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

Gábor Ivanyos† Luc Sanselme‡ Miklos Santha§

January 31, 2007

Abstract

Extraspecial groups form a remarkable subclass of p-groups. They are also present in quantum information theory, in particular in quantum error correction. We give here a polynomial time quantum algorithm for finding hidden subgroups in extraspecial groups. Our approach is quite different from the recent algorithms presented in [17] and [2] for the Heisenberg group, the extraspecial p-group of size p^3 and exponent p. Exploiting certain nice automorphisms of the extraspecial groups we define specific group actions which are used to reduce the problem to hidden subgroup instances in abelian groups that can be dealt with directly.

1 Introduction

The most important challenge of quantum computing is to find quantum algorithms that achieve exponential speedup over the best known classical solutions. In this respect, the most extensively studied problem is the paradigmatic hidden subgroup problem. Stated in a group theoretical setting, in HSP(G, f) we are given explicitely a finite group G and we also have at our disposal a function f that can be queried via an oracle, and which maps G into a finite set. We are promised that for some subgroup H, f is constant on each left coset of H and distinct on different left cosets. We say that f hides the subgroup H. The task is to determine the hidden subgroup H. We measure the time complexity of an algorithm by the overall running time when a query counts as one computational step. An algorithm is called efficient if its time complexity is polynomial in the logarithm of the order of G.

We don't know any classical algorithm of polynomial query complexity for the HSP, even in the restricted case of abelian groups. In this respect, probably the most important result of quantum computing is that the HSP can be solved efficiently for abelian groups by quantum algorithms. We will call this solution, for which one can find an excellent description for example in Mosca's thesis [15], the standard algorithm for HSP. The main quantum tool used in the standard algorithm is Fourier sampling based on the approximate quantum Fourier transform that can be efficiently implemented by a quantum algorithm in case of abelian groups [11]. Among the important special cases of this general solution one can mention Simon's xor-mask finding [21], Shor's factorization and discrete logarithm finding algorithms [19], and Kitaev's algorithm [11] for the abelian stabilizer problem.

Since the realization of the importance of the abelian HSP, intensive efforts have been made to solve the hidden subgroup problem also in finite non-abelian groups. The intrinsic mathematical interest of this challenge is increased by the fact that several famous classical algorithmic problems can be cast in

*Research supported by the European Commission IST Integrated Project Qubit Applications (QAP) 015848, the OTKA grants T42559 and T46234, the NWO visitor's grant Algebraic Aspects of Quantum Computing, and by the ANR Blanc AlgoQP grant of the French Research Ministry.

†SZTAKI, Hungarian Academy of Sciences, H-1111 Budapest, Hungary. ivanyos@sztaki.hu

‡UMR 8623 Université Paris–Sud 91405 Orsay, France. sanselme@lri.fr

§CNRS–LRI, UMR 8623 Université Paris–Sud 91405 Orsay, France. santha@lri.fr

this framework, like for example the graph isomorphism problem. The successful efforts for solving the problem can roughly be divided into two categories. The standard algorithm has been extended to some non-abelian groups by Rötteler and Beth [18], Hallgren, Russell and Ta-Shma [8], Grigni, Schulman, Vazirani and Vazirani [7] and Moore, Rockmore, Russell and Schulman [14] using efficient implementations of the quantum Fourier transform over these groups. In a different approach, Ivanyos, Magniez and Santha [10] and Friedl, Ivanyos, Magniez, Santha and Sen [5] have efficiently reduced the HSP in some non-abelian groups to HSP instances in abelian groups using classical and quantum group theoretical tools, but not the non-abelian Fourier transform.

All groups where the HSP has been efficiently solved are in some sense "close" to abelian groups. Extraspecial groups, in which we present here an efficient quantum algorithm, are no exception in this respect: they have the property that all their proper factor groups are abelian. They form a subclass of p-groups, where p is a prime number, and play an important role in the theory of this family of groups. Extensive treatment of extraspecial groups can be found for example in the books of Huppert [9] and Aschbacher [1].

Extraspecial 2-groups are heavily present in the theory of quantum error correction. They provide a bridge between quantum error correcting codes and binary orthogonal geometry [3]. They form the real subgroup of the Pauli group [4] which plays a crucial role in the theory of stabilizer codes [6]. For general p, extraspecial p-groups give rise to the simplest examples of Clifford codes, see [12].

Efficient solutions for the HSP have already been given in several specific extraspecial groups. Extraspecial p-groups are of order p^{2k+1} for some integer k. For odd p, they are of exponent p or p^2, and extraspecial 2-groups are of exponent 4. The class of groups for which Ivanyos, Magniez and Santha [10] provide a solution include extraspecial p-groups when p is a fixed constant and the input size grows with k. When p is fixed, the smallest extraspecial groups are of size p^3. Up to isomorphism there are two extraspecial groups of order p^3. Recently two independent works dealt with quantum algorithms for the HSP in the group of exponent p, the Heisenberg group. Radhakrishnan, Rötteler and Sen [17] have followed the standard algorithm with non-abelian Fourier transform, and proved that strong Fourier sampling with a random basis leads to a query efficient quantum solution. In a subsequent work, Bacon, Childs and van Dam [2] devised an efficient quantum algorithm, where a state estimation technique, called the pretty good measurement, is used to reduce the HSP to some matrix sum problem that they could solve classically.

