Quantum Computation

Lecture 18

Hidden-subgroup problem
**Period finding**

Function \( f : \{0,1\}^L \rightarrow \{0,1\}^L \), \( f(z+r) = f(z) \)

\[
\begin{array}{c}
|0\rangle^L \otimes |0\rangle^L \rightarrow \frac{1}{2^{|z|/2}} \sum_{z=0}^{2^{|z|/2}} |z\rangle |f(z)\rangle \\
\rightarrow \frac{1}{2^{|z|/2}} \sum_{z=0}^{2^{|z|/2}} \left( \frac{1}{2^{|z|/2}} \sum_{z} e^{2\pi i z s/|y|} |z\rangle \right) |u_s\rangle \\
\text{or}
\end{array}
\]

measure L small qubits in standard basis

quantum parallelism

near-momentum eigenstate with \( q_s = s/|y| \)

unnormalized

In the momentum basis the state is concentrated near momenta \( s/|y| \).

**Hidden-subgroup problem**

finite group \( G \)

\( \text{cosets of } H \)

\( \text{subgroup } H \)

\( a_i H \)

\( f \) is constant and distinct on cosets:

\[ f(gh) = f(g), \quad \forall \ h \in H \]

\[ f(a_i h) = f_j, \quad f_j \neq f_k \text{ if } j \neq k \]

**Task:** Given a black box that evaluates \( f \), find \( H \), i.e.,

find a set of generators for \( H \).

\[ U_f |g \rangle |x\rangle = |g\rangle |x \oplus f(g)\rangle \]
$|0^\oplus\rangle \otimes |0^\ominus\rangle \rightarrow \frac{1}{\sqrt{|G|}} \sum_g |g\rangle |f(g)\rangle$

\begin{align*}
\text{measure ancilla} & \rightarrow \frac{1}{\sqrt{|H|}} \sum_{g \in G|H} |g\rangle \\
\text{equal superposition of members of one coset} & \rightarrow \text{Abelian groups}
\end{align*}

There are $N = |G|$ irreps, all 1D. It is useful to label the irreps with the same symbols as the group elements.

$\chi_{gg'} = \begin{pmatrix} \text{character of } g' \end{pmatrix} = \chi(\bar{p}_g(g')) = \bar{p}_g(g') = \begin{pmatrix} \text{root of} \end{pmatrix}$

$f: G \rightarrow \mathbb{C}$

\[ \hat{f}(g) = \frac{1}{\sqrt{N}} \sum_{g \in G} f(g') p_g(g') = \frac{1}{\sqrt{N}} \sum_{g \in G} f(g') \chi_{gg'} \]

\[ f(g) = \frac{1}{\sqrt{N}} \sum_{g \in G} \chi(\hat{f}(g) p_g(g^{-1})) = \frac{1}{\sqrt{N}} \sum_{g \in G} \hat{f}(g) \chi_{gg}^* \]

Orthogonality and completeness:

1. $\sum_{g \in G} \chi_{gg'} = \delta_{ge} \Rightarrow \sum_{g \in G} \chi_{gg'} \chi_{gg''} = \sum_{g \in G} \chi_{g,g'g''} = \delta_{g',g''}$

2. $\sum_{g \in G} p_g(g') \bar{p}_g(g) = \sum_{g \in G} \chi_{gg}^* \chi_{gg} = \delta_{g',g''}$
Group Fourier transform

\( G, \quad |G| = N, \quad f: G \to \mathbb{C} \)

\[ \rho(g) \text{ is the } d_p \times d_p \text{ matrix that represents } g \text{ in irrep } \rho. \]

dimension \( d_p \)

F.T. \( \hat{f}: G \to \text{matrices} \)

\[ \hat{f}(\rho) = \sqrt{\frac{d_p}{N}} \sum_{g \in G} f(g) \rho(g) \]

\[ f(g) = \frac{1}{\sqrt{N}} \sum_{\rho \in \hat{G}} \sqrt{d_p} \text{ tr}(\hat{f}(\rho) \rho(g')) \]

These are related by orthogonality and completeness relations:

1. \( \sum_{\rho \in \hat{G}} d_p \chi_{\rho}(g) = N \delta_{ge} \quad \Rightarrow \quad g = e: \quad \sum_{\rho \in \hat{G}} d_p^2 = N \)

   \( \chi_{\rho}(g) = \text{tr}(\rho(g)) = (\text{character of } g) \quad \text{in irrep } \rho \)

2. \( \sum_{g \in G} \text{tr}(A \rho'(g')) \rho(g) = \frac{N}{d_p} A \delta_{pp'} \)

\[ \frac{1}{N} \sum_{\rho \in \hat{G}} \text{tr}(\hat{f}(\rho) \rho(g')) = \frac{1}{N} \sum_{\rho' \in \hat{G}} f(g') \sum_{\rho \in \hat{G}} d_p \text{ tr}(\rho(g') \rho(g')) = \sum_{\rho \in \hat{G}} \text{tr}(\rho(g'g)) = \chi_{\rho}(g'g) \]

\[ = N \delta_{g'g} \delta_{e,e} = N \delta_{g'g} \]

\[ = f(g) \]
Examples:

1. $Z_N$ with addition mod $N$: \[ X_{ijk} = \frac{1}{\sqrt{N}} e^{-2\pi i jk/N} \] group element

