# An Introduction to Quantum Error Correction

**Ian Glendinning**

**May 31, 2005**

# Outline

- Introduction
- Quantum Circuits
- Classical Error Correction
- Quantum Error Correction
- Conclusion

# Introduction

- What is a Quantum Computer?
- What Makes Quantum Computers Different?
- Quantum Algorithms
- Building Quantum Computers
- Quantum Error Correction

# What is a quantum computer?

- A device that processes information using physical phenomena unique to quantum mechanics
- What makes quantum computers so exciting?
  - They can solve hard problems
  - The execution time of the best known classical algorithm for prime factorization scales exponentially with the no. of digits
  - Shor's quantum algorithm for prime factorization scales roughly quadratically, *exponentially faster!*

# What Makes Quantum Computers Different?

- The quantum analogue of a bit is a two-state quantum system such as an electron's spin or a photon's polarization, a *qubit*
- A qubit can exist not only in the classical 0 and 1 states, but also in a *superposition* of both
- A quantum register with $N$ qubits can be in a state that's a superposition of all values in the range 0 to $2^N - 1$
- Quantum operations act on *all* $2^N$ values *simultaneously*! This is known as quantum parallelism
- However...
  - Measurement gives only one of the $2^N$ values, at random

# Quantum Algorithms

- The probabilities of measuring the different values can be manipulated by operating on a quantum register with *quantum gates*, the analogue of logic gates
- Quantum algorithms consist of sequences of quantum gate operations and optionally measurements
- Algorithms exist that are able to exploit quantum parallelism, and leave an output register in a state where the probability of obtaining the answer to the problem is very close to one, giving an advantage over some classical algorithms

# Quantum Algorithms

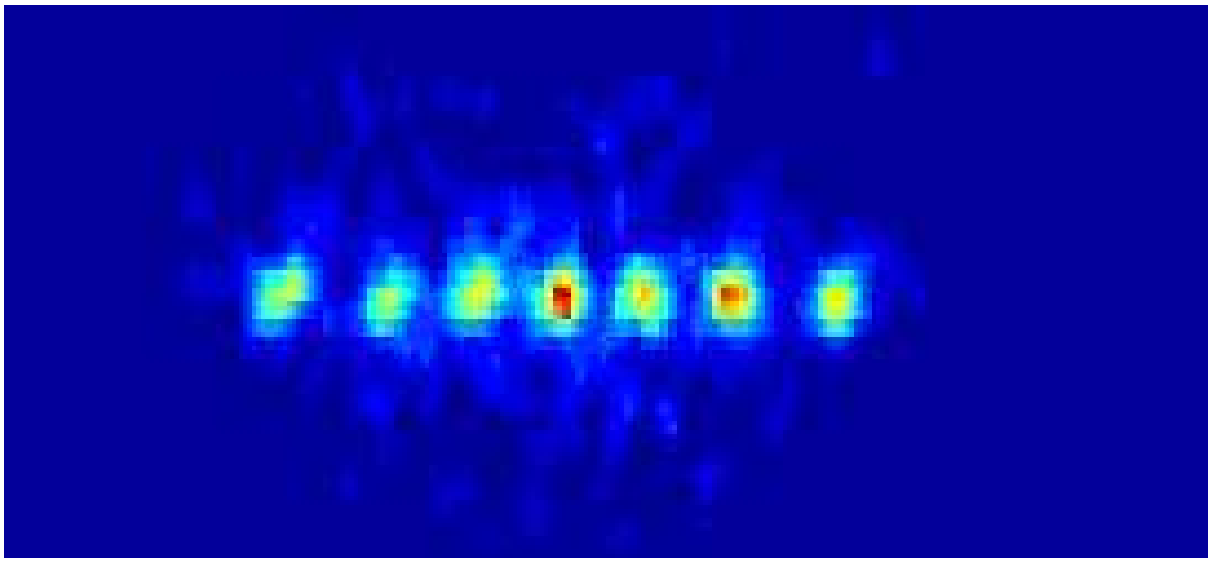
- Early algorithms
  - Deutsch (1985): two function evaluations for the price of one
  - Deutsch-Jozsa (1992): $O(2^n)$ evaluations for the price of one
- Most important known algorithms
  - Shor (1994): factorizing large numbers in polynomial time
    - Discrete logarithm, period finding, Quantum Fourier Transform (QFT), special cases of *hidden subgroup problem*
  - Grover (1996): unstructured search in time $O(\sqrt{N})$
    - Minimum, Quantum counting, speeding up solution of NP-complete problems
  - Simulation of quantum systems

