Hidden Subgroup Minicourse - Abelian HSP

Gábor Ivanyos
MTA SZTAKI & TU/e

CWI Amsterdam, October 30 - November 3, 2006

Contents

1. Abelian Fourier sampling
   - The HSP
   - Coset states
   - Abelian Fourier sampling
   - Abelian Fourier sampling without measurements
   - Application: small commutator subgroup
2. Reduction to smaller groups
   - Reduction scheme
   - Function value superposition
   - Hidden shift problem

HSP - the hidden subgroup problem

- G finite group
- $f : G \to \{\text{objects}\}$ **hides** the subgroup $H \leq G$, if

  $f(x) = f(y) \Leftrightarrow xH = yH$

  i.e., x and y are in the same left coset of H.
  - In words, f is constant on the left cosets of H and takes different values on different cosets.
- f is provided by an oracle (or an efficient algorithm) performing $|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$
- Task: find (generators for) H.
- Examples:

  Order $G = \mathbb{Z}_n$, $f(k) = u^k$ $H = Z_{n/m}$, where m is the order of u.

  Discrete log $G = Z_n \times Z_n$, $f(k,\ell) = u^k v^{-\ell}$, $H = \{(k,\ell) | u^k = v^\ell\}$.

Coset states 1

$$
\begin{aligned}
|1_G\rangle|0..0\rangle &\rightarrow \text{(usually easy)} \\
\frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle|0..0\rangle &\rightarrow \text{(f-oracle)} \\
\frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle|f(x)\rangle &= \\
\frac{1}{\sqrt{|G|}}\sum_{s}\sum_{\substack{x\in G\\ f(x)=s}}|x\rangle|s\rangle &= \frac{1}{\sqrt{|G|}}\sum_{a\in T}\sum_{x\in H}|ax\rangle|f(a)\rangle
\end{aligned}
$$

T: left transversal of H: a set of left coset representatives by H

Coset states 2

$$\frac{1}{\sqrt{|G|}}\sum_{a\in T}\sum_{x\in H}|ax\rangle|f(a)\rangle =$$

$$\frac{1}{\sqrt{|G:H|}}\sum_{a\in T}\left(\frac{1}{\sqrt{|H|}}\sum_{x\in H}|ax\rangle\right)|f(a)\rangle$$ measure/ignore $f \to$

coset state $|aH\rangle := \frac{1}{\sqrt{|H|}}\sum_{x\in H}|ax\rangle$ with random $a \in T$

or $\frac{1}{|G:H|}\sum_{a\in T}|aH\rangle\langle aH|$ mixed state,

the hidden subgroup state

Coset states

Coset state (with random $a \in T$ (random $a \in G$)

$$|aH\rangle = \frac{1}{\sqrt{|H|}} \sum_{x \in H} |ax\rangle$$

or

Hidden subgroup state: mixed state with density matrix

$$\frac{1}{|G:H|} \sum_{a \in T} |aH\rangle\langle aH|$$

$$= \frac{1}{|G|} \sum_{g \in G} |gH\rangle\langle gH|$$

Abelian Fourier sampling 1.

$$\frac{1}{\sqrt{|H|}}\sum_{x\in H}|ax\rangle \quad \rightarrow$$

$$\frac{1}{\sqrt{|H|}}\sum_{x\in H}\frac{1}{\sqrt{|G|}}\sum_{\chi\in\hat{G}}\chi(ax)|\chi\rangle \quad =$$

$$\frac{1}{\sqrt{|G|}}\sum_{\chi\in\hat{G}}\left(\chi(a)\frac{1}{\sqrt{|H|}}\sum_{x\in H}\chi(x)\right)|\chi\rangle$$

Abelian Fourier sampling 2.

Coefficient of χ

$$\frac{\chi(a)}{\sqrt{|G:H|}}\frac{1}{|H|}\sum_{x\in H}\chi(x) = \begin{cases} \frac{\chi(a)}{\sqrt{|G:H|}} & \text{if } \chi_H = 1, \\ 0 & \text{otherwise.} \end{cases}$$

orthogonality of 1_H and χ_H

$$\frac{1}{|H|}\sum_{x\in H}\chi(x) = \begin{cases} 1 & \text{if } \chi_H = 1, \\ 0 & \text{otherwise} \end{cases}$$

Probability of χ:

$$\begin{cases} \frac{1}{|G:H|} & \text{if } \chi \in H^{\perp}, \\ 0 & \text{otherwise.} \end{cases}$$

Computing H

- $H^\perp = \{\chi \in \hat{G} \mid \chi_H = 1\}$ subgroup of $\hat{G}$.
- generating set Γ of $H^\perp$ collected expectedly in $O(\log |G|)$ repetitions.
- $H = \{x \in G \mid \chi(x) = 1 \text{ for every } \chi \in \Gamma\}$. (Solving a system of homogeneous linear congruences.)