In this paper we provide an efficient quantum algorithm for the HSP in any extraspecial group. Our main contribution is an efficient algorithm in extraspecial p-groups of exponent p when p grows with the input size. A simplified version of this algorithm gives another solution for the groups of constant exponent. The remaining case, groups of exponent p^2 when p is large is easily reducible to the case of groups of exponent p.

Our approach for groups of exponent p is completely different from the above two solutions for the Heisenberg group. In our solution only abelian Fourier transforms and von Neumann measurements are used. In fact, our algorithm is a series of reductions, where we repeatedly use the standard algorithm for abelian groups, or a slight extension of it. In this extension, instead of a classical hiding functions we have an efficient quantum hiding procedure at our disposal. This procedure outputs a quantum state for every group element so that the states corresponding to group elements coming from the same left coset of the hidden subgroup are identical, whereas the states corresponding to group elements from different left cosets are orthogonal. Repeated invocations of the procedure might yield different states for the same group element.

At the end of our reductions we are faced with the problem of creating an efficient hiding procedure in the above sense for the subgroup HG' of G, where G is an extraspecial p-group of exponent p when p is large, $G' = \{z^i \ : \ 0 \leq i \leq p-1\}$ is its commutator, and H is the hidden subgroup. It is easy to see, that if we could create the coset state $|aHG'\rangle$ for some $a \in G$, then the group action multiplication from the right, which on a given group element g would output $|aHG' \cdot g\rangle$, is a hiding procedure. Unfortunately, we can create these states efficiently only when p is constant. In the general case, we can create efficiently only the states $|aHG'_u\rangle$ for a random $0 \leq u \leq p-1$, where $|G'_u\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} \omega^{-ui} |z^i\rangle$. Our main technical contribution is to show that several (in fact four) copies of these states can be combined together so that the disturbing phases cancel each other. To achieve this goal we exploit certain nice automorphisms of the group to define more sophisticated group actions that can be used for our purposes.

The structure of the paper is quite simple. After a discussion on the extension of the standard algorithm

and a basic description of extraspecial groups in Section 2, our reduction steps are presented in Section 3. The summary of these reductions is stated in Theorem 1: An efficient hiding procedure for HG' is sufficient to solve the HSP in an extraspecial group G. In Section 4 we establish our main result in Theorem 2, the existence of an efficient solution for the HSP in extraspecial groups. The proof is given according to the three cases discussed above. The most important case of groups of exponent p when p is large is dealt with in Section 4.2, where in Theorem 3 we provide the hiding procedure for HG'.

2 Preliminaries

2.1 Extensions of the standard algorithm for the abelian HSP

We will use standard notions of quantum computing for which one can consult for example [13]. For a finite set X, we denote by $|X\rangle$ the uniform superposition $\frac{1}{\sqrt{|X|}}\sum_{x\in X}|x\rangle$ over X. For a superposition $|\Psi\rangle$, we denote by $\mathsf{supp}(|\Psi\rangle)$ the support of $|\Psi\rangle$, that is the set of basis elements with non-zero amplitude.

The general solution for the abelian HSP consists essentially of Fourier sampling of the hiding function f. More specifically, it involves the creation of the superposition $\sum_{g\in G}|g\rangle|f(g)\rangle$ and the Fourier transform over G. Clearly, for the former part it is essential to have access to a hiding function. In fact, this requirement can be relaxed in some sense, and in this paper we will use such a relaxation. A relaxation was already used by Ivanyos et al. [10] who extended the notion of the hiding function to quantum functions. More precisely, for a finite set X, and a quantum function $f : G \to \mathbb{C}^X$, we say that f *hides* the subgroup H of G if $|f(g)\rangle$ is a unit vector for every $g \in G$, and f is constant on the left cosets of H, and maps elements from different cosets into orthogonal states. The simple fact is proven in Lemma 1 of [10] that in the standard solution of HSP for abelian groups, one can just as well use a quantum hiding function.

The standard algorithms for the abelian HSP in fact repeats polynomially many times the Fourier sampling involving the same (classical or quantum) hiding function. In fact, in each iteration a random element is obtained from the subgroup orthogonal to H. Our extension is based on the observation, that for the sampling, one doesn't have to use the same hiding function in each iteration, different hiding functions will do just as well the game. For the sake of completeness we formalize this here and state the exact conditions that will be used in our case.

We say that a set of vectors $\{|\Psi_g\rangle : g \in G\}$ from some Hilbert space $\mathcal{H}$ is a *hiding set* for the subgroup H of G if

- $|\Psi_g\rangle$ is a unit vector for every $g \in G$,
- if g and g' are in the same left coset of H then $|\Psi_g\rangle = |\Psi_{g'}\rangle$,
- if g and g' are in different left cosets of H then $|\Psi_g\rangle$ and $|\Psi_{g'}\rangle$ are orthogonal.

