Last week:

- Review of Problem Set 1

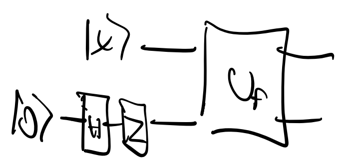
This week:

- Bit vs. phase oracles
- "Multi-output" Deutsch-Josza

For a function $f\colon \{0,1\}^n \to \{0,1\}^n$, denote by U_f the unitary $|x,y\rangle \mapsto |x,(y \oplus f(x))\rangle$.

(a) Suppose $n = 1$. Show how to build a circuit that computes the unitary $|x\rangle \mapsto (-1)^{f(x)}|x\rangle$ (known as the phase oracle). You may use Z gates, ancilla qubits initialized to $|0\rangle$, and **two** U_f gates. You must ensure that any ancilla qubits return to the state $|0\rangle$ so that they can be safely discarded. Prove that your circuit is correct.

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



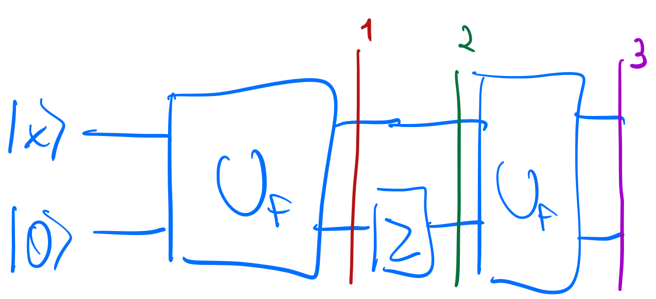
$$\Rightarrow |x\rangle|0\rangle \mapsto (-1)^{f(x)}|x\rangle|0\rangle$$

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

$$f:\{0,1\}^n \to \{0,1\}^n \quad \begin{cases} \text{Condition 1: } f(x)=y \\ \text{Condition 2: } f \text{ is a bije} \end{cases}$$

1 query to U_f

$\Omega(n)$ queries to f



$$\begin{cases} |x\rangle|0\rangle \text{ if } f(x)=0 \\ -|x\rangle|1\rangle \text{ if } f(x)=1 \end{cases}$$

$$f(x)\oplus f(x)=0$$

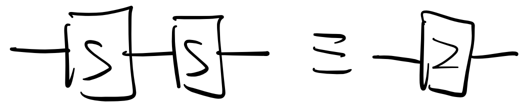
$$|x\rangle|0\rangle \xmapsto{1} |x\rangle|f(x)\rangle \xmapsto{2} (-1)^{f(x)}|x\rangle|f(x)\rangle \xmapsto{3} (-1)^{f(x)}|x\rangle|0\rangle$$

(b) Suppose now (and for the remaining parts of this question) that $n = 2$. The gate S maps $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto i\,|1\rangle$. Show that $S^2 = Z$.

$S|0\rangle = |0\rangle$

$S|1\rangle = i|1\rangle$

$S^2 = Z$



$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

$S^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$

$S^2|0\rangle = |0\rangle = Z|0\rangle$

$S^2|1\rangle = S \cdot (i|1\rangle)$

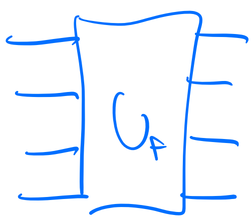
$= i^2|1\rangle$

$= -|1\rangle = Z|1\rangle$

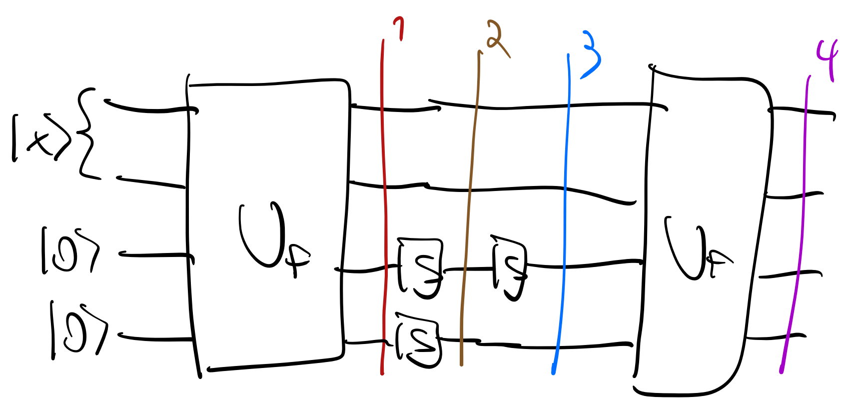
(c) Show how to build a circuit that computes the unitary that maps $|x\rangle \mapsto i^{\,2f(x)_1+f(x)_2}\,|x\rangle$, where $f(x)_1, f(x)_2$ are the first and second bits of $f(x)$, respectively. You may use S gates, ancilla qubits initialised to $|0\rangle$, and **two** U_f gates. You must ensure that any ancilla qubits return to the state $|0\rangle$ so that they can be safely discarded. Prove that your circuit is correct.

