Lecture 3 on Quantum Computing

Desy workshop seminar w. 2023. Notes by Isak Stomberg

References

- Lecture notes: Ronald de Wolf's lecture notes ch. 6.
- Books: Quantum Computing: A gentle introduction by Eleanor Rieffel, App. B
- Video: The hidden subgroup problem: Lecture 17 of Quantum computing at CMU

Last couple of lectures

- Studied various "Problems" in quantum computing and found solutions to them.

Examples

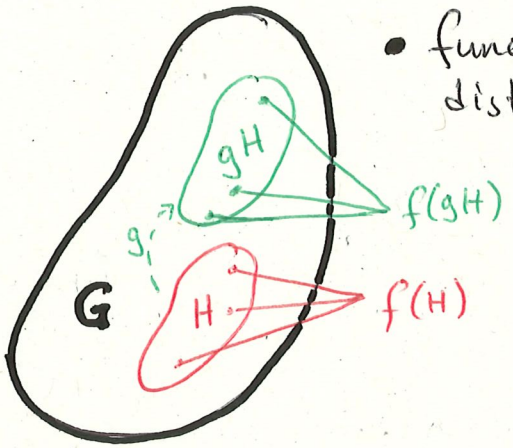
- Simon's problem: $f(x \oplus a) = f(x)$, find a.
  $x, a \in \mathbb{Z}_2^n$ = binary strings, e.g. $x = 0010110$
- Shor's period finding: $f(x+kr) = f(x)$, find r.
  $x, r \in \mathbb{Z}_n$ and r is the period of f.

This lecture

- Introduce a more general problem phrased in the language of group theory.
- This defines a class of problems, and we will see that this generalized formulation contain the two examples above, including many others.

Warmup: graphically illustrate the idea

The hidden subgroup problem (HSP)



- group G, subgroup H, cosets gH, $g \in G$
- function f which is constant and distinct on every coset gH, $g \in G$.
- f "hides" H, which we are now tasked to find.

Some group theory

Definition

- A group G = set of elements with operation "$\circ$" satisfying
  - $g_1 \circ g_2 \in G \quad \forall g_1, g_2 \in G$ (closure)
  - $e \in G : e \circ g = g \circ e = g$ (identity element)
  - g has inverse $g^{-1} : g^{-1} \circ g = g \circ g^{-1} = e$, $g^{-1} \in G$ (inverse).

Note Often, we omit $\circ$, e.g. $g \circ h = gh$.

Examples $(\mathbb{Z}_n, +)$ = additive group of integers $\{0, 1, \ldots, n-1\}$

$(\mathbb{Z}_2^n, \oplus)$ = n-bit strings under bitwise addition modulo 2.

Properties of groups and subgroups

- $|G|$ = number of elements in G, called the "order" of G.
- H is a subgroup of G if H is a subset of G which is itself a group.
- A set of generators of G is a subset of G such that all elements of G can be written as a finite product of generators and their inverses,
- A cyclic group is one which can be generated by a single element.
- A coset of of G is the translation gH of $H \subset G$, $g \in G$.

Abelian groups

- A group is Abelian if $g_1 \circ g_2 = g_2 \circ g_1 \quad \forall g_1, g_2 \in G$
- Any finite Abelian group is cyclically decomposable

$$G = Z_{c_1} \otimes \cdots \otimes Z_{c_k}$$

Representations of finite Abelian groups

- A representation of an Abelian group G is a group homomorphism $\chi : G \to \mathbb{C}$ where $\mathbb{C}$ is the multiplicative group of complex numbers.

Note. Homomorphism $\longrightarrow \chi(g_1 \circ g_2) = \chi(g_1)\,\chi(g_2)$

- χ is called the "character" of G.

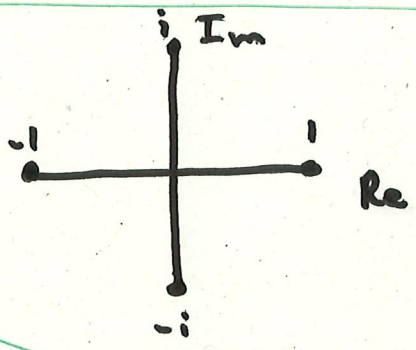
Note: • $\chi(g) = \chi(eg) = \chi(e)\chi(g) \Rightarrow \boxed{\chi(e) = 1}$

• $\chi(e) = \chi(g^{-1}g) = \chi(g^{-1})\chi(g) = 1 \Rightarrow \boxed{\chi(g^{-1}) = \overline{\chi(g)}}$

• $\chi(g)$ is a k:th root of unity, $k = |G|$

• An Abelian group has $k = |G|$ distinct representations χ_i.