A quantum procedure is *hiding* the subgroup H of G if for every $g \in G$, on input $|g\rangle|0\rangle$ it outputs $|g\rangle|\Psi_g\rangle$ where $\{|\Psi_g\rangle : g \in G\}$ is a hiding set for H. Let us underline that we don't require from a quantum hiding procedure to output the same hiding set in different calls. The following fact recasts the existence of the standard algorithm for the abelian HSP in the context of hiding sets.

Fact 1. *Let G be a finite abelian group. If there exists an efficient quantum procedure which hides the subgroup H of G then there is an efficient quantum algorithm for finding H.*

Proof. It is immediate from the proof of Lemma 1 in [10]: indeed, the exact property of the quantum hiding function f which is used there is that $\{|g\rangle|f(g)\rangle : g \in G\}$ forms a hiding set for H. □ □

2.2 Extraspecial groups

Let G be a finite group. For two elements g_1 and g_2 of G, we usually denote their product by g_1g_2. If we conceive group multiplication from the right as a group action of G on itself, we will use the notation $g_1 \cdot g_2$

for $g_1 g_2$. For a subset X of G, we will denote by $\langle X \rangle$ the subgroup generated by X. The derived subgroup G' of G is defined as $\langle \{x^{-1}y^{-1}xy \ : \ x, y \in G\} \rangle$, and its center $Z(G)$ as $\{z \in G \ : \ gz = zg \ \text{ for all } \ g \in G\}$. The Frattini subgroup $\Phi(G)$ is the intersection of all maximal subgroups of G.

For an integer n, we denote by $\mathbb{Z}_n$ the group of integers modulo n, and for a prime number p, we denote by $\mathbb{Z}_p^*$ the multiplicative group of integers relatively prime with p. A p-group is a finite group whose order is a power of p. A p-group G is *extraspecial* if $G' = Z(G) = \Phi(G)$, and its center is cyclic of prime order p.

If G is an extraspecial p-group then $|G| = p^{2k+1}$ for some integer k. The elements of G can be encoded by binary strings of length $O(k \log p)$, and an efficient algorithm on that input has to be polynomial in both k and $\log p$.

The smallest non-abelian extraspecial groups are of order p^3. For $p = 2$, we have, up to isomorphism, two extraspecial 2-groups of order 8. These are the quaternion group Q, and the dihedral group D_4, the symmetry group of the square in two dimensions. The exponent of both of these groups is $p^2 = 4$.

For $p > 2$, up to isomorphism we have again two extraspecial p-groups of order p^3. The first one is the Heisenberg group H_p, which is the group of upper triangular 3×3 matrices over the field $\mathbb{F}_p$ whose diagonal contains everywhere 1. The exponent of H_p is p. The other one is A_p, the group of applications $t \mapsto at + b$ from $\mathbb{Z}_{p^2}$ to $\mathbb{Z}_{p^2}$, where $a \equiv 1$ modulo p and $b \in \mathbb{Z}_{p^2}$. The exponent of A_p is p^2.

We give now via relations equivalent definitions of the extraspecial p-groups of order p^3. These definitions will be useful for the arguments we will develop in our algorithms. To emphasize the similarities between these groups, we will take three generator elements x, y, z for each of them. The element z will always generate the center of the group. Here are the definitions via relations:

$$Q = \langle x^2 = y^2 = [x, y] = z, \ z^2 = 1 \rangle,$$

$$D_4 = \langle x^2 = y^2 = z^2 = 1, \ [x, y] = z, \ [x, z] = [y, z] = 1 \rangle,$$

$$H_p = \langle x^p = y^p = z^p = 1, \ [x, y] = z, \ [x, z] = [y, z] = 1 \rangle,$$

$$A_p = \langle x^{p^2} = y^p = 1, \ [x, y] = z = x^p, \ [y, z] = 1 \rangle.$$

From these definitions it is clear that every element in an extraspecial group of order p^3 has a unique representation of the form $x^i y^j z^\ell$ where $i, j, \ell \in \mathbb{Z}_p$.

Extraspecial p-groups of order p^{2k+1}, for $k > 1$, can be obtained as the central product of k extraspecial p-groups of order p^3. If $G_1, \ldots, G_k$ are extraspecial p-groups of order p^3 then their *central product* $G_1 \mathbf{Y} \ldots \mathbf{Y} G_k$ is the factor group

$$G_1 \times \ldots \times G_k \bmod z_1 = \cdots = z_k,$$

where z_i is an arbitrary generator of $Z(G_i)$ for $i = 1, \ldots, k$.

