Deutsch–Jozsa algorithm

The **Deutsch–Jozsa algorithm** is a quantum algorithm, proposed by David Deutsch and Richard Jozsa in 1992[1] with improvements by Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca in 1998.[2] Although of little practical use, it is one of the first examples of a quantum algorithm that is exponentially faster than any possible deterministic classical algorithm and is the inspiration for Simon's Algorithm which is, in turn, the inspiration for Shor's Algorithm.[3] It is also a deterministic algorithm, meaning that it always produces an answer, and that answer is always correct.

Contents

Problem statement

In the Deutsch-Jozsa problem, we are given a black box quantum computer known as an oracle that implements some function $f : \{0,1\}^n \to \{0,1\}$. The function takes n-digit binary values as input and produces either a 0 or a 1 as output for each such value. We are promised that the function is either constant (0 on all outputs or 1 on all outputs) or *balanced*[4] (returns 1 for half of the input domain and 0 for the other half); the task then is to determine if f is constant or balanced by using the oracle.

Motivation

The Deutsch–Jozsa problem is specifically designed to be easy for a quantum algorithm and hard for any deterministic classical algorithm. The motivation is to show a black box problem that can be solved efficiently by a quantum computer with no error, whereas a deterministic classical computer would need a large number of queries to the black box to solve the problem. More formally, it yields an oracle relative to which **EQP**, the class of problems that can be solved exactly in polynomial time on a quantum computer, and **P** are different.[5]

Since the problem is easy to solve on a probabilistic classical computer, it does not yield an oracle separation with **BPP**, the class of problems that can be solved with bounded error in polynomial time on a probabilistic classical computer. Simon's problem is an example of a problem that yields an oracle separation between **BQP** and **BPP**.

Classical solution

For a conventional deterministic algorithm where n is number of bits, $2^{n-1}+1$ evaluations of f will be required in the worst case. To prove that f is constant, just over half the set of inputs must be evaluated and their outputs found to be identical (remembering that the function is guaranteed to be either balanced or constant, not somewhere in between). The best case occurs

where the function is balanced and the first two output values that happen to be selected are different. For a conventional randomized algorithm, a constant k evaluations of the function suffices to produce the correct answer with a high probability (failing with probability $\epsilon \leq 1/2^k$ with $k \geq 1$). However, $k = 2^{n-1} + 1$ evaluations are still required if we want an answer that is always correct. The Deutsch-Jozsa quantum algorithm produces an answer that is always correct with a single evaluation of f.

History

The Deutsch–Jozsa Algorithm generalizes earlier (1985) work by David Deutsch, which provided a solution for the simple case. Specifically we were given a boolean function whose input is 1 bit, $f : \{0,1\} \to \{0,1\}$ and asked if it is constant.[6]

The algorithm as Deutsch had originally proposed it was not, in fact, deterministic. The algorithm was successful with a probability of one half. In 1992, Deutsch and Jozsa produced a deterministic algorithm which was generalized to a function which takes n bits for its input. Unlike Deutsch's Algorithm, this algorithm required two function evaluations instead of only one.

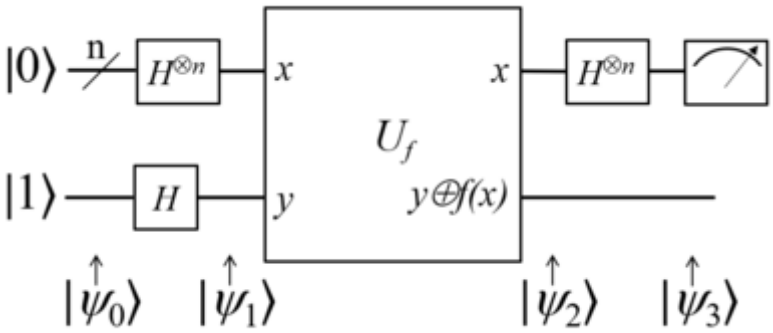
Further improvements to the Deutsch–Jozsa algorithm were made by Cleve et al.,[2] resulting in an algorithm that is both deterministic and requires only a single query of f. This algorithm is still referred to as Deutsch–Jozsa algorithm in honour of the groundbreaking techniques they employed.[2]

Algorithm

For the Deutsch–Jozsa algorithm to work, the oracle computing $f(x)$ from x has to be a quantum oracle which doesn't decohere x. It also mustn't leave any copy of x lying around at the end of the oracle call.

