An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups.

Gábor Ivanyos [1] Luc Sanselme [2] Miklos Santha [2]

SZTAKI, Hungarian Academy of Sciences, H-1111 Budapest, Hungary.

Univ Paris-Sud, CNRS, LRI, UMR 8623, Orsay, F-91405

March 4, 2007

The Hidden subgroup problem (HSP).

The problem

- *Input*
  - *A finite group* G
  - *A hiding function* $f : G \to S$ *which hides* $H \leq G$ ($f(x) = f(y) \Leftrightarrow xH = yH$).
- *Output*
  - *Generators for* H.

Theorem (Shor'94)

If G *is Abelian then there is an efficient quantum algorithm using Fourier sampling and classical postprocessing:*

- *which finds* H *with probability* $\geq 1 - 1/|G|$,
- *in polynomial time in* $\log|G|$.

Extraspecial groups.

A p-group is a finite group whose order is a power of p.

Definition

If G is a group,

- the derived (commutator) subgroup $G' = \langle \{[x, y] \ : \ x, y \in G\} \rangle$ and $[x, y] = x^{-1}y^{-1}xy$,
- the center $Z(G) = \{z \in G \ : \ gz = zg \ \text{ for all } \ g \in G\}$,

Property

An extraspecial group G is a p-group which satisfies:

- $G' = Z(G)$,
- $Z(G)$ *is cyclic of prime order* p,

Beginning remarks.

Application.

Quantum error correction:

- Stabilizer codes: extraspecial 2-groups form the real part of the Pauli group,
- Clifford codes.

Efficiency.

If G is extraspecial then:

- $|G| = p^{2k+1}$
- an efficient algorithm should run in $\mathrm{poly}(\log(|G|)) = \mathrm{poly}(k \log(p))$, and both k and p can grow to infinity.

Efficient solutions for HSP:

- [Ivanyos,Magniez,Santha'01] when p is fixed constant,
- [Bacon,Childs,van Dam'05] Heisenberg group (case $k = 1$).

Extraspecial groups of size p^3 for odd p

There are two extraspecial groups of size p^3:

- one of exponent p (all elements of the groups are of order p),
- one of exponent p^2(elements of the group are of order p or p^2).

H_p, Heisenberg group of exponent p.

$$\begin{aligned} H_p &= \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} ;\ (a,b,c) \in \mathbb{Z}_p^3 \right\} \\ &= \langle x, y, z; x^p = y^p = z^p = 1,\ [x,y] = z,\ [x,z] = [y,z] = 1 \rangle \end{aligned}$$

A_p, application group of exponent p^2.

$$\begin{aligned} A_p &= \left\{ \begin{array}{ccc} \mathbb{Z}_{p^2} & \to & \mathbb{Z}_{p^2} \\ t & \mapsto & at+b \end{array} \text{ where } a \equiv 1 \text{ modulo } p \text{ and } b \in \mathbb{Z}_{p^2} \right\} \\ &= \langle x, y, z; x^{p^2} = y^p = 1,\ [x,y] = z = x^p,\ [y,z] = 1 \rangle \end{aligned}$$

$$G' = Z(G) = \{z^\ell | \ell \in \mathbb{Z}_p\}$$

Every element has a unique representation of the form

$$x^i y^j z^\ell, \text{where } i, j, \ell \in \mathbb{Z}_p.$$

Extraspecial groups of size p^{2k+1} by generators

There are two extraspecial groups of size p^{2k+1}, one of exponent p, and one of exponent p^2.

Extraspecial group of exponent p

$$H_p \times \ldots \times H_p \bmod z_1 = \cdots = z_k,$$

It is generated by $2k+1$ elements $x_1, y_1, \ldots, x_k, y_k$ and z which satisfy the relations $x_i^p = y_i^p = z^p = 1,\ [x_i, y_i] = z$ for $i \in \mathbb{Z}_p$,

$$[x_i, x_j] = [x_i, y_j] = [y_i, y_j] = [x_i, z] = [y_i, z] = 1 \text{ for } i \neq j \in \mathbb{Z}_p.$$

$$G' = Z(G) = \{z^\ell | \ell \in \mathbb{Z}_p\}$$

Elements have a unique representation of the form:
$x_1^{i_1} y_1^{i_1'} \cdots x_k^{i_k} y_k^{i_k'} z^\ell$,where $i_1, i_1', \ldots, i_k, i_k', \ell \in \mathbb{Z}_p$.