Since $D_4 \mathbf{Y} D_4 = Q \mathbf{Y} Q$, up to isomorphism the unique extraspecial 2-groups of order 2^{2k+1} are $\mathbf{Y}_{i=1}^{k} D_4$ and $(\mathbf{Y}_{i=1}^{k-1} D_4) \mathbf{Y} Q$. All of these groups are of exponent $p^2 = 4$. When $p > 2$, we have $H_p \mathbf{Y} A_p = A_p \mathbf{Y} A_p$. Therefore, up to isomorphism the unique extraspecial p-groups of order p^{2k+1} are $\mathbf{Y}_{i=1}^{k} H_p$ and $(\mathbf{Y}_{i=1}^{k-1} H_p) \mathbf{Y} A_p$. The former groups are of exponent p, the latter ones are of exponent p^2.

It follows from the above that any extraspecial group of order p^{2k+1} can be generated by $2k+1$ elements $x_1, y_1, \ldots, x_k, y_k$ and z. Any element of the group has 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 $i_1, i_1', \ldots, i_k, i_k', \ell \in \mathbb{Z}_p$. Also, $G' = Z(G) = \{z^\ell | \ell \in \mathbb{Z}_p\}$.

3 Reduction lemmas

Our results leading to our main technical contribution can be the best described via a series of reduction lemmas.

Lemma 1. *Let G be an extraspecial p-group, and let us given an oracle f which hides the subgroup H of G. Then finding H is efficiently reducible to find HG'.*

Proof. Since G' is a cyclic group of prime order, either $G' \subseteq H$ or $G' \cap H = \{1\}$. It is simple to decide which one of this cases holds by checking if $f(z) = f(1)$. If $G' \subseteq H$ then $H = HG'$, and therefore the algorithm which finds HG' yields immediatly H.

If $G' \cap H = \{1\}$ then we claim that HG' is abelian. To see this, it is sufficient to show that H is abelian, since G' is the center of G. Let h_1 and h_2 be two elements of H. Then there exists $\ell \in \mathbb{Z}_p$ such that $h_1 h_2 = h_2 h_1 z^\ell$. This implies that z^ℓ is in $G' \cap H$ and therefore $z^\ell = 1$.

The restriction of the hiding function f to the abelian subgroup HG' of G hides H. Therefore the standard algorithm for solving the HSP in abelian groups applied to HG' with oracle f yields H. □ □

We will show that finding HG' can be efficiently reduced to the hidden subgroup problem in an abelian group. For every element $g = x_1^{i_1} y_1^{j_1} \dots x_k^{i_k} y_k^{j_k} z^\ell$ of G, we denote by $\overline{g}$ the element $x_1^{i_1} y_1^{j_1} \dots x_k^{i_k} y_k^{j_k}$. We define now the group $\overline{G}$ whose base set is $\{\overline{g} : g \in G\}$. Observe that this set of elements does not form a subgroup in G. To make $\overline{G}$ a group, its law is defined by $\overline{g_1} * \overline{g_2} = \overline{g_1 g_2}$ for all $\overline{g_1}$ and $\overline{g_2}$ in $\overline{G}$. It is easy to check that $*$ is well defined, and is indeed a group multiplication. The group $\overline{G}$ is isomorphic to G/G' and therefore is abelian. For our purposes a nice way to think about $\overline{G}$ as a representation of G/G' with unique encoding. In fact, it is also easy to check that $\overline{G}$ is isomorphic to $\mathbb{Z}_p^{2k}$. Finally let us observe that $HG' \cap \overline{G}$ is a subgroup of $(\overline{G}, *)$ since HG'/G' is a subgroup of G/G',

Lemma 2. *Let G be an extraspecial p-group, and let us given an oracle f which hides the subgroup H of G. Then finding HG' is efficiently reducible to find $HG' \cap \overline{G}$ in $\overline{G}$.*

Proof. Since $HG' = (HG' \cap \overline{G})G'$, a generator set of HG' in G is composed of a generator set of $HG' \cap \overline{G}$ in $\overline{G}$ together with z. □ □

The group $\overline{G}$ is abelian but we don't have a hiding function for $HG' \cap \overline{G}$. The main technical result of our paper is that using the hiding function f for H in G, we will be able to implement an efficient quantum *hiding procedure* for HG' in G. Our last reduction lemma just states that this is sufficient for finding $HG' \cap \overline{G}$.

Lemma 3. *Let G be an extraspecial p-group, and let us given an oracle f which hides the subgroup H of G. If we have an efficient quantum procedure (using f) which hides HG' in G then we can find efficiently $HG' \cap \overline{G}$ in $\overline{G}$.*

Proof. The procedure which hides HG' in G hides also $HG' \cap \overline{G}$ in $\overline{G}$. Since $\overline{G}$ is abelian, Fact 1 implies that we can find efficiently $HG' \cap \overline{G}$. □ □

Our first theorem is the consequence of these three lemmas. It says that if in an extraspecial group we succeed to transform the oracle hiding the subgroup H into a quantum procedure hiding HG' then we can determine H. This reduction is the basis of our algorithm.

Theorem 1. *Let G be an extraspecial p-group, and let us given an oracle f which hides the subgroup H of G. If we have an efficient quantum procedure (using f) which hides HG' in G then* $\mathrm{HSP}(G, f)$ *can be solved efficiently.*

Observe that if $G' \subseteq H$ then $HG' = H$, and therefore the following corollary is immediate.

