Simon’s Algorithm

Based on notes by John Watrous
Outline

- $(\text{BPP} \subseteq) \text{ QBP} \subseteq \text{PSPACE}$ (finish from last time)

- Simon’s problem: an example where quantum operations are exponentially more efficient than classical operations
BQP is in PSPACE (finish from last time)

• Let $L$ be in BQP, $x$ an instance of $L$, and $Q_x$ a circuit that with high probability outputs 1 if $x$ is in $L$ and 0 if $x$ is not in $L$
Consider the *state tree* of circuit Qx:

- Nodes are classical superpositions, with initial node $|x\rangle |0\rangle |0\rangle$ (and rightmost bit being output bit)
- Each level $i$ corresponds to application of either a Hadamard or Toffoli operation
  - if Toffoli, one edge from each node at level $i$ to node at level $i+1$
  - if Hadamard, two edges
- Each edge has an associated $+/-$ *sign*
  - sign is “-” iff the edge corresponds to a Hadamard operation in which a 1-valued bit remains 1
We can write the final superposition of the qubits of Qx as a sum over all paths in the tree:

$$|\text{final}\rangle = \sum_p \text{amp}(p) |p\rangle,$$

$$= \left(\frac{1}{\sqrt{2}}\right)^h \sum_p \text{sign}(p) |p\rangle$$

where sign(p) is the product of signs along path p and h is the number of Hadamard matrices along any path.
BQP is in PSPACE

- The amplitude of some fixed superposition $|s\rangle$ is

$$
\left(\frac{1}{\sqrt{2}}\right)^h \sum_{p : |p\rangle = |s\rangle} \text{sign}(p)
$$

- The probability of measuring output $|s\rangle$ is

$$
Pr(s) = 2^{-h} \sum_{p, p'} \text{sign}(p) \text{sign}(p')
$$

where the sum is over all $p, p'$ with $p = p' = s$

- The probability of measuring output bit 1 is

$$
2^{-h} \sum_{p, p'} \text{sign}(p) \text{sign}(p')
$$

where the sum is over all $p, p'$ with $p = p'$ and with both $p$ and $p'$ having rightmost bit 1
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 $x \oplus y \in \{0^n, s\}$

Given a "black box" for $f$, 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 problem

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

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

If $s = 0^n$ then

• $f$ is 1-1, i.e. a permutation function
• if $f(x) = f(y)$ then $x \oplus y = 0^n$
Let $f: \{0,1\}^n \to \{0,1\}^n$ be s.t. \( \exists s \in \{0,1\}^n, \forall x, y \in \{0,1\}^n \) 
\[ f(x) = f(y) \text{ if and only if } x \oplus y \in \{0^n, s\} \]

If $s \neq 0^n$ then

<table>
<thead>
<tr>
<th>$x$</th>
<th>$f(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>101</td>
</tr>
<tr>
<td>001</td>
<td>010</td>
</tr>
<tr>
<td>010</td>
<td>000</td>
</tr>
<tr>
<td>011</td>
<td>110</td>
</tr>
<tr>
<td>100</td>
<td>000</td>
</tr>
<tr>
<td>101</td>
<td>110</td>
</tr>
<tr>
<td>110</td>
<td>101</td>
</tr>
<tr>
<td>111</td>
<td>010</td>
</tr>
</tbody>
</table>
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 $x \oplus y \in \{0^n, s\}$

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 $x_z \oplus s$
- $|\text{range}(f)| = 2^{n-1}$

<table>
<thead>
<tr>
<th>$x$</th>
<th>$f(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>101</td>
</tr>
<tr>
<td>001</td>
<td>010</td>
</tr>
<tr>
<td>010</td>
<td>000</td>
</tr>
<tr>
<td>011</td>
<td>110</td>
</tr>
<tr>
<td>100</td>
<td>000</td>
</tr>
<tr>
<td>101</td>
<td>110</td>
</tr>
<tr>
<td>110</td>
<td>101</td>
</tr>
<tr>
<td>111</td>
<td>010</td>
</tr>
</tbody>
</table>
Simon’s algorithm (quantum part)

