Lecture 3: Algorithms: Phase kick-back

Luís Soares Barbosa

Universidade do Minho

HASLab HIGH-ASSURANCE SOFTWARE LABORATORY

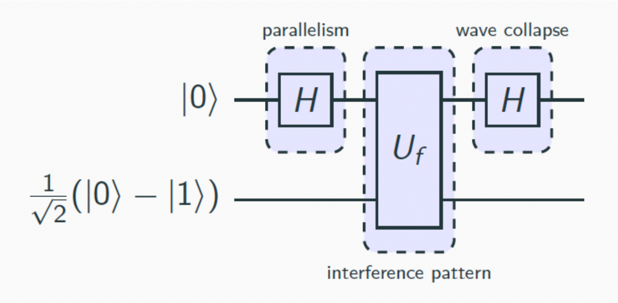
INL INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY

UNU

Mestrado em Engenharia Física

Universidade do Minho, 2025-26

Revisiting the Deutsch algorithm



Basic ingredients

- Input in superposition
- An oracle for f taking the form of a controlled gate on the input
- A specific preparation of the first qubit

Revisiting the Deutsch algorithm

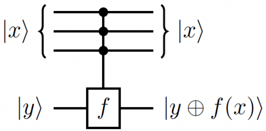
The oracle for the Deutsch algorithm

$$|x\rangle|y) \;\mapsto\; |x\rangle|y \oplus f(x)\rangle\rangle$$

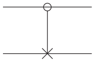
takes the form of a generalised cX gate:

$$\boxed{\sum_{x\in\{0,1\}^n} |x\rangle\langle x|\; X^{f(x)}}$$

where $X^{f(x)}$ is the identity I (when $f(x) = 0$) or X (when $f(x) = 1$).



Going even simpler: cX as an oracle



$$\overbrace{\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}}^{cX} \quad \text{corresponds to the oracle:} \quad |xy\rangle \mapsto |x, x \oplus y\rangle$$

$$\begin{aligned} cX|0\rangle|\varphi\rangle &= |0\rangle I|\varphi\rangle \\ cX|1\rangle|\varphi\rangle &= |1\rangle X|\varphi\rangle \end{aligned}$$

Seen as an oracle, note that input is presented at the control qubit and output is produced on the target qubit.

Going even simpler: cX as an oracle

Consider now a special case: prepare the target qubit with $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ which is an eigenvector of both

- X (with $\lambda = -1$) and of I (with $\lambda = 1$)
- and, thus, $X\frac{|0\rangle - |1\rangle}{\sqrt{2}} = -1\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ and $I\frac{|0\rangle - |1\rangle}{\sqrt{2}} = 1\frac{|0\rangle - |1\rangle}{\sqrt{2}}$

Therefore,

$$\begin{aligned} cX\,|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) &= |1\rangle\left(X\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \\ &= |1\rangle\left((-1)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \\ &= -|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

while $cX\,|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$

Going even simpler: cX as an oracle

A phase (1 or -1, i.e., a eigenvalue)

jumps, or is kicked back

from the second (target) to the first (control) qubit where the input is presented.

This effect is suitably recorded in the following formulation of cX:

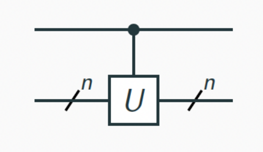
$$cX|b\rangle|-\rangle = (-1)^b|b\rangle|-\rangle \qquad \text{with } b \in \mathbf{2}$$

Observe now that, through the kick-back effect, ouput arises in the control qubit, whereas the target qubit remains unchanged.
Example:

$$cX\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

The phase kick-back pattern

This can be generalised to every controlled quantum operation:



Let v be an eigenvector of U (*i.e.* $Uv = e^{i\theta} v$). Thus,

$$
\begin{aligned}
& cU\Big((\alpha|0\rangle + \beta|1\rangle) \otimes v\Big) \\
= \;& cU(\alpha|0\rangle \otimes v + \beta|1\rangle \otimes v) \\
= \;& \alpha|0\rangle \otimes v + \beta|1\rangle \otimes Uv \\
= \;& \alpha|0\rangle \otimes v + \beta|1\rangle \otimes e^{i\theta} v \\
= \;& \alpha|0\rangle \otimes v + e^{i\theta}\beta|1\rangle \otimes v \\
= \;& (\alpha|0\rangle + e^{i\theta}\beta|1\rangle) \otimes v
\end{aligned}
$$

The phase kick-back pattern

Again

- Global phase $e^{i\theta}$ (introduced to v) was 'kicked-back' as a relative phase in the control qubit
- Some information of U is now encoded in the control qubit

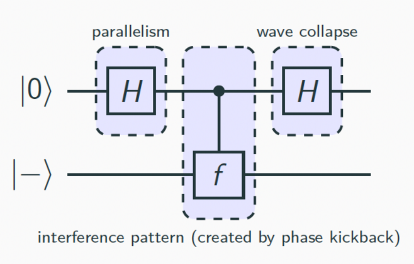
In general kicking-back such phases causes interference patterns that give away information about U.

