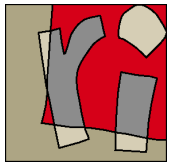


An efficient quantum algorithm for the Hidden Translation Problem

Miklos Santha

MSRI, LRI (Orsay)

ongoing work with

Katalin Friedl — SZTAKI (Budapest)

Frédéric Magniez — MSRI, LRI (Orsay)

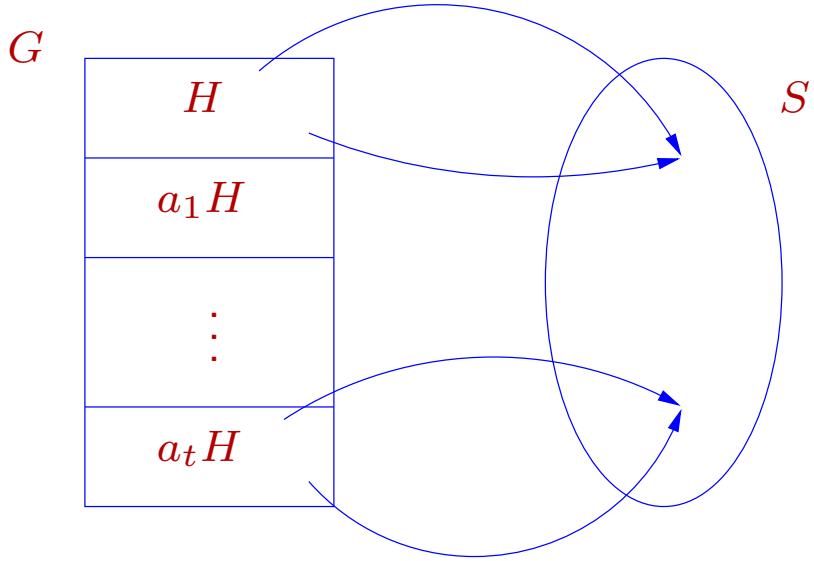
Pranab Sen — LRI (Orsay)

Hidden Subgroup Problem (HSP)

Input: G finite group, and $f : G \to S$ hiding $H \leq G$:

$\forall x \in G, h \in H, f(x) = f(xh)$ and $\forall x, y \in G,\ xH \neq yH \implies f(x) \neq f(y)$.

Output: Generators for H.



Theorem: HSP can be solved in quantum $\mathrm{poly}(\log|G|)$-time when

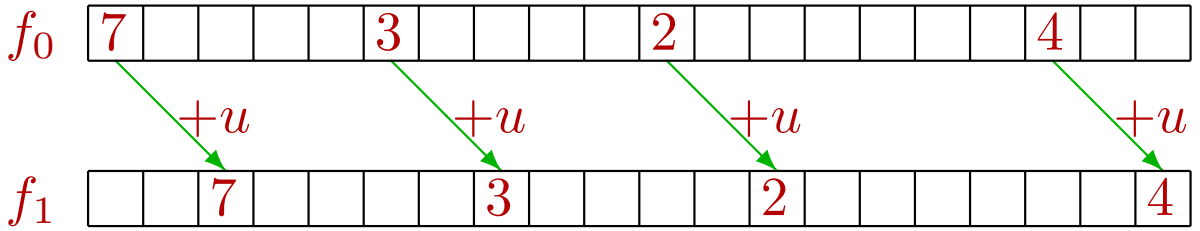
- G is Abelian
- $G = \mathbb{Z}_2^k \wr \mathbb{Z}_2$ [Roetteler,Beth'98]
- H is normal and QFT_G is available [Hallgren,Russell,Ta-Shma'00]
- H is normal and G is solvable [Ivanyos,Magniez,Santha'01]
- $\cap\{N(H) \ : H \leq G\}$ is large [Grigni,Schulman,Vazirani,Vazirani'01]
- $G = \mathbb{Z}_n \rtimes \mathbb{Z}_2$ with exponential postprocessing [Ettinger,Høyer'00]
- $G = \mathbb{Z}_p^n \rtimes \mathbb{Z}_2$ for fixed prime p.

Input: G finite Abelian group.

$f_0, f_1 : G \to S$ injective functions having a translation $u \in G$:

$$\forall x \in G, \quad f_0(x) = f_1(x+u).$$

Output: u.



