GROUPS AND PROBABILTY

June 30–July 4, Budapest

Quantum algorithms for groups

Katalin Friedl

&

Gábor Ivanyos

MTA SZTAKI (Budapest)

BABAI-BEALS 1993

G a black box group without "large" composition factors of Lie type $\Rightarrow$

We can compute "the structure" of G in polynomial time using oracles for

- computing and factoring $|g|$ for $g \in G$
- solving discrete log in $GL(\mathbb{F}_p)$
- testing memberhsip effectively in abelian subgroups of G

These tasks can be solved efficiently on quantum computers (if the encoding is unique).

HIDDEN SUBGROUP

Input: G (finite) group,
$f : G \to S$ 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.

Examples:

Order finding: $G = \mathbb{Z}$, $f(z) = u^z$
(u from a group,
e.g, from $\mathbb{Z}_n^*$ for factoring n)

Discrete log: $G = \mathbb{Z} \times \mathbb{Z}$, $f(y, z) = u^y v^{-z}$,
(u, v from a group, want x: $u^x = v$)

Abelian membership test: $G = \mathbb{Z}^n \times \mathbb{Z}$
$f(y_1, \ldots, y_n, z) = u_1^{y_1} \cdots u_n^{y_n} \cdot v^{-z}$,
(want $x_1, \ldots, x_n$: $u_1^{x_1} \cdots u_n^{x_n} = v$)

Graph automorphisms: $G = S_n$,
$f(\pi) =$ graph Γ permuted by π

ABELIAN FOURIER TRANSFORM

$$|g\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{\chi \in G^*} \chi(g)|\chi\rangle$$

$$\sum_{g \in G} \alpha_g |g\rangle$$

$$\downarrow$$

$$\frac{1}{\sqrt{|G|}} \sum_{\chi \in G^*} \sum_{g \in G} \alpha_g \chi(g)|\chi\rangle$$

ABELIAN HIDDEN SUBGROUP

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle\otimes|*\rangle$$

$$\downarrow$$

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

$$= \frac{1}{\sqrt{|G|}}\sum_{y}\sum_{h\in H}|g_y h\rangle\otimes|y\rangle$$

$$\downarrow (\textbf{Fourier})$$

$$\frac{1}{|G|}\sum_{y}\sum_{\chi\in G^*}\Big(\sum_{h\in H}\chi(g_y h)\Big)|\chi\rangle\otimes|y\rangle =$$

$$= \frac{|H|}{|G|}\sum_{y}\left\{\begin{array}{ll}\chi(g_y) & \text{if } \chi_{|H}=1\\ 0 & \text{otherwise}\end{array}\right\}|\chi\rangle\otimes|y\rangle$$

Noncommutative results:

HIDDEN SUBGROUP can be solved in quantum 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 involves no
 large composition factors of Lie type,
 e.g., G is solvable or $G \leq S_n$
 [*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*]

– $G = \mathbb{Z}_n \rtimes \mathbb{Z}_2$ + exponential postprocessing
 [*[Ettinger,Høyer'00]*]

Friedl, Ivanyos, Magniez, Santha, Sen 2003, :

HIDDEN SUBGROUP can be solved in quantum poly(log|G|)-time when
– G is a solvable group of bounded length &
– G' has bounded exponent:

$\exists$ constants c_1, c_2 and subnormal subgroups

$$G' = N_0 \rhd N_1 \cdots \rhd N_{c_1-1} \rhd N_{c_1} = \{1\}$$

s.t.

$$N_{i-1}/N_i \cong \mathbb{Z}_{p_i}^{n_i} \qquad (p_i \text{ prime, } p_i \le c_2)$$

Example: triangle matrix groups of constant degree and constant characteristic

$$G \le \begin{pmatrix} \mathbb{F}_q^* & \mathbb{F}_q & \mathbb{F}_q \\ 0 & \mathbb{F}_q^* & \mathbb{F}_q \\ 0 & 0 & \mathbb{F}_q^* \end{pmatrix}$$

($q =$ power of a fixed prime)

IDEA (illustration)

$G \subseteq S_\Omega$, e.g, $\Omega = \{$graphs on n points$\}$
$\omega_0, \omega_1 \in \Omega$

$$\exists g \in G \text{ s.t. } \omega_1 = \omega_0^g$$
$$\Updownarrow$$
$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |\omega_0^g\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |\omega_1^g\rangle$$

