An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups [*]

Gábor Ivanyos[†] Luc Sanselme[‡] Miklos Santha[§]

March 2, 2010

Abstract

In this paper we show that the hidden subgroup problem in nil-2 groups, that is in groups of nilpotency class at most 2, can be solved efficiently by a quantum procedure. The algorithm is an extension of our earlier method for extraspecial groups in [13], but it has several additional features. It contains a powerful classical reduction for the hidden subgroup problem in nilpotent groups of constant nilpotency class to the specific case where the group is a p-group of exponent p and the subgroup is either trivial or cyclic. This reduction might also be useful for dealing with groups of higher nilpotency class. The quantum part of the algorithm uses well chosen group actions based on some automorphisms of nil-2 groups. The right choice of the actions requires the solution of a system of quadratic and linear equations. The existence of a solution is guaranteed by the Chevalley-Warning theorem, and we prove that it can also be found efficiently.

Key words: Quantum computing, efficient algorithm, hidden subgroup problem, nilpotent group.

[*] Research supported by the European Commission IST Integrated Project Qubit Applications (QAP) 015848, the OTKA grants NK72845 and T77476, the French ANR QRAC project under contract ANR-08-EMER-012 and by the CNRS-MTA joint project 21434. A preliminary version of this paper was presented at the 8th Latin American Theoretical Informatics Symposium (LATIN'08), LNCS vol. 4957, pages 759-771, 2008.

[†] Computer and Automation Research Institute of the Hungarian Academy of Sciences, Kende u. 13-17, H-1111 Budapest, Hungary. Phone: +36 1 2796164, Fax: +36 1 2095269, E-mail: Gabor.Ivanyos@sztaki.hu

[‡] LRI, Université Paris–Sud 91405 Orsay, France. E-mail: luc.sanselme@laposte.net

[§] LRI, Univ. Paris-Sud, CNRS; F-91405 Orsay, France and Centre for Quantum Technologies, National University of Singapore, Singapore 117543. E-mail: Miklos.Santha@lri.fr. Research at the Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation.

1 Introduction

Efficient solutions to some cases of the hidden subgroup problem (HSP), a paradigmatic group theoretical problem, constitute probably the most notable successes of quantum computing. The problem consists in finding a subgroup H in a finite group G hidden by some function which is constant on each coset of H and is distinct on different cosets. The hiding function can be accessed by an oracle, and in the overall complexity of an algorithm, a query counts as a single computational step. To be efficient, an algorithm has to be polylogarithmic in the order of G. While classically even no algorithms of polynomial query complexity are possible for the HSP, it can be solved efficiently in abelian groups by a quantum algorithm. A detailed description of the so called standard algorithm can be found for example in [19]. The main quantum tool of this algorithm is Fourier sampling, based on the efficiently implementable Fourier transform in abelian groups. Factorization and discrete logarithm [28] are special cases of this solution.

After the settling of the abelian case, substantial research was devoted to the HSP in some finite non-abelian groups. Beside being the natural generalization of the abelian case, the interest of this problem is enhanced by the fact that important algorithmic problems, such as graph isomorphism, can be cast in this framework. The standard algorithm has been extended to some non-abelian groups by Rötteler and Beth [25], Hallgren, Russell and Ta-Shma [9], Grigni, Schulman, Vazirani and Vazirani [7] and Moore, Rockmore, Russell and Schulman [21]. For the Heisenberg group, Bacon, Childs and van Dam [1] used the pretty good measurement to reduce the HSP to some matrix sum problem that they could solve classically. Ivanyos, Magniez and Santha [12] 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. This latter approach was used recently by Ivanyos, Sanselme and Santha [13] for extraspecial groups.

The so far unknown complexity of two special cases of the HSP would be of particular interest. The first one is the hidden subgroup problem in the symmetric group because it contains as special instance the graph isomorphism problem. Recently, Moore, Russell and Sniady [22] have shown that no algorithm based one a particular approach can solve the graph isomorphism problem efficiently. The other one is the hidden subgroup problem in the dihedral group because of its relation to certain lattice problems investigated by Regev [26].

In this work we extend the family of groups where the HSP is efficiently solvable by a quantum algorithm to nilpotent groups of nilpotency class at most 2 (nil-2 groups, in short). These are groups whose lower (and upper) central series are of length at most 2. Equivalently, a group is nil-2 group if the derived subgroup is contained in the center. Nilpotent groups form a rich subclass of solvable groups, they contain for example all (finite) p-groups. Extraspecial groups are, in particular, in nil-2 groups. Our main result is:

Theorem 1. *Let G be a nil-2 group, and let f be an oracle that hides the subgroup H of G. Then there is an efficient quantum procedure which finds H.*

The overall structure of the algorithm presented here is closely related to the algorithm in [13] for extraspecial groups, but has also several additional features. The quantum part of the algorithm is restricted to specific nil-2 groups, which are also p-groups and are of exponent p. It consists essentially in the creation of a quantum hiding procedure (a natural quantum generalization of a hiding function) for the subgroup HG' of G, where G' stands for the derived (a.k.a. commutator) subgroup of G. The procedure uses certain automorphisms of the groups to define some appropriate group actions, and is analogous to what has been done in [13] for extraspecial p-groups of exponent p.

While dealing with extraspecial p-groups of exponent p basically solves the HSP for all extraspecial groups (the case of remaining groups, of exponent p^2, easily reduces to groups of exponent p), this is far from being true for nil-2 groups. Indeed, one of the main new features of the current algorithm is a classical reduction of the HSP in nil-2 groups to the HSP in p-groups of exponent p and nilpotency class at most 2, where moreover the hidden subgroup is either trivial or of cardinality p. In fact, our result is much more general: we prove an analogous reduction in nil-k groups for any constant k. We believe that this general reduction might be useful for designing efficient quantum algorithms for the HSP in groups of higher nilpotency class.

Our second main novel feature concerns the quantum hiding procedure for HG'. While in extraspecial groups it was reduced to the efficient solvability of a single quadratic and a single linear equation modulo p, here we look for a nontrivial solution of a homogeneous system of d quadratic and d linear equations, where d can be any integer. The reason for this is that while in extraspecial groups the derived subgroup is one dimensional, in nil-2 groups we have no a priori bound on its dimension. If the number of variables exceeds the global degree of the system then the solvability itself is an immediate consequence of the Chevalley-Warning theorem [3, 29]: the number of solutions is divisible by p and therefore there is always a nontrivial one. (See [20] for the complexity theory aspects of search problems where existence of solution is granted by mathematical theorems.) Our result is that if the number of variables is sufficiently large, more precisely is of $\Omega(d^3)$, then we can also *find* a nontrivial solution in polynomial time.

