

1.10: Quantum Computation- A Short Course

The last several tutorials were a bit off the theme of quantum computation. We get back on track with a look at data base searching the quantum way, or the best way to find a needle in a hay stack. This is followed by a demonstration of Simon's algorithm, an illustration of quantum dense coding and an example of quantum error correction.

Grover Search Algorithm Implementation for Two Items

Chris Monroe's research group recently published an experimental implementation of the Grover search algorithm in Nature Communications 8, 1918 (2017). In this report the Grover search is implemented for $N = 3$ using the three qubit quantum circuit shown below. In this particular example it is demonstrated that the search algorithm successfully searches for two items in one operation of the circuit. The lead sentence in the paper states "The Grover search algorithm has four stages: initialization (red), oracle (green), amplification (blue) and measurement (black)."

$$\begin{array}{lcl}
 |0\rangle \triangleright H & \left[\begin{array}{c} | \\ | \\ | \end{array} \right] & H \quad X \quad \cdot \quad X \quad H \triangleright \text{Measure} \\
 |0\rangle \triangleright H & \left[\begin{array}{c} | \\ | \\ | \end{array} \right] \text{Oracle} & H \quad X \quad | \quad X \quad H \triangleright \text{Measure} \\
 |0\rangle \triangleright H & \left[\begin{array}{c} | \\ | \\ | \end{array} \right] & H \quad X \quad Z \quad X \quad H \triangleright \text{Measure}
 \end{array}$$

The oracle, highlighted below, contains 3 ($|011\rangle$) and 5 ($|101\rangle$).

$$\begin{aligned}
 H &:= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} & X &:= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
 \text{Oracle} &= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\
 \text{CCZ} &:= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}
 \end{aligned}$$

$$\text{HHH} := \text{kroncker}(H, \text{kroncker}(H, H)) \quad \text{XXX} := \text{kroncker}(X, \text{kroncker}(X, X))$$

The initial Hadamard gates on the three circuit wires feed the Grover search algorithm (in blue) a superposition of all possible queries yielding a superposition of the correct answers.

$$\text{GroverSearch} := \text{HHH} \cdot \text{XXX} \cdot \text{CCZ} \cdot \text{XXX} \cdot \text{HHH} \cdot \text{Oracle} \cdot \text{HHH}$$

$$\text{GroverSearch} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -0.707 \\ 0 \\ -0.707 \\ 0 \\ 0 \end{pmatrix} = -\frac{1}{\sqrt{2}}[|011\rangle + |101\rangle]$$

Aspects of Simon's Algorithm

A concealed quantum algorithm calculates $f(x)$ from an input register containing a superposition of all x -values. Pairs of x -values (x, x') generate the same output. Simon's algorithm is an efficient method for finding the relationship between the pairs: $f(x) = f(x') = f(x \oplus s)$, where s is a secret string and the addition on the right is bitwise modulo 2. In a classical calculation one could compute $f(x)$ until some pattern emerged and find the pairs by inspection. This approach is illustrated below.

Decimal	Binary		Binary	Decimal
$ 0\rangle$	$ 000\rangle$	$\xrightarrow{f(0)}$	$ 011\rangle$	$ 3\rangle$
$ 1\rangle$	$ 001\rangle$	$\xrightarrow{f(1)}$	$ 001\rangle$	$ 1\rangle$
$ 2\rangle$	$ 010\rangle$	$\xrightarrow{f(2)}$	$ 010\rangle$	$ 2\rangle$
$ 3\rangle$	$ 011\rangle$	$\xrightarrow{f(3)}$	$ 000\rangle$	$ 0\rangle$
$ 4\rangle$	$ 100\rangle$	$\xrightarrow{f(4)}$	$ 001\rangle$	$ 1\rangle$
$ 5\rangle$	$ 101\rangle$	$\xrightarrow{f(5)}$	$ 011\rangle$	$ 3\rangle$
$ 5\rangle$	$ 101\rangle$	$\xrightarrow{f(5)}$	$ 011\rangle$	$ 3\rangle$
$ 6\rangle$	$ 110\rangle$	$\xrightarrow{f(6)}$	$ 000\rangle$	$ 0\rangle$
$ 7\rangle$	$ 111\rangle$	$\xrightarrow{f(7)}$	$ 010\rangle$	$ 2\rangle$

The table of results reveals the pairs $\{(0,5), (1,4), (2,7), (3,6)\}$ and that $|s\rangle = |101\rangle$. Adding $|s\rangle$ bitwise modulo 2 to any $|x\rangle$ reveals its partner $|x'\rangle$.

