Simon’s Algorithm

An example where quantum operations are exponentially more efficient than classical operations

Based on notes by John Watrous

Simon’s Problem

Simon's Problem

Let $f: \{0,1\}^n \rightarrow \{0,1\}^n$ be s.t. $\exists$ s in $\{0,1\}^n$, $\forall$ x, y in $\{0,1\}^n$

$f(x)=f(y)$ if and only if $x \oplus y \in \{0^n, s\}$

Simon's Problem

Let f: $\{0,1\}^n \rightarrow \{0,1\}^n$ be s.t. $\exists$ s in $\{0,1\}^n$, $\forall$ x, y in $\{0,1\}^n$

$$f(x)=f(y) \text{ if and only if } x \oplus y \in \{0^n, s\}$$

Examples: Suppose that $s = 0^n$.

Simon's Problem

Let f: $\{0,1\}^n \rightarrow \{0,1\}^n$ be s.t. $\exists$ s in $\{0,1\}^n$, $\forall$ x, y in $\{0,1\}^n$

$$f(x)=f(y) \text{ if and only if } x \oplus y \in \{0^n, s\}$$

Examples: Suppose that $s = 0^n$. In this case,

- $f(x)=f(y)$ if and only if $x \oplus y = 0^n$
- f is a permutation function or bijection

Simon's Problem

Let f: $\{0,1\}^n \rightarrow \{0,1\}^n$ be s.t. $\exists$ s in $\{0,1\}^n$, $\forall$ x, y in $\{0,1\}^n$

$f(x)=f(y)$ if and only if $x \oplus y \in \{0^n, s\}$

Examples: The function given by:

x	$f(x)$
000	101
001	010
010	000
011	110
100	000
101	110
110	101
111	010

Simon's Problem

Let f: $\{0,1\}^n \rightarrow \{0,1\}^n$ be s.t. $\exists$ s in $\{0,1\}^n$, $\forall$ x, y in $\{0,1\}^n$

$$f(x)=f(y) \text{ if and only if } x \oplus y \in \{0^n, s\}$$

Examples: The function given by:

x	$f(x)$
000	101
001	010
010	000
011	110
100	000
101	110
110	101
111	010

More generally, if $s \neq 0^n$ then

- $f(x) = f(x \oplus s)$, and so $f(0^n) = f(s)$.
- Exactly two strings map to each z in the range of f; call them x_z and $x_z \oplus s$
- If A = range(f), then $|A| = 2^{n-1}$

Simon's Problem

Let f: $\{0,1\}^n \rightarrow \{0,1\}^n$ be s.t. $\exists$ s in $\{0,1\}^n$, $\forall$ x, y in $\{0,1\}^n$

f(x)=f(y) if and only if $x \oplus y \in \{0^n, s\}$

Simon's Problem

Let $f: \{0,1\}^n \rightarrow \{0,1\}^n$ be s.t. $\exists$ s in $\{0,1\}^n$, $\forall$ x, y in $\{0,1\}^n$

$$f(x)=f(y) \text{ if and only if } x \oplus y \in \{0^n, s\}$$

Instance: A "black box circuit" B_f that computes f

Problem: How many queries are needed to find s with high probability?

Simon's Problem

Let f: $\{0,1\}^n \rightarrow \{0,1\}^n$ be s.t. $\exists$ s in $\{0,1\}^n$, $\forall$ x, y in $\{0,1\}^n$

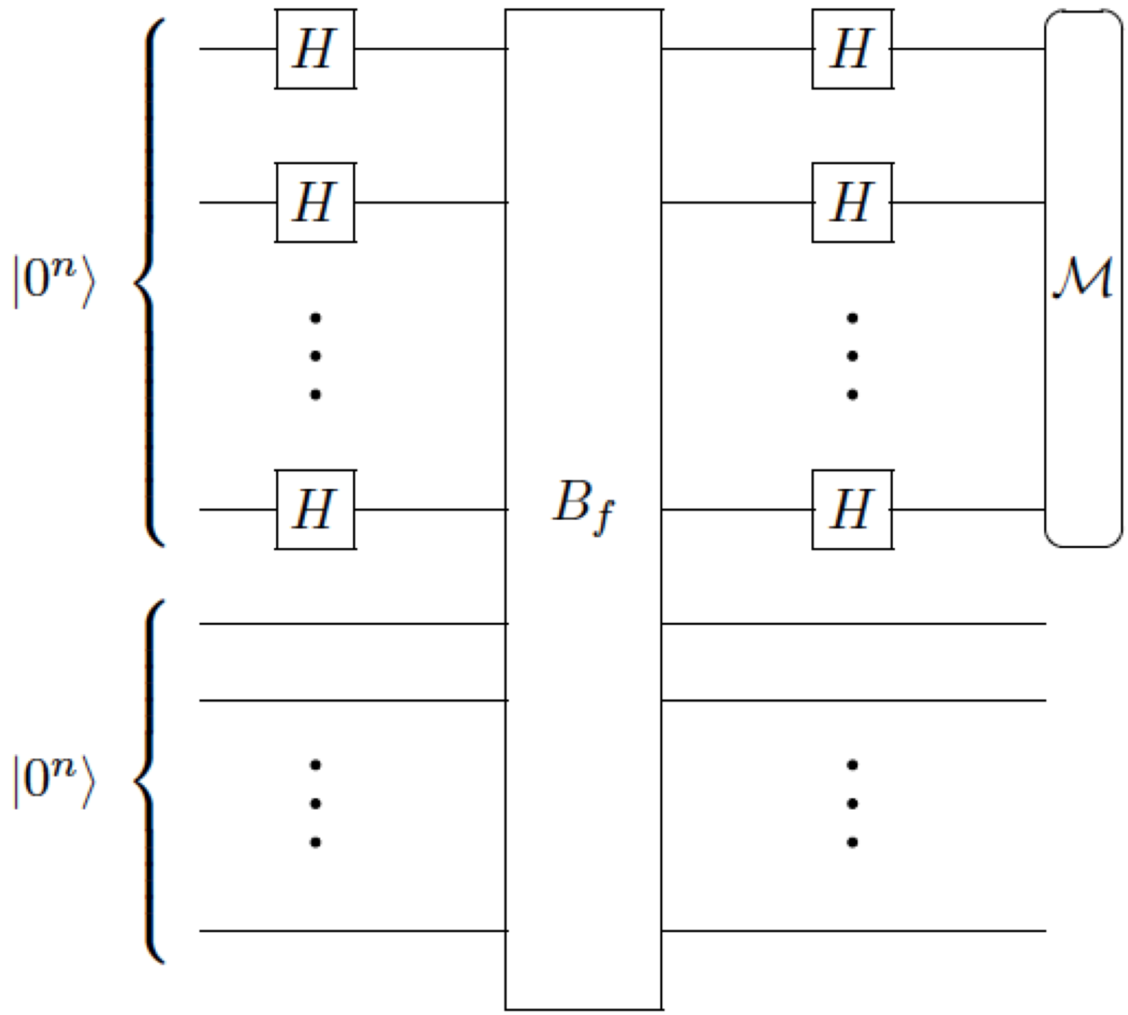
$$f(x)=f(y) \text{ if and only if } x \oplus y \in \{0^n, s\}$$