Corollary 1. *Let G be an extraspecial p-group, and let us given an oracle f which hides the subgroup H of G. If $G' \subseteq H$ then we can solve efficiently* $\mathrm{HSP}(G, f)$.

4 The algorithm

We now describe the quantum algorithm which solves the HSP in extraspecial groups. In fact, we will deal separately with three cases: groups of constant exponent, groups of exponent p when p is large, and groups of exponent p^2 when p is large. The case of constant exponent is actually not new, it follows from a general result in [10]. Nevertheless, for the sake of completeness we show how a simplified version of the algorithm

for the second case works here. The algorithm for extraspecial groups of exponent p that goes to infinity is our main result. Finally, the case of groups of exponent p^2 can be easily reduced to the case of groups of exponent p. These results are summarized in our main theorem.

Theorem 2. *Let G be an extraspecial p-group, and let us given an oracle f which hides the subgroup H of G. Then there is an efficient quantum procedure which finds H.*

4.1 Groups of constant exponent

In Theorem 9 of [10] it is proven that in general the HSP can be solved by a quantum algorithm in polynomial time in the size of the input and the cardinality of G'. This includes the case of extraspecial groups of constant exponent. Nonetheless, for the sake of completeness we describe here an efficient procedure, similar in spirit to the one used for the next case but much simpler.

First remark that for every $a \in G$, the set $\{|aHG' \cdot g\rangle : g \in G\}$ is hiding for HG' in G. The efficient hiding procedure for HG' computes, for some $a \in G$, the superposition $\frac{1}{\sqrt{p}} \sum_{u \in \mathbb{Z}_p} |u\rangle |aHG'_u\rangle$ which by Lemma 4 of Section 4.2 can be done efficiently. Then the first register is measured. This is repeated until the result of the observation is 0. Since p is constant, after a constant number of iteration the superposition $|0\rangle|aHG'_0\rangle = |0\rangle|aHG'\rangle$ is created and finally $|aHG' \cdot g\rangle$ is computed.

Observe that this simplified approach can not work for large exponents since p, the expected number of iterations, is not polynomial in the size of the input.

4.2 Groups of exponent p when p is large

For every $u \in \mathbb{Z}_p$, let $|G'_u\rangle = \frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} \omega^{-ui} |z^i\rangle$ and observe that $|G'_u \cdot z\rangle = \omega^u |G'_u\rangle$.

Lemma 4. *There is an efficient quantum procedure which creates $\frac{1}{\sqrt{p}} \sum_{u \in \mathbb{Z}_p} |u\rangle |aHG'_u\rangle$ where a is a random element from G.*

Proof. We start with $|0\rangle|0\rangle|0\rangle$. Since we have access to the hiding function f, we can create the superposition $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |0\rangle|g\rangle|f(g)\rangle$. Observing and discharging the third register we get $|0\rangle|aH\rangle$ for a random element a. Applying the Fourier transform over $\mathbb{Z}_p$ to the first register gives $|\mathbb{Z}_p\rangle|aH\rangle$. Multiplying the second register by z^{-i} when i is the content of the first one results in $\frac{1}{\sqrt{p}} \sum_{i \in \mathbb{Z}_p} |-i\rangle|aHz^i\rangle$. A final Fourier transform in the first register creates the required superposition. □ □

For $j = 1, \ldots, p-1$, we define the automorphisms ϕ_j of G mapping x_i to x_i^j, y_i to y_i^j and z to z^{j^2} when $i \in \{1, \ldots, k\}$. These maps (defined on generators) extend in fact to automorphisms of G since the elements $x_1^j, y_1^j, \ldots x_k^j, y_k^j, z^{j^2}$ generate the group G and satisfy the defining relations.

In our next lemma we claim that the states $|aHG'_u\rangle$ are eigenvectors of the group action of multiplication from the right by $\phi_j(g)$, whenever g is from HG'. Moreover, the corresponding eigenvalues are some powers of the root of the unity, the exponent does not depend on a, and the dependence on u and j is relatively simple.

Lemma 5. *We have*

1. $\forall h \in H, \exists \ell \in \mathbb{Z}_p, \forall a \in G, \forall u \in \mathbb{Z}_p, \forall j \in \mathbb{Z}_p^*, \quad |aHG'_u \cdot \phi_j(h)\rangle = \omega^{u(j-j^2)\ell} |aHG'_u\rangle,$
2. $\forall a \in G, \forall u \in \mathbb{Z}_p, \forall j \in \mathbb{Z}_p^*, \quad |aHG'_u \cdot \phi_j(z)\rangle = \omega^{uj^2} |aHG'_u\rangle.$

Proof. To begin with let's remark that for $h \in H$, we have $|aHG'_u \cdot h\rangle = |aHG'_u\rangle$ and that $|aHG'_u \cdot z\rangle = \omega^u |aHG'_u\rangle$.

