Deutsch algorithm and Deutsch-Josza algorithm.

Géraud Sénizergues

LaBRI, Bordeaux.

GT Calcul quantique, April 22nd 2020

Aims

We present an algorithmic problem about boolean functions. The quantum-algorithms provided by Deutsch[1982] and Deutsch-Josza [1992] show :
- how the superposition of quantum states leads to some parallelism in quantum computations
- how it can happen that a quantum computation leads to an exact result (even though measurement is a probabilistic process in quantum-mechanics)

contents

1 Introduction

2 Boolean functions vs unitary operators

3 Deutsch algorithm over boolean functions

4 Devil's advocate criticism

5 Quantum parallelism

6 Deutsch-Josza algorithm over boolean functions

Boolean functions vs unitary operators

booleans

We aim at solving problems about *boolean* functions. Every boolean function :

$$f : \{0,1\}^n \to \{0,1\}$$

can be translated into a boolean bijection :

$$f_\oplus : \{0,1\}^{n+1} \to \{0,1\}^{n+1} :$$

$$f_\oplus(\vec{x}, y) := (\vec{x}, y \oplus f(\vec{x})).$$

booleans turned into a Hilbert space

Let $\mathcal{B} = \mathrm{Vect}_{\mathbb{C}}(|0\rangle, |1\rangle)$ be a two-dimensional Hilbert space, with orthonormal basis $\{|0\rangle, |1\rangle\}$. Then $\mathcal{B}^{\otimes n}$ is a vectorial space over $\mathbb{C}$ of dimension 2^n with basis

$$\{|b_1\rangle \otimes |b_2\rangle \otimes \ldots \otimes |b_n\rangle \mid b_i \in \{0,1\}\}.$$

We define a structure of Hilbert space over $\mathcal{B}^{\otimes n}$ by choosing this basis as orthonormal. We use the short notation $|b_1 b_2 \cdots b_n\rangle$ for the vector above. Every boolean bijection $F : \{0,1\}^n \to \{0,1\}^n$ defines a *unitary* transformation :

$$\hat{F} : \mathcal{B}^{\otimes n} \to \mathcal{B}^{\otimes n}$$

by

$$\hat{F} : \left|\vec{b}\right\rangle \mapsto \left|F(\vec{b})\right\rangle.$$

boolean functions : examples

$f = NOT$

$f_\oplus : (x, y) \mapsto (x, y \oplus (NOTx)$

$\hat{f_\oplus}$ has matrix $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ in the basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

$f = \text{AND}$

$f_\oplus : (x, y, z) \mapsto (x, y, z \oplus x \cdot y)$ (a.k.a. Toffoli gate)

$\hat{f_\oplus}$ is the only linear map $\mathcal{B}^{\otimes 3} \to \mathcal{B}^{\otimes 3}$ such that

$$\hat{f_\oplus} : |xyz\rangle \mapsto |xy(z \oplus x \cdot y)\rangle.$$

We also note $U_f := \hat{f_\oplus}$ (the unitary expression of f). We recall the Hadamard gate :

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

Deutsch algorithm over boolean functions

boolean functions

There are 4 functions $\{0,1\} \to \{0,1\}$:

x	0	1
$f_0(x)$	0	0
$f_1(x)$	0	1
$f_2(x)$	1	0
$f_3(x)$	1	1

f_0 et f_3 are *constant* while f_1, f_2 are *equilibrated*.

Deutsch problem

PROBLEM :
INPUT(v1) :$f : \{0,1\} \to \{0,1\}$
QUESTION : Is f equilibrated ?

Deutsch problem

PROBLEM :
INPUT(v1) :$f : \{0,1\} \to \{0,1\}$
QUESTION : Is f equilibrated ?

INPUT(v2,classical) : some circuit, with arity (1,1), that computes f
QUESTION : Is f equilibrated ?