Example Z_4 : $\chi_j(k) = e^{\frac{2\pi i}{4} jk}$



Example $Z_2 \otimes Z_2 \otimes \cdots \otimes Z_2 = Z_2^{\otimes n}$

$$a, b = (a_0, a_1, \ldots, a_{n-1}), (b_0, b_1, \ldots, b_{n-1}) \in Z_2^{\otimes n}$$

$$\chi_b(a) = \chi_{b_0}(a_0) \overset{n}{\cdots} \chi_{b_{n-1}}(a_{n-1}) =$$

$$= e^{\frac{2\pi i}{2} a_0 b_0} \cdots e^{\frac{2\pi i}{2} a_{n-1} b_{n-1}} =$$

$$= (-1)^{a_0 b_0 + \ldots + a_{n-1} b_{n-1}} \equiv (-1)^{a \cdot b}$$

Example $Z_n \otimes Z_m$

$$\chi_a(b) = \chi_{a_n}(b_n)\chi'_{a_m}(b_m)$$

Note Since any Abelian group is isomorphic to $Z_{n_0} \otimes \ldots \otimes Z_{n_k}$ we see that the characters $\chi_b(a)$ provide a representation for all groups we are interested in.

Quantum Fourier Transform

Last time:

- $$|X\rangle = \sum_{j=0}^{N-1} a_j |j\rangle \xrightarrow{F} F|X\rangle = \sum_{k=0}^{N-1} A_k |k\rangle \qquad (1)$$

  where $$A_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j e^{\frac{2\pi i}{N} jk}$$

- If we insert A_k in (1), we have

$$F|X\rangle = \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j e^{\frac{2\pi i}{N} jk} \right) |k\rangle$$

$$= \sum_{j=0}^{N-1} a_j \left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i}{N} jk} |k\rangle \right)$$

$$\equiv \sum_{j=0}^{N-1} a_j |x_j\rangle$$

Thus, the QFT can be defined as

$$\mathcal{F}: |j\rangle \xrightarrow{F} |x_j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i}{N} jk} |k\rangle$$

- We wish to generalize this result to finite abelian groups, and do this by the following mapping:

$$\frac{1}{\sqrt{N}} \rightarrow \frac{1}{\sqrt{|G|}}$$

$$\sum_{k=0}^{N-1} \rightarrow \sum_{g \in G}$$

$$e^{\frac{2\pi i}{N} jk} \rightarrow \chi_h(g)$$

$$|k\rangle \rightarrow |g\rangle$$

where $g, h \in G$.

This time

- Therefore, we define $|\chi_k\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \chi_k(g) |g\rangle$ where $g, k \in G$, and the generalized QFT as the map

$$\mathcal{F}: |g\rangle \xrightarrow{\mathcal{F}} \mathcal{F}|g\rangle = |\chi_g\rangle .$$

Note $|\chi_g\rangle$ forms a basis which we call the Fourier basis: $\langle \chi_g | \chi_k \rangle = \delta_{gk}$

- The Fourier transform can then be written

$$\mathcal{F} = \sum_{g \in G} |\chi_g\rangle\langle g| \quad \text{with inverse} \quad \mathcal{F}^{-1} = \sum_{g \in G} |g\rangle\langle \chi_g|$$

- The elements of $\mathcal{F}$ are

$$\mathcal{F}_{gh} = \langle g|\mathcal{F}|h\rangle = \sum_{g' \in G} \langle g|\chi_{g'}\rangle\langle g'|h\rangle =$$

$$= \langle g|\chi_h\rangle = \frac{1}{\sqrt{|G|}} \sum_{k \in G} \chi_h(k) \langle g|k\rangle = \frac{\chi_h(g)}{\sqrt{|G|}}$$

i.e. $\mathcal{F}_{gh} = \frac{\chi_h(g)}{\sqrt{|G|}}$. Likewise,

$$\left(\mathcal{F}^{-1}\right)_{gh} = \frac{\overline{\chi_g(h)}}{\sqrt{|G|}}$$

- With the notion of QFT Generalized to finite abelian groups, lets look at a few examples.

