The Deutsch-Jozsa problem: de-quantisation and entanglement

Alastair A. Abbott

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

8 December 2015

Alexander Jansing, Brittany Zeo

SUNY POLYTECHNIC INSTITUTE

Definitions

What is *de-quantisation*?

> De-quantisation is taking a *quantum algorithm* and computing its *classical algorithm* counterpart.

Definitions

What is *de-quantisation*?

De-quantisation is taking a *quantum algorithm* and computing its *classical algorithm* counterpart.

Classical algorithms are algorithms that can be computed on a Turing machine.

Quantum algorithms are algorithms that can be computed by a sequence of unitary operators.

Definitions

What is *de-quantisation*?

De-quantisation is taking a *quantum algorithm* and computing its *classical algorithm* counterpart.

Classical algorithms are algorithms that can be computed on a Turing machine.

Quantum algorithms are algorithms that can be computed by a sequence of unitary operators.

The *oracle computational problem* means that an input is given and we use a black-box and the goal is to find something out about the black-box.

Deutsch's problem

Deutsch's problem considers a Boolean function

$$\mathfrak{f} : \{0,1\} \to \{0,1\},$$

and we're given an oracle to compute $\mathfrak{f}$. Deutsch's problem is to determine whether or not $\mathfrak{f}$ is balanced or constant in as few calls as possible.

Quantum Solution

Using only call to the quantum black-box computing $\mathfrak{f}$, we can determine with probability 1 if $\mathfrak{f}$ is balanced or constant.

The quantum black-box can be described as the unitary operator

$$U_{\mathfrak{f}}\big|x\big\rangle\big|y\big\rangle = \big|x\big\rangle\big|y \oplus \mathfrak{f}(x)\big\rangle.$$

Quantum Solution

Using only call to the quantum black-box computing $\mathfrak{f}$, we can determine with probability 1 if $\mathfrak{f}$ is balanced or constant.
The quantum black-box can be described as the unitary operator

$$U_{\mathfrak{f}}\left|x\right\rangle\left|y\right\rangle = \left|x\right\rangle\left|y \oplus \mathfrak{f}(x)\right\rangle.$$

Noting that

$$\begin{aligned} U_{\mathfrak{f}}(U_{\mathfrak{f}}\left|x\right\rangle\left|y\right\rangle) &= U_{\mathfrak{f}}\left|x\right\rangle\left|y \oplus \mathfrak{f}(x)\right\rangle = \left|x\right\rangle\left|y \oplus \mathfrak{f}(x) \oplus \mathfrak{f}(x)\right\rangle \\ &= \left|x\right\rangle\left|y\right\rangle, \end{aligned}$$

Quantum Solution

Using only call to the quantum black-box computing $\mathfrak{f}$, we can determine with probability 1 if $\mathfrak{f}$ is balanced or constant.
The quantum black-box can be described as the unitary operator

$$U_{\mathfrak{f}}\left|x\right\rangle\left|y\right\rangle = \left|x\right\rangle\left|y \oplus \mathfrak{f}(x)\right\rangle.$$

Noting that

$$\begin{aligned} U_{\mathfrak{f}}(U_{\mathfrak{f}}\left|x\right\rangle\left|y\right\rangle) &= U_{\mathfrak{f}}\left|x\right\rangle\left|y \oplus \mathfrak{f}(x)\right\rangle = \left|x\right\rangle\left|y \oplus \mathfrak{f}(x) \oplus \mathfrak{f}(x)\right\rangle \\ &= \left|x\right\rangle\left|y\right\rangle, \end{aligned}$$

shows that

$$U_{\mathfrak{f}}U_{\mathfrak{f}} = \mathbb{I}\cdots$$

Quantum Solution

Using only call to the quantum black-box computing $\mathfrak{f}$, we can determine with probability 1 if $\mathfrak{f}$ is balanced or constant.
The quantum black-box can be described as the unitary operator

$$U_{\mathfrak{f}}\left|x\right\rangle\left|y\right\rangle = \left|x\right\rangle\left|y \oplus \mathfrak{f}(x)\right\rangle.$$

