Quantum Algorithms

Phase Kickback,Joza,Deutsch-Joza algorithm, A direct comparison with classical computing

Anish Ghosh

UMBC

Recap from Last Week

For computational-basis states, we usually write

$$CX_{12}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle,$$

which makes it appear that only the **target qubit** changes.

However, last week we saw

$$\boxed{H^{\otimes 2} CX_{12} H^{\otimes 2} = CX_{21}.}$$

Thus, the interpretation of which qubit is being affected depends on the **state and basis** in which the controlled operation is considered.

A controlled operation can have an observable effect on the control.

Eigenvectors

In linear algebra, a nonzero vector v is called an **eigenvector** of a matrix A if

$$\boxed{Av = \lambda v}$$

for some scalar λ.

The scalar λ is called the corresponding **eigenvalue**.

Applying A to an eigenvector does not produce a new independent direction. The result remains a scalar multiple of the same vector:

$$\boxed{v \xrightarrow{A} \lambda v}$$

Eigenstates

A quantum state $|\psi\rangle$ is called an **eigenstate** of a unitary operator U if

$$\boxed{U|\psi\rangle = \lambda|\psi\rangle}$$

where λ is the corresponding **eigenvalue**.

This is the quantum analogue of an eigenvector:

$$\boxed{|\psi\rangle \xrightarrow{U} \lambda|\psi\rangle}$$

Since U is unitary,

$$|\lambda| = 1, \qquad \lambda = e^{i\theta}.$$

A Useful Eigenstate for Phase Kickback

Consider

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

For the Pauli-X gate,

$$XH|1\rangle = X\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -H|1\rangle.$$

$$\boxed{\lambda_X = -1}$$

For the identity gate,

$$IH|1\rangle = I\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = H|1\rangle.$$

$$\boxed{\lambda_I = 1}$$

$$\boxed{XH|1\rangle = -H|1\rangle, \qquad IH|1\rangle = H|1\rangle}$$

Quantum Oracle: Single-Bit Case

Consider a Boolean function

$$f : \{0,1\} \longrightarrow \{0,1\}.$$

For the phase-kickback discussion, we use the corresponding two-qubit quantum oracle

$$\boxed{U_f\left(|x\rangle \otimes |y\rangle\right) = |x\rangle \otimes |y \oplus f(x)\rangle,} \qquad x, y \in \{0,1\}.$$

The first qubit stores the input x and is unchanged, while the second qubit stores the action of f through XOR:

$$\underbrace{|x\rangle}_{\text{input}} \otimes \underbrace{|y\rangle}_{\text{target}} \quad \xrightarrow{U_f} \quad \underbrace{|x\rangle}_{\text{unchanged}} \otimes \underbrace{|y \oplus f(x)\rangle}_{\text{output}}.$$

The operation is reversible since

$$U_f^2 = I, \qquad U_f^{-1} = U_f,$$

and therefore U_f is unitary.

Recall that $\oplus$ denotes addition modulo 2.

Note: This is the single-bit oracle used here for phase kickback; it is not the most general definition of a quantum oracle.

Phase Kickback: Applying the Oracle

Prepare the target qubit in

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Therefore,

$$|x\rangle \otimes H|1\rangle = \frac{1}{\sqrt{2}} \left(|x\rangle|0\rangle - |x\rangle|1\rangle\right).$$

Apply U_f and use linearity:

$$\begin{aligned} U_f\left(|x\rangle \otimes H|1\rangle\right) &= \frac{1}{\sqrt{2}} U_f\left(|x\rangle|0\rangle - |x\rangle|1\rangle\right) \\ &= \frac{1}{\sqrt{2}} \left(U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle\right). \end{aligned}$$

Using

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

we obtain

$$\boxed{U_f\left(|x\rangle \otimes H|1\rangle\right) = |x\rangle \otimes \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}.}$$

Phase Kickback: The Two Cases

We have

$$U_f\left(|x\rangle \otimes H|1\rangle\right) = |x\rangle \otimes \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}.$$

Case 1: $f(x) = 0$

$$\begin{aligned} |x\rangle \otimes \frac{|0 \oplus 0\rangle - |1 \oplus 0\rangle}{\sqrt{2}} &= |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ &= |x\rangle \otimes H|1\rangle. \end{aligned}$$

Thus the eigenvalue is $+1$.