The following quantum circuit is a rudimentary implementation of Simon's algorithm. The section in blue is the concealed algorithm. It has been discussed in two other tutorials: **Quantum Parallel Calculation** and **An Illustration of the Deutsch-Jozsa Algorithm**. Its operation yields the results shown in the following table.

$\begin{pmatrix} x & 0 & 1 & 2 & 3 \\ f(x) & 1 & 0 & 0 & 1 \end{pmatrix}$									
Initial	1	2	3	4	5	Final			
$ 0\rangle$	$\triangleright H$	H	\triangleright
$ 0\rangle$	$\triangleright H$	H	\triangleright
$ 0\rangle$	\triangleright	NOT	\triangleright Measure, 0 or 1

Next we prepare a table showing the results of a classical calculation. It is clear that the pairs are (0,3) and (1,2), and that $|s\rangle = |11\rangle$.

Decimal	Binary		Binary	Decimal
$ 0\rangle$	$ 000\rangle$	$\xrightarrow{f(0)}$	$ 011\rangle$	$ 3\rangle$
$ 1\rangle$	$ 001\rangle$	$\xrightarrow{f(1)}$	$ 001\rangle$	$ 1\rangle$
$ 2\rangle$	$ 010\rangle$	$\xrightarrow{f(2)}$	$ 010\rangle$	$ 2\rangle$
$ 3\rangle$	$ 011\rangle$	$\xrightarrow{f(3)}$	$ 000\rangle$	$ 0\rangle$

Now we examine the operation of the quantum circuit that implements Simon's algorithm by two different, but equivalent methods. The matrices representing the quantum gates in the circuit are:

$$\begin{aligned}
 I &:= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \text{NOT} &:= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & H &:= \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\
 \text{CNOT} &:= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\
 \text{CnNOT} &:= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}
 \end{aligned}$$

The three qubit input state is:

$$\Psi_{\text{in}} := (1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0)^T$$

The concealed algorithm:

$$U_f := \text{kronecker}(I, \text{kronecker}(I, \text{NOT})) \cdot \text{kronecker}(I, \text{CNOT}) \cdot \text{CnNOT}$$

The complete quantum circuit:

$$\text{QuantumCircuit} := \text{kronecker}(H, \text{kronecker}(H, I)) \cdot U_f \cdot \text{kronecker}(H, \text{kronecker}(H, I))$$

The operation of the quantum circuit on the input state yields the following result:

$$\begin{aligned}
 \text{QuantumCircuit} \cdot \Psi_{\text{in}} &= \begin{pmatrix} 0.5 \\ 0.5 \\ 0 \\ 0 \\ 0 \\ 0 \\ -0.5 \\ 0.5 \end{pmatrix} \\
 &= \frac{1}{2} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{2} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\
 &= \frac{1}{2} [|00\rangle - |11\rangle] |0\rangle + \frac{1}{2} [|00\rangle + |11\rangle] |1\rangle
 \end{aligned}$$

The terms in brackets are superpositions of the x-values which are related by $x' = x \oplus s$. Thus we see by inspection that $|s\rangle = |11\rangle$. The actual implementation of Simon's algorithm involves multiple measurements in order to determine the secret string. The

Appendix modifies the quantum circuit to include the effect of measurement on the bottom wire.

The second method of analysis uses the following truth tables for the quantum gates and the operation of the Hadamard gate to trace the evolution of the input qubits through the quantum circuit.