Noting that

$$\begin{aligned} U_{\mathfrak{f}}(U_{\mathfrak{f}}\left|x\right\rangle\left|y\right\rangle) &= U_{\mathfrak{f}}\left|x\right\rangle\left|y \oplus \mathfrak{f}(x)\right\rangle = \left|x\right\rangle\left|y \oplus \mathfrak{f}(x) \oplus \mathfrak{f}(x)\right\rangle \\ &= \left|x\right\rangle\left|y\right\rangle, \end{aligned}$$

shows that

$$U_{\mathfrak{f}} U_{\mathfrak{f}} = \mathbb{I} \cdots$$

Measuring the first qubit we obtain with probability 1

- 0 if $\mathfrak{f}$ is constant,
- and 1 if $\mathfrak{f}$ is balanced.

Classical Solution

In the classical solution, we can use the set $\{1, i\}$ as a computational basis just as the quantum calculations use $\{|0\rangle, |1\rangle\}$.

Now an arbitrary $z = a + bi$, where $z \in \mathbb{C}$ and $a, b \in \mathbb{R}$, has a natural superposition of the basis elements. And we can think of a classical black-box,

$C_{\mathfrak{f}} : \mathbb{C} \to \mathbb{C}$, that is analogous to the quantum $U_{\mathfrak{f}} : \{0, 1\} \to \{0, 1\}$.

Classical Solution

In the classical solution, we can use the set $\{1, i\}$ as a computational basis just as the quantum calculations use $\{|0\rangle, |1\rangle\}$.

Now an arbitrary $z = a + bi$, where $z \in \mathbb{C}$ and $a, b \in \mathbb{R}$, has a natural superposition of the basis elements. And we can think of a classical black-box,

$C_{\mathfrak{f}} : \mathbb{C} \to \mathbb{C}$, that is analogous to the quantum $U_{\mathfrak{f}} : \{0, 1\} \to \{0, 1\}$.

- If $\mathfrak{f}$ is constant, $C_{\mathfrak{f}}$ is the identity operation to within a factor of -1.
- If $\mathfrak{f}$ is balanced, $C_{\mathfrak{f}}$ is the conjugate operation.

Classical Solution

In the classical solution, we can use the set $\{1, i\}$ as a computational basis just as the quantum calculations use $\{\left|0\right\rangle, \left|1\right\rangle\}$.

Now an arbitrary $z = a + bi$, where $z \in \mathbb{C}$ and $a, b \in \mathbb{R}$, has a natural superposition of the basis elements. And we can think of a classical black-box,

$C_{\mathfrak{f}} : \mathbb{C} \to \mathbb{C}$, that is analogous to the quantum $U_{\mathfrak{f}} : \{0, 1\} \to \{0, 1\}$.

- If $\mathfrak{f}$ is constant, $C_{\mathfrak{f}}$ is the identity operation to within a factor of -1.
- If $\mathfrak{f}$ is balanced, $C_{\mathfrak{f}}$ is the conjugate operation.

In order to observe our results, we need to be able to project these complex numbers to the computational basis. Which can be done by multiplying the input so that the output is purely imaginary or real.

Deutsch-Jozsa problem

The Deutsch-Jozsa problem is an expansion on the original Deutsch problem that works on a general case of n-bit inputs.
So $\mathfrak{f} : \{0,1\}^n \to \{0,1\}$ and suppose we are given a black-box computing $\mathfrak{f}$ with the guarantee that $\mathfrak{f}$ is constant or balanced.

Deutsch-Jozsa problem

The Deutsch-Jozsa problem is an expansion on the original Deutsch problem that works on a general case of n-bit inputs.
So $\mathfrak{f} : \{0,1\}^n \to \{0,1\}$ and suppose we are given a black-box computing $\mathfrak{f}$ with the guarantee that $\mathfrak{f}$ is constant or balanced.

Like the Deutsch problem, the Deutsch-Jozsa problem tried to determine if $\mathfrak{f}$ is constant or balanced in as few calls as possible. Unlike Deutsch's problem, the distribution of constant and balanced is asymmetrical in the Deutsch-Jozsa problem.

In general, there are $N = 2^n$ possible input stings, each with two possible outputs (0 or 1). Hence for any n, there are 2^N (2^{2^n}) possible functions, $\mathfrak{f}$.

