

Exercises 6.1.1, 6.1.2, and 6.1.3 (pages 172–173)

Here are all the possible binary functions from $\{0,1\}$ to $\{0,1\}$, with their corresponding matrix representations shown below:

$$f_0: \begin{array}{l} 0 \mapsto 0 \\ 1 \mapsto 0 \end{array} \quad f_1: \begin{array}{l} 0 \mapsto 1 \\ 1 \mapsto 1 \end{array} \quad f_2: \begin{array}{l} 0 \mapsto 0 \\ 1 \mapsto 1 \end{array} \quad f_3: \begin{array}{l} 0 \mapsto 1 \\ 1 \mapsto 0 \end{array}$$

$$F_0 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \quad F_1 = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \quad F_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad F_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Not all of these functions are reversible. This is because some of the matrices are not unitary. The condition for a unitary matrix is $UU^\dagger = U^\dagger U = I$, but only F_2 and F_3 satisfy this property:

$$F_0 F_0^\dagger = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} \neq I$$

$$F_1 F_1^\dagger = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix} \neq I$$

$$F_2 F_2^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$F_3 F_3^\dagger = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Therefore, instead of trying to use the above matrices as quantum gates, we will construct slightly more complicated versions of them that are all unitary, and hence reversible. The corresponding gates will take two qubits as input: $|x\rangle$ and $|y\rangle$, and output the qubits $|x\rangle$ (unchanged) and $|y \oplus f(x)\rangle$. These new 4×4 matrices will operate on 2 qubits at a time, by taking as input a 4-dimensional state vector representing both qubits together, and producing a new 4-dimensional state vector as output. Each gate U_n will transform $|x\rangle$ and $|y\rangle$ to $|x'\rangle$ and $|y'\rangle$ according to the truth tables below, with the corresponding matrices shown to the right:

$U_0:$	x	y	$y \oplus f_0(x)$	x'	y'
	0	0	$0 \oplus f_0(0) = 0 \oplus 0$	0	0
	0	1	$1 \oplus f_0(0) = 1 \oplus 0$	0	1
	1	0	$0 \oplus f_0(1) = 0 \oplus 0$	1	0
	1	1	$1 \oplus f_0(1) = 1 \oplus 0$	1	1

$$U_0 = \begin{matrix} & \mathbf{00} & \mathbf{01} & \mathbf{10} & \mathbf{11} \\ \mathbf{00} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \\ \mathbf{01} & \\ \mathbf{10} & \\ \mathbf{11} & \end{matrix}$$

$U_1:$	x	y	$y \oplus f_1(x)$	x'	y'
	0	0	$0 \oplus f_1(0) = 0 \oplus 1$	0	1
	0	1	$1 \oplus f_1(0) = 1 \oplus 1$	0	0
	1	0	$0 \oplus f_1(1) = 0 \oplus 1$	1	1
	1	1	$1 \oplus f_1(1) = 1 \oplus 1$	1	0

$$U_1 = \begin{matrix} & \mathbf{00} & \mathbf{01} & \mathbf{10} & \mathbf{11} \\ \mathbf{00} & \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \\ \mathbf{01} & \\ \mathbf{10} & \\ \mathbf{11} & \end{matrix}$$

$U_2:$	x	y	$y \oplus f_2(x)$	x'	y'
	0	0	$0 \oplus f_2(0) = 0 \oplus 0$	0	0
	0	1	$1 \oplus f_2(0) = 1 \oplus 0$	0	1
	1	0	$0 \oplus f_2(1) = 0 \oplus 1$	1	1
	1	1	$1 \oplus f_2(1) = 1 \oplus 1$	1	0

$$U_2 = \begin{matrix} & \mathbf{00} & \mathbf{01} & \mathbf{10} & \mathbf{11} \\ \mathbf{00} & \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} \\ \mathbf{01} & \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix} \\ \mathbf{10} & \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix} \\ \mathbf{11} & \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix} \end{matrix}$$

$U_3:$	x	y	$y \oplus f_3(x)$	x'	y'
	0	0	$0 \oplus f_3(0) = 0 \oplus 1$	0	1
	0	1	$1 \oplus f_3(0) = 1 \oplus 1$	0	0
	1	0	$0 \oplus f_3(1) = 0 \oplus 0$	1	0
	1	1	$1 \oplus f_3(1) = 1 \oplus 0$	1	1

$$U_3 = \begin{matrix} & \mathbf{00} & \mathbf{01} & \mathbf{10} & \mathbf{11} \\ \mathbf{00} & \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix} \\ \mathbf{01} & \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} \\ \mathbf{10} & \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix} \\ \mathbf{11} & \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix} \end{matrix}$$

