Simon's Algorithm and Fourier Sampling

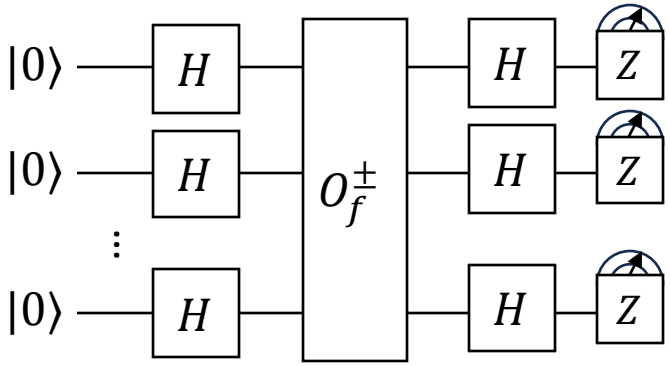
CPSC 4470/5470

Introduction to Quantum Computing

Instructor: Prof. **Yongshan Ding**

Computer Science, Applied Physics, Yale Quantum Institute

Power of Phase Oracles

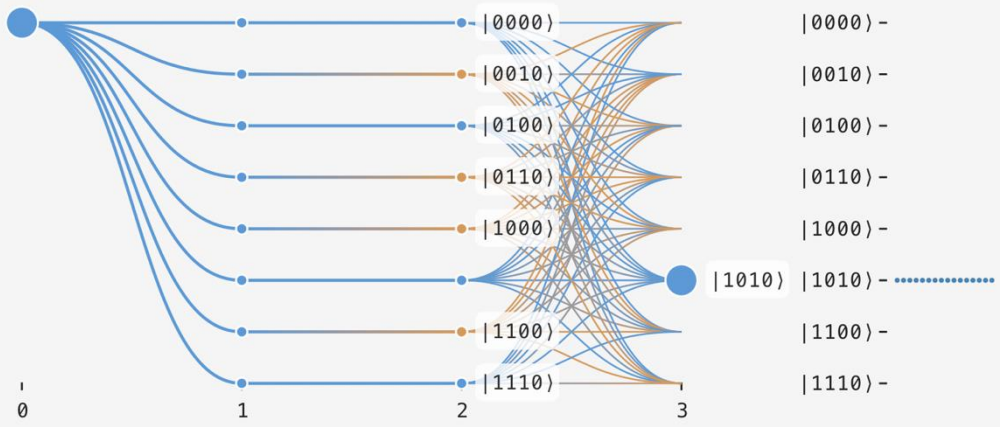


Quantum Algorithmic Recipe:

1. **Superposition**: $H^{\otimes n}$
2. **Query**: $O_f^{\pm} = \sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle\langle x|$
3. **Interference**: $H^{\otimes n}$

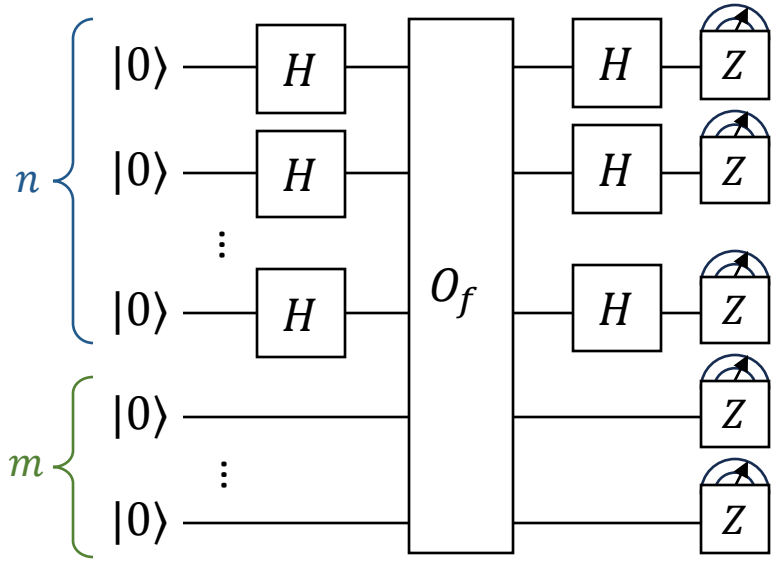
Revealing "patterns" in $f:\{0,1\}^n \to \{0,1\}$:

- (Deutsch-Jozsa) Distinguishing either **constant/balanced** functions:
  - $f(x)$ outputs consistently or equal mix of 0s and 1s.
- (Bernstein-Vazirani) Extracting **secret string** s from a function:
  - $f(x) = x \cdot s = \sum_i x_i s_i \pmod 2$, for some $s \in \{0,1\}^n$.



