Fast Quantum Algorithms Lectures 3 and 4

Gábor Ivanyos
MTA SZTAKI

3rd de Brún Workshop, Galway 7-10 December, 2009.

Contents

HSP - the hidden subgroup problem

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

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

  x and y are in the same left coset of H

  f is constant on the left cosets of H
  and takes different values on different cosets
- f given by an oracle (or an efficient algorithm) performing

  $$|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$$
- Task: find (generators for) H.

  preferably in time $\text{poly}\log|G|$

Coset states - summary

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

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

Query complexity of the HSP

- **Theorem.** (*Ettinger, Høyer, Knill 2004*)
  $O(\log|G|)$ coset states of H sufficient for determining H
- **Main idea:**
  - If $K \leq H$, then every coset state $|aH\rangle$ of H
    is in the subspace spanned by the coset states of K,
  - otherwise sufficiently "far away"
- Provides test for deciding whether $K \leq H$
- Does not destruct coset state $|aH\rangle$

  $\Downarrow$
- Can be reused for the next subgroup K

Projection to coset states

- for $K \leq G$ map $P_K : |g\rangle \mapsto \frac{1}{\sqrt{|K|}}|gK\rangle$
- P_K orthogonal projection on the subspace of coset states of K
  - $P_K^2 = P_K$,
  - $P_K^*|g\rangle = \frac{1}{|K|}\sum_{h\in K} gh^* = \frac{1}{|K|}\sum_{h\in K} gh^{-1}\frac{1}{\sqrt{|K|}}|gK\rangle = P_K|g\rangle$
- **Lemma:** $|P_K|uH\rangle|^2 = \frac{|H\cap K|}{|K|} = \begin{cases} 1 & \text{if } K \leq H \\ \leq \frac{1}{2} & \text{otherwise} \end{cases}.$

Proof. $|P_K|uH\rangle|^2 = \frac{|1|}{|K||H|}|\sum_{h\in H}|uhK\rangle|^2 =$
$\frac{|1|}{|K||H|}|\sum_{h\in H}|hK\rangle|^2 = \frac{|H:K\cap H||H\cap K|^2}{|K||H|} = \frac{|H\cap K|}{|K|}$

Test for $K \leq H$

- $P_K =$ the orthogonal projection to the subspace spanned by the cosets states of K
- $U_K := \begin{pmatrix} I - P_K & P_K \\ P_K & I - P_K \end{pmatrix}$
- U_K unitary on $\mathbb{C}G \oplus \mathbb{C}G \cong \mathbb{C}G \otimes \mathbb{C}^2$
- $U_K(|y\rangle \otimes |0\rangle) = ((I - P_K)|y\rangle) \otimes |0\rangle + (P_K|y\rangle) \otimes |1\rangle.$

Test for $K \leq H$ part 2.

- $U_K(|y\rangle \otimes |0\rangle) = ((I - P_K)|y\rangle) \otimes |0\rangle + (P_K|y\rangle) \otimes |1\rangle$.
- $\Psi = \Psi(K, u, H) = U_K(|uH\rangle \otimes |0\rangle) = \Psi^0 \otimes |0\rangle + \Psi^1 \otimes |1\rangle$
- $|\Psi_1|^2 = |P_K|uH\rangle|^2 = \begin{cases} = 1 & \text{if } K \leq H \\ \leq \frac{1}{2} & \text{otherwise} \end{cases}$.
- If $K \leq H$ then $\Psi = \Psi^1 \otimes |1\rangle$
- If $K \not\leq H$ then $\Psi = \Psi_0 \otimes |0\rangle + \Psi_1 \otimes |1\rangle$, where $|\Psi_1|^2 \leq \frac{1}{2}$

The HSP algorithm.

- Starting state: $|u_1H\rangle \otimes |0\rangle \otimes |u_2H\rangle \otimes |0\rangle \otimes \ldots \otimes |u_\ell H\rangle \otimes |0\rangle$
- List the cyclic subgroups of G. Unmark all. $K =$ first in the list.