Each of these matrices has the property $U_n^\dagger = U_n$, meaning they are all hermitian. Furthermore, each one is unitary, since U_n^\dagger acts as U_n 's inverse: $U_n U_n^\dagger = U_n^\dagger U_n = I$. Hence, each one is reversible and its own inverse:

$$U_0 U_0^\dagger = U_0^\dagger U_0 = U_0 U_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I$$

$$U_1 U_1^\dagger = U_1^\dagger U_1 = U_1 U_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I$$

$$U_2 U_2^\dagger = U_2^\dagger U_2 = U_2 U_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I$$

$$U_3 U_3^\dagger = U_3^\dagger U_3 = U_3 U_3 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I$$

For each of the corresponding gates, if we hold the y input fixed at 0 and ignore the x' output, focusing only on how the x input is transformed into the y' output, we get the following behaviors, which match the functions f_0 , f_1 , f_2 , and f_3 :

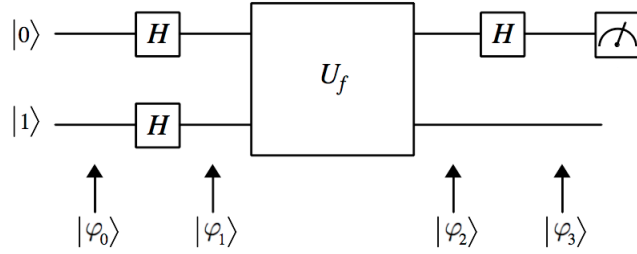
$U_0:$	x	$0 \oplus f_0(x)$	y'
	0	$0 \oplus f_0(0) = 0 \oplus 0$	0
	1	$0 \oplus f_0(1) = 0 \oplus 0$	0

$U_1:$	x	$0 \oplus f_1(x)$	y'
	0	$0 \oplus f_1(0) = 0 \oplus 1$	1
	1	$0 \oplus f_1(1) = 0 \oplus 1$	1

$U_2:$	x	$0 \oplus f_2(x)$	y'
	0	$0 \oplus f_2(0) = 0 \oplus 0$	0
	1	$0 \oplus f_2(1) = 0 \oplus 1$	1

$U_3:$	x	$0 \oplus f_3(x)$	y'
	0	$0 \oplus f_3(0) = 0 \oplus 1$	1
	1	$0 \oplus f_3(1) = 0 \oplus 0$	0

Deutsch's algorithm (standard version)



$$|\varphi_0\rangle = |0\rangle \otimes |1\rangle$$

$$|\varphi_1\rangle = H|0\rangle \otimes H|1\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix}$$

$$U_0|\varphi_1\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = +H|0\rangle \otimes H|1\rangle \quad (\text{constant})$$

$$U_1|\varphi_1\rangle = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{bmatrix} = \begin{bmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = -H|0\rangle \otimes H|1\rangle \quad (\text{constant})$$

$$U_2|\varphi_1\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = +H|1\rangle \otimes H|1\rangle \quad (\text{balanced})$$

$$U_3|\varphi_1\rangle = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = -H|1\rangle \otimes H|1\rangle \quad (\text{balanced})$$

In general, $|\varphi_2\rangle = U_f|\varphi_1\rangle = \begin{cases} \pm H|0\rangle \otimes H|1\rangle & \text{if } f \text{ is constant} \\ \pm H|1\rangle \otimes H|1\rangle & \text{if } f \text{ is balanced} \end{cases}$

The first qubit of $|\varphi_2\rangle$ will be in one of the states $\pm H|0\rangle$ or $\pm H|1\rangle$, in which the component amplitudes are all $\pm\frac{1}{\sqrt{2}}$. Therefore, measuring this qubit will not provide any useful information, because the probability of obtaining $|0\rangle$ or $|1\rangle$ is $\frac{1}{2}$ in all cases. However, since the H operator is unitary and hermitian, applying an H gate to $\pm H|0\rangle$ will give $H(\pm H|0\rangle) = \pm HH|0\rangle = \pm|0\rangle$, and likewise applying it to $\pm H|1\rangle$ will give $\pm|1\rangle$:

$$(H \otimes I)U_0|\varphi_1\rangle = \begin{bmatrix} H \otimes I \\ \\ \\ \\ \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = +|0\rangle \otimes H|1\rangle \quad (\text{constant})$$

$$(H \otimes I)U_1|\varphi_1\rangle = \begin{bmatrix} H \otimes I \\ \\ \\ \\ \end{bmatrix} \begin{bmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{bmatrix} = \begin{bmatrix} \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = -|0\rangle \otimes H|1\rangle \quad (\text{constant})$$

$$(H \otimes I)U_2|\varphi_1\rangle = \begin{bmatrix} H \otimes I \\ \\ \\ \\ \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = +|1\rangle \otimes H|1\rangle \quad (\text{balanced})$$

$$(H \otimes I)U_3|\varphi_1\rangle = \begin{bmatrix} H \otimes I \\ \\ \\ \\ \end{bmatrix} \begin{bmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = -|1\rangle \otimes H|1\rangle \quad (\text{balanced})$$

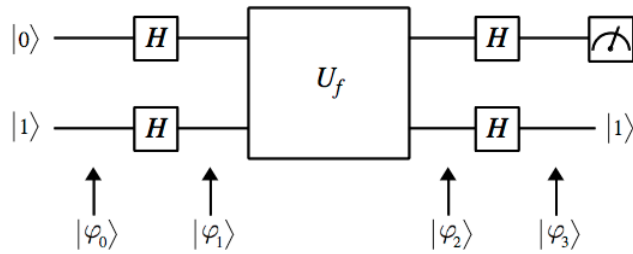
In general, $|\varphi_3\rangle = (H \otimes I)U_f|\varphi_1\rangle = \begin{cases} \pm|0\rangle \otimes H|1\rangle & \text{if } f \text{ is constant} \\ \pm|1\rangle \otimes H|1\rangle & \text{if } f \text{ is balanced} \end{cases}$

We can now obtain useful information by measuring the first qubit of $|\varphi_3\rangle$. If we get $|0\rangle$, that means f is constant; if we get $|1\rangle$, that means f is balanced. Thus with only a single application of U_f we can determine with certainty whether f is constant or balanced, whereas with a classical computer we would have had to evaluate f twice.

Summary:

1. $(H \otimes I)U_f(H \otimes H)|01\rangle$
2. Measure first qubit: $|0\rangle \Rightarrow f$ is constant, $|1\rangle \Rightarrow f$ is balanced

Deutsch's algorithm (Marshall's variation)



We can apply H to *both* output qubits instead of just the top one, although this is not necessary. Doing so turns the bottom qubit $H|1\rangle$ back into $|1\rangle$. The final output state $|\varphi_3\rangle$ is then:

$$(H \otimes H)U_0|\varphi_1\rangle = \begin{bmatrix} H \otimes H \\ \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = +|0\rangle \otimes |1\rangle \quad (\text{constant})$$

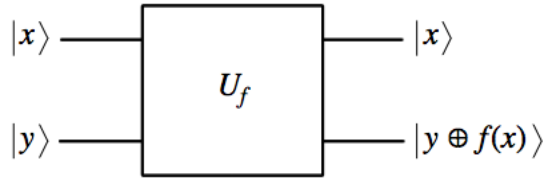
$$(H \otimes H)U_1|\varphi_1\rangle = \begin{bmatrix} H \otimes H \\ \begin{bmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = -|0\rangle \otimes |1\rangle \quad (\text{constant})$$

$$(H \otimes H)U_2|\varphi_1\rangle = \begin{bmatrix} H \otimes H \\ \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = +|1\rangle \otimes |1\rangle \quad (\text{balanced})$$

$$(H \otimes H)U_3|\varphi_1\rangle = \begin{bmatrix} H \otimes H \\ \begin{bmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = -|1\rangle \otimes |1\rangle \quad (\text{balanced})$$

In general, $|\varphi_3\rangle = (H \otimes H)U_f|\varphi_1\rangle = \begin{cases} \pm|0\rangle \otimes |1\rangle & \text{if } f \text{ is constant} \\ \pm|1\rangle \otimes |1\rangle & \text{if } f \text{ is balanced} \end{cases}$

Analysis of Deutsch's algorithm



When $|y\rangle$ is the basis state $|0\rangle$ or $|1\rangle$, applying U_f gives:

- $U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |0 \oplus f(x)\rangle = |x\rangle \otimes |f(x)\rangle$
- $U_f(|x\rangle \otimes |1\rangle) = |x\rangle \otimes |1 \oplus f(x)\rangle = |x\rangle \otimes |\overline{f(x)}\rangle$