Instance: A "black box circuit" B_f that computes f

Problem: How many queries are needed to find s with high probability?

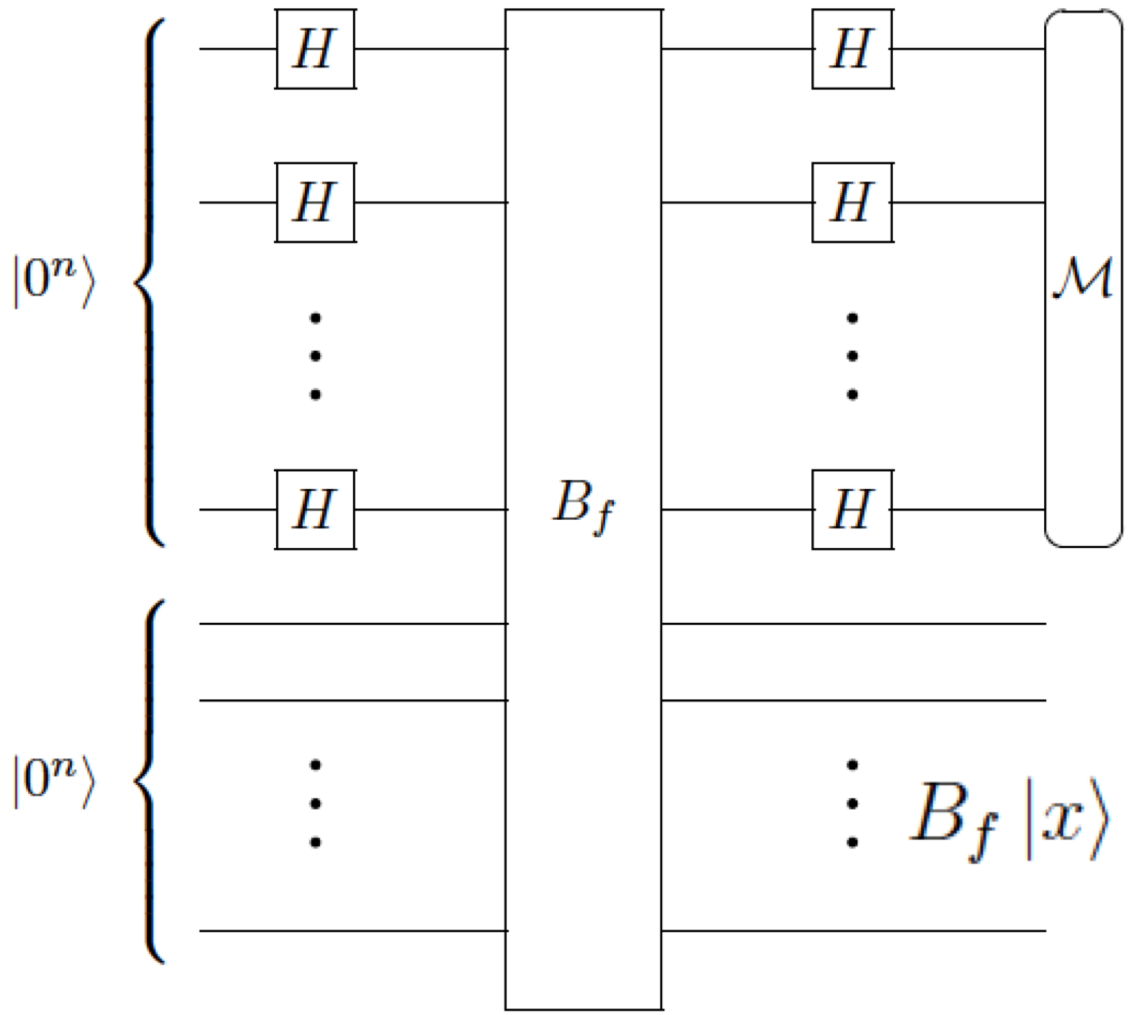
- $\Omega(\sqrt{2^n})$ queries needed classically
- O(n) queries are needed with quantum operations

Simon's Algorithm (Quantum Part)



(plus some classical post-processing)