(*) Apply $U_K^{\otimes \ell}$

- If all the aux bits are 1 then mark K.
- reverse $U_K^{\otimes \ell}$
- take next K, go to (*).
- For constant error probability, $\ell = O(\log |G|)$

The HSP algorithm - error analysis

- State: $\Psi = \Psi_1 \otimes \Psi_2 \otimes \cdots \Psi_\ell \otimes |Marked/Unmarked\rangle$,
  where $\Psi_i = U_K(|u_i H\rangle \otimes |0\rangle)$
- $\Psi_i = \Psi_i^0 \otimes |0\rangle + \Psi_i \otimes |1\rangle$
- By the lemma:
- If $K \leq H$ then $\Psi_i^0 = 0$ and $|\Psi_i^1| = 1$,
  $$\Psi = \Psi_1 \otimes \Psi_2 \otimes \cdots \Psi_\ell \otimes |Marked\rangle$$
- If $K \not\leq H$ then $|\Psi_i^1|^2 \leq \frac{1}{2}$,

$$|\Psi - \Psi_1 \otimes \Psi_2 \otimes \cdots \Psi_\ell \otimes |Unmarked\rangle|^2 =$$

$$|\Psi_1 \otimes \Psi_2 \otimes \cdots \Psi_\ell \otimes |Marked\rangle|^2 = \prod |\Psi_i^1|^2 \leq 2^{-\ell}.$$

i.e., distance from correct sate $\leq 2^{-\ell/2}$.

On noncommutative Fourier Transform

- **Abelian Fourier transform:** linear extension of

$$\sum_{\rho\in\hat{G}} \left(\frac{\rho(a)}{|G|^{\frac{1}{2}}|H|^{\frac{1}{2}}} \sum_{x\in H} \rho(x) \right) |\rho\rangle$$

- **Noncommutative Fourier transform:** linear extension of

$$|g\rangle \mapsto \sum_{\rho\in\hat{G}} \sum_{i,j=1}^{d_\rho} \frac{\sqrt{d_\rho}}{\sqrt{|G|}} \sum_{i,j=1}^{d_\rho} \rho(g)_{ij} \left| E_{ij}^{\rho} \right\rangle$$

- $\left| E_{ij}^{\rho} \right\rangle$ represented as $|\rho\rangle|i\rangle|j\rangle$
- **Fourier sampling:** apply Fourier transform to coset state,
- measure $|\rho\rangle$ (and $|i\rangle|j\rangle$)

Noncommutative Fourier sampling

- Fourier transform:

$$|g\rangle \mapsto \sum_{\rho \in \hat{G}} \sum_{i,j=1}^{d_\rho} \frac{\sqrt{d_\rho}}{\sqrt{|G|}} \sum_{i,j=1}^{d_\rho} \rho(g)_{ij} \left| E_{ij}^{\rho} \right\rangle$$

- Weak Fourier sampling: use only $|\rho\rangle$
  - was useful for normal hidden subgroups
- Strong Fourier sampling: use $|\rho\rangle|i\rangle$
  - if have $|i\rangle$, $|j\rangle$ "useless"
  - useful for large hidden subgroups of affine $AGL(1, q)$

Noncommutative Fourier Transform - limitations

- a few successful applications of noncommutative QFT to HSP
- most of these can be explained without referring to QFT
- still gives good guidelines
  (e.g., hidden subgroups in Heisenberg groups)
- $\exists$ results on limitations of *certain* QFT-based approaches
  (even on strong Fourier sampling)
- Open: poly time QFT in
  - general solvable groups
  - general permutation groups
  - classical groups
- existing efficient QFT algorithms
  - Symmetric, alternating groups (Beals)
  - *Certain* solvable groups
  - A general scheme (Moore, Rockmore, Russell)
    efficient for *certain* groups

Possible reduction to subgroups and factors

$N \triangleleft G$

- Solve the HSP in N for f: find $H \cap N$.
- X Implement $F : |x\rangle \mapsto \sum_{y \in N} |f(xy)\rangle$
- Solve the HSP in G/N for F: find NH/N.
- X Find $X_i = \overline{x_i} \cap H$.

  for every generator $\overline{x_i}$ for NH/N

$X_i = x_i(H \cap N)$

- $(H \cap N) \cup \bigcup \{x_i\}$ generate H.