Otherwise

$$\langle \frac{1}{\sqrt{|G|}} \sum_{g \in G} |\omega_0^g\rangle, \frac{1}{\sqrt{|G|}} \sum_{g \in G} |\omega_1^g\rangle\rangle = 0$$

Two problems:

– testing equality of these states
– computing $\frac{1}{\sqrt{|G|}} \sum_{g \in G} \omega^g$

QUANTUM STATE EQUALITY TEST: Given (sufficiently many copies of) two quantum states (unit vectors) ψ_1, ψ_2 s.t. either $\psi_1 = \psi_2$ or $\langle \psi_1, \psi_2 \rangle = 0$ decide which is the case

SWAP TEST:

$$|0\rangle \otimes \psi_1 \otimes \psi_2$$
$$\downarrow$$
$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \psi_1 \otimes \psi_2$$
$$\downarrow$$
$$\frac{1}{\sqrt{2}}(|0\rangle \otimes \psi_1 \otimes \psi_2 + |1\rangle \otimes \psi_2 \otimes \psi_1)$$

$\sim$ HIDDEN SUBGROUP on $\mathbb{Z}_2$, but "quantum state valued".

ORBIT SUPERPOSITION

$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|\omega^g\rangle$ difficult

Easy: $\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle\otimes\omega^g$

How to "forget" $|g\rangle$ from $|g\rangle\otimes|\omega^g\rangle$?
Assume that G is (semi-)regular and there is an efficient algorithm for finding g s.t. $\omega=\omega_0^g$:

$$U : |\omega_0\rangle|1\rangle\otimes|\omega_0^g\rangle \mapsto |\omega_0\rangle|g\rangle\otimes|\omega_0^g\rangle$$

Then:

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|\omega_0\rangle\otimes|g\rangle\otimes|\omega^g\rangle$$
$$\downarrow U^{-1}$$
$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|\omega_0\rangle\otimes|1\rangle\otimes|\omega^g\rangle$$

HIDDEN TRANSLATION

$\sim$ finding g from ω_0, ω_0^g

Given injective functions f_0, f_1 on G s.t. either $f_1(g) = f_0(ug)$ form some x or $Range(f_1) \cap Range(f_0) = 0$, decide, which is the case and find u.

Remark. [*Ettinger-Høyer'00]*. For a finite abelian G HIDDEN TRANSLATION in $G \Leftrightarrow$ HIDDEN SUBGROUP in $G \rtimes \mathbb{Z}_2$.

Theorem.
For 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 $(n+p)^{O(p)}$.

The algorithm for HIDDEN TRANSLATION in $\mathbb{Z}_p^n$: Part 1 (quantum)

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

State:

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

Rewrite using the hidden translation:

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

For all x, y the coeff. of $|y\rangle \otimes |1\rangle \otimes |f_0(x)\rangle$ 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:

– depends only on $y \cdot u$
– for every $(y, 1)$ observed: $\quad y \cdot u \neq 0 \mod p$.

Decision version: Decide if f_1 is a translate of f_0: distinguish a distribution of the above type from the uniform one.

Search for u is similar.

Part 2 (classical postprocessing)

We consider observed values of type $(y, 1)$

$\exists$ hidden translation $u \implies$

$\exists\ P \in \mathbb{F}_p[x_1, \ldots, x_n]$

$\deg P \leq p - 1$

$P(y) = 0$ for every observed $(y, 1)$

$$P(x) = (x \cdot u)^{p-1} - 1$$

disjoint ranges (uniform distr) +

many observations $y_1, \ldots, y_N \implies$

$$P(y_1) = 0$$
$$\vdots$$
$$P(y_N) = 0$$

with high probability

a system of lin. eqn's

(in the coeff's of P)

with solution only 0.

Iterateting
the HIDDEN TRANSLATION (and some variants)
$\rightarrow$ a solution of the HIDDEN SUBGROUP in solvable G of constant length with G' of constant exponent...

Remarks, Questions

Solution for HIDDEN TRANSLATION in $\mathbb{Z}_p^n$ is exponential in p: Is there a method polynomial in p (or even in $\log p$)?

Is there a direct method
for HIDDEN TRANSLATION in $\mathbb{Z}_k^n$? For prime power k we know one. For $k = 6$ or $k = 15$???