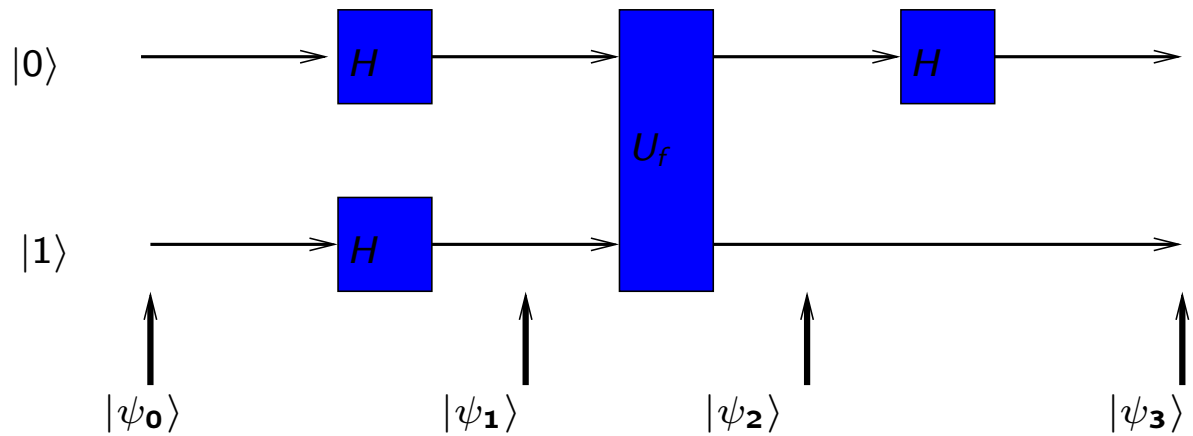
Deutsch problem

PROBLEM :
INPUT(v1) :$f : \{0,1\} \to \{0,1\}$
QUESTION : Is f equilibrated ?

INPUT(v2,classical) : some circuit, with arity (1,1), that computes f
QUESTION : Is f equilibrated ?

INPUT(v3,quantum) : some quantum circuit, with arity (2,2), that computes U_f.
QUESTION : Is f equilibrated ?
Quantum algorithm : a quantum circuit (involving U_f), and a measurement device, that gives the answer.

Deutsch circuit



where the $|\psi_i\rangle$ denote the successive *states* of the system during the computation.

Deutsch algorithm

Evolution of the system :

$$|\psi_0\rangle \mapsto |\psi_1\rangle \mapsto |\psi_2\rangle \mapsto |\psi_3\rangle \,.$$

step 0 : $|\psi_0\rangle = |01\rangle$
step 1 :

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}\left[\sum_{x=0,1} |x\rangle\right](|0\rangle - |1\rangle) \\ &= \frac{1}{2}\sum_{x=0,1}[|x,0\rangle - |x,1\rangle] \end{aligned}$$

Deutsch algorithm

step 2

$$|\psi_2\rangle = \frac{1}{2}\sum_{x=0,1}\left[|x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle\right].$$

For every $x \in \{0, 1\}$

$$|x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle = (-1)^{f(x)}\left[|x, 0\rangle - |x, 1\rangle\right]$$

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2}\sum_{x=0,1}(-1)^{f(x)}\left[|x, 0\rangle - |x, 1\rangle\right] \\ &= \left\{\frac{1}{2}\sum_{x=0,1}(-1)^{f(x)}|x\rangle\right\} \otimes (|0\rangle - |1\rangle) \end{aligned}$$

Deutsch algorithm

step 3 :
An Hadamard gate is applied on the first qbit ; the resulting state is

$$
\begin{aligned}
|\psi_3\rangle &= \frac{1}{2\sqrt{2}}\left\{(-1)^{f(0)}(|0\rangle+|1\rangle)+(-1)^{f(1)}(|0\rangle-|1\rangle)\right\}\otimes(|0\rangle-|1\rangle) \\
&= \frac{1}{2\sqrt{2}}\left\{\left[(-1)^{f(0)}+(-1)^{f(1)}\right]|0\rangle+\left[(-1)^{f(0)}-(-1)^{f(1)}\right]|1\rangle\right\}\otimes(|0\rangle-
\end{aligned}
$$

If f is *constant*, then $f(0)=f(1)$ so that the final state belongs to $(\mathbb{C}\,|0\rangle)\otimes\mathcal{B}$;
If f is *equilibrated*, then $f(0)=-f(1)$ so that the final state belongs to $(\mathbb{C}\,|1\rangle)\otimes\mathcal{B}$.

Deutsch algorithm

Final *measurement* :

A measurement of the first qubit, will give, with probability one :

- $|0\rangle$ if f is constant
- $|1\rangle$ if f is equilibrated.