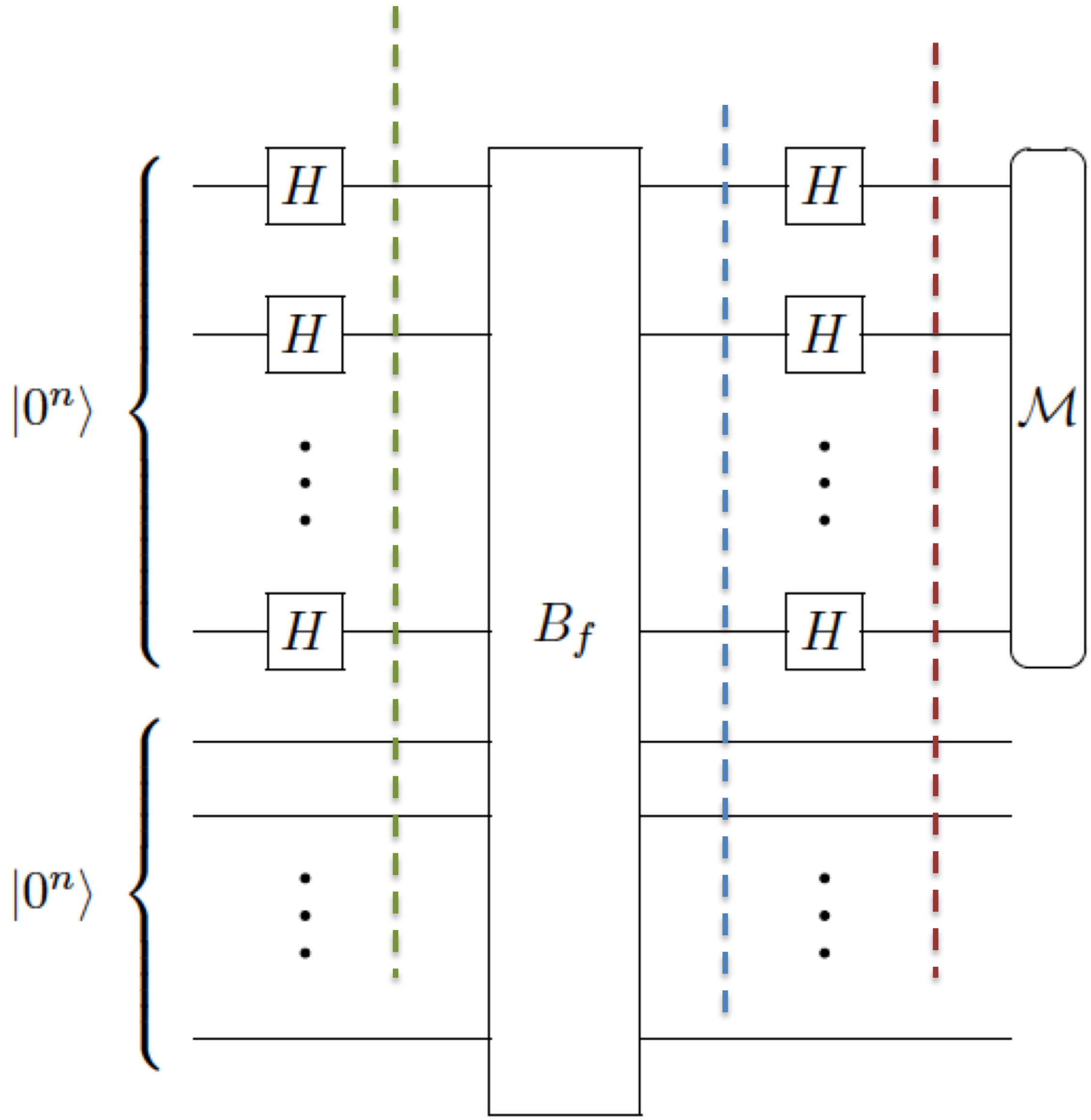
Simon's Algorithm (Quantum Part)



(plus some classical post-processing)

