Hidden Subgroup Minicourse - Abelian hidden shift

Gábor Ivanyos
MTA SZTAKI & TU/e

CWI Amsterdam, October 30 - November 3, 2006
1 Dihedral HSP
   - Definition and significance
   - Abelian Fourier sampling for hidden reflection
   - Classical post-processing

2 Hidden shift in \( \mathbb{Z}_p^n \).
   - Abelian hidden shift
   - Reduction to hyperplane cover
   - Solving hyperplane cover
   - Conclusion
Dihedral groups

- $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$ where $t \in \mathbb{Z}_2$ acts on $\mathbb{Z}_n$ as taking inverses.
- $D_n = \{ r^i t^j | i \text{ mod } n, j \text{ mod } 2 \}$
- $r^{i_1} t^{j_1} \cdot r^{i_2} t^{j_2} = r^{i_1-i_2 j_1} t^{i_1+i_2}$
- rotations: $r^i$, reflections: $r^i t$. 
Significance of dihedral HSP

- HSP in $D_n$ equivalent to the hidden shift problem in $\mathbb{Z}_n$
- would give a useful induction tool for HSP in solvable groups:

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_\ell = 1$$

$$G_{i-1}/G_i$$ cyclic.
Easy reduction of dihedral HSP

- $f$ hides $H$
- Abelian Fourier sampling finds $N = H \cap \mathbb{Z}_n$.
- $N \triangleleft D_n$
- If $N = \mathbb{Z}_n$ then $H = \mathbb{Z}_n$ (if $t \notin H$) or $H = D_n$ (if $t \in H$).
To hidden reflection

If $N = \mathbb{Z}_n \cap H \neq \mathbb{Z}_n$

- $D_n/N \cong D_m$ where $m = n/|N|$
- $f$ defined on $D_m \cong D_n/N$, hides a subgroup $\overline{H}$ with $H \cap \mathbb{Z}_m = 1$.
- $\overline{H}$ is $\{1\}$ or $\{1\} \cup \{a \text{ reflection}\}$.

Dihedral HSP reduces to:

**hidden reflection**

$f$ hides in $D_n$ the subgroup $\{1\}$ or $\{1\} \cup \{\text{a reflection}\}$. 
Dihedral HSP
Hidden shift in $\mathbb{Z}_n^p$.

Additive notation for $\mathbb{Z}_n$: $v \leftrightarrow r^v$.

- hidden reflection $(u, 1)$ (subgroup $\{(0, 0), (u, 1)\}$
- coset $(v, 0)\{(0, 0), (u, 1)\} = \{(v, 0), (u + v, 1)\}$
- or coset $(v, 1)\{(0, 0), (u, 1)\} = \{(v, 1), (v - u, 0)\} = \{(v', 0), (u + v', 1)\}$ where $v' = v - u$.
- coset state $\frac{1}{\sqrt{2}} (|v, 0\rangle + |u + v, 1\rangle)$
- in the form $\frac{1}{\sqrt{2}} (|v\rangle|0\rangle + |u + v\rangle|1\rangle)$.
Abelian Fourier sampling for hidden reflections

- coset state $\frac{1}{\sqrt{2}} (|v\rangle|0\rangle + |u + v\rangle|1\rangle)$.
- apply Fourier transform of $\mathbb{Z}_n \times \mathbb{Z}_2$.
- $\frac{1}{2\sqrt{n}} \sum_{w \in \mathbb{Z}_n, r \in \mathbb{Z}_2} (\omega^{vw} + (-1)^r \omega^{(u+v)w}) |w\rangle|r\rangle$
- $|\text{coeff}|^2$ of $|w\rangle|0\rangle$: $\frac{1}{4n} |1 + \omega^{uw}|^2 = \frac{1}{n} \cos^2(\pi uw/n)$
- $|\text{coeff}|^2$ of $|w\rangle|1\rangle$: $\frac{1}{4n} |1 - \omega^{uw}|^2 = \frac{1}{n} \sin^2(\pi uw/n)$
Dihedral HSP
Hidden shift in $\mathbb{Z}_p^n$.