Case 2: $f(x) = 1$

$$\begin{aligned} |x\rangle \otimes \frac{|0 \oplus 1\rangle - |1 \oplus 1\rangle}{\sqrt{2}} &= |x\rangle \otimes \frac{|1\rangle - |0\rangle}{\sqrt{2}} \\ &= -|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ &= -|x\rangle \otimes H|1\rangle. \end{aligned}$$

Thus the eigenvalue is -1.

$$\boxed{U_f\left(|x\rangle \otimes H|1\rangle\right) = (-1)^{f(x)}\left(|x\rangle \otimes H|1\rangle\right).}$$

Phase Kickback in Superposition

Now let the first qubit be in the general state

$$\alpha_0|0\rangle + \alpha_1|1\rangle.$$

The second qubit is again prepared in

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Hence the joint state is

$$(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes H|1\rangle.$$

Applying U_f and using linearity,

$$\begin{aligned} &U_f\left[(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes H|1\rangle\right] \\ &= \alpha_0 U_f\left(|0\rangle \otimes H|1\rangle\right) + \alpha_1 U_f\left(|1\rangle \otimes H|1\rangle\right). \end{aligned}$$

From phase kickback,

$$U_f\left(|x\rangle \otimes H|1\rangle\right) = (-1)^{f(x)}|x\rangle \otimes H|1\rangle.$$

Therefore,

$$\boxed{\begin{aligned} &U_f\left[(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes H|1\rangle\right] \\ &= \left((-1)^{f(0)}\alpha_0|0\rangle + (-1)^{f(1)}\alpha_1|1\rangle\right) \otimes H|1\rangle. \end{aligned}}$$

Why Is the Phase “Kicked Back”?

For a basis state,

$$U_f\left(|x\rangle \otimes H|1\rangle\right) = (-1)^{f(x)}\left(|x\rangle \otimes H|1\rangle\right).$$

Since $(-1)^{f(x)}$ is a scalar,

$$(-1)^{f(x)}\left(|x\rangle \otimes H|1\rangle\right) = \left((-1)^{f(x)}|x\rangle\right) \otimes H|1\rangle.$$

Thus we may view the action as

$$\boxed{|x\rangle \longmapsto (-1)^{f(x)}|x\rangle,}$$

while the second qubit remains in the same state $H|1\rangle$.

For a superposition,

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

becomes

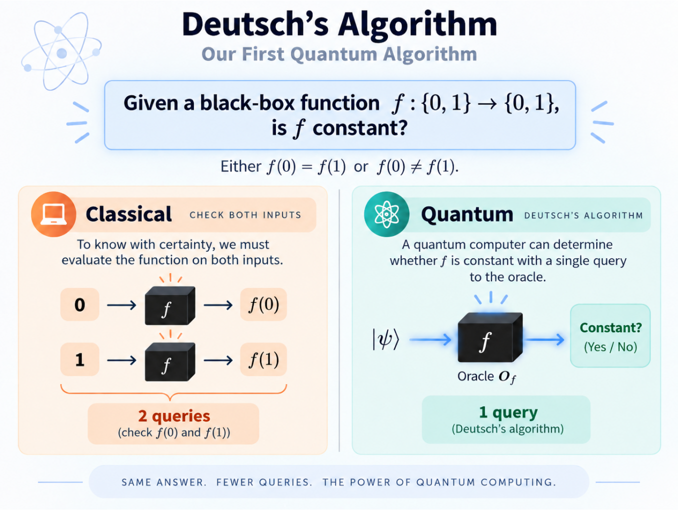
$$\boxed{(-1)^{f(0)}\alpha_0|0\rangle + (-1)^{f(1)}\alpha_1|1\rangle.}$$

Hence the values of f are encoded in the **phases of the basis-state coefficients**.

$$f(x) = 0 \Rightarrow +1, \qquad f(x) = 1 \Rightarrow -1.$$

This transfer of phase information to the first qubit is called **phase kickback**.

Deutsch's Algorithm: The Problem



Deutsch's Algorithm: What Must We Figure Out?

The oracle U_f is already given to us.

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle.$$

So the question is not how to construct the oracle.