What it means is : take an observable M over the first qbit, with two possible outcomes eigenvalues : $\lambda_0 \neq \lambda_1 \in \mathbb{R}$
eigenspaces :$\mathbb{C}|0\rangle, \mathbb{C}|1\rangle$.
The observation is described on the full system by $M \otimes \mathrm{Id}_2$,
eigenvalues : λ_0, λ_1
eigenspaces :$E_0 = (\mathbb{C}|0\rangle) \otimes \mathcal{B}, E_1 = (\mathbb{C}|1\rangle) \otimes \mathcal{B}$.
The observation of the first qbit will both deliver the result λ_i and project the final state on to the corresponding eigenspace :

- $\mu = \lambda_0$ if f is constant.
- $\mu = \lambda_1$ if f is equilibrated.

Deutsch algorithm

Algorithm :
1- construct the circuit
2- initialize the state with ψ_0
3- make the system evolve along the circuit
4- Make one measurement on final state :
if $\mu = \lambda_0$, output :="constant"
if $\mu = \lambda_1$, output :="equilibrated".
Note that U_f is used only once and we have tested a global property of function f.

Devil's advocate criticism

Classical circuits

C1- There is also a classical circuit with depth 2 solving the problem :
first layer : two copies of $\mathcal{O}_f$ (the "oracle"), outputs $f(0), f(1)$ in parallel
second layer :a gate $\oplus$, outputs $f(0) \oplus f(1)$
conclusion : $r = 0$ -> f is constant,$r = 1$ -> f is equilibrated.
A1 : yes. But it uses TWO copies of the circuit $\mathcal{O}_f$.

Classical circuits

C1- There is also a classical circuit with depth 2 solving the problem :
first layer : two copies of $\mathcal{O}_f$ (the "oracle"), outputs $f(0), f(1)$ in parallel
second layer :a gate $\oplus$, outputs $f(0) \oplus f(1)$
conclusion : $r = 0$ -> f is constant,$r = 1$ -> f is equilibrated.
A1 : yes. But it uses TWO copies of the circuit $\mathcal{O}_f$.
C2 [Calude, arxiv 2006] :We could define a new kind of gates, hence of circuits, that would be realizable by classical systems, and would allow linear superposition. A similar solution would be available for such linear-classical-circuits, with only one gate for f.
A2 : Yes. But extension to boolean functions with n arguments seems unpossible(? ?)

Quantum parallelism

Hadamard gate

The fundamental trick for computing all values of f, extended to n qbits, is :

$$
\begin{aligned}
H^{\otimes n}\left|0^n\right\rangle &= \bigotimes_{j=0}^{n-1} H\left|0\right\rangle = \bigotimes_{j=0}^{n-1} \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle) \\
&= \bigotimes_{j=0}^{n-1} \frac{1}{\sqrt{2}}(\sum_{z_j=0}^{1} \left|z_j\right\rangle) \\
&= \frac{1}{\sqrt{2^n}} \sum_{z_0 z_1 \cdot z_{n-1}} \otimes_{j=0}^{n-1} \left|z_j\right\rangle) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\vec{z} \in \mathbb{B}^n} \left|\vec{z}\right\rangle \qquad (1)
\end{aligned}
$$

U_f box

A single application of U_f gives :

$$\begin{aligned} U_f H^{\otimes(n+1)} |0^n\rangle |1\rangle &= \frac{1}{\sqrt{2^{n+1}}} U_f \left(\sum_{\vec{z} \in \mathbb{B}^n} |\vec{z}\rangle \right) \otimes (|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{\vec{z} \in \mathbb{B}^n} (-1)^{f(\vec{z})} |\vec{z}\rangle \otimes (|0\rangle - |1\rangle) \end{aligned}$$

Hadamard is Fourier over $(Z/2Z)^n$

Starting with an arbitrary $|\vec{x}\rangle$ instead of $|0^n\rangle$ we obtain :

$$\begin{aligned} H^{\otimes n}|\vec{x}\rangle &= \bigotimes_{j=0}^{n-1} H|x_j\rangle \\ &= \bigotimes_{j=0}^{n-1} \frac{1}{\sqrt{2}}\left(\sum_{z_j=0}^{1}(-1)^{x_j\cdot z_j}|z_j\rangle\right) \\ &= \frac{1}{\sqrt{2^n}}\sum_{z_0 z_1\cdots z_{n-1}} \otimes_{j=0}^{n-1}(-1)^{x_j\cdot z_j}|z_j\rangle) \\ &= \frac{1}{\sqrt{2^n}}\sum_{\vec{z}\in\mathbb{B}^n}(-1)^{\vec{x}\cdot\vec{z}}|\vec{z}\rangle \end{aligned} \tag{2}$$