Deutsch-Jozsa problem

The Deutsch-Jozsa problem is an expansion on the original Deutsch problem that works on a general case of n-bit inputs.
So $\mathfrak{f} : \{0,1\}^n \rightarrow \{0,1\}$ and suppose we are given a black-box computing $\mathfrak{f}$ with the guarantee that $\mathfrak{f}$ is constant or balanced.

Like the Deutsch problem, the Deutsch-Jozsa problem tried to determine if $\mathfrak{f}$ is constant or balanced in as few calls as possible. Unlike Deutsch's problem, the distribution of constant and balanced is asymmetrical in the Deutsch-Jozsa problem.

In general, there are $N = 2^n$ possible input stings, each with two possible outputs (0 or 1). Hence for any n, there are 2^N (2^{2^n}) possible functions, $\mathfrak{f}$.
Of these, exactly two are constant and $\begin{pmatrix} N \\ N/2 \end{pmatrix}$ are balanced.

Quantum Solution

For $n = 2$ the quantum black-box is given three qubits. We initially prepare our system in the state $\left|00\right\rangle\left|1\right\rangle$, and apply $H^{\otimes 3}$...

Quantum Solution

For $n = 2$ the quantum black-box is given three qubits. We initially prepare our system in the state $\left|00\right\rangle\left|1\right\rangle$, and apply $H^{\otimes 3}$...

This state is separable iff $(-1)^{\mathfrak{f}(00)}(-1)^{\mathfrak{f}(11)}c_{00}c_{11} = (-1)^{\mathfrak{f}(01)}(-1)^{\mathfrak{f}(10)}c_{01}c_{10}$. The state is further simplified by nothing that the mapping

$$(-1)^{\mathfrak{f}(a)}(-1)^{\mathfrak{f}(b)} \iff \mathfrak{f}(a) \oplus \mathfrak{f}(b); a, b \in \{0, 1\}^2$$

is a bijection.

Quantum Solution

For $n = 2$ the quantum black-box is given three qubits. We initially prepare our system in the state $\left|00\right\rangle\left|1\right\rangle$, and apply $H^{\otimes 3}$...

This state is separable iff $(-1)^{\mathfrak{f}(00)}(-1)^{\mathfrak{f}(11)}c_{00}c_{11} = (-1)^{\mathfrak{f}(01)}(-1)^{\mathfrak{f}(10)}c_{01}c_{10}$. The state is further simplified by nothing that the mapping

$$(-1)^{\mathfrak{f}(a)}(-1)^{\mathfrak{f}(b)} \iff \mathfrak{f}(a) \oplus \mathfrak{f}(b);\, a, b \in \{0, 1\}^2$$

is a bijection.

And the separability condition reduces to $\mathfrak{f}(00) \oplus \mathfrak{f}(11) = \mathfrak{f}(01) \oplus \mathfrak{f}(10) \cdots$

Quantum Solution

For $n = 2$ the quantum black-box is given three qubits. We initially prepare our system in the state $|00\rangle|1\rangle$, and apply $H^{\otimes 3}$...

This state is separable iff $(-1)^{\mathfrak{f}(00)}(-1)^{\mathfrak{f}(11)}c_{00}c_{11} = (-1)^{\mathfrak{f}(01)}(-1)^{\mathfrak{f}(10)}c_{01}c_{10}$. The state is further simplified by nothing that the mapping

$$(-1)^{\mathfrak{f}(a)}(-1)^{\mathfrak{f}(b)} \iff \mathfrak{f}(a) \oplus \mathfrak{f}(b);\, a, b \in \{0, 1\}^2$$

is a bijection.

And the separability condition reduces to $\mathfrak{f}(00) \oplus \mathfrak{f}(11) = \mathfrak{f}(01) \oplus \mathfrak{f}(10) \cdots$ By measuring both qubits if both are measured as 0 then $\mathfrak{f}$ is constant, otherwise $\mathfrak{f}$ is balanced.