The structure of the paper is the following. In Section 2 we briefly describe the extension of the standard algorithm for quantum hiding procedures, and then we discuss some basic properties of nilpotent groups, in particular p-groups of exponent p and of nilpotency class at most 2. Section 3 contains the description of the classical reduction of the HSP in groups of constant nilpotency class to instances where the group is also p-group of exponent p, and the subgroup is either trivial or cyclic of order p. Section 4 gives the description of the quantum algorithm in p-groups of exponent p and of nilpotency class at most 2: we briefly describe the reduction of finding H to the design of an efficient hiding procedure for HG', and prove the existence of such a procedure. Finally Section 5 gives the proof of the efficient solvability of the system of quadratic and linear equations occurring in the design of the hiding procedure.

Even if the hidden subgroup problem is hard for the symmetric group and also for general solvable groups, it may happen that there is an efficient solution in nilpotent groups. The works [1, 13] and this paper can be considered as the first steps in investigating the complexity of the HSP for this family of groups.

2 Preliminaries

2.1 Extension of the standard algorithm for the abelian HSP

We will use standard notions of quantum computing for which one can consult for example [23]. 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 that occur in $|\Psi\rangle$ with non-zero amplitude.

The standard algorithm for the abelian HSP repeats polynomially many times Fourier sampling involving the same hiding function, to obtain in each iteration a random element from the subgroup orthogonal to the hidden subgroup. In fact, for repeated Fourier samplings, the existence of a common hiding function can be relaxed in several ways. Firstly, in different iterations different hiding functions can be used, and secondly, classical hiding functions can be replaced by quantum hiding functions. This was formalized in [13], and we recall here the precise definition.

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 $g_1, \ldots, g_N \in G$, on input $|g_1\rangle \ldots |g_N\rangle|0\rangle$ it outputs $|g_1\rangle \ldots |g_N\rangle|\Psi^1_{g_1}\rangle \ldots |\Psi^N_{g_N}\rangle$, where $\{|\Psi^i_g\rangle : g \in G\}$ is a hiding set for H for all $1 \leq i \leq N$.

The following fact whose proof is immediate from Lemma 1 in [12] 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.*

2.2 Nilpotent 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_1g_2. We write $H \leq G$ if H is a subgroup of G, and $H < G$ if it is a proper subgroup. Normal subgroups and proper normal subgroups will be denoted respectively by $H \trianglelefteq G$ and $H \triangleleft G$. For a subset X of G, let $\langle X \rangle$ be the subgroup generated by X. The *normalizer* of X in G is $N_G(X) = \{g \in G \ : \ gX = Xg\}$. 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.

The commutator $[x, y]$ of elements x and y is $x^{-1}y^{-1}xy$. For two subgroups X and Y of G, let $[X, Y]$ be $\langle\{[x, y] \ : \ x \in X, y \in Y\}\rangle$. The commutator subgroup or derived subgroup G' of G is defined as $[G, G]$, and its center $Z(G)$ as $\{z \in G \ : \ gz = zg \text{ for all } g \in G\}$. The *lower central series* of G is the series of subgroups $G = A_1 \trianglerighteq A_2 \trianglerighteq A_3 \ldots$, where $A_{i+1} = [A_i, G]$ for every $i \geq 1$. The *upper central series* of G is the series of subgroups $\{1\} = Z_0 \trianglelefteq Z_1 \trianglelefteq Z_2 \ldots$, where $Z_{i+1} = \{x \in G \ : \ [x, g] \in Z_i \text{ for all } g \in G\}$ for every $i \geq 0$. Clearly $A_2 = G'$ and $Z_1 = Z(G)$. The group G is *nilpotent* if there is a natural number n such that $A_{n+1} = \{1\}$. If n is the smallest integer such that $A_{n+1} = \{1\}$ then G is *nilpotent of nilpotency class n*. It is a well known fact that G is nilpotent of nilpotency class n if and only if $Z_n = G$ in the upper central series. Nilpotent groups of nilpotency class 1 are simply the nontrivial abelian groups. A nilpotent group of nilpotency class at most n is called a *nil-n* group.

A detailed treatment of nilpotent groups can be found for example in Hall [8]. Let us just recall here that nilpotent groups are solvable, and that every p-group is nilpotent, where a p-group is a finite group whose order is a power of some prime number p.

2.3 Nil-2 p-groups of exponent p

It is clear from the definition of nilpotent groups that G is a nil-2 group if $G' \leq Z(G)$. It is easy to see that this property implies that the commutator is a bilinear function in the following sense.

Fact 2. *Let G be a nil-2 group. Then for every g_1, g_2, g_3, g_4 in G,*

$$[g_1g_2, g_3g_4] = [g_1, g_3][g_1, g_4][g_2, g_3][g_2, g_4].$$

The quantum part of our algorithm will deal only with special nilpotent groups of nilpotency class 2, which are also p-groups and are of exponent p. The structure of these special groups is well known, and is expressed in the following simple fact.

Fact 3. *Let G be a p-group of exponent p and of nilpotency class at most 2. Then there exist integers $m > 0$ and $d \geq 0$, group elements $x_1, \dots, x_m \in G$ and $z_1, \dots, z_d \in G'$ such that*

1. *$G/G' \cong \mathbb{Z}_p^m$ and $G' \cong \mathbb{Z}_p^d$,*
2. *for every $g \in G$ there exists a unique $(e_1, \dots, e_m, f_1, \dots f_d) \in \mathbb{Z}_p^{m+d}$ such that*

$$g = x_1^{e_1} \dots x_m^{e_m} z_1^{f_1} \dots z_d^{f_d},$$

3. *$G = \langle x_1, \dots, x_m \rangle$ and $G' = \langle z_1, \dots, z_d \rangle$.*

We will say that a p-group G of exponent p and of nilpotency class at most 2 has parameters (m, d) if $G/G' \cong \mathbb{Z}_p^m$ and $G' \cong \mathbb{Z}_p^d$. In those groups we will identify G' and $\mathbb{Z}_p^d$. Thus, for two elements z and z' of G', the product zz' is just $z \oplus z'$ where $\oplus$ denotes the coordinate-wise addition modulo p. If G is a such a group then $|G| = p^{m+d}$. The elements of G can be encoded by binary strings of length $O((m + d) \log p)$, and therefore, an efficient algorithm on input G has to be polynomial in m, d and $\log p$.