Theorem. [Ettinger-Høyer'00]. If G finite Abelian group then

HTP on $G \simeq$ HSP on $G \rtimes \mathbb{Z}_2$.

Group operation on $G \rtimes \mathbb{Z}_2$: $(x_1, b_1) \cdot (x_2, b_2) = (x_1 + (-1)^{b_1} x_2, b_1 \oplus b_2)$.

Fact. $f(x, b) = f_b(x)$ hides $H = \{(0,0); (u,1)\}$ on $G \rtimes \mathbb{Z}_2$.

Theorem. For every prime p, HTP can be solved on $\mathbb{Z}_p^n$ by a quantum algorithm with query complexity $O(p(n+p)^{p-1})$ and time complexity $(n+p)^{O(p)}$.

Idea of [EH'00]: Apply QFT on the direct product $\mathbb{Z}_p^n \times \mathbb{Z}_2$.

State: $$\frac{1}{2p^n} \sum_{x \in \mathbb{Z}_p^n} \sum_{b=0}^{1} \sum_{y \in \mathbb{Z}_p^n} \sum_{c=0}^{1} \omega_p^{x \cdot y} (-1)^{bc} |y\rangle |c\rangle |f_b(x)\rangle$$

Rewrite using the hidden translation:

$$\frac{1}{2p^n} \sum_{x \in \mathbb{Z}_p^n} \sum_{y \in \mathbb{Z}_p^n} \sum_{c=0}^{1} \left(\omega_p^{x \cdot y} + \omega_p^{(x+u) \cdot y} (-1)^c\right) |y\rangle |c\rangle |f_0(x)\rangle$$

For all x, y the amplitude of $|y\rangle|1\rangle|f_0(x)\rangle$ is:

$$\frac{1}{2p^n} \omega_p^{x \cdot y} (1 - \omega_p^{y \cdot u})$$

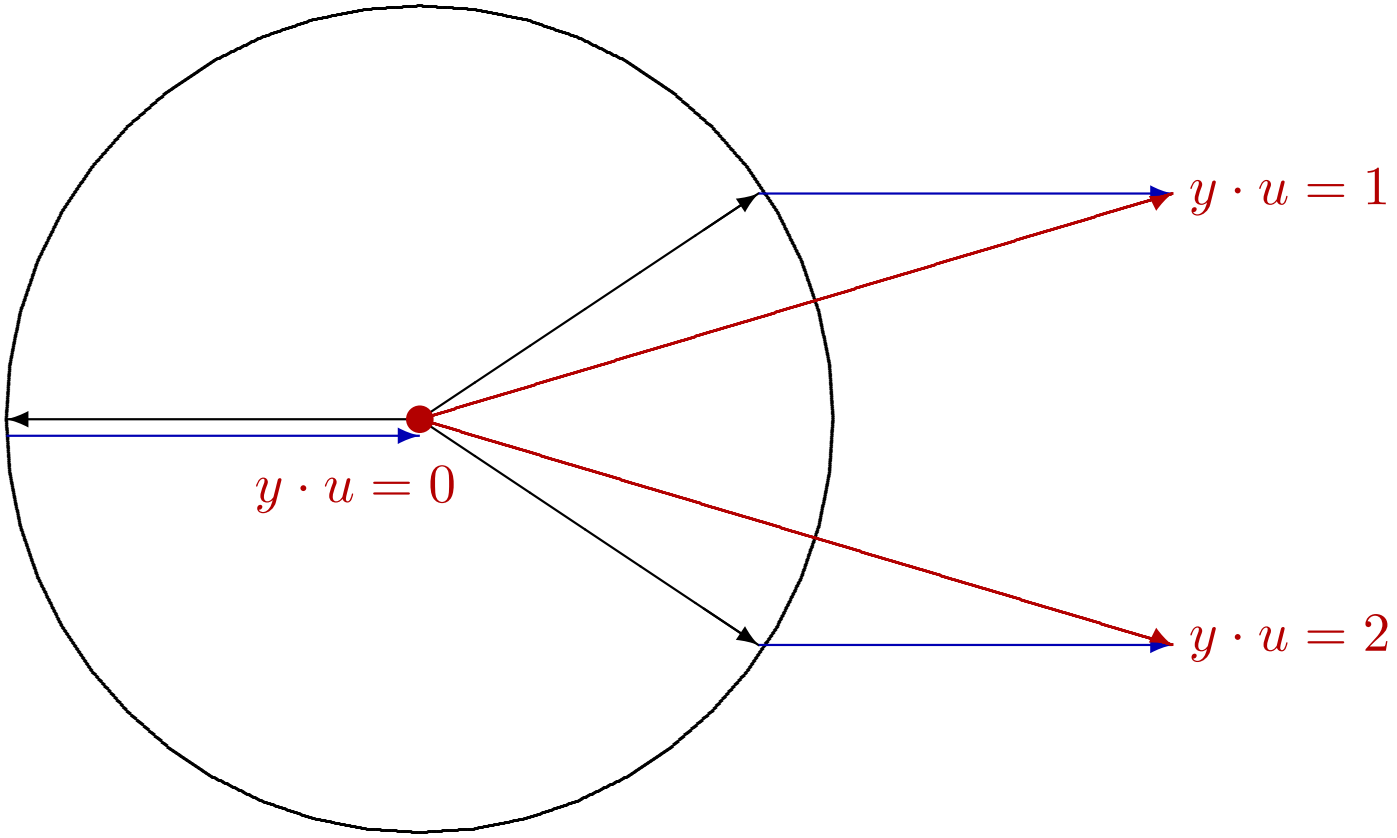
After observation:

$$\Pr[\text{output} = (y, 1)] = \frac{1}{4p^{2n}} |1 - \omega_p^{y \cdot u}|^2.$$

Properties of the output distribution:

- $\Pr[c = 1] = \frac{1}{2}$
- depends only on $y \cdot u$
- for every $(y, 1)$ observed: $y \cdot u \neq 0 \mod p$.

Drawing $\boxed{1-\omega_3^{y\cdot u}}$:



Sample $(y, 1)$ such that $y \cdot u \neq 0 \mod p$ (*i.e.* $y \notin u^{\perp}$)

Linear non-equations $\mapsto$ polynomial equations

$$y \cdot u \neq 0 \mod p \iff (y \cdot u)^{p-1} = 1 \mod p$$

Fact. Solving polynomial equations is NP-complete.

Idea: 'Linearize' the system in the symmetric power of $\mathbb{Z}_p^n$

Definition. $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ is the vector space of homogeneous polynomials in n-variables of degree $(p-1)$ over $\mathbb{Z}_p$.

- A basis: Monomials of degree $(p-1)$
- Dimension: $\binom{n+p-2}{p-1}$

Transfer from $\mathbb{Z}_p^n$ via $(\mathbb{Z}_p^n)^*$ to $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$:

Definition. For $y = (a_1, \ldots, a_n) \in \mathbb{Z}_p^n$ let $y^{(p-1)} = (\sum_j a_j x_j)^{p-1}$.

$$y \cdot u \neq 0 \mod p \implies y^{(p-1)} \cdot u^* = (y \cdot u)^{p-1} = 1 \mod p,$$

where in $u^* \in \mathbb{Z}_p^n$ the monomial $x_1^{e_1} \cdots x_n^{e_n}$ has coordinate $u_1^{e_1} \cdots u_n^{e_n}$.

End of the algorithm:

- Hopefully the linear system in $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ has unique solution
- Find the solution $U = u^*$
- Try the $(p-1)$ candidates v such that $v^* = u^*$

Example. $p = 3$, $n = 3$, $u = (1, 2, 0)$.

Sample in $\mathbb{Z}_3^3$	Non-equation	Equation in $\mathbb{Z}_3^{(2)}[x_1, x_2, x_3]$
$y_1 = (0, 1, 0)$	$x_2 \cdot u \neq 0$	$x_2^2 \cdot U = 1$
$y_1 = (0, 2, 1)$	$(2x_2 + x_3) \cdot u \neq 0$	$(x_2^2 + x_3^2 + 2x_2x_3) \cdot U = 1$
$y_1 = (0, 2, 2)$	$(2x_2 + 2x_3) \cdot u \neq 0$	$(x_2^2 + x_3^2 + x_2x_3) \cdot U = 1$
$\vdots$	$\vdots$	$\vdots$

where $x_1 = (1, 0, 0)$, $x_2 = (0, 1, 0)$, $\ldots$, $x_1^2 = (1, 0, 0, 0, 0, 0)$, $\ldots$

System of full rank $\implies$ unique solution $U = x_1^2 + x_2^2 + 2x_1x_2$.
Try the 2 possible translations $(1, 2, 0)$ and $(2, 1, 0) \rightsquigarrow u = (1, 2, 0)$.