Table 1 All possible Boolean functions $f : \{0, 1\}^2 \to \{0, 1\}$

$f(x)$	Constant		Balanced						Invalid							
$f(00) =$	0	1	0	1	0	1	1	0	1	0	1	0	1	0	0	1
$f(01) =$	0	1	0	1	1	0	0	1	1	0	1	0	0	1	1	0
$f(10) =$	0	1	1	0	1	0	1	0	1	0	0	1	1	0	1	0
$f(11) =$	0	1	1	0	0	1	0	1	0	1	1	0	1	0	1	0

Classical Solution

We can extend the classical $C_{\mathfrak{f}} : \mathbb{C} \to \mathbb{C}$ to two inputs and it becomes

$$C_{\mathfrak{f}} : \mathbb{C}^2 \to \mathbb{C}^2.$$

Let z_1, z_2 be complex numbers,

$$\begin{aligned} C_f \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} &= C_f \begin{pmatrix} a_1 + b_1 i \\ a_2 + b_2 i \end{pmatrix} \\ &= (-1)^{f(00)} \begin{pmatrix} a_1 + (-1)^{f(00) \oplus f(10)} b_1 i \\ a_2 + (-1)^{f(10) \oplus f(11)} b_2 i \end{pmatrix}. \end{aligned}$$

Classical Solution

$$
\begin{aligned}
C_f\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} &= C_f\begin{pmatrix} a_1 + b_1 i \\ a_2 + b_2 i \end{pmatrix} \\
&= (-1)^{f(00)}\begin{pmatrix} a_1 + (-1)^{f(00)\oplus f(10)} b_1 i \\ a_2 + (-1)^{f(10)\oplus f(11)} b_2 i \end{pmatrix}.
\end{aligned}
$$

To project each qubit back onto the computation basis, we multiply each of the complex numbers that the black-box output by their respective inputs.

Classical Solution

$$C_f\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = C_f\begin{pmatrix} a_1 + b_1 i \\ a_2 + b_2 i \end{pmatrix}$$
$$= (-1)^{f(00)}\begin{pmatrix} a_1 + (-1)^{f(00)\oplus f(10)} b_1 i \\ a_2 + (-1)^{f(10)\oplus f(11)} b_2 i \end{pmatrix}.$$

To project each qubit back onto the computation basis, we multiply each of the complex numbers that the black-box output by their respective inputs.
Let $z_1 = z_2 = 1 + i$, and we get the following:

$$\frac{(1+i)}{2} \times C_f\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \frac{(-1)^{f(00)}}{2}$$
$$\times \begin{cases} \begin{pmatrix} (1+i)(1+i) \\ (1+i)(1+i) \end{pmatrix} = \begin{pmatrix} i \\ i \end{pmatrix} & \text{if } f \text{ is constant,} \\ \begin{pmatrix} (1+i)(1-i) \\ (1+i)(1+i) \end{pmatrix} = \begin{pmatrix} 1 \\ i \end{pmatrix} & \\ \begin{pmatrix} (1+i)(1+i) \\ (1+i)(1-i) \end{pmatrix} = \begin{pmatrix} i \\ 1 \end{pmatrix} & \text{if } f \text{ is balanced.} \\ \begin{pmatrix} (1+i)(1-i) \\ (1+i)(1-i) \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} & \end{cases}$$

Classical Solution

Let $z_1 = z_2 = 1 + i$, and we get the following:

$$\frac{(1+i)}{2} \times C_f \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \frac{(-1)^{f(00)}}{2}$$

$$\times \begin{cases} \begin{pmatrix} (1+i)(1+i) \\ (1+i)(1+i) \end{pmatrix} = \begin{pmatrix} i \\ i \end{pmatrix} & \text{if } f \text{ is constant,} \\ \begin{pmatrix} (1+i)(1-i) \\ (1+i)(1+i) \end{pmatrix} = \begin{pmatrix} 1 \\ i \end{pmatrix} & \\ \begin{pmatrix} (1+i)(1+i) \\ (1+i)(1-i) \end{pmatrix} = \begin{pmatrix} i \\ 1 \end{pmatrix} & \text{if } f \text{ is balanced.} \\ \begin{pmatrix} (1+i)(1-i) \\ (1+i)(1-i) \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} & \end{cases}$$

If both complex numbers are imaginary, then f is constant; otherwise it is balanced.

Conclusion

Because the quantum solution is separable, it is possible to write the output as a list of two complex numbers, otherwise finding a classical solution in this fashion would have required a list of complex numbers exponential in the number of input qubits.

Due to time constraints, proofs are omitted.