X: critical subtask

Function value superposition

(for the first critical subtask)

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

see remark later

Fct. val. superpos. and Graph Isomorphism

- **permuted graph**

  Γ graph on $\{1,\ldots,n\}$, $\sigma \in S_n$,
  permuted graph Γ^σ, with edges:
  $(\sigma(i),\sigma(j))$ where (i,j) edge of Γ.

- **Graph isomorphism**

  $\left|\widetilde{\Gamma}\right\rangle := \frac{1}{\sqrt{|T|}} \sum_{\sigma \in S_n} |\Gamma^\sigma\rangle$
  $\Gamma_1 \cong \Gamma_2 \Leftrightarrow \left|\widetilde{\Gamma}_1\right\rangle = \left|\widetilde{\Gamma}_2\right\rangle$, otherwise $\left|\widetilde{\Gamma}_1\right\rangle \perp \left|\widetilde{\Gamma}_2\right\rangle$.
  Tested with the **swap test**.

Swap test

- $|0\rangle \left|\widetilde{\Gamma}_1\right\rangle \left|\widetilde{\Gamma}_2\right\rangle$

  $\downarrow$ Hadamard

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

  $\downarrow$ swap if 1

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

  $\downarrow$ Hadamard

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

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

Intersection with cosets- the second critical subtask

- Setting: $N \triangleleft G$, f hides H, $N \cap H$ known, given $y \in G$.
- Task: find $Ny \cap H$
- Let $u \in N$.
  $uy \in H \Leftrightarrow xuy \in xH$ 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 which is the case
  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).

The Hidden Shift problem - further remarks

- **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**
  - Graph isomorphism is an instance:
    - Γ_0, Γ_1 graphs, $G = S_n$,
    - $f_i(\sigma) = \Gamma_i^\sigma$.
    - if $\Gamma_1 = \Gamma^\pi$ then $f_1(\sigma) = f_0(\sigma\pi)$
  - Disentangling in a *certain version* of function value superposition can be done using hidden shift (is reducible to hidden shift) (*Friedl, ∼, Magniez, Santha, Sen 2003)*

Contents

Abelian hidden shift problem problem

- Abelian hidden shift
  - Given $f_0, f_1 : G \to \mathbb{C}^X$ such that
    - f_0, f_1 hide subgroup H.
    - either $\exists u \in G$ s.t. $f_1(x) = f_0(x+u)$ 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
  - Just one hidden subgroup H.
  - H practically known (abelian hidden subgroup)
  - Solutions: a coset of H

Abelian hidden shift - observations

- H can be found by the Abelian Fourier Sampling
- f_0, f_1 give a hidden shift problem on G/H, hide $1_{G/H}$
- If $G \cong \mathbb{Z}_p^n$ then $G/H \cong \mathbb{Z}_p^{n'}$
- Equivalent with the hidden subgroup problem in $G \rtimes \mathbb{Z}_2$ ($\mathbb{Z}_2$ acts on G by flipping signs.)
- If $G = \mathbb{Z}_2^n$ then $G \rtimes \mathbb{Z}_2 = \mathbb{Z}_2^{n+1}$
- In $\mathbb{Z}_2^n$ the hidden shift can be solved by the abelian HSP-algorithm ($\mathbb{Z}_2^n \rtimes \mathbb{Z}_2 \cong \mathbb{Z}_2^{n+1}$). (like Simon's problem.)

- Hidden shift for $\mathbb{Z}_p^n$
  - Given $f_0, f_1 : \mathbb{Z}_p^n \to \mathbb{C}^X$ such that
    - f_0, f_1 injective.
    - either $\exists u \in \mathbb{Z}_p^n$ s.t. $f_1(x) = f_0(x+u)$ for every $x \in \mathbb{Z}_p^n$,
    - or $f_1(x) \perp f_0(x')$ for every $x, x' \in \mathbb{Z}_p^n$.
  - Task: Decide and find u as above (if exists).
- algorithm outline
  - Find the "direction" of u: $\{au | a \in \mathbb{Z}_p\}$
  - Find u on that line in time $O(p)$

Coset states for hidden shift

- $\sum_{x \in \mathbb{Z}_p^n} (|0\rangle + |1\rangle)|x\rangle|f_0(x)\rangle|f_1(x)\rangle$

