Hidden Translation and Orbit Coset in Quantum Computing

Miklos Santha

MSRI, LRI (Orsay)

joint work with

Katalin Friedl	SZTAKI (Budapest)
Gábor Ivanyos	SZTAKI (Budapest)
Frédéric Magniez	LRI (Orsay)
Pranab Sen	LRI (Orsay)

Structure of the talk

- HIDDEN TRANSLATION

  Efficient quantum algorithm in elementary Abelian groups

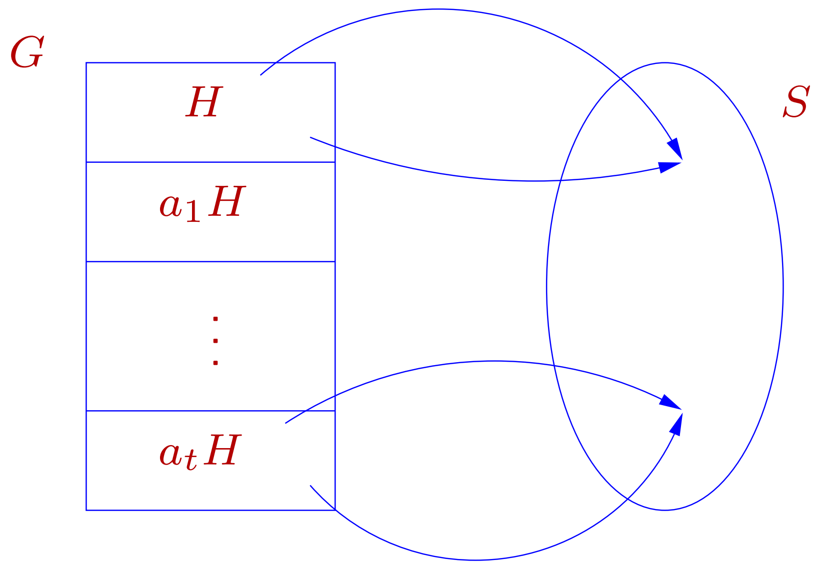
- ORBIT COSET

  Efficient recursive quantum algorithm in smoothly solvable groups

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

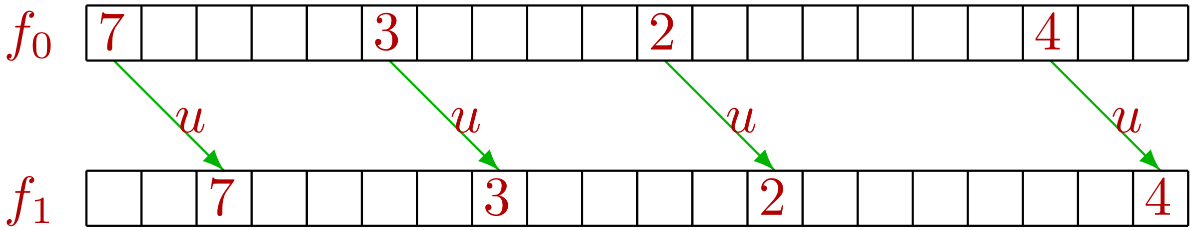
- $G = \mathbb{Z}_2^k \wr \mathbb{Z}_2$ [Roetteler,Beth'98]
- H is normal and QFT_G is available [Hallgren,Russell,Ta-Shma'00]
- H is normal and G is solvable [Ivanyos,Magniez,Santha'01]
- $\cap\{N(H) \ : H \leq G\}$ is large [Grigni,Schulman,Vazirani,Vazirani'01]
- $G = \mathbb{Z}_p \rtimes \mathbb{Z}_q$ when $q = \frac{p-1}{(\log p)^c}$ [Moore,Rockmore,Russell,Schulman'02]
- $G = \mathbb{Z}_n \rtimes \mathbb{Z}_2$ with exponential postprocessing [Ettinger,Høyer'00]
- $G = \mathbb{Z}_p^n \rtimes \mathbb{Z}_2$ for fixed prime p

Input: G finite group.

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

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

Output: u.