# Building Quantum Computers

The technologies being explored include:

- Ion traps
- Cavity Quantum Electrodynamics
- Nuclear Magnetic Resonance (NMR)
- Optical interferometers
- Macroscopic superconductivity (SQUIDs)
- Semiconductors

# Trapped Ions



# Quantum Error Correction

- Quantum states are very fragile
- To protect them against the effects of noise, we would like to develop quantum error-correcting codes based on similar principles to classical error correction
- But there are some important differences between quantum and classical information, requiring new ideas to be introduced
- At first glance there are three rather formidable difficulties:
  - Arbitrary quantum states cannot be copied - no cloning
  - Errors are continuous
  - Measurement destroys quantum information
- Fortunately, none of these problems is fatal, as I shall show!

# Quantum Circuits

- Quantum Bits
- Quantum Registers
- Quantum Gates

# Quantum Bits

A quantum bit, or *qubit* is the unit of quantum information. The states of a qubit corresponding to the classical values 0 and 1 are called the *computational basis states*, and are written $|0\rangle$ and $|1\rangle$.

In general a qubit can be in a *superposition* of these two states:

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

where $\alpha$ and $\beta$ are complex numbers called *amplitudes*, which are subject to the requirement that:

$$|\alpha|^2 + |\beta|^2 = 1$$

# Qubits - Measurement

A *measurement* of the state of a qubit always gives either the result $|0\rangle$, with probability $|\alpha|^2$, or the result $|1\rangle$, with probability $|\beta|^2$, so the requirement:

$$|\alpha|^2 + |\beta|^2 = 1$$

expresses the fact that the sum of the probabilities of all possible outcomes must be one. For example, a qubit can be in the state:

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

which when measured, gives either the result 0, with probability $|1/\sqrt{2}|^2 = 1/2$, or the result 1, also with probability $1/2$.

# Qubits - Vector Representation

The general state of a qubit can be represented as a unit vector in a two-dimensional complex vector space. It is conventional to define the computational basis vectors as:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

So a general qubit state can be written:

$$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

subject to the *normalization* condition:

$$|\alpha|^2 + |\beta|^2 = 1$$

# Quantum Registers

The computational basis vectors of a two-qubit register correspond to the classical binary values 00, 01, 10 and 11, and are written $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$.

They can be represented as four-dimensional unit vectors, and are conventionally defined as:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

# Quantum Registers

- A general two-qubit state is a (complex) linear combination of the basis vectors, subject to the normalization constraint that it has length 1.
- The state of an $n$-qubit register can be represented as a $2^n$-dimensional complex unit vector

# Quantum Gates

- Classical computer circuits are built from logic gates which operate on bits and registers
- By analogy we can define quantum gates which operate on qubits and quantum registers

# The Quantum NOT Gate

The only non-trivial classical single-bit gate is the NOT gate, defined by its 'truth table' in which $0 \rightarrow 1$ and $1 \rightarrow 0$.

We can define an analagous quantum NOT gate, conventionally written as an operator $X$, such that $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$

This does not tell us what happens to superpositions of the states $|0\rangle$ and $|1\rangle$. In fact, the quantum NOT gate acts *linearly*, i.e.:

$$\begin{aligned} X(\alpha|0\rangle + \beta|1\rangle) &= X\alpha|0\rangle + X\beta|1\rangle \\ &= \alpha X|0\rangle + \beta X|1\rangle \\ &= \alpha|1\rangle + \beta|0\rangle \end{aligned}$$

# Matrix Representation

Linearity is a general property of quantum mechanics, and means that quantum gates can be conveniently represented as matrices:

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

The operation of a gate on a quantum register is implemented by matrix multiplication, so for $X$ operating on the state $\alpha|0\rangle + \beta|1\rangle$ we have

$$X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

Notice that $X$ preserves the normalization. This is a property of *all* quantum gates, and turns out to be the *only* constraint on them.