For $j = 0, 1, \dots, p - 1$, we consider maps

$$\phi_j : x_1^{e_1} \cdots x_m^{e_m} z_1^{f_1} \cdots z_m^{f_m} \mapsto x_1^{je_1} \cdots x_m^{je_m} z_1^{j^2 f_1} \cdots z_m^{j^2 f_m}. \tag{1}$$

Proposition 1. *Let G be a p group of nilpotency class and most 2 and of exponent p. Then the maps ϕ_j defined in (1) for $j = 0, \dots, p - 1$ are group endomorphisms of G. Actually, $\phi_1, \dots, \phi_{p-1}$ are automorphisms of G.*

Proof. Assume that G has parameters (m, d). For $i, k \in \{1, \dots, m\}$ and $\ell \in \{1, \dots, d\}$ define elements γ_{ik}^ℓ such that

$$[x_i, x_j] = \prod_{\ell=1}^{d} z_\ell^{\gamma_{ij}^\ell}.$$

(We use the notation $\prod$ for products in the commutative group G'.) Fact 2 implies that

$$[x_k^{e_k}, x_i^{e'_i}] = \prod_{\ell=1}^{d} z_\ell^{\gamma_{ki}^\ell e_k e'_i},$$

whence

$$\begin{aligned} x_1^{e_1}\cdots x_m^{e_m} z_1^{f_1}\cdots z_m^{f_m} \quad &\cdot \quad x_1^{e'_1}\cdots x_m^{e'_m} z_1^{f'_1}\cdots z_m^{f'_m} \\ &= \quad x_1^{e_1+e'_1}\cdots x_m^{e_m+e'_m}\prod_{\ell=1}^{d} z_\ell^{\,f_\ell+f'_\ell+\sum\limits_{i=1}^{m}\sum\limits_{k=i+1}^{m}\gamma_{ki}^{\ell} e_k e'_i} \end{aligned}$$

and

$$\begin{aligned} x_1^{je_1}\cdots x_m^{je_m} z_1^{j^2 f_1}\cdots z_m^{j^2 f_m} \quad &\cdot \quad x_1^{je'_1}\cdots x_m^{je'_m} z_1^{j^2 f'_1}\cdots z_m^{j^2 f'_m} \\ &= \quad x_1^{j(e_1+e'_1)}\cdots x_m^{j(e_m+e'_m)}\prod_{\ell=1}^{d} z_\ell^{\,j^2\left(f_\ell+f'_\ell+\sum\limits_{i=1}^{m}\sum\limits_{k=i+1}^{m}\gamma_{ki}^{\ell} e_k e'_i\right)}, \end{aligned}$$

therefore $\phi_j(gg') = \phi_j(g)\phi_j(g')$, where $g = x_1^{e_1}\cdots x_m^{e_m} z_1^{f_1}\cdots z_m^{f_m}$ $g' = x_1^{e'_1}\cdots x_m^{e'_m} z_1^{f'_1}\cdots z_m^{f'_m}$. This shows that the maps ϕ_j are endomorphisms of G. If $j \neq 0$ then the kernel of ϕ_j consists obviously of the identity element only and therefore ϕ_j is an automorphism. □

We will exploit the following properties of the automorphisms ϕ_j.

Proposition 2. *Let G be a p-group of exponent p and of nilpotency class at most 2. Then the mappings ϕ_j have the following properties:*

1. $\forall j \in \mathbb{Z}_p, \forall z \in G', \quad \phi_j(z) = z^{j^2}$,

2. $\forall g \in G, \exists z_g \in G', \forall j \in \mathbb{Z}_p, \quad \phi_j(g) = g^j z_g^{j-j^2}$.

Proof. The first statement is obvious from the definition of ϕ_j. To see the second statement, let g be an element of G and let j_0 be a fixed primitive element of $\mathbb{Z}_p^*$. From the definition of ϕ_j one can see that $\phi_{j_0}(g) = g^{j_0}s$ for some $s \in G'$. Put $z_g = s^{(j_0-j_0^2)^{-1}}$. We have $\phi_{j_0}(g) = g^{j_0} z_g^{j_0-j_0^2}$. Let $k = gz_g$, then $\phi_{j_0}(k) = g^{j_0} z_g^{j_0-j_0^2} z_g^{j_0^2} = k^{j_0}$. Therefore, for all $j \in \mathbb{Z}_p$, we have $\phi_j(k) = k^j$ and $\phi_j(g) = \phi_j(k)\phi_j(z_g^{-1}) = g^j z_g^j z_g^{-j^2}$.

□

Clearly, for every $g \in G$, the element z_g whose existence is stated in the second part of Proposition 2, is unique. From now on, let z_g denote this unique element.

One of the remarkable properties of the automorphisms ϕ_j is that they preserve subgroups modulo the derived subgroup G': Let H be a subgroup of G. Then $\phi_j(HG') = HG'$ for every $j = 1, \ldots, p-1$. Indeed, by the first statement of Proposition 2, $\phi_j(G') = G'$, and the second statement implies that ϕ_j preserves cyclic, and therefore all, subgroups modulo G'.

3 Classical reductions in groups of constant nilpotency class

In order to present the reduction methods in a sufficiently general way, in this section we assume that our groups are presented in terms of so-called *refined polycyclic presentations* [10]. Such a presentation of a finite solvable group G is based on a sequence $G = G_1 \rhd \ldots \rhd G_{s+1} = \{1\}$, where for each $1 \leq i \leq s$ the subgroup G_{i+1} is a normal subgroup of G_i and the factor group G_i/G_{i+1} is cyclic of prime order r_i. For each $i \leq s$ an element $g_i \in G_i \setminus G_{i+1}$ is chosen. Then $g_i^{r_i} \in G_{i+1}$. Every element g of G can be uniquely represented as a product of the form $g_1^{e_1} \cdots g_s^{e_s}$, called the normal word for g, where $0 \leq e_i < r_i$.

In the abstract presentation the generators are $g_1, \ldots, g_s$, and for each index $1 \leq i \leq s$, the following relations are included:

- $g_i^{r_i} = u_i$, where $u_i = g_{i+1}^{a_{i,i+1}} \cdots g_s^{a_{i,s}}$ is the normal word for $g^{r_i} \in G_{i+1}$,
- $g_i^{-1} g_j g_i = w_{ij}$ for every $j > i$, where $w_{ij} = g_{i+1}^{b_{i,j,i+1}} \cdots g_s^{b_{i,j,s}}$ is the normal word for $g_i^{-1} g_j g_i \in G_{i+1}$.

We assume that elements of G are encoded by normal words and there is a polynomial time algorithm in $\log |G|$, the so called *collection procedure*, which computes normal words representing products.

Efficiency of most algorithms for computing with polycyclic presentations depends on existence of an efficient collection procedure. Although there are several methods which work well in practice and even some method whose complexity is polynomial (in $\log |G|$, that is in $\sum_{i=1}^{s} \log r_i$) in special cases (see [16, 17, 6]), it is an open question whether there exists a polynomial time collection procedure in general finite polycyclic groups. In nilpotent groups of constant nilpotency class, the complexity of the collection method proposed by Leedham-Green and Soicher [17] is polynomial (in $\log |G|$, i.e., in $\sum \log r_i$) for polycyclic presentations of restricted form, where the series $G = G_1 \rhd \ldots \rhd G_{s+1} = \{1\}$ satisfies $[G, G_j] \leq G_{j+1}$. For a more general method with careful complexity analysis which works for arbitrary polycyclic presentations which works in polynomial time in groups of constant nilpotency class we refer the reader to Höfling's work [11]. (Actually, in a general finite solvable group the complexity of Höfling's method is $(\log |G|)^{O(t)}$, where t is the so called *derived length* of G, which, for a nilpotent group, is logarithmic in the nilpotency class.)

