Hidden Subgroup Minicourse - "smooth" groups

Gábor Ivanyos
MTA SZTAKI & TU/e

CWI Amsterdam, October 30 - November 3, 2006

Contents

Motivation: Hidden shift → value superposition

- $f : G \to \mathbb{C}^X$ hides H, $N \lhd G$.
- Would like to obtain a HSP in G/N,
- implement $|F(y)\rangle = \frac{1}{\sqrt{|N|}} \sum_{x \in N} |f(xy)\rangle$.

  Assume $H \cap N = 1$.
- Entangled state $|y\rangle \frac{1}{\sqrt{|N|}} \sum_{x \in N} |x\rangle |f(xy)\rangle$.
- Assume procedure for $|y\rangle|f(xy)\rangle|0\rangle \to |y\rangle|f(xy)\rangle|x\rangle$ ($\sim$ discrete log.)
- Inverse could disentangle $|x\rangle$

Motivation for permutation problems

- Wish $|y\rangle|f(xy)\rangle|0\rangle \to |y\rangle|f(xy)\rangle|x\rangle$
- Harder $|f(y)\rangle|f(xy)\rangle|0\rangle \to |f(y)\rangle|f(xy)\rangle|x\rangle$
- A discrete log-like problem.
- Inverse (of the harder problem) could compute $f(xy)$ from x and $f(y)$.
- Insetad the f-oracle, we assume oracle for this.
- G acts as a permutation group on the domain of f.
- Oracle performs this action.

Permutation problems

Permutation action

- $\Omega \subseteq C^X$ pairwise orthogonal unit vectors
- Permutation action $G \times \Omega \rightarrow \Omega$ $\quad ((g_1 g_2)\omega = g_1(g_2\omega))$
- Oracle for $|g\rangle|\omega\rangle|g\omega\rangle$

Stabilizer - spec. Hidden subgroup

- Given $\omega \in \Omega$, compute G_ω.
- find G_ω = hidden subgroup of $f(x) = x\omega$.

(Effective) Orbit membership - spec. Shift problem

- Given $\omega_0, \omega_1 \in \Omega$, compute G_ω.
- Find $u \in G$ such that $\omega_1 = u\omega_0$

  Shift problem for $f_0(x) = x\omega_0$, $f_1(x) = x\omega_1$.

The action on "curves"

- $f : G \to \mathbb{C}^X$ hides H
- Shifted f: $f_u(x) = f(xu)$
- Permutation action on $\{f_u | u \in G\}$:
  $(f_u)_v(x) = f_u(xv) = f(xvu) = f_{vu}(x)$
  $(f_{(v_1 v_2)u}(x) = f(x(v_1 v_2)u) = f(xv_1(v_2 u)) = f_{v_1(v_2 u)}(x)$.
- Curve of f: $|f\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |f(x)\rangle$
- $|f_u\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |f(xu)\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} |xu^{-1}\rangle |f(x)\rangle$
- $|u\rangle|f\rangle \to |u\rangle|f_u\rangle$ implemented by multiplying the first register of $|f\rangle$ by u^{-1}.

The action on "curves" 2

- $f : G \to \mathbb{C}^X$ hides H
- The states $|f_u\rangle$ are pairwise either orthogonal or identical.
- So we have a permutation action of G on these states.
- Stabilizer of $|f\rangle = |f_1\rangle$ is H.
- Stabilizer of $|f_u\rangle$ is $H^u = uHu^{-1}$.

The action on "curves" 3

- $f, f' : G \to \mathbb{C}^X$ hide H_0 resp. H_1
- Shift problem for f and f' becomes Orbit membership for $|f\rangle$ and $|f'\rangle$.

Conclusion

- Function problems ($f : G \to \mathbb{C}^X$) are equivalent with permutation problems in the general sense ($\Omega \subset \mathbb{C}^X$).
- Remark: the class of permutation problems with $\Omega \subseteq X$ may be more restrictive than the classical-valued function problems.

Orbit membership → Orbit superposition

- Assume we can solve Stabilizer and Orbit membership in G:
- $|\omega\rangle \rightarrow$ generators for G_ω
- $|\omega_0\rangle|\omega_1\rangle|0\rangle \rightarrow |\omega_0\rangle|\omega_1\rangle|u\rangle$; where $u \in G$ s. t, $u\omega_0 = \omega_1$.
- Assume further that we can compute $|G_\omega\rangle = \frac{1}{\sqrt{|G_\omega|}} \sum_{x \in G_\omega} |x\rangle$ from the generators of G_ω. (If G is given in an explicit way, usually easy. In solvable black box groups see Watrous-exercise.)
- Together: $|\omega_0\rangle|\omega_1\rangle|0\rangle \rightarrow |\omega_0\rangle|\omega_1\rangle|uG_{\omega_0}\rangle$

Orbit membership → Orbit superposition 2.

