A First View of Quantum Algorithmics

Renato Neves

Universidade do Minho

HASLab
HIGH-ASSURANCE
SOFTWARE LABORATORY

Table of Contents

Our First Encounter with ‘Quantum Advantage’

The Problem

Receive a ‘single-bit’ function $f : \{0, 1\} \to \{0, 1\}$

Either $f(0) = f(1)$ or $f(0) \neq f(1)$

Tell us whether the first or second case hold

Our First Encounter with ‘Quantum Advantage’

The Problem

Receive a ‘single-bit’ function $f : \{0,1\} \to \{0,1\}$

Either $f(0) = f(1)$ or $f(0) \neq f(1)$

Tell us whether the first or second case hold

Classically, to determine which case holds requires running f twice

Our First Encounter with 'Quantum Advantage'

The Problem

Receive a 'single-bit' function $f : \{0,1\} \to \{0,1\}$

Either $f(0) = f(1)$ or $f(0) \neq f(1)$

Tell us whether the first or second case hold

Classically, to determine which case holds requires running f twice

Quantumly, it suffices to run f once . . .

Our First Encounter with 'Quantum Advantage'

The Problem

Receive a 'single-bit' function $f : \{0,1\} \to \{0,1\}$

Either $f(0) = f(1)$ or $f(0) \neq f(1)$

Tell us whether the first or second case hold

Classically, to determine which case holds requires running f twice

Quantumly, it suffices to run f once ...

due to two quantum effects superposition and interference

The Need for a Quantum Computational Language

Quantum solution to the previous problem given as an algorithm

In order to describe it, it is convenient to use a computational language . . .

. . . just like in the classical case

Table of Contents

Postulates of Pure Quantum Systems

States

State of n-qubits encoded as a unit vector

$$v \in \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} \cong \mathbb{C}^{2^n}$$

State operations

n-qubit operation encoded as an isometry

$$\mathbb{C}^{2^n} \longrightarrow \mathbb{C}^{2^n}$$

i.e. a linear map that preserves norms

Recall: we can sequentially compose and tensor isometries

Table of Contents

Genesis

We start with a set of quantum operations

Each operation U_i manipulates the state of n_i-qubits received from its left-hand side . . .

. . . and returns the result on its right-hand side

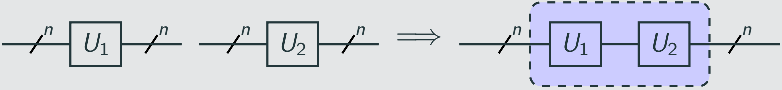
Examples of Quantum Operations

$$\left[\!\left[\;-\!\boxed{X}\!-\; \right]\!\right] = X : \mathbb{C}^2 \to \mathbb{C}^2 \text{ (not operation)}$$

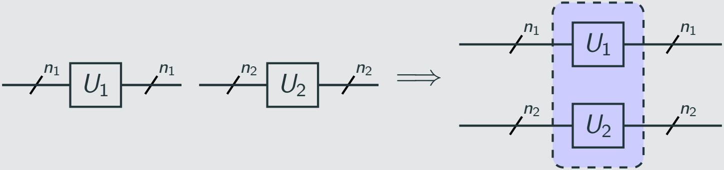
$[\![x]\!]$ reads as "the mathematical meaning of x"

$$\left[\!\left[\;-\!\boxed{H}\!-\; \right]\!\right] = H : \mathbb{C}^2 \to \mathbb{C}^2 \text{ (Hadamard operation)}$$

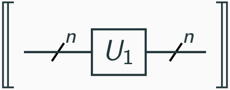
Sequential Composition



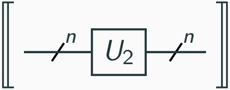
Parallel Composition



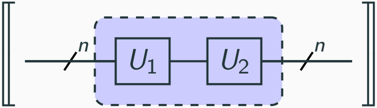
Mathematical Meaning of Sequential Composition



$= f : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ and

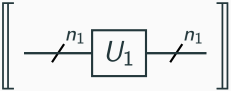


$= g : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ entails ...