To prove the first part, let h be an element of H. Then $\phi_j(h) = h^j z^t$ where t depends on h and j. We will show that $t = (j - j^2)\ell$ where ℓ depends only on h. This will imply the claim.

Let j_0 be a fixed primitive element of $\mathbb{Z}_p^*$. Then $\phi_{j_0}(h) = h^{j_0} z^s$, for some $s \in \mathbb{Z}_p$. We set $\ell = s(j_0 - j_0^2)^{-1}$, and $k = hz^\ell$. Then $\phi_{j_0}(k) = h^{j_0} z^{\ell(j_0 - j_0^2)} z^{\ell j_0^2} = k^{j_0}$. Therefore $\phi_j(k) = k^j$ and $\phi_j(h) = \phi_j(k)\phi_j(z^{-\ell}) = h^j z^{\ell(j-j^2)}$. The proof of the second part is immediate. □ □

The principal idea now is to take several copies of the states $|a_i HG'_{u_i}\rangle$ and choose j_i so that the product of the corresponding eigenvalues becomes the unity. Therefore the actions $\phi_j(g)$, when g is from HG', will not modify the combined state. It turns out that we can achieve this with four copies.

For $\overline{a} = (a_1, a_2, a_3, a_4) \in G^4$, $\overline{u} = (u_1, u_2, u_3, u_4) \in \mathbb{Z}_p^4$, $\overline{j} = (j_1, j_2, j_3, j_4) \in (\mathbb{Z}_p^*)^4$ and $g \in G$, we define the quantum state $|\Psi_g^{\overline{a},\overline{u},\overline{j}}\rangle$ in $\mathbb{C}^{G^4}$ by

$$|\Psi_g^{\overline{a},\overline{u},\overline{j}}\rangle = |a_1 HG'_{u_1} \cdot \phi_{j_1}(g), a_2 HG'_{u_2} \cdot \phi_{j_2}(g), a_3 HG'_{u_3} \cdot \phi_{j_3}(g), a_4 HG'_{u_4} \cdot \phi_{j_4}(g)\rangle.$$

Our purpose is to find an efficient procedure to generate triples $(\overline{a}, \overline{u}, \overline{j})$ such that for every $g \in HG'$ we have $|\Psi_g^{\overline{a},\overline{u},\overline{j}}\rangle = |a_1 HG'_{u_1}, a_2 HG'_{u_2}, a_3 HG'_{u_3}, a_4 HG'_{u_4}\rangle$. We call such triples *appropriate*. The reason to look for appropriate triples is that they lead to hiding sets for HG' in G as stated in the next lemma.

Lemma 6. *If $(\overline{a}, \overline{u}, \overline{j})$ is an appropriate triple then $\{|\Psi_g^{\overline{a},\overline{u},\overline{j}}\rangle : g \in G\}$ is hiding for HG' in G.*

Proof. To see this, first observe that HG' is a normal subgroup of G. If g_1 and g_2 are in different cosets of HG' in G then for every $j \in \mathbb{Z}_p^*$, the elements $\phi_j(g_1)$ and $\phi_j(g_2)$ are in different cosets of HG' in G since ϕ_j is an automorphism of G. Also, for every $a \in G$ and for every $u \in \mathbb{Z}_p$ we have $\mathsf{supp}(|aHG'_u\rangle) = \mathsf{supp}(|aHG'\rangle)$, and therefore $\mathsf{supp}(|aHG'_u \cdot \phi_j(b)\rangle)$ and $\mathsf{supp}(|aHG'_u \cdot \phi_j(b')\rangle)$ are included in different cosets and are disjoint. Thus for every $\overline{a} \in G^4, \overline{u} \in \mathbb{Z}_p^4$ and $\overline{j} \in (\mathbb{Z}_p^*)^4$, the states $|\Psi_{g_1}^{\overline{a},\overline{u},\overline{j}}\rangle$ and $|\Psi_{g_2}^{\overline{a},\overline{u},\overline{j}}\rangle$ are orthogonal.

If g_1 and g_2 are in the same coset of HG' then $g_1 = gg_2$ for some $g \in HG'$, and $\phi_{j_i}(g_1) = \phi_{j_i}(g)\phi_{j_i}(g_2)$. Thus $|\Psi_{g_1}^{\overline{a},\overline{u},\overline{j}}\rangle = |\Psi_{gg_2}^{\overline{a},\overline{u},\overline{j}}\rangle = |\Psi_{g_2}^{\overline{a},\overline{u},\overline{j}}\rangle$. □ □