Example: $G = Z_2 = \{0, 1\}$

$$\chi_i(j) = \frac{1}{\sqrt{2}} e^{\frac{2\pi i}{2} ij} = \frac{(-1)^{ij}}{\sqrt{2}} \Rightarrow F = \frac{1}{\sqrt{2}} \begin{pmatrix} (-1)^{0\cdot 0} & (-1)^{0\cdot 1} \\ (-1)^{0\cdot 1} & (-1)^{1\cdot 1} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

This is just the Hadamar transform.

Example: $Z_4 = \{0, 1, 2, 3\}$

$$F = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Example: $Z_2 \circ Z_2 = \{(0,0), (0,1), (1,0), (1,1)\}$

$$F_{gh} = \frac{\chi_g(h)}{\sqrt{|G|}} = \frac{\chi_{g_1}(h_1)\chi_{g_2}(h_2)}{\sqrt{4}} = \frac{1}{2}(-1)^{g_1 h_1}(-1)^{g_2 h_2} = \frac{1}{2}(-1)^{g \cdot h}$$

Thus

$$F = \frac{1}{2} \begin{pmatrix} (-1)^{0\cdot 0+0\cdot 0} & (-1)^{0\cdot 0+0\cdot 1} & (-1)^{0\cdot 1+0\cdot 0} & (-1)^{0\cdot 1+0\cdot 1} \\ (-1)^{0\cdot 0+1\cdot 0} & (-1)^{0\cdot 0+1\cdot 1} & (-1)^{0\cdot 1+1\cdot 0} & (-1)^{0\cdot 1+1\cdot 1} \\ (-1)^{1\cdot 0+0\cdot 0} & (-1)^{1\cdot 0+0\cdot 1} & (-1)^{1\cdot 1+0\cdot 0} & (-1)^{1\cdot 1+0\cdot 1} \\ (-1)^{1\cdot 0+1\cdot 0} & (-1)^{1\cdot 0+1\cdot 1} & (-1)^{1\cdot 1+1\cdot 0} & (-1)^{1\cdot 1+1\cdot 1} \end{pmatrix} \begin{matrix} (0,0) \\ (0,1) \\ (1,0) \\ (1,1) \end{matrix}$$

$$(0,0) \quad (0,1) \quad (1,0) \quad (1,1)$$

$$= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} H & H \\ H & -H \end{pmatrix} = \frac{1}{2} H \otimes H = F_2 \otimes F_2$$

- We see from the last example how $\mathcal{F}$ can be obtained for general Abelian groups with cyclic decompositions.

In general $G \cong \mathbb{Z}_m \otimes \mathbb{Z}_n \otimes \cdots \otimes \mathbb{Z}_\ell$

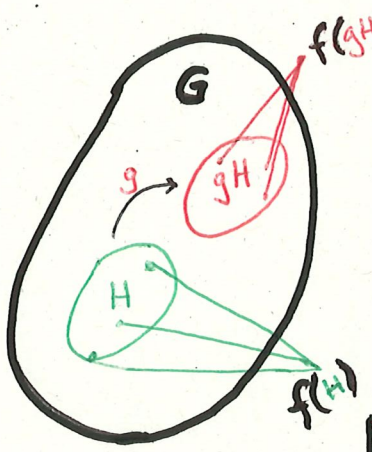
$$\rightarrow \boxed{\mathcal{F} = \mathcal{F}_{\mathbb{Z}_m} \otimes \mathcal{F}_{\mathbb{Z}_n} \otimes \cdots \otimes \mathcal{F}_{\mathbb{Z}_\ell}}$$

Comment For non-Abelian groups, it is still possible to define the QFT, but the representations are more complicated.

General solution to the finite Abelian Subgroup Problem

Problem

Graphically



$f(H) = const_H$

$f(gH) = const_{gH} \neq const_H$

for $gH \neq H$.

