This paper follows a lecture Peter Shor has given at

https://openlearninglibrary.mit.edu/courses/course-v1:MITx+8.370.2x+1T2018/courseware/Week2/lectures_U2_3_simons_alg/?child=last

In the first part we use a simple function $f(x): \{0\ 1\} \times \{0\ 1\} \rightarrow \{0\ 1\} \times \{0\ 1\}$ and examine the case the function is $1:1$ and the case the function is $2:1$.

$1:1$ the function is bijective, $f(x_1) \neq f(x_2)$ for $x_1 \neq x_2$.

$2:1$ there exists a constant c with: $f(x) = f(x \oplus c)$.

Note: $\oplus =$ addition modulo 2.

We work through the first part on conceptual level as well as on basic level.

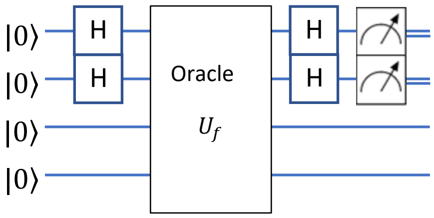
In the second part we use a more elaborated function:

$$f(x): \{0\ 1\} \times \{0\ 1\} \times \ldots \times \{0\ 1\} \rightarrow \{0\ 1\} \times \{0\ 1\} \times \ldots \times \{0\ 1\}$$

We go through the process again, this time only on conceptual level and try to generalize it.

Simple example, conceptual level

For our example we use the following circuit:



Note: The oracle takes the first two qubits as input but modifies the second two qubits only.

We use a function $\boldsymbol{f(x)}$: $\{\mathbf{0}\ \mathbf{1}\} \times \{\mathbf{0}\ \mathbf{1}\} \rightarrow \{\mathbf{0}\ \mathbf{1}\} \times \{\mathbf{0}\ \mathbf{1}\}$:

$f(00) = 01$	$f(01) = 10$	$f(10) = 11$	$f(11) = 00$

Obviously f is $1:1$, the constant $c = 00$, $f(x) = f(x \oplus c)$.

For information only: The matrix for this function (shortform):

$$
\begin{array}{cc|c}
 & & f(x) \\
 & & \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\
\hline
x & \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}
\end{array}
$$

Note: This is a typical permutation matrix with a single "1" in every row/column. This matrix is equivalent to the identity matrix and in the end we have no oracle at all.

Note: You find the complete matrix in the basic level.

We start with input $|0000\rangle$.

We apply the Hadamards:

$$\frac{1}{2}\big((|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|00\rangle\big) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)|00\rangle =$$

$$\frac{1}{2}(|0000\rangle + |0100\rangle + |1000\rangle + |1100\rangle)$$

We apply the oracle, using our example function above:

$$\frac{1}{2}(|0001\rangle + |0110\rangle + |1011\rangle + |1100\rangle)$$

We apply the Hadamards after the oracle a second time. This results in:

$$\frac{1}{4}\big((|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|01\rangle + (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)|10\rangle + (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)|11\rangle + (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)|00\rangle\big)$$

We expand the products and get:

$$\frac{1}{4}(|0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle - |0100\rangle + |0101\rangle - |0110\rangle + |0111\rangle - |1000\rangle + |1001\rangle + |1010\rangle - |1011\rangle + |1100\rangle + |1101\rangle - |1110\rangle - |1111\rangle)$$

We collect the first two qubits:

$$\frac{1}{4}\big(|00\rangle(|00\rangle + |01\rangle + |10\rangle + |11\rangle) - |01\rangle(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \\ - |10\rangle(|00\rangle - |01\rangle - |10\rangle + |11\rangle) + |11\rangle(|00\rangle + |01\rangle - |10\rangle - |11\rangle)\big)$$

We get probabilities:

$|00\rangle > 0$	$|01\rangle > 0$	$|10\rangle > 0$	$|11\rangle > 0$

We achieved no reduction and assume the function is $1{:}\,1$.

We change the function to:

$f(00) = 00$	$f(01) = 01$	$f(10) = 00$	$f(11) = 01$

Obviously f is $2{:}\,1$, the constant $c = 10$: $f(x) = f(x \oplus c)$

For information only: The matrix for this function (shortform):

$$\begin{array}{c|c} & f(x) \\ & \begin{matrix} 00 & 01 & 10 & 11 \end{matrix} \\ \hline x \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

Note: The matrix is not of full rank 4×4.

Note: You find the complete matrix in the basic level.

We start with input $|0000\rangle$.

We apply the Hadamards:

$$\frac{1}{2}\big((|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|00\rangle\big) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)|00\rangle =$$

$$\frac{1}{2}(|0000\rangle + |0100\rangle + |1000\rangle + |1100\rangle)$$

Note: The oracle takes the first two qubits as input but modifies the second two qubits only.

We apply the oracle, using our example function above:

$$\frac{1}{2}(|0000\rangle + |0101\rangle + |1000\rangle + |1101\rangle)$$

We apply the Hadamards after the oracle a second time. This results in:

$$\frac{1}{4}\big((|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|00\rangle + (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)|01\rangle + (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)|00\rangle \\ + (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)|01\rangle\big)$$

We expand the products and get:

$$\frac{1}{4}(|0000\rangle + |0100\rangle + |1000\rangle + |1100\rangle + |0001\rangle - |0101\rangle + |1001\rangle - |1101\rangle + |0000\rangle + |0100\rangle \\ - |1000\rangle - |1100\rangle + |0001\rangle - |0101\rangle - |1001\rangle + |1101\rangle) =$$

$$\frac{1}{2}(|0000\rangle + |0100\rangle + |0001\rangle - |0101\rangle)$$

We collect the first two qubits:

$$\frac{1}{2}\big(|00\rangle(|00\rangle + |01\rangle) + |01\rangle(|00\rangle - |01\rangle)\big)$$

We get probabilities:

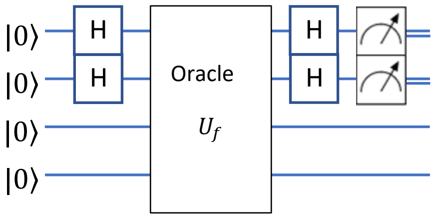
$\|00\rangle > 0$	$\|01\rangle > 0$	$\|10\rangle = 0$	$\|11\rangle = 0$

As 00 is no valid value for c we got the result $c = 01$.