- T: a left transversal of G_{ω_0}
- Assume procedure P: $|\omega_0\rangle|\omega_1\rangle|0\rangle \to |\omega_0\rangle|\omega_1\rangle|uG_{\omega_0}\rangle$ where $u \in T$ such that $u\omega_0 = \omega_1$.
- entangled state $\frac{1}{\sqrt{|G|}}\sum_{x\in G}|\omega\rangle|x\omega\rangle|x\rangle =$ $\frac{1}{\sqrt{|G:G_\omega|}}\sum_{u\in T}\frac{1}{\sqrt{|G_\omega|}}\sum_{x\in G_\omega}|\omega\rangle|u\omega\rangle|ux\rangle =$ $\frac{1}{\sqrt{|G:G_\omega|}}\sum_{u\in T}|\omega\rangle|u\omega\rangle|uG_\omega\rangle \to P^{-1} \to$
- $\frac{1}{\sqrt{|G:G_\omega|}}\sum_{u\in T}|\omega\rangle|u\omega\rangle|0\rangle =$ desired state

A serious problem

- In the solution of the shift problem for $\mathbb{Z}_p^n$:
- Repetitions in Fourier sampling requires several calls of the oracle for f_i.
- Here we have quantum states, Simulating several oracle calls would require cloning.
- Solution: repeated states in input.

Permutation problems with repeated input

Stabilizer

- Given $|\omega\rangle^{\otimes \ell} \in \Omega$, compute G_ω.
- find G_ω

(Effective) Orbit membership

- Given $|\omega_0, \omega_1\rangle^{\otimes \ell} \in \Omega$, compute G_ω.
- Find $u \in G$ such that $\omega_1 = u\omega_0$

Orbit superposition

- Given $|\omega\rangle^{\otimes \ell} \in \Omega$, compute $|G\omega\rangle = \frac{1}{\sqrt{|T|}} \sum_{x \in T} |x\omega\rangle$.
- where T is a transversal of G_ω.

Tools

We can efficiently solve in the repeated input model:

- Stabilizer in Abelian groups in poly time.
- Orbit membership in $\mathbb{Z}_p^n$ in time $poly(n^p)$.

With some error probability!

- Interpret probabilistic error as numerical error of unitary procedures:
- We have unitary procedures such that output state may have some (short) distance from a correct one.
- For error at most ϵ, input repetition $\ell = O(poly(\log|G|)\log 1/\epsilon)$ resp. $\ell = O(poly(n^p)\log 1/\epsilon)$ required.

Orbit membership → Orbit superposition

- Assume for $N \lhd G$ we can solve Stabilizer and Orbit membership in N in time $t(N)$ with repetition ℓ within error ϵ.
- Then, given $|\omega\rangle^{\otimes 2\ell}$ we can compute in time $poly(t(N))$ within error ϵ the state

$$|N\omega^{\otimes \ell}\rangle = \frac{1}{\sqrt{|T|}} \sum_{x \in T} |x\omega\rangle^{\otimes \ell}.$$

:(This is an entangled state, not $|N\omega\rangle\otimes^{\ell}$

- G/N acts on $\{|N\omega^{\otimes \ell}\rangle | \omega \in \Omega\}$.

:) This action is equivalent with the action on $\{|N\omega\rangle | \omega \in \Omega\}$.

Recall

Intersections with cosets

Setting: $N \lhd G$, G acts on Ω, $\omega \in \Omega$, $H = G_\omega$.

Task: find $Ny \cap H$

for $u \in N$: $uy \in G_\omega \Leftrightarrow uy\omega = \omega$

Orbit membership problem in N with $\omega_0 = y\omega$, $\omega_1 = \omega$.

Was: exercise

$Ny_1, \ldots, Ny_s$ generate $NH/N \Rightarrow (H \cap N) \cup Y_1 \cup \cdots \cup Y_s$ generate H, where $Y_i = H \cap Ny_i$.

Induction for Stabilizer 1.

- $N \triangleleft G$, G/N abelian, $\omega \in \Omega$
- Assume we can solve Stabilizer and Orbit membership in N in time $t(N)$ with error ϵ on ℓ-repeated input.
- Input $\omega^{\otimes \ell \cdot r}$, where $r = O(poly(\log |G/|) \log(1/\epsilon)$.
- Compute stabilizer N_ω
- Compute $|N\omega^{\otimes \ell}\rangle^{\otimes r}$,
- Use Abelian Fourier Sampling for computing generators for the stabilizer of $|N\omega^{\otimes \ell}\rangle$. (This is NG_ω/N.)

Induction for Stabilizer 2.

- We have generators $y_j N$ for NG_ω / N.
- For each generator $y_j N$ of NG_ω / N compute $x_j N \cap G_\omega$ using Orbit membership in N.
- Compute G_ω form $y_j N \cap G_\omega$ $(j = 1, 2, \ldots)$ and N_ω.
- time

Induction for Orbit membership

- $N \lhd G$, $G/N \cong \mathbb{Z}_{p^n}$, $\omega_0, \omega_1 \in \Omega$
- Assume we can solve Stabilizer and Orbit membership in G in time $t(G)$ with error ϵ on ℓ-repeated input.
- Input $\omega_1^{\otimes \ell \cdot r} \otimes \omega_2^{\otimes \ell \cdot r}$, where $r = O(poly(\log |G/N| 2^p) \log(1/\epsilon)$.
- Compute $|N\omega_0^{\otimes \ell}\rangle^{\otimes r} |N\omega_1^{\otimes \ell}\rangle^{\otimes r}$
- Use the hidden shift algorithm for $G/N \cong \mathbb{Z}_p^n$ to find $y \in G$ (is there is any) such that $N\omega_1 = yN\omega_0$ ($\Leftrightarrow |N\omega_1^{\otimes \ell}\rangle |yN\omega_0^{\otimes \ell}\rangle$).
- Then there is an $x \in yN$ such that $\omega_1 = x\omega_0$.
- Search for x in the form $x = zy$ where $z \in N$.
- Such a z satisfies $y^{-1}\omega_1 = z\omega_0$, a solution of an orbit membership in N.