Quantum Computation - Lecture 04 - Hidden Subgroup

Mateus de Oliveira Oliveira

TCS-KTH

November 26, 2012

- Simons Alogorithm

- Simons Alogorithm
- Hidden Subgroup Problem

- Simons Alogorithm
- Hidden Subgroup Problem
  - Deutsch's Problem as HSP

- Simons Alogorithm
- Hidden Subgroup Problem
  - Deutsch's Problem as HSP
  - Deutsch-Jozsa as HSP

- Simons Alogorithm
- Hidden Subgroup Problem
  - Deutsch's Problem as HSP
  - Deutsch-Jozsa as HSP
  - Bernstein-Vazirani as HSP

- Simons Alogorithm
- Hidden Subgroup Problem
  - Deutsch's Problem as HSP
  - Deutsch-Jozsa as HSP
  - Bernstein-Vazirani as HSP
  - Simon's Algorithm as HSP

- Simons Alogorithm
- Hidden Subgroup Problem
  - Deutsch's Problem as HSP
  - Deutsch-Jozsa as HSP
  - Bernstein-Vazirani as HSP
  - Simon's Algorithm as HSP
  - Period Finding

- Simons Alogorithm
- Hidden Subgroup Problem
  - Deutsch's Problem as HSP
  - Deutsch-Jozsa as HSP
  - Bernstein-Vazirani as HSP
  - Simon's Algorithm as HSP
  - Period Finding
  - Discrete Logarithm

- Simons Alogorithm
- Hidden Subgroup Problem
  - Deutsch's Problem as HSP
  - Deutsch-Jozsa as HSP
  - Bernstein-Vazirani as HSP
  - Simon's Algorithm as HSP
  - Period Finding
  - Discrete Logarithm
- Quantum Fourier Transform

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there is an $a \in \{0,1\}^n$ such that $f(x \oplus a) = f(x)$. Find a.

- Prepare the state. (We saw how to do that in the last lecture.)

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there is an $a \in \{0,1\}^n$ such that $f(x \oplus a) = f(x)$. Find a.

- Prepare the state. (We saw how to do that in the last lecture.)

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

- But we know that $f(x \oplus a) = f(x)$ for every x.

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there is an $a \in \{0,1\}^n$ such that $f(x \oplus a) = f(x)$. Find a.

- Prepare the state. (We saw how to do that in the last lecture.)

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

- But we know that $f(x \oplus a) = f(x)$ for every x.
- Meausuring the second register $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle)|f(x_0)\rangle$

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there is an $a \in \{0,1\}^n$ such that $f(x \oplus a) = f(x)$. Find a.

- Prepare the state. (We saw how to do that in the last lecture.)

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

- But we know that $f(x \oplus a) = f(x)$ for every x.
- Meausuring the second register $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle)|f(x_0)\rangle$
  - Suppose we could clone states.

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there is an $a \in \{0,1\}^n$ such that $f(x \oplus a) = f(x)$. Find a.

- Prepare the state. (We saw how to do that in the last lecture.)

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

- But we know that $f(x \oplus a) = f(x)$ for every x.
- Meausuring the second register $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle)|f(x_0)\rangle$
  - Suppose we could clone states.
  - Eventually we would measure $|x_0\rangle$

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there is an $a \in \{0,1\}^n$ such that $f(x \oplus a) = f(x)$. Find a.

- Prepare the state. (We saw how to do that in the last lecture.)

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$$

- But we know that $f(x \oplus a) = f(x)$ for every x.
- Meausuring the second register $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle)|f(x_0)\rangle$
  - Suppose we could clone states.
  - Eventually we would measure $|x_0\rangle$
  - Eventually we would measure $|x_0 + a\rangle$

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there is an $a \in \{0,1\}^n$ such that $f(x \oplus a) = f(x)$. Find a.

- Prepare the state. (We saw how to do that in the last lecture.)

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$$

- But we know that $f(x \oplus a) = f(x)$ for every x.
- Meausuring the second register $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle)|f(x_0)\rangle$
  - Suppose we could clone states.
  - Eventually we would measure $|x_0\rangle$
  - Eventually we would measure $|x_0 + a\rangle$
  - Compute $x_0 \oplus (x_0 + a) = a$.