$$\begin{array}{c}
 \text{NOT} \begin{pmatrix} 0 & ' & 1 \\ 1 & ' & 0 \end{pmatrix} \\
 \\
 \text{CNOT} \begin{pmatrix} \text{Decimal} & \text{Binary} & ' & \text{Binary} & \text{Decimal} \\ 0 & 00 & ' & 00 & 0 \\ 1 & 01 & ' & 01 & 1 \\ 2 & 10 & ' & 11 & 3 \\ 3 & 11 & ' & 10 & 2 \end{pmatrix} \\
 \\
 \text{CnNOT} \begin{pmatrix} \text{Decimal} & \text{Binary} & ' & \text{Binary} & \text{Decimal} \\ 0 & 000 & ' & 000 & 0 \\ 1 & 001 & ' & 001 & 1 \\ 2 & 010 & ' & 010 & 3 \\ 3 & 011 & ' & 011 & 3 \\ 4 & 100 & ' & 101 & 5 \\ 5 & 101 & ' & 100 & 4 \\ 6 & 110 & ' & 111 & 7 \\ 7 & 111 & ' & 110 & 6 \end{pmatrix} \\
 \\
 \text{Hadamard operation:} \begin{bmatrix} 0 & ' & H & ' & \frac{1}{\sqrt{2}} \cdot (0+1) & ' & H & ' & 0 \\ 1 & ' & H & ' & \frac{1}{\sqrt{2}} \cdot (0-1) & ' & H & ' & 1 \end{bmatrix} \\
 \\
 |000\rangle \\
 H \otimes H \otimes I \\
 \frac{1}{\sqrt{2}} [|0\rangle + |1\rangle] \frac{1}{\sqrt{2}} [|0\rangle + |1\rangle] |0\rangle = \frac{1}{2} [|000\rangle + |010\rangle + |100\rangle + |110\rangle] \\
 \text{CnNOT} \\
 \frac{1}{2} [|000\rangle + |010\rangle + |101\rangle + |111\rangle] \\
 I \otimes \text{CNOT} \\
 \frac{1}{2} [|000\rangle + |011\rangle + |101\rangle + |110\rangle] \\
 I \otimes I \otimes \text{NOT} \\
 \frac{1}{2} [|001\rangle + |010\rangle + |100\rangle + |111\rangle] \\
 H \otimes H \otimes I \\
 \frac{1}{2} [(|00\rangle - |11\rangle)|0\rangle + (|00\rangle + |11\rangle)|1\rangle]
 \end{array}$$

Appendix:

The circuit modification shown below includes the effect of measurement on the bottom wire.

Measure $|0\rangle$ on the bottom wire:

$$\text{QuantumCircuit} := \text{kroncker} \left(\text{H}, \text{kroncker} \left[\text{H}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}^T \right] \right) \cdot U_f \cdot \text{kroncker}(\text{H}, \text{kroncker}(\text{H}, \text{I}))$$

$$\text{QuantumCircuit} \cdot \Psi_{\text{in}} = \begin{pmatrix} 0.5 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -0.5 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 0.5 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -0.5 \\ 0 \end{pmatrix} = \frac{1}{2} \cdot \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Measure $|1\rangle$ on the bottom wire:

$$\text{QuantumCircuit} := \text{kroncker} \left(\text{H}, \text{kroncker} \left[\text{H}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}^T \right] \right) \cdot U_f \cdot \text{kroncker}(\text{H}, \text{kroncker}(\text{H}, \text{I}))$$

$$\text{QuantumCircuit} \cdot \Psi_{\text{in}} = \begin{pmatrix} 0 \\ 0.5 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0.5 \end{pmatrix}$$

$$\begin{pmatrix} 0 \\ 0.5 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0.5 \end{pmatrix} = \frac{1}{2} \cdot \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Quantum Dense Coding

Quantum superdense coding reliably transmits two classical bits through an entangled pair of particles, even though only one member of the pair is handled by the sender.
Charles Bennett, Physics Today, October 1995, p. 27

This tutorial is based on Brad Rubin's "Superdense Coding" at the Wolfram Demonstration Project: <http://demonstrations.wolfram.com/SuperdenseCoding/>. The quantum circuit shown below impliments quantum dense coding. Alice and Bob share the entangled pair of photons in the Bell basis shown at the left. Alice encodes two classical bits of information (four possible messages) on her photon, and Bob subsequently reads her message by performing a Bell state measurement on the

modified entangled photon pair. In other words, although Alice encodes two bits on her photon Bob's readout requires a measurement involving both photons. In this example Alice sends $|11\rangle$ to Bob.

$$\begin{array}{ccccccc} \cdot & X^1 & \cdot & Z^1 & \cdot & \cdot & H \\ \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{pmatrix} & & \begin{pmatrix} 0 \\ 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \end{pmatrix} & & \begin{pmatrix} 0 \\ 1/\sqrt{2} \\ -1/\sqrt{2} \\ 0 \end{pmatrix} & | & \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \\ \cdot & I & \cdot & I & \cdot & \oplus & I \end{array} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The operation of the circuit is outlined in both matrix and algebraic format. The necessary truth tables and matrix operators are provided in the Appendix.