We achieved reduction and assume the function is $2:1$.

Simple example, basic level

We use the circuit above:



We work with the $1:1$ function

The first Hadamards applied to the input vector:

$$\frac{1}{2}\begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 \\
1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1
\end{pmatrix}
\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}
= \frac{1}{2}\begin{pmatrix}1\\0\\0\\0\\1\\0\\0\\0\\1\\0\\0\\0\\1\\0\\0\\0\end{pmatrix}$$

We construct the oracle.

We use the function:

$f(00) = 01$	$f(01) = 10$	$f(10) = 11$	$f(11) = 00$

The oracle acts:

$\|0000\rangle \to \|0001\rangle$	$\|0001\rangle \to \|0000\rangle$	$\|0010\rangle \to \|0011\rangle$	$\|0011\rangle \to \|0010\rangle$
$\|0100\rangle \to \|0110\rangle$	$\|0101\rangle \to \|0111\rangle$	$\|0110\rangle \to \|0100\rangle$	$\|0111\rangle \to \|0101\rangle$
$\|1000\rangle \to \|1011\rangle$	$\|1001\rangle \to \|1010\rangle$	$\|1010\rangle \to \|1001\rangle$	$\|1011\rangle \to \|1000\rangle$
$\|1100\rangle \to \|1100\rangle$	$\|1101\rangle \to \|1101\rangle$	$\|1110\rangle \to \|1110\rangle$	$\|1111\rangle \to \|1111\rangle$

We construct the oracle from the conceptual level:

$$
\begin{array}{cc}
 & \begin{array}{cccccccccccccccc} |0000\rangle & & & & & & & & & & & & & & & |1111\rangle \ \text{output} \\ \downarrow & & & & & & & & & & & & & & & \downarrow \end{array} \\
\begin{array}{c} |0000\rangle \rightarrow \\ \\ \\ \\ \\ \\ \\ \text{input} \\ \\ \\ \\ \\ \\ \\ \\ |1111\rangle \rightarrow \end{array} &
\begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\end{array}
$$

We apply the oracle:

$$
\begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\frac{1}{2}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}
= \frac{1}{2}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}
$$

We apply the Hadamards again:

$$
\frac{1}{2}\begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 \\
1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1
\end{pmatrix}
\frac{1}{2}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}
= \frac{1}{4}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ 1 \\ -1 \\ 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}
$$

We compare with the result from the conceptual level. There we got:

$$
\frac{1}{4}(|0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle - |0100\rangle + |0101\rangle - |0110\rangle + |0111\rangle - |1000\rangle + |1001\rangle + |1010\rangle - |1011\rangle + |1100\rangle + |1101\rangle - |1110\rangle - |1111\rangle)
$$

These are 16 basis vectors, we build them with the appropriate signs:

$$\frac{1}{4}\begin{pmatrix}1\\1\\1\\1\\-1\\1\\-1\\1\\-1\\1\\1\\-1\\1\\1\\-1\\-1\end{pmatrix}$$

Both results match. The probability to measure one of the basis vectors is $\left(\frac{1}{4}\right)^2$, we achieved no reduction in probability.

We work with the $2:1$ function.

The first Hadamards applied to the input vector:

$$\frac{1}{2}\begin{pmatrix}
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
1&0&0&0&-1&0&0&0&1&0&0&0&-1&0&0&0\\
0&1&0&0&0&-1&0&0&0&1&0&0&0&-1&0&0\\
0&0&1&0&0&0&-1&0&0&0&1&0&0&0&-1&0\\
0&0&0&1&0&0&0&-1&0&0&0&1&0&0&0&-1\\
1&0&0&0&1&0&0&0&-1&0&0&0&-1&0&0&0\\
0&1&0&0&0&1&0&0&0&-1&0&0&0&-1&0&0\\
0&0&1&0&0&0&1&0&0&0&-1&0&0&0&-1&0\\
0&0&0&1&0&0&0&1&0&0&0&-1&0&0&0&-1\\
1&0&0&0&-1&0&0&0&-1&0&0&0&1&0&0&0\\
0&1&0&0&0&-1&0&0&0&-1&0&0&0&1&0&0\\
0&0&1&0&0&0&-1&0&0&0&-1&0&0&0&1&0\\
0&0&0&1&0&0&0&-1&0&0&0&-1&0&0&0&1
\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1\\0\\0\\0\\1\\0\\0\\0\\1\\0\\0\\0\\1\\0\\0\\0\end{pmatrix}$$

We construct the oracle.

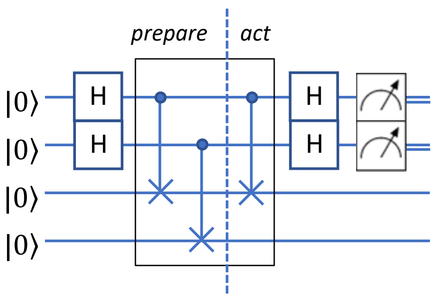
We use the function:

$f(00) = 00$	$f(01) = 01$	$f(10) = 00$	$f(11) = 01$

The constant or "secret string" $s := 10$

$$f(x) = f(x \oplus 10)$$

We apply the oracle:



The logic behind the scheme:

1. We place a CNOT on every pair of qubits – we prepare the calculation.
2. We search for the first "1" in the secret string. This defines the control line.
3. For every "1" in the secret string we place a CNOT between the control line and the target qubits – we are acting.