Irreps of abelian groups

$$G = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} = \{\underline{z} = (z_1, \ldots, z_r) \mid z_i \bmod m_i \}$$

$$m = LCM(m_1, \ldots, m_r), \ \ \omega = \sqrt[m]{1} (= e^{2\pi i/m})$$

$$\hat{G} = \{\chi_{\underline{u}} \mid \underline{u} \in G\}$$

$$\chi_{\underline{u}}(\underline{z}) = \omega^{\sum_{i=1}^{r} \frac{m}{m_i} u_i z_i} = \omega^{\underline{u} \cdot \underline{z}}$$

$$\underline{u} \cdot \underline{z} = \sum_{i=1}^{r} \frac{m}{m_i} u_i z_i \bmod m$$

System of congruences

$$\underline{z} \in H$$

$$\Updownarrow$$

$$\underline{z} \cdot \underline{u} \equiv 0 \text{ mod } m \text{ for every } u \text{ s.t. } \chi_u \in H^\perp$$

$$\Updownarrow$$

$$\underline{z} \cdot \underline{u} \equiv 0 \text{ mod } m \text{ for every } u \text{ s.t. } \chi_u \in \Gamma$$

(if Γ generates $H^\perp$)

Abelian Fourier sampling - without measurement 1.

$$\frac{1}{\sqrt{|G:H|}}\sum_{a\in T}\frac{1}{\sqrt{|H|}}\sum_{x\in H}|ax\rangle|f(a)\rangle \quad \rightarrow$$

$$\frac{1}{\sqrt{|G:H|}}\sum_{a\in T}\frac{1}{\sqrt{|H|}}\sum_{x\in H}\frac{1}{\sqrt{|G|}}\sum_{\chi\in\hat{G}}\chi(ax)|\chi\rangle|f(a)\rangle \quad =$$

$$\frac{1}{\sqrt{|G:H|}}\sum_{a\in T}\frac{1}{\sqrt{|G|}}\sum_{\chi\in\hat{G}}\left(\chi(a)\frac{1}{\sqrt{|H|}}\sum_{x\in H}\chi(x)\right)|\chi\rangle|f(a)\rangle$$

Abelian Fourier sampling - without measurement 2.

Coefficient of $|\chi\rangle|f(a)\rangle$

$$\frac{1}{\sqrt{|G:H|}}\frac{\chi(a)}{\sqrt{|G:H|}}\frac{1}{|H|}\sum_{x\in H}\chi(x) = \begin{cases} \frac{\chi(a)}{|G:H|} & \text{if } \chi_H = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Probability of $|\chi\rangle|f(a)\rangle$

$$\begin{cases} \frac{1}{|G:H|^2} & \text{if } \chi \in H^{\perp}, \\ 0 & \text{otherwise.} \end{cases}$$

Remarks on Abelian Fourier Sampling

- No need of measuring the value of f
- f can be quantum-state valued.

  $f : G \rightarrow \mathbb{C}^X$ hides H if:
  - f constant on left cosets of H
  - $f(a) \perp f(b)$ if $aH \neq bH$
- Fourier sampling finds H efficiently if G is abelian and f hides H.
- Even the function f can be different in different steps, only they must hide the same H.

Application: small G'

- Assume $f : G \rightarrow \mathbb{C}^X$ hides H
- New function F on G:

$$|F(x)\rangle = \frac{1}{\sqrt{|G'|}} \sum_{y \in G'} |f(xy)\rangle.$$

- Implement $|x\rangle \rightarrow |x\rangle|F(x)\rangle$:
  $G' = \{y_1, \ldots, y_m\}$.
  - $|x\rangle|$lex. sorted list of $f(xy_1), \ldots f(xy_m)\rangle \rightarrow$
  - $\frac{1}{\sqrt{m}}|x\rangle|f(xy_1)\rangle + \ldots + |f(xy_m)\rangle$

  Cost: $O(m \log m \cdot cost(f))$

Small G' 2.

