An Efficient Quantum Algorithm for the Hidden Subgroup Problem in Nil-2 Groups*

Gábor Ivanyos[1], Luc Sanselme[2], and Miklos Santha[3]

[1] SZTAKI, Hungarian Academy of Sciences, H-1111 Budapest, Hungary
[2] LRI, UMR 8623, Université Paris-Sud, Orsay, France, F-91405
[3] CNRS–LRI, Université Paris–Sud, 91405 Orsay, France and Centre for Quantum Technologies, National University of Singapore

Abstract. In this paper we extend the algorithm for extraspecial groups in [12], and 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 presented here 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.

1 Introduction

Efficient solutions to some cases of the hidden subgroup problem (HSP), a paradigmatic group theoretical problem, constitute probably the most notable success 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 in 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 not even query efficient algorithms are known 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 [23] are special cases of this solution.

* 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 the ANR Blanc AlgoQP grant of the French Research Ministry.

E.S. Laber et al. (Eds.): LATIN 2008, LNCS 4957, pp. 759–771, 2008.

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 [21], Hallgren, Russell and Ta-Shma [8], Grigni, Schulman, Vazirani and Vazirani [6] and Moore, Rockmore, Russell and Schulman [17]. 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 [11] 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 [12] 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 isomorphims problem. Recently Moore, Russell and Sniady [18] have shown that no algorithm based one a particular approach can solve the graph isomorhism 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 [20].

In this work we extend the class of groups where the HSP is efficiently solvable by a quantum algorithm to nilpotent groups of nilpotency class at most 2 (shortly nil-2 groups). 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 group is a subgroup of 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.Let us given an oracle f which 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 [12] 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. The procedure uses certain automorphisms of the groups to define some appropriate group actions, and is analogous to what have been done in [12] 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 nil-2 p-groups of exponent p, 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