Deutsch's algorithm

Assume some function $f:\{0,1\} \to \{0,1\}$

<u>Question:</u> Is f constant $(f(0)=f(1))$
or is f balanced $(f(0) \neq f(1))$

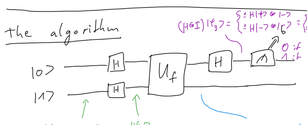
<u>Assumption</u>
f is implemented as unitary U_f
$U_f|x,y\rangle = |x, y \oplus f(x)\rangle$

Bad approach:

⇒ not unitary

<u>Fact:</u> If f can be implemented with a classical circuit, then U_f can be impl. with a Q circuit (or twice the size)

The algorithm



$(H\otimes I)|\psi_3\rangle = \begin{cases} \frac{1}{2}: H|+\rangle \otimes |-\rangle \\ \frac{1}{2}: H|-\rangle \otimes |-\rangle \end{cases} = \begin{cases} |0\rangle \otimes |-\rangle \\ |1\rangle \otimes |-\rangle \end{cases}$

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

$H|0\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = |+\rangle$

$H|1\rangle = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} = |-\rangle$

$H|+\rangle = |0\rangle$
$H|-\rangle = |1\rangle$

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
$|0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle$
$|1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle$

$|\psi_1\rangle = |0\rangle \otimes |1\rangle = |01\rangle$

$|\psi_2\rangle = (H\otimes H)|\psi_1\rangle$
$= (H\otimes H)(|0\rangle \otimes |1\rangle)$
$= H|0\rangle \otimes H|1\rangle$
$= |+\rangle \otimes |-\rangle$
$= \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$
$= \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$

$|\psi_3\rangle = U_f(\text{———} \;''\; \text{———})$
$= \frac{1}{2}|0, f(0)\rangle - \frac{1}{2}|0, \overline{f(0)}\rangle + \frac{1}{2}|1\, f(1)\rangle - \frac{1}{2}|1\, \overline{f(1)}\rangle$

$|\psi_3\rangle = U_f|\psi_2\rangle$
$= \begin{cases} \pm\, |+\rangle \otimes |-\rangle \\ \pm\, |-\rangle \otimes |-\rangle \end{cases}$

=

$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$	$f(0)$	$f(1)$
+	−	+	−	0	0
−	+	−	+	1	1
−	+	+	−	1	0
+	−	−	+	0	1

} same up to ±
} same up to ±

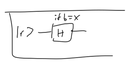
$= \begin{cases} \pm\, |+\rangle \otimes |-\rangle & (f(0)=f(1)) \\ \pm\, |-\rangle \otimes |-\rangle & (f(0) \neq f(1)) \end{cases}$

Toy crypto example

$|0\rangle, |1\rangle$ $|+\rangle, |-\rangle$

- Alice has a secret bit/basis $b \in \{+, \times\}$
- Choose random $r \in \{0,1\}$
- Encodes r in basis $+$ or $\times$ (dep. on b)

b	r	$\|\psi\rangle$
+	0	$\|0\rangle$
+	1	$\|1\rangle$
×	0	$\|+\rangle$
×	1	$\|-\rangle$



- Alice sends $|\psi\rangle$ (to adv.)

Is this secure? (Does this hide b?)

<u>Sec. def:</u> $|\psi\rangle$ (for $b=+$) should be physically indistinguishable for $|\psi\rangle$ (for $b=\times$).

<u>Quantum state probability distrib / ensemble:</u>

$E_+ = \{ |0\rangle @ \frac{1}{2}, \; |1\rangle @ \frac{1}{2} \}$
$E_\times = \{ |+\rangle @ \frac{1}{2}, \; |-\rangle @ \frac{1}{2} \}$

Q: Are E_+ and $E_\times$ <u>phys indist.</u>?

What does <u>phys indist</u> mean?