- $|F(x)\rangle = \frac{1}{\sqrt{|G'|}} \sum_{y \in G'} |f(xy)\rangle$.
- F hides the subgroup HG'.
- F defines a function $\overline{F}$ on G/G'.
  ($\overline{F}(\overline{x}) = F(x)$, $x \in \overline{x}$ arbitrary.)
- Fourier sampling on G/G' finds generators $\overline{x_1}, \ldots, \overline{x_\ell}$ for HG'/G'. Set $\overline{x_0} = 1_{G'}$
- Enumerate each $\overline{x_i}$, find $X_i = \overline{x_i} \cap H$ (time $\ell \cdot |G'|$.)
- $\bigcup_{i=0}^{\ell} X_i$ generate H.
  Why ?

Why - exercise

Exercise. $N \lhd G$, $H \leq G$, $\overline{x_1}, \ldots, \overline{x_\ell}$ generate $NH/N \Rightarrow (H \cap N) \cup X_1 \cup \cdots \cup X_l$ generate H, where $X_i = H \cap \overline{x_i}$.

Why - exercise

Exercise. $N \lhd G$, $H \leq G$, $\overline{x_1}, \ldots, \overline{x_\ell}$ generate $NH/N \Rightarrow$ $(H \cap N) \cup X_1 \cup \cdots \cup X_l$ generate H, where $X_i = H \cap \overline{x_i}$.

- K =subgroup generated by $(H \cap N) \cup X_1 \cup \cdots \cup X_l$.
- $K \leq H$,
- $K \cap N$=$H \cap N$,
- $KN = HN$.
- $KN/N \cong K/(K \cap N)$,
- $HN/N \cong H/(H \cap N)$ (isomorphism theorem)
- $K/(N \cap K) \cong H/(N \cap H)$.
- $K = H$.

Contents

1. Abelian Fourier sampling
   - The HSP
   - Coset states
   - Abelian Fourier sampling
   - Abelian Fourier sampling without measurements
   - Application: small commutator subgroup
2. Reduction to smaller groups
   - Reduction scheme
   - Function value superposition
   - Hidden shift problem

Reduction scheme

$N \lhd G$

- Solve the HSP in N for f: find $H \cap N$.
- Implement $F(x) = \frac{1}{\sqrt{N}} \sum_{y \in N} |f(xy)\rangle$
- Solve the HSP in G/N for F: find NH/N.
- For every generator $\overline{x_i}$ for NH/N find $X_i = \overline{x_i} \cap H$.
- $(H \cap N) \cup \bigcup X_i$ generate H.

  (By why-exercise)

xxx: critical subtask

Function value superposition

(for the first critical subtask)

- $f : G \to \mathbb{C}^X$ by oracle, hides H, T transversal
- Task: compute $\frac{1}{\sqrt{|T|}} \sum_{x \in T} |f(x)\rangle$ (using the oracle).
- Computing $\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle|f(x)\rangle$ usually easy.
- An entangled state!!!!
- Wish: "forget" ("disentangle") $|x\rangle$ from $|x\rangle|f(x)\rangle$.

Fct. val. superpos. and Graph Isomorphism

permuted graph

Γ graph on $\{1, \ldots, n\}$, $\sigma \in S_n$,

permuted graph $\sigma(\Gamma)$, with edges:

$(\sigma(i), \sigma(j))$ where (i, j) edge of Γ.

Graph isomorphism

$|\widetilde{\Gamma}\rangle := \frac{1}{\sqrt{|T|}} \sum_{\sigma \in S_n} |\sigma(\Gamma)\rangle$

$\Gamma_1 \cong \Gamma_2 \Leftrightarrow |\widetilde{\Gamma}_1\rangle = |\widetilde{\Gamma}_2\rangle$, otherwise $|\widetilde{\Gamma}_1\rangle \perp |\widetilde{\Gamma}_2\rangle$.

Tested with the swap test.