$\downarrow$ swap if 1

- $\sum_{x \in \mathbb{Z}_p^n} (|0\rangle|x\rangle|f_0(x)\rangle|f_1(x)\rangle + |1\rangle|x\rangle|f_1(x)\rangle|f_0(x)\rangle)$

$\downarrow$ measure

- $|0\rangle|x\rangle + |1\rangle|x + u\rangle$

Abelian Fourier sampling for hidden shift

normalizing factos included on this slide

- coset state $\frac{1}{\sqrt{2}}(|x\rangle|0\rangle + |u+x\rangle|1\rangle)$.
- apply Fourier transform of $\mathbb{Z}_p^n \times \mathbb{Z}_2$.
- $\frac{1}{2\sqrt{n}} \sum_{w\in\mathbb{Z}_p^n, r\in\mathbb{Z}_2} \left(\omega^{(x,w)} + (-1)^r \omega^{(u+x,w)}\right) |w\rangle|r\rangle$
- $|\text{coeff}|^2$ of $|w\rangle|0\rangle$: $\frac{1}{4p^n}\left|1+\omega^{(u,w)}\right|^2 = \frac{1}{n}\cos^2(\pi(u,w)/n)$
- $|\text{coeff}|^2$ of $|w\rangle|1\rangle$: $\frac{1}{4p^n}\left|1-\omega^{(u,w)}\right|^2 = \frac{1}{n}\sin^2(\pi(u,w)/n)$

$(,)$ = scalar product in $\mathbb{Z}_p^n$: $(u,w) = \sum_{i=1}^n u_i w_i$.

Result of sampling

- exclude case $u = 0$ (compare $f_0(0)$ and $f_1(0)$)
- keep only $(w_1, 1), \ldots, (w_\ell, 1)$
- notice only the direction of w_i (line in $\mathbb{Z}_p^n$ through 0 and w_i)
- The probability of the lines in $u^\perp$ are 0, the others are equal.
- $\frac{1}{2p^n} \sum_{\alpha=1}^{p-1} |1-\omega^{(u,\alpha w)}|^2 = \frac{1}{2p^n} \sum_{\alpha=1}^{p-1} (2-\omega^{(u,\alpha w)} - \omega^{-(u,\alpha w)}) = \frac{p-1}{p^n} - \frac{1}{p^n} \sum_{\alpha=1}^{p-1} (\omega^{(u,w)})^\alpha = \begin{cases} 0 & \text{if } (u,w) = 0, \\ \frac{1}{p^{n=1}} & \text{otherwise.} \end{cases}$
- If no u, the probability of every line is $\frac{p-1}{p^n}$.

Random linear disequations

- Search version:
  - Can query samples of vectors from $\mathbb{Z}_p^n \setminus u^\perp$
  - (nearly) uniformly
  - Find direction of u
- Reducible to the **decision version:**
  - Can query samples from a distribution over $\mathbb{Z}_p^n$,
  - the distribution is either (nearly) uniform,
  - or (nearly) uniform on $\mathbb{Z}_p^n \setminus u^\perp$ for a certain u
  - Which is the case?
- Solution (Friedl, ∼, Magniez, Santha, Sen 2003): Polynomial in $p(n+p)^{p-1}$.

Contents

Cyclic hidden shift ← Dihedral HSP

- Hidden shift: 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 $u \in \mathbb{Z}_n$.

  $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$

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

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

Cyclic hidden shift ← Dihedral HSP

- Hidden shift: Both $f_0, f_1 : \mathbb{Z}_n \rightarrow \mathbb{C}^X$ 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 $u \in \mathbb{Z}_n$.