Translation finding$^f(\mathbb{Z}_p^n)$

0. If $f_0(0) = f_1(0)$ then return 0.
1. $N \leftarrow 13p\binom{n+p-2}{p-1}$.

2. For $i = 1, \ldots, N$ do $(z_i, b_i) \leftarrow$ **Fourier sampling**$^f(\mathbb{Z}_p^n \times \mathbb{Z}_2)$.
3. $\{y_1, \ldots, y_m\} \leftarrow \{z_i : b_i = 1\}$.

4. For $i = 1, \ldots, m$ do $Y_i \leftarrow y_i^{(p-1)}$.
5. Solve $Y_1 \cdot U = 1, \ldots, Y_m \cdot U = 1$.
6. If several solutions then abort.

7. Let j be such that the coefficient of x_j^{p-1} in U is 1.
8. Let $v \in \mathbb{Z}_p^n$ be such that $v_k v_j$ is the coefficient of $x_k x_j^{p-2}$ in U.

9. Find $0 < a < p$ such that $f_0(0) = f_1(av)$.
10. Return av.

Line Lemma. Let $L_{z,y} = \{(z+ay)^{(p-1)} : 0 \le a \le p-1\}$ for $y, z \in \mathbb{Z}_p^n$. Then $y^{(p-1)} \in \mathrm{Span}(L_{z,y})$.

Proof. Let $M_{z,y} = \{\binom{p-1}{k} z^{(k)} y^{(p-1-k)} : 0 \le k \le p-1\}$.

Claim: $\mathrm{Span}(L_{z,y}) = \mathrm{Span}(M_{z,y})$.

	$z^{(p-1)}$	$(z+y)^{(p-1)}$	$(z+2y)^{(p-1)}$	$\dots$	$(z+(p-1)y)^{(p-1)}$
$\binom{p-1}{0} z^{(p-1)}$	1	1	1	$\dots$	1
$\binom{p-1}{1} z^{(p-2)} y^{(1)}$	0	1	2	$\dots$	$(p-1)$
$\binom{p-1}{2} z^{(p-3)} y^{(2)}$	0	1	2^2	$\dots$	$(p-1)^2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
$\binom{p-1}{p-1} y^{(p-1)}$	0	1	$(p-1)^2$	$\dots$	$(p-1)^{(p-1)}$

Corollary. $\mathbb{Z}_p^{(p-1)}[x_1, \dots, x_n]$ is spanned by $\{y^{(p-1)} : y \in \mathbb{Z}_p^n\}$.

Lemma. Let $W \leq \mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ and $R = \{y \in \mathbb{Z}_p^n : y^{(p-1)} \in W\}$.
Set $V_k = \{y \in \mathbb{Z}_p^n : y \cdot u = k\}$, and $R_k = R \cap V_k$.
If $W \neq \mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ then $\frac{|R_k|}{|V_k|} \leq \frac{p-1}{p}$ for $k = 1, \ldots, p-1$.

Proof. Corollary $\implies R \neq \mathbb{Z}_p^n$.

Case 1: $R_0 = V_0$. Then $R_k \neq V_k$ for $k = 1, \ldots, p-1$. Let $y \in V_1 - R_1$.

Line Lemma $\implies$ in each coset of $<y>$ an element is outside R.

	$<y>$	$\ldots$	$z + <y>$	$\ldots$
V_0	0	$\ldots$	z	$\ldots$
V_1	y	$\ldots$	$z+y$	$\ldots$
$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$
V_{p-1}	$(p-1)y$	$\ldots$	$z+(p-1)y$	$\ldots$

$\implies \frac{|R|}{|Z_p^n|} \leq \frac{p-2}{p-1} \implies \frac{|R_k|}{|V_k|} \leq \frac{p-2}{p-1}$.

Case 2: $R_0 \neq V_0$. Let $y \in V_0 - R_0$, then V_k is union of cosets of $<y>$.

Line Lemma $\implies \frac{|R_k|}{|V_k|} \leq \frac{p-1}{p}$.