# The Controlled-NOT Gate

The prototypical multi-qubit gate is the *controlled*-NOT or CNOT gate.

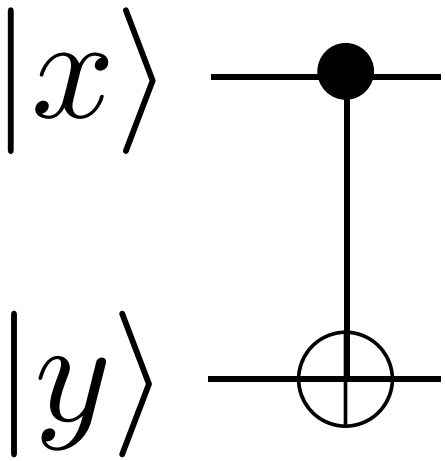
It has two inputs, known as the *control* and *target* qubits, and two outputs.

If the control qubit is set to 0, the target qubit is unchanged, and if the control qubit is set to 1, the target qubit is flipped ($|c, t\rangle$):

$$|00\rangle \rightarrow |00\rangle;\ |01\rangle \rightarrow |01\rangle;\ |10\rangle \rightarrow |11\rangle;\ |11\rangle \rightarrow |10\rangle$$

CNOT is a generalization of the classical XOR gate, since its action may be summarized as $|x, y\rangle \rightarrow |x, y \oplus x\rangle$, where $\oplus$ is addition modulo two, which is the same as XOR.

# Circuit Symbol for The CNOT Gate



# Matrix Representation of CNOT

The matrix representation of CNOT is:

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

Every $n$-qubit gate (operator) can be represented as a $2^n \times 2^n$ unitary matrix, i.e. a complex matrix $U$ with the property that $U^\dagger U = I$, which guarantees that the normalization of states is preserved.

# The Hadamard Gate

One of the most useful single-qubit gates is the *Hadamard* gate

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

Acting on the Basis states $|0\rangle$ and $|1\rangle$:

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

and

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

An important property of $H$ is that $H^2 = I$.

# The Y and Z Gates

Two more single-qubit gates we will need are $Y$ and $Z$, defined as:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

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

$Z$ is known as the phase flip gate because

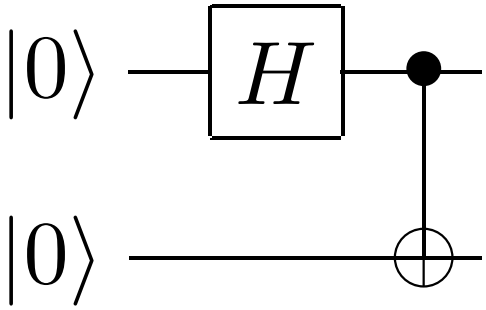
$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

$X$, $Y$ and $Z$ have the properties:

$$X^2 = Y^2 = Z^2 = -iXYZ = I$$

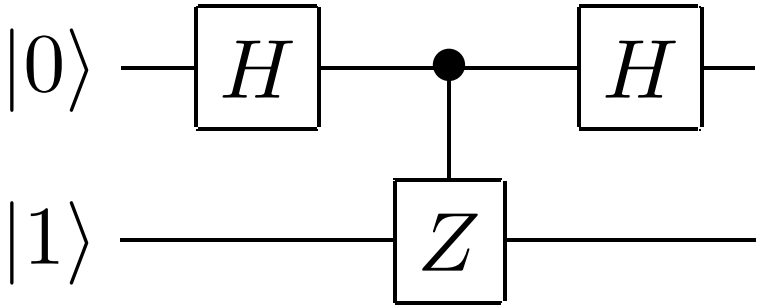
# Entanglement

The circuit below produces the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ which can not be written as a product of any two-qubit state! Such states are said to be *entangled*. Measuring either qubit results in either the state $|00\rangle$ or the state $|11\rangle$ with equal probability.



# Interpreting Quantum Circuit Diagrams

When interpreting quantum circuit diagrams it is important to remember that they are not classical. They must be applied to each component of a superposition one at a time, and the results added together to get the final result.