$$B_f\,|x\rangle\,|0\rangle = |x\rangle\,|f(x) \oplus 0\rangle$$

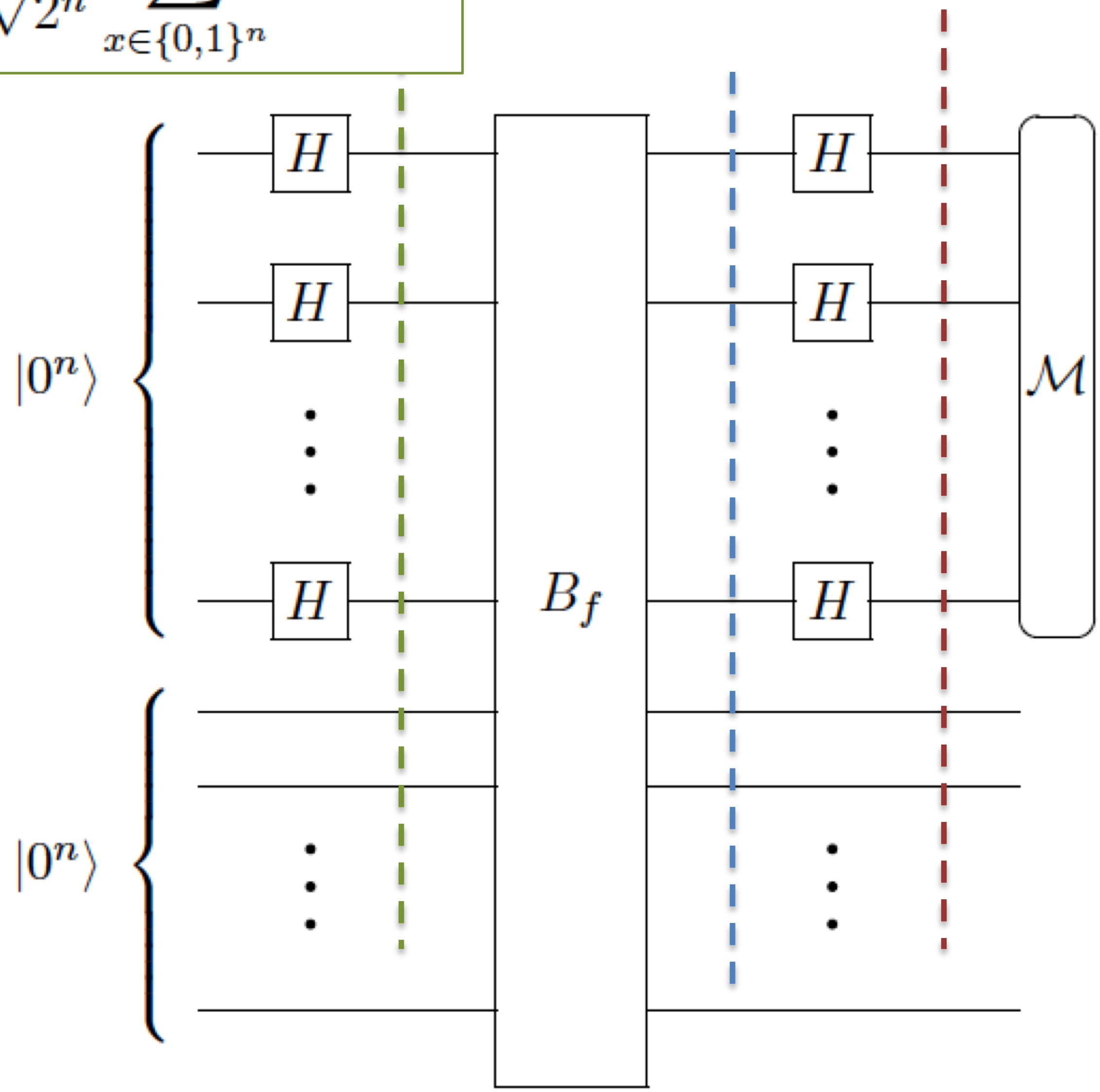
Simon's Algorithm: Superpositions



(plus some classical post-processing)

Simon's Algorithm: Superpositions

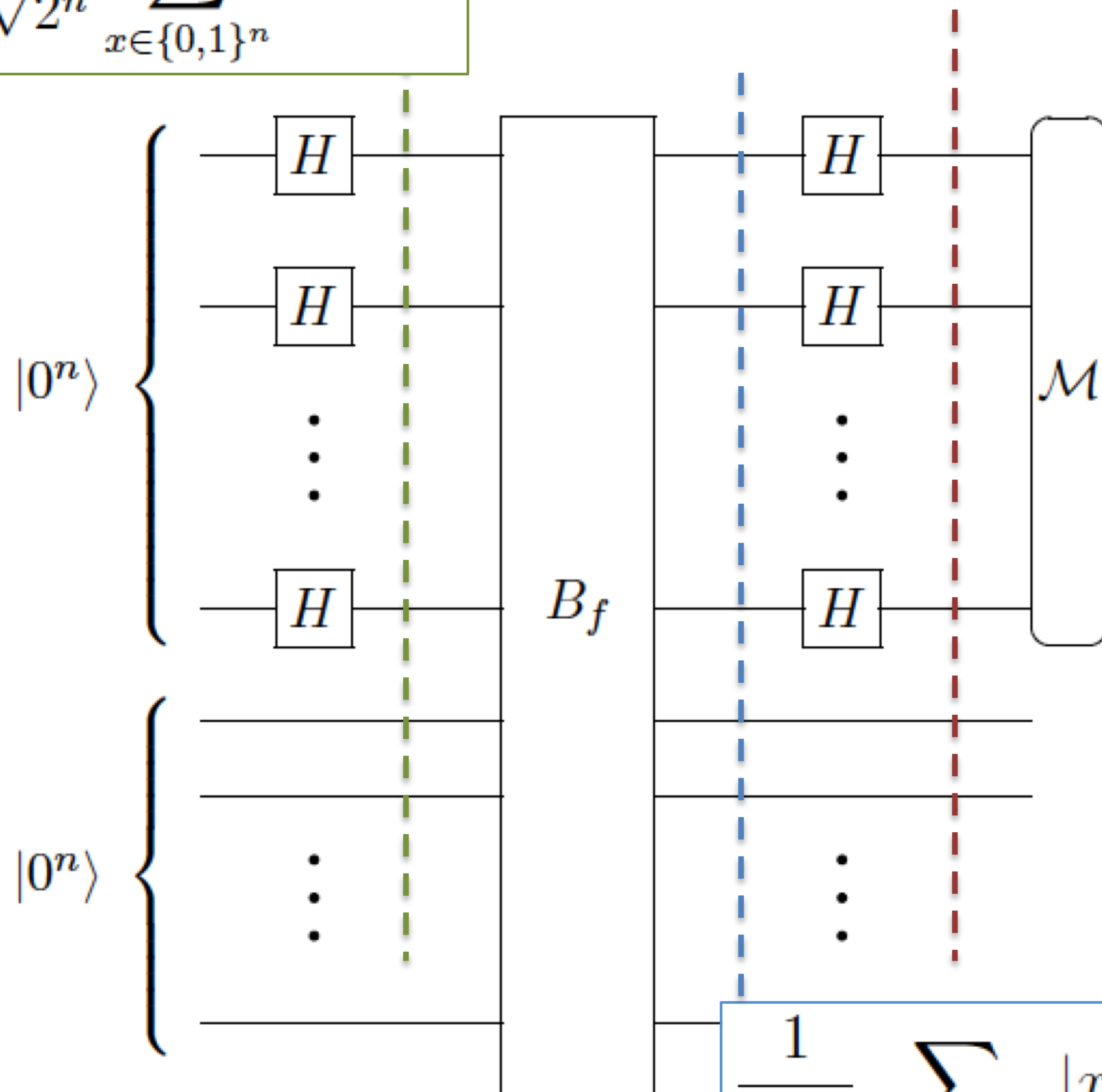
$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\,|0^n\rangle$$



(plus some classical post-processing)