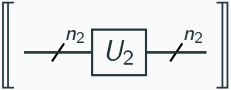


$= g \cdot f : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$

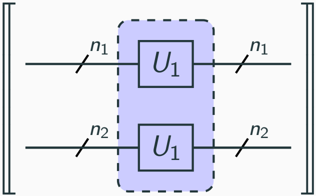
Mathematical Meaning of Parallel Composition



$= f : \mathbb{C}^{2^{n_1}} \to \mathbb{C}^{2^{n_1}}$ and



$= g : \mathbb{C}^{2^{n_2}} \to \mathbb{C}^{2^{n_2}}$ entails ...



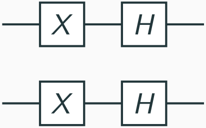
$$= f \otimes g : \underbrace{\mathbb{C}^{2^{n_1}} \otimes \mathbb{C}^{2^{n_2}}}_{\cong\ \mathbb{C}^{2^{n_1+n_2}}} \to \underbrace{\mathbb{C}^{2^{n_1}} \otimes \mathbb{C}^{2^{n_2}}}_{\cong\ \mathbb{C}^{2^{n_1+n_2}}}$$

Two Warm-up Exercises

1. Show that

Our first case of quantum interference

2. Prove that the circuit



can be built in two different ways and that despite that its mathematical meaning is unambiguous

Table of Contents

Turning f into a Quantum Operation pt. I

$f : \{0,1\} \to \{0,1\}$ extends to a linear map $\mathbb{C}^2 \to \mathbb{C}^2$

... but not necessarily to an isometry

Example

When f is constant on 0 we obtain $f\,|0\rangle = |0\rangle$ and $f\,|1\rangle = |0\rangle$. Then we know that $\left\| \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right\| = 1$ and calculate,

$$\left\| f\left(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \right\| = \left\| \tfrac{1}{\sqrt{2}}(|0\rangle + |0\rangle) \right\| = \left\| \tfrac{2}{\sqrt{2}}\,|0\rangle \right\| = \tfrac{2}{\sqrt{2}}$$

Turning f into a Quantum Operation pt. II

What is the problem intuitively?

Turning f into a Quantum Operation pt. II

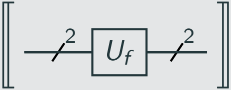
What is the problem intuitively?

f potentially loses information and it is general consensus that pure quantum operations are reversible

Charles Bennett, 1973

N.b.: isometricity implies injectivity so if a map loses information it cannot be isometric

Proposed Solution

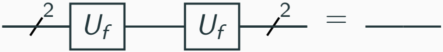


$$= |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle$$

Addition modulo 2

U_f encodes f: $U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |0 \oplus f(x)\rangle = |x\rangle \otimes |f(x)\rangle$

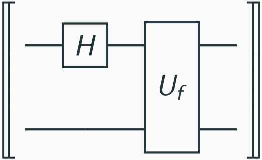
U_f is reversible, in particular



Tackling the Problem via Quantum Parallelism pt. I

Need to somehow evaluate f with $|0\rangle$ and $|1\rangle$ in one step

So take the circuit



$$= U_f(H \otimes I)$$

and calculate ...

Tackling the Problem via Quantum Parallelism pt. II

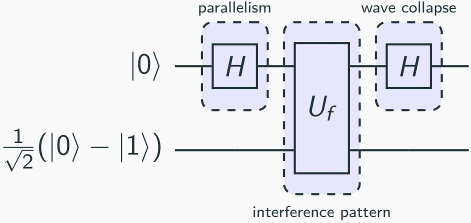
$$
\begin{aligned}
& U_f(H \otimes I)\,|0\rangle \otimes |0\rangle \\
&= U_f\left(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) && \{\text{Defn. of } H \text{ and } I\} \\
&= U_f\left(\tfrac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) && \{\otimes \text{ distributes over } +\} \\
&= \tfrac{1}{\sqrt{2}}(|0\rangle\,|0 \oplus f(0)\rangle + |1\rangle\,|0 \oplus f(1)\rangle) && \{\text{Defn. of } U_f\} \\
&= \underbrace{\tfrac{1}{\sqrt{2}}(|0\rangle\,|f(0)\rangle + |1\rangle\,|f(1)\rangle)}_{f(0) \text{ and } f(1) \text{ in a single run}} && \{0 \oplus x = x\}
\end{aligned}
$$

