International Journal of Foundations of Computer Science
© World Scientific Publishing Company

Efficient quantum algorithms for some instances of the non-Abelian hidden subgroup problem[*]

Gábor Ivanyos[†]
SZTAKI, Hungarian Academy of Sciences, H-1111 Budapest, Hungary

and

Frédéric Magniez[†]
CNRS–LRI, UMR 8623, Université Paris–Sud, 91405 Orsay, France

and

Miklos Santha[†]
CNRS–LRI, UMR 8623, Université Paris–Sud, 91405 Orsay, France

Received (received date)
Revised (revised date)
Communicated by Editor's name

ABSTRACT

In this paper we show that certain special cases of the hidden subgroup problem can be solved in polynomial time by a quantum algorithm. These special cases involve finding hidden normal subgroups of solvable groups and permutation groups, finding hidden subgroups of groups with small commutator subgroup and of groups admitting an elementary Abelian normal 2-subgroup of small index or with cyclic factor group.

Keywords: Quantum computing, Hidden subgroup problem, Black-box groups.

1. Introduction

A growing trend in recent years in quantum computing is to cast quantum algorithms in a group theoretical setting. Group theory provides a unifying framework for several quantum algorithms, clarifies their key ingredients, and therefore contributes to a better understanding why they can, in some context, be more efficient than the best known classical ones.

[*] A preliminary version of this paper appeared in *Proceedings of the 13th ACM Symposium on Parallel Algorithms and Architectures*, pp. 263–270, 2001.

Research partially supported by the EU 5th framework programs QAIP IST-1999-11234, RESQ IST-2001-37559, and RAND-APX IST-1999-14036, by the ACI Cryptologie CR/02 02 0040 grant of the French Research Ministry, by CNRS/STIC 01N80/0502 grant, by OTKA T030059, T030132, and NWO-OTKA N34040 grants.

[†] Emails: `Gabor.Ivanyos@sztaki.hu`, `magniez@lri.fr` and `santha@lri.fr`

The most important unifying problem of group theory for the purpose of quantum algorithms turned out to be the *hidden subgroup problem* (HSP) which can be cast in the following broad terms. Let G be a finite group (given by generators), and let H be a subgroup of G. We are given (by an oracle) a function f mapping G into a finite set such that f is constant and distinct on different left cosets of H, and our task is to determine the unknown subgroup H.

While no classical algorithm is known to solve this problem in time faster than polynomial in the order of the group, the biggest success of quantum computing until now is that it can be solved by a quantum algorithm *efficiently*, which means in time polynomial in the logarithm of the order of G, whenever the group is Abelian. The main tool for this solution is the (approximate) quantum Fourier transform which can be efficiently implemented by a quantum algorithm [20]. Simon's algorithm for finding an xor-mask [30], Shor's seminal factorization and discrete logarithm finding algorithms [29], Boneh and Lipton's algorithm for finding hidden linear functions [7] are all special cases of this general solution, as well as the algorithm of Kitaev [20] for the Abelian stabilizer problem, which was the first problem set in a general group theoretical framework. That all these problems are special cases of the HSP, and that an efficient solution comes easily once an efficient Fourier transform is at our disposal, was realized and formalized by several people, including Brassard and Høyer [8], Mosca and Ekert [25] and Jozsa [17]. An excellent description of the general solution can be found for example in Mosca's thesis [24].

We believe that addressing the HSP in the non-Abelian case is the most important challenge at present in quantum computing. Beside its intrinsic mathematical interest, the importance of this problem is enhanced by the fact that it contains as special case the graph isomorphism problem. Unfortunately, the non-Abelian HSP seems to be much more difficult than the Abelian case, and although considerable efforts were spent on it in the last years, only limited success can be reported. Rötteler and Beth [28] have presented an efficient quantum algorithm for the wreath products $\mathbb{Z}_2^k \wr \mathbb{Z}_2$. In the case of the dihedral groups, Ettinger and Høyer [10] designed a quantum algorithm which makes only $O(\log |G|)$ queries. However, this doesn't make their algorithm efficient since the (classical) post-processing stage of the results of the queries is done in exponential time in $O(\log |G|)$. Actually, this result was extended by Ettinger, Høyer and Knill [11] in the sense that they have shown that in any group, with only $O(\log |G|)$ queries to the oracle, sufficiently statistical information can be obtained to solve the the HSP. However, it is not known how to implement efficiently these queries, and therefore even the "quantum part" of their algorithm is remaining exponential. Hallgren, Russel and Ta-Shma [16] proved that the generic efficient quantum procedure for the HSP in Abelian groups works also for non-Abelian groups to find any normal subgroup, under the condition that the Fourier transform on the group can efficiently be computed. Grigni, Schulman, Vazirani and Vazirani could show that the HSP is solvable efficiently in groups where the intersection of the normalizers of all subgroups is large [14]. In a subsequent work extending some of the results of this paper Friedl, Ivanyos, Magniez, Santha and Sen [13] presented efficient quantum algorithms for the HSP in a class of groups which includes solvable groups of bounded exponent and having a derived series of bounded length. Moore, Rockemore, Russell and Schulman [23] proved that the strong Fourier sampling paradigm efficiently determines the HSP in the semi-direct product $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ for p and q primes when q divides $p-1$ and $q = \frac{p-1}{(\log p)^c}$. A recent survey on the status of the non-Abelian HSP problem was written by Jozsa [18].