Simon's Algorithm: Superpositions

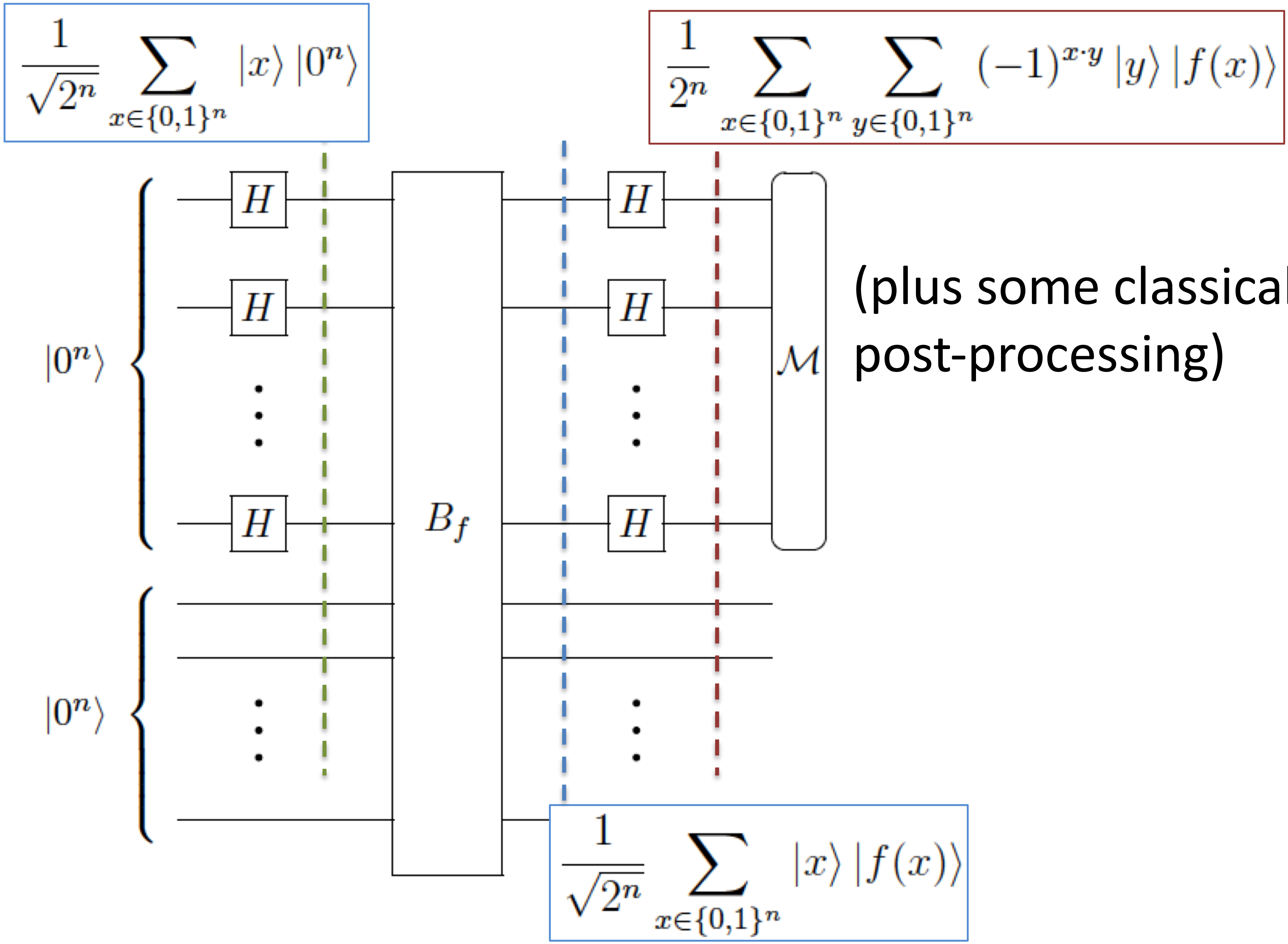
$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle\,|0^n\rangle$$



(plus some classical post-processing)

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle\,|f(x)\rangle$$

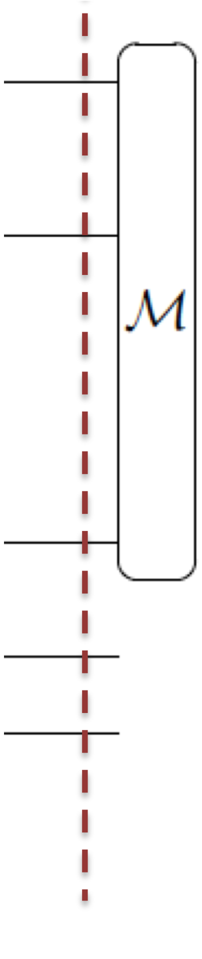
Simon's Algorithm: Superpositions



(plus some classical post-processing)

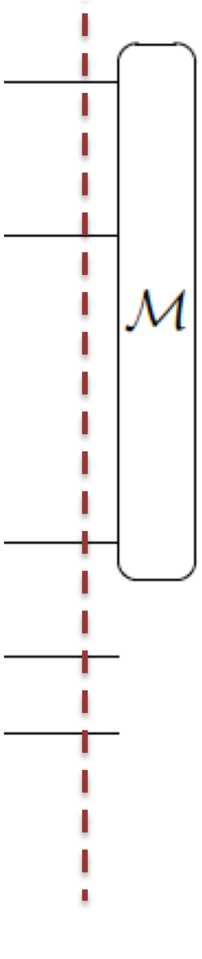
Simon's Algorithm: Superpositions

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} \left| y \right\rangle \left| f(x) \right\rangle$$



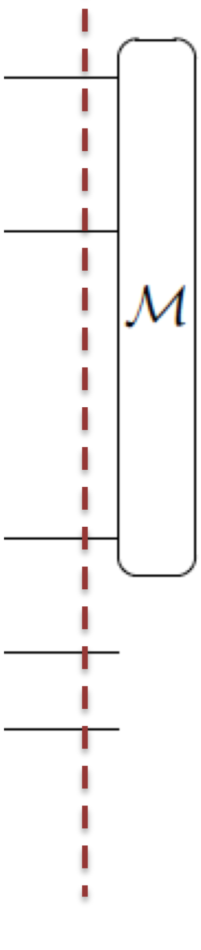
Simon's Algorithm: Superpositions

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}\,|y\rangle\,|f(x)\rangle = \sum_{y\in\{0,1\}^n}|y\rangle\left(\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot y}\,|f(x)\rangle\right)$$



