Hidden subgroup problem.

Def-n. Let G be a (finite) group and $H \subset G$ a subgroup. The set of elements $gH := \{gh \mid h \in H\}$ is called a left coset of H in G.

Rmk. $G = \bigcup_{g \in G} gH$ (set theoretically).

Example. $G = \mathbb{Z}$, $H = 5\mathbb{Z}$. The left cosets are $j + 5\mathbb{Z}$, $j \in \{0,1,2,3,4\}$. In this case the set of left cosets $G/H = \mathbb{Z}/5\mathbb{Z}$ is a group. This is true if $H \subset G$ is normal: $gHg^{-1} = H$ $\forall g \in G$.

(HSP) Hidden subgroup problem: let $f: G \to S$ be a function satisfying $f(gh) = f(g) \Leftrightarrow h \in H$ (some unknown subgroup). The goal is to find H.

In case G is a finite abelian group, the solution can be obtained using Shor's algorithm. It will be convenient to interpret the DFT in terms of characters of G, these are homomorphisms $\chi: G \to \mathbb{C}^*$, where $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ is a group under multiplication and

$$\chi(gh) = \chi(g)\chi(h) \quad \forall g, h \in G.$$
$$\chi(e) = 1.$$

Properties:

1. If $g \in G$ is of finite order, i.e. $\exists r \in \mathbb{Z}_{>0}$ with $g^r = id$, then

$$\underbrace{\chi(g^r)}_{= \chi^r(g)} = \chi(id) = 1 \quad \text{giving } \chi(g) = \left(e^{\frac{2\pi i}{r}}\right)^s \text{ for some } s \in \mathbb{Z}.$$

In particular, $|\chi(g)| = 1$.

2. If G is finite, then the image of χ is contained in $S^1 \subset \mathbb{C}^*$ (the unit circle).

3. The characters form a group under pointwise multiplication. It is called the <u>dual group of G</u> and will be denoted by $G^\vee$.

<u>Example.</u> $G = \mathbb{Z}_N$, let $\chi : G \to \mathbb{C}^*$ be a character.

$\chi(k) = \chi(\underbrace{1 + \dots + 1}_{k}) = \chi^k(1)$, hence, χ is completely determined by its value at 1. Moreover, $\chi(\underbrace{1 + \dots + 1}_{N}) = \chi^N(1) = 1$, $\underbrace{1 + \dots + 1}_{N} = 0$, so $\chi(0)$

So $\chi(1) = \omega^s$ for some $0 \leq s \leq N-1$ (as before, $\omega = e^{2\pi i/N}$).

Let's denote such a character by χ_s, then $G^\vee = \{\chi_0, \dots, \chi_{N-1}\}$ with $\chi_s \cdot \chi_j = \chi_{s+j \,(\mathrm{mod}\, N)}$ as

$$\chi_s \cdot \chi_j(k) = \chi_s(k)\chi_j(k) = \omega^{sk}\omega^{jk} = \omega^{(s+j)k} \;\forall j, k, s \in \mathbb{Z}_N$$

Notice that there is an isomorphism $G \simeq G^\vee$ (via $s \mapsto \chi_s$).

Furthermore, the discrete Fourier transform for $\mathbb{Z}_N$ can be written as $F_N(k) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{jk} |j\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \chi_k(j)|j\rangle$, which can (informally) be written as

$$F_N(\underset{\text{delta fn}}{\delta_k}) = \chi_k.$$

Rmk. Similarly for any finite abelian G, we have $G \simeq G^\vee$ via $g \mapsto \chi_g$.

Recall that we defined the Fourier transform as a map from $\mathbb{C}[G]$ (functions on G with values in $\mathbb{C}$) to itself. The physical interpretation of δ's and χ's is as functions of precise position and momenta, respectively.

Next we sketch an algorithm for solving HSP for a finite abelian group G and a finite set S.

① Start with a state $|0^{|G|}\rangle|0^{|S|}\rangle$ and apply $H^{\otimes|G|}\otimes Id^{\otimes|S|}$ to get the generic state $\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle|0^{|S|}\rangle$.

② Apply the oracle of f to obtain $\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle|f(g)\rangle$ and measure the second register. The outcome will be some $s\in S$ and the state vector turns into

$$\frac{1}{\sqrt{|H|}}\sum_{h\in H}|ah\rangle, \quad \underset{(a\in G)}{f(a)=s.}$$

③ Apply the DFT to come up with

$$\frac{1}{\sqrt{|H|}}\sum_{h\in H}\frac{1}{\sqrt{|G|}}\sum_{g\in G}\chi_{ah}(g)\,|g\rangle = \frac{1}{\sqrt{|H|\cdot|G|}}\sum_{h\in H}\sum_{g\in G}\chi_a(g)\chi_h(g)|g\rangle$$

$$= \frac{1}{\sqrt{|H|\cdot|G|}}\sum_{g\in G}\chi_a(g)\Big(\sum_{h\in H}\chi_h(g)\Big)|g\rangle.$$

Lemma. $\sum_{h\in H}\chi_h(g) = \begin{cases}|H|, & \chi_g\in H^\perp\\ 0, & \text{o/wise.}\end{cases}$ Here $H^\perp = \{\chi_g \mid \chi_g(h)=1\ \forall h\in H\}$

Proof. $\sum_{h\in H}\chi_h(g) \underset{\substack{\uparrow\\ \text{'}\omega^{gh}=\omega^{hg}\text{'}\\ \text{(coordinate-wise for } G=\mathbb{Z}_{N_1}\times\dots\times\mathbb{Z}_{N_k})}}{=} \sum_{h\in H}\chi_g(h)$, so if $\chi_g\in H^\perp$ the statement follows.