When $|y\rangle$ is the superposition state $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, applying U_f gives:

$$\begin{aligned}
 & U_f\left(|x\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)\right) \\
 = & U_f\left(|x\rangle \otimes \frac{1}{\sqrt{2}}|0\rangle - |x\rangle \otimes \frac{1}{\sqrt{2}}|1\rangle\right) \\
 = & U_f\left(\frac{1}{\sqrt{2}}|x\rangle \otimes |0\rangle - \frac{1}{\sqrt{2}}|x\rangle \otimes |1\rangle\right) \\
 = & U_f\left(\frac{1}{\sqrt{2}}|x\rangle \otimes |0\rangle\right) - U_f\left(\frac{1}{\sqrt{2}}|x\rangle \otimes |1\rangle\right) \quad \text{since } U_f \text{ is a linear operator} \\
 = & \frac{1}{\sqrt{2}}U_f(|x\rangle \otimes |0\rangle) - \frac{1}{\sqrt{2}}U_f(|x\rangle \otimes |1\rangle) \quad \text{since } U_f \text{ is a linear operator} \\
 = & \frac{1}{\sqrt{2}}(|x\rangle \otimes |f(x)\rangle) - \frac{1}{\sqrt{2}}(|x\rangle \otimes |\overline{f(x)}\rangle) \\
 = & \left(|x\rangle \otimes \frac{1}{\sqrt{2}}|f(x)\rangle\right) - \left(|x\rangle \otimes \frac{1}{\sqrt{2}}|\overline{f(x)}\rangle\right) \\
 = & |x\rangle \otimes \left(\frac{1}{\sqrt{2}}|f(x)\rangle - \frac{1}{\sqrt{2}}|\overline{f(x)}\rangle\right) \\
 = & \begin{cases} |x\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = |x\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) & \text{if } f(x) = 0 \\ |x\rangle \otimes \left(\frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle\right) = |x\rangle \otimes -\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) & \text{if } f(x) = 1 \end{cases}
 \end{aligned}$$

which, using some fancy notation, we can write more concisely as:

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

since $(-1)^{f(x)}$ is $+1$ when $f(x) = 0$ and -1 when $f(x) = 1$

In general, $A \otimes \alpha B = \alpha A \otimes B$, so we can move the sign coefficient $(-1)^{f(x)}$ from the second qubit to the first qubit, which gives us a general expression for the output of U_f when applied to the input qubits $|x\rangle$ and $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$:

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

Now let's put the first qubit in the superposition state $|x\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. The output becomes:

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

The precise state of the first output qubit depends on the behavior of the function f at 0 and 1, whereas the state of the second output is the same as the second input. Specifically, the first output qubit is:

$$(-1)^{f(0)} \frac{1}{\sqrt{2}}|0\rangle + (-1)^{f(1)} \frac{1}{\sqrt{2}}|1\rangle = \begin{cases} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle & \text{if } f \text{ is the "constant 0" function} \\ -\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle & \text{if } f \text{ is the "constant 1" function} \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle & \text{if } f \text{ is the identity function} \\ -\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle & \text{if } f \text{ is the NOT function} \end{cases}$$

which we can rewrite in the equivalent form below:

$$\text{state of the first output qubit} = \begin{cases} + \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) & \text{if } f \text{ is the "constant 0" function} \\ - \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) & \text{if } f \text{ is the "constant 1" function} \\ + \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) & \text{if } f \text{ is the identity function} \\ - \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) & \text{if } f \text{ is the NOT function} \end{cases}$$

We now apply a final Hadamard gate H to the first output qubit. Since H is a linear operator, $H(\alpha|\psi\rangle) = \alpha H(|\psi\rangle)$, which means that the \pm signs remain the same:

$$\text{state of the first output qubit} = \begin{cases} +|0\rangle & \text{if } f \text{ is the "constant 0" function} \\ -|0\rangle & \text{if } f \text{ is the "constant 1" function} \\ +|1\rangle & \text{if } f \text{ is the identity function} \\ -|1\rangle & \text{if } f \text{ is the NOT function} \end{cases}$$

Now when we measure the first output qubit, we will get 0 with 100% certainty if f is a constant function, or 1 with 100% certainty if f is a balanced function (identity or NOT). We can thus determine, using just one application of U_f , whether the function f is constant or balanced. With a classical computer, we would need to evaluate f twice in order to determine this.