Example

For $k = 2$
$x_1 y_1^2 y_2 \cdot x_1 y_1 x_2^2 z = x_1^2 y_1^2 y_2 z^2 \cdot y_1 x_2^2 z = x_1^2 y_2 z^2 \cdot x_2^2 z = x_1^2 x_2^2 y_2 z \cdot z = x_1^2 x_2^2 y_2 z^2$

Extraspecial groups of size p^{2k+1} by generators

There are two extraspecial groups of size p^{2k+1}, one of exponent p, and one of exponent p^2.

Extraspecial group of exponent p^2

$$A_p \times H_p \times \ldots \times H_p \text{ mod } z_1 = \cdots = z_k,$$

It is generated by $2k$ elements $x_1, y_1, \ldots, x_k, y_k$ which satisfy the relations $x_i^p = y_i^p = 1,\ [x_i, y_i] = x_1^p$ for $i \in \mathbb{Z}_p$, with $i \neq 1$, $x_1^{p^2} = y_1^p = 1$, and

$$[x_i, x_j] = [x_i, y_j] = [y_i, y_j] = 1 \text{ for } i \neq j \in \mathbb{Z}_p.$$

$$G' = Z(G) = \{z^\ell | \ell \in \mathbb{Z}_p\} \text{ where } z = x_1^p.$$

Elements have a unique representation of the form:
$x_1^{i_1} y_1^{i_1'} \cdots x_k^{i_k} y_k^{i_k'} z^\ell$,where $i_1, i_1', \ldots, i_k, i_k', \ell \in \mathbb{Z}_p$.

Overview of the algorithm

Reduction lemma.

If f can be transformed into an efficient quantum hiding function for $HG' \leq G$ then the HSP has an efficient solution in G.

Hiding function lemma.

There is an efficient quantum hiding function for HG'.

- Groups of exponent p when p is large: hard case,
- Groups of constant exponent: easy (special case of previous),
- Groups of exponent p^2 when p is large: reduces to first case.

Theorem

We can solve the HSP *in any extraspecial p-group.*

Reduction.

Finding H is reducible to finding HG'.

Case 1: $G' \subseteq H$. Then $H = HG'$.
Case 2: $G' \cap H = \{1\}$.

- Then H is abelian since $h_1 h_2 = h_2 h_1 z^\ell \implies z^\ell \in G' \cap H$.
- Therefore HG' is abelian since G' is the center.
- The function f restricted to HG' hides H. This is an instance of the abelian HSP.

$\square$

Example

$G = H_3 = \{x^i y^j z^\ell \ : \ 0 \le i, j, \ell \le 2\}$
$H = \{1,\ x^2yz,\ xy^2z\}, \qquad G' = \{1, z, z^2\}$
$HG' = \{1, z, z^2,\ \ x^2y, x^2yz, x^2yz^2,\ \ xy^2, xy^2z, xy^2z^2\}$

Reduction.

Finding HG' is reducible to a hiding function for HG'.

- For $g = x_1^{i_1} y_1^{j_1} \dots x_k^{i_k} y_k^{j_k} z^{\ell}$ let $\overline{g} = x_1^{i_1} y_1^{j_1} \dots x_k^{i_k} y_k^{j_k}$
- $\overline{G} = \{\overline{g} : g \in G\}$.
  To make $\overline{G}$ a group define $\overline{g_1} * \overline{g_2} = \overline{g_1 g_2}$.
- Then $(\overline{G}, *) \simeq (G/G', .) \simeq \mathbb{Z}_p^{2k}$ is abelian and $HG' \cap \overline{G}$ is a subgroup of $(\overline{G}, *)$.
- The function hiding HG' in G hides also $HG' \cap \overline{G}$ in $\overline{G}$.
- $HG' = (HG' \cap \overline{G})G'$.