On the other hand, if $\chi_g \notin H^\perp$, then $\exists h' \in H : \chi_g(h') \neq 1$. Notice that $h'H = H$ (for instance, $h = h' \cdot (h'^{-1} \cdot h)$), hence,

$$\sum_{h \in H} \chi_g(h) = \sum_{h \in H} \chi_g(h'h) = \sum_{h \in H} \chi_g(h')\, \chi_g(h) =$$

$$= \chi_g(h') \cdot \sum_{h \in H} \chi_g(h) \iff (\chi_g(h') - 1) \sum_{h \in H} \chi_g(h) = 0, \text{ but } \chi_g(h') \neq 1,$$

so $\sum_{h \in H} \chi_g(h) = 0$.

It follows from the lemma that our current state is

$$\frac{1}{\sqrt{|H||G|}} \cdot \sum_{g \in G} \chi_a(g) \sum_{h \in H} \chi_h(g) |g\rangle = \frac{|H|}{\sqrt{|H| \cdot |G|}} \sum_{g, \chi_g \in H^\perp} \chi_a(g) |g\rangle =$$

$$= \sqrt{\frac{|H|}{|G|}} \cdot \sum_{g, \chi_g \in H^\perp} \chi_a(g) |g\rangle.$$

Finally, we measure the first register and get an element $g \in G$ with $\chi_g \in H^\perp$. This gives a constraint on H, since $h \in H$ implies $\chi_g(h) = 1$. After repeating the procedure a few times we get enough constraints to find the generators of H.

Discrete logarithm problem.

As we have already observed in the RSA cryptosystem, one needs a function, which is fast to evaluate given an extra piece of information (factorization of $n=pq$ in case of RSA) and extremely difficult without it (a very long time is required to find this info with known algorithms). Here is the most frequently used type of examples.

Let G be a group and $g \in G$ an element of finite order r. Choose a number $1 < k \leq r-1$ and take $h = g^k$. The discrete logarithm problem is to find k, given G, g and r. The name comes from the shorthand notation

$$h = g^k \iff k = \log_g h.$$

Examples.

① $G = (\mathbb{Z}/100\mathbb{Z}, +)$, $g = 3$. As $\gcd(3,100)=1$, we get $r=100$, so 3 is a generator. Let $h = 11$, then we need to find k:

$$3k \equiv 11 \pmod{100} \iff k \equiv 11 \cdot 3^{-1} \pmod{100}.$$

We use extended Euclid's algorithm to find 3^{-1}:

$$100 = 33 \cdot 3 + 1 \iff 1 = 100 - 33 \cdot 3 \Rightarrow 1 \equiv -33 \cdot 3 \pmod{100},$$

giving $3^{-1} \equiv -33 \equiv 67$. and $k \equiv 11 \cdot 67 \equiv 37 \pmod{100}$

Check: $3 \cdot 37 = 111 \equiv 11 \pmod{100}$ ✓

② $G = (\mathbb{Z}/17\mathbb{Z}^{\times}, \times)$, $g = 2$, $h = 15$, $r = 16$. We need to find k: $2^k \equiv 15 \pmod{17}$

A straightforward calculation (check) shows that $k=5$: $2^5 = 32 \equiv 15$ (17)

Rmk. The DLP for multiplicative group $\mathbb{Z}_N^*$ with $N>>0$ is already difficult but can be solved reasonably fast. We will talk about the DLP problem for different abelian groups, where no reasonably algorithm (classically) is known.

DLP as HSP.

We will show how to 'paraphrase' the discrete logarithm problem as a hidden subgroup problem for an abelian group $\mathbb{K}$. Therefore, the quantum algorithm discussed in the previous lecture is 'applicable'.

Let's take $\mathbb{K} = \mathbb{Z}_r \times \mathbb{Z}_r$, where r is the order of g and $\mathbb{Z}_r$ is the cyclic subgroup generated by g in G. The key observation is that

$$g^a h^{-b} = g^a g^{-kb} = g^{a-kb}$$

depends only on the value of $a-kb$, but not a and b independently. We consider the function

$$f: K \to \mathbb{Z}_r = \langle g \rangle$$

$$f(k) = f(a,b) = g^a h^{-b} \; (= g^{a-kb}).$$

Notice that $f(k) = f(ks)$ for any s in the subgroup

$$K > H = \{(\alpha,\beta) \in K \mid k\alpha - \beta \equiv 0 \pmod r\}.$$

Indeed, $f(a+\alpha, b+\beta) = g^{a+\alpha} h^{-b-\beta} = g^{a+\alpha-k(b+\beta)} = g^{a-kb} \cdot g^{\alpha-k\beta} =$
$= g^{a-kb} = g^a h^{-b} = f(a,b)$.

Moreover, solving the HSP (finding H) allows to find k as $(1,k) \in H$.