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there is an $a \in \{0,1\}^n$ such that $f(x \oplus a) = f(x)$. Find a.

- Prepare the state. (We saw how to do that in the last lecture.)

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$$

- But we know that $f(x \oplus a) = f(x)$ for every x.
- Meausuring the second register $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle)|f(x_0)\rangle$
  - Suppose we could clone states.
  - Eventually we would measure $|x_0\rangle$
  - Eventually we would measure $|x_0 + a\rangle$
  - Compute $x_0 \oplus (x_0 + a) = a$.
  - Unfortunately, we are not in cloneland.

- Instead, apply $H^{\otimes n}$ to $\frac{1}{2}(|x_0\rangle + |x_0 \oplus a\rangle)$:

$$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus a) \cdot y})|y\rangle$$

- Instead, apply $H^{\otimes n}$ to $\frac{1}{2}(|x_0\rangle + |x_0 \oplus a\rangle)$:

$$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus a) \cdot y})|y\rangle$$

- $$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y} + (-1)^{x_0 \cdot y}(-1)^{a \cdot y})|y\rangle$$

- Instead, apply $H^{\otimes n}$ to $\frac{1}{2}(|x_0\rangle + |x_0 \oplus a\rangle)$:

$$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus a) \cdot y})|y\rangle$$

- $$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y} + (-1)^{x_0 \cdot y}(-1)^{a \cdot y})|y\rangle$$

- $$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y}[1 + (-1)^{a \cdot y}])|y\rangle$$

- Instead, apply $H^{\otimes n}$ to $\frac{1}{2}(|x_0\rangle + |x_0 \oplus a\rangle)$:

$$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus a) \cdot y})|y\rangle$$

- $$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y} + (-1)^{x_0 \cdot y}(-1)^{a \cdot y})|y\rangle$$

- $$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y}[1 + (-1)^{a \cdot y}])|y\rangle$$

- $[1 + (-1)^{a \cdot y}] = 2$ if $a \cdot y = 0$ and $[1 + (-1)^{a \cdot y}] = 0$ if $a \cdot y = 1$.

- Instead, apply $H^{\otimes n}$ to $\frac{1}{2}(|x_0\rangle + |x_0 \oplus a\rangle)$:

$$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus a) \cdot y})|y\rangle$$

- $$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y} + (-1)^{x_0 \cdot y}(-1)^{a \cdot y})|y\rangle$$

- $$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y}[1 + (-1)^{a \cdot y}])|y\rangle$$

- $[1 + (-1)^{a \cdot y}] = 2$ if $a \cdot y = 0$ and $[1 + (-1)^{a \cdot y}] = 0$ if $a \cdot y = 1$.
- $a \cdot y = 0$ For half of the $a's \in \{0,1\}^n$ and $a \cdot y = 1$ for the other half.

- Instead, apply $H^{\otimes n}$ to $\frac{1}{2}(|x_0\rangle + |x_0 \oplus a\rangle)$:

$$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus a) \cdot y})|y\rangle$$

- $$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y} + (-1)^{x_0 \cdot y}(-1)^{a \cdot y})|y\rangle$$

- $$\frac{1}{2^{(n+1)/2}} \sum_{y=0}^{2^n-1} ((-1)^{x_0 \cdot y}[1 + (-1)^{a \cdot y}])|y\rangle$$

- $[1 + (-1)^{a \cdot y}] = 2$ if $a \cdot y = 0$ and $[1 + (-1)^{a \cdot y}] = 0$ if $a \cdot y = 1$.
- $a \cdot y = 0$ For half of the $a's \in \{0,1\}^n$ and $a \cdot y = 1$ for the other half.
- Then the state of the input register becomes indeed

$$\frac{1}{2^{(n+1)/2}} \sum_{a \cdot y = 0} 2(-1)^{x_0 \cdot y}|y\rangle = \frac{1}{2^{(n-1)/2}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y}|y\rangle$$

- Continuing...

$$\frac{1}{2^{n-1/2}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle$$

- Continuing...

$$\frac{1}{2^{n-1/2}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle$$

- Measuring the input register we get an y such that $a \cdot y = 0$, cutting the number of choices of a by half.

