8.74: 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: $\mathrm{f(x) = f(x') = f(x \oplus s)}$, 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.

$$\begin{array}{ccccc} \text{Decimal} & \text{Binary} & & \text{Binary} & \text{Decimal} \\ |0\rangle & |000\rangle & \xrightarrow{f(0)} & |011\rangle & |3\rangle \\ |1\rangle & |001\rangle & \xrightarrow{f(1)} & |001\rangle & |1\rangle \\ |2\rangle & |010\rangle & \xrightarrow{f(2)} & |010\rangle & |2\rangle \\ |3\rangle & |011\rangle & \xrightarrow{f(3)} & |000\rangle & |0\rangle \\ |4\rangle & |100\rangle & \xrightarrow{f(4)} & |001\rangle & |1\rangle \\ |5\rangle & |101\rangle & \xrightarrow{f(5)} & |011\rangle & |3\rangle \\ |6\rangle & |110\rangle & \xrightarrow{f(6)} & |010\rangle & |2\rangle \end{array}$$

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

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.

$$\begin{pmatrix} \mathrm{x} & 0 & 1 & 2 & 3 \\ \mathrm{f(x)} & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{array}{cccccccccccccccc} \text{Initial} & & 1 & & 2 & & 3 & & 4 & & 5 & & \text{Final} \\ |0\rangle & \triangleright & \boxed{\mathrm{H}} & \cdots & \cdot & \cdots & \cdots & \cdots & \cdots & \cdots & \boxed{\mathrm{H}} & \triangleright & \\ & & & & | & & & & & & & & \\ |0\rangle & \triangleright & \boxed{\mathrm{H}} & \cdots & | & \cdots & \cdot & \cdots & \cdots & \cdots & \boxed{\mathrm{H}} & \triangleright & \\ & & & & | & & | & & & & & & \\ |0\rangle & \triangleright & \cdots & \cdots & \oplus & \cdots & \oplus & \cdots & \boxed{\mathrm{NOT}} & \cdots & \cdots & \triangleright & \text{Measure, 0 or 1} \end{array}$$

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> = |11>.

$$\begin{array}{ccccc} \text{Decimal} & \text{Binary} & & \text{Binary} & \text{Decimal} \\ |0\rangle & |00\rangle & \xrightarrow{f(0)} & |01\rangle & |1\rangle \\ |1\rangle & |01\rangle & \xrightarrow{f(1)} & |00\rangle & |0\rangle \\ |2\rangle & |10\rangle & \xrightarrow{f(2)} & |00\rangle & |0\rangle \\ |3\rangle & |11\rangle & \xrightarrow{f(3)} & |01\rangle & |1\rangle \end{array}$$

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

$$\mathrm{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \mathrm{NOT} = \begin{pmatrix} 0 & 1\,1 & 0 \end{pmatrix} \quad \mathrm{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

The three qubit input state is: $\Psi_{in} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}^T$

The concealed algorithm: $\text{U}_\text{f} = \text{kronecker}(\text{I}, \text{kronecker}(\text{I}, \text{NOT}))\ \text{kronecker}(\text{I}, \text{CNOT})\ \text{CnNOT}$

The complete quantum circuit: $\text{QuantumCircuit} = \text{kronecker}(\text{H}, \text{kronecker}(\text{H}, \text{kronecker}(\text{H}, \text{I}))\ \text{U}_\text{f}\ \text{kronecker}(\text{H}, \text{kronecker}(\text{H}, \text{I}))$

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

$$\text{QuantumCircuit}\Psi_{in}$$

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

$$= \frac{1}{2}[|00\rangle - |11\rangle]\,|0\rangle + \frac{1}{2}[|00\rangle + |11\rangle]\,|1\rangle$$

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> = |11>. 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 quibits through the quantum circuit.

