Quantum Computation

Lecture 18

Hidden-subgroup problem

Period finding

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

find this period

$$|0\rangle^{\otimes t}|0\rangle^{\otimes L} \longrightarrow \frac{1}{2^{t/2}} \sum_{z=0}^{2^t-1} |z\rangle|f(z)\rangle$$

$\longleftrightarrow$ quantum parallelism

$$\longrightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \underbrace{\left(\frac{1}{2^{t/2}} \sum_z e^{2\pi i z(s/r)} |z\rangle \right)}_{\text{near-momentum eigenstate with } p_\phi = s/r} |u_s\rangle$$

or

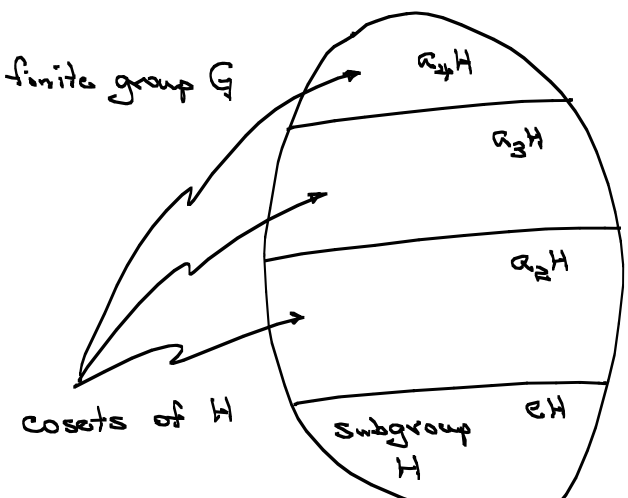
$$\longrightarrow \frac{1}{2^{t/2}} \sum_{\{z \mid f(z)=f_j\}} |z\rangle$$

$\longleftarrow$ unnormalized

measure L ancilla qubits in standard basis

In the momentum basis the state is concentrated near momenta s/r.

Hidden-subgroup problem



Function $f: G \to X$

finite set w/ binary operation $\oplus$

f is <u>constant</u> and <u>distinct</u> on cosets:

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

$$f(a_j h) = f_j, \quad f_j \neq f_k \text{ if } j \neq k$$

<u>Task</u>: Given a $\boxed{\text{black box that evaluates } f,}$ find H, i.e., find a set of generators for H.

$$U_f|g\rangle|x\rangle = |g\rangle|x \oplus f(g)\rangle$$

$$|0\rangle^{\otimes t}\,|0\rangle^{\otimes L} \longrightarrow \frac{1}{\sqrt{|G|}}\sum_{g} |g\rangle\,|f(g)\rangle$$

$$\xrightarrow[\text{ancilla}]{\text{measure}} \frac{1}{\sqrt{|H|}}\sum_{g\in a_j H} |g\rangle \longleftarrow \text{equal superposition of members of one coset}$$

?

Abelian groups

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

$$\chi_{gg'} = \begin{pmatrix}\text{character of } g' \\ \text{in irrep } g\end{pmatrix} = \mathrm{tr}\left(\rho_g(g')\right) = \rho_g(g') = \begin{pmatrix}\text{root of} \\ \text{unity}\end{pmatrix}$$

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

$$\chi_{gg'}\chi_{gg''} = \chi_{g,g'g''}$$

F.T. $$\hat{f}(g) = \frac{1}{\sqrt{N}}\sum_{g'\in G} f(g')\,\rho_g(g') = \frac{1}{\sqrt{N}}\sum_{g'\in G} f(g')\,\chi_{gg'}$$

$$f(g') = \frac{1}{\sqrt{N}}\sum_{g\in G} \mathrm{tr}\left(\hat{f}(g)\,\rho_g(g'^{-1})\right) = \frac{1}{\sqrt{N}}\sum_{g\in G} \hat{f}(g)\,\chi^*_{gg'}$$

Orthogonality and completeness:

① $$\sum_{g\in G}\chi_{gg'} = \delta_{g'e} \Rightarrow \sum_{g\in G}\chi_{gg'}\chi^*_{gg''} = \sum_{g\in G}\chi_{g,g'g''^{-1}} = \delta_{g',g''}$$

② $$\sum_{g\in G}\rho_{g'}(g^{-1})\,\rho_{g''}(g) = \sum_{g\in G}\chi^*_{g'g}\,\chi_{g''g} = \delta_{g',g''}$$

Group Fourier transform

G, $|G| = N$, $f: G \to \mathbb{C}$

$\uparrow$

unitary irreps $\rho \in \hat{G}$

$\downarrow$

dimension d_ρ

$\rho(g)$ is the $d_\rho \times d_\rho$ matrix that represents g in irrep ρ.

F.T. $\hat{f}: \hat{G} \longrightarrow$ matrices

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{N}} \sum_{g \in G} f(g)\rho(g)$$

$$f(g) = \frac{1}{\sqrt{N}} \sum_{\rho \in \hat{G}} \sqrt{d_\rho}\, \mathrm{tr}\left(\hat{f}(\rho)\rho(g^{-1})\right)$$

These are related by orthogonality and completeness relations:

① $$\sum_{\rho \in \hat{G}} d_\rho \chi_\rho(g) = N \delta_{ge} \Longrightarrow g = e: \sum_{\rho \in \hat{G}} d_\rho^2 = N$$

$$\chi_\rho(g) = \mathrm{tr}(\rho(g)) = \begin{pmatrix} \text{character of } g \\ \text{in irrep } \rho \end{pmatrix}$$

② $$\sum_{g \in G} \mathrm{tr}\left(A \rho'(g^{-1})\right)\rho(g) = \frac{N}{d_\rho} A\, \delta_{\rho\rho'}$$

$$\frac{1}{\sqrt{N}} \sum_{\rho \in \hat{G}} \sqrt{d_\rho}\, \mathrm{tr}\left(\hat{f}(\rho)\rho(g^{-1})\right) = \frac{1}{N} \sum_{g' \in G} f(g') \underbrace{\sum_{\rho \in \hat{G}} d_\rho \underbrace{\mathrm{tr}\left(\rho(g')\rho(g^{-1})\right)}_{= \mathrm{tr}(\rho(g'g^{-1})) = \chi_\rho(g'g^{-1})}}_{\text{①}\ = N\delta_{g'g^{-1},e} = N\delta_{g',g}}$$

$$= f(g) \quad \checkmark$$

B

$$\sqrt{\frac{d_\rho}{N}} \sum_{g\in G} f(\rho)\,\rho(g) = \frac{\sqrt{d_\rho}}{N} \sum_{\rho'\in\hat{G}} \sqrt{d_{\rho'}}\, \underbrace{\sum_{g\in G} \mathrm{tr}\left(\hat{f}(\rho')\,\rho'(g^{-1})\right)\rho(g)}_{\frac{N}{d_\rho}\hat{f}(\rho')\,\delta_{\rho\rho'}}$$

$$= \hat{f}(\rho) \quad \checkmark$$

Examples:

① $\mathbb{Z}_N$ with addition mod N: $\chi_{jk} = \frac{1}{\sqrt{N}} e^{-2\pi i jk/N}$

j: rep, k: group element

② $\mathbb{Z}_2$ with addition mod 2: $\chi_{ab} = \frac{1}{\sqrt{2}} e^{-2\pi i ab/2} = \frac{1}{\sqrt{2}} (-1)^{ab}$ (Hadamard)

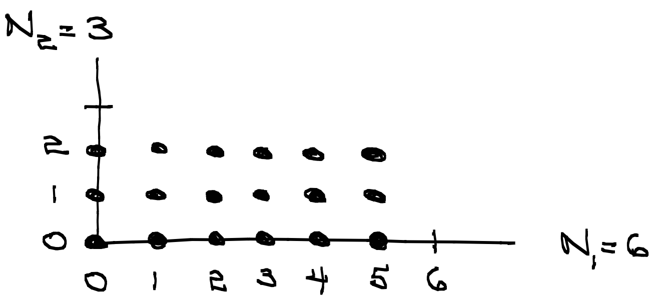
③ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ with bitwise addition mod 2:

$$\chi_{xy} = \frac{1}{2^{n/2}} (-1)^{x\cdot y}, \qquad x\cdot y \longrightarrow x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n$$