Having a polynomial time collection procedure at hand for a family of nilpotent groups, refined polycyclic presentations for subgroups and factor groups can be obtained in polynomial time [10]. There are also polynomial time methods for computing the Sylow subgroups, as well as the center and the commutator. Furthermore, in p-groups with refined polycyclic presentation, normalizers of subgroups can be computed in polynomial time using the technique of [4], combined with the subspace stabilizer algorithm of [18].

Finally we remark that, using a quantum implementation [12] of an algorithm of Beals and Babai [2], a refined polycyclic presentation for a solvable black box group can be computed in polynomial time. Therefore our choice of the model for computing with nilpotent groups is not really restrictive.

Our first theorem is a classical reduction for the HSP in groups of constant nilpotency class. The proof is given by the subsequent three lemmas.

Theorem 2. *Let $\mathcal{C}$ be a family of groups of nilpotency class bounded by a constant. Assume that $\mathcal{C}$ is closed under taking subgroups and factor groups. Then the hidden subgroup problem in members of $\mathcal{C}$ can be reduced to the case where the group is a p-group of exponent p, and the the subgroup is either trivial or of cardinality p.*

Corollary 1. *The hidden subgroup problem in nil-2 groups can be reduced to the case where the group is a p-group of exponent p, and the the subgroup is either trivial or of cardinality p.*

Lemma 1. *Let $\mathcal{C}$ be a family of groups of nilpotency class bounded by a constant. Assume that $\mathcal{C}$ is closed under taking subgroups and factor groups. Then the HSP in $\mathcal{C}$ can be reduced to the HSP of p-groups belonging to $\mathcal{C}$.*

Proof. As a nilpotent group G is the direct product of its Sylow subgroups, any subgroup H of G is the product of its intersections with the Sylow subgroups of G. □

Lemma 2. *Let $\mathcal{C}$ be a family of p-groups of nilpotency class bounded by a constant. Assume that $\mathcal{C}$ is closed under taking subgroups and factor groups. Then the hidden subgroup problem in members of $\mathcal{C}$ can be reduced to the case where the subgroup is either trivial or of cardinality p.*

Proof. Assume that we have a procedure $\mathcal{P}$ which finds hidden subgroups in $\mathcal{C}$ under the promise that the hidden subgroup is trivial or is of order p. Let G be a group in $\mathcal{C}$ and let f be a function on G hiding the subgroup H of G. We describe an iterative procedure which uses $\mathcal{P}$ as a subroutine and finds H in G. The basic idea is to compute a refined polycyclic sequence $G = G_1 \rhd \ldots \rhd G_s \rhd 1$ for G and to proceed calling $\mathcal{P}$ on the subgroups in the sequence starting with G_s. When $\mathcal{P}$ finds for the first time a nontrivial subgroup generated by h, then we would like to restart the process in $G/\langle h\rangle$, and at the end, collect all the generators. Since $\langle h\rangle$ is not necessarily a normal subgroup of G we will actually restart the process instead in $N_G(\langle h\rangle)$.

More formally, let us suppose that f hides H in G, and let $\widetilde{H}$ be some subgroup of H. Then f hides $N_G(\widetilde{H}) \cap H$ in $N_G(\widetilde{H})$, and therefore it hides $(N_G(\widetilde{H}) \cap H)/\widetilde{H}$ in $N_G(\widetilde{H})/\widetilde{H}$. We consider the following algorithm:

Algorithm 1

```
success:= TRUE, $\widetilde{H} = \{1\}$.
while success=TRUE do
  if $G \neq \widetilde{H}$ then
    compute $N_G(\widetilde{H})/\widetilde{H} = G_1 \rhd \ldots \rhd G_s \rhd 1$ a refined polycyclic representation
    $i := s$
    while $i > 0$ do
      call $\mathcal{P}$ on $G_i$
      if $\mathcal{P}$ returns $\langle h\rangle$ then
        $\widetilde{H} := \langle \widetilde{H} \cup \{h\}\rangle, i = 0$
      else
        $i := i - 1$
        if $i = 0$ then
          success := FALSE
        end if
      end if
    end while
  else
    success:=FALSE
  end if
end while
```

Algorithm 1 stops when the subgroup $\widetilde{H}$ is such that $(N_G(\widetilde{H}) \cap H)/\widetilde{H} = \{1\}$, that is when $N_G(\widetilde{H}) \cap H = \widetilde{H}$. We claim that this implies $\widetilde{H} = H$. Indeed, suppose that $\widetilde{H}$ is a proper subgroup of H. Since in nilpotent groups a proper subgroup is also a proper subgroup of its normalizer (Corollary 10.3.1 in [8]), $\widetilde{H}$ is also a proper subgroup of $N_H(\widetilde{H}) = N_G(\widetilde{H}) \cap H$.

Finally observe that the whole process makes $O(\log_p^2 |G|)$ calls to $\mathcal{P}$.

□

Lemma 3. *Let $\mathcal{C}$ be a family of p-groups of nilpotency class bounded by a constant. Assume that $\mathcal{C}$ is closed under taking subgroups and factor groups. Then the instances of the hidden subgroup problem in members of $\mathcal{C}$, when the subgroup is either trivial or of cardinality p, can be reduced to groups in $\mathcal{C}$ of exponent p.*

Proof. If G/G' has exponent larger than p then H is obviously contained in the proper subgroup $G_0 = \{x \in G | x^p \in G'\}$. G_0 can be efficiently computed by observing that $g_1, \ldots, g_t$ is an irredundant system of generators for G then G_0 is generated by G' and $g_1^{p^{\alpha_1 - 1}}, \ldots, g_t^{p^{\alpha_t - 1}}$, where p^{α_i} is the order of $g_i G'$ in the factor group G/G' ($i = 1, \ldots, t$). (By Theorems 10.4.1 and 10.4.3 of [8], an irredundant system of generators for G does not contain elements from G' and hence $\alpha_i > 0$.) Therefore we can replace G by the subgroup G_0. We can repeat this procedure until the exponent of G/G' becomes p. Theorem 5.2.5 of [24] states that taking commutators of elements of A_i by elements of G induces a homomorphism of $G/G' \otimes A_i/A_{i+1}$ for every integer $1 \leq i \leq c$, where $G = A_1 \rhd A_2 \rhd A_3 \ldots \rhd A_c \rhd A_{c+1} = \{1\}$ is the lower central series of G and c the nilpotency class of G. (The notation $\otimes$ is used for the tensor product of $\mathbb{Z}$-modules, i.e., Abelian groups.) Induction based on this theorem proves that if the G/G' is of exponent p then so are all the factors A_i/A_{i+1}, and therefore the exponent of G is at most p^c. (Indeed, for every $g \in G$ we see by induction on i that $g^{p^i} \in A_{i+1}$, whence $g^{p^c} = 1$.)