Swap test

$$|0\rangle|\widetilde{\Gamma}_1\rangle|\widetilde{\Gamma}_2\rangle \qquad \text{Hadamard} \longrightarrow$$

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|\widetilde{\Gamma}_1\rangle|\widetilde{\Gamma}_2\rangle \qquad \text{swap if 1} \longrightarrow$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle|\widetilde{\Gamma}_1\rangle|\widetilde{\Gamma}_2\rangle+|1\rangle|\widetilde{\Gamma}_2\rangle|\widetilde{\Gamma}_1\rangle\right) \qquad \text{Hadamard} \longrightarrow$$

$$\frac{1}{2}|0\rangle\left(|\widetilde{\Gamma}_1\rangle|\widetilde{\Gamma}_2\rangle+|\widetilde{\Gamma}_2\rangle|\widetilde{\Gamma}_1\rangle\right)+\frac{1}{2}|1\rangle\left(|\widetilde{\Gamma}_1\rangle|\widetilde{\Gamma}_2\rangle-|\widetilde{\Gamma}_2\rangle|\widetilde{\Gamma}_1\rangle\right)$$

$$Prob(|1\rangle|*\rangle)=\begin{cases} 0 & \text{if } |\widetilde{\Gamma}_1\rangle=|\widetilde{\Gamma}_2\rangle \\ 1/2 & \text{if } |\widetilde{\Gamma}_1\rangle\perp|\widetilde{\Gamma}_2\rangle \end{cases}$$

Intersection with cosets- the second critical subtask

Setting: $N \lhd G$, f hides H, $N \cap H$ known, given $y \in G$.

Task: find $Ny \cap H$

for $u \in N$:
$uy \in H \Leftrightarrow xuy \in xH$ for every $x \in N \Updownarrow$
$f(xuy) = f(x)$ for every $x \in N$.

Hidden shift problem in N with $f_0(x) = f(xy)$, $f_1(x) = f(x)$.

Solutions: a right coset of $H \cap N$ in N.

Hidden shift problem

Find u s. t. $f_1(x) = f_0(xu)$ for every $x \in N$.

The hidden shift problem

Hidden shift

Given $f_0, f_1 : G \to \mathbb{C}^X$ such that

f_0, f_1 hide subgroups H_0 resp. H_1.
either $\exists u \in G$ s.t. $f_1(x) = f_0(xu)$ for every $x \in G$,
or $f_1(x) \perp f_0(x')$ for every $x, x' \in G$.

Task: Decide and find u as above (if exists).

Remarks.

- subcases: H_0, H_1 known/unknown.
- $H_1 = H_0^u = uH_0u^{-1}$ for arbitrary solution u.
- Solutions: a left coset of H_0 (right coset of H_1).

Cyclic hidden shift $\longrightarrow$ Dihedral HSP

From hidden shift problem of $\mathbb{Z}_n$

Find u s. t. $f_1(x) = f_0(xu)$ for every $x \in \mathbb{Z}_n$.

To Dihedral HSP

Both $f_0, f_1 : \mathbb{Z}_n \to \mathbb{C}^X$ hide the same subgroup H of $\mathbb{Z}_n$.
Either $f_1(\mathbb{Z}_n) \perp f_0(\mathbb{Z}_n)$ or $f_1(x) = f_2(xu)$ for some $u \in \mathbb{Z}_n$.

$$D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2; f(x,t) = \begin{cases} f_0(x) & \text{if } t = 0 \\ f_1(x) & \text{if } t = 1 \end{cases}$$

implementable version: $$|f(x,t)\rangle = \begin{cases} |f_0(x)\rangle|f_1(x)\rangle & \text{if } t = 0 \\ |f_1(x)\rangle|f_0(x)\rangle & \text{if } t = 1 \end{cases}$$

$$f \text{ hides } \begin{cases} H \cup uH & \text{if } f_1(x) = f_0(ux) \\ H & \text{if no such } u \end{cases}$$

Dihedral HSP $\longrightarrow$ Cyclic hidden shift

From Dihedral HSP

$f : D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2 \rightarrow \mathbb{C}^X$ hides H $f_t(x) = f(x,t)$

$H = H_0 \cap H_1$ $H_0 =$ hidden subgroup of $f_H = H \cap \mathbb{Z}_n$,

$H_1 = H \cap t\mathbb{Z}_n$.

for $x \in Z_n$: $(xt) \in H_1 \Leftrightarrow f_1(x) = f(x,1) = f(x,0) = f_0(x)$.

To hidden shift

Find u s. t. $f_1(x) = f_0(xu)$ for every $x \in \mathbb{Z}_n$.