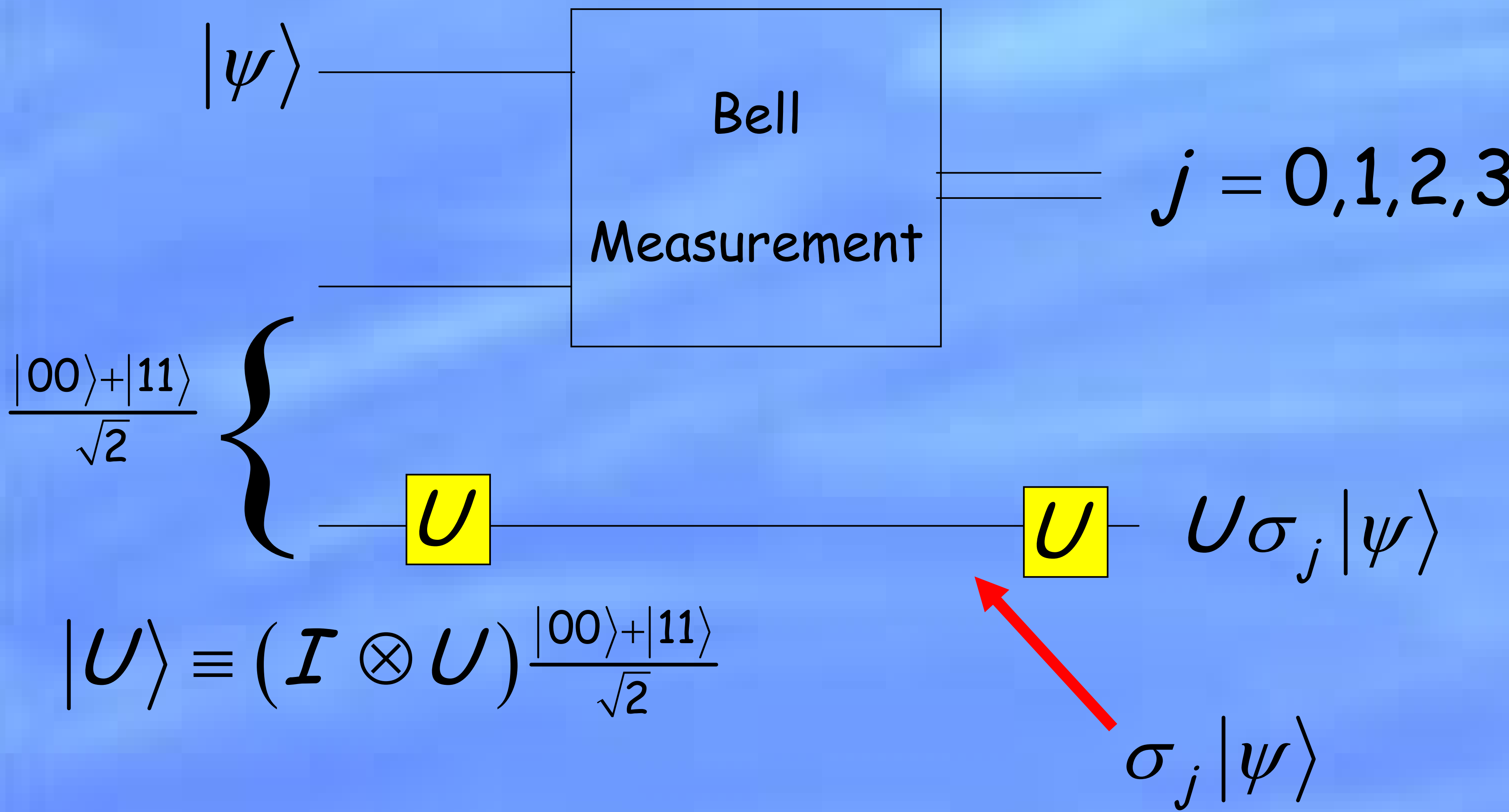
Challenge exercise: Prove the no-programming theorem.