Theorem. [Ettinger-Høyer'00]. If G finite Abelian group then HIDDEN TRANSLATION on $G \simeq$ HIDDEN SUBGROUP 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, HIDDEN TRANSLATION 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: $\quad y \cdot u \neq 0 \mod p$.

The algorithm: Part 2 (classical postprocessing)

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

Linear inequations $\mapsto$ 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 $\mathbb{Z}_3^3$	Inequation in $\mathbb{Z}_3^3$	Equation in $\mathbb{Z}_3^{(2)}[x_1, x_2, x_3]$
$y_1 = (0, 1, 0)$	$x_2 \cdot u \neq 0$	$x_2^2 \cdot U = 1$
$y_2 = (0, 2, 1)$	$(2x_2 + x_3) \cdot u \neq 0$	$(x_2^2 + x_3^2 + x_2 x_3) \cdot U = 1$
$y_3 = (0, 2, 2)$	$(2x_2 + 2x_3) \cdot u \neq 0$	$(x_2^2 + x_3^2 + 2x_2 x_3) \cdot U = 1$
$\vdots$	$\vdots$	$\vdots$

where $x_1 = (1, 0, 0)$, $x_2 = (0, 1, 0)$, $x_3 = (0, 0, 1)$,
$x_1^2 = (1, 0, 0, 0, 0, 0)$, $\ldots$

System of full rank $\Longrightarrow$ unique solution $U = x_1^2 + x_2^2 + 2x_1 x_2$.

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

Proof. Let $M_{z,y} = \{\binom{p-1}{k} z^{(k)} y^{(p-1-k)} : 0 \leq k \leq p-1\}$.
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 $\implies \frac{|R_k|}{|V_k|} \leq \frac{p-1}{p}$.

G a finite group given by generators

Elements are encoded in $\{0,1\}^n$ where $n = O(\log |G|)$

Group operations are performed by oracles

For G solvable, the derived series is computable in probabilistic polynomial time [Babai et al.'95]

$$G = G^{(0)} \rhd G^{(1)} \rhd \ldots \rhd G^{(m)} = \{1_G\}$$

For G solvable, the composition series is computable in quantum polynomial time [Watrous'01] [Ivanyos et al.'01]

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_m = \{1_G\}$$

where $|G_i/G_{i+1}|$ is prime

G finite group, Γ mutually orthogonal quantum states

Action of G on Γ is a homomorphism

$$\begin{array}{rcl} \alpha \ : \ G & \rightarrow & \mathrm{Perm}(\Gamma) \\ x & \mapsto & \alpha_x \end{array}$$

Notation. $\alpha_x(|\varphi\rangle) = |x \cdot \varphi\rangle$

Oracle for a group action : $|x\rangle|\varphi\rangle \mapsto |x\rangle|x \cdot \varphi\rangle$

Example 1. For $t \geq 1$, α^t is an action on $\Gamma^t = \{|\varphi\rangle^{\otimes t} : |\varphi\rangle \in \Gamma\}$

$$\alpha^t_x \ : \ |\varphi\rangle^{\otimes t} \mapsto |x \cdot \varphi\rangle^{\otimes t}$$

Example 2. Let $f \ : \ G \rightarrow S$ a hiding function,

$$|f\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle.$$

The y-translate of f is $y \cdot f : g \mapsto f(gy)$

$$\Gamma(f) = \{|y \cdot f\rangle : y \in G\}$$

.

The translation action on $\Gamma(f)$ is $\tau_x \ : \ |f'\rangle \mapsto |x \cdot f'\rangle$

Oracle for $f \implies$ oracle for the translation action :

$$|x\rangle|x \cdot f'\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |x\rangle|g\rangle|f'(gx)\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |x\rangle|gx^{-1}\rangle|f'(g)\rangle$$

The stabilizer of $|\varphi\rangle$ is $G_{|\varphi\rangle} = \{x \in G : |x \cdot \varphi\rangle = |\varphi\rangle\}$.

The orbit of $|\varphi\rangle$ is $G(|\varphi\rangle) = \{|x \cdot \varphi\rangle, x \in G\}$.