Our two examples

Phase kick-back can be represented as

in the cX gate: $cX|b\rangle|-\rangle = (-1)^b|b\rangle|-\rangle$

in Deutsch algorithm: $U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$



A parenthesis on global/local phase

$$(\quad \ldots$$

Global phase factor

Definition

Let $|v\rangle, |u\rangle \in \mathbb{C}^{2^n}$. If $|v\rangle = e^{i\theta}|u\rangle$ we say they are equal up to global phase factor $e^{i\theta}$

Theorem

$e^{i\theta}|v\rangle$ and $|v\rangle$ are indistinguishable in the world of quantum mechanics

Proof sketch

Show that equality up to global phase is preserved by operators and normalisation; thus the probability outcomes associated with $|v\rangle$ and $e^{i\theta}|v\rangle$ are the same.

Relative phase factor

Definition

We say that vectors $\sum_{x \in 2^n} \alpha_x |x\rangle$ and $\sum_{x \in 2^n} \beta_x |x\rangle$ differ by a relative phase factor if for all $x \in 2^n$

$$\alpha_x = e^{i\theta_x} \beta_x \qquad \text{(for some angle } \theta_x\text{)}$$

Example

Vectors $|0\rangle + |1\rangle$ and $|0\rangle - |1\rangle$ differ by a relative phase factor.

Vectors that differ by a relative phase factor are distinguishable.

End of parenthesis

$\ldots \quad \Big)$

The Bernstein-Vazirani algorithm

Let $2^n = \{0,1\}^n = \{0,1,2,\cdots 2^n - 1\}$ be the set of non-negative integers (represented as bit strings up to n bits). Then, consider the following problem:

The problem

Let s be an unknown non-negative integer less than 2^n, encoded as a bit string, and consider a function $f : \{0,1\}^n \longrightarrow \{0,1\}$ which hides secret s as follows: $f(x) = x \cdot s$, where $\cdot$ is the bitwise product of x and s modulo 2. i.e.

$$x \cdot s \;=\; x_1 s_1 \oplus x_2 s_2 \oplus \cdots \oplus x_n s_n$$

Find s.

Note that juxtaposition abbreviates conjunction, i.e. $x_1 s_1 \;=\; x_1 \wedge s_1$

Setting the stage

Lemma

(1) *For* $a, b \in 2$ *the equation* $(-1)^a(-1)^b = (-1)^{a \oplus b}$ *holds.*

Proof sketch

Build a truth table for each case and compare the corresponding contents.

Lemma

(2) *For any three binary strings* $x, a, b \in 2^n$ *the equation* $(x \cdot a) \oplus (x \cdot b) = x \cdot (a \oplus b)$ *holds.*

Proof sketch

Follows from the fact that for any three bits $a, b, c \in 2$ the equation $(a \wedge b) \oplus (a \wedge c) = a \wedge (b \oplus c)$ holds.

Setting the stage

Lemma

(3) *For any element $|b\rangle$ in the computational basis of $\mathbb{C}^2$,*

$$H|b\rangle = \frac{1}{\sqrt{2}} \sum_{z \in 2} (-1)^{b \wedge z} |z\rangle$$

Proof sketch

Build a truth table and compare the corresponding contents.

Theorem

(1) *For any element $|b\rangle$ in the computational basis of $\mathbb{C}^{2^n}$,*

$$H^{\otimes n}|b\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in 2^n} (-1)^{b \cdot z} |z\rangle$$

Proof sketch

Follows by induction on the size of n.