The oracle acts:

$\|0000\rangle \rightarrow \|0000\rangle$	$\|0001\rangle \rightarrow \|0001\rangle$	$\|0010\rangle \rightarrow \|0010\rangle$	$\|0011\rangle \rightarrow \|0011\rangle$
$\|0100\rangle \rightarrow \|0101\rangle$	$\|0101\rangle \rightarrow \|0100\rangle$	$\|0110\rangle \rightarrow \|0111\rangle$	$\|0111\rangle \rightarrow \|0110\rangle$
$\|1000\rangle \rightarrow \|1000\rangle$	$\|1001\rangle \rightarrow \|1001\rangle$	$\|1010\rangle \rightarrow \|1010\rangle$	$\|1011\rangle \rightarrow \|1011\rangle$
$\|1100\rangle \rightarrow \|1101\rangle$	$\|1101\rangle \rightarrow \|1100\rangle$	$\|1110\rangle \rightarrow \|1111\rangle$	$\|1111\rangle \rightarrow \|1110\rangle$

We construct the oracle from the conceptual level:

$$
\begin{array}{cc}
 & \begin{array}{cccccccccccccccc} 0000 & 0001 & 0010 & 0011 & 0100 & 0101 & 0110 & 0111 & 1000 & 1001 & 1010 & 1011 & 1100 & 1101 & 1110 & 1111 \end{array} \quad \text{output} \\
\text{input}\ \begin{pmatrix} 0000\\0001\\0010\\0011\\0100\\0101\\0110\\0111\\1000\\1001\\1010\\1011\\1100\\1101\\1110\\1111 \end{pmatrix} \rightarrow &
\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0
\end{pmatrix}
\end{array}
$$

Note: This looks like a CNOT from qubit 2 to qubit 4. In fact, that is what remains from the three CNOTs, because the first CNOT and the third CNOT cancel. A CNOT applied to itself gives the identity matrix.

Note: We can shift operators in the circuit from left to right as long as we do not cross "hot spots".

We construct the matrices:

CNOT one

$$\text{input}\quad \begin{pmatrix}0000\\0001\\0010\\0011\\0100\\0101\\0110\\0111\\1000\\1001\\1010\\1011\\1100\\1101\\1110\\1111\end{pmatrix} \rightarrow \begin{array}{c} \begin{array}{cccccccccccccccc} 0000 & 0001 & 0010 & 0011 & 0100 & 0101 & 0110 & 0111 & 1000 & 1001 & 1010 & 1011 & 1100 & 1101 & 1110 & 1111 \end{array} \\ \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0
\end{pmatrix}\end{array}\quad \text{output}$$

CNOT two

$$\text{input}\quad \begin{pmatrix}0000\\0001\\0010\\0011\\0100\\0101\\0110\\0111\\1000\\1001\\1010\\1011\\1100\\1101\\1110\\1111\end{pmatrix} \rightarrow \begin{array}{c} \begin{array}{cccccccccccccccc} 0000 & 0001 & 0010 & 0011 & 0100 & 0101 & 0110 & 0111 & 1000 & 1001 & 1010 & 1011 & 1100 & 1101 & 1110 & 1111 \end{array} \\ \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0
\end{pmatrix}\end{array}\quad \text{output}$$

CNOT three is the same as CNOT one.

We build the matrix product: $(CNOT\ one) \cdot (CNOT\ two) \cdot (CNOT\ one)$:

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

This is the same matrix we constructed from the conceptual level.

We apply the oracle:

$$\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0
\end{pmatrix}
\frac{1}{2}\begin{pmatrix}1\\0\\0\\0\\1\\0\\0\\0\\1\\0\\0\\0\\1\\0\\0\\0\end{pmatrix}
=\frac{1}{2}\begin{pmatrix}1\\0\\0\\0\\0\\1\\0\\0\\1\\0\\0\\0\\0\\1\\0\\0\end{pmatrix}$$

We apply the Hadamards again:

$$\frac{1}{2}\begin{pmatrix}
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
1&0&0&0&-1&0&0&0&1&0&0&0&-1&0&0&0\\
0&1&0&0&0&-1&0&0&0&1&0&0&0&-1&0&0\\
0&0&1&0&0&0&-1&0&0&0&1&0&0&0&-1&0\\
0&0&0&1&0&0&0&-1&0&0&0&1&0&0&0&-1\\
1&0&0&0&1&0&0&0&-1&0&0&0&-1&0&0&0\\
0&1&0&0&0&1&0&0&0&-1&0&0&0&-1&0&0\\
0&0&1&0&0&0&1&0&0&0&-1&0&0&0&-1&0\\
0&0&0&1&0&0&0&1&0&0&0&-1&0&0&0&-1\\
1&0&0&0&-1&0&0&0&-1&0&0&0&1&0&0&0\\
0&1&0&0&0&-1&0&0&0&-1&0&0&0&1&0&0\\
0&0&1&0&0&0&-1&0&0&0&-1&0&0&0&1&0\\
0&0&0&1&0&0&0&-1&0&0&0&-1&0&0&0&1
\end{pmatrix}
\frac{1}{2}\begin{pmatrix}1\\0\\0\\0\\0\\1\\0\\0\\1\\0\\0\\0\\0\\1\\0\\0\end{pmatrix}
=\frac{1}{2}\begin{pmatrix}1\\1\\0\\0\\1\\-1\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}$$