A stochastic programmable quantum computer



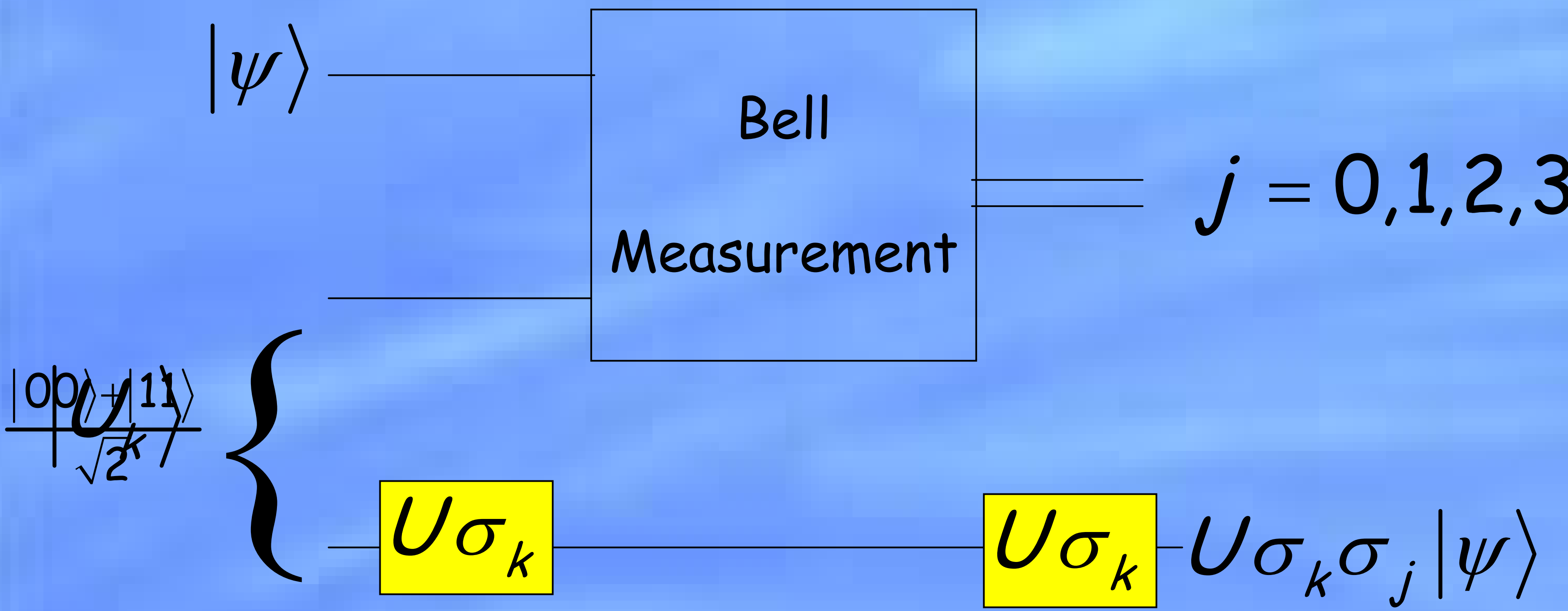
$$|U\rangle \equiv (I \otimes U)\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Why it works



$$|U\rangle \equiv (I \otimes U)\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

How to do single-qubit gates using measurements alone



$$|U_k\rangle \equiv (I \otimes U\sigma_k)\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

With probability $\frac{1}{4}$, $j = k$, and the gate succeeds.

Coping with failure

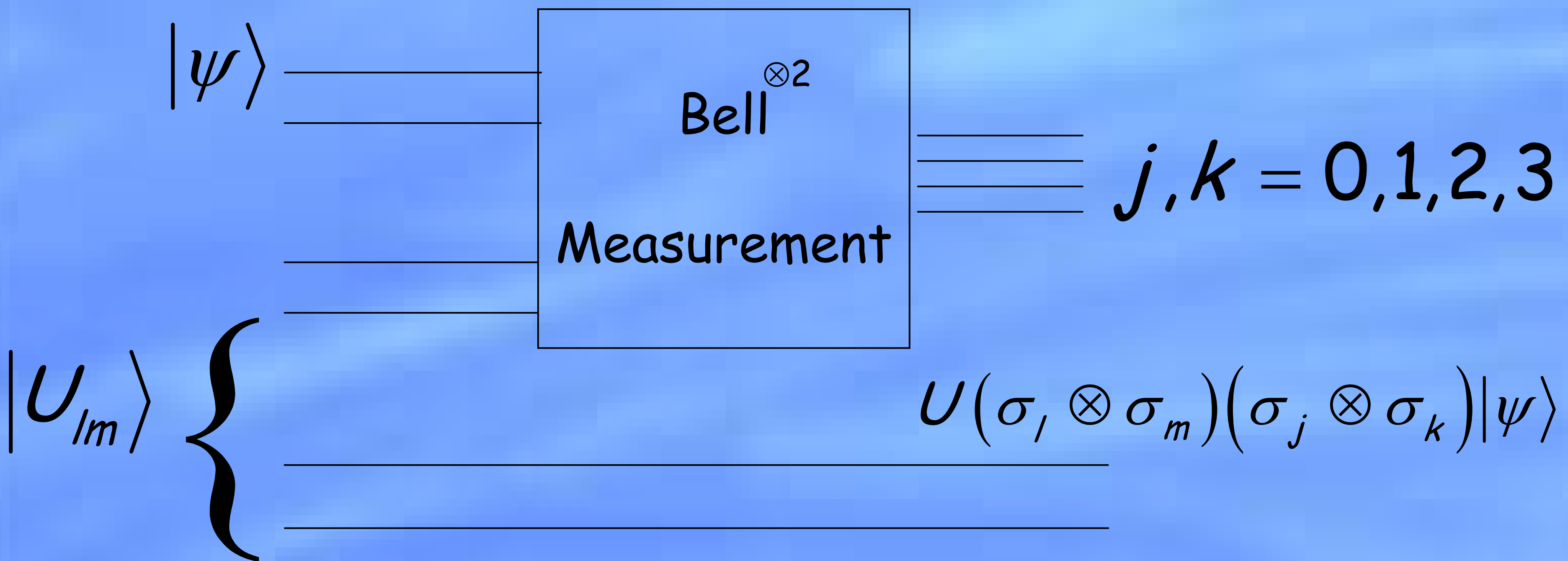
Action was $U\sigma_k\sigma_j, j \neq k$ - a known unitary error.