The orbit coset of $|\varphi_0\rangle$ and $|\varphi_1\rangle$ is $\{u \in G : |u \cdot \varphi_1\rangle = |\varphi_0\rangle\}$.

The orbit coset is empty or a left coset $uG_{|\varphi_1\rangle}$.

STABILIZER

Input: $G, \alpha, \Gamma, |\varphi\rangle$.

Output: $G_{|\varphi\rangle}$

ORBIT COSET

Input: $G, \alpha, \Gamma, |\varphi_0\rangle, |\varphi_1\rangle$.

$$\text{Output: } \begin{cases} \texttt{reject}, & \text{if } G(|\varphi_0\rangle) \cap G(|\varphi_1\rangle) = \emptyset; \\ u \in G \text{ s.t. } |u \cdot \varphi_1\rangle = |\varphi_0\rangle \text{ and generators for } G_{|\varphi_1\rangle}, & \text{ow.} \end{cases}$$

Theorem. When $t = \text{poly}(\log|G|)$ then for the translation action τ^t

- HIDDEN SUBGROUP $\leq$ STABILIZER
- HIDDEN TRANSLATION $\leq$ ORBIT COSET

Proof. The subgroup hidden by f is the stabilizer of $|f\rangle$. The translation of (f_0, f_1) is the orbit coset of $(|f_0\rangle, |f_1\rangle)$.

Theorem. Let G Abelian. When $t = \Omega(\log(|G|)$, STABILIZER for α^t is solvable in quantum time $\mathrm{poly}(\log|G|)$.

Proof. On input $|\varphi\rangle^{\otimes t}$ let $f(x) = |x \cdot \varphi\rangle$. Then f hides $G_{|\varphi\rangle}$. Run the algorithm for HIDDEN SUBGROUP, simulating the i^{th} query $|x\rangle|0\rangle_S$ using the i^{th} copy of $|\varphi\rangle$.

Theorem. Let $G = \mathbb{Z}_p^n$. When $t = \Omega(p(n+p)^{p-1})$, ORBIT COSET for α^t is solvable in quantum time $(n+p)^{O(p)}$.

Proof. One can suppose w.l.o.g. that the stabilizers of the input $|\varphi_0\rangle^{\otimes t}$, $|\varphi_1\rangle^{\otimes t}$ are trivial. Let $f_b(x) = |x \cdot \varphi_b\rangle$. Then the translation of (f_0, f_1) is the orbit coset of $(|\varphi_0\rangle, |\varphi_1\rangle)$. Run the algorithm **Translation finding**.

Idea. Let $N \lhd G$. Given PROBLEM on G, establish self-reducibility

$$\text{PROBLEM}(G) \leq \{\text{PROBLEM}(N), \text{PROBLEM}(G/N)\}$$

Definition. Orbit superposition

$$|N \cdot \varphi\rangle = \frac{1}{\sqrt{|N(|\varphi\rangle)|}} \sum_{|\varphi'\rangle \in N(|\varphi\rangle)} |\varphi'\rangle$$

Definition. Factor group action

$$\Gamma_N = \{|N \cdot \varphi\rangle : |\varphi\rangle \in \Gamma\}$$

$$\begin{array}{rcl} \alpha_N \; : \; G/N & \rightarrow & \text{Perm}(\Gamma_N) \\ xN & \mapsto & \alpha_{N,x} \end{array}$$

$$\alpha_{N,x}(|N \cdot \varphi\rangle) = |x \cdot (N \cdot \varphi)\rangle$$

How to create the orbit superposition $|N \cdot \varphi\rangle$?

Theorem. G solvable. Given $|\varphi\rangle^{\otimes(s+\lfloor\log|G|\rfloor+1)}$, realizing $|\varphi\rangle|G\cdot\varphi\rangle^{\otimes s}$ is reducible to ORBIT COSET in subgroups of G for α.

Proof. Let $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_m = \{1_G\}$ where G_n/G_{n+1} is cyclic of prime order r_n and is generated by $z_n G_{n+1}$.