We compare with the result from the conceptual level. There we got:

$$\frac{1}{2}(|0000\rangle + |0001\rangle + |0100\rangle - |0101\rangle)$$

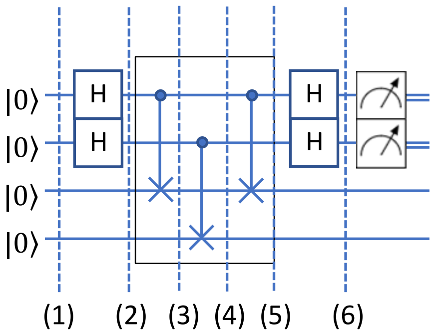
These are 4 basis vectors, we build them with the appropriate signs:

$$\begin{pmatrix} 00|00 \\ 00|01 \\ 00|10 \\ 00|11 \\ 01|00 \\ 01|01 \\ 01|10 \\ 01|11 \\ 10|00 \\ 10|01 \\ 10|10 \\ 10|11 \\ 11|00 \\ 11|01 \\ 11|10 \\ 11|11 \end{pmatrix} \to \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

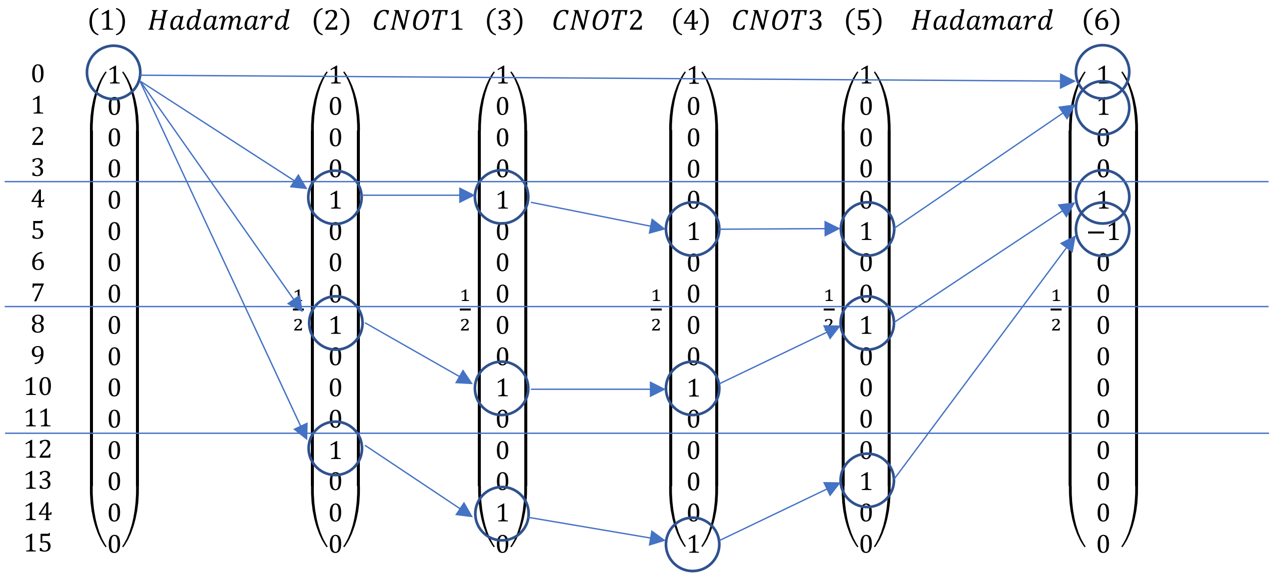
Both results match. We get a probability $\left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}\right)$ for vectors $|00\rangle$ and $|01\rangle$ and zero probability for vectors $|10\rangle$ and $|11\rangle$.

Basic level, slow motion

We take a closer look at the action of the oracle.



We take a look at how the input changes after each matrix:



The input is a single basis vector in position 0.

The first pair of Hadamards set the superposition, the positions $4, 8$ and 12.

The first CNOT moves position 8 to 10 and 12 to 14.

The second CNOT moves position 4 to 5 and 14 to 15.

The third CNOT shifts back position 10 to 8 and 15 to 13.

The last Hadamard "goes fail" and produces another superposition by shifting position $13, 8$ and 5 to 5,4 and 3.

Second part

We use a function

$$f(x): \{0\ 1\} \times \{0\ 1\} \times \dots \times \{0\ 1\} \to \{0\ 1\} \times \{0\ 1\} \times \dots \times \{0\ 1\}$$

Domain and range are bit strings of length n.

$f(x)$ is either $1:1$, bijective $x \neq y \to f(x) \neq f(y)$ or $f(x)$ is $2:1$ with $f(x) = f(x \oplus c)$.

$\oplus$ = addition modulo 2.

The task:

Determine which of the two options applies to f and, if applicable, determine the constant c.

Example:

$$f(x): \{0\ 1\}^4 \to \{0\ 1\}^4$$

x $\to$	$f(x)$	x $\to$	$f(x)$
$\{0000\}$	$\{1101\}$	$\{1000\}$	$\{1000\}$
$\{0001\}$	$\{0110\}$	$\{1001\}$	$\{1011\}$
$\{0010\}$	$\{0101\}$	$\{1010\}$	$\{1001\}$
$\{0011\}$	$\{1111\}$	$\{1011\}$	$\{0001\}$
$\{0100\}$	$\{0110\}$	$\{1100\}$	$\{1011\}$
$\{0101\}$	$\{1101\}$	$\{1101\}$	$\{1000\}$
$\{0110\}$	$\{1111\}$	$\{1110\}$	$\{0001\}$
$\{0111\}$	$\{0101\}$	$\{1111\}$	$\{1001\}$

The function is $2:1$, the constant $c = 0101$. c is often referred as "secret string".

Solving classically

We need to find one pair $f(x) = f(x \oplus s)$.

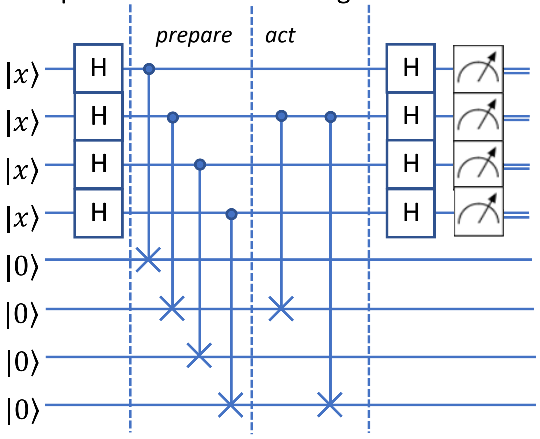
For n bits we have 2^n pairs $\left(x_i, f(x_i)\right)$.

