From interference to quantum algorithms

Artur Ekert and Alastair Kay

The networks and quantum gates that we have introduced so far are more than just tools for constructing unitary operations. We want to give them some computational meaning, associate them with algorithms and quantify the complexity of these algorithms.

I. BOOLEAN FUNCTIONS

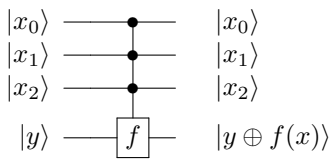
Classical computers evaluate Boolean functions,

$$f : \{0,1\}^n \mapsto \{0,1\}.$$

Quantum computers embed them into reversible computation and evaluate unitary operations

$$U_f : |x\rangle|y\rangle \longrightarrow |x\rangle|y \oplus f(x)\rangle,$$

where $x \in \{0,1\}^n$, $y \in \{0,1\}$. The corresponding network diagram is (for $n = 3$),



What makes the quantum evaluation of Boolean functions really interesting is its action on a superposition of different inputs x. For example,

$$\sum_x |x\rangle|0\rangle \mapsto \sum_x |x\rangle|f(x)\rangle$$

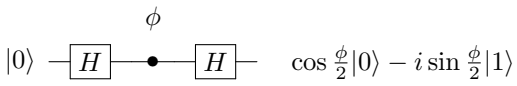
produces $f(x)$ for all x in a single run (we have dropped the normalisation factor). Unfortunately, we cannot learn all the values $f(x)$ from the entangled state $\sum_x |x\rangle|f(x)\rangle$ because any bit by bit measurement on the first n qubits will yield one particular value $x' \in \{0,1\}^n$ and the final qubit will then be found with the value $f(x') \in \{0,1\}$. In order to achieve novel results, different to classical computation, we usually sandwich a quantum function evaluation in between other operations, such as the Hadamard transform, and ask questions about some global properties of f that depend on many values of $f(x)$, e.g. periodicity.

II. ORACLES

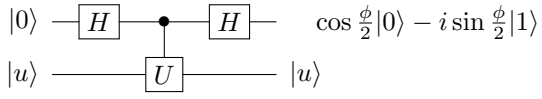
The first quantum algorithms demonstrated the advantage of quantum computation over classical without referring to computational complexity, as measured by the scaling properties of network sizes. The computational power of quantum interference was, instead, discovered by counting how many times certain Boolean functions have to be evaluated in order to find the answer to a given problem. Imagine a "black box" (also called an *oracle*) computing a Boolean function and a scenario in which one wants to learn about a given property of the Boolean function but has to pay for each use of the box (often referred to as a *query*). In such a setting, the objective is to minimise number of queries to this oracle. The massive advantage of such an approach is that often both lower bounds and upper bounds can be determined for the query cost, which allows a genuine proof of a distinction between classical and quantum computation.

III. INTERFERENCE REVISITED

Quantum computers are basically multi-particle interferometers with phase shifts that result from quantum function evaluations. To illustrate this point we start with the simplest single-qubit interference circuit



The role of the three gates is clear: the first Hadamard prepares an equally weighted superposition of possible inputs, here $|0\rangle$ and $|1\rangle$, the phase shit determines the nature of interference (constructive or destructive), and the second Hadamard brings all computational paths together, erasing any trace of which particular path was followed. The phase shift can be also "computed" with the help of an auxiliary qubit (or a set of qubits) in a prescribed state $|u\rangle$ and some controlled-U transformation where $U|u\rangle = e^{i\phi}|u\rangle$,



This network effects the following sequence of transformations (normalisation factors neglected)

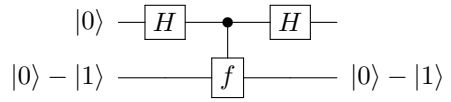
$$\begin{aligned}
|0\rangle|u\rangle &\stackrel{H}{\mapsto} (|0\rangle + |1\rangle)|u\rangle = |0\rangle|u\rangle + |1\rangle)|u\rangle \\
&\stackrel{f}{\mapsto} |0\rangle|u\rangle + |1\rangle)U|u\rangle = |0\rangle|u\rangle + e^{i\phi}|1\rangle)|u\rangle \\
&= (|0\rangle + e^{i\phi}|1\rangle)|u\rangle \\
&\stackrel{H}{\mapsto} (\cos\frac{\phi}{2}|0\rangle - i\sin\frac{\phi}{2}|1\rangle)|u\rangle
\end{aligned}$$

Since quantum phases can be introduced by some controlled-U operations, it is natural to ask whether effecting these operations can be described as an interesting computational problem.