Now if p is not larger than the nilpotency class c of G then G has exponent at most the constant c^c and the algorithm of [5] is applicable. Otherwise the elements of order p or 1 form a subgroup G^*, see Chapter 12 of [8]. The hidden subgroup H is also a subgroup of G^* since $|H| \leq p$. The function hiding H in G also hides it in G^*, therefore the reduction will consist in determining G^*.

We design an algorithm that finds G^* by induction on the length of refined polycyclic presentations. If $|G| = p$ then $G^* = G$. Otherwise, let $G = G_1 \rhd G_2 \rhd \ldots \rhd G_s \rhd \{1\}$ be a refined polycyclic presentation with $s \geq 2$. It is easy to construct a presentation where G_s is a subgroup of the center of G, which we suppose from now on. For the ease of notation we set $M = G_2$ and $N = G_s$.

We first describe the inductive step in a simplified case, with the additional hypothesis $(G/N)^* = G/N$. Observe that the hypothesis is equivalent to saying that the map $\phi : x \mapsto x^p$ sends every element of G into N. From this it is also clear that the hypothesis carries over to M, that is $(M/N)^* = M/N$. We further claim that either $G^* = G$ or G^* is a subgroup of G of index p. In fact this follows Theorem 12.4.4 of [8] which states that the map ϕ is constant on cosets of G^* and distinct on different cosets. From a polycyclic presentation of G it can be read off whether or not $G = G^*$. If $G^* = G$ we are done. Otherwise we compute inductively M^*. If $M^* = M$ then $G^* = M$. If M^* is a proper subgroup of M then M^* has index p^2 in G. (To see this, observe that $M^* = M \cap G^*$, whence $|M/M^*| = |M/(G^*/M)| = |MG^*/G^*|$ by the isomorphism theorem, therefore $|M/M^*| = |MG^*/G^*| \leq |G/G^*| = p$.) Pick an arbitrary $u \in M \setminus M^*$ and $y \in G \setminus M$. By the assumptions, $u^p = g_s^{j_u}$ for some integer $0 < j_u < p$, and $y^p = g_s^{j_y}$ for some integer $0 \leq j_y < p$. Recall that in the polycyclic presentation model, computing normal words for u^p and y^p – using fast exponentiation – amounts to computing j_u and j_y. Set $x = u^{j_y j_u^{-1}}$. For this x

we have $x^p = y^p$, and therefore $xy^{-1} \in G^*$, again by Theorem 12.4.4 of [8]. Since $xy^{-1} \in G^* \setminus M^*$, we have $G^* = \langle M^*, xy^{-1}\rangle$.

In the general case first $(G/N)^*$ is computed inductively. If $(G/N)^* = G/N$ then one proceeds as in the simplified case. Otherwise we set $K = (G/N)^*N$. We claim that $G^* = K^*$. For this we will show that $G^* \subseteq K$. To see this, let x be an element of G^*. Then $x = yz$ where $y \in G/N$ and $z \in N$. We show that y is in $(G/N)^*$ which implies that $x \in K$. Indeed, $y^p = y^p z^p = (yz)^p = 1$, where the first equality follows from $|N| = p$, the second from $N \leq Z(G)$ and the third from $x \in G^*$. Finally observe that $(K/N)^* = K/N$ since $K/N = (G/N)^*$. Therefore one can determine K^* inductively as in the simplified case.

Let $c(s)$ denote the number of recursive calls when the length of a presentation is s. In the simplified case the number of calls is $s-1$. Therefore in the general case we have $c(s) = c(s-1)+s-2$, whose solution is $c(s) = O(s^2)$.

□

4 The quantum algorithm

The quantum part of our algorithm, up to technicalities, follows the same lines as the algorithm given in [13] for extraspecial groups.

Theorem 3. *Let G be a p-group of exponent p and of nilpotency class 2, and let f be an oracle f which hides a subgroup H of G whose cardinality is either 1 or p. If we have an efficient quantum procedure (using f) which hides HG' in G then H can be found efficiently.*

Proof. First observe that finding H is efficiently reducible to finding HG'. Indeed, HG' is an abelian subgroup of G since H is abelian. The restriction of the hiding function f to HG' of G hides H. Therefore the standard algorithm for solving the HSP in abelian groups applied to HG' with oracle f yields H.

Let us now suppose that G has parameters (m, d). We will show that finding HG' can be efficiently reduced to the hidden subgroup problem in an abelian group. Let us denote for every element $g = x_1^{e_1} \dots x_m^{e_m} z_1^{f_1} \dots z_d^{f_d}$ of G, by $\overline{g}$ the element $x_1^{e_1} \dots x_m^{e_m}$. We define 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. In fact, the group $\overline{G}$ is isomorphic to G/G' and therefore is isomorphic to $\mathbb{Z}_p^m$. For our purposes a nice way to think about $\overline{G}$ as a representation of G/G' with unique encoding. Observe also that $HG' \cap \overline{G}$ is a subgroup of $(\overline{G}, *)$ because HG'/G' is a subgroup of G/G'. Since $HG' = (HG' \cap \overline{G})G'$, finding HG' is efficiently reducible to finding $HG' \cap \overline{G}$ in $\overline{G}$.

To finish the proof, let us remark that 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 $HG' \cap \overline{G}$. □

Now we turn to the construction of the hiding procedure for HG'. The basic idea is the following. Suppose that we could create, for some $a \in G$, the coset state $|aHG'\rangle$. Then the group action $g \to |aHG' \cdot g\rangle$ is a hiding procedure for the subgroup HG'. (In general, for $a \in G$ and $K \leq G$ the map $g \to |aKg\rangle$ is a hiding procedure for *right* cosets of K. In our case the subgroup HG' is normal therefore the left and right cosets are the same.) Unfortunately, we are able to create states of the form $|aHG'\rangle$ efficiently when p and d are constant. In general, we can create efficiently $|aHG'_u\rangle$ for random $a \in G$ and an independent random $u \in G'$, where by definition

$$|G'_u\rangle = \frac{1}{\sqrt{|G'|}} \sum_{z \in \mathbb{Z}_p^d} \omega^{-<u,z>} |z\rangle. \tag{2}$$

Then $|aHG'_u \cdot h\rangle = |aHG'_u\rangle$ for every $h \in H$, and $|G'_u \cdot z\rangle = \omega^{<u,z>}|G'_u\rangle$. To cancel the disturbing phase $\omega^{<u,z>}$ we will use more sophisticated group action via the group automorphisms ϕ_j on several copies of the states $|aHG'_u\rangle$. We remark that, over extraspecial groups, this idea has an interpretation in terms of Fourier sampling in noncommutative groups and Clebsch-Gordan transforms (decomposition of tensor products of irreducible representations), see [15]. We formulate our result as follows.

Theorem 4. *Let G be a p-group of exponent p and of nilpotency class 2, and let f be an oracle f which hides a subgroup H of G. Then there is an efficient quantum procedure which hides HG' in G.*

Proof. The proof is segmented into several statements. The first lemma states that we can indeed create the states $|aHG'_u\rangle$ efficiently, where G'_u is defined as in (2).