How should we prepare and manipulate the quantum state so that one application of U_f tells us whether

$$f(0) = f(1) \qquad \text{or} \qquad f(0) \neq f(1)?$$

In other words, we need to design the circuit so that

$$\boxed{f(0) = f(1) \longrightarrow |0\rangle}$$

and

$$\boxed{f(0) \neq f(1) \longrightarrow |1\rangle}$$

on the qubit that we measure.

superposition $\longrightarrow$ phase kickback $\longrightarrow$ interference $\longrightarrow$ measurement.

Deutsch's Algorithm: Pseudocode

Input: Oracle U_f for $f : \{0,1\} \to \{0,1\}$.

Initialize

$$|\psi\rangle \leftarrow |0\rangle \otimes |1\rangle$$

Apply Hadamard gates

$$|\psi\rangle \leftarrow (H \otimes H)|\psi\rangle$$

Query the oracle

$$|\psi\rangle \leftarrow U_f|\psi\rangle$$

Apply Hadamard to the first qubit

$$|\psi\rangle \leftarrow (H \otimes I)|\psi\rangle$$

Measure

$$z \leftarrow \text{Measure}(\text{first qubit})$$

$$\begin{array}{ll} \textbf{if } z = 0, & \textbf{return } f(0) = f(1), \\ \textbf{else}, & \textbf{return } f(0) \neq f(1). \end{array}$$

$$\boxed{\textbf{Oracle queries: } 1}$$

Step 1: Apply Hadamard Gates

Start from the initialized state

$$|0\rangle \otimes |1\rangle .$$

Apply a Hadamard gate to both qubits:

$$(H \otimes H)\left(|0\rangle \otimes |1\rangle\right).$$

Using the tensor-product property,

$$\begin{aligned}(H \otimes H)\left(|0\rangle \otimes |1\rangle\right) &= H|0\rangle \otimes H|1\rangle \\ &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).\end{aligned}$$

Equivalently,

$$\boxed{\frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right)}$$

The first qubit is now in a superposition of both possible inputs, while the second qubit is in the state $H|1\rangle$ required for phase kickback.

Step 2: Query the Oracle

From Step 1, the state is

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes H|1\rangle.$$

Apply the oracle:

$$U_f\left[\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes H|1\rangle\right].$$

Using linearity,

$$\begin{aligned} &U_f\left[\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes H|1\rangle\right] \\ &= \frac{1}{\sqrt{2}}\left[U_f\left(|0\rangle \otimes H|1\rangle\right) + U_f\left(|1\rangle \otimes H|1\rangle\right)\right]. \end{aligned}$$

Since

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

the first term is

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

Step 2: Query the Oracle

For the second term,

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

Substituting the two oracle actions,

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

Therefore, after the oracle,

$$\boxed{\left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right) \otimes H|1\rangle}$$

The values $f(0)$ and $f(1)$ are now encoded in the **relative phases of the first qubit**.

Step 3: Apply Hadamard to the First Qubit

After the oracle, the state is

$$\left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right) \otimes H|1\rangle.$$

Apply H only to the first qubit:

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

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

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

$$\boxed{\frac{\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle}{2} \otimes H|1\rangle}$$