Definition and significance
Abelian Fourier sampling for hidden reflection
Classical post-processing

Distributions

- If $H = \{(0, 0)\}$: uniform.
- If $H = \{(0, 0), (u, 1)\}$: $\text{Prob}(w, 0) = \frac{1}{n} \cos^2(\pi uw / n)$
- exclude $H = \{(0, 0), (0, 1)\}$ and $H = \{(0, 0), (n/2, 1)\}$ (compare $f(0, 0)$, $f(0, 1)$ and/or $f(n/2, 1)$).
- take only samples of type $(w_1, 0), \ldots, (w_\ell, 0)$ ($\ell$ will be in $O(\log n)$)
- This simulates sample for variable $W$ where $\text{Prob}(W = w) = \frac{2}{n} \cos^2(\pi uw / n) = \frac{1}{n} + \frac{2}{n} \cos(2\pi uw / n)$ (or uniform if $H$ trivial).
For $\nu, x \in \mathbb{Z}_n$ set $f_\nu(x) = \cos(2\pi \nu x / n)$

$E(f_\nu(w)) = \begin{cases} 
1/2 & \text{if } \nu = \pm u \\
0 & \text{otherwise}
\end{cases}$

”otherwise” includes the case $H = \{(0,0)\}$.

$\frac{1}{\ell} \sum f_\nu(w_i)$ deviates by more than $\frac{1}{4}$ from $E(f_\nu(W))$ with exponentially small probability (in $\ell$). (From, e.g., Hoeffding’s Lemma.)

Sample of size $\ell = O(\log n)$ sufficient (for error $< \frac{1}{n}$).

choose $\nu$ such that $\frac{1}{\ell} \sum f_\nu(w_i) > \frac{1}{4}$ and return $\{(0,0), \{\nu, 1\}\}$

$H$ will be trivial if no such $\nu$. 
1 Dihedral HSP
   - Definition and significance
   - Abelian Fourier sampling for hidden reflection
   - Classical post-processing

2 Hidden shift in $\mathbb{Z}_p^n$
   - Abelian hidden shift
   - Reduction to hyperplane cover
   - Solving hyperplane cover
   - Conclusion
The hidden shift problem

**Hidden shift**

Given \( f_0, f_1 : G \rightarrow \mathbb{C}^X \) 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 \( H_1 \)).
Abelian hidden shift 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 ($\mathbb{Z}_2^n \rtimes \mathbb{Z}_2 \cong \mathbb{Z}_2^{n+1}$). ($\sim$ Simon’s problem.)
Hidden shift for $\mathbb{Z}_p^n$

Given $f_0, f_1 : \mathbb{Z}_p^n \rightarrow \mathbb{C}^X$ 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

\[
\frac{1}{\sqrt{2^p n}} \sum_{x \in \mathbb{Z}_p^n} (|0\rangle + |1\rangle) |x\rangle |f_0(x)\rangle |f_1(x)\rangle
\]
swap if \(1 \rightarrow \)

\[
\frac{1}{\sqrt{2^p n}} \sum_{x \in \mathbb{Z}_p^n} (|0\rangle |x\rangle |f_0(x)\rangle |f_1(x)\rangle + |1\rangle |x\rangle |f_1(x)\rangle |f_0(x)\rangle)
\]
measure \(\rightarrow \)

\[
\frac{1}{\sqrt{2}} (|0\rangle |x\rangle + |1\rangle |x + u\rangle)
\]
Abelian Fourier sampling for hidden shift

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

$$\frac{1}{2p^n} \sum_{\alpha=1}^{p-1} |1 - \omega^{\alpha u \cdot w}|^2 = \frac{1}{2p^n} \sum_{\alpha=1}^{p-1} (2 - \omega^{\alpha u \cdot w} - \omega^{-\alpha u \cdot w}) = \frac{p-1}{p^n} - \frac{1}{p^n} \sum_{\alpha=1}^{p-1} (\omega^{u \cdot w})_\alpha = \begin{cases} 0 & \text{if } u \cdot w = 0, \\ \frac{1}{p^n-1} & \text{otherwise.} \end{cases}$$

- If no $u$, the probability of every line is $\frac{p-1}{p^n}$. 
Hyperplane cover

We can query samples from a distribution over the points of the $n-1$-dimensional projective space over $\mathbb{Z}_p$.
The distribution is either uniform,
or uniform on points not on a specific hyperplane.
Which is the case?