  $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$

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

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

  implementable version

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

Fourier sampling and the resulting states

- $\mathbb{Z}_n \rtimes \mathbb{Z}_2$
- $(a,0)(b,i) = (a+b,i),\ (a,1)(b,i) = (a-b,i+1)$
- Interesting hidden subgroup: $\{(0,0),(u,1)\}$
- coset state

$$|a\rangle|0\rangle + |a+u\rangle|1\rangle$$

$$\downarrow \qquad \text{QFT and measure first part}$$

$$\omega^{aj}|j\rangle\left(|0\rangle + \omega^{ju}|1\rangle\right) = \omega^{aj}|j\rangle\theta_j$$

- $\theta_j = |0\rangle + \omega^{ju}|1\rangle$

Desired sampled states

- would like (several copies of) θ_1:

  Hadamard on θ_1:

$$(1+\omega^u)|0\rangle + (1-\omega^u)|1\rangle$$

  measure and make statistics

  $\downarrow$

  compute ω

Coupling

- $\theta_j = |0\rangle + \omega^{ju}|1\rangle$
- $\theta_{j_1} \otimes \theta_{j_2} =$

$$\begin{cases} |0\rangle|0\rangle + \omega^{(j_1+j_2)}u|1\rangle|1\rangle \\ + \\ \omega^{j_2 u}\left(|0\rangle|1\rangle + \omega^{(j_1-j_2)u}|1\rangle|0\rangle\right) \end{cases}$$

$$\downarrow |x\rangle|y\rangle \mapsto |x\rangle|x+y\rangle$$

$$\begin{cases} \left(|0\rangle + \omega^{(j_1+j_2)u}|1\rangle\right)|0\rangle \\ + \\ \omega^{j_2 u}\left(|0\rangle|1\rangle + \omega^{(j_1-j_2)u}|1\rangle\right)|1\rangle \end{cases}$$

$$= \frac{1}{\sqrt{2}}\left(\theta_{j_1+j_2}|0\rangle + \omega^{j_2 u}\theta_{j_1-j_2}|1\rangle\right)$$

$\downarrow$measure second part

$\theta_{j_1+j_2}$ or $\theta_{j_1-j_2}$ (prob. $\frac{1}{2}$)

Breeding sampled states

- N states θ_{j_i} where j_i random from $\{0,\ldots,n-1\}$

  partition into $2^{\sqrt{\log n}}$ intervals of $\{0,\ldots,n-1\}$ of size $n/2^{\sqrt{\log n}}$
- $\frac{1}{2}N - 2^{\sqrt{\log n}}$ pairs $|j_{i_1} - j_{i_2}| \le n/2^{\sqrt{\log n}}$

  $\downarrow$
- $\approx \frac{1}{4}N$ θ_{j_i}s where j_i random from $\{0,\ldots,n/2^{\sqrt{\log n}}\}$

  $\downarrow$
- $\approx \frac{1}{4^2}N$ θ_{j_i}s where j_i random from $\{0,\ldots,n/2^{2\sqrt{\log n}}\}$

  $\vdots$
- $\approx$ sufficiently many θ_1

  if $N = 2^{O(\sqrt{\log n})}$

Relation to a lattice problem

- $f(n)$-unique SVP
  - Given: Lattice $\Lambda \subset \mathbb{R}^n$
  - Promise: $\exists 0 \neq u \in \Lambda$, s.t.

$$|v| = \Omega(f(n)) \text{ for } v \in \Lambda \setminus \mathbb{Z}u.$$

  - Task: find $\pm u$.
- Regev (2004): $n^{\frac{1}{2}+\epsilon}$-unique SVP in quantum poly time reducible to

  a **version** of dihedral HSP:
  - Given $\bigotimes_{i=1}^{\ell} |a_i\rangle|0\rangle + |a_i + u\rangle|1\rangle$ (ℓ coset states)
  - Find u

Contents

Some top noncommutative HSP-related results

- Dihedral HSP/Cyclic hidden shift *Kuperberg 06*
- Relation of dihedral HSP to SVP in lattices Regev 2004
- Polynomial time hidden shift in $\mathbb{Z}_p^n$ (p constant)
  Friedl, ∼, Magniez, Santha, Sen 03
- HSP in solvable groups of constant exponent
  Friedl, ∼, Magniez, Santha, Sen 03
- Polynomial time hidden shift in certain cylcic/abelian p-groups *Bacon, Childs, van Dam, 05*
- Similar algorithm for hidden polynomials
  Decker, Draisma, Wocjan 09
- Polynomial time HSP in class 2 nilpotent groups
  ∼, Sanselme, Santha 08

Hidden shifts - open questions

- *trivial* in $\mathbb{Z}_m^n$: $2^{O(n \log m)}$
- *Kuperberg* in $\mathbb{Z}_m^n$: $2^{O(\sqrt{n \log m})}$
- *Friedl et al.* in $\mathbb{Z}_m^n$: $2^{O(nm \log m)}$
- any improvement in any direction?

  would give improved result for HSP in solvable groups
- better unique-SVP algorithms?
- class 3 nilpotent groups?
- related: polynomial time Chevalley-Warning–theorem for systems degree 3 equations

Towards quantum algorithms for (graph) isomorphism problem?