... cannot extract this information from the resultant state :(

but fortunately no need to know the values of $f(0)$ and $f(1)$ – only whether they are equal or not

Tackling the Problem via Parallelism and Interference pt. I

We create an interference pattern dependent on this property



... and the wave collapse informs us

An Auxiliary Computation

$$
\begin{aligned}
& U_f\,(|x\rangle \otimes (|0\rangle - |1\rangle)) \\
&= U_f\,(|x\rangle\,|0\rangle - |x\rangle\,|1\rangle) && \{\otimes \text{ distributes over } + \} \\
&= |x\rangle\,|0 \oplus f(x)\rangle - |x\rangle\,|1 \oplus f(x)\rangle && \{\text{Defn. of } f\} \\
&= |x\rangle\,|f(x)\rangle - |x\rangle\,|\neg f(x)\rangle && \{0 \oplus x = x, 1 \oplus x = \neg x\} \\
&= |x\rangle \otimes (|f(x)\rangle - |\neg f(x)\rangle) && \{\otimes \text{ distributes over } +\}
\end{aligned}
$$

We then proceed by case distinction

$$
|x\rangle \otimes (|f(x)\rangle - |\neg f(x)\rangle) = \begin{cases} |x\rangle \otimes (|0\rangle - |1\rangle) & \text{if } f(x) = 0 \\ |x\rangle \otimes (|1\rangle - |0\rangle) & \text{if } f(x) = 1 \end{cases}
$$

and conclude

$$
|x\rangle \otimes (|f(x)\rangle - |\neg f(x)\rangle) = (-1)^{f(x)}\,|x\rangle \otimes (|0\rangle - |1\rangle)
$$

Tackling the Problem via Parallelism and Interference pt. II

$$
\begin{aligned}
&(H \otimes I)U_f(H \otimes I)\left(|0\rangle \otimes |-\rangle\right) \\
&= (H \otimes I)U_f\left(|+\rangle \otimes |-\rangle\right) && \{\ldots\} \\
&= \tfrac{1}{\sqrt{2}}(H \otimes I)U_f\left((|0\rangle + |1\rangle) \otimes |-\rangle\right) && \{\ldots\} \\
&= \tfrac{1}{\sqrt{2}}(H \otimes I)\left(U_f\,|0\rangle \otimes |-\rangle + U_f\,|1\rangle \otimes |-\rangle\right) && \{\ldots\} \\
&= \tfrac{1}{\sqrt{2}}(H \otimes I)\left((-1)^{f(0)}\,|0\rangle \otimes |-\rangle + (-1)^{f(1)}\,|1\rangle \otimes |-\rangle\right) && \{\text{Previous slide}\} \\
&= \begin{cases} (H \otimes I)(\pm 1)\,|+\rangle \otimes |-\rangle & \text{if } f(0) = f(1) \\ (H \otimes I)(\pm 1)\,|-\rangle \otimes |-\rangle & \text{if } f(0) \neq f(1) \end{cases} && \{\text{Case distinction}\} \\
&= \begin{cases} (\pm 1)\,|0\rangle \otimes |-\rangle & \text{if } f(0) = f(1) \\ (\pm 1)\,|1\rangle \otimes |-\rangle & \text{if } f(0) \neq f(1) \end{cases} && \{\ldots\}
\end{aligned}
$$

What's Next?

A simplification of the first algorithm with ‘quantum advantage’ presented in literature [Deutsch, 1985]

All other quantum algorithms crucially rely on similar ideas of quantum interference

We will study them in the following lectures