- Continuing...

$$\frac{1}{2^{n-1/2}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle$$

- Measuring the input register we get an y such that $a \cdot y = 0$, cutting the number of choices of a by half.
- Some linear algebra over $\mathbb{F}_2^n$:

- Continuing...

$$\frac{1}{2^{n-1/2}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle$$

- Measuring the input register we get an y such that $a \cdot y = 0$, cutting the number of choices of a by half.
- Some linear algebra over $\mathbb{F}_2^n$:
  - a is completely determ. if we know lin. indep. $y_1, ..., y_{n-1}$ with $y_j \cdot a = 0$ (Gaussian Elimination)

- Continuing...

$$\frac{1}{2^{n-1/2}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle$$

- Measuring the input register we get an y such that $a \cdot y = 0$, cutting the number of choices of a by half.
- Some linear algebra over $\mathbb{F}_2^n$:
  - a is completely determ. if we know lin. indep. $y_1, ..., y_{n-1}$ with $y_j \cdot a = 0$ (Gaussian Elimination)
  - Suppose we have $y_1, ..., y_i$, with $y_j \cdot a = 0$

- Continuing...

$$\frac{1}{2^{n-1/2}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle$$

- Measuring the input register we get an y such that $a \cdot y = 0$, cutting the number of choices of a by half.
- Some linear algebra over $\mathbb{F}_2^n$:
  - a is completely determ. if we know lin. indep. $y_1, ..., y_{n-1}$ with $y_j \cdot a = 0$ (Gaussian Elimination)
  - Suppose we have $y_1, ..., y_i$, with $y_j \cdot a = 0$
  - $\dim(span(y_1, y_2, ..., y_i)) \leq n - 2 \Rightarrow |span(y_1, y_2, ..., y_i)| \leq 2^{n/2} \leq \frac{1}{2}\{y | y \cdot a = 0\}$

- Continuing...

$$\frac{1}{2^{n-1/2}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle$$

- Measuring the input register we get an y such that $a \cdot y = 0$, cutting the number of choices of a by half.
- Some linear algebra over $\mathbb{F}_2^n$:
  - a is completely determ. if we know lin. indep. $y_1, ..., y_{n-1}$ with $y_j \cdot a = 0$ (Gaussian Elimination)
  - Suppose we have $y_1, ..., y_i$, with $y_j \cdot a = 0$
  - $\dim(span(y_1, y_2, ..., y_i)) \leq n - 2 \Rightarrow |span(y_1, y_2, ..., y_i)| \leq 2^{n/2} \leq \frac{1}{2}\{y | y \cdot a = 0\}$
- At each measurement we get an $y \notin span(y_1, y_2, ...y_i)$ with probability greater than $1/2$.

- Continuing...

$$\frac{1}{2^{n-1/2}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle$$

- Measuring the input register we get an y such that $a \cdot y = 0$, cutting the number of choices of a by half.
- Some linear algebra over $\mathbb{F}_2^n$:
  - a is completely determ. if we know lin. indep. $y_1, ..., y_{n-1}$ with $y_j \cdot a = 0$ (Gaussian Elimination)
  - Suppose we have $y_1, ..., y_i$, with $y_j \cdot a = 0$
  - $\dim(span(y_1, y_2, ..., y_i)) \leq n - 2 \Rightarrow |span(y_1, y_2, ..., y_i)| \leq 2^{n/2} \leq \frac{1}{2}\{y | y \cdot a = 0\}$
- At each measurement we get an $y \notin span(y_1, y_2, ...y_i)$ with probability greater than $1/2$.
- After $O(n)$ measurements we have $n - 1$ linearly independent $y's$ such that $y \cdot a = 0$.

- Continuing...

$$\frac{1}{2^{n-1/2}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle$$

- Measuring the input register we get an y such that $a \cdot y = 0$, cutting the number of choices of a by half.
- Some linear algebra over $\mathbb{F}_2^n$:
  - a is completely determ. if we know lin. indep. $y_1, ..., y_{n-1}$ with $y_j \cdot a = 0$ (Gaussian Elimination)
  - Suppose we have $y_1, ..., y_i$, with $y_j \cdot a = 0$
  - $\dim(span(y_1, y_2, ..., y_i)) \leq n - 2 \Rightarrow |span(y_1, y_2, ..., y_i)| \leq 2^{n/2} \leq \frac{1}{2}\{y | y \cdot a = 0\}$
- At each measurement we get an $y \notin span(y_1, y_2, ...y_i)$ with probability greater than $1/2$.
- After $O(n)$ measurements we have $n - 1$ linearly independent $y's$ such that $y \cdot a = 0$.
- Solve the system $Ya = \vec{0}$ to get a.