Bernstein-Vazirani: secret string 101

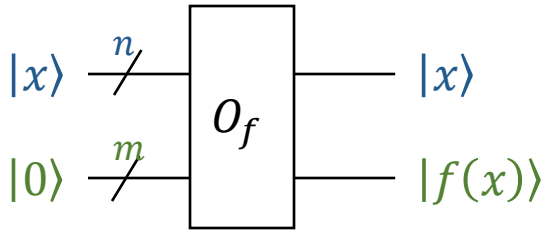
Can We Do More with Bit Oracles?



Bit oracle for function $f: \{0,1\}^n \to \{0,1\}^m$

$$O_f = \sum_{x \in \{0,1\}^n} |x\rangle\langle x| \otimes \left(X^{f(x)_0} \otimes \cdots \otimes X^{f(x)_{m-1}}\right)$$

Bit Oracle:



What patterns of f can we reveal?

Can You Guess the Period?

Boolean function $f: \{0,1\}^3 \to \{0,1\}^2$

Promise: this is a **periodic** function:

$\forall x, f(x) = f(x \oplus s)$ for some non-zero s.

Bit-wise add (mod 2): $x \oplus s = (x_0 \oplus s_0, x_1 \oplus s_1, \ldots, x_{n-1} \oplus s_{n-1})$

E.g., $110 \oplus 010 = 100$

Question: What is the period s?

	Input: x	Output: $f(x)$
000	000	01
$000 \oplus 011$	011	01

Input: x	Output: $f(x)$
000	01
001	10
010	10
011	01
100	11
101	00
110	00
111	11

Can You Guess the Period?

Boolean function $f: \{0,1\}^5 \to \{0,1\}^3$

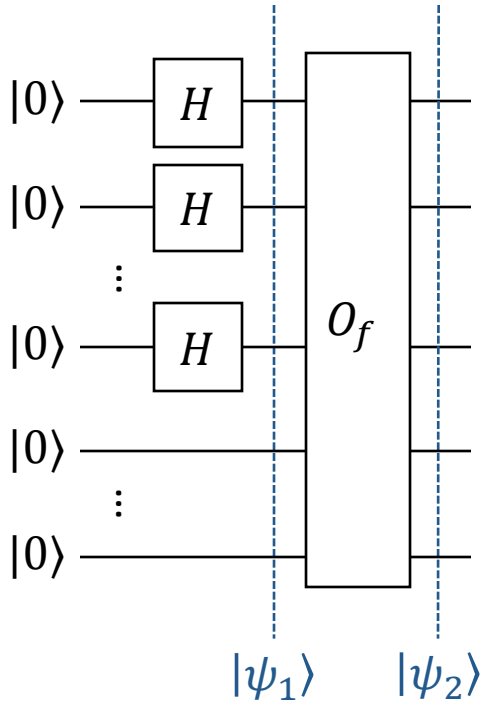
Promise: this is a **periodic** function:
$\forall x, f(x) = f(x \oplus s)$ for some non-zero s.

Question: What is the period s?

	Input: x	Output: $f(x)$
00000	00000	101
01000	01000	101
$00000 \oplus 10110$	10110	101
$01000 \oplus 10110$	11110	101

Input: x	Output: $f(x)$
00000	101
00001	000
00010	011
00011	110
00100	001
00101	100
00110	111
00111	010
01000	101
01001	000
01010	011
01011	110
01100	001
01101	100
01110	111
01111	010
10000	111
10001	010
10010	001
10011	100
10100	011
10101	110
10110	101
10111	000
11000	111
11001	010
11010	001
11011	100
11100	011
11101	110
11110	101
11111	000

Quantum Strategy: Finding Period with a Bit Oracle



- $|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle\,|0\rangle$
- $|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$
- Derive on board: What is $|\psi_3\rangle$?