Find H

In words

Let G be finite abelian $\Rightarrow G \cong \mathbb{Z}_{n_0} \oplus \dots \oplus \mathbb{Z}_{n_L}$

Let $H < G$ be a subgroup of G implicitly defined by a function $f: G \to G$ that is constant and distinct on every coset gH of H. **Find H or a generating set for H**

Solution

- The solution consists of steps which we outline below.

(1)

$$|\psi_0\rangle = \left\{ \begin{array}{l} |0\rangle \to \boxed{H} \to \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \\ |0\rangle \longrightarrow |0\rangle \end{array} \right\} = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|0\rangle = |\psi_1\rangle$$

This prepares the state $|\psi_1\rangle$ as the maximally entangled state $H|0\rangle$ in the first register and $|0\rangle$ in the second.

(2) Now, apply U_f to $|\psi_1\rangle$. This produces

$$|\psi_2\rangle = U_f |\psi_1\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle$$

(3) Measure the second register. Since f is constant on all cosets gH, this measurement cause the first register to collapse onto a uniform superposition on all states belonging to a $\tilde{g}H$.

From now, we consider only the first register, whose state is now

$$|\psi_3\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |\tilde{g}h\rangle$$

(4) We now apply QFT to $|\psi_3\rangle$

$$\mathcal{F}|\psi_3\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} \mathcal{F}|\tilde{g}h\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |\chi_{\tilde{g}h}\rangle$$

$$= \frac{1}{\sqrt{|H|}} \sum_{h \in H} \frac{1}{\sqrt{|G|}} \sum_{g' \in G} \chi_{\tilde{g}h}(g') |g'\rangle =$$

$$= \frac{1}{\sqrt{|G||H|}} \sum_{g' \in G} \chi_{\tilde{g}}(g') \underbrace{\left[\sum_{h \in H} \chi_h(g')\right]}_{= \begin{cases} |H| & \text{iff } \chi_h(g') = 1 \ \forall h \in H \\ 0 & \text{otherwise} \end{cases}} |g'\rangle$$

Schur's lemma for subgroups

(4) continuation

Schur's lemma for subgroups says

$$\sum_{h\in H}\chi_h(g)=\begin{cases}|H| & \text{iff } \chi_h(g)=1\ \forall h\in H\\ 0 & \text{otherwise}\end{cases}$$

Therefore, define the set $H^{\perp}=\{g\in G \mid \chi_h(g)=1\ \forall h\in H\}$.

$F|x_3\rangle$ can now be written as

$$F|x_3\rangle=\sqrt{\frac{|H|}{|G|}}\sum_{g\in H^{\perp}}\chi_g(g)\,|g\rangle\equiv|x_4\rangle$$

$\chi_g(g)$ is just a phase, so $|\chi_g(g)|^2=1$.

Therefore, F simply projects $|x_3\rangle$ onto a uniform superposition of states $|g\rangle$, $g\in H^{\perp}$.

(5) Above 4 steps samples uniformly over all elements in $H^{\perp}$. Thus, next step, a masurement, yields a state $|g^*\rangle$, $g^*\in H^{\perp}$, with equal probability. This measurement, therefore, presents a constraint on H:

$$\chi_h(g^*)=1\ \forall h\in H$$

Repeating the procedure k times yields a set of equations

$$\begin{aligned}&\chi_h(g_1^*)=1\\ &\chi_h(g_2^*)=1 \qquad \forall h\in H\\ &\quad\vdots\\ &\chi_h(g_k^*)=1\end{aligned}$$

(5) continuation

The form of these equations vary from problem to problem, but we will see below how H can be determined by solving them for a few cases.

Simon's problem revisited

Given a (two-to-one) function f such that $f(x) = f(x \oplus a)$ for $x = (x_0 x_1 x_2 \ldots x_{n-1}) \in \mathbb{Z}_2^n$, find a.

We will phrase this as an instance of the HSP.

Let $G = \mathbb{Z}_2^n$, $H = \{0^n, a\}$, then f is constant and distinct on all cosets $xH = \{x \oplus 0^n, x \oplus a\}$ $\forall x \in G$.

$\Rightarrow$ this is an HSP.