Now attempt to apply the gate $U(U\sigma_k\sigma_j)^\dagger$ to the qubit, using a similar procedure based on measurements alone.

Successful with probability $\frac{1}{4}$, otherwise repeat.

Failure probability ε can be achieved with $O\left(\log\frac{1}{\varepsilon}\right)$ repetitions.

How to do the controlled-not



$$|U_{lm}\rangle \equiv (I \otimes U\sigma_l \otimes \sigma_m)|\text{Bell}\rangle^{\otimes 2}$$

With probability $\frac{1}{16}$, $j = l, k = m$, and the gate succeeds.

Simplification: reducing to two-qubit measurements

The only measurement of more than two qubits presently required is for preparing the input to the controlled-not.

$$|U_{lm}\rangle \equiv (I \otimes U\sigma_l \otimes \sigma_m)|\text{Bell}\rangle^{\otimes 2}$$

Simplify by taking $l = m = 0$.

$$|U_{00}\rangle = (|0000\rangle + |0101\rangle + |1011\rangle + |1110\rangle)$$

The first and third bits always have even parity, so it suffices to create:
$(|0\rangle + |1\rangle)(|000\rangle + |101\rangle + |011\rangle + |110\rangle)$,
and then measure the parity of bits 1 and 3.

Simplification: reducing to two-qubit measurements

Reduces to the problem of creating:

$$(|000\rangle + |101\rangle + |011\rangle + |110\rangle).$$

Recall the identity underlying teleportation:

$$|\psi\rangle(|00\rangle + |11\rangle) = (|00\rangle + |11\rangle)|\psi\rangle + (|00\rangle - |11\rangle)Z|\psi\rangle + (|01\rangle + |10\rangle)X|\psi\rangle + (|01\rangle - |10\rangle)XZ|\psi\rangle$$

$$|0\rangle(|00\rangle + |11\rangle) = (|00\rangle + |11\rangle)|0\rangle + (|00\rangle - |11\rangle)|0\rangle + (|01\rangle + |10\rangle)|1\rangle + (|01\rangle - |10\rangle)|1\rangle$$

Project onto the subspace of the first two qubits spanned by $(|00\rangle + |11\rangle)$ and $(|01\rangle + |10\rangle)$.

Discussion

Measurement is now recognized as a powerful tool in many schemes for the implementation of quantum computation.

Research problem: Is there a practical variant of this scheme?

Research problem: What sets of measurement are sufficient to do universal quantum computation?

Research problem: We have talked about attempts to quantify the "power" of different entangled states. Can a similar quantitative theory of the power of quantum measurements be developed?

Thankyou to:

Organizing Committee

Michael Bremner
Jennifer Dodd
Anna Rogers

The Godparents

Gerard Milburn
Halina Rubinsztein-Dunlop
Andrew White

Tutors

Michael Bremner
Paul Cochrane
Chris Dawson
Jennifer Dodd
Alexei Gilchrist
Sarah Morrison
Duncan Mortimer
Tobias Osborne
Rodney Polkinghorne
Damian Pope

Speakers

Dave Bacon
Steve Bartlett
Bob Clark
Alex Hamilton
Ping Koy Lam
Keith Schwab
Matt Sellars
Ben Travaglione
Andrew White
Howard Wiseman

Volunteers

Tamyka Bell, Andrew Hines
Mark Dowling, Michael Gagen, Joel Gilmore, Nathan Langford, Austin Lund, Jeremy O'Brien, Geoff Pryde, Doug Turk