Group theory: A group is a set G with an action $\cdot : G \times G \to G$ s.t.

① $\exists$ an element $e \in G$ s.t.

$$e \cdot g = g \cdot e = g \quad \forall\ g \in G.$$

② $$g_1 \cdot (g_2 \cdot g_3) = (g_1 g_2) \cdot g_3 \quad \forall\ g_1, g_2, g_3 \in G.$$

③ $\forall\ g \in G$, $\exists$ a unique element $h \in G$ s.t.

$g \cdot h = h \cdot g = e$. So, we denote h by g^{-1}.

Let H be a non-empty subset of G. H is a subgroup if

① $\forall\ g, h \in H$, $g \cdot h \in H$

② $\forall\ h \in H$, $h^{-1} \in H$.

A group is abelian if $\forall\ g, h \in G$, $g \cdot h = h \cdot g$ (commutes).

For abelian groups, the group action $\cdot$ is often represented as $+$. So $g + h = h + g \in G$. And the identity is expressed as 0. And h^{-1} as $-h$.

For $h_1, \ldots, h_k \in G$, let $\langle h_1, \ldots, h_k \rangle$ be the subgroup of elements expressible by combining $h_1, \ldots, h_k$ and $h_1^{-1}, \ldots, h_k^{-1}$.

For a subgroup $H \leq G$, $\{h_1 \ldots h_k\}$ is a generating set for H if $H = \langle h_1, \ldots, h_k \rangle$.

Think of a generating set as a basis in the case of abelian groups.

Def: Given an abelian group G and a subgroup $H \leq G$, a fn $f: G \to \{0,1\}^m$ hides H if $\forall x, y \in G$,

$f(x) = f(y)$ iff $x - y \in H$.

equiv. f is constant on every coset and varies across cosets.

In Simon's problem, $G = \{0,1\}^n$ and $H = \{0, s\}$.
and the fn f hides H.

For a general abelian group G, in order to define F_G, we need the notion of a character from group theory.

A character is a fn $\varphi : G \to \mathbb{C} \setminus \{0\}$ s.t.

$$\varphi(h_1 + h_2) = \varphi(h_1) \cdot \varphi(h_2).$$

For abelian groups, the set of characters can be indexed by $g \in G$.

Defining $\chi(g,h) = \varphi_g(h)$ gives us the following def:

For now, $\chi : G \times G \to \mathbb{C} \setminus \{0\}$ s.t.

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

② $\chi(g, h_1 + h_2) = \chi(g,h_1)\,\chi(g,h_2)$. $\quad \forall\, g, h_1, h_2 \in G$

③ $\sum_{h \in G} \chi(g,h)^* \chi(g',h) = |G|\, \mathbb{1}\{g = g'\}$ $\quad \forall\, g, g' \in G$.

(orthogonality of characters condition).

Note: the labeling is a choice – like choosing coordinates.
We will fix it throughout.

Let G be a group and χ a fn satisfying above.

Then let $\mathcal{H}$ be a Hilbert space $\mathbb{C}^G$ with a basis indexed by group elements $\{|g\rangle : g \in G\}$.

$$F_G\ |g\rangle := \frac{1}{\sqrt{|G|}} \sum_{h \in G} \chi(g,h)\ |h\rangle.$$

$$F_G = \frac{1}{\sqrt{|G|}} \sum_{g,h \in G} \chi(g,h)\ |h\rangle\langle g|.$$

Pf that F_G is unitary:

$$\langle g_1 |\ F_G^\dagger F_G\ | g_2 \rangle = \frac{1}{|G|} \sum_{h_1, h_2 \in G} \langle h_1 |\ \chi(g_1,h_1)^*\ \chi(g_2,h_2)\ | h_2 \rangle$$

$$= \frac{1}{|G|} \sum_{h \in G} \chi(g_1, h)^* \chi(g_2, h)$$

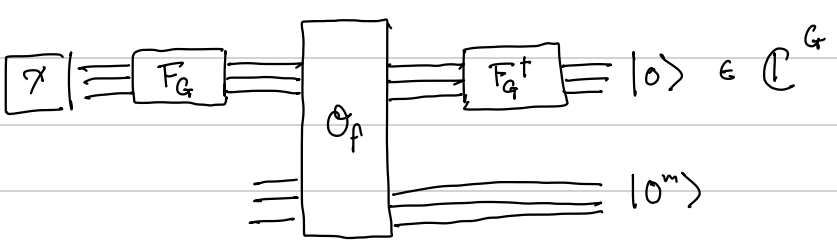
$$= \frac{1}{|G|} \cdot |G| \, \mathbb{1}\{g = g'\} = \mathbb{1}\{g = g'\}.$$

Def. Abelian Hidden Subgroup Problem (AHSP)

given group $G \geq H$ subgroup and fn $f: G \to \{0,1\}^m$ that hides H, identify a generating set for H.