Doing this in a deterministic way we need $\leq 2^{n-1} + 1$ queries to find c according to the pigeonhole principle: $\Theta(2^n)$

Probabilistic we need $\Theta\left(2^{\frac{n}{2}}\right)$ queries to get the solution with high probability.

Solving quantum

For our example we use the following circuit:



Note: double lines mean classical bits.

Note: $|x\rangle$ are the input values, ranging from $|0000\rangle$ to $|1111\rangle$.

Note: we need to apply this quantum circuit several times to compute c.

Note: The oracle takes the first four qubits as input but modifies the second four ones.

We start with input $|x\rangle|0\rangle = |01010000\rangle$.

We apply the Hadamards:

$$\frac{1}{\sqrt{2^4}}\big((|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)|0000\rangle\big) =$$

$$\frac{1}{4}(|0000\rangle - |0001\rangle + |0010\rangle - |0011\rangle - |0100\rangle + |0101\rangle - |0110\rangle + |0111\rangle + |1000\rangle - |1001\rangle$$
$$+ |1010\rangle - |1011\rangle - |1100\rangle + |1101\rangle - |1110\rangle + |1111\rangle)|0000\rangle =$$

$$\frac{1}{4}(|00000000\rangle - |00010000\rangle + |00100000\rangle - |00110000\rangle - |01000000\rangle + |01010000\rangle$$
$$- |01100000\rangle + |01110000\rangle + |10000000\rangle - |10010000\rangle + |10100000\rangle$$
$$- |10110000\rangle - |11000000\rangle + |11010000\rangle - |11100000\rangle + |11110000\rangle)$$

We apply the oracle, using our example function above:

$$\frac{1}{4}(|00001101\rangle - |00010110\rangle + |00100101\rangle - |00111111\rangle - |01000110\rangle + |01011101\rangle$$
$$- |01101111\rangle + |01110101\rangle + |10001000\rangle - |10011011\rangle + |10101001\rangle$$
$$- |10110001\rangle - |11001011\rangle + |11011000\rangle - |11100001\rangle + |11111001\rangle)$$

We apply the Hadamards after the oracle a second time. This results in:

$\frac{1}{16}[$
$+\big((\|0\rangle + \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle + \|1\rangle)\|1101\rangle\big)$
$-\big((\|0\rangle + \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle - \|1\rangle)\|0110\rangle\big)$
$+\big((\|0\rangle + \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle - \|1\rangle)(\|0\rangle + \|1\rangle)\|0101\rangle\big)$
$-\big((\|0\rangle + \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle - \|1\rangle)(\|0\rangle - \|1\rangle)\|1111\rangle\big)$
$-\big((\|0\rangle + \|1\rangle)(\|0\rangle - \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle + \|1\rangle)\|0110\rangle\big)$
$+\big((\|0\rangle + \|1\rangle)(\|0\rangle - \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle - \|1\rangle)\|1101\rangle\big)$
$-\big((\|0\rangle + \|1\rangle)(\|0\rangle - \|1\rangle)(\|0\rangle - \|1\rangle)(\|0\rangle + \|1\rangle)\|1111\rangle\big)$
$+\big((\|0\rangle + \|1\rangle)(\|0\rangle - \|1\rangle)(\|0\rangle - \|1\rangle)(\|0\rangle - \|1\rangle)\|0101\rangle\big)$
$+\big((\|0\rangle - \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle + \|1\rangle)\|1000\rangle\big)$
$+\big((\|0\rangle - \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle - \|1\rangle)\|1011\rangle\big)$
$+\big((\|0\rangle - \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle - \|1\rangle)(\|0\rangle + \|1\rangle)\|1001\rangle\big)$
$-\big((\|0\rangle - \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle - \|1\rangle)(\|0\rangle - \|1\rangle)\|0001\rangle\big)$
$-\big((\|0\rangle - \|1\rangle)(\|0\rangle - \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle + \|1\rangle)\|1011\rangle\big)$
$+\big((\|0\rangle - \|1\rangle)(\|0\rangle - \|1\rangle)(\|0\rangle + \|1\rangle)(\|0\rangle - \|1\rangle)\|1000\rangle\big)$

$-\big((\lvert 0\rangle - \lvert 1\rangle)(\lvert 0\rangle - \lvert 1\rangle)(\lvert 0\rangle - \lvert 1\rangle)(\lvert 0\rangle + \lvert 1\rangle)\lvert 0001\rangle\big)$
$+\big((\lvert 0\rangle - \lvert 1\rangle)(\lvert 0\rangle - \lvert 1\rangle)(\lvert 0\rangle - \lvert 1\rangle)(\lvert 0\rangle - \lvert 1\rangle)\lvert 1001\rangle\big)$
$]$

We expand the products and get:

$\frac{1}{16}[$
$\lvert 00001101\rangle + \lvert 00011101\rangle + \lvert 00101101\rangle + \lvert 00111101\rangle + \lvert 01001101\rangle + \lvert 01011101\rangle + \lvert 01101101\rangle + \lvert 01111101\rangle + \lvert 10001101\rangle + \lvert 10011101\rangle + \lvert 10101101\rangle + \lvert 10111101\rangle + \lvert 11001101\rangle + \lvert 11011101\rangle + \lvert 11101101\rangle + \lvert 11111101\rangle$
$-\lvert 00000110\rangle + \lvert 00010110\rangle - \lvert 00100110\rangle + \lvert 00110110\rangle - \lvert 01000110\rangle + \lvert 01010110\rangle - \lvert 01100110\rangle + \lvert 01110110\rangle - \lvert 10000110\rangle + \lvert 10010110\rangle - \lvert 10100110\rangle + \lvert 10110110\rangle - \lvert 11000110\rangle + \lvert 11010110\rangle - \lvert 11100110\rangle + \lvert 11110110\rangle$
$+\lvert 00000101\rangle + \lvert 00010101\rangle - \lvert 00100101\rangle - \lvert 00110101\rangle + \lvert 01000101\rangle + \lvert 01010101\rangle - \lvert 01100101\rangle - \lvert 01110101\rangle + \lvert 10000101\rangle + \lvert 10010101\rangle - \lvert 10100101\rangle - \lvert 10110101\rangle + \lvert 11000101\rangle + \lvert 11010101\rangle - \lvert 11100101\rangle - \lvert 11110101\rangle$
$-\lvert 00001111\rangle + \lvert 00011111\rangle + \lvert 00101111\rangle - \lvert 00111111\rangle - \lvert 01001111\rangle + \lvert 01011111\rangle + \lvert 01101111\rangle - \lvert 01111111\rangle - \lvert 10001111\rangle + \lvert 10011111\rangle + \lvert 10101111\rangle - \lvert 10111111\rangle - \lvert 11001111\rangle + \lvert 11011111\rangle + \lvert 11101111\rangle - \lvert 11111111\rangle$
$-\lvert 00000110\rangle - \lvert 00010110\rangle - \lvert 00100110\rangle - \lvert 00110110\rangle + \lvert 01000110\rangle + \lvert 01010110\rangle + \lvert 01100110\rangle + \lvert 01110110\rangle - \lvert 10000110\rangle - \lvert 10010110\rangle - \lvert 10100110\rangle + \lvert 10110110\rangle + \lvert 11000110\rangle + \lvert 11010110\rangle + \lvert 11100110\rangle + \lvert 11110110\rangle$
$+\lvert 00001101\rangle - \lvert 00011101\rangle + \lvert 00101101\rangle - \lvert 00111101\rangle - \lvert 01001101\rangle + \lvert 01011101\rangle - \lvert 01101101\rangle + \lvert 01111101\rangle + \lvert 10001101\rangle - \lvert 10011101\rangle + \lvert 10101101\rangle - \lvert 10111101\rangle - \lvert 11001101\rangle + \lvert 11011101\rangle - \lvert 11101101\rangle + \lvert 11111101\rangle$
$-\lvert 00001111\rangle - \lvert 00011111\rangle + \lvert 00101111\rangle + \lvert 00111111\rangle + \lvert 01001111\rangle + \lvert 01011111\rangle - \lvert 01101111\rangle - \lvert 01111111\rangle - \lvert 10001111\rangle - \lvert 10011111\rangle + \lvert 10101111\rangle + \lvert 10111111\rangle + \lvert 11001111\rangle + \lvert 11011111\rangle - \lvert 11101111\rangle - \lvert 11111111\rangle$
$+\lvert 00000101\rangle - \lvert 00010101\rangle - \lvert 00100101\rangle + \lvert 00110101\rangle - \lvert 01000101\rangle + \lvert 01010101\rangle + \lvert 01100101\rangle - \lvert 01110101\rangle + \lvert 10000101\rangle - \lvert 10010101\rangle - \lvert 10100101\rangle + \lvert 10110101\rangle - \lvert 11000101\rangle + \lvert 11010101\rangle + \lvert 11100101\rangle - \lvert 11110101\rangle$
$+\lvert 00001000\rangle + \lvert 00011000\rangle + \lvert 00101000\rangle + \lvert 00111000\rangle + \lvert 01001000\rangle + \lvert 01011000\rangle + \lvert 01101000\rangle + \lvert 01111000\rangle - \lvert 10001000\rangle - \lvert 10011000\rangle - \lvert 10101000\rangle - \lvert 10111000\rangle - \lvert 11001000\rangle - \lvert 11011000\rangle - \lvert 11101000\rangle - \lvert 11111000\rangle$
$+\lvert 00001011\rangle - \lvert 00011011\rangle + \lvert 00101011\rangle - \lvert 00111011\rangle + \lvert 01001011\rangle - \lvert 01011011\rangle + \lvert 01101011\rangle - \lvert 01111011\rangle - \lvert 10001011\rangle + \lvert 10011011\rangle - \lvert 10101011\rangle + \lvert 10111011\rangle - \lvert 11001011\rangle + \lvert 11011011\rangle - \lvert 11101011\rangle + \lvert 11111011\rangle$
$+\lvert 00001001\rangle + \lvert 00011001\rangle - \lvert 00101001\rangle - \lvert 00111001\rangle + \lvert 01001001\rangle + \lvert 01011001\rangle - \lvert 01101001\rangle - \lvert 01111001\rangle - \lvert 10001001\rangle - \lvert 10011001\rangle + \lvert 10101001\rangle + \lvert 10111001\rangle - \lvert 11001001\rangle - \lvert 11011001\rangle + \lvert 11101001\rangle + \lvert 11111001\rangle$
$-\lvert 00000001\rangle + \lvert 00010001\rangle + \lvert 00100001\rangle - \lvert 00110001\rangle - \lvert 01000001\rangle + \lvert 01010001\rangle + \lvert 01100001\rangle - \lvert 01110001\rangle + \lvert 10000001\rangle - \lvert 10010001\rangle - \lvert 10100001\rangle + \lvert 10110001\rangle + \lvert 11000001\rangle - \lvert 11010001\rangle - \lvert 11100001\rangle + \lvert 11110001\rangle$
$+\lvert 00001011\rangle + \lvert 00011011\rangle + \lvert 00101011\rangle + \lvert 00111011\rangle - \lvert 01001011\rangle - \lvert 01011011\rangle - \lvert 01101011\rangle - \lvert 01111011\rangle - \lvert 10001011\rangle - \lvert 10011011\rangle - \lvert 10101011\rangle - \lvert 10111011\rangle + \lvert 11001011\rangle + \lvert 11011011\rangle + \lvert 11101011\rangle + \lvert 11111011\rangle$
$+\lvert 00001000\rangle - \lvert 00011000\rangle + \lvert 00101000\rangle - \lvert 00111000\rangle - \lvert 01001000\rangle + \lvert 01011000\rangle - \lvert 01101000\rangle + \lvert 01111000\rangle - \lvert 10001000\rangle + \lvert 10011000\rangle - \lvert 10101000\rangle + \lvert 10111000\rangle + \lvert 11001000\rangle - \lvert 11011000\rangle + \lvert 11101000\rangle - \lvert 11111000\rangle$
$-\lvert 00000001\rangle - \lvert 00010001\rangle + \lvert 00100001\rangle + \lvert 00110001\rangle + \lvert 01000001\rangle + \lvert 01010001\rangle - \lvert 01100001\rangle - \lvert 01110001\rangle + \lvert 10000001\rangle + \lvert 10010001\rangle - \lvert 10100001\rangle - \lvert 10110001\rangle - \lvert 11000001\rangle - \lvert 11010001\rangle + \lvert 11100001\rangle + \lvert 11110001\rangle$
$+\lvert 00001001\rangle - \lvert 00011001\rangle - \lvert 00101001\rangle + \lvert 00111001\rangle - \lvert 01001001\rangle + \lvert 01011001\rangle + \lvert 01101001\rangle - \lvert 01111001\rangle - \lvert 10001001\rangle + \lvert 10011001\rangle + \lvert 10101001\rangle - \lvert 10111001\rangle + \lvert 11001001\rangle - \lvert 11011001\rangle - \lvert 11101001\rangle + \lvert 11111001\rangle$
$]$