Step 4: Measurement — Case $f(0) = f(1)$

After the final Hadamard, the first qubit is

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

If

$$f(0) = f(1),$$

then

$$(-1)^{f(0)} = (-1)^{f(1)}.$$

Therefore,

$$(-1)^{f(0)} - (-1)^{f(1)} = 0,$$

so the coefficient of $|1\rangle$ vanishes.
The first qubit is therefore

$$\boxed{(-1)^{f(0)}|0\rangle}$$

which differs from $|0\rangle$ only by a global phase.
Hence,

$$\boxed{\text{Measurement gives } 0 \text{ with probability } 1.}$$

$$\boxed{0 \implies f(0) = f(1).}$$

Step 4: Measurement — Case $f(0) \neq f(1)$

After the final Hadamard, the first qubit is

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

If

$$f(0) \neq f(1),$$

then one of $f(0), f(1)$ is 0 and the other is 1, so

$$(-1)^{f(0)} = -(-1)^{f(1)}.$$

Therefore,

$$(-1)^{f(0)} + (-1)^{f(1)} = 0,$$

so the coefficient of $|0\rangle$ vanishes.
The first qubit is therefore

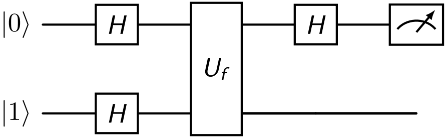
$$\boxed{\pm|1\rangle}$$

which differs from $|1\rangle$ only by a global phase.
Hence,

$$\boxed{\text{Measurement gives } 1 \text{ with probability } 1.}$$

$$\boxed{1 \Longrightarrow f(0) \neq f(1).}$$

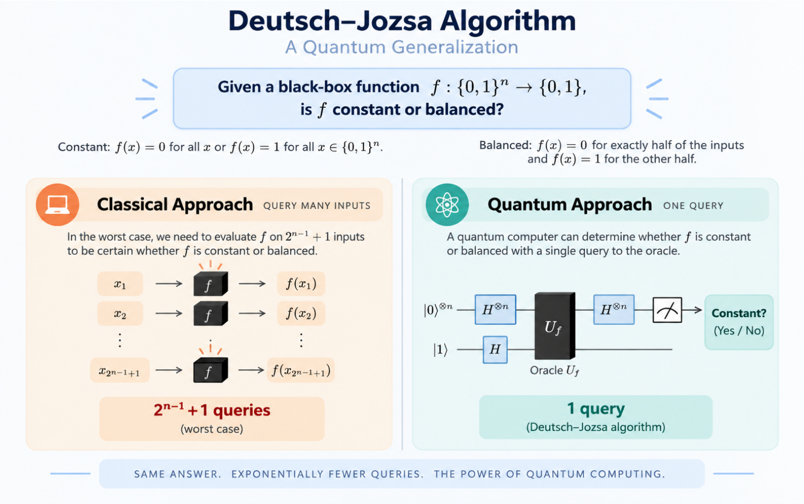
Deutsch's Algorithm: Circuit Diagram



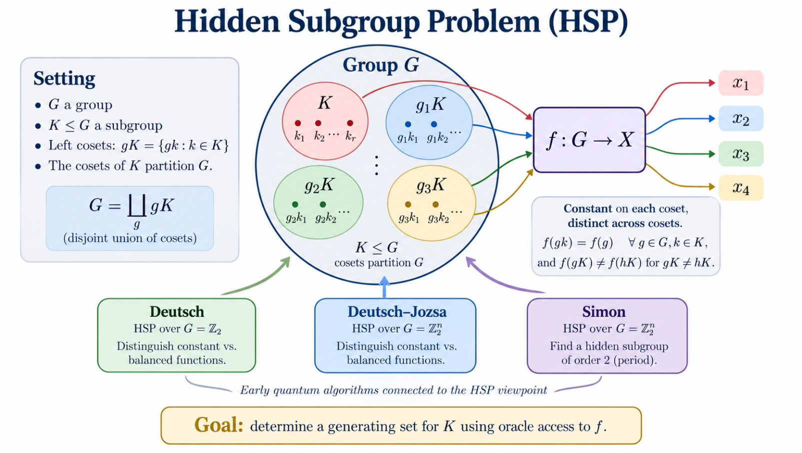
$$U_f\left(|x\rangle \otimes |y\rangle\right) = |x\rangle \otimes |y \oplus f(x)\rangle.$$

$$\boxed{\text{Measure } 0 \Rightarrow f(0) = f(1), \qquad \text{Measure } 1 \Rightarrow f(0) \neq f(1).}$$

Deutsch-Jozsa Algorithm: The Problem



HSP


Hidden Subgroup Problem (HSP)
Setting
• G a group
• $K \le G$ a subgroup
• Left cosets: $gK = \{gk : k \in K\}$
• The cosets of K partition G.
$G = \coprod_g gK$
(disjoint union of cosets)
Group G
K
k_1 $k_2 \cdots$ k_r
g_1K
g_1k_1 $g_1k_2 \cdots$
g_2K
g_2k_1 $g_2k_2 \cdots$
g_3K
g_3k_1 $g_3k_2 \cdots$
$K \le G$
cosets partition G
$f : G \to X$
x_1
x_2
x_3
x_4
Constant on each coset, distinct across cosets.
$f(gk) = f(g) \quad \forall\, g \in G, k \in K,$
and $f(gK) \neq f(hK)$ for $gK \neq hK$.
Deutsch
HSP over $G = \mathbb{Z}_2$
Distinguish constant vs. balanced functions.
Deutsch–Jozsa
HSP over $G = \mathbb{Z}_2^n$
Distinguish constant vs. balanced functions.
Simon
HSP over $G = \mathbb{Z}_2^n$
Find a hidden subgroup of order 2 (period).
Early quantum algorithms connected to the HSP viewpoint
Goal: determine a generating set for K using oracle access to f.