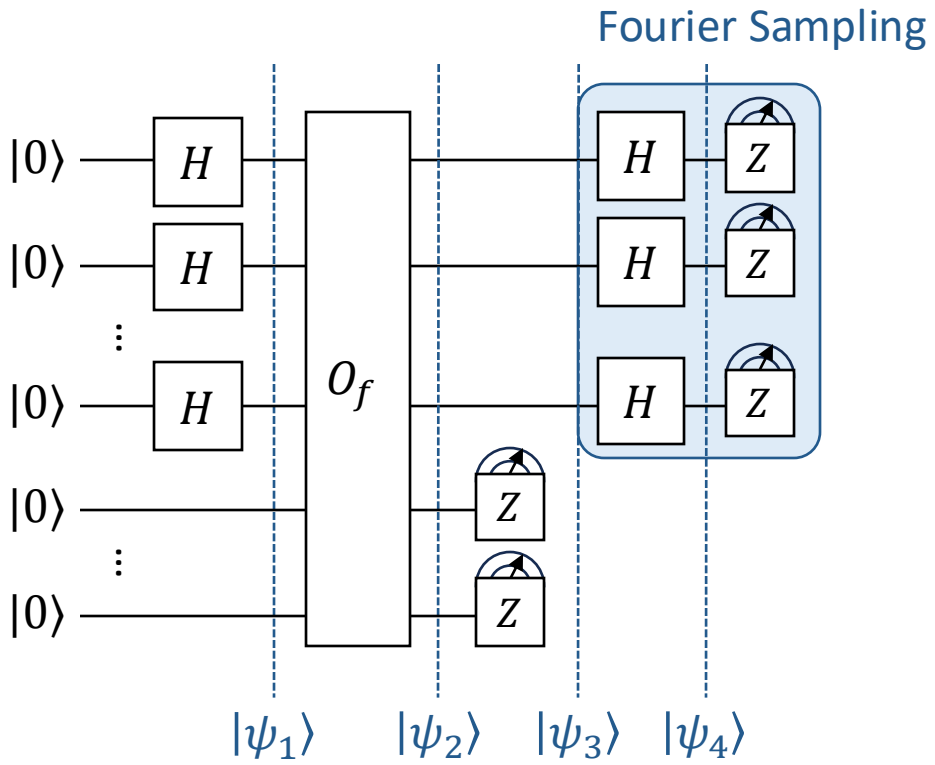
$$|\psi_3\rangle = \frac{1}{\sqrt{|C|}} \sum_{x:f(x)=c} |x\rangle|c\rangle \text{ if measured } c.$$

Example:

$$|\psi_3\rangle = \frac{1}{2}(|00000\rangle|101\rangle + |01000\rangle|101\rangle + |10110\rangle|101\rangle + |11110\rangle|101\rangle)$$

- How do we learn period s from $|\psi_3\rangle$?

Fourier Sampling



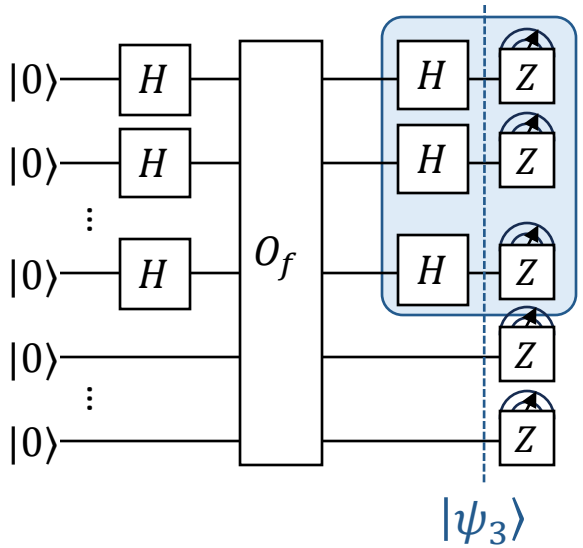
- $|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle\,|0\rangle$
- $|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$
- $|\psi_3\rangle = \frac{1}{\sqrt{|C|}} \sum_{x:f(x)=c} \frac{|x\rangle|c\rangle + |x \oplus s\rangle|c\rangle}{2}$

Derive on board (Fourier sampling):

$$H^{\otimes n}|\psi_3\rangle$$

- What is the measurement outcome?
- How to learn period s from the measurement outcome?