To begin with, suppose that the phase shifter in the interference network is set either to $\phi = 0$ or to $\phi = \pi$. Can we tell the difference? Of course we can. In fact, a single instance of the experiment determines the difference: for $\phi = 0$ the particle *always* ends up in the detector "0" and for $\phi = \pi$ *always* in the detector "1". The first quantum algorithm, proposed by David Deutsch in 1985, is related to this effect.

IV. DEUTSCH'S ALGORITHM

Consider the Boolean functions f that map $\{0,1\}$ to $\{0,1\}$. There are exactly four such functions: two constant functions ($f(0) = f(1) = 0$ and $f(0) = f(1) = 1$) and two "balanced" functions ($f(0) = 0, f(1) = 1$ and $f(0) = 1, f(1) = 0$). Informally, in Deutsch's problem, one is allowed to evaluate the function f *only once* and required to deduce from the result whether f is constant or balanced (in other words, whether the binary numbers $f(0)$ and $f(1)$ are the same or different). Note that we are not asked for the particular values $f(0)$ and $f(1)$ but for a global property of f. Classical intuition tells us that to determine this global property of f, we have to evaluate both $f(0)$ and $f(1)$ anyway, which involves evaluating f twice. We shall see that this is not so in the setting of quantum information, where we can solve Deutsch's problem with a single function evaluation, by employing an algorithm that has the same mathematical structure as the quantum interferometry



First we notice that

$$\begin{aligned} |x\rangle(|0\rangle - |1\rangle) &\overset{f}{\mapsto} |x\rangle(|f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \end{aligned}$$

During the function evaluation the second register "kicks back" the phase factor $(-1)^{f(x)}$ in front of $|x\rangle$. The state of the second register remains unchanged while the first is modified as follows

$$\begin{aligned} |0\rangle &\overset{H}{\mapsto} |0\rangle + |1\rangle) \\ &\overset{f}{\mapsto} (-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle \\ &= |0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle \\ &\overset{H}{\mapsto} |f(0) \oplus f(1)\rangle \end{aligned}$$

Therefore, the first qubit is finally in state $|0\rangle$ if the function f is constant and in state $|1\rangle$ if the function is balanced, and a measurement of this qubit distinguishes these cases with certainty.

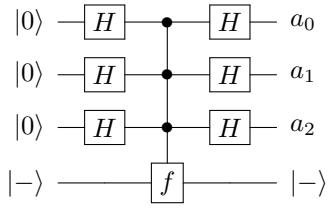
Deutsch's result laid the foundation for the new field of quantum computation, and was followed by several other quantum algorithms for various problems, which all seem to rest on the same generic sequence: a Hadamard transform, followed by a function evaluation, followed by another Hadamard (Fourier) transform. In some cases, such as Grover's "database search" algorithm, this sequence is repeated several times.

V. BERNSTEIN-VAZIRANI PROBLEM

Suppose that $f : \{0,1\}^n \to \{0,1\}$ is of the form

$$f(x) = a \cdot x \equiv (a_1 \cdot x_1) \oplus \cdots \oplus (a_n \cdot x_n)$$

where $a \in \{0,1\}^n$ and $b \in \{0,1\}$, and the task is to find a. The classical determination of a requires at least n calls to the oracle evaluating f. This is because a contains n bits of information and each classical evaluation of f yields a single bit of information. Nevertheless, by running the quantum network shown below it is possible to determine a with a single call to the oracle.



Here $|-\rangle = |0\rangle - |1\rangle$. Stepping through the execution of the network, the state after the first n-qubit Hadamard transform is applied is

$$\sum_{x\in\{0,1\}^n} |x\rangle|-\rangle$$

which, after the function evaluation, becomes

$$\sum_{x\in\{0,1\}^n} (-1)^{a\cdot x}|x\rangle|-\rangle$$

and finally, after the second Hadamard transform,

$$\sum_{z\in\{0,1\}^n} \left(\sum_{x\in\{0,1\}^n} (-1)^{x\cdot(a\oplus z)} \right) |z\rangle|-\rangle$$

If you take the sum over x, then all the terms always cancel out unless $a \oplus z = 00\ldots0$ i.e. $z = a$. The final state at the output is then $= |a\rangle|-\rangle$. Upon measurement of the first register, we get the result a after a single evaluation of the oracle. The power of multiqubit interference.