One might naively expect that the above circuit would leave the top qubit unchanged, as $H^2 = I$, but in fact it flips it to $|1\rangle$, leaving the bottom qubit unchanged!

# Classical Error Correction

- Protects information against the effects of noise when it is communicated or stored
- The key idea is to *encode* the information by adding redundant information in such a way that even if some of the encoded information is lost, enough will be left so that it is possible to *decode* it and recover all the original information
- For example, suppose the effect of a noisy communication channel is to flip the bit being transmitted with probability $p$, while with probability $1 - p$ the bit is unchanged

# Classical Error Correction

A simple way to protect the bit against the effects of noise is to use a *repetition code*, replacing it with three copies of itself:

$$0 \rightarrow 000$$
$$1 \rightarrow 111$$

The bit strings 000 and 111 are sometimes called the *logical* 0 and *logical* 1.

Suppose the output of the channel is 001. Provided $p$ is not too high, it is very likely that the third bit was flipped, and that 0 was sent.

This type of decoding is called *majority voting*, and succeeds if only one bit is flipped, but fails otherwise.

# Quantum Error Correction

- The Three Qubit Bit Flip Code
- The Three Qubit Phase Flip Code
- The Shor Code

# The Three Qubit Bit Flip Code

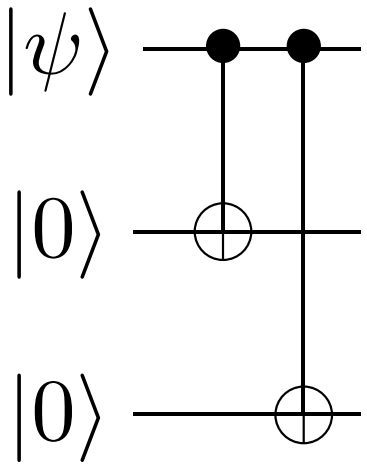
- The simplest quantum error correction code is a three-qubit repetition code, which can be used to protect quantum information in the presence of a restricted type of error
- Suppose we send qubits down a channel that leaves them untouched with probability $1 - p$ or flips them with probability $p$
- That is, with probability $p$, state $|\psi\rangle$ is taken to state $X|\psi\rangle$
- This is called the *bit flip channel*. The *bit flip code* encodes the single qubit state $\alpha|0\rangle + \beta|1\rangle$ in three qubits as $\alpha|000\rangle + \beta|111\rangle$

$$\begin{aligned} |0\rangle &\rightarrow |0_L\rangle \equiv |000\rangle \\ |1\rangle &\rightarrow |1_L\rangle \equiv |111\rangle \end{aligned}$$

- where $|0_L\rangle$ and $|1_L\rangle$ denote the *logical* $|0\rangle$ and $|1\rangle$ states

# The Three Qubit Bit Flip Code

We adopt the convention of calling the source Alice and the receiver Bob. Alice encodes her quantum state $|\psi\rangle$ with the following circuit:




The initial state of the three qubits is $\alpha|000\rangle + \beta|100\rangle$. After the first CNOT gate the state is $\alpha|000\rangle + \beta|110\rangle$, and after the second CNOT gate the state is $\alpha|000\rangle + \beta|111\rangle$, as required.

# The Three Qubit Bit Flip Code

Bob receives the three qubits, but they have been acted on by noise in the channel, and their state is one of the following:

| state | probability |
|---|---|
| $\alpha\|000\rangle + \beta\|111\rangle$ | $(1-p)^3$ |
| $\alpha\|100\rangle + \beta\|011\rangle$ | $p(1-p)^2$ |
| $\alpha\|010\rangle + \beta\|101\rangle$ | $p(1-p)^2$ |
| $\alpha\|001\rangle + \beta\|110\rangle$ | $p(1-p)^2$ |
| $\alpha\|110\rangle + \beta\|001\rangle$ | $p^2(1-p)$ |
| $\alpha\|101\rangle + \beta\|010\rangle$ | $p^2(1-p)$ |
| $\alpha\|011\rangle + \beta\|100\rangle$ | $p^2(1-p)$ |
| $\alpha\|111\rangle + \beta\|000\rangle$ | $p^3$ |

