NOTES ON
THE HIDDEN SUBGROUP PROBLEM FOR ABELIAN GROUPS

MATTHEW MOORE

The Hidden Subgroup Problem

`Input:`	group $\mathbb{G}$, function $f : G \to X$ (as a blackbox)
`Promise:`	f hides a subgroup $\mathbb{H} \leq \mathbb{G}$
`Task:`	determine $\mathbb{H}$

By the Fundamental Theorem of Finitely Generated Abelian Groups, if $\mathbb{G}$ is finitely generated and Abelian then there are $m_i \in \mathbb{Z}$ such that

$$\mathbb{G} \cong \prod \mathbb{Z}_{m_i}.$$

Represent $g \in G$ as a vector $g = (g_i)$ in $\prod \mathbb{Z}_{m_i}$. Define a bilinear map $\mu : G \times G \to \mathbb{C}^*$ by

$$\mu(g, h) = \prod \omega_{m_i}^{g_i h_i}$$

where $\omega_k = e^{2\pi i/k}$ is the k-th root of unity. The function μ yields a notion of orthogonality: for $\mathbb{H} \leq \mathbb{G}$,

$$\mathbb{H}^\perp = \big\{ g \in G \mid \mu(g, h) = 1 \big\},$$
$$|\mathbb{H}^\perp| = [\mathbb{G} : \mathbb{H}] = |\mathbb{G}|/|\mathbb{H}|, \qquad (\mathbb{H}^\perp)^\perp = \mathbb{H}.$$

Lemma 1. $\displaystyle\sum_{h \in H} \mu(g, h) = \begin{cases} |\mathbb{H}| & \text{if } g \in H^\perp, \\ 0 & \text{otherwise.} \end{cases}$

Proof. For $\lambda \in \mathbb{C}^*$ define

$$H_\lambda = \big\{ h \in H \mid \mu(g, h) = \lambda \big\} \qquad \text{and} \qquad L = \big\{ \lambda \mid H_\lambda \neq \emptyset \big\}.$$

Observe that $H_1 = H^\perp$ and if $h \in H_\lambda$ then $H_\lambda = h + H_1$. It follows that all non-empty H_λ are cosets and hence of the same size, say P.

The set L is closed under multiplication and is hence a subgroup of $\mathbb{C}^*$. Since L is finite it is cyclic (elements are roots of unity — the generator is the root of unity or order equal to the least common multiple). Therefore

$$\sum_{h \in H} \mu(g, h) = \sum_{\lambda \in L} P\lambda = P \sum_{k=1}^{|L|} \nu^k$$

where ν is the generator of L. If $|L| > 1$ then this sum is 0. If $|L| = 1$ then $L = \{1\}$. The lemma follows. □

Date: April 27, 2020.

For $A \subseteq G$, define the quantum state

$$|A\rangle = \frac{1}{\sqrt{|A|}} \sum_{a \in A} |a\rangle .$$

Define the operators

$$\begin{aligned}
\mathcal{F}_{\mathbb{G}} &= \frac{1}{\sqrt{|\mathbb{G}|}} \sum_{g,h \in G} \mu(g,h) \, |g\rangle \langle h| && \text{(the } \textit{quantum Fourier transform} \text{ for } \mathbb{G}\text{)}, \\
\tau_t &= \sum_{g \in G} |t+g\rangle \langle g| && \text{(the } \textit{translation operator for } t \in G\text{)}, \\
\varphi_t &= \sum_{g \in G} \mu(t,g) \, |g\rangle \langle g| && \text{(the } \textit{phase-change operator for } t \in G\text{)}.
\end{aligned}$$

Theorem 2.