Hidden Subgroup Problem:

- $f : G \to S$ is a function given as a black box, from a group G to an arbitrary set S.

Hidden Subgroup Problem:

- $f : G \to S$ is a function given as a black box, from a group G to an arbitrary set S.
- Promise: there exists a subgroup $H \leq G$ such that for all $x, y \in G$, $f(x) = f(y)$ if and only if $Hx = Hy$.

Hidden Subgroup Problem:

- $f : G \to S$ is a function given as a black box, from a group G to an arbitrary set S.
- Promise: there exists a subgroup $H \leq G$ such that for all $x, y \in G$, $f(x) = f(y)$ if and only if $Hx = Hy$.
- Find generators $g_1 g_2 ... g_k$ of H.

Hidden Subgroup Problem:

- $f : G \to S$ is a function given as a black box, from a group G to an arbitrary set S.
- Promise: there exists a subgroup $H \leq G$ such that for all $x, y \in G$, $f(x) = f(y)$ if and only if $Hx = Hy$.
- Find generators $g_1 g_2 ... g_k$ of H.
- Fact: Any group H can be generated by a subset of its elements $g_1, g_2, ..., g_k$ for $k = O(\log n)$

Deutsch's problem: Given $f : \{0,1\} \to \{0,1\}$ with the promise that $f(0) = f(1)$ or $f(0) \neq f(1)$ determine which is the case.

- Underlying group: $G = \mathbb{Z}_2$

Deutsch's problem: Given $f : \{0,1\} \to \{0,1\}$ with the promise that $f(0) = f(1)$ or $f(0) \neq f(1)$ determine which is the case.

- Underlying group: $G = \mathbb{Z}_2$
- f is constant $\Rightarrow H = \mathbb{Z}_2$

Deutsch's problem: Given $f : \{0,1\} \to \{0,1\}$ with the promise that $f(0) = f(1)$ or $f(0) \neq f(1)$ determine which is the case.

- Underlying group: $G = \mathbb{Z}_2$
- f is constant $\Rightarrow H = \mathbb{Z}_2$
- f is balanced $\Rightarrow H = \{0\}$

Given $f : \{0,1\}^n \to \{0,1\}$ with the promise that either f is constant or half of the inputs evaluate to 0 and half to 1.

- Exercise.

Given $f : \{0,1\}^n \to \{0,1\}$ with the promise that either f is constant or half of the inputs evaluate to 0 and half to 1.

- Exercise.
- What is the underlying group G?

Given $f : \{0,1\}^n \to \{0,1\}$ with the promise that either f is constant or half of the inputs evaluate to 0 and half to 1.

- Exercise.
- What is the underlying group G?
- Who is H for each possible answer?

Bernstein-Vazirani's problem: Given $f : \{0,1\}^n \to \{0,1\}$ with the promise that there is an $a \in \{0,1\}^n$ for which $f(x) = a \cdot x$. Find a.

- Underlying Group: $G = \mathbb{Z}_2^n$

Bernstein-Vazirani's problem: Given $f : \{0,1\}^n \to \{0,1\}$ with the promise that there is an $a \in \{0,1\}^n$ for which $f(x) = a \cdot x$. Find a.

- Underlying Group: $G = \mathbb{Z}_2^n$
- Hidden Subgroup: $H = \{y | a \cdot y = 0\}$

Simon's problem: Given $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there is an $a \in \{0,1\}^n$ such that $f(x \oplus a) = f(x)$ for every $x \in \{0,1\}^n$, find a.

- Underlying Group: $G = \mathbb{Z}_2^n$

Simon's problem: Given $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there is an $a \in \{0,1\}^n$ such that $f(x \oplus a) = f(x)$ for every $x \in \{0,1\}^n$, find a.