Hyperplane cover - dual formulation

We can query samples from a distribution over the hyperplanes of the $n-1$-dimensional projective space over $\mathbb{Z}_p$.
The distribution is either uniform,
or uniform on hyperplanes not on a specific point.
Which is the case?
Hyperplane cover - search version

In the dual formulation: find the point.
Reducible to the decision version (if \( p \) is counted as unary in the input size).

- If there is such a point:
- Cover the space with \( p + 1 \) hyperplanes:
  \( H_i = \{[i, 1, *, \ldots, *]\} \) (\( i = \{0, \ldots, p - 1\} \)),
  \( H_\infty = \{[1, 0, *, \ldots, *]\} \).
- Find \( i \) s.t. \( H_i \) contain the point
- descend to \( H_i \)
Hyperplane cover and polynomials 1.

\[ u \cdot w \neq 0 \iff (u \cdot w)^{p-1} = 1 \]

\[ f(x) = f(x_1, \ldots, x_n) = (u \cdot x)^{p-1} - 1 = (\sum_{i=1}^{n} u_i x_i)^{p-1} - 1: \]

polynomial in \( x = x_1, \ldots, x_n \) of degree at most \( p - 1 \).

Reformulation of Hyperplane cover

- either uniform distribution
- or \( \exists \) a nonzero polynomial \( f \in \mathbb{Z}_p[x] = \mathbb{Z}_p[x_1, \ldots, x_n] \) of total degree at most \( p - 1 \) such that \( \text{Prob}(w) = 0 \) for every \( w \) which is not a zero of \( f \).
Hyperplane cover and polynomials 1.

1. $L = \{ g \in \mathbb{Z}_p[x] \mid \deg g \leq p - 1 \}$ vector space of dimension $O((n + p)^{p-1})$.

2. For $w \in \mathbb{Z}_p^n$, $S_w : L \rightarrow \mathbb{Z}_p$ linear function defined as $S_w(g) = g(w)$

3. For $w_1, \ldots, w_j \in \mathbb{Z}_p^n$, $K = K(w_1, \ldots, w_j) = \{ g \in L \mid g(w_1) = \ldots = g(w_j) = 0 \}$ subspace of $L$:

$$K = \bigcap_{i=1}^{j} \ker S_{w_i}$$
Cosequence of Schwartz-Zippel lemma

\( w_1, \ldots, w_j \in \mathbb{Z}_p^n, \ K = \{ g \in L | g(w_1) = \ldots = g(w_j) = 0 \} \).
Assume that \( K \neq 0 \). Then
\[ \text{Prob}_{w \in \mathbb{Z}_p^n} (g(w) = 0 \text{ for every } g \in K) \leq \frac{p-1}{p}. \]
(Let \( 0 \neq g \in K \). Then \( \text{Prob}_{w} (g(w) = 0) \leq \frac{p-1}{p} \).)

Conclusion

When \( \ell = O(p \dim L) = O(p(n + p)^{p-1}) \),
- in the uniform case \( K_{w_1, \ldots, w_\ell} = 0 \) with high prob.
- Otherwise \( K_{w_1, \ldots, w_\ell} \) never 0.
Hyperplane cover - the algorithm

- \( \ell = O(p \dim L) \), take sample \( w_1, \ldots, w_\ell \).
- Compute \( K = \{ g \in L | g(w_1) = \ldots = g(w_\ell) = 0 \} \).
  - System of linear equations in the coefficients of \( g \).
- If \( K = 0 \): uniform; If \( K \neq 0 \): there exists \( u \).
- Costs: Polynomial in \( p \dim L = O(p(n + p)^{p-1}) \).
Hidden shift in $\mathbb{Z}_p^k$ - conclusion

- Hyperplane cover can be solved classically in time $poly(n^p)$.
- Quantum algorithm for hidden shift in $\mathbb{Z}_p^n$ of complexity $poly(n^p)$.
- No need of measurement, works with "quantum" functions.
- Open: method of complexity $poly(n + p)$?
Remarks on Hyperplane cover

- Method can be generalized to $\mathbb{Z}_{p^k}^n$. Costs: $poly(n^{p^k})$.
- Open: any method polynomial in $n$ for $\mathbb{Z}_{pq}^n$ ($p, q$ distinct small primes)? Already for $\mathbb{Z}_6^n$.