(1) $\mathcal{F}_{\mathbb{G}} |H\rangle = \left|H^{\perp}\right\rangle$ *for a subgroup* $\mathbb{H} \leq \mathbb{G}$,

(2) $\mu(s,t)\tau_t\varphi_s = \varphi_s\tau_t$ *for* $s,t \in G$,

(3) $\mathcal{F}_{\mathbb{G}}\varphi_s = \tau_{-s}\mathcal{F}_{\mathbb{G}}$ *for* $s \in G$,

(4) $\mathcal{F}_{\mathbb{G}}\tau_s = \varphi_s\mathcal{F}_{\mathbb{G}}$ *for* $s \in G$.

Proof. **(1):** We have

$$\begin{aligned}
\mathcal{F}_{\mathbb{G}} |H\rangle &= \left(\frac{1}{\sqrt{|\mathbb{G}|}} \sum_{g,h \in G} \mu(g,h) \, |g\rangle \langle h| \right) |H\rangle = \frac{1}{\sqrt{|\mathbb{G}||\mathbb{H}|}} \sum_{\substack{g \in G \\ h \in H}} \mu(g,h) \, |g\rangle \\
&= \frac{1}{\sqrt{|\mathbb{G}||\mathbb{H}|}} \sum_{g \in G} \left(\sum_{h \in H} \mu(g,h) \right) |g\rangle = \frac{1}{\sqrt{|\mathbb{G}||\mathbb{H}|}} \sum_{g \in H^{\perp}} |\mathbb{H}| \, |g\rangle \\
&= \frac{1}{\sqrt{|\mathbb{H}^{\perp}|}} \sum_{g \in H^{\perp}} |g\rangle = \left|H^{\perp}\right\rangle ,
\end{aligned}$$

where Lemma 1 is applied at the fourth equality.

(2): We have

$$\begin{aligned}
\mu(s,t)\tau_t\varphi_s &= \mu(s,t) \left(\sum_{g \in G} |t+g\rangle \langle g| \right) \left(\sum_{g \in G} \mu(s,g) \, |g\rangle \langle g| \right) \\
&= \sum_{g \in G} \mu(s,t+g) \, |t+g\rangle \langle g| \\
&= \left(\sum_{g \in G} \mu(s,t+g) \, |t+g\rangle \langle t+g| \right) \left(\sum_{g \in G} |t+g\rangle \langle g| \right) \\
&= \left(\sum_{g \in G} \mu(s,g) \, |g\rangle \langle g| \right) \left(\sum_{g \in G} |t+g\rangle \langle g| \right) = \varphi_s\tau_t.
\end{aligned}$$

(3): We have

$$\begin{aligned}\mathcal{F}_{\mathbb{G}}\varphi_s &= \left(\frac{1}{\sqrt{|\mathbb{G}|}}\sum_{g,h\in G}\mu(g,h)\,|g\rangle\,\langle h|\right)\left(\sum_{g\in G}\mu(g,s)\,|g\rangle\,\langle g|\right)\\ &= \frac{1}{\sqrt{|\mathbb{G}|}}\sum_{g,h\in G}\mu(g+s,h)\,|g\rangle\,\langle h| = \frac{1}{\sqrt{|\mathbb{G}|}}\sum_{g,h\in G}\mu(g,h)\,|g-s\rangle\,\langle h|\\ &= \left(\sum_{g\in G}|g-s\rangle\,\langle g|\right)\left(\frac{1}{\sqrt{|\mathbb{G}|}}\sum_{g,h\in G}\mu(g,h)\,|g\rangle\,\langle h|\right) = \tau_{-s}\mathcal{F}_{\mathbb{G}}.\end{aligned}$$