# The Three Qubit Bit Flip Code

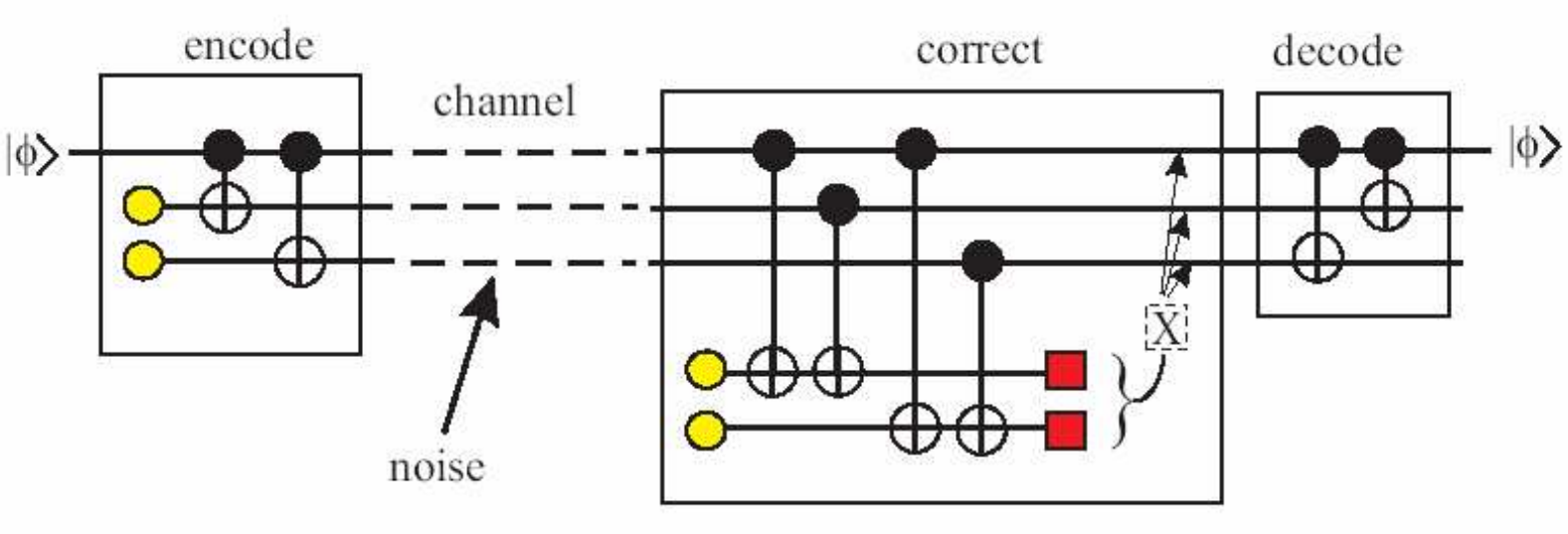
As in the classical case, decoding is accomplished by majority logic. However it must be implemented carefully, to avoid destroying the quantum information.

Bob introduces two more qubits of his own, prepared in the state $|00\rangle$.

This extra pair of qubits, referred to as an *ancilla*, is not strictly necessary, but makes the error correction easier to understand, and becomes necessary when fault-tolerant methods are needed.

# The Three Qubit Bit Flip Code

Bob uses the ancilla to gather information about the noise:



# The Three Qubit Bit Flip Code

The total state of all qubits is now:

| state | probability |
|---|---|
| $(\alpha\|000\rangle + \beta\|111\rangle)\|00\rangle$ | $(1-p)^3$ |
| $(\alpha\|100\rangle + \beta\|011\rangle)\|11\rangle$ | $p(1-p)^2$ |
| $(\alpha\|010\rangle + \beta\|101\rangle)\|10\rangle$ | $p(1-p)^2$ |
| $(\alpha\|001\rangle + \beta\|110\rangle)\|01\rangle$ | $p(1-p)^2$ |
| $(\alpha\|110\rangle + \beta\|001\rangle)\|01\rangle$ | $p^2(1-p)$ |
| $(\alpha\|101\rangle + \beta\|010\rangle)\|10\rangle$ | $p^2(1-p)$ |
| $(\alpha\|011\rangle + \beta\|100\rangle)\|11\rangle$ | $p^2(1-p)$ |
| $(\alpha\|111\rangle + \beta\|000\rangle)\|00\rangle$ | $p^3$ |