$\square$

Example

$G = \{x^i y^j z^{\ell} \ : \ 0 \leq i, j, \ell \leq 2\}$
$H = \{1, \ x^2yz, \ xy^2z\}, \qquad G' = \{1, z, z^2\}$
$HG' = \{1, z, z^2, \ \ x^2y, x^2yz, x^2yz^2, \ \ xy^2, xy^2z, xy^2z^2\}$

$\overline{G} = \{1, y, y^2, x, xy, xy^2, x^2, x^2y, x^2y^2\}$
$HG' \cap \overline{G} = \{1, x^2y, xy^2\}$

Hiding function for HG': Overview

Coset state.

- For random $a \in G$

$$|aHG'\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} |aHz^i\rangle$$

- Group action of g on the coset state:

$g \mapsto |aHG' \cdot g\rangle$

- Eigenvalues:

$\forall g = hz^t \in HG'$,

$|aHG' \cdot g\rangle = |aHG'\rangle$

Hiding function for HG': Overview

Coset state.

- For random $a \in G$

$$|aHG'\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} |aHz^i\rangle$$

- Group action of g on the coset state:

$g \mapsto |aHG' \cdot g\rangle$

- Eigenvalues:

$\forall g = hz^t \in HG'$,

$|aHG' \cdot g\rangle = |aHG'\rangle$

Perturbed coset state.

- For random $a \in G$ and $u \in \mathbb{Z}_p$

$$|aHG'_u\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} \omega^{-ui} |aHz^i\rangle$$

Hiding function for HG': Overview

Coset state.

- For random $a \in G$

$$|aHG'\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} |aHz^i\rangle$$

- Group action of g on the coset state:

$$g \mapsto |aHG' \cdot g\rangle$$

- Eigenvalues:

$$\forall g = hz^t \in HG',$$

$$|aHG' \cdot g\rangle = |aHG'\rangle$$

Perturbed coset state.

- For random $a \in G$ and $u \in \mathbb{Z}_p$

$$|aHG'_u\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} \omega^{-ui} |aHz^i\rangle$$

$$g \mapsto |aHG'_u \cdot g\rangle$$

$$\forall g = hz^t \in HG',$$

$$|aHG'_u \cdot g\rangle = \omega^{tu} |aHG'_u\rangle$$

Hiding function for HG': Overview

Coset state.

- For random $a \in G$

$$|aHG'\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} |aHz^i\rangle$$

- Group action of g on the coset state:

$g \mapsto |aHG' \cdot g\rangle$

- Eigenvalues:

$\forall g = hz^t \in HG'$,

$|aHG' \cdot g\rangle = |aHG'\rangle$

Perturbed coset state.

- For random $a \in G$ and $u \in \mathbb{Z}_p$

$$|aHG'_u\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} \omega^{-ui} |aHz^i\rangle$$

?

?

To cancel the disturbing phase: more sophisticated group action via group automorphisms.

Hiding function for HG': Overview

Coset state.

- For random $a \in G$

$$|aHG'\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} |aHz^i\rangle$$

- Group action of g on the coset state:

$g \mapsto |aHG' \cdot g\rangle$

- Eigenvalues:

$\forall g = hz^t \in HG'$,

$|aHG' \cdot g\rangle = |aHG'\rangle$

Perturbed coset state.

- For random $a \in G$ and $u \in \mathbb{Z}_p$

$$|aHG'_u\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} \omega^{-ui} |aHz^i\rangle$$

?

?

To cancel the disturbing phase: more sophisticated group action via group automorphisms.

Definition

For $j = 1, \ldots, p-1$, automorphisms ϕ_j of G: $x_i \mapsto x_i^j, \quad y_i \mapsto y_i^j, \quad z \mapsto z^{j^2}$ for $i \in \{1, \ldots, k\}$.

Hiding function for HG': Overview

Coset state.

- For random $a \in G$

$$|aHG'\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} |aHz^i\rangle$$

- Group action of g on the coset state:

$g \mapsto |aHG' \cdot g\rangle$

- Eigenvalues:

$\forall g = hz^t \in HG'$,

$|aHG' \cdot g\rangle = |aHG'\rangle$

Perturbed coset state.