$f: \{0,1\}^2 \to \{0,1\}^2$

$$U_f \rightsquigarrow |x\rangle|00\rangle \;\Big\downarrow\; i^{2f(x)_1+f(x)_2}\,|x\rangle|00\rangle$$



$$U_f|x_1\rangle|x_2\rangle|y_1\rangle|y_2\rangle$$
$$= |x_1\rangle|x_2\rangle|f(x)_1 \oplus y_1\rangle|f(x)_2 \oplus y_2\rangle$$



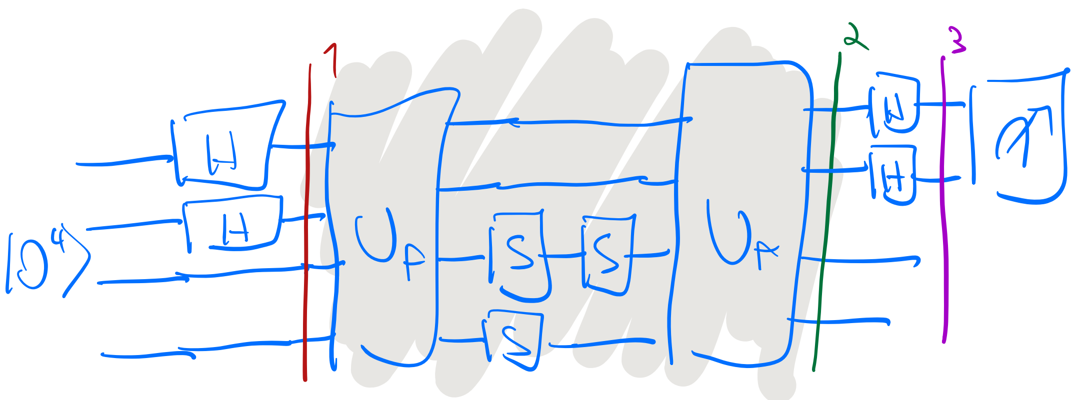
$$|x\rangle|00\rangle \;\Big\downarrow\; i^{2f(x)_1}\,|x\rangle|00\rangle$$

$(-1)^{f(x)_1}$

(d) Design a circuit that determines whether f is constant or one-to-one. You may use:

- any number of qubits initialized to $|0\rangle$,
- Hadamard (H) gates,
- S gates,
- measurements in the computational basis, and
- **two** U_f gates.

Prove that your circuit is correct.



$$|0000\rangle \xmapsto{1} \frac{1}{2}\sum_{x\in\{0,1\}^2} |x\rangle|00\rangle \xmapsto{2} \frac{1}{2}\sum_x i^{2f(x)_1+f(x)_2}|x\rangle|00\rangle$$

$$\xmapsto{3} \frac{1}{4}\sum_x\sum_y (-1)^{x\cdot y}\, i^{2f(x)_1+f(x)_2}|y\rangle|00\rangle$$

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2}^n}\sum_y (-1)^{x\cdot y}|y\rangle$$

$$H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2}^n}\sum_y |y\rangle$$

$$\left|\frac{1}{4}\sum_x i^{2f(x)_1+f(x)_2}\right|^2 \begin{cases} 1 \text{ if } f \text{ c.} \\ 0 \text{ if } 1\text{-to-}1 \end{cases}$$

$$i^0+i+i^2+i^3=0$$

$ab \mapsto 2a+b$

$00 \mapsto 0$

$01 \mapsto 1$

$10 \mapsto 2$

$11 \mapsto 3$