- Underlying Group: $G = \mathbb{Z}_2^n$
- Hidden subgroup: $H = \{0, a\}$

Period finding: Given $f : Z_N \to \mathbb{Z}_n$ such that there exists an r with $r|N$ for which $f(x+r) = f(x)$ for all $x \in Z_N$, find the smallest such an r.

- Underlying group: $\mathbb{Z}_N$

Period finding: Given $f : Z_N \to \mathbb{Z}_n$ such that there exists an r with $r|N$ for which $f(x+r) = f(x)$ for all $x \in Z_N$, find the smallest such an r.

- Underlying group: $\mathbb{Z}_N$
- Hidden subgroup $r\mathbb{Z}_N$

Reduction from Integer Factorization To Period Finding

- Example: $f : Z_N \to \mathbb{Z}_n$

Reduction from Integer Factorization To Period Finding

- Example: $f : Z_N \to \mathbb{Z}_n$
- $f(x) = a^x \mod n$

Reduction from Integer Factorization To Period Finding

- Example: $f : Z_N \to \mathbb{Z}_n$
- $f(x) = a^x \mod n$
- find r such that $f(a + r) = a^{x+r}$

Reduction from Integer Factorization To Period Finding

- Example: $f : Z_N \to \mathbb{Z}_n$
- $f(x) = a^x \mod n$
- find r such that $f(a + r) = a^{x+r}$
- n is the number to be factorized.

Reduction from Integer Factorization To Period Finding

- Example: $f : Z_N \to \mathbb{Z}_n$
- $f(x) = a^x \mod n$
- find r such that $f(a + r) = a^{x+r}$
- n is the number to be factorized.
- Ideally N is a multiple of r, but since we don't know r choosing $N >> n$ will do.

Reduction from Integer Factorization To Period Finding

- Example: $f : Z_N \to \mathbb{Z}_n$
- $f(x) = a^x \mod n$
- find r such that $f(a + r) = a^{x+r}$
- n is the number to be factorized.
- Ideally N is a multiple of r, but since we don't know r choosing $N >> n$ will do.
- The idea is that f has a sufficient number of periods.

Discrete Logarithm:

- Let p be a prime.

Discrete Logarithm:

- Let p be a prime.
- Suppose there exists an integer r such that $x = g^r \mod p$.

Discrete Logarithm:

- Let p be a prime.
- Suppose there exists an integer r such that $x = g^r \mod p$.
- Compute $r = log_g x \mod p$.

Discrete Logarithm:

- Let p be a prime.
- Suppose there exists an integer r such that $x = g^r \mod p$.
- Compute $r = log_g x \mod p$.
- Function: $f : \mathbb{Z}_{p-1}^{+} \times \mathbb{Z}_{p-1}^{+} \to \mathbb{Z}_{p}^{\times}$

Discrete Logarithm:

- Let p be a prime.
- Suppose there exists an integer r such that $x = g^r \mod p$.
- Compute $r = log_g x \mod p$.
- Function: $f : \mathbb{Z}_{p-1}^{+} \times \mathbb{Z}_{p-1}^{+} \to \mathbb{Z}_{p}^{\times}$
- where $f(a, b) = g^a x^{-b} \mod p$

Discrete Logarithm:

- Let p be a prime.
- Suppose there exists an integer r such that $x = g^r \mod p$.
- Compute $r = log_g x \mod p$.
- Function: $f : \mathbb{Z}_{p-1}^{+} \times \mathbb{Z}_{p-1}^{+} \to \mathbb{Z}_{p}^{\times}$
- where $f(a,b) = g^a x^{-b} \mod p$
- f is a homomorphism from $Z_{p-1}^{+} \times Z_{p-1}^{+} \to \mathbb{Z}_{p}^{\times}$,
  $f(a_1 + a_2, b_1 + b_2) = f(a_1, b_1) f(a_2, b_2) \mod p$

Discrete Logarithm:

- Let p be a prime.
- Suppose there exists an integer r such that $x = g^r \mod p$.
- Compute $r = log_g x \mod p$.
- Function: $f : \mathbb{Z}_{p-1}^+ \times \mathbb{Z}_{p-1}^+ \to \mathbb{Z}_p^\times$
- where $f(a,b) = g^a x^{-b} \mod p$
- f is a homomorphism from $Z_{p-1}^+ \times Z_{p-1}^+ \to \mathbb{Z}_p^\times$, $f(a_1 + a_2, b_1 + b_2) = f(a_1, b_1) f(a_2, b_2) \mod p$
- Kernel of f: $Ker(f) = \{0, (r,1)\}$. Which is a subgroup of $\mathbb{Z}_{p-1}^+ \times \mathbb{Z}_{p-1}^+$ since f is an homomorphism.