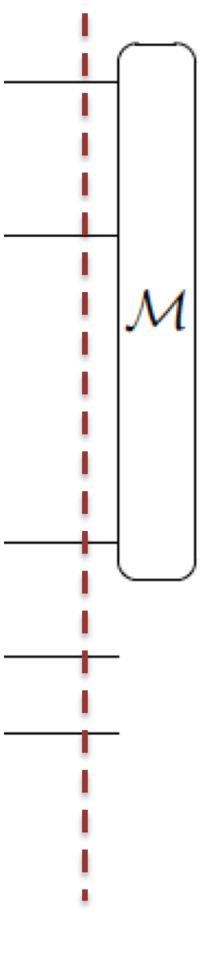
Simon's Algorithm: Superpositions

$$\sum_{y\in\{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \, |f(x)\rangle \right)$$



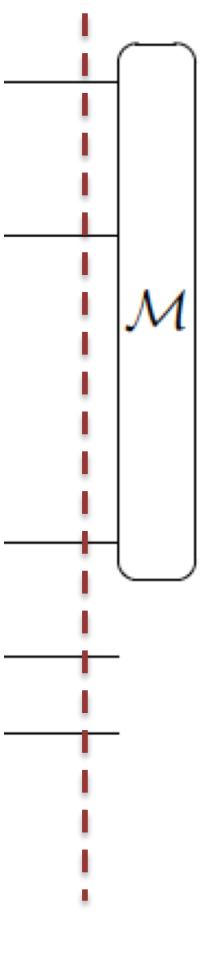
Simon's Algorithm Analysis

$$\sum_{y\in\{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \, |f(x)\rangle \right)$$



Simon’s Algorithm Analysis

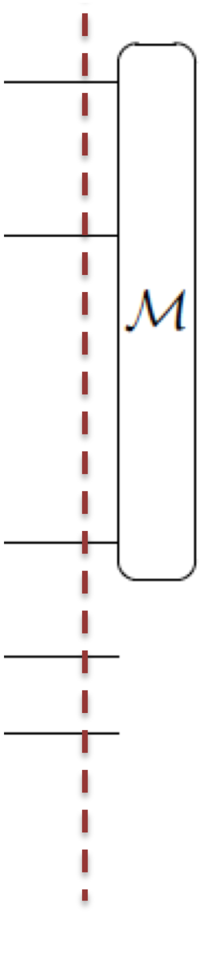
$$\sum_{y \in \{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} \, |f(x)\rangle \right)$$



Probability of measuring a given y in $\{0,1\}^n$?

Simon’s Algorithm Analysis

$$\sum_{y\in\{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \, |f(x)\rangle \right)$$

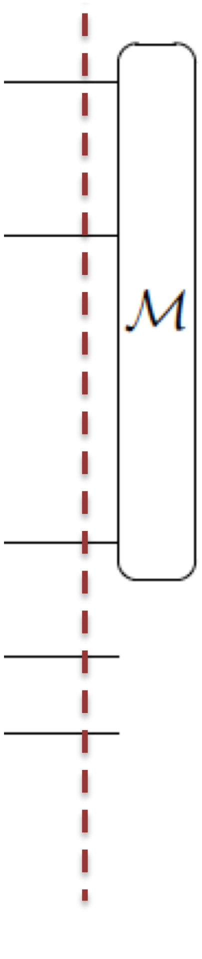


Probability of measuring a given y in $\{0,1\}^n$?

$$\left\| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \, |f(x)\rangle \right\|^2$$

Simon's Algorithm Analysis

$$\sum_{y\in\{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \, |f(x)\rangle \right)$$



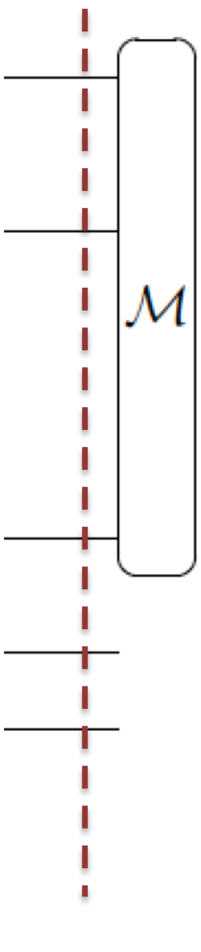
Probability of measuring a given y in $\{0,1\}^n$?

- If $s = 0^n$:

$$\left\| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \, |f(x)\rangle \right\|^2$$

Simon's Algorithm Analysis

$$\sum_{y\in\{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} |f(x)\rangle \right)$$



Probability of measuring a given y in $\{0,1\}^n$?

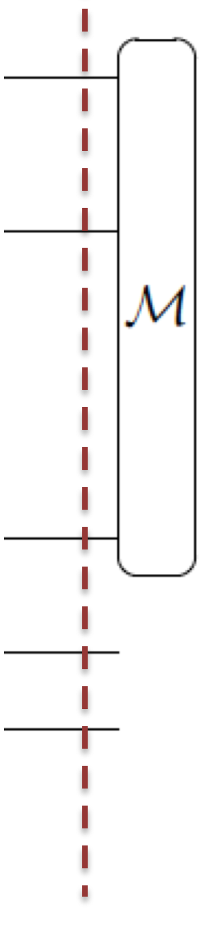
- If $s = 0^n$:

$$\left\| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} |f(x)\rangle \right\|^2$$

Since f is a permutation function when $s = 0^n$, every entry in this superposition is either $1/2^n$ or $-1/2^n$

Simon's Algorithm Analysis

$$\sum_{y\in\{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} |f(x)\rangle \right)$$



Probability of measuring a given y in $\{0,1\}^n$?