The algorithm begins with the $n + 1$ bit state $|0\rangle^{\otimes n}|1\rangle$. That is, the first n bits are each in the state $|0\rangle$ and the final bit is $|1\rangle$. A Hadamard transform is applied to each bit to obtain the state

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|0\rangle - |1\rangle).$$



Deutsch-Jozsa algorithm quantum circuit

We have the function f implemented as a quantum oracle. The oracle maps the state $|x\rangle|y\rangle$ to $|x\rangle|y \oplus f(x)\rangle$, where $\oplus$ is addition modulo 2 (see below for details of implementation). Applying the quantum oracle gives

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|f(x)\rangle - |1 \oplus f(x)\rangle).$$

For each x, $f(x)$ is either 0 or 1. Testing these two possibilities, we see the above state is equal to

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle(|0\rangle - |1\rangle).$$

At this point the last qubit may be ignored. We apply a Hadamard transform to each qubit to obtain

$$\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\left[\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle\right] = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\left[\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot y}\right]|y\rangle$$

where $x \cdot y = x_0y_0 \oplus x_1y_1 \oplus \cdots \oplus x_{n-1}y_{n-1}$ is the sum of the bitwise product.

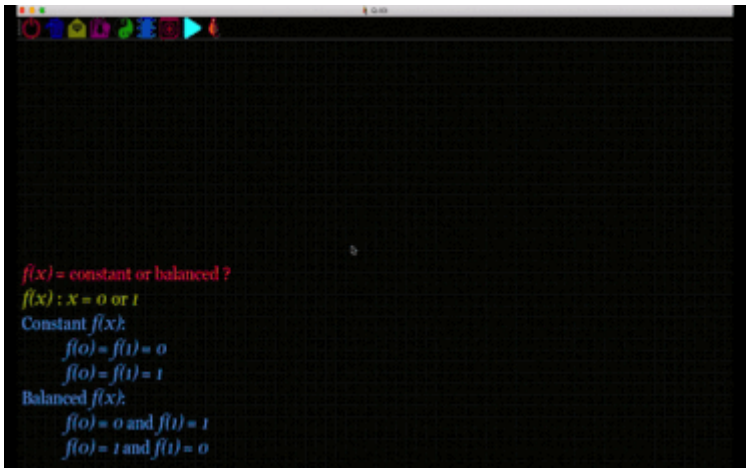
Finally we examine the probability of measuring $|0\rangle^{\otimes n}$,

$$\left|\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\right|^2$$

which evaluates to 1 if $f(x)$ is constant (constructive interference) and 0 if $f(x)$ is balanced (destructive interference).

Deutsch's algorithm

Deutsch's algorithm is a special case of the general Deutsch–Jozsa algorithm. We need to check the condition $f(0) = f(1)$. It is equivalent to check $f(0) \oplus f(1)$ (where $\oplus$ is addition modulo 2, which can also be viewed as a quantum XOR gate implemented as a Controlled NOT gate), if zero, then f is constant, otherwise f is not constant.