- classical complexity of GI $2^{O(\sqrt{n \log n})}$
- no better (simpler?) quantum algorithm known
- complexity of HSP over S_n - no nontrivial result
- special cases of GI?
- other iso/automorphism problems?
  - group iso/auto (in size G) - best known: trivial $|G|^{O(\log |G|)}$
  - even for class 2 groups
  - lattices (integral quadratic forms)

Contents

Coset states in certain semidirect products

- $G = \mathbb{Z}_p^m \rtimes \mathbb{Z}_s$
- conjugation
  - $A \in \mathrm{GL}(\mathbb{Z}_p^m) \cong \mathbb{Z}_p^{m \times m}$, $A^s = 1$
  - $(0,1)(u,0)(0,1)^{-1} = (Au, 0)$
- Important hidden subgroup: $H = \langle (v,1) \rangle$
- elements of H:

$$(v,1)^t = \left(\sum_{j=0}^{t-1} A^j v, t \right)$$

- Coset state

$$|(u,0)H\rangle = \sum_{t \in \mathbb{Z}_s} \left| (u + \sum_{j=0}^{t-1} A^j v, t) \right\rangle$$

Hidden curve states

- Hidden curve states
  - S set, Given $Q : S \to \mathbb{F}^{m\times n}$ (e.g., $S = \mathbb{F}$, $Q(t) \in \mathbb{F}[t]^{m\times n}$)
  - States

$$|Q_{v,u}\rangle = \sum_{t\in S} |u + Q(t)v\rangle |t\rangle$$

- Example 1:semidirect HSP:

$$Q(t) = \sum_{j=0}^{t-1} A^j$$

if $s = p$ then $Q(t)$ polynomial

Hidden curve states 2

- Hidden curve states

$$|Q_{v,u}\rangle = \sum_{t \in S} |u + Q(t)v\rangle |t\rangle$$

- Example 2.: Hidden polynomial
  - $f(t) = \sum_{j=1}^{n} v_i t^i$
  - $g(s,t) = s - f(t)$
  - oracle

$$|s\rangle|t\rangle|0\rangle \mapsto |s\rangle|t\rangle|g(t)\rangle$$

  - Task: find v
  - Sampling gives state

$$\sum_{g(t)=u} |s\rangle|t\rangle = \sum_{s-f(t)=u} |s\rangle|t\rangle = \sum_{t \in \mathbb{F}} |u + f(t)\rangle|t\rangle \quad \text{for random } u$$

  - matrix: $Q(t) = (t, t^2, \ldots, t^n)$, $f(t) = Q(t)v$

PGM-based approach

- simplification: $q = p$ prime, $\omega = \sqrt[p]{1}$
- (similar approach works for q prime power)
- $\sum_{t \in S} |u + Q(t)v, t\rangle$

  $\downarrow$ QFT on first part
- $\sum_{y \in \mathbb{F}^m} \sum_{t \in S} \omega^{(y,u)+(y,Q(t)v)} |y\rangle |t\rangle$

  $\downarrow$ measure y
- $\omega^{(y,u)} \sum_{t \in S} \omega^{(y,Q(t)v)} |t\rangle$

- one copy $\sum_{t\in S}\omega^{(Q(t)^T y,v)}|t\rangle$
- ℓ copies:

$$\sum_{\underline{t}\in S^\ell}\omega^{(\sum_{i=1}^{\ell}Q(t_i)^T y_i,v)}|t_1,\ldots,t_\ell\rangle$$

for random $Y=(y_1,\ldots,y_\ell)\in\mathbb{F}^{m\times\ell}$

$\downarrow$

$$\sum_{\underline{t}\in S^\ell}\omega^{(\sum_{i=1}^{\ell}Q(t_i)^T y_i,v)}|t_1,\ldots,t_\ell\rangle\left|\sum_{i=1}^{\ell}Q(t_i)^T y_i\right\rangle$$

for random $Y=(y_1,\ldots,y_\ell)\in\mathbb{F}^{m\times\ell}$

$$* = \sum_{\underline{t}\in S^\ell} \omega^{(\sum_{i=1}^{\ell} Q(t_i)^T y_i, v)} |t_1, \ldots, t_\ell\rangle \left| \sum_{i=1}^{\ell} Q(t_i)^T y_i \right\rangle$$