Note: This is the sum:

$$\frac{1}{2^n}\sum_{\substack{x\in\{0,1\}^n\\ b\in\{0,1\}^n}}(-1)^{x\cdot b}\,|b\rangle|f(x)\rangle$$

We collect the first four qubits:

$$|0000\rangle(|1101\rangle-|0110\rangle+|0101\rangle-|1111\rangle-|0110\rangle+|1101\rangle-|1111\rangle+|0101\rangle+|1000\rangle$$
$$+|1011\rangle+|1001\rangle-|0001\rangle+|1011\rangle+|1000\rangle-|0001\rangle+|1001\rangle)=$$

$$2|0000\rangle(|1101\rangle-|0110\rangle+|0101\rangle-|1111\rangle+|1101\rangle+|1000\rangle+|1001\rangle-|0001\rangle)$$

The possibility for measuring $|0000\rangle$ is >0.

$$|0001\rangle(|1101\rangle+|0110\rangle+|0101\rangle+|1111\rangle-|0110\rangle-|1101\rangle-|1111\rangle-|0101\rangle+|1000\rangle$$
$$-|1011\rangle+|1001\rangle+|0001\rangle+|1011\rangle-|1000\rangle-|0001\rangle-|1001\rangle)=0$$

The possibility for measuring $|0001\rangle$ is zero.

We do this for the other qubits and get probabilities:

$\|0000\rangle > 0$	$\|0001\rangle \to 0$	$\|0010\rangle > 0$	$\|0011\rangle \to 0$
$\|0100\rangle \to 0$	$\|0101\rangle > 0$	$\|0110\rangle \to 0$	$\|0111\rangle > 0$
$\|1000\rangle > 0$	$\|1001\rangle \to 0$	$\|1010\rangle > 0$	$\|1011\rangle \to 0$
$\|1100\rangle \to 0$	$\|1101\rangle > 0$	$\|1110\rangle \to 0$	$\|1111\rangle > 0$

The first run reduces the candidates for c from 15 to 7. Remember that $|0000\rangle$ is not a valid candidate because the function then would be $1:1$.

We generalize.

We apply the Hadamards $H^{\otimes n}|x\rangle$:

This is the inner product of x and b modulo 2.

$$H^{\otimes n}|x\rangle=\frac{1}{\sqrt{2^n}}\sum_{i=1}^{n}(-1)^{\sum_{i=1}^{n}x_ib_i}\,|b\rangle=$$

$$\frac{1}{\sqrt{2^n}}\sum_{b\in\{0,1\}^n}(-1)^{x\cdot b}\,|b\rangle$$

Note: $|x\rangle$ are the first four qubits, $|b\rangle$ are all qubits from $|0000\rangle$ to $|1111\rangle$.

Note: x is the input vector we chose randomly.

Note: $x\cdot b$ is the inner product of the string $|x\rangle$ and all possible values of a bit string $|b\rangle$ of length n.

Then the oracle is acting. It modifies the second half of the input. As we chose $|0000\rangle$ for input we get $|0000\oplus f(x)\rangle=|f(x)\rangle$.

We apply the Hadamards to the upper qubits $|b\rangle$:

$$H\left(\frac{1}{\sqrt{2^n}}\sum_{b\in\{0,1\}^n}(-1)^{x\cdot b}\,|b\rangle|f(x)\rangle\right)$$

We get:

$$\frac{1}{2^n} \sum_{\substack{x \in \{0,1\}^n \\ b \in \{0,1\}^n}} (-1)^{x \cdot b} \, |b\rangle |f(x)\rangle$$

We are measuring the upper part $|b\rangle$ of $|b\rangle|f(x)\rangle$. This gives an information about the type of function. We must repeat this with different qubits $|x\rangle$ to determine the type of function.

We group the terms giving the same $|b\rangle$ in the $|0\rangle/|1\rangle$ basis and square the coefficients of the basis elements. This way we get the probability of seeing $|b\rangle|f(x)\rangle$.

We remember that $|b\rangle|f(x)\rangle$ comes from two different sources: x_0 and $x_0 \oplus c$.