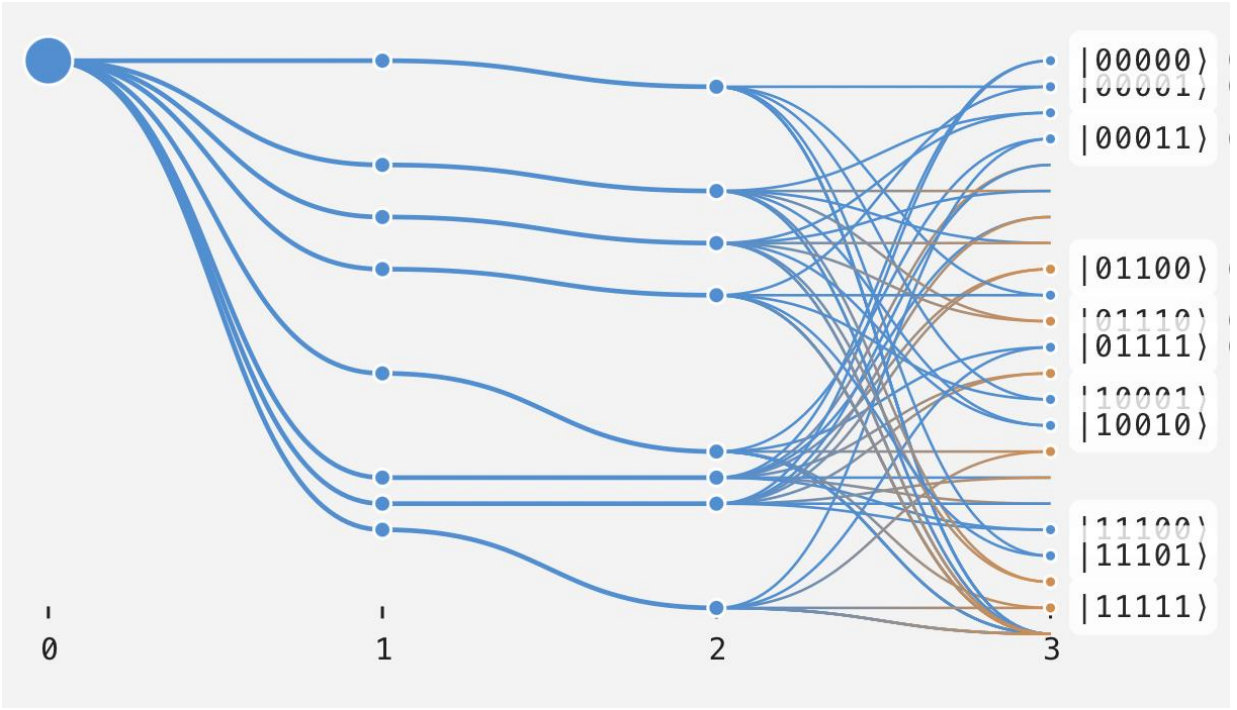
Fourier Sampling



$$|\psi_3\rangle = \frac{1}{4}(|000\rangle|00\rangle + |011\rangle|00\rangle + |100\rangle|00\rangle + |111\rangle|00\rangle +$$
$$|000\rangle|01\rangle + |011\rangle|01\rangle + |100\rangle|01\rangle + |111\rangle|01\rangle +$$
$$|000\rangle|10\rangle + |011\rangle|10\rangle + |100\rangle|10\rangle + |111\rangle|10\rangle +$$
$$|000\rangle|11\rangle + |011\rangle|11\rangle + |100\rangle|11\rangle + |111\rangle|11\rangle)$$

If we measure $y = 011$, what do we know about s?