Let us now address the question of existence of appropriate triples and efficient ways to generate them. Let $(\overline{a}, \overline{u}, \overline{j})$ be an arbitrary element of $G^4 \times \mathbb{Z}_p^4 \times (\mathbb{Z}_p^*)^4$, and let g be an element of HG'. Then $g = hz^t$ for some $h \in H$ and $t \in \mathbb{Z}_p$, and $\phi_{j_i}(g) = \phi_{j_i}(h)\phi_{j_i}(z^t)$ for $i = 1, \ldots, 4$. By Lemma 5 there exists ℓ such that $|a_i HG'_{u_i} \cdot \phi_j(h)\rangle = \omega^{u_i(j_i - j_i^2)\ell} |a_i HG'_{u_i}\rangle$ and $|a_i HG'_{u_i} \cdot \phi_j(z^t)\rangle = \omega^{u_i j_i^2 t} |a_i HG'_{u_i}\rangle$, and therefore

$$|\Psi_g^{\overline{a},\overline{u},\overline{j}}\rangle = \omega^{\sum_{i=1}^4 (u_i(j_i - j_i^2)\ell + u_i j_i^2 t)} |a_1 HG'_{u_1}, a_2 HG'_{u_2}, a_3 HG'_{u_3}, a_4 HG'_{u_4}\rangle.$$

We say that $\overline{u} \in \mathbb{Z}_p^4$ is *good* if the following system of quadratic equations has a nonzero solution:

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

and we call a solution $\overline{j}$ a *witness* of u being good. It should be clear that for every $\overline{u}$, if $\overline{u}$ is good and $\overline{j}$ witnesses that then $(\overline{a}, \overline{u}, \overline{j})$ is an appropriate triple.

The next lemma states that a random $\overline{u}$ is good with constant probability, and that in this case one can find efficiently $\overline{j}$ witnessing that.

Lemma 7. *For every $\overline{a} \in G^4$, we have*

$$\mathsf{Pr}\, \overline{u} \in \mathbb{Z}_p^4 \overline{u} \text{ is good} \geq (p-9)/2p.$$

Moreover, when $\overline{u}$ is good a witness $\overline{j}$ can be found efficiently.

Proof. Let us simplify system (1) to the equivalent system

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

To solve (2), we take $j_3 = 1$ and $j_4 = -1$, and we set $v = u_3 + u_4$ and $w = u_3 - u_4$. We will show that for random $(u_1, u_2, v, w) \in \mathbb{Z}_p^4$, the reduced system (3) has a solution $(j_1, j_2) \in (\mathbb{Z}_p^*)^2$ with probability at least $(p-9)/2p$, and that the solution is easy to find:

$$\begin{cases} u_1 j_1^2 + u_2 j_2^2 &= -v \\ u_1 j_1 + u_2 j_2 &= -w. \end{cases} \tag{3}$$

With probability at least $1 - 3p$ we have $u_1 \neq 0$, $u_2 \neq 0$, $u_1 + u_2 \neq 0$. In that case we can substitute $j_2 = -\frac{w+u_1 j_1}{u_2}$ in the first equation and get in j_1 the quadratic equation $(u_1 u_2 + u_1^2) j_1^2 + 2u_1 w j_1 + (w^2 + v u_2) = 0$. It is a non degenerate quadratic equation whose discriminant $D = -4u_1 u_2 (w^2 + (u_2 + u_1)v)$ is uniformly distributed in $\mathbb{Z}_p$ since it is linear in v. Therefore D is a quadratic residue with probability $(p-1)/2p$, and we can efficiently compute a square root of D modulo p (see, for example, subsection 13.3.1 of [20]). We also have to ensure that $j_2 \neq 0$. If j_2 is zero, then $w^2 = -v u_1$, which happens with probability $1/p$. Therefore the probability of finding a solution $(j_1, j_2) \in (\mathbb{Z}_p^*)^2$ is at least $(p-1)/2p - 4/p$. □ □

Theorem 3. *Let G be an extraspecial p-group of exponent p, where p grows with the input size, and let us given an oracle f which hides the subgroup H of G. Then there is an efficient quantum procedure which hides HG' in G.*

Proof. We describe the efficient hiding procedure. It computes, for some $\overline{a} \in G^4$, the superposition

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

which by Lemma 4 can be done efficiently, and then it measures the registers for the u_i. This is repeated until a good $\overline{u} \in \mathbb{Z}_p^4$ is measured. By Lemma 7, this requires a constant expected number of iterations. Also, when a good $\overline{u}$ is measured, it finds efficiently a solution $\overline{j} \in (\mathbb{Z}_p^*)^4$ for system (1). Such a triple $(\overline{a}, \overline{u}, \overline{j})$ is appropriate, and therefore by Lemma 6 $\{|\Psi_g^{\overline{a},\overline{u},\overline{j}}\rangle : g \in G\}$ is hiding for HG' in G. Using the additional input $|g\rangle$, the procedure finally computes $|\Psi_g^{\overline{a},\overline{u},\overline{j}}\rangle$. □ □

The proof of Theorem 2 in that case follows from Theorem 1 and Theorem 3.

4.3 Groups of exponent p^2 when p is large

Here we deal with the group $G = A_p \mathbf{Y}(\mathbf{Y}_{i=1}^{k-1} H_p)$, where we start with a function f hiding some subgroup H. As in Lemma 1, we will distinguish the cases when $G' \subseteq H$ and when $G' \cap H = \{e\}$. The first case is already taken care of by Corollary 1.