④ $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$ with systemwise addition mod N_1 and mod N_2

$$\chi_{j_1j_2,k_1k_2} = \frac{1}{\sqrt{N_1N_2}} e^{-2\pi i (j_1k_1/N_1 + j_2k_2/N_2)}$$

$\longleftarrow$ 2D discrete FT with different periodicites in the two dimensions



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

$$C(g) = \{ g^k \mid k = 0, \ldots, \underbrace{|C(g)|}_{N_g} - 1 \} = \mathbb{Z}_{N_g}, \quad g^{N_g} = e$$

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

$$G = \{ g_1^{k_1} \cdots g_n^{k_n} \mid k_1 = 0, \ldots, N_1 - 1, \ldots, k_n = 0, \ldots, N_n - 1 \} = \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_n}$$

$$g = g_1^{k_1} \cdots g_n^{k_n} \longleftrightarrow k_1 \ldots k_n \equiv \kappa, \qquad N = N_1 \cdots N_n \qquad n = O(\log N)$$

$$\chi_{gg'} = \chi_{k_1\ldots k_n, l_1 \ldots l_m} = \exp\left(-2\pi i \sum_{j=1}^{n} k_j l_j / N_l\right) = e^{-2\pi i \kappa\cdot\lambda} = \chi_{\kappa\lambda}$$

Digression:

① $\mathbb{Z}_2 \times \mathbb{Z}_2 \neq \mathbb{Z}_4$

$\mathbb{Z}_2\times\mathbb{Z}_2$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

$\mathbb{Z}_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

② $\mathbb{Z}_6 \times \mathbb{Z}_3 \neq \mathbb{Z}_{18}$, $\quad \mathbb{Z}_9 \times \mathbb{Z}_2 = \mathbb{Z}_{18}$

↑ decomposition into direct product of cyclic groups is not unique.

③ $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} = \mathbb{Z}_{N_1 N_2/\gcd(N_1,N_2)} \times \mathbb{Z}_{\gcd(N_1,N_2)}$

$$\mathbb{Z}_6 \times \mathbb{Z}_5 \times \mathbb{Z}_2 = \mathbb{Z}_{10} \times \mathbb{Z}_6 = \mathbb{Z}_{30} \times \mathbb{Z}_2$$

④ Standard form: $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_n}$, $\quad N_1 \geq N_2 \geq \ldots \geq N_n$, $\quad N_j$ is a factor of N_k for $k<j$.

$$(k_2 \bmod N_2)(k_1 \bmod N_1) \longleftrightarrow (k_2 \bmod \gcd)\left((k_1 + N_1 k_2) \bmod \left(\frac{N_1 N_2}{\gcd}\right)\right)$$

Any subgroup H has its own generators $h_1, \dots, h_m$, $m = O(\log N)$, each of which, when written in terms of the generators of g, corresponds to a string:

$$h_j = g_1^{\ell_{j1}} \cdots g_n^{\ell_{jn}} \Longleftrightarrow \ell_{j1} \dots \ell_{jn} \equiv \lambda_j$$

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

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

$$\Leftrightarrow f(\mathcal{K} \oplus \lambda_j) = f(\mathcal{K}), \ j = 1, \dots, m$$

periodicity under "displacement" λ_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. $$F|g\rangle = \sum_{g'} \chi^*_{gg'} |g'\rangle \Longleftrightarrow F|\mathcal{K}\rangle = \sum_{\lambda} \chi^*_{\mathcal{K}\lambda} |\lambda\rangle$$

$$= \sum_{\lambda} e^{+2\pi i \mathcal{K} \cdot \lambda} |\lambda\rangle$$