Lemma 4. *There is an efficient quantum procedure which creates $\frac{1}{\sqrt{p^d}} \sum_{u \in \mathbb{Z}_p^d} |u\rangle|aHG'_u\rangle$ 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 $\mathbb{Z}_p^d$ to the first register gives $|\mathbb{Z}_p\rangle|aH\rangle$. Multiplying the second register by the opposite of the first one results in $\frac{1}{\sqrt{p^d}} \sum_{z \in \mathbb{Z}_p^d} |-z\rangle|aHz\rangle$. A final Fourier transform in the first register creates the required superposition. □

Our next lemma which is an immediate consequence of Proposition 2 claims 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. $\forall z \in \mathbb{Z}_p^d, \forall a \in G, \forall u \in \mathbb{Z}_p^d, \forall j \in \mathbb{Z}_p, \quad |aHG'_u \cdot \phi_j(z)\rangle = \omega^{<u,z>j^2}|aHG'_u\rangle,$
2. $\forall h \in H, \forall a \in G, \forall u \in \mathbb{Z}_p^d, \forall j \in \mathbb{Z}_p, \quad |aHG'_u \cdot \phi_j(h)\rangle \;=\; \omega^{<u,z_h>(j-j^2)}|aHG'_u\rangle.$

The principal idea now is to take several copies of the states $|a_i HG'_{u_i}\rangle$ and choose the j_i so that the product of the corresponding eigenvalues becomes the unity. Therefore the combined actions $\phi_{j_i}(g)$, when g is from HG', will not modify the combined state. It turns out that we can achieve this with a sufficiently big enough number of copies. Let $n = n(d)$ some function of d to be determined later.

For $\overline{a} = (a_1, \dots, a_n) \in G^n$, $\overline{u} = (u_1, \dots, u_n) \in (\mathbb{Z}_p^d)^n$, $\overline{j} = (j_1, \dots, j_n) \in (\mathbb{Z}_p)^n \setminus \{0^n\}$ and $g \in G$, we define the quantum state $|\Psi_g^{\overline{a},\overline{u},\overline{j}}\rangle$ in $\mathbb{C}^{G^n}$ by

$$|\Psi_g^{\overline{a},\overline{u},\overline{j}}\rangle = \bigotimes_{i=1}^{n} |a_i HG'_{u_i} \cdot \phi_{j_i}(g)\rangle.$$

Our purpose is to find an efficient procedure to generate triples $(\overline{a}, \overline{u}, \overline{j})$ such that for every g in HG', $|\Psi_g^{\overline{a},\overline{u},\overline{j}}\rangle = \bigotimes_{i=1}^{n} |a_i HG'_{u_i}\rangle$. 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 let $1 \leq i \leq n$ such that $j_i \neq 0$. The elements $\phi_{j_i}(g_1)$ and $\phi_{j_i}(g_2)$ are in different cosets of HG' in G since ϕ_{j_i} is an automorphism of G. Also, we have $\mathsf{supp}(|aHG'_u\rangle) = \mathsf{supp}(|aHG'\rangle)$, and therefore $\mathsf{supp}(|aHG'_u \cdot \phi_{j_i}(g_1)\rangle)$ and $\mathsf{supp}(|aHG'_u \cdot \phi_{j_i}(g_2)\rangle)$ are included in different cosets and are disjoint. Thus 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 for all $1 \leq i \leq n$, we have $\phi_{j_i}(g_1) = \phi_{j_i}(g)\phi_{j_i}(g_2)$. 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 $G^n \times (\mathbb{Z}_p^d)^n \times (\mathbb{Z}_p)^n \setminus \{0^n\}$, and let g be an element of HG'. Then $g = hz$ for some $h \in H$ and $z \in \mathbb{Z}_p^d$, and $\phi_{j_i}(g) = \phi_{j_i}(h)\phi_{j_i}(z)$ for $i = 1, \dots, n$. By Lemma 5, we have $|a_i HG'_{u_i} \cdot \phi_{j_i}(z)\rangle = \omega^{<u_i,z>j_i^2}|a_i HG'_{u_i}\rangle$, and $|a_i HG'_{u_i} \cdot \phi_{j_i}(h)\rangle = \omega^{<u_i,z_h>(j_i - j_i^2)}|a_i HG'_{u_i}\rangle$, and therefore

$$|\Psi_g^{\overline{a},\overline{u},\overline{j}}\rangle = \omega^{\sum_{i=1}^{n} <u_i,z_h>(j_i - j_i^2) + <u_i,z>j_i^2} \bigotimes_{i=1}^{n} |a_i HG'_{u_i}\rangle.$$

For a given $\overline{u}$, we consider the following system of quadratic equations, written in vectorial form:

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

It should be clear that when this system has a nontrivial solution $\overline{j}$ (that is $\overline{j} \neq 0^d$) then $(\overline{a}, \overline{u}, \overline{j})$ is an appropriate triple, for every $\overline{a}$. In fact, the Chevalley-Warning theorem [3, 29] implies that the following equivalent system of vectorial equations has a nontrivial solution for every $\overline{u}$, whenever $n > 3d$.

$$\begin{cases} \sum_{i=1}^{n} u_i j_i^2 & = & 0^d \\ \sum_{i=1}^{n} u_i j_i & = & 0^d. \end{cases} \tag{3}$$

Moreover, if we take a substantially larger number of variables, we can find a solution in polynomial time.

Theorem 5. *If $n = (d+1)^2(d+2)/2$ then we can find a nontrivial solution for the system (3) in polynomial time.*

The proof of Theorem 5 will be given in the next section. To finish the proof of Theorem 4 we describe the efficient hiding procedure. On input $|g\rangle$, it computes, for some $\overline{a} \in G^n$, the superposition

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

which by Lemma 4 can be done efficiently, and then it measures the registers for the u_i. Then, by Theorem 5 it finds efficiently a nontrivial solution $\overline{j}$ for system (3). 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 $|\Psi_g^{\overline{a},\overline{u},\overline{j}}\rangle$. □

5 Solving the system of equations

This section is fully dedicated to the proof of Theorem 5. If $p = 2$ then the d quadratic and the d linear equations coincide, and the (linear) system can easily be solved in polynomial time. Therefore, from now on, we suppose that $p > 2$. Let us examine in detail the system (3), where we set $u_i = (u_{1,i}, u_{2,i}, \ldots, u_{d,i})$. We have the following system of d homogeneous quadratic and d homogeneous linear one equations with n variables:

$$\begin{cases} \forall \ell \in [|1,d|], & \sum_{i=1}^{n} u_{\ell,i} j_i^2 & = & 0 \\ \forall \ell \in [|1,d|], & \sum_{i=1}^{n} u_{\ell,i} j_i & = & 0 \end{cases} \tag{4}$$

We start by considering only the quadratic part of the (4), that is

$$\begin{cases} \forall \ell \in [|1,d|], & \sum_{i=1}^{n'} u_{\ell,i} j_i^2 & = & 0 \end{cases} \tag{5}$$

for some integer n'.