(4): We have

$$\begin{aligned}\mathcal{F}_{\mathbb{G}}\tau_s &= \left(\frac{1}{\sqrt{|\mathbb{G}|}}\sum_{g,h\in G}\mu(g,h)\,|g\rangle\,\langle h|\right)\left(\sum_{g\in G}|g+s\rangle\,|g\rangle\right)\\ &= \frac{1}{\sqrt{|\mathbb{G}|}}\sum_{g,h\in G}\mu(g,h+s)\,|g\rangle\,\langle h| = \frac{1}{\sqrt{|\mathbb{G}|}}\sum_{g,h\in G}\mu(g,h)\mu(g,s)\,|g\rangle\,\langle h|\\ &= \left(\sum_{g\in G}\mu(g,s)\,|g\rangle\,\langle g|\right)\left(\frac{1}{\sqrt{|\mathbb{G}|}}\sum_{g,h\in G}\mu(g,h)\,|g\rangle\,\langle h|\right) = \varphi_s\mathcal{F}_{\mathbb{G}}.\end{aligned}$$

□

Define the operator

$$\mathcal{HSP}_{\mathbb{G},f} = (\mathcal{F}_{\mathbb{G}}\otimes I)\circ\widehat{f}\circ(\mathcal{F}_{\mathbb{G}}^{-1}\otimes I),$$

where $\widehat{f}$ is the unitary form of the blackbox function f, defined by

$$\widehat{f}\,|x,y\rangle = |x, f(x)+y\rangle\,.$$

Theorem 3. *Let $\mathcal{M}_1$ be the measurement operator for the first register and define a distribution*

$$(z) = \mathcal{M}_1\circ\mathcal{HSP}_{\mathbb{G},f}\,|0,0\rangle\,,$$

where the first register contains group elements (with $0\in G$ as the identity) and the second register contains elements of X (regarded as a subset of $\{0,\ldots,|G|-1\}$). Then (z) is a uniform distribution over $\mathbb{H}^{\perp}$, where $\mathbb{H}$ is the hidden subgroup.

Proof. Fix a transversal T of $\mathbb{H}$ in $\mathbb{G}$ and note that $|T| = |\mathbb{G}|/|\mathbb{H}| = |\mathbb{H}^{\perp}|$. We have

$$\begin{aligned}\mathcal{HSP}_{\mathbb{G},f}\,|0,0\rangle &= (\mathcal{F}_{\mathbb{G}}\otimes I)\circ\widehat{f}\circ(\mathcal{F}_{\mathbb{G}}^{-1}\otimes I)\,|0,0\rangle = (\mathcal{F}_{\mathbb{G}}\otimes I)\circ\widehat{f}\;\;|G\rangle\otimes|0\rangle\\ &= (\mathcal{F}_{\mathbb{G}}\otimes I)\frac{1}{\sqrt{|\mathbb{G}|}}\sum_{g\in G}|g,f(g)\rangle = (\mathcal{F}_{\mathbb{G}}\otimes I)\frac{1}{\sqrt{|T|}}\sum_{t\in T}\frac{1}{\sqrt{|\mathbb{H}|}}\sum_{h\in H}|t+h,f(t)\rangle\\ &= (\mathcal{F}_{\mathbb{G}}\otimes I)\frac{1}{\sqrt{|\mathbb{H}^{\perp}|}}\sum_{t\in T}\tau_t\,|H\rangle\otimes|f(t)\rangle = \frac{1}{\sqrt{|\mathbb{H}^{\perp}|}}\sum_{t\in T}\mathcal{F}_{\mathbb{G}}\tau_t\,|H\rangle\otimes|f(t)\rangle\\ &= \frac{1}{\sqrt{|\mathbb{H}^{\perp}|}}\sum_{t\in T}\varphi_t\mathcal{F}_{\mathbb{G}}\,|H\rangle\otimes|f(t)\rangle = \frac{1}{\sqrt{|\mathbb{H}^{\perp}|}}\sum_{t\in T}\varphi_t\left|H^{\perp}\right\rangle\otimes|f(t)\rangle\end{aligned}$$

(Theorem 2 is used in equalities 2, 7,and 8). The operator φ_t is a phase shift and therefore has no effect on the probability of measurement. It follows that the first register is a uniform distribution on $\mathbb{H}^{\perp}$, as claimed. □