Solution

In the last step of the solution to the general problem, we measure a state $x^* \in H^\perp$ where

$$H^\perp = \{x \in G \mid \chi_h(x) = 1 \ \forall \ h \in H\}$$

In other words, ($x \cdot y$: dot product)

$$H^\perp = \{x \in \mathbb{Z}_2^n \mid (-1)^{x \cdot y} = 1 \ \forall \ y \in \{0^n, a\}\}$$

$$= \{x \in \mathbb{Z}_2^n \mid x \cdot y = 0 \bmod 2 \ \forall \ y \in \{0^n, a\}\}$$

$$= \{x \in \mathbb{Z}_2^n \mid x \cdot a = 0 \bmod 2\}$$

So the measured x^* obeys $\boxed{x^* \cdot a = 0 \bmod 2}$

Suppose we make k measurements, we have k linear equations

$$x_1^* \cdot a = 0 \mod 2$$
$$x_2^* \cdot a = 0 \mod 2$$
$$\vdots$$
$$x_k^* \cdot a = 0 \mod 2$$

Example $a = 010 \Longrightarrow H^+ = \{000, 001, 100, 101\}$

we dont know this beforehand

Can measure these

Equations:

$$000 \cdot a = 0 = 0 \mod 2$$
$$001 \cdot a = a_3 = 0 \mod 2 \Longrightarrow a_3 = 0$$
$$100 \cdot a = a_1 = 0 \mod 2 \Longrightarrow a_1 = 0$$
$$101 \cdot a = a_1 + a_3 = 0 \mod 2$$
$$\Longrightarrow a_2 \text{ is free } \in \{0, 1\}$$

Thus, $H = \{000, 010\}$ and we have found H.

We see that HSP + classical computation solves Simon's problem

Note Need to repeat measurement until $n-1$ linearly independent equations are found. This should take $O(n)$ measurements.

Note Classical computation takes $O(n^2)$

So if U_f has polylog time complexity, then the whole solution has polylog time complexity.

Shor's period finding revisited

The periodic function f has the property $f(x+r) = f(x)$, find x.

Let $G = \mathbb{Z}_n$, $H = \{kr \mid k \in [0, \dots, \frac{n}{r})\}$ (assume r divides n)

$\mathbb{Z}_n$ has representations $\chi_g(h) = e^{\frac{2\pi i}{n} gh}$, $g, h \in G = \mathbb{Z}_n$.

Again, the method to solve the HSP reduces the problem to perform a set of measurements x^* and use classical algorithms to find $H = \langle r \rangle$ (generated by r)

$$\text{All } x^* \in H^\perp = \{x \in G \mid \chi_h(x) = 1 \ \forall h \in H\}$$

$$= \{x \in G \mid e^{\frac{2\pi i}{n} xh} = 1 \ \forall h \in H\}$$

$$= \{x \in \mathbb{Z}_n \mid \frac{xh}{n} = a = \text{integer} \ \forall h \in H\}$$

$$= \{x \in \mathbb{Z}_n \mid \frac{xkr}{n} = a \ \forall k \in [0, \dots, \tfrac{n}{r})\}$$

i.e. x^* satisfies $\frac{x^* k r}{n} = a$. If $a = \text{integer}$ for $k = 1$, then ka is also an integer, so WLOG take $k = 1$.

$\Rightarrow$ condition $\frac{x^* k r}{n} = \{k = 1\} = \boxed{\frac{x^* r}{n} = a}$, which we write as $\boxed{\frac{x^*}{n} = \frac{a}{r}}$ (known / unknown). Thus any measured x^* is a multiple of $\left(\frac{n}{r}\right)$ and a series of measurements will allow us to infer what r is.

Example

Take $n=20$, and let the unknown $r=5$.

Any x^* which we measure is a multiple of $\frac{n}{r}=4$, so we measure some $x^* \in \{0,4,8,12,16\}$

eg. $x_1^* = 12 = a_1\left(\frac{20}{r}\right)$

$x_2^* = 16 = a_2\left(\frac{20}{r}\right)$

$x_3^* = 4 = a_3\left(\frac{20}{r}\right)$

(greatest common divisor)

We see that $\frac{20}{r}$ is the gcd of all x^*. This is clearly 4, so $\frac{20}{r}=4 \Rightarrow r=\frac{20}{5}$, and we have infered what r is.

Now $H=\langle r \rangle = \{kr \mid k \in \{[0,1,\ldots,\frac{n}{r})\}\}$ which solves the HSP.