Motivation for Generalized Phase Kickback

Ordinary phase kickback considers a Boolean function

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

and encodes its single-bit output into a phase:

$$U_f\left(|\vec{x}\rangle_n \otimes H|1\rangle\right) = (-1)^{f(\vec{x})}|\vec{x}\rangle_n \otimes H|1\rangle.$$

But many quantum algorithms use functions with a multi-bit output,

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

We therefore want a way to extract information from $f(\vec{x})$ directly into the phase without measuring the m-qubit output register.

Generalized phase kickback uses a binary marker

$$\vec{y} \in \{0,1\}^m$$

and produces

$$\boxed{U_f\left(|\vec{x}\rangle_n \otimes H^{\otimes m}|\vec{y}\rangle_m\right) = (-1)^{\vec{y}\cdot f(\vec{x})}|\vec{x}\rangle_n \otimes H^{\otimes m}|\vec{y}\rangle_m.}$$

Binary XOR and the Binary Pairing

We work with the binary field

$$\boxed{\mathbb{F}_2 = \{0,1\}},$$

where addition is performed modulo 2:

$$0 \oplus 0 = 0, \qquad 0 \oplus 1 = 1, \qquad 1 \oplus 0 = 1, \qquad 1 \oplus 1 = 0.$$

Let

$$\vec{y} = (y_1, \ldots, y_m), \qquad \vec{z} = (z_1, \ldots, z_m) \in \{0,1\}^m.$$

For binary strings, XOR is applied componentwise:

$$\boxed{\vec{y} \oplus \vec{z} = (y_1 \oplus z_1, \ldots, y_m \oplus z_m).}$$

We also define the binary pairing

$$\boxed{\vec{y} \cdot \vec{z} = (y_1 z_1) \oplus \cdots \oplus (y_m z_m).}$$

Equivalently,

$$\vec{y} \cdot \vec{z} = \left(\sum_{i=1}^{m} y_i z_i \right) \bmod 2 \in \mathbb{F}_2.$$

Important: this is not the ordinary real-valued scalar product.
A key identity is

$$\boxed{\vec{x} \cdot (\vec{y} \oplus \vec{z}) = (\vec{x} \cdot \vec{y}) \oplus (\vec{x} \cdot \vec{z}).}$$

Source: Ossorio-Castillo, Pastor-Díaz, and Tornero [2].

What is the Marker?

Consider

$$f : \{0,1\}^n \to \{0,1\}^m, \qquad f(\vec{x}) = \big(f_1(\vec{x}), \ldots, f_m(\vec{x})\big).$$

We choose

$$\boxed{\vec{y} = (y_1, \ldots, y_m) \in \{0,1\}^m}$$

called the **marker**.
The marker selects which bits of $f(\vec{x})$ contribute:

$$\boxed{\vec{y} \cdot f(\vec{x}) = y_1 f_1(\vec{x}) \oplus \cdots \oplus y_m f_m(\vec{x}).}$$

Thus,

$$y_i = 1 \Rightarrow f_i(\vec{x}) \text{ is used}, \qquad y_i = 0 \Rightarrow f_i(\vec{x}) \text{ is ignored}.$$

The marker is prepared in the second register as

$$\boxed{H^{\otimes m}|\vec{y}\rangle_m.}$$

After applying the oracle,

$$\boxed{U_f\left(|\vec{x}\rangle_n \otimes H^{\otimes m}|\vec{y}\rangle_m\right) = (-1)^{\vec{y}\cdot f(\vec{x})}|\vec{x}\rangle_n \otimes H^{\otimes m}|\vec{y}\rangle_m.}$$

The second register stays unchanged, while the information $\vec{y} \cdot f(\vec{x})$ appears as a phase on the corresponding state $|\vec{x}\rangle_n$ in the first register.

Source: Ossorio-Castillo, Pastor-Díaz, and Tornero [2].