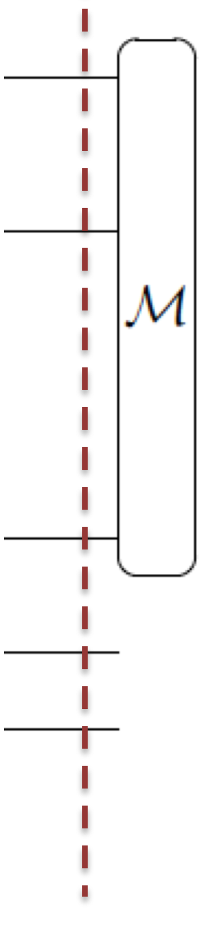
- If $s = 0^n$:

$$\left\| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} |f(x)\rangle \right\|^2 = \frac{1}{2^n}$$

Since f is a permutation function when $s = 0^n$, every entry in this superposition is either $1/2^n$ or $-1/2^n$

Simon's Algorithm Analysis

$$\sum_{y \in \{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} |f(x)\rangle \right)$$

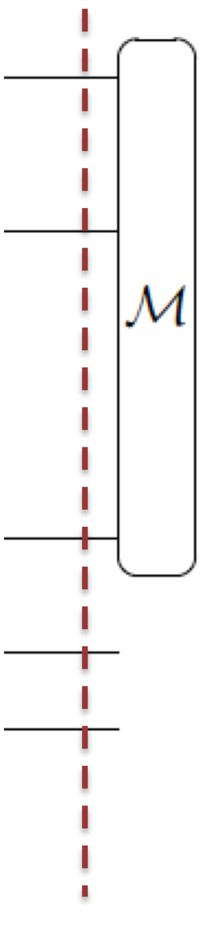


Probability of measuring a given y in $\{0,1\}^n$?

- If $s \neq 0^n$:

Simon's Algorithm Analysis

$$\sum_{y\in\{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \, |f(x)\rangle \right)$$



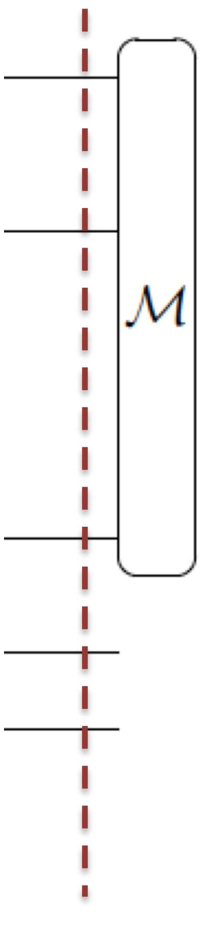
Probability of measuring a given y in $\{0,1\}^n$?

- If $s \neq 0^n$:

$$\left\| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \, |f(x)\rangle \right\|^2$$

Simon's Algorithm Analysis

$$\sum_{y\in\{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} |f(x)\rangle \right)$$



Probability of measuring a given y in $\{0,1\}^n$?

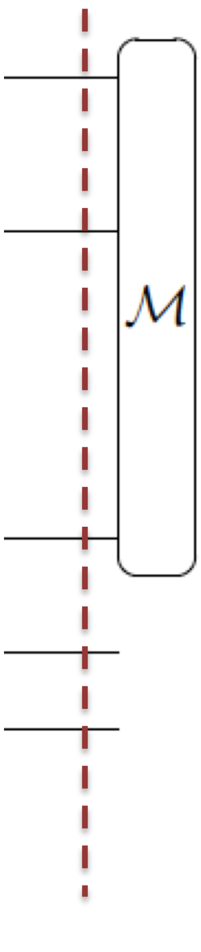
- If $s \neq 0^n$:

$$\left\| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} |f(x)\rangle \right\|^2 = \left\| \frac{1}{2^n} \sum_{z\in A} \left((-1)^{x_z\cdot y} + (-1)^{(x_z\oplus s)\cdot y} \right) |z\rangle \right\|^2$$

- Here, A is range(f), and $|A| = 2^{n-1}$
- Recall that when $s \neq 0^n$, exactly two strings, namely x_z and $x_z \oplus s$, map to each z in the range of f

Simon's Algorithm Analysis

$$\sum_{y\in\{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} |f(x)\rangle \right)$$



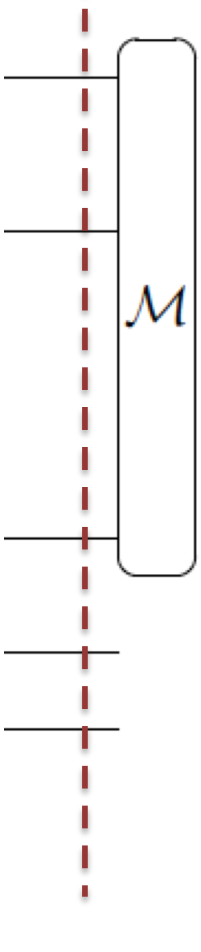
Probability of measuring a given y in $\{0,1\}^n$?

- If $s \neq 0^n$:

$$\left\| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} |f(x)\rangle \right\|^2 = \left\| \frac{1}{2^n} \sum_{z\in A} \left((-1)^{x_z\cdot y} + (-1)^{(x_z\oplus s)\cdot y} \right) |z\rangle \right\|^2$$

Simon's Algorithm Analysis

$$\sum_{y\in\{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \, |f(x)\rangle \right)$$



Probability of measuring a given y in $\{0,1\}^n$?