The Bernstein-Vazirani algorithm

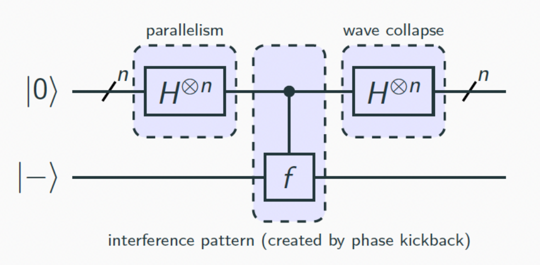
$\boxed{\text{How many times } f \text{ has to be called to determine } s\text{?}}$

- Classically, we run f n-times by computing

$$f(1\dots0) = (s_1 \wedge 1) \oplus \cdots \oplus (s_n \wedge 0) = s_1$$
$$\vdots$$
$$f(0\dots1) = (s_1 \wedge 0) \oplus \cdots \oplus (s_n \wedge 1) = s_n$$

- With a quantum algorithm, we may discover s by running f only once

The circuit


parallelism
wave collapse
|0⟩
n
H⊗n
H⊗n
n
|−⟩
f
interference pattern (created by phase kickback)

The computation

$$
\begin{array}{ll}
H^{\otimes n}|0\rangle|-\rangle & \\
= \frac{1}{\sqrt{2^n}} \sum_{z\in 2^n} |z\rangle|-\rangle & \{\text{Theorem (1)}\} \\
\overset{U_f}{\mapsto} \quad \frac{1}{\sqrt{2^n}} \sum_{z\in 2^n} (-1)^{f(z)}|z\rangle|-\rangle & \{\text{Definition}\} \\
\overset{H^{\otimes n}\otimes I}{\mapsto} \quad \frac{1}{2^n} \sum_{z\in 2^n} (-1)^{f(z)} \left(\sum_{z'\in 2^n} (-1)^{z\cdot z'} |z'\rangle \right)|-\rangle & \{\text{Theorem (1)}\} \\
= \frac{1}{2^n} \sum_{z\in 2^n} \sum_{z'\in 2^n} (-1)^{(z\cdot s)\oplus(z\cdot z')}|z'\rangle|-\rangle & \{\text{Lemma (1)}\} \\
= \frac{1}{2^n} \sum_{z\in 2^n} \sum_{z'\in 2^n} (-1)^{z\cdot(s\oplus z')}|z'\rangle|-\rangle & \{\text{Lemma (2)}\} \\
= |s\rangle|-\rangle & \{\text{Why?}\}
\end{array}
$$

Why?

$$\cdots = \frac{1}{2^n} \sum_{z \in 2^n} \sum_{z' \in 2^n} (-1)^{z \cdot (s \oplus z')} |z'\rangle|-\rangle = \cdots$$

For each z, $\frac{1}{2^n} \sum_{z=0}^{2^n-1} (-1)^{z \cdot (s \oplus z')}$ is 1 iff $(s \oplus z') = 0$, which happens only if $s = z'$ In all other cases $\frac{1}{2^n} \sum_{z=0}^{2^n-1} (-1)^{z \cdot (s \oplus z')}$ is 0.

The reason is easy to guess:

- for $s \oplus z' = 0$, $\frac{1}{2^n} \sum_{z=0}^{2^n-1} (-1)^{z \cdot (s \oplus z')} = \frac{1}{2^n} \sum_{z=0}^{2^n-1} 1 = 1$.
- for $s \oplus z' \neq 0$, as z spans all numbers from 0 to $2^n - 1$, half of the 2^n factors in the sum will be -1 and the other half 1, thus summing up to 0.

Thus, the only non-zero amplitude is the one associated with s.

Why?

Alternatively, consider the probability of measuring s at the end of the computation:

$$\left|\frac{1}{2^n}\sum_{z\in 2^n}(-1)^{z\cdot(s\oplus s)}\right|^2$$
$$=\left|\frac{1}{2^n}\sum_{z\in 2^n}(-1)^{z\cdot 0}\right|^2$$
$$=\left|\frac{1}{2^n}\sum_{z\in 2^n}1\right|^2$$
$$=\left|\frac{2^n}{2^n}\right|^2$$
$$=1$$

This means that somehow all values yielding wrong answers were completely cancelled.

Deutsch-Josza

The Problem

Take a function $f : \{0,1\}^n \rightarrow \{0,1\}$, which is known to be either constant or balanced.

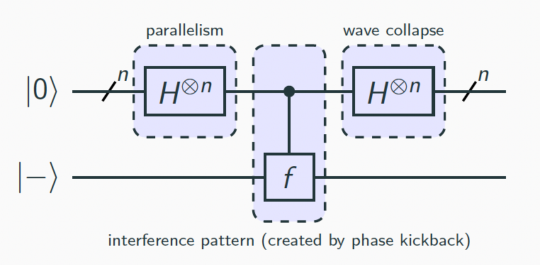
Find out which case holds.

Classically, we evaluate half of the inputs ($\frac{2^n}{2} = 2^{n-1}$), evaluate one more and run the decision procedure,

- output always the same $\Longrightarrow$ constant
- otherwise $\Longrightarrow$ balanced

which requires running f $2^{n-1}+1$ times.
A quantum algorithm replies by running f only once.