We calculate the coefficient of $|b\rangle|f(x)\rangle$:

$$\left|\frac{1}{2^n}\left((-1)^{x_0 \cdot b} + (-1)^{(x_0 \oplus c) \cdot b)}\right)\right|^2 = \left|\frac{1}{2^n}\left((-1)^{x_0 \cdot b} + (-1)^{x_0 \cdot b \oplus c \cdot b}\right)\right|^2 =$$

$$\left|\frac{1}{2^n}\left((-1)^{x_0 \cdot b} + (-1)^{x_0 \cdot b}(-1)^{c \cdot b}\right)\right|^2 = \left|\frac{1}{2^n}\left((-1)^{x_0 \cdot b}\left(1 + (-1)^{c \cdot b}\right)\right)\right|^2 =;$$

We note that $\left|\left((-1)^{x_0 \cdot b}\right)\right|^2$ always gives 1 and proceed:

$$\left|\frac{1}{2^n}\left(1 + (-1)^{c \cdot b}\right)\right|^2$$

If the inner product $c \cdot b = 0$ we get the probability $\frac{2^2}{2^{2n}} = 4^{1-n}$,
if the inner product $c \cdot b = 1$ we get 0.

Note that we calculate all by using $\oplus$.

Note: In our example we have 16 vectors b, we have 8 possibilities for $f(x)$ and half of the scalar products is zero. The total probability thus gives $4^{1-4} \cdot 16 \cdot 4 = 1$.

This gives one bit of information about c. We need n bit, so we need to repeat this n times.

We go back to the example and run the function three times.

We have 15 possible $c's$ because $c = 0000$ is not a valid value.

We might get:

$$b_1 = 0010, b_2 = 0111, b_3 = 1000$$

After each run the number of possible $c's$ reduces.

We build the scalar product of b_1 and all possible c-vectors. Note that all calculations are made modulo 2:

$(0010)\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=0$	$(0010)\begin{pmatrix}0\\0\\1\\0\end{pmatrix}=1$	$(0010)\begin{pmatrix}0\\0\\1\\1\end{pmatrix}=1$	$(0010)\begin{pmatrix}0\\1\\0\\0\end{pmatrix}=0$
$(0010)\begin{pmatrix}0\\1\\0\\1\end{pmatrix}=0$	$(0010)\begin{pmatrix}0\\1\\1\\0\end{pmatrix}=1$	$(0010)\begin{pmatrix}0\\1\\1\\1\end{pmatrix}=1$	$(0010)\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=0$
$(0010)\begin{pmatrix}1\\0\\0\\1\end{pmatrix}=0$	$(0010)\begin{pmatrix}1\\0\\1\\0\end{pmatrix}=1$	$(0010)\begin{pmatrix}1\\0\\1\\1\end{pmatrix}=1$	$(0010)\begin{pmatrix}1\\1\\0\\0\end{pmatrix}=0$
$(0010)\begin{pmatrix}1\\1\\0\\1\end{pmatrix}=0$	$(0010)\begin{pmatrix}1\\1\\1\\0\end{pmatrix}=1$	$(0010)\begin{pmatrix}1\\1\\1\\1\end{pmatrix}=1$	

We have 7 possible solutions for c.

We build the scalar product of b_2 and all possible c-vectors we got from the first pass. Note that all calculations are made modulo 2:

$(0111)\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=1$			$(0111)\begin{pmatrix}0\\1\\0\\0\end{pmatrix}=1$
$(0111)\begin{pmatrix}0\\1\\0\\1\end{pmatrix}=0$			$(0111)\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=0$
$(0111)\begin{pmatrix}1\\0\\0\\1\end{pmatrix}=1$			$(0111)\begin{pmatrix}1\\1\\0\\0\end{pmatrix}=1$
$(0111)\begin{pmatrix}1\\1\\0\\1\end{pmatrix}=0$			

The number of possible solutions reduces to 3.

We build the scalar product of b_3 and all possible c-vectors we got from the second pass. Note that all calculations are made modulo 2:

$(1000)\begin{pmatrix}0\\1\\0\\1\end{pmatrix}=0$			$(1000)\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=1$
$(1000)\begin{pmatrix}1\\1\\0\\1\end{pmatrix}=1$			

We get $c = 0101$.

Note: if the vectors b_i are not linear independent, we might get no reduction and use more trials so this is not a deterministic access.

We generalize this to an input of n bit.

In our example we had the reduction chain:

$\frac{15}{16}$ after the first trial, $\frac{7}{8}$ after the second trial, $\frac{3}{4}$ after the third trial. The fourth trial then brought the result.

For the n-bit case we get the converging chain:

$$\frac{2^n-1}{2^n}\cdot \ldots \cdot \frac{15}{16}\cdot\frac{7}{8}\cdot\frac{3}{4}=\left(1-\frac{1}{2^n}\right)\ldots\left(1-\frac{1}{16}\right)\left(1-\frac{1}{8}\right)\left(1-\frac{1}{4}\right)\sim$$

$$e^{-\frac{1}{2^n}}\cdot \ldots \cdot e^{-\frac{1}{16}}\cdot e^{-\frac{1}{8}}\cdot e^{-\frac{1}{4}}=e^{-\left(\frac{1}{2^n}+\frac{1}{2^2}\right)}=e^{-\frac{1}{4}}\sim 78\%$$

This is the probability to get the correct solution after n-1 trials for large n.

Notebooks

You find a jupyter notebook, dealing with simon’s algorithm, at:

https://github.com/amazon-braket/amazon-braket-examples/blob/main/examples/advanced_circuits_algorithms/Simons_Algorithm/Simons_Algorithm.ipynb

Note: You need simons_utils.py to run this notebook.

Note: You need to install the amazon-plugin via “pip install amazon-braket-sdk”.

Note: You find a copy of Simons_Algorithm.ipynb and simons_utils.py on this website too.

I would like to thank my students Alex Heinz, Luca Kölsch, Matthias Hospach and Simon Schaal who made this paper possible.