2. $Z_2$ with addition mod 2: \[ X_{ab} = \frac{1}{\sqrt{2}} e^{-\pi i ab} = \frac{1}{\sqrt{2}} (-1)^{ab} \] (Hadamard)

3. $Z_2 \times Z_2 \times \ldots \times Z_2$ with bitwise addition mod 2:

   \[ X_{xy} = \frac{1}{2^n} \sum_{a=0}^{n-1} (-1)^{a} X_{a} \rightarrow X_{xy} = X_{x_1 y_1} \oplus X_{x_2 y_2} \oplus \ldots \oplus X_{x_n y_n} \]

4. $Z_{N_1} \times Z_{N_2}$ with systemwise addition mod $N_1$ and mod $N_2$:

   \[ X_{ij,ka} = \frac{1}{\sqrt{N_1 N_2}} \sum_{j,k} e^{-2\pi i (j k_1 / N_1 + j k_2 / N_2)} \]

   $N_1 = 6$  $N_2 = 3$

   \[ g_j \rightarrow \begin{array}{c}
   0 \ 1 \ 2 \\
   3 \ 4 \ 5 \\
   6 \end{array} \]

   Generally, each $g \in G$ generates a cyclic subgroup

   \[ C(g) = \{ g^k \mid k = 0, \ldots, |C(g)|-1 \} = Z_{N_g}, \quad gN_g = e \]

   $G$ itself can always be generated by a set of independent generators $g_1, \ldots, g_n$:

   \[ G = \{ g_1^{k_1} \ldots g_n^{k_n} \mid k_1 = 0, \ldots, N_1-1, \ldots, k_n = 0, \ldots, N_n-1 \} = Z_{N_1} \times \ldots \times Z_{N_n} \]

   \[ g = g_1^{k_1} \ldots g_n^{k_n} \rightarrow k_1, \ldots, k_n \equiv \mathbb{Z}, \quad N = N_1 \ldots N_n \quad n = O(\log N) \]

   \[ X_{gg'} = X_{g_1^{k_1} \ldots g_n^{k_n} g_1^{l_1} \ldots g_n^{l_n}} = \exp \left( -2\pi i \sum_{j=1}^{n} k_j l_j / N_j \right) = e^{-2\pi i \sum_{j=1}^{n} k_j l_j / N} = X_{g g'} \]
Digression:

<table>
<thead>
<tr>
<th>$Z_2 \times Z_2$</th>
<th>$00$</th>
<th>$01$</th>
<th>$10$</th>
<th>$11$</th>
<th>$Z_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$00$</td>
<td>$00$</td>
<td>$01$</td>
<td>$10$</td>
<td>$11$</td>
<td>$0$</td>
</tr>
<tr>
<td>$01$</td>
<td>$01$</td>
<td>$00$</td>
<td>$11$</td>
<td>$10$</td>
<td>$1$</td>
</tr>
<tr>
<td>$10$</td>
<td>$10$</td>
<td>$11$</td>
<td>$00$</td>
<td>$01$</td>
<td>$2$</td>
</tr>
<tr>
<td>$11$</td>
<td>$11$</td>
<td>$10$</td>
<td>$01$</td>
<td>$00$</td>
<td>$3$</td>
</tr>
</tbody>
</table>

* $Z_6 \times Z_3 \neq Z_{18}$, $Z_9 \times Z_2 = Z_{18}$

↑

decomposition into direct product of cyclic groups is not unique.

* $Z_{N_1} \times Z_{N_2} = Z_{N_1 N_2 / \gcd(N_1, N_2)} \times Z_{\gcd(N_1, N_2)}$

$Z_6 \times Z_5 \times Z_2 = Z_{10} \times Z_6 = Z_{30} \times Z_2$

* Standard form: $Z_{N_1} \times Z_{N_2} \times \cdots \times Z_{N_n}$, $N_1 \geq N_2 \geq \cdots \geq N_n$, $N_j$ is a factor of $N_k$ for $k < j$.

$\left( k_2 \mod N_2 \right) (k_1 \mod N_1) \leftrightarrow \left( k_2 \mod \gcd \right) \left( k_1 + N_j k_2 \mod \left( \frac{N_j N_2}{\gcd} \right) \right)$
Any subgroup $H$ has its own generators $h_1, \ldots, h_m$, $m = O(\log N)$, each of which, when written in terms of the generators of $G$, corresponds to a string:

$$h_j = g_1^{e_{1j}} \cdots g_m^{e_{mj}} \iff \lambda_{ij} = \lambda_j$$

To say that a function is constant on cosets of $h$ is to say that for all $g \in G$,

$$f(gh) = f(g), \ \forall h \in H \iff f(gh_j) = f(g), \ j = 1, \ldots, m$$

$$\iff f(K_\lambda \lambda_j) = f(K_\lambda), \ j = 1, \ldots, m$$

periodicity under "displacement" $\lambda_j$

So we end up in the abelian case, looking for a number of periodicities $= o(\log N)$, and we have an appropriate FT to do the looking. Once we've found one periodicity, we can eliminate it from $G$ and look for another.

F.T. $F |g\rangle = \sum_{g'} X_{gg'} |g'\rangle \iff F |K_\lambda\rangle = \sum_{\chi} X_{\chi \lambda} |\chi\rangle$

$$= \sum_{\chi} e^{2\pi i \chi K_\lambda \lambda} |\chi\rangle$$