For $n = m$ downto 0, produce the state $|\varphi\rangle|G_n \cdot \varphi\rangle^{\otimes(s+n)}$.

Induction step. Set $k = s+n+1$. Given $|\varphi\rangle|G_{n+1}\cdot\varphi\rangle^{\otimes k}$

- Compute k copies of $\frac{1}{\sqrt{r_n}}\sum_{i=0}^{r_n-1}|i\rangle|z_n^i\cdot(G_{n+1}\cdot\varphi)\rangle$
- Disentangle the first registers by the method of Watrous

QFT: $(\frac{1}{\sqrt{r_n}}\sum_{j=0}^{r_n-1}|j\rangle|\psi_j\rangle)^{\otimes k}$ where $|\psi_j\rangle = \frac{1}{\sqrt{r_n}}\sum_{i=0}^{r_n-1}\omega_{r_n}^{ij}|z_n^i\cdot(G_{n+1}\cdot\varphi)\rangle$.

Suppose $j_0 \neq 0$. Then $|(z_n^i g)^{jj_0^{-1}}\cdot\psi_{j_0}\rangle = \omega_{r_n}^{-ij}|\psi_{j_0}\rangle$ for $g \in G_{n+1}$.

ORBIT COSET on $|\varphi\rangle$ and $|z_n^i g\cdot\varphi\rangle$ gives $z_n^i g$.

Theorem. Let $N \lhd G$, N solvable. When $t = \Omega(s + \log|G|)$

- OC(G, α^t) $\leq$ $\{$ OC(Subgroups of N, α), OC$(G/N, (\alpha_N)^s)$ $\}$
- STAB(G, α^t) $\leq$ $\{$ OC(Subgroups of N, α), STAB$(G/N, (\alpha_N)^s)$ $\}$

Proof for STABILIZER.

Compute $N_{|\varphi\rangle} = G_{|\varphi\rangle} \cap N$ by STAB(N, α).

Construct $H \leq G$ such that

$$N_{|\varphi\rangle} \leq H \leq G_{|\varphi\rangle} \text{ and } HN/N = G_{|\varphi\rangle}N/N.$$

Then $H = G_{|\varphi\rangle}$ since $H \cap N = G_{|\varphi\rangle} \cap N$ and $HN/N = G_{|\varphi\rangle}N/N$.

Add to $N_{|\varphi\rangle}$ generators of $G_{|\varphi\rangle}N/N$ which are in $G_{|\varphi\rangle}$

Fact. $G_{|\varphi\rangle}N/N$ is the stabilizer of $|N \cdot \varphi\rangle$ in G/N.

- Compute V such that $\langle V \rangle = G_{|\varphi\rangle}N/N$ by STAB$(G/N, (\alpha_N)^s)$
- Create input $|N \cdot \varphi\rangle^{\otimes s}$ by OC(N, α)
- Let $z \in V$. Then $z = gn^{-1}$ for $g \in G_{|\varphi\rangle}$ and $n \in N$. In N the orbit coset of $|z^{-1}\varphi\rangle$ and $|\varphi\rangle$ is $nN_{|\varphi\rangle}$. Find n by OC(N, α).

Definition. A solvable group is smoothly solvable if it is of bounded exponent and its derived series is of bounded length.

Fact. A smoothly solvable group G has a smooth series

$$G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_m = \{1_G\}$$

where m bounded and G_i/G_{i+1} is elementary Abelian of bounded exponent.

Theorem. Let G smoothly solvable. When $t = \log^{\Omega(1)}|G|$ then ORBIT COSET can be solved for α^t in quantum time $\mathrm{poly}(\log|G|)$.

Theorem. Let G solvable such that G' is smoothly solvable. When $t = \log^{\Omega(1)}|G|$ then STABILIZER can be solved for α^t in quantum time $\mathrm{poly}(\log|G|)$.

Corollary There is a quantum polynomial time algorithm for

- HIDDEN TRANSLATION in smoothly solvable groups
- HIDDEN SUBGROUP in solvable groups having a smoothly solvable commutator subgroup