Discrete Logarithm:

- Let p be a prime.
- Suppose there exists an integer r such that $x = g^r \mod p$.
- Compute $r = log_g x \mod p$.
- Function: $f : \mathbb{Z}_{p-1}^+ \times \mathbb{Z}_{p-1}^+ \to \mathbb{Z}_p^\times$
- where $f(a,b) = g^a x^{-b} \mod p$
- f is a homomorphism from $Z_{p-1}^+ \times Z_{p-1}^+ \to \mathbb{Z}_p^\times$, $f(a_1 + a_2, b_1 + b_2) = f(a_1, b_1) f(a_2, b_2) \mod p$
- Kernel of f: $Ker(f) = \{0, (r,1)\}$. Which is a subgroup of $\mathbb{Z}_{p-1}^+ \times \mathbb{Z}_{p-1}^+$ since f is an homomorphism.
- $H = \{0, (r,1)\}$

Quantum fourier Transform: $\omega = e^{\frac{2\pi i}{N}}$, $e^{i\pi} = -1$, $e^{2i\pi} = 1$

$$QFT|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} |k\rangle$$

$$F_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \dots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{(N-1)} & \omega^{(N-1)2} & \dots & \omega^{(N-1)(N-1)} \end{bmatrix}$$

- Writing j in binary:

$$j = j_1 2^{n-1} + j_2 2^{n-2} + \ldots + j_n 2^0$$

- Writing j in binary:

$$j = j_1 2^{n-1} + j_2 2^{n-2} + ... + j_n 2^0$$

- Notation: $0.j_l j_{l+1} ... j_m$ represents the sum

$$j_l/2 + j_{l+1}/4 + ... + j_m/2^{m-l+1}$$

- Writing j in binary:

$$j = j_1 2^{n-1} + j_2 2^{n-2} + ... + j_n 2^0$$

- Notation: $0.j_l j_{l+1} ... j_m$ represents the sum

$$j_l/2 + j_{l+1}/4 + ... + j_m/2^{m-l+1}$$

- Want to prove that: $QFT|j\rangle =$

$$\frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle) \otimes (|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle) \otimes ... \otimes (|0\rangle + e^{2\pi i 0.j_1 j_2 ... j_n})|1\rangle}{2^{n/2}}$$

- Writing j in binary:

$$j = j_1 2^{n-1} + j_2 2^{n-2} + ... + j_n 2^0$$

- Notation: $0.j_l j_{l+1} ... j_m$ represents the sum

$$j_l/2 + j_{l+1}/4 + ... + j_m/2^{m-l+1}$$

- Want to prove that: $QFT|j\rangle =$

$$\frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle) \otimes (|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle) \otimes ... \otimes (|0\rangle + e^{2\pi i 0.j_1 j_2 ... j_n})|1\rangle}{2^{n/2}}$$

- This expression will yield an elegant quantum circuit for computing $QFT|j\rangle$.

- Start with the definition of $QFT|j\rangle$

$$QFT|j\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n}|k\rangle$$

- Start with the definition of $QFT|j\rangle$

$$QFT|j\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n}|k\rangle$$

- Expand k in binary:

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{\frac{2\pi ij}{2^n}(\sum_{l=1}^{n} k_l 2^{n-l})}|k_1\rangle|k_2\rangle\dots|k_n\rangle$$

- Start with the definition of $QFT|j\rangle$

$$QFT|j\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n}|k\rangle$$

- Expand k in binary:

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{\frac{2\pi ij}{2^n}(\sum_{l=1}^{n} k_l 2^{n-l})}|k_1\rangle|k_2\rangle\dots|k_n\rangle$$

- Simplifying the exponent:

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{2\pi ij(\sum_{l=1}^{n} k_l 2^{-l})}|k_1\rangle|k_2\rangle\dots|k_n\rangle$$

- Start with the definition of $QFT|j\rangle$

$$QFT|j\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n}|k\rangle$$

- Expand k in binary:

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{\frac{2\pi ij}{2^n}(\sum_{l=1}^{n} k_l 2^{n-l})}|k_1\rangle|k_2\rangle\dots|k_n\rangle$$

- Simplifying the exponent:

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{2\pi ij(\sum_{l=1}^{n} k_l 2^{-l})}|k_1\rangle|k_2\rangle\dots|k_n\rangle$$

- Writing the tensor product Concisely:

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi ijk_l 2^{-l}}|k_l\rangle$$

- Continuing (last expression of the previous slide):

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle$$

- Continuing (last expression of the previous slide):

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle$$

- Swapping $\bigotimes$ and $\sum$:

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right]$$

- Continuing (last expression of the previous slide):

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle$$

- Swapping $\otimes$ and $\sum$:

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right]$$

- Expanding k_l:

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right]$$

- Continuing (last expression of the previous slide):

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle$$

- Swapping $\otimes$ and $\sum$:

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right]$$

- Expanding k_l:

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right]$$

- To exercise your patience (A lot of elementary algebraic manipulations):

$$= \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)\ldots(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)}{2^{n/2}}$$

On 3 qubits. Fourier transform over $\mathbb{Z}_8$.

$$F_{2^3} = \frac{1}{\sqrt{2^3}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}$$

$$|x_1, x_2, x_3\rangle \rightarrow \frac{1}{\sqrt{2^3}}(|0\rangle + e^{2\pi i[0.x_3]}|1\rangle) \otimes (|0\rangle + e^{2\pi i[0.x_2x_3]}|1\rangle) \otimes (|0\rangle + e^{2\pi i[0.x_1x_2x_3]}|1\rangle)$$

$$|x_1, x_2, x_3\rangle \rightarrow \frac{1}{\sqrt{2^3}}(|0\rangle + e^{2\pi i[0.x_3]}|1\rangle) \otimes (|0\rangle + e^{2\pi i[0.x_2 x_3]}|1\rangle) \otimes (|0\rangle + e^{2\pi i[0.x_1 x_2 x_3]}|1\rangle)$$

$$R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \qquad CR_\theta = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{bmatrix}$$

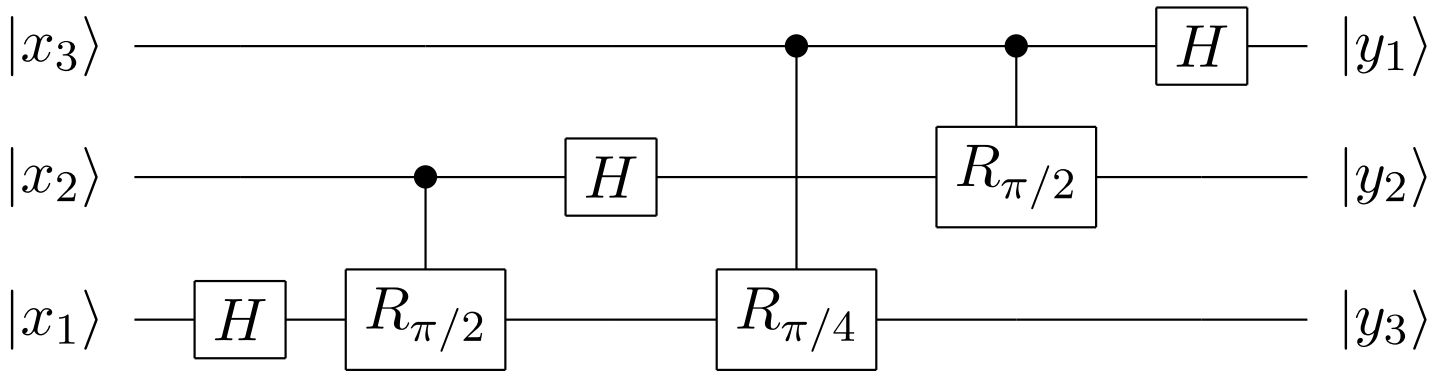

Figure: QFT 3 qubits