Simulation of quantum circuit for Deutsch's algorithm using Q-Kit (https://sites.google.com/view/quantum-kit/)

We begin with the two-qubit state $|0\rangle|1\rangle$ and apply a Hadamard transform to each qubit. This yields

$$\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle).$$

We are given a quantum implementation of the function f that maps $|x\rangle|y\rangle$ to $|x\rangle|f(x) \oplus y\rangle$. Applying this function to our current state we obtain

$$\begin{aligned}
&\frac{1}{2}(|0\rangle(|f(0)\oplus 0\rangle - |f(0)\oplus 1\rangle) + |1\rangle(|f(1)\oplus 0\rangle - |f(1)\oplus 1\rangle)) \\
&= \frac{1}{2}((-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)) \\
&= (-1)^{f(0)}\frac{1}{2}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right)(|0\rangle - |1\rangle).
\end{aligned}$$

We ignore the last bit and the global phase and therefore have the state

$$\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle).$$

Applying a Hadamard transform to this state we have

$$\begin{aligned}
&\frac{1}{2}(|0\rangle + |1\rangle + (-1)^{f(0)\oplus f(1)}|0\rangle - (-1)^{f(0)\oplus f(1)}|1\rangle) \\
&= \frac{1}{2}((1 + (-1)^{f(0)\oplus f(1)})|0\rangle + (1 - (-1)^{f(0)\oplus f(1)})|1\rangle).
\end{aligned}$$

Obviously $f(0) \oplus f(1) = 0$ if and only if we measure a zero and $f(0) \oplus f(1) = 1$ if and only if we measure a one. So with certainty we know whether $f(x)$ is constant or balanced.

References

1. David Deutsch and Richard Jozsa (1992). "Rapid solutions of problems by quantum computation". *Proceedings of the Royal Society of London A*. **439** (1907): 553–558. Bibcode:1992RSPSA.439..553D (https://ui.adsabs.harvard.edu/abs/1992RSPSA.439..553D). CiteSeerX 10.1.1.655.5997 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.655.5997). doi:10.1098/rspa.1992.0167 (https://doi.org/10.1098%2Frspa.1992.0167).
2. R. Cleve; A. Ekert; C. Macchiavello; M. Mosca (1998). "Quantum algorithms revisited". *Proceedings of the Royal Society of London A*. **454** (1969): 339–354. arXiv:quant-ph/9708016 (https://arxiv.org/abs/quant-ph/9708016). Bibcode:1998RSPSA.454..339C (https://ui.adsabs.harvard.edu/abs/1998RSPSA.454..339C). doi:10.1098/rspa.1998.0164 (https://doi.org/10.1098%2Frspa.1998.0164).
3. Simon, Daniel (November 1994). "On the Power of Quantum Computation" (http://citeseer.ist.psu.edu/viewdoc/download?doi=10.1.1.51.5477&rep=rep1&type=pdf). *94 Proceedings of the 35th Annual Symposium on Foundations of Computer Science*: 116–123.
4. "Certainty from Uncertainty" (https://web.archive.org/web/20110406191104/http://www.fortunecity.com/emachines/e11/86/qcomp2.html). Archived from the original (http://www.fortunecity.com/emachines/e11/86/qcomp2.html) on 2011-04-06. Retrieved 2011-02-13.
5. Johansson, N. ; Larsson, JÅ. https://doi.org/10.1007/s11128-017-1679-7 (2017). "Efficient classical simulation of the Deutsch–Jozsa and Simon's algorithms". *Quantum Inf Process (2017)*. **16** (9): 233. arXiv:1508.05027 (https://arxiv.org/abs/1508.05027). doi:10.1007/s11128-017-1679-7 (https://doi.org/10.1007%2Fs11128-017-1679-7).
6. David Deutsch (1985). "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer" (http://coblitz.codeen.org:3125/citeseer.ist.psu.edu/cache/papers/cs/13701/http:zSzzSzwww.qubit.orgzSzresourcezSzdeutsch85.pdf/deutsch85quantum.pdf) (PDF). *Proceedings of the Royal Society of London A*. **400** (1818): 97–117. Bibcode:1985RSPSA.400...97D (https://ui.adsabs.harvard.edu/abs/1985RSPSA.400...97D). CiteSeerX 10.1.1.41.2382 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.41.2382). doi:10.1098/rspa.1985.0070 (https://doi.org/10.1098%2Frspa.1985.0070).

External links

- Deutsch's lecture about the Deutsch-Jozsa algorithm (http://www.quiprocone.org/Protected/Lecture_5.htm)