Claim 1. *If $n' = (d+1)(d+2)/2$ then we can find a nontrivial solution for (5) in polynomial time.*

Proof. For the ease of notation we are going to represent this system by the $d \times n'$ matrix

$$M = \begin{pmatrix} u_{1,1} & \ldots & u_{1,n'} \\ \vdots & & \vdots \\ u_{d,1} & \ldots & u_{d,n'} \end{pmatrix}.$$

We will present a recursive algorithm whose complexity will be polynomial in d and in $\log p$. When $d = 1$, the unique quadratic equation is of the form $u_{1,1}j_1^2 + u_{1,2}j_2^2 + u_{1,3}j_3^2 = 0$. According to a special case of the main result in the thesis of van de Woestijne (Theorem A3 of [30]), a nontrivial solution for this can be found in polynomial time in $\log p$.

Let us suppose now that we have d equations in $n' = (d+1)(d+2)/2$ variables. We can make elementary operations on M (adding two rows and multiplying a row with a nonzero constant) without changing the solutions of the system. Our purpose is to reduce it with such operations to $d-1$ equations in at least $d(d+1)/2$ variables. If the system is of rank less than d, then we can erase an equation and get an equivalent system with only $d-1$ equations in the same number of variables. Otherwise, we perform Gaussian elimination resulting in the matrix

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & u^{(1)}_{1,d+1} & \cdots & u^{(1)}_{1,n'} \\ 0 & 1 & 0 & \dots & 0 & u^{(1)}_{2,d+1} & \cdots & u^{(1)}_{2,n'} \\ \vdots & & \ddots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 1 & 0 & u^{(1)}_{d-1,d+1} & \cdots & u^{(1)}_{d-1,n'} \\ 0 & \dots & 0 & 0 & 1 & u^{(1)}_{d,d+1} & \cdots & u^{(1)}_{d,n'} \end{pmatrix}.$$

Since checking quadratic residuosity is simple, and for odd p, half of the elements of $\mathbb{Z}_p^*$ are squares, we can easily compute a quadratic non-residue λ in probabilistic polynomial time. Then every quadratic non-residue is the product of a square and λ. We will look at column $d+1$ of M_1. If the column is everywhere 0 then $j_{d+1} = 1$ and $j_i = 0$ for $i \neq d+1$ is a nontrivial solution of the whole system. Otherwise, without loss of generality, we can suppose that for some $(k_1, k_2) \neq (0, 0)$ the first k_1 elements of column $d+1$ are squares, the following k_2 elements are the product of λ and a square, and the last $d - k_1 - k_2$ elements are zero. Thus there exist $v_1, \dots, v_{k_1+k_2}$ different from 0, such that $u^{(1)}_{i,d+1} = v_i^2$ for $1 \leq i \leq k_1$, and $u^{(1)}_{i,d+1} = \lambda v_i^2$ for $k_1 + 1 \leq i \leq k_1 + k_2$. Once we have a quadratic non-residue, the square roots $v_1, \dots, v_{k_1+k_2}$ can be found in deterministic polynomial time in $\log p$ by the Shanks-Tonelli algorithm [27]. We set the variables $j_{k_1+k_2+1}, \dots, j_d$ to 0, and eliminate columns $k_1 + k_2 + 1, \dots, d$ from M_1. Then for $i = 1, \dots, k_1 + k_2$, we divide the row i by v_i^2. Introducing the new variables $j'_i = j_i v_i^{-1}$ for $1 \leq i \leq k_1 + k_2$, the matrix of the system in the $n' - d + k_1 + k_2$ variables $j'_1, \dots, j'_{k_1+k_2}, j_{d+1}, \dots j_{n'}$ is

$$M_2 = \begin{pmatrix} 1 & 0 & & \dots & & & 0 & 1 & u^{(2)}_{1,d+2} & \cdots & u^{(2)}_{1,n'} \\ 0 & \ddots & & & & & & \vdots & \vdots & & \vdots \\ & & 1 & \ddots & & & \vdots & 1 & u^{(2)}_{k_1,d+2} & \cdots & u^{(2)}_{k_1,n'} \\ \vdots & & \ddots & 1 & & & & \lambda & u^{(2)}_{k_1+1,d+2} & \cdots & u^{(2)}_{k_1+1,n'} \\ & & & & \ddots & & 0 & \vdots & \vdots & & \vdots \\ 0 & & \dots & & & 0 & 1 & \lambda & u^{(2)}_{k_1+k_2,d+2} & \cdots & u^{(2)}_{k_1+k_2,n'} \\ 0 & & & \dots & & & & 0 & u^{(2)}_{k_1+k_2+1,d+2} & \cdots & u^{(2)}_{k_1+k_2+1,n'} \\ \vdots & & & & & & \vdots & \vdots & \vdots & & \vdots \\ 0 & & & \dots & & & & 0 & u^{(2)}_{d,d+2} & \cdots & u^{(2)}_{d,n'} \end{pmatrix}.$$

In M_2 we subtract the first row from rows $2, \dots, k_1$ and row $k_1 + 1$ from rows $k_1 + 2, \dots, k_1 + k_2$. Then we set the variables $j'_2, \dots, j'_{k_1}$ to j'_1, and variables $j'_{k_1+2}, \dots, j'_{k_1+k_2}$ to j'_{k_1+1}. The corresponding changes in the matrix are eliminating columns $2, \dots k_1$ and $k_1 + 2, \dots k_1 + k_2$ and putting in columns 1 and $k_1 + 1$ everywhere 0 but respectively in row 1 and row $k_1 + 1$. Finally, by exchanging row 2 and row $k_1 + 1$, we get the matrix

$$M_3 = \begin{pmatrix} 1 & 0 & 1 & u^{(3)}_{1,d+2} & \cdots & u^{(3)}_{1,n'} \\ 0 & 1 & \lambda & u^{(3)}_{2,d+2} & \cdots & u^{(3)}_{2,n'} \\ 0 & 0 & 0 & u^{(3)}_{3,d+2} & \cdots & u^{(3)}_{3,n'} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & u^{(3)}_{d,d+2} & \cdots & u^{(3)}_{d,n'} \end{pmatrix}$$

in variables $j'_1, j'_{k_1+1}, j_{d+1}, \ldots, j_{n'}$.

To finish the reduction, we will distinguish two cases, depending on the congruency class of p modulo 4. When $p \equiv 1$, the element -1 is a square, and in polynomial time in $\log p$ we can find s such that $s^2 = -1$. We set $j'_1 = s j_{d+1}$, eliminate column 1 from matrix M_3, put 0 in row 1 column $d+1$, and exchange row 1 and row 2. When $p \equiv 3$ modulo 4, the element -1 is not a square, and therefore we can choose $\lambda = -1$. We set $j_{k_1+1} = j_{d+1}$, eliminate column 2 from matrix M_3, and put 0 in row 2 column $d+1$.