Idea: Subroutine to learn random element of $H^\perp$

where $H^\perp$ is the subgroup $\{ g \mid \chi(g, h) = 1 \ \forall \ h \in H \}$.



Before O_f query: $\frac{1}{\sqrt{|G|}} \sum_{g \in G} \chi(0,g)^* |g\rangle |0^m\rangle$

$$= \frac{1}{\sqrt{|G|}} \sum_{g} |g\rangle |0^m\rangle$$

since $\chi(0,g)^* \chi(h,g)^* = \chi(0+h,g)^* \Rightarrow \chi(0,g) = 1$

Consider measuring second register and getting outcome z.

After O_f query and measurement: For some $z \in \{0,1\}^m$,

$$\propto \sum_{g\,:\,f(g)=z} |g\rangle$$

$$\{ g : f(g) = z \} = g_0 + H = \{ g_0 + h \mid h \in H \} \quad \text{for some } g_0.$$

So state equals $\frac{1}{\sqrt{|H|}} \sum_{h \in H} |g_0 + h\rangle$

Apply F_G :

$$\frac{1}{\sqrt{|G|\cdot|H|}} \sum_{h\in H} \sum_{g\in G} \chi(g_0+h, g)\,|g\rangle$$

$$= \frac{1}{\sqrt{|G|\cdot|H|}} \sum_{h\in H} \sum_{g\in G} \chi(g_0, g)\,\chi(h, g)\,|g\rangle$$

$$= \frac{1}{\sqrt{|G|\cdot|H|}} \sum_{g\in G} \chi(g_0, g) \Big(\underbrace{\sum_{h\in H} \chi(h, g)}_{= |H|\,\mathbb{1}_{\{g\in H^\perp\}} \quad (*)} \Big)\,|g\rangle$$

$$= \sqrt{\frac{|H|}{|G|}} \sum_{g\in H^\perp} \chi(g_0, g)\,|g\rangle = \frac{1}{\sqrt{|H^\perp|}} \sum_{g\in H^\perp} \chi(g_0, g)\,|g\rangle$$

Measuring gives $g \in H^\perp$ uniformly randomly. ∎

Pf of (*): if $g \in H^\perp$ then $\chi(h, g) = 1 \quad \forall\, h \in H$.

so $\sum_{h\in H} \chi(h, g) = |H|$.

if $g \notin H^\perp$, then $\exists\, h_0 \in H$ s.t. $\chi(h_0, g) \neq 1$.

$$\sum_{h\in H} \chi(h, g) = \sum_{h\in H} \chi(h+h_0, g) = \chi(h_0, g) \left(\sum_{h\in H} \chi(h, g) \right)$$

This implies $\sum_{h \in H} \chi(h, g) = 0$.

Rearranging gives the statement of (*).

Ok, learning samples from $H^\perp$ can be used to calculate a generating set for H using Gaussian elimination.

For Simon's problem, $H = \{0, s\}$ so $H^\perp = \{y : y \cdot s = 0\}$.

Ex. Solving AHSP when $G = \mathbb{Z}_Q$, r divides Q

$f(x) = f(x')$ iff $x' - x$ is a multiple of r:

When $G = \mathbb{Z}_Q$, $\chi(g, h) = \omega^{g \cdot h}$ where $\omega = e^{2\pi i / Q}$

Each sample gives y s.t. $\chi(y, r) = 1 \iff yr \equiv 0 \bmod Q$

or $yr = kQ$. Since r divides Q, $\frac{Q}{r}$ is an int.

Each sample $y_i = k_i \cdot \frac{Q}{r}$ is an integer.

$\mathrm{GCD}(\{y_i\}) = \frac{Q}{r}$ with high probability with $O(\log Q)$ samp.