In a somewhat different line of research, recently several group theoretical problems have been considered in the context of black-box groups. The notion of *black-box groups* has been introduced by Babai and Szemerédi in [3]. In this model, the elements of a group G are encoded by words over a finite alphabet, and the group operations are performed by an oracle (the black box). The groups are assumed to be input by generators, and the encoding is not necessarily unique. There has been a considerable effort to develop classical algorithms for computations with them [5, 1, 19], for example to identify the composition factors (especially the non-commutative ones). Efficient black-box algorithms give rise automatically to efficient algorithms whenever the black-box operations can be replaced by efficient procedures. Permutation groups, matrix groups over finite fields and even finite matrix groups over algebraic number fields fit in this model. In particular, Watrous [31] has recently considered solvable black-box groups in the restricted model of unique encoding, and using some new quantum algorithmic ideas, he could construct efficient quantum algorithms for finding composition series, decomposing Abelian factors, computing the order and testing membership in these groups.

In this paper we will focus on the HSP, and we will show that it can be solved in polynomial time in several black-box groups. In particular, we will present efficient quantum algorithms for this problem for groups with small commutator subgroup and for groups having an elementary Abelian normal 2-subgroup of small index or with cyclic factor group. Our basic ingredient will be a series of deep algorithmic results of Beals and Babai from classical computational group theory. Indeed, in [5] they have shown that, up to certain computationally difficult subtasks – the so-called Abelian obstacles – such as factoring integers and constructive membership test in Abelian groups many problems related to the structure of black-box groups, such as finding composition series, can be solved efficiently for groups without large composition factors of Lie type, and in particular, for solvable groups. As quantum computers can factor integers and take discrete logarithms, and, more generally, perform the constructive membership test in Abelian groups efficiently, one expects that a large part of the Beals–Babai algorithms can be efficiently implemented by quantum algorithms. Indeed, the above results of Watrous partly fulfill this task, although his algorithms are not using the Beals–Babai algorithms. Here we will describe efficient quantum implementations of some of the Beals–Babai algorithms. It turns out, that beside paving the way for solving the HSP in the groups mentioned previously, these implementations give also almost "for free" efficient solutions for finding hidden *normal* subgroups in many cases, including solvable groups and permutation groups.

The rest of the paper is structured as follows. In Section 2 we review the necessary definitions about black-box groups in the quantum computing framework, and will summarize the most important results about Abelian and solvable groups. In Section 3 we state the result of Beals and Babai and **Corollary 1** which makes explicit two hypotheses (disposability of oracles for order computing and for constructive membership test in elementary Abelian subgroups) under which the algorithms have efficient quantum implementations. Section 4 deals with these quantum implementations in the following cases: unique encoding (**Theorem 5**), modulo a hidden normal subgroup (**Theorem 6**) and modulo a normal subgroup given by generators in case of unique encoding (**Theorem 8**). As a consequence, we can derive the efficient quantum solution for the normal HSP in solvable and permutation groups without any assumption on the computability of noncommutative Fourier transforms (**Theorem 7**). Section 5 contains the efficient quantum algorithm for the HSP for groups with small commutator subgroup (**Theorem 9**), and Section 6 for groups having an elementary Abelian normal 2-subgroup of small index or with cyclic factor group (**Theorem 10**).

As a conclusion, we consider that this work underlines the computational power of the Abelian quantum Fourier transform for dealing with group theoretical problems in non-Abelian groups. Indeed, our algorithms use extensively the standard quantum algorithm for the Abelian HSP but never the quantum non-Abelian Fourier transform.

2. Preliminaries

For basic group theory we refer the reader to [27]. In order to achieve sufficiently general results we shall work in the context of black-box groups