In both cases we end up with a matrix of the form

$$M_4 = \begin{pmatrix} 1 & \alpha & u^{(3)}_{1,d+2} & \cdots & u^{(3)}_{1,n'} \\ 0 & 0 & u^{(3)}_{2,d+2} & \cdots & u^{(3)}_{2,n'} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & u^{(3)}_{d,d+2} & \cdots & u^{(3)}_{d,n'} \end{pmatrix}$$

in the variables $j', j_{d+1}, \ldots, j_{n'}$ where $\alpha = \lambda$ and $j' = j'_{k_1+1}$ when $p \equiv 1$ modulo 4, and $\alpha = 1$ and $j' = j'_1$ otherwise. Without the first row it represents a system of $d-1$ equations in $n' - (d+1) = d(d+1)/2$ variables for which we can find a nontrivial solution by induction. Let $j_{d+2}, \ldots, j_{n'}$ such a solution, and set $b = \sum_{k=d+2}^{n'} u^{(3)}_{1,k} j_k$. To give values to the remaining two variables we have to solve the equation $j'^2 + \alpha j^2_{d+1} + b = 0$. As $\alpha \neq 0$, the expression $-\alpha j^2_{d+1} - b$ takes $\frac{p+1}{2}$ different values for $j_{d+1} \in \mathbb{Z}_p$. At least one of these values must be a square since there are most $\frac{p-1}{2}$ non-squares in $\mathbb{Z}_p$. Therefore the equation $j'^2 + \alpha j^2_{d+1} + b = 0$ is always solvable, and by Theorem A3 of [30] a solution can be found deterministically in polynomial time.

Gaussian elimination on M can be done in time $O(d^4)$. Finding a nontrivial solution for a quadratic homogeneous equation in 3 variables takes time $q_1(\log p)$, solving a quadratic equation in two variables takes time $q_2(\log p)$, and finding a square roots modulo p takes time $q_3(\log p)$ where q_1, q_2 and q_3 are polynomials. Therefore the complexity of solving system (3) is $O(d^5 + d^2 q_3(\log p) + d q_2(\log p) + q_1(\log p))$.

□

We now turn to the system (4). Let $n' = n/(d+1)$, and for $0 \leq k \leq d$, consider the the system of d quadratic equations in n' variables:

$$\Big\{ \forall \ell \in [|1, d|], \quad \sum_{i=kn'+1}^{(k+1)n'} u_{\ell,i} j_i^2 \quad = \quad 0.$$

By Claim 1, each of these systems has a nontrivial solution that we can find in polynomial time. For each k, let $(j_{kn'+1}, \ldots, j_{(k+1)n'})$ such a solution of the kth quadratic system. Then the set

$$\{(\lambda_0 j_1, \ldots, \lambda_0 j_{n'}, \lambda_1 j_{n'+1}, \ldots, \lambda_1 j_{2n'}, \ldots, \lambda_d j_{dn'+1}, \ldots, \lambda_d j_{(d+1)n'}) \ : \ (\lambda_0, \lambda_1, \ldots, \lambda_d) \in \mathbb{Z}_p^{d+1}\}$$

is a $d+1$ dimensional subspace of $\mathbb{Z}_p^n$ whose elements are solutions of the d quadratic equations in (4). Since in (4) there are d linear equations, we can find a nontrivial $(\lambda_0, \lambda_1, \ldots, \lambda_d) \in \mathbb{Z}_p^{d+1}$ such that $(\lambda_0 j_1, \ldots, \lambda_0 j_{n'}, \lambda_1 j_{n'+1}, \ldots, \lambda_1 j_{2n'}, \ldots, \lambda_d j_{dn'+1}, \ldots, \lambda_d j_{(d+1)n'})$ is a (nontrivial) solution of the linear part of (4), and therefore of the whole system. □

Observe that the only probabilistic part of the algorithm is the generation of a quadratic non-residue modulo p.

Acknowledgments.

The authors are indebted to Csaba Schneider and to the anonymous referees for helpful remarks and suggestions.

References

[1] 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.

[2] R. Beals and L. Babai. Las Vegas algorithms for matrix groups. In *Proc. 34th IEEE FOCS*, pages 427–436, 1993.

[3] C. Chevalley. Démonstration d'une hypothèse de M. Artin. *Abhand. Math. Sem. Univ. Hamburg*, 11:73–75, 1936.

[4] B. Eick, Orbit-stabilizer problems and computing normalizers for polycyclic groups, *J. Symbolic Comput.*, 34, pages 1–19, 2002.

[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] V. Gebhardt. Efficient collection in infinite polycyclic groups, J. Symbolic Comput., 34, pages 213–228, 2002.

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

[8] M. Hall Jr., Theory of groups, *AMS Chelsea Publishing*, 1999.

[9] 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.

[10] D. F. Holt, B. Eick and E. O'Brien, Handbook of computational group theory, *Chapman & Hall/CRC Press*, 2005.

[11] B. Hø"fling. Efficient multiplication algorithms for finite polycyclic groups, *Preprint*, 2004.

[12] 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.

[13] G. Ivanyos, L. Sanselme and M. Santha. An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups. *Proc. 24th STACS*, LNCS vol. 4393, pages 586–597, 2007.

[14] 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`.

[15] H. Krovi and M. Rötteler. An efficient algorithm for the hidden subgroup problem in Weyl-Heisenberg groups. *Proc. MMICS 2008*, LNCS vol. 5393, pages 70–88, 2008.

[16] C. R. Leedham-Green and L. H. Soicher. Collection from the left and other strategies. *J. Symbolic Comput.*, 9, pages 665–675, 1990.

[17] C. R. Leedham-Green and L. H. Soicher. Symbolic collection using Deep Thought. *LMS J. Comput. Math.*, 1, pages 9–24, 1998.

[18] E. M. Luks. Computing in solvable matrix groups. In *Proc. 33rd IEEE FOCS*, pages 111–120, 1992.

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

[20] N. Meggido and C. Papadimitriou. On total functions, existence theorems, and computational complexity. *Theor. Comp. Sci.*, 81:317–324, 1991.

[21] 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.

[22] C. Moore, A. Russell and P. Sniady. On the impossibility of a quantum sieve algorithm for graph isomorphism. In *Proc. 39th ACM STOC*, pages 536–545, 2007.

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

[24] D. J. S. Robinson. A course in the theory of groups. Second edition. *Springer,* 1996.

[25] 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`.

[26] O. Regev. Quantum Computation and Lattice Problems. *SIAM J. Comp.*, 33(3):738–760, 2004.

[27] D. Shanks. Five number-theoretic algorithms. In *Proc. 2nd Manitoba Conference on Numerical Mathematics*, pages 51–70, 1972.

[28] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. factoring. *SIAM J. Comp.*, 26(5):1484–1509, 1997.

[29] E. Warning. Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. *Abhand. Math. Sem. Univ. Hamburg*, 11:76–83, 1936.

[30] C. van de Woestijne. *Deterministic equation solving over finite fields.* PhD thesis, Universiteit Leiden, 2006.