# The Three Qubit Bit Flip Code

Bob measures the two ancilla qubits, which gives him two classical bits of information, called the *error syndrome*, since it diagnoses the errors in the received qubits:

| measured syndrome | action |
|---|---|
| 00 | do nothing |
| 01 | apply $X$ to third qubit |
| 10 | apply $X$ to second qubit |
| 11 | apply $X$ to first qubit |

Finally, Bob uses two CNOT gates to restore the second and third qubits in the encoded data to their inital values of $|0\rangle$. Crucially, no information about $\alpha$ and $\beta$ was obtained, preserving the quantum state.

# The Three Qubit Bit Flip Code

The probability of an error is the probability that two or more qubits are flipped:

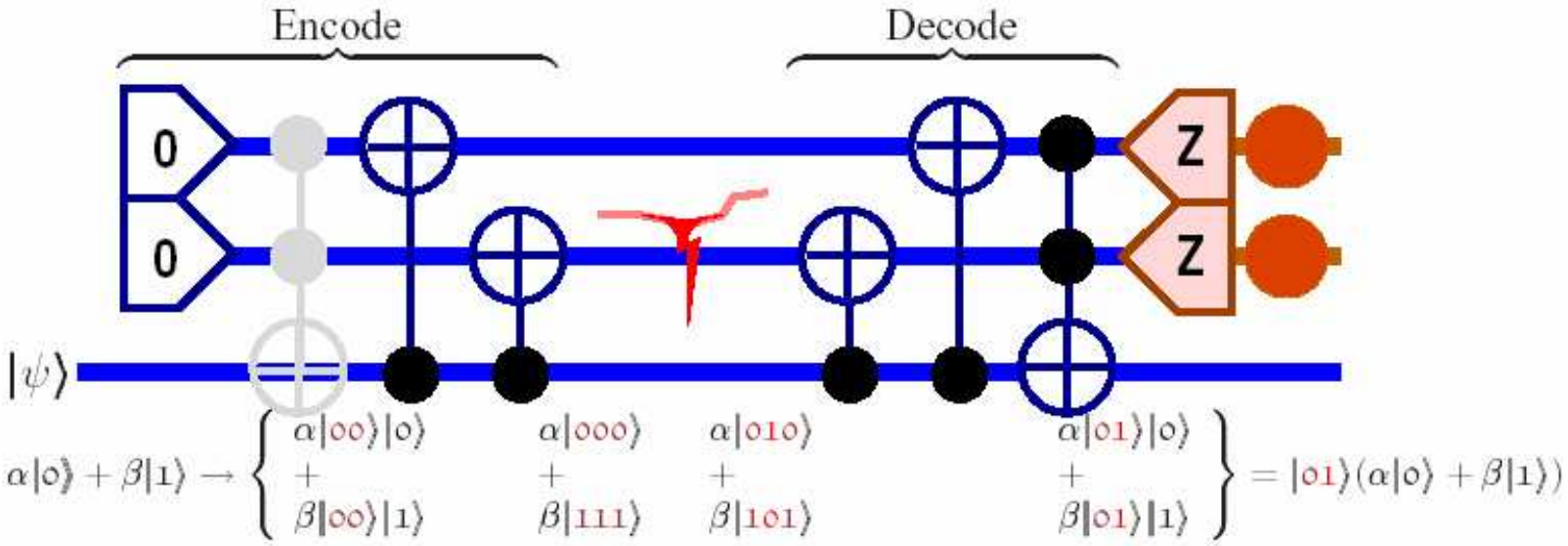
$$\begin{aligned} p_e &= 3p^2(1-p) + p^3 \\ &= 3p^2 - 2p^3 \end{aligned}$$

Without encoding, the probability of an error was $p$, so the code makes the transmission more reliable provided $p_e < p$, which is the case when $p < \frac{1}{2}$.

This error analysis is not completely adequate, because unlike in the classical case, bit flip errors corrupt some states more than others. Extreme examples are the the state $(|0\rangle + |1\rangle)/\sqrt{2}$, which is not affected at all, and the states $|0\rangle$ and $|1\rangle$, which are interchanged. To address this problem, so-called *fidelity* measures are introduced.