(plus some classical post-processing)
Simon’s algorithm (quantum part)

\[ |0^n\rangle \]

\[ B_f \ |x\rangle \ |y\rangle = |x\rangle \ |f(x) \oplus y\rangle \]
Simon's algorithm: superpositions

\[ |0^n\rangle \}
\[ H \quad H \quad H \quad H \quad \mathcal{M} \]
\[ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \]
\[ H \quad H \quad H \quad H \quad \]

\[ |0^n\rangle \}
\[ B_f \quad |x\rangle \quad |y\rangle \quad = \quad |x\rangle \quad |f(x) \oplus y\rangle \]

(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)
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

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

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

(plus some classical post-processing)
Simon’s algorithm: superpositions

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

- If \( s = 0^n \):
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 \( s = 0^n \):

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

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

(because the superposition is one in which every entry is either \( 1/2^n \) or \(-1/2^n \))
Simon’s algorithm analysis

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

- If \( s \neq 0^n \):

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

- 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 $s \neq 0^n$:

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

*here, $A$ is range($f$)*
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 \( s \neq 0^n \):
  \[
  \left\| \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} |f(x)\rangle \right\|^2 = \left\| \frac{1}{2^n} \sum_{z \in A} ((-1)^{xz \cdot y} + (-1)^{(xz \oplus s) \cdot y}) |z\rangle \right\|^2
  \]
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 \( s \neq 0^n \):

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

\[
= \left\| \frac{1}{2^n} \sum_{z \in A} (-1)^{xz \cdot y} (1 + (-1)^{s \cdot y}) |z\rangle \right\|^2
\]
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 \( s \neq 0^n \):

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

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

\[
= \begin{cases} 
2^{-(n-1)} & \text{if } s \cdot y = 0 \\
0 & \text{if } s \cdot y = 1.
\end{cases}
\]
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 \( s = 0^n \): \( p_y = \frac{1}{2^n} \) (and \( s \cdot y = 0 \))

- If \( s \neq 0^n \):
  \[
  p_y = \begin{cases} 
  2^{-n+1} & \text{if } s \cdot y = 0 \\
  0 & \text{if } s \cdot y = 1
  \end{cases}
  \]
Back to Simon’s algorithm

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

\[
\begin{align*}
y_1 \cdot s &= 0 \\
y_2 \cdot s &= 0 \\
&\vdots \\
y_{n-1} \cdot s &= 0
\end{align*}
\]
Back to Simon’s algorithm

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

\[
y_1 \cdot s = 0 \\
y_2 \cdot s = 0 \\
\vdots \\
y_{n-1} \cdot s = 0
\]

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

\[
\prod_{k=1}^{\infty} \left(1 - \frac{1}{2^k}\right) = 0.288788 \ldots > \frac{1}{4}.
\]
Back to Simon’s algorithm

- Use the circuit n times to get $y_1, y_2, \ldots y_{n-1}$ such that
  
  \[
  \begin{align*}
  y_1 \cdot s &= 0 \\
  y_2 \cdot s &= 0 \\
  \vdots \\
  y_{n-1} \cdot s &= 0
  \end{align*}
  \]

- The system has a unique solution $s \neq 0^n$ iff the $y_i$ are linearly independent, which happens with probability
  
  \[
  \prod_{k=1}^{\infty} \left( 1 - \frac{1}{2^k} \right) = 0.288788 \ldots > \frac{1}{4}.
  \]

- Repeat, say 10 times, so that probability we don’t get linearly independent $y$ with probability at most
  
  \[
  \left( 1 - \frac{1}{4} \right)^{4m} < e^{-m} < \frac{1}{20000}
  \]
Classical post-processing

- Suppose that we have $y_1, y_2, \ldots, y_{n-1}$ such that:

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

- 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

- $\text{BPP} \subseteq \text{QBP} \subseteq \text{PSPACE}$

- Simon’s problem, while artificial, demonstrates the power of quantum operations over classical operations

- Shor’s factoring algorithm builds on the ideas of Simon’s algorithm
Next classes

- Molecular programming and models of computation