The Hadamard Transform

For a single qubit,

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

For an n-qubit register,

$$\boxed{H^{\otimes n} = \underbrace{H \otimes H \otimes \cdots \otimes H}_{n \text{ times}}.}$$

Let

$$\vec{x}, \vec{z} \in \{0,1\}^n.$$

The Hadamard transform of a computational basis state is

$$\boxed{H^{\otimes n} |\vec{x}\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{\vec{z} \in \{0,1\}^n} (-1)^{\vec{x} \cdot \vec{z}} |\vec{z}\rangle_n.}$$

Here

$$\vec{x} \cdot \vec{z} = \vec{x_1} \vec{z_1} \oplus \cdots \oplus \vec{x_n} \vec{z_n} \in \{0,1\}.$$

In particular, for the binary string

$$\vec{0} = 00 \cdots 0,$$

we have

$$\boxed{H^{\otimes n} |\vec{0}\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{\vec{z} \in \{0,1\}^n} |\vec{z}\rangle_n.}$$

Thus, $H^{\otimes n}$ transforms $|\vec{0}\rangle_n$ into a uniform superposition of all n-bit computational basis states.

See Nannicini [1]; Ossorio-Castillo et al. [2].

Oracle and Phase Kickback: Lemma 1

Consider a Boolean function

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

Its quantum oracle is defined by

$$\boxed{U_f\left(|\vec{x}\rangle_n \otimes |y\rangle\right) = |\vec{x}\rangle_n \otimes |y \oplus f(\vec{x})\rangle.}$$

Here,

$$\vec{x} \in \{0,1\}^n, \qquad y \in \{0,1\}.$$

Lemma 1 (Phase Kickback).
If the second qubit is prepared in

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

then

$$\boxed{U_f\left(|\vec{x}\rangle_n \otimes H|1\rangle\right) = (-1)^{f(\vec{x})}|\vec{x}\rangle_n \otimes H|1\rangle.}$$

Thus,

$$|\vec{x}\rangle_n \otimes H|1\rangle$$

is an eigenstate of U_f with eigenvalue

$$\boxed{(-1)^{f(\vec{x})}}.$$

The second qubit remains unchanged, while $f(\vec{x})$ is encoded as a phase on the corresponding state $|\vec{x}\rangle_n$.

Source: Ossorio-Castillo, Pastor-Díaz, and Tornero [2].

Generalized Phase Kickback: Lemma 2

Now consider a function with an m-bit output,

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

The corresponding oracle acts as

$$U_f\left(|\vec{x}\rangle_n \otimes |\vec{z}\rangle_m\right) = |\vec{x}\rangle_n \otimes |\vec{z} \oplus f(\vec{x})\rangle_m.$$

Choose a marker

$$\vec{y} \in \{0,1\}^m$$

and prepare the second register as

$$H^{\otimes m}|\vec{y}\rangle_m.$$

Lemma 2 (Generalized Phase Kickback).
For every

$$\vec{x} \in \{0,1\}^n,$$

we have

$$\boxed{U_f\left(|\vec{x}\rangle_n \otimes H^{\otimes m}|\vec{y}\rangle_m\right) = (-1)^{\vec{y}\cdot f(\vec{x})}|\vec{x}\rangle_n \otimes H^{\otimes m}|\vec{y}\rangle_m.}$$

Thus,

$$|\vec{x}\rangle_n \otimes H^{\otimes m}|\vec{y}\rangle_m$$

is an eigenstate of U_f with eigenvalue

$$\boxed{(-1)^{\vec{y}\cdot f(\vec{x})}.}$$

The second register remains unchanged, while $\vec{y} \cdot f(\vec{x})$ is encoded as a phase on $|\vec{x}\rangle_n$.

Source: Ossorio-Castillo, Pastor-Díaz, and Tornero [2].

References

Giacomo Nannicini.
Quantum Algorithms for Optimizers.
Society for Industrial and Applied Mathematics (SIAM), 2025.
https://doi.org/10.1137/1.9781611978766

J. Ossorio-Castillo, U. Pastor-Díaz, and J. M. Tornero, *A Generalisation of the Phase Kick-Back*, Quantum Information Processing, Vol. 22, Article 143, 2023. https://doi.org/10.1007/s11128-023-03884-8

J. Ossorio-Castillo, U. Pastor-Díaz, and J. M. Tornero, *Further Applications of the Generalised Phase Kick-Back*, arXiv preprint arXiv:2405.03850, 2024. https://arxiv.org/abs/2405.03850