If $G' \cap H = \{e\}$ then H contains only elements whose order is at most p. Indeed an element of order p^2 cannot be in H since the p^{th} power of such an element is in G'. Therefore H is a subgroup of $K = \langle y_1, x_2, y_2, \ldots, x_k, y_k, z \rangle$, where x_1 is the unique generator of order p^2 of G. The subgroup K is also (isomorphic to) a subgroup of $\mathbf{Y}_{i=1}^{k} H_p$. We claim that we can extend the restriction of f to K into a function F defined on the whole group $\mathbf{Y}_{i=1}^{k} H_p$ that also hides H. Such an extension can be defined for example as $F(x_1^{i_1} y_1^{j_1} \ldots x_k^{i_k} y_k^{j_k} z^\ell) = (i_1, f(y_1^{j_1} \ldots x_k^{i_k} y_k^{j_k} z^\ell))$, and it is easy to see that it is indeed a hiding function. Therefore the problem is reduced to the HSP in extraspecial groups of exponent p.

5 Concluding remarks

The main technical contribution of the present paper is a quantum procedure which hides HG' in an extrapsecial p-group G where p is a large prime. We remark that it is possible to present the proof of its correctness in terms of irreducible representations of G. However, the present approach is shorter and it does not make use of concepts of noncommutative representation theory. Finally, our method can in turn be

extended to finding hidden subgroups efficiently in arbitrary finite two-step nilpotent groups, that is groups G satisfying $G' \leq Z(G)$. This extension will be the subject of a subsequent paper.

Acknowledgment.

The authors are grateful to Péter Pál Pálfy for his useful remarks and suggestions.

References

[1] M. Aschbacher. *Finite Group Theory*. Cambridge University Press, 2000.

[2] D. Bacon, A. Childs, and W. van Dam. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups. In *Proc. 46th IEEE FOCS*, pages 469–478, 2005.

[3] A. Calderbank, E. Rains, P. Shor and N. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78:405–408, 1997.

[4] A. Calderbank, E. Rains, P. Shor and N. Sloane. Quantum error correction via codes over GF(4). *IEEE Transactions on Information Theory*, 44(4):1369–1387, 1998.

[5] K. Friedl, G. Ivanyos, F. Magniez , M. Santha and P. Sen. Hidden translation and orbit coset in quantum computing. In *Proc. 35th ACM STOC*, pages 1–9, 2003.

[6] D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD Thesis, Caltech, 1997.

[7] M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani. Quantum mechanical algorithms for the non-abelian Hidden Subgroup Problem. In *Proc. 33rd ACM STOC*, pages 68–74, 2001.

[8] S. Hallgren, A. Russell, and A. Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. *SIAM J. Comp.*, 32(4):916–934, 2003.

[9] B. Huppert. *Endliche Gruppen*. Vol. 1, Springer Verlag, 1983.

[10] G. Ivanyos, F. Magniez, and M. Santha. Efficient quantum algorithms for some instances of the non-Abelian hidden subgroup problem. *Int. J. of Foundations of Computer Science*, 14(5):723–739, 2003.

[11] A. Kitaev. Quantum measurements and the Abelian Stabilizer Problem. Technical report, Quantum Physics e-Print archive, 1995. `http://xxx.lanl.gov/abs/quant-ph/9511026`.

[12] A. Klappenecker, P. K. Sarvepalli. Clifford Code Constructions of Operator Quantum Error Correcting Codes Technical report, Quantum Physics e-Print archive, 2006. `http://xxx.lanl.gov/abs/quant-ph/0604161`.

[13] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[14] C. Moore, D. Rockmore, A. Russell, and L. Schulman. The power of basis selection in Fourier sampling: Hidden subgroup problems in affine groups. In *Proc. 15th ACM-SIAM SODA*, pages 1106–1115, 2004.

[15] M. Mosca. *Quantum Computer Algorithms*. PhD Thesis, University of Oxford, 1999.

[16] M. Püschel, M. Rötteler, and T. Beth. Fast quantum Fourier transforms for a class of non-Abelian groups. In *Proc. 13th AAECC*, volume 1719, pages 148–159. LNCS, 1999.

[17] J. Radhakrishnan, M. Rötteler and P. Sen. On the power of random bases in Fourier sampling: hidden subgroup problem in the Heisenberg group. In *Proc. 32nd ICALP*, LNCS vol. 3580, pages 1399–1411, 2005.

[18] M. Rötteler and T. Beth. Polynomial-time solution to the Hidden Subgroup Problem for a class of non-abelian groups. Technical report, Quantum Physics e-Print archive, 1998. http://xxx.lanl.gov/abs/quant-ph/9812070.

[19] P. Shor. Algorithms for quantum computation: Discrete logarithm and factoring. *SIAM J. Comp.*, 26(5):1484–1509, 1997.

[20] V. Shoup. *A Computational Introduction to Number Theory and Algebra.* Cambridge University Press, 2005.

[21] D. Simon. On the power of quantum computation. *SIAM J. Comp.*, 26(5):1474–1483, 1997.