where

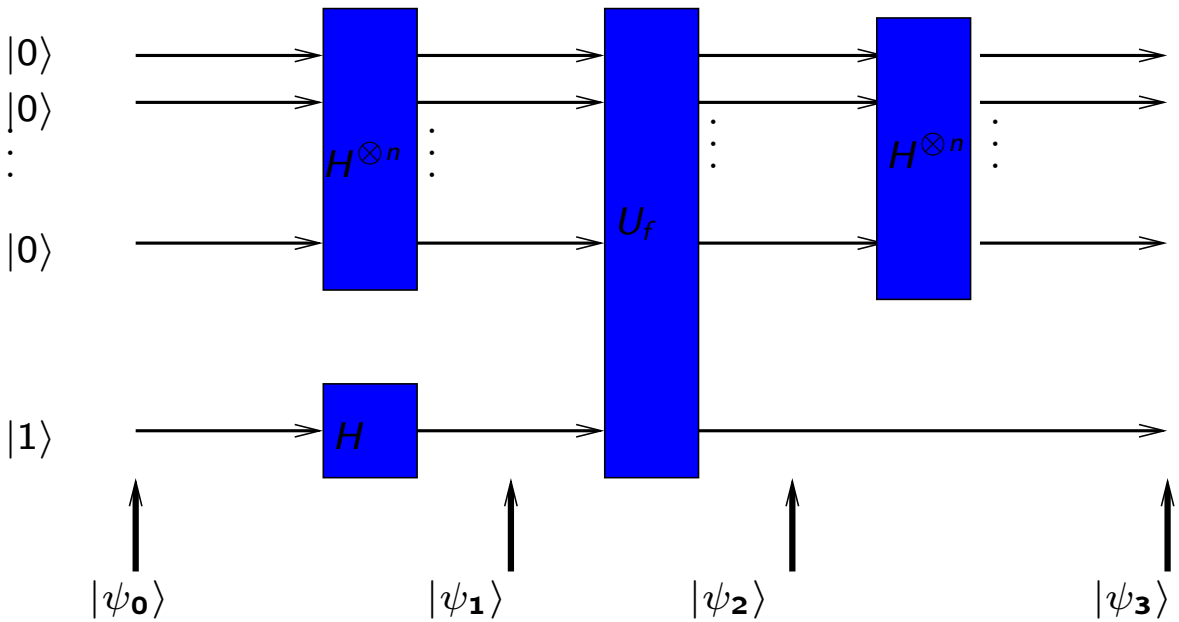
$$\vec{x}\cdot\vec{z} = x_1z_1 + x_2z_2 + \cdots x_nz_n \quad \text{in } \mathbb{Z}/2\mathbb{Z}.$$

Deutsch-Josza algorithm over boolean functions.

Deutsch-Josza problem

INPUT(v1) :$f : \{0,1\}^n \to \{0,1\}$
promised to be either *constant* or *equilibrated*.
Let $N = 2^n$.
QUESTION : Is f equilibrated ?
INPUT (v2,classical) : some circuit, with arity $(n, 1)$, that computes f.
QUESTION : Is f equilibrated ?
Classical algorithm : must evaluate f on at least $N/2 + 1$ different arguments.
Probabilistic algorithm : with k evaluations, $proba(error) \leq \frac{2\sqrt{2}}{N^{N/2}}$.
INPUT(v3,quantum) : some quantum circuit, with arity $(n, 1)$, that computes U_f.
QUESTION : Is f equilibrated ?
Quantum algorithm : a quantum circuit (involving U_f), and a q-measurement device, that gives the answer.