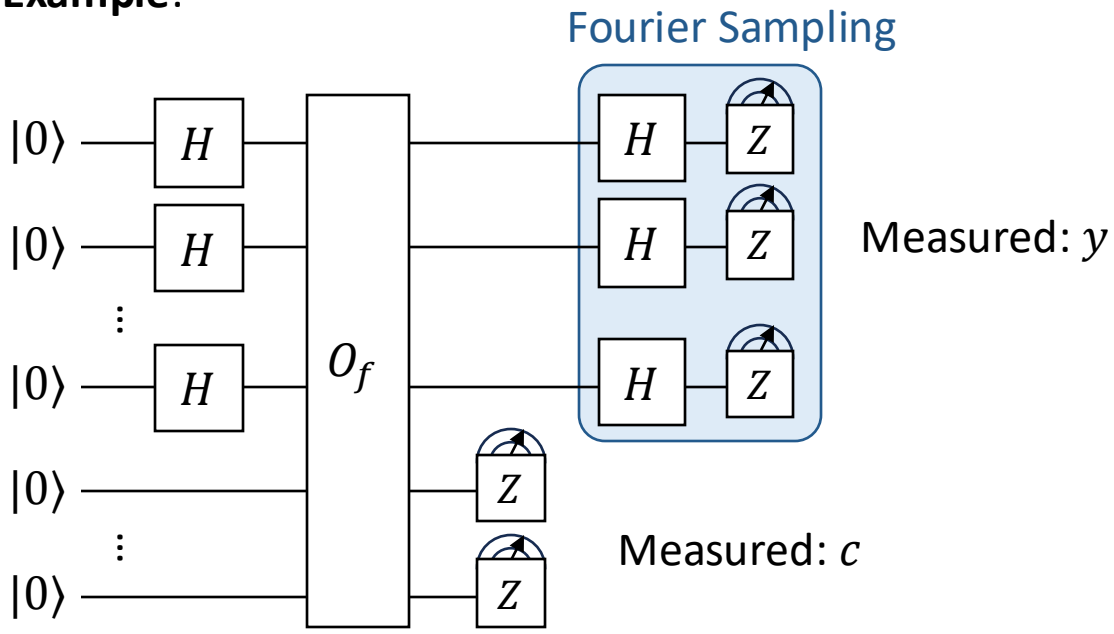
Input: x	Output: $f(x)$
000	01
001	10
010	10
011	01
100	11
101	00
110	00
111	11



Classical Processing

Observation:
Amplitude on $|y\rangle$ is non-zero, if $y \cdot s = 0$.

Example:



- If we measured $y = 000$
  - What do we know about s?

$$0 \cdot s_0 + 0 \cdot s_1 + 0 \cdot s_2 = 0 \pmod 2$$

- If we measured $y = 100$
  - What do we know about s?

$$1 \cdot s_0 + 0 \cdot s_1 + 0 \cdot s_2 = 0 \pmod 2$$

$s_0 = 0$

- Let's repeat! We measured $y = 011$
  - What do we know about s?

$$0 \cdot s_0 + 1 \cdot s_1 + 1 \cdot s_2 = 0 \pmod 2$$

$s_0 = 0$ $\quad$ $s_1 \oplus s_2 = 0$

- Derive on board: How many times do we need to repeat?

$$\begin{bmatrix} - & y_1 & - \\ - & y_2 & - \\ & \vdots & \\ - & y_{n-1} & - \end{bmatrix} \begin{bmatrix} | \\ s \\ | \end{bmatrix} = 0 \text{ (over } \mathbb{F}_2)$$

Quantum v.s. Classical

Given an oracle O_f to function $f: \{0,1\}^n \to \{0,1\}^m$, s.t. $f(x \oplus s) = f(x), \forall x$, for some $s \in \{0,1\}^n$.

Quantumly, we need only $O(n)$ queries to O_f.
Classically, this is really hard: $\approx \sqrt{2^n}$ queries to f. ("Birthday Paradox")

- Simon's "period finding" algorithm finds a hidden pattern in a black-box function.
- *This is the inspiration for my factoring algorithm.* – Peter Shor