# The Three Qubit Bit Flip Code

As already mentioned, the ancilla is not stictly necessary. Here is an optimized circuit that uses the two extra qubits from the encoded qubit to hold the error syndrome during decoding:



# The Three Qubit Phase Flip Code

- The bit flip code is interesting, but does not appear to be a very significant improvement over classical error-correcting codes, and it does not correct all the errors that can happen to qubits
- A more interesting noisy quantum channel is the *phase flip* channel, which has no classical equivalent
- In this error model the qubit is left unchanged with probability $1-p$ and with probability $p$ the relative phase of the $|0\rangle$ and $|1\rangle$ states is flipped
- More precisely, the phase flip operator $Z$ is applied to the qubit with probability $p$, so the state $\alpha|0\rangle + \beta|1\rangle$ is taken to the state $\alpha|0\rangle - \beta|1\rangle$ and vice versa

# The Three Qubit Phase Flip Code

Although classical channels don't have any property equivalent to phase, there is an easy way to turn the phase flip channel into a bit flip channel. Consider the states:

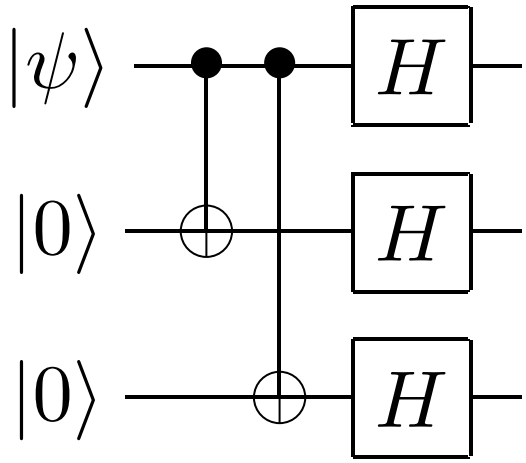
$$\begin{aligned} |+\rangle &\equiv (|0\rangle + |1\rangle)/\sqrt{2} \\ |-\rangle &\equiv (|0\rangle - |1\rangle)/\sqrt{2} \end{aligned}$$

The $Z$ operator takes $|+\rangle$ to $|-\rangle$, and vice versa, so it is just like a bit flip with respect to the labels $+$ and $-$.

This suggests using the states $|0_L\rangle \equiv |++\rangle$ and $|1_L\rangle \equiv |--\rangle$ as logical zero and one states for protection against phase flip errors.

# The Three Qubit Phase Flip Code

The following circuit produces this encoding:




When Bob receives the three qubits, he can then simply apply $H$ to each of them, changing $|+++\rangle \rightarrow |000\rangle$ and $|---\rangle \rightarrow |111\rangle$, and he can they apply the bit flip error correction procedure.

# The Shor Code

- There is a simple quantum code that can protect against the effects of an *arbitrary* error on a single qubit!
- It is called the *Shor* code, after its inventor, and it is a combintation of the three qubit phase flip and bit flip codes
- We first encode the qubit using the phase flip code:

$$\begin{aligned} |0\rangle &\rightarrow |+++\rangle \\ |1\rangle &\rightarrow |---\rangle \end{aligned}$$

- then we encode these qubits using the three qubit bit flip code:

$$\begin{aligned} |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} &\rightarrow (|000\rangle + |111\rangle)/\sqrt{2} \\ |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} &\rightarrow (|000\rangle - |111\rangle)/\sqrt{2} \end{aligned}$$