Deutsch-Josza circuit



Deutsch-Josza algorithm

Evolution of the system : $|\psi_0\rangle \mapsto |\psi_1\rangle \mapsto |\psi_2\rangle \mapsto |\psi_3\rangle$

step 0

$$|\psi_0\rangle = |00...0\rangle\,|1\rangle \in \mathcal{B}^{\otimes(n+1)}$$

step 1

$$\begin{aligned} |\psi_1\rangle &= H^{\otimes n}\,|0^n\rangle\,|1\rangle \\ &= \frac{1}{\sqrt{2^n}}\left[\sum_{x\in\mathbb{B}^n}|x\rangle\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \end{aligned}$$

Deutsch-Josza algorithm

Evolution of the system :

step 2

$$\begin{aligned} |\psi_2\rangle &= U_f |\psi_1\rangle \\ &= \frac{1}{\sqrt{2^n}} \left[\sum_{x \in \mathbb{B}^n} (-1)^{f(x)} |x\rangle \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \end{aligned}$$

step 3

$$\begin{aligned} |\psi_3\rangle &= H^{\otimes n} \otimes \mathrm{I}_2 |\psi_2\rangle \\ &= \left[\sum_{z \in \mathbb{B}^n} A(z) |z\rangle \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \end{aligned}$$

where, by (2)

$$A(\vec{z}) = \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \mathbb{B}^n} (-1)^{\vec{x} \cdot \vec{z} + f(x)}.$$

Deutsch-Josza algorithm

Let us evaluate $A(\vec{z})$.
if f is constant :

$$A(0^n) = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{B}^n} (-1)^{f(0^n)} = (-1)^{f(0^n)}$$

i.e.

$$|\psi_3\rangle = \pm |0^n\rangle$$

If f is equilibrated :

$$A(\vec{z}) = \frac{1}{\sqrt{2^n}} \Big(\sum_{f(\vec{x})=0} (-1)^{\vec{x}\cdot\vec{z}} + \sum_{f(\vec{x})=1} (-1)^{\vec{x}\cdot\vec{z} \oplus 1} \Big).$$

$$A(0^n) = 0.$$

i.e.

$$|\psi_3\rangle \in |0^n\rangle^{\perp}$$

Deutsch-Josza algorithm : final measurement

Final measurement

Let M be an observable on one qbit associated with a hermitian matrix $M = \begin{pmatrix} \lambda_0 & 0 \\ 0 & \lambda_1 \end{pmatrix}$ where $\lambda_i \in \mathbb{R}$.

One measures successively qbit 1, then qbit 2, etc ...and obtain results

$$\mu_1, \mu_2, \ldots, \mu_n.$$

Measurement of the k-ith qbit uses the observable

$$M_k = \mathrm{I}_{2^{k-1}} \otimes M \otimes \mathrm{I}_{2^{n-k+1}}$$

with eigenspaces

$$E_{k,0} = \mathcal{B}^{\otimes(k-1)} \otimes |0\rangle \otimes \mathcal{B}^{\otimes(n-k+1)}, \quad E_{k,1} = \mathcal{B}^{\otimes(k-1)} \otimes |1\rangle \otimes \mathcal{B}^{\otimes(n-k+1)}$$

Deutsch-Josza algorithm : final measurement

If f is constant :
$|\psi_3\rangle \in \mathbb{C}\,|0^n\rangle$ hence, with probability 1 :

$$\mu_1 = \mu_2 = \ldots = \mu_n = \lambda_0$$

If f is equilibrated :
$|\psi_3\rangle \in |0^n\rangle^{\perp}$. State reached after $k$ith measurement : η_k.
$\eta_0 \in |0^n\rangle^{\perp}$
By induction over k :
with probability 1 : $|\eta_k\rangle \in |0^n\rangle^{\perp}$
hence,
with probability 1 : $|\eta_n\rangle \in |0^n\rangle^{\perp}$,
implying that, with probability 1 :

$$(\mu_1, \mu_2, \ldots, \mu_n) \neq (\lambda_0, \lambda_0, \ldots, \lambda_0)$$

Deutsch-Josza algorithm

q-Algorithm :
1- construct the circuit for inputs of size n.
2- initialize the state with ψ_0
3- make the system evolve along the circuit
4- Make n measurements on final state :
if $\mu_1 = \mu_2 = \ldots = \mu_n = \lambda_0$, output := "constant"
otherwise, output :="equilibrated".

Comparison

In favour of q-computation :
The DJ-algorithm "evaluates" f only once.
$proba(error) = 0$, circuit uses $2n + 1$ gates,has depth 3.
Classical algorithm : must evaluate f on at least $N/2 + 1$ different arguments.
Probabilistic algorithm : with k evaluations, $proba(error) \leq \frac{2\sqrt{2}}{N^{N/2}}$.