- For random $a \in G$ and $u \in \mathbb{Z}_p$

$$|aHG'_u\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} \omega^{-ui} |aHz^i\rangle$$

$g \mapsto |aHG'_u \cdot \phi_j(g)\rangle$

?

To cancel the disturbing phase: more sophisticated group action via group automorphisms.

Definition

For $j = 1, \ldots, p-1$, automorphisms ϕ_j of G: $x_i \mapsto x_i^j, \quad y_i \mapsto y_i^j, \quad z \mapsto z^{j^2}$ for $i \in \{1, \ldots, k\}$.

Hiding function for HG': Overview

Coset state.

- For random $a \in G$

$$|aHG'\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} |aHz^i\rangle$$

- Group action of g on the coset state:

$$g \mapsto |aHG' \cdot g\rangle$$

- Eigenvalues:

$$\forall g = hz^t \in HG',$$

$$|aHG' \cdot g\rangle = |aHG'\rangle$$

Perturbed coset state.

- For random $a \in G$ and $u \in \mathbb{Z}_p$

$$|aHG'_u\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} \omega^{-ui} |aHz^i\rangle$$

$$g \mapsto |aHG'_u \cdot \phi_j(g)\rangle$$

$$\forall g = hz^t \in HG',$$

$$|aHG'_u \cdot g\rangle = \omega^{u(j-j^2)\ell + uj^2 t} |aHG'_u\rangle$$

To cancel the disturbing phase: more sophisticated group action via group automorphisms.

Definition

For $j = 1, \ldots, p-1$, automorphisms ϕ_j of G: $x_i \mapsto x_i^j, \quad y_i \mapsto y_i^j, \quad z \mapsto z^{j^2}$ for $i \in \{1, \ldots, k\}$.

The hiding function

Four copies state.

For $\bar{a} \in G^4$, $\bar{u} \in \mathbb{Z}_p^4$, $\bar{j} \in (\mathbb{Z}_p^*)^4$ and $g \in G$, let

$$|\Psi_g^{\bar{a},\bar{u},\bar{j}}\rangle = \bigotimes_{i=1}^{4} |a_i HG'_{u_i} \cdot \phi_{j_i}(g)\rangle = \omega^{\sum_{i=1}^{4} u_i((j_i - j_i^2)\ell + j_i^2 t)} \bigotimes_{i=1}^{4} |a_i HG'_{u_i}\rangle.$$

Fact

$g \mapsto |\Psi_g^{\bar{a},\bar{u},\bar{j}}\rangle$ *is hiding* HG' *for* $\bar{j} \in (\mathbb{Z}_p^*)^4$ *solution of*

$$\begin{cases} \sum_{i=1}^{4} u_i(j_i - j_i^2) & = & 0 \\ \sum_{i=1}^{4} u_i j_i^2 & = & 0. \end{cases}$$

Lemma

$$\Pr_{\bar{u} \in \mathbb{Z}_p^4}[\exists \bar{j} \in (\mathbb{Z}_p^*)^4 \text{ solution}] \approx \frac{1}{2}.$$

The system is efficiently solvable.

Hiding function for HG' in groups of exponent (large) p

Algorithm

1. *Compute, for some* $\overline{a} \in G^4$*, the superposition*

$$\frac{1}{p^2} \bigotimes_{i=1}^{4} \sum_{u_i \in \mathbb{Z}_p} |u_i\rangle |a_i HG'_{u_i}\rangle$$

2. *Measure the registers for* $\overline{u}$
3. *Solve the equation*

$$\begin{cases} \sum_{i=1}^{4} u_i(j_i - j_i^2) & = & 0 \\ \sum_{i=1}^{4} u_i j_i^2 & = & 0 \end{cases}$$

4.
   - *If the system has a solution* $\overline{j} \in (\mathbb{Z}_p^*)^4$ *then*

$$|g\rangle \mapsto \bigotimes_{i=1}^{4} |a_i HG'_{u_i} \cdot \phi_{j_i}(g)\rangle$$

   - *else repeat 1.,2. and 3.*

A constant number of repetitions is enough.

Extension and future work.

- We can generalise this method to nilpotent p-groups of class 2.
- Extend to higher classes.