E, E' are phys. indist. if for <u>any</u> Q circuit C, we have:
Prob. distrib of meas outcomes in $C(E)$
= ——— " ——— in $C(E')$

The Q circuit can contain:
- unitaries
- measurements
- add subsystems $(|\phi\rangle \mapsto |\phi\rangle \otimes |r\rangle)$

<u>Our approach:</u>
1) Describe mathematically what the 3 Q circuit ops can do to Q st. pr. distr.
2) Find a compact representation of QSPD s.t. we can compute all these ops on the compact repr.

<u>Unitary:</u> $E = \{ |\phi_1\rangle @ p_1, \dots, |\phi_n\rangle @ p_n \}$
$\downarrow$ apply U
$UE = \{ U|\phi_1\rangle @ p_1, \dots, U|\phi_n\rangle @ p_n \}$

<u>Adding subsystem $|r\rangle$</u>

$E = \{ |\phi_1\rangle @ p_1, \dots, |\phi_n\rangle @ p_n \}$
$\downarrow \otimes |r\rangle$
$E \otimes |r\rangle = \{ |\phi_1\rangle \otimes |r\rangle @ p_1, \dots, |\phi_n\rangle \otimes |r\rangle @ p_n \}$

<u>Measurement:</u> $M = \{ P_1, \text{———}, P_k \}$

$E = \{ |\phi_1\rangle @ p_1 \text{———} |\phi_n\rangle @ p_n \}$
$\downarrow M$

$\frac{P_1|\phi_1\rangle}{\|P_1|\phi_1\rangle\|}, 1$ $\quad \frac{P_2|\phi_1\rangle}{\|\cdots\|}, 2$ $\quad \frac{P_3|\phi_1\rangle}{\|\cdots\|}, 3$ $\quad \dots$ $\quad \frac{P_k|\phi_1\rangle}{\|\cdots\|}, k$ $\quad \frac{P_2|\phi_2\rangle}{\|\cdots\|}, 2$ $\quad \frac{P_3|\phi_2\rangle}{\|\cdots\|}, 3$ etc etc

$\left(\frac{P_j|\phi_\ell\rangle}{\|P_j|\phi_\ell\rangle\|}, j \right) @ p_\ell \cdot \underbrace{\Pr[\text{outcome } j \text{ given } |\phi_\ell\rangle]}_{\|P_j|\phi_\ell\rangle\|^2}$ $\quad (j = 1 \dots k, \; \ell = 1 \dots n)$

$\Pr[\text{outcome } j] = \sum_{\ell=1}^{n} p_\ell \|P_j|\phi_\ell\rangle\|^2$

What is $E_{M\to j}$, the QSPD in case of outcome j

$E_{M\to j} = \left\{ \frac{P_j|\phi_\ell\rangle}{\|P_j|\phi_\ell\rangle\|} @ \frac{p_\ell \|P_j|\phi_\ell\rangle\|^2}{\Pr[\text{outcome } j]} \right\}_{\ell=1\dots n}$

A, B RV
$\Pr[A=a \mid B=b] = \frac{\Pr[A=a \wedge B=b]}{\Pr[B=b]}$

New idea: density operator (density matrix)

For $E = \{ |\phi_1\rangle @ p_1 \text{———} |\phi_n\rangle @ p_n \}$
the density op $\rho_E := \sum_{j=1}^{n} p_j |\phi_j\rangle\langle\phi_j|$

$\langle\phi_j| = |\phi_j\rangle^\dagger$
Eg: $|\phi_j\rangle = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \Rightarrow \langle\phi_j| = (1 \;\; 2)$
$\rightsquigarrow |\phi_j\rangle\langle\phi_j| = \begin{pmatrix} 1 \\ 2 \end{pmatrix} (1 \;\; 2) = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$

Important: If $|\phi_j\rangle$ is Q state, then $|\phi_j\rangle\langle\phi_j|$ is projector onto $|\phi_j\rangle$

We will see:
Given ρ_E, we can compute many of the above things much more easily