Matrix Method

$$H \otimes I \cdot \text{CNOT} \cdot Z \otimes I \cdot X \otimes I \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |11\rangle$$

Algebraic Method

$$\begin{aligned} \frac{|00\rangle + |11\rangle}{\sqrt{2}} &\xrightarrow{X^1 \otimes I} \frac{|10\rangle + |01\rangle}{\sqrt{2}} \xrightarrow{Z^1 \otimes I} \frac{-|10\rangle + |01\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{-|11\rangle + |01\rangle}{\sqrt{2}} \xrightarrow{H \otimes I} \frac{-(|0\rangle - |1\rangle)|1\rangle + (|0\rangle + |1\rangle)|1\rangle}{2} \\ &= |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{aligned}$$

Appendix:

Truth tables for the quantum circuit:

$$X = \text{NOT} \begin{pmatrix} 0 & \text{to} & 1 \\ 1 & \text{to} & 0 \end{pmatrix} \quad Z \begin{pmatrix} 0 & \text{to} & 0 \\ 1 & \text{to} & -1 \end{pmatrix} \quad H = \text{Hadamard} \begin{bmatrix} 0 & \text{to} & \frac{1}{\sqrt{2}} \cdot (0+1) \\ 1 & \text{to} & \frac{1}{\sqrt{2}} \cdot (0-1) \end{bmatrix} \quad \text{CNOT} \begin{pmatrix} 00 & \text{to} & 00 \\ 01 & \text{to} & 01 \\ 10 & \text{to} & 11 \\ 11 & \text{to} & 10 \end{pmatrix}$$

Circuit elements in matrix format:

$$I \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad H \equiv \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{CNOT} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Quantum Error Correction

This tutorial deals with quantum error correction as presented by Julian Brown on pages 274-278 in *The Quest for the Quantum Computer*. Brown's three-qubit example includes an input qubit and two ancillary qubits in the initial state $|\Psi_{00}\rangle$. This state is encoded and subsequently decoded, with the possibility that in between it acquires an error. The quantum circuit demonstrates how correction occurs if a qubit is flipped due to decoherence at the intermediate state.

The quantum gates required for the error correction algorithm are:

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{CNOT} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

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

$$\text{IToffoli} := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The encoding and decoding elements of the circuit in terms of these gates are shown in the appropriate place above the circuit diagram.

$$\begin{array}{cccccccccccccccc} \text{Encode} := \text{CnNOT} \cdot \text{kronecker}(\text{CNOT}, I) & & \text{Decode} := \text{IToffoli} \cdot \text{Encode} \\ \sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle & \dots & \cdot & \dots & \cdot & \dots & \text{E} & \dots & \cdot & \dots & \cdot & \dots & \oplus & \triangleright & \sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle \\ & & & & & & \text{R} & & & & & & & & \\ |0\rangle & \dots & \oplus & \dots & | & \dots & \text{R} & \dots & \oplus & \dots & | & \dots & \cdot & \triangleright & |0\rangle \text{ or } |1\rangle \\ & & & & & & \text{O} & & & & & & & & \\ |0\rangle & \dots & \dots & \dots & \oplus & \dots & \text{R} & \dots & \dots & \dots & | & \dots & \cdot & \triangleright & |0\rangle \text{ or } |1\rangle \end{array}$$

Given an initial state, the encoding step creates an entangled Bell state as demonstrated below.

Initial State

$$\left(\sqrt{\frac{1}{3}}\right) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Encode

$$\text{Encode} = \begin{pmatrix} \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.577 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0.816 \end{pmatrix}$$

Encoded state

$$\left(\sqrt{\frac{1}{3}}\right) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \left(\sqrt{\frac{2}{3}}\right) \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \end{pmatrix}$$

As an initial example, it is assumed that between encoding and decoding no errors are introduced to the encoded state. This case demonstrates that decoding simply returns the initial state. Subsequent to this the operation of the circuit when errors occur on each of the wires are examined. These cases demonstrate that the original state appears on the top wire at the completion of the error correction circuit.

No errors:

$$\begin{aligned} &\left(\sqrt{\frac{1}{3}}\right) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \left(\sqrt{\frac{2}{3}}\right) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \end{pmatrix} \\ &\text{Decode} \cdot \begin{pmatrix} 0.577 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0.816 \end{pmatrix} = \begin{pmatrix} 0.577 \\ 0 \\ 0 \\ 0 \\ 0.816 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \left(\sqrt{\frac{1}{3}}\right) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \\ 0 \\ 0 \end{pmatrix} \end{aligned}$$

Next it is shown that if the input state, $|\Psi\rangle$, is corrupted that the decoder corrects the error and returns the original $|\Psi\rangle$ to the top wire of the circuit. In the example shown below the top qubit is flipped.

Top qubit flipped:

$$\begin{pmatrix} 0 \\ \sqrt{\frac{1}{3}} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} \sqrt{\frac{2}{3}} \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \\ \sqrt{\frac{1}{3}} \\ 0 \\ 0 \end{pmatrix} \quad \text{Decode} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \\ \sqrt{\frac{1}{3}} \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0.577 \\ 0 \\ 0 \\ 0.816 \end{pmatrix}$$

$$\begin{pmatrix} \sqrt{\frac{1}{3}} \\ \sqrt{\frac{2}{3}} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \end{pmatrix}$$

The circuit can also be expressed using Dirac notation. Truth tables for the gates are provided in the Appendix.

$$\begin{aligned} & \left(\sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle \right) |00\rangle \xrightarrow{\text{encode}} \sqrt{\frac{1}{3}}|000\rangle + \sqrt{\frac{2}{3}}|111\rangle \xrightarrow[\text{qubit}]{\text{flip top}} \sqrt{\frac{1}{3}}|100\rangle + \sqrt{\frac{2}{3}}|011\rangle \xrightarrow{\text{CNOT, I}} \sqrt{\frac{1}{3}}|110\rangle \\ & + \sqrt{\frac{2}{3}}|011\rangle \xrightarrow{\text{CnNOT}} \sqrt{\frac{1}{3}}|111\rangle + \sqrt{\frac{2}{3}}|011\rangle \xrightarrow{\text{InToffoli}} \sqrt{\frac{1}{3}}|011\rangle + \sqrt{\frac{2}{3}}|111\rangle = \left(\sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle \right) |11\rangle \end{aligned}$$

Naturally the ancillary qubits are also susceptible to errors. The following examples show that if a qubit flip occurs on the middle or bottom wire, the circuit still functions properly.

Middle qubit flipped:

$$\begin{pmatrix} \sqrt{\frac{1}{3}} \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \sqrt{\frac{2}{3}} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \\ 0 \\ 0 \end{pmatrix} \quad \text{Decode} \cdot \begin{pmatrix} 0 \\ 0 \\ \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0.577 \\ 0 \\ 0 \\ 0 \\ 0.816 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} \sqrt{\frac{1}{3}} \\ \sqrt{\frac{2}{3}} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \\ 0 \end{pmatrix}$$

$$\begin{aligned} \left(\sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle \right) |00\rangle &\xrightarrow{\text{encode}} \sqrt{\frac{1}{3}}|000\rangle + \sqrt{\frac{2}{3}}|111\rangle \xrightarrow[\text{qubit}]{\text{flip middle}} \sqrt{\frac{1}{3}}|010\rangle + \sqrt{\frac{2}{3}}|101\rangle \xrightarrow{\text{CNOT, I}} \sqrt{\frac{1}{3}}|010\rangle \\ &\xrightarrow{\text{CnNOT}} \sqrt{\frac{1}{3}}|010\rangle + \sqrt{\frac{2}{3}}|110\rangle \xrightarrow{\text{InTofoli}} \sqrt{\frac{1}{3}}|010\rangle + \sqrt{\frac{2}{3}}|110\rangle = \left(\sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle \right) |10\rangle \end{aligned}$$