# The Shor Code

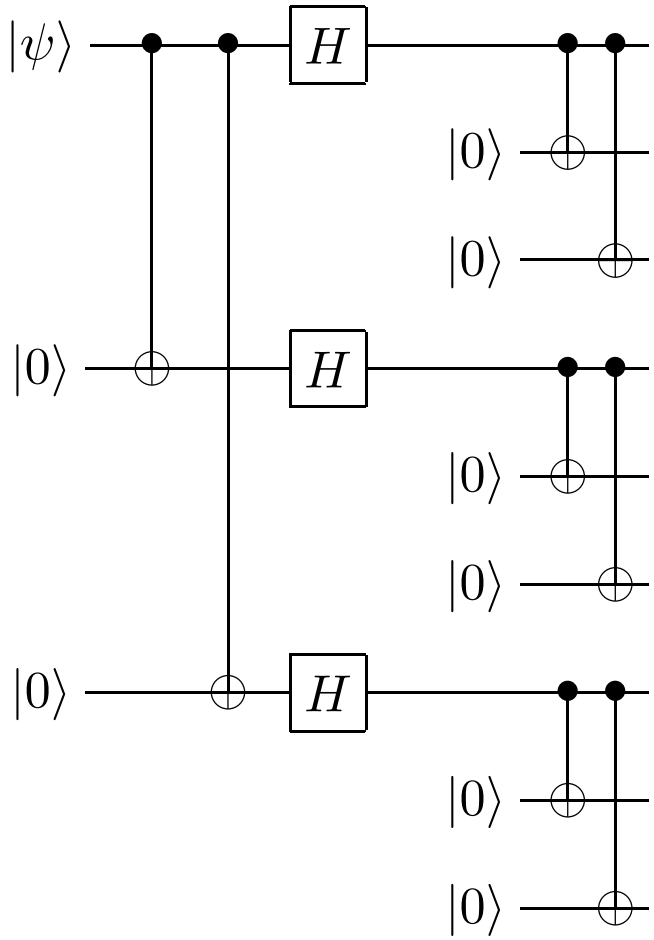
The result is a nine qubit code, with codewords given by:

$$|0\rangle \rightarrow |0_L\rangle \equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \rightarrow |1_L\rangle \equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

The encoding is peformed by the following circuit, where some of the $|0\rangle$ states have been indented to emphasise the concatenated nature of the code:

# Encoding Circuit for The Shor Code



# The Shor Code

- It is clear that the Shor code can protect against bit flips, as all we need is three copies of the bit flip correction circuit
- The code can also protect against a phase flip on any qubit, which is less obvious, but notice that a phase flip on *any* of the qubits within one of the blocks of three changes $|000\rangle + |111\rangle$ to $|000\rangle - |111\rangle$ and vice versa
- It thus suffices to detect a phase flip on one of the blocks and to correct it, which can be done with the ideas introduced so far, though more concise methods exist, which I will not discuss here
- The procedures for correcting bit and phase flip errors are independent of one another, so the Shor code is able to correct combined bit and phase flips on a single qubit

# The Shor Code

- The Shor code can protect against much more than just bit and phase flip errors - in fact it protects against completely *arbitrary* errors, as long as they only affect a single qubit!
- The error can be tiny, or apparently disastrous, like removing the qubit and replacing it with garbage, but no additional work has to be done - the procedure already described works fine!
- This is because the most general form of single-qubit error can be written as

$$|\psi\rangle \rightarrow E|\psi\rangle$$

where $E$ is an arbitrary operator, which can be decomposed as

$$E = e_i I + e_x X + e_y Y + e_z Z$$

# The Shor Code

- but $Y = iXZ$, so we can write

$$E = e_0 I + e_1 X + e_2 Z + e_3 XZ$$

- Measuring the error syndrome collapses the superposition into one of the four states $|\psi\rangle$, $X|\psi\rangle$, $Z|\psi\rangle$, or $XZ|\psi\rangle$. In the case of $|\psi\rangle$ no action is necessary, and the other three cases are all correctable with the Shor code!
- This is a fundamental deep fact about quantum error correction, that by correcting just a discrete set of errors, in this case the bit flip, phase flip and combined bit-phase flip, a quantum error-correcting code can correct an apparently much larger (continuous!) class of errors

# Conclusion

- Quantum computers can solve hard problems
- Quantum computer hardware can be constructed
- Quantum errors can be corrected
- We have submitted a proposal to the FET Open scheme of FP6
  - Title: Improving Quantum Computing through High-End Simulation (IQ-SIM)
  - Objective: to improve the implementation of quantum algorithms by employing numerical simulation of realistic ion trap devices
  - Consortium: VCPC (coordinator), ARCS, FZJ, RuG, IQOQI
- Further information from http://www.vcpc.univie.ac.at/qc/