The circuit



parallelism
wave collapse
$|0\rangle$
$|-\rangle$
n
$H^{\otimes n}$
f
$H^{\otimes n}$
n
interference pattern (created by phase kickback)

The computation

$$
\begin{aligned}
& H^{\otimes n}|0\rangle|-\rangle \\
& = \frac{1}{\sqrt{2^n}} \sum_{z \in 2^n} |z\rangle|-\rangle && \{\text{Theorem } 1\} \\
& \overset{U_f}{\mapsto} \quad \frac{1}{\sqrt{2^n}} \sum_{z \in 2^n} (-1)^{f(z)} |z\rangle|-\rangle && \{\text{Definition }\} \\
& \overset{H^{\otimes n} \otimes I}{\mapsto} \quad \underbrace{\frac{1}{2^n} \sum_{z \in 2^n} (-1)^{f(z)} \left(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \right)}_{\square \text{ upper qubits}} |-\rangle && \{\text{Theorem } 1\}
\end{aligned}
$$

Developing □ by case distinction

f is constant

$$\frac{1}{2^n}\sum_{z\in 2^n}(-1)^{f(z)}\left(\sum_{z'\in 2^n}(-1)^{z\cdot z'}|z'\rangle\right)$$
$$=\frac{1}{2^n}(\pm 1)\sum_{z\in 2^n}\left(\sum_{z'\in 2^n}(-1)^{z\cdot z'}|z'\rangle\right)$$

Therefore, at state $|0\rangle$ is

$\boxed{f \text{ is constant at } 1}$ $\rightsquigarrow$ $\frac{-(2^n)}{2^n}|\mathbf{0}\rangle = -|\mathbf{0}\rangle$

$\boxed{f \text{ is constant at } 0}$ $\rightsquigarrow$ $\frac{(2^n)}{2^n}|\mathbf{0}\rangle = |\mathbf{0}\rangle$

Developing $\square$ by case distinction

Actually the probability of measuring $|0\rangle$ at the end given by

$$\left|\frac{1}{2^n}(\pm 1)\sum_{z\in 2^n}(-1)^{z\cdot 0}\right|^2$$
$$=\left|\frac{1}{2^n}(\pm 1)\sum_{z\in 2^n}1\right|^2$$
$$=\left|\frac{2^n}{2^n}\right|^2$$
$$=1$$

So if f is constant we measure $|0\rangle$ with probability 1.

Developing $\square$ by case distinction

f is balanced

$$\frac{1}{2^n} \sum_{z \in 2^n} (-1)^{f(z)} \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big)$$

$$= \frac{1}{2^n} \Big(\sum_{z \in 2^n, f(z)=0} (-1)^{f(z)} \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big)$$

$$+ \sum_{z \in 2^n, f(z)=1} (-1)^{f(z)} \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big) \Big)$$

$$= \frac{1}{2^n} \Big(\sum_{z \in 2^n, f(z)=0} \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big)$$

$$+ \sum_{z \in 2^n, f(z)=1} (-1) \Big(\sum_{z' \in 2^n} (-1)^{z \cdot z'} |z'\rangle \Big) \Big)$$

Developing $\square$ by case distinction

Probability of measuring $|0\rangle$ at the end given by

$$\begin{aligned}
&\left|\frac{1}{2^n}\left(\sum\nolimits_{z\in 2^n, f(z)=0}(-1)^{z\cdot 0}+\sum\nolimits_{z\in 2^n, f(z)=1}(-1)(-1)^{z\cdot 0}\right)\right|^2\\
&=\left|\frac{1}{2^n}\left(\sum\nolimits_{z\in 2^n, f(z)=0}1+\sum\nolimits_{z\in 2^n, f(z)=1}(-1)\right)\right|^2\\
&=\left|\frac{1}{2^n}\left(\sum\nolimits_{z\in 2^n, f(z)=0}1-\sum\nolimits_{z\in 2^n, f(z)=1}1\right)\right|^2\\
&=0
\end{aligned}$$

So if f is balanced we measure $|0\rangle$ with probability 0

Concluding

Deutsch problem

Classically, need to run f twice. With a quantum algorithm once is enough.

Berstein-Varziani problem

Classically, need to run f n times. With a quantum algorithm once is enough.

Deutsch-Joza problem

Classically, need to evaluate half of the inputs ($\frac{2^n}{2} = 2^{n-1}$), evaluate one more and run the decision procedure,

- output always the same $\Longrightarrow$ constant
- otherwise $\Longrightarrow$ balanced

With a quantum algorithm once is enough.