Notation:

$\mathcal{T}_Y^z = \{(t \in S^\ell | \sum_{i=1}^n Q(t_i)^T y_i = z\}$

$\tau_Y^z = |\mathcal{T}_Y^z|,$

$|\mathcal{T}_Y^z\rangle = \frac{1}{\sqrt{\tau_Y^z}} \sum_{t\in\mathcal{T}_Y^z} |t\rangle$

$(|\mathcal{T}_Y^z\rangle = |"\emptyset"\rangle$, if $\mathcal{T}_Y^z = \emptyset)$

$* = \sum_{z\in\mathbb{F}^n} \omega^{(z,v)} \sqrt{\tau_Y^z} |\mathcal{T}_Y^z\rangle |z\rangle$

$\downarrow$

$\sum_{z\in\mathbb{F}^n} \omega^{(z,v)} \sqrt{\tau_Y^z} |0\rangle |z\rangle$

$\downarrow$

$|0\rangle |v\rangle$

WISH: uncompute $|\mathcal{T}_Y^z\rangle$

QFT^{-1}

- Assume procedures

$$P_0 : |Y\rangle|z\rangle|0\rangle \mapsto |Y\rangle|z\rangle \begin{cases} |\text{good}\rangle \\ |\text{bad}\rangle \end{cases},$$

$$P_1 : |Y\rangle|z\rangle|0\rangle \mapsto |Y\rangle|z\rangle \begin{cases} |\mathcal{T}_Y^z\rangle & \text{if good} \\ \\ |?\rangle & \text{if bad} \end{cases}$$

- P_1 solves "relaxed" system

$$\sum_{i=1}^{n} Q^T(t_i)y_i = z$$

- "original" system

$$Q^T(t)y = z$$

$$\sum_{i=1}^{\ell} Q^T(t_i)y_i = z$$

Uncomputing using procedures P_0 and P_1

- $\sum_{z\in\mathbb{F}^n} \omega^{(z,v)} \sqrt{\tau_Y^z} |\mathcal{T}_Y^z\rangle |z\rangle |0\rangle$

  $\downarrow$ P_0

  $c_1 \sum_{z\in\mathbb{F}^n} \omega^{(z,v)} \sqrt{\tau_Y^z} |\mathcal{T}_Y^z\rangle |z\rangle |\text{good}\rangle + c_2 |\ldots\rangle |\text{bad}\rangle$

  $\downarrow$ P_1^{-1} if good

- $\Psi = c_1 \sum_{z\in\mathbb{F}^n} \omega^{(z,v)} \sqrt{\tau_Y^z} |0\rangle |z\rangle |\text{good}\rangle + c_2 |\ldots\rangle |\text{bad}\rangle$

- $\Psi = c_1 \sum_{z\in\mathbb{F}^n} \omega^{(z,v)} \sqrt{\tau_Y^z}|0\rangle|z\rangle|\text{good}\rangle + c_2|\ldots\rangle|\text{bad}\rangle$
- if $c_1 >$ constant and $\tau_Y^z \approx_{\text{const}}$ average then

$$|\langle\Psi, \sum_{z\in\mathbb{F}^n} \omega^{(z,v)}|0\rangle|z\rangle|\text{good}\rangle\rangle| > \text{constant:}$$

- $\Psi \approx_{\text{const}} \sum_{z\in\mathbb{F}^n} \omega^{(z,v)}|0\rangle|z\rangle|\text{good}\rangle$

$$\downarrow \qquad \text{QFT}^{-1}$$

- $\Psi' \approx_{\text{const}} |0\rangle|v\rangle|\text{good}\rangle$
- measuring Ψ' gives v with $>$ constant > 0 prob.