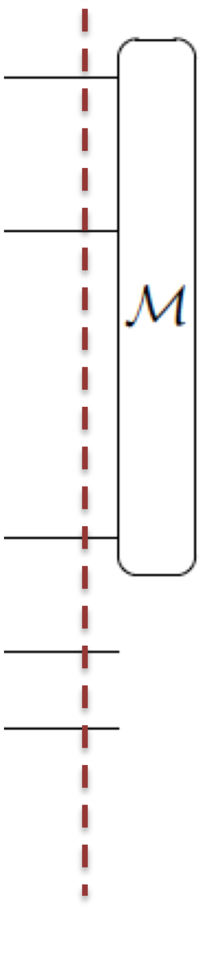
- If s $\neq$ 0^n :

$$\left\| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \, |f(x)\rangle \right\|^2 = \left\| \frac{1}{2^n} \sum_{z\in A} \left((-1)^{x_z \cdot y} + (-1)^{(x_z \oplus s)\cdot y} \right) |z\rangle \right\|^2$$

$$= \left\| \frac{1}{2^n} \sum_{z\in A} (-1)^{x_z \cdot y} \left(1 + (-1)^{s\cdot y}\right) |z\rangle \right\|^2$$

Simon's Algorithm Analysis

$$\sum_{y\in\{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} |f(x)\rangle \right)$$



Probability of measuring a given y in $\{0,1\}^n$?

- If s $\neq$ 0^n :

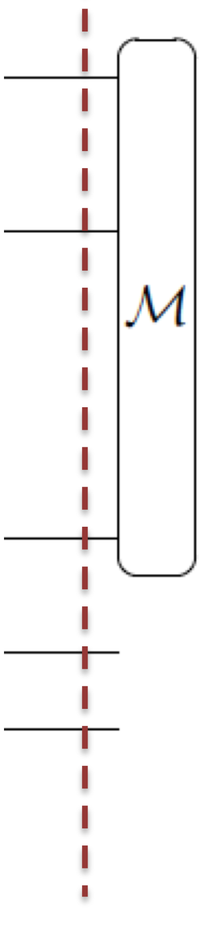
$$\left\| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} |f(x)\rangle \right\|^2 = \left\| \frac{1}{2^n} \sum_{z\in A} \left((-1)^{x_z\cdot y} + (-1)^{(x_z\oplus s)\cdot y} \right) |z\rangle \right\|^2$$

$$= \left\| \frac{1}{2^n} \sum_{z\in A} (-1)^{x_z\cdot y} \left(1 + (-1)^{s\cdot y}\right) |z\rangle \right\|^2$$

$$= \begin{cases} 2^{-(n-1)} & \text{if } s\cdot y = 0 \\ 0 & \text{if } s\cdot y = 1. \end{cases}$$

Simon's Algorithm Analysis

$$\sum_{y\in\{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \, |f(x)\rangle \right)$$



Probability of measuring a given y in $\{0,1\}^n$?

- If s = 0^n : $p_y = \dfrac{1}{2^n}$ (and s . y = 0 (mod 2))

- If s ≠ 0^n : $p_y = \begin{cases} 2^{-(n-1)} & \text{if } s \cdot y = 0 \\ 0 & \text{if } s \cdot y = 1 \end{cases}$

Back to Simon's Algorithm

- Use the circuit n times to get y_1, y_2, … y_{n-1} such that

$$\begin{gathered} y_1 \cdot s = 0 \\ y_2 \cdot s = 0 \\ \vdots \\ y_{n-1} \cdot s = 0 \end{gathered}$$

Back to Simon's Algorithm

- Use the circuit n times to get y_1, y_2, … y_{n-1} such that

$$\begin{aligned} y_1 \cdot s &= 0 \\ y_2 \cdot s &= 0 \\ &\vdots \\ y_{n-1} \cdot s &= 0 \end{aligned}$$

- The system has a unique solution $s \neq 0^n$ iff the y_i are linearly independent.

Back to Simon's Algorithm

- Use the circuit n times to get y_1, y_2, … y_{n-1} such that

$$
\begin{aligned}
y_1 \cdot s &= 0 \\
y_2 \cdot s &= 0 \\
&\vdots \\
y_{n-1} \cdot s &= 0
\end{aligned}
$$

- The system has a unique solution $s \neq 0^n$ iff the y_i are linearly independent. The probability of lin. ind. is ≥

$$\prod_{k=1}^{\infty}\left(1-\frac{1}{2^k}\right) = 0.288788\cdots > \frac{1}{4}.$$

Back to Simon's Algorithm

- Use the circuit n times to get $y_1, y_2, \ldots y_{n-1}$ such that

$$\begin{aligned} y_1 \cdot s &= 0 \\ y_2 \cdot s &= 0 \\ &\vdots \\ y_{n-1} \cdot s &= 0 \end{aligned}$$

- The system has a unique solution $s \neq 0^n$ iff the y_i are linearly independent. The probability of lin. ind. is ≥

$$\prod_{k=1}^{\infty} \left(1 - \frac{1}{2^k}\right) = 0.288788\cdots > \frac{1}{4}.$$

- Repeat, m times, so that probability we don't get linearly independent y with probability at most

$$\left(1 - \frac{1}{4}\right)^{4m} < e^{-m}$$

Classical Post-Processing

- Use the circuit n times to get y_1, y_2, … y_{n-1} such that

$$
\begin{aligned}
y_1 \cdot s &= 0 \\
y_2 \cdot s &= 0 \\
&\vdots \\
y_{n-1} \cdot s &= 0
\end{aligned}
$$

Classical Post-Processing

- Use the circuit n times to get $y_1, y_2, \ldots y_{n-1}$ such that

$$\begin{aligned} y_1 \cdot s &= 0 \\ y_2 \cdot s &= 0 \\ &\vdots \\ y_{n-1} \cdot s &= 0 \end{aligned}$$

- Solve the system of equations to get a unique solution $s' \neq 0^n$

- If $f(0^n) = f(s')$, then return $s = s'$
- If $f(0^n) \neq f(s')$, then return $s = 0$

Summary

We've covered:

- Basics of quantum computing: quantum bits, operations, circuits, complexity classes
- Two algorithms: Superdense coding and Simon's algorithm, suggesting the power of quantum algorithms

Other Things

- Reading project: Written reports or virtual presentations?

Last Topic, Starting Next Week:

- Molecular programming and models of computation