Bottom qubit flipped:

$$\begin{pmatrix} \sqrt{\frac{1}{3}} \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ \sqrt{\frac{2}{3}} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \\ 0 \end{pmatrix} \quad \text{Decode} \cdot \begin{pmatrix} 0 \\ \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0.577 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0.816 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} \sqrt{\frac{1}{3}} \\ \sqrt{\frac{2}{3}} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \sqrt{\frac{1}{3}} \\ 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{\frac{2}{3}} \\ 0 \end{pmatrix}$$

$$\begin{aligned} \left(\sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle \right) |00\rangle &\xrightarrow{\text{encode}} \sqrt{\frac{1}{3}}|000\rangle + \sqrt{\frac{2}{3}}|111\rangle \xrightarrow[\text{quibt}]{\text{flip bottom}} \sqrt{\frac{1}{3}}|001\rangle + \sqrt{\frac{2}{3}}|110\rangle \xrightarrow{\text{CNOT, I}} \sqrt{\frac{1}{3}}|001\rangle \\ &+ \sqrt{\frac{2}{3}}|100\rangle \xrightarrow{\text{CnNOT}} \sqrt{\frac{1}{3}}|001\rangle + \sqrt{\frac{2}{3}}|101\rangle \xrightarrow{\text{InTofoli}} \sqrt{\frac{1}{3}}|001\rangle + \sqrt{\frac{2}{3}}|101\rangle = \left(\sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle \right) |01\rangle \end{aligned}$$

Appendix:

CNOT

Decimal	Binary	to	Binary	Decimal
0	00	to	00	0
1	01	to	01	1
2	10	to	11	3
3	11	to	10	2

CnNOT

Decimal	Binary	to	Binary	Decimal
0	000	to	000	0
1	001	to	001	1
2	010	to	010	2
3	011	to	011	3
4	100	to	101	5
5	101	to	100	4
6	110	to	111	7
7	111	to	110	6

IToffoli

Decimal	Binary	to	Binary	Decimal
0	000	to	000	0
1	001	to	001	1
2	010	to	010	2
3	011	to	111	7
4	100	to	100	4
5	101	to	101	5
6	110	to	110	6
7	111	to	011	3

And now we move to Bell's theorem and the battle between local realism and quantum mechanics.

Quantum theory is both stupendously successful as an account of the small-scale structure of the world and it is also the subject of unresolved debate and dispute about its interpretation. J. C. Polkinghorne, The Quantum World.

So we end this short course with the conflict between quantum mechanics and the classical view of reality held by Einstein and others known as local realism. Until the work of John Bell this battle was regarded by most scientists as a distracting philosophical debate. According to David Mermin quantum physicists were admonished to ignore the debate and "Shut up and calculate!"

In 1964 Bell demonstrated that experiments were possible for which quantum theory and local realism gave conflicting predictions, thus moving the disagreement from the realm of philosophical debate to the jurisdiction of the laboratory. In *Where Does the Weirdness Go?* David Lindley summarized Bell's achievement.

The hallmark of Bell's work was his success in locating precisely the point at which classical views of reality ran into trouble with quantum mechanics, and in devising a means by which the two viewpoints could be empirically compared. Bell's sympathies seem often to have lain with Bohm and the effort to establish a hidden variables version of quantum mechanics. His greatest achievement, though, was to demonstrate incontrovertibly the price that must be paid to make such a theory work.

Bell said that if a theory of reality was local it would not agree with quantum mechanics, and if it agreed with quantum mechanics it would contain non-local interactions, in other words “spooky interactions at a distance” to use Einstein’s phrase. Here’s the best description of this spookiness that I have read: “A non-local interaction links up one location with another without crossing space, without decay, and without delay. A non-local event is, in short, unmediated, unmitigated and immediate.” Nick Herbert, *Quantum Reality*, page 214.

In 1981 Richard Feynman gave a lecture titled “Simulating Nature with Computers.” His thesis was that the simulation of nature at the nanoscopic level required a quantum computer. “I’m not happy with all the analyses that go with just the classical theory, because nature isn’t classical, dammit. And if you want to make a simulation of nature, you’d better make it quantum mechanical ...”

This page titled [1.10: Quantum Computation- A Short Course](#) is shared under a [CC BY 4.0](#) license and was authored, remixed, and/or curated by [Frank Rioux](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.