$$\text{NOT} \quad \begin{pmatrix} 0 & ' & 1 \\ 1 & ' & 0 \end{pmatrix}$$

$$\text{CNOT} \quad \begin{pmatrix} \text{Decimal} & \text{Binary} & ' & \text{Binary} & \text{Decimal} \\ 0 & 00 & ' & 00 & 0 \\ 1 & 01 & ' & 01 & 1 \\ 2 & 10 & ' & 11 & 3 \\ 3 & 11 & ' & 10 & 2 \end{pmatrix}$$

$$\text{CnNOT} \quad \begin{pmatrix} \text{Decimal} & \text{Binary} & ' & \text{Binary} & \text{Decimal} \\ 0 & 000 & ' & 000 & 0 \\ 1 & 001 & ' & 001 & 1 \\ 2 & 010 & ' & 010 & 2 \\ 3 & 011 & ' & 011 & 3 \\ 4 & 100 & ' & 101 & 5 \\ 5 & 101 & ' & 100 & 4 \\ 6 & 110 & ' & 111 & 7 \\ 7 & 111 & ' & 110 & 6 \end{pmatrix}$$

$$\text{Hadamard operation:} \quad \begin{bmatrix} 0 & ' & \text{H} & ' & \frac{1}{\sqrt{2}}(0+1) & ' & \text{H} & ' & 0 \\ 1 & ' & \text{H} & ' & \frac{1}{\sqrt{2}}(0-1) & ' & \text{H} & ' & 1 \end{bmatrix}$$

$$|000\rangle$$
$$\mathrm{H} \otimes \mathrm{H} \otimes \mathrm{I}$$
$$\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]\,\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]\,|0\rangle = \frac{1}{2}[|000\rangle + |010\rangle + |100\rangle + |110\rangle]$$
$$\mathrm{CnNOT}$$
$$\frac{1}{2}[|000\rangle + |010\rangle + |101\rangle + |111\rangle]$$
$$\mathrm{I} \otimes \mathrm{CNOT}$$
$$\frac{1}{2}[|000\rangle + |011\rangle + |101\rangle + |110\rangle]$$
$$\mathrm{I} \otimes \mathrm{I} \otimes \mathrm{NOT}$$
$$\frac{1}{2}[|001\rangle + |010\rangle + |100\rangle + |111\rangle]$$
$$\mathrm{H} \otimes \mathrm{H} \otimes \mathrm{I}$$
$$\frac{1}{2}[(|00\rangle - |11\rangle)\,|0\rangle + (|00\rangle + |11\rangle)\,|1\rangle]$$

Appendix

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

Measure |0> on the bottom wire:

$$\mathrm{QuantumCircuit} = \mathrm{kronecker}\left[\mathrm{H},\ \mathrm{kronecker}\left[\mathrm{H},\ \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}^T\right]\right]\mathrm{U}_f\mathrm{kronecker}(\mathrm{H},\ \mathrm{kronecker}(\mathrm{H},\ \mathrm{I}))$$

$$\mathrm{QuantumCircuit}\Psi_{in} = \begin{pmatrix}0.5\\0\\0\\0\\0\\0\\-0.5\\0\end{pmatrix}\quad\begin{pmatrix}0.5\\0\\0\\0\\0\\0\\-0.5\\0\end{pmatrix} = \frac{1}{2}\left[\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\right]\begin{pmatrix}1\\0\end{pmatrix}$$

Measure |1> on the bottom wire:

$$\mathrm{QuantumCircuit} = \mathrm{kronecker}\left[\mathrm{H},\ \mathrm{kronecker}\left[\mathrm{H},\ \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}^T\right]\right]\mathrm{U}_f\mathrm{kronecker}(\mathrm{H},\ \mathrm{kronecker}(\mathrm{H},\ \mathrm{I}))$$

$$\mathrm{QuantumCircuit}\Psi_{in} = \begin{pmatrix}0\\0.5\\0\\0\\0\\0\\0\\0.5\end{pmatrix}\quad\begin{pmatrix}0\\0.5\\0\\0\\0\\0\\0\\0.5\end{pmatrix} = \frac{1}{2}\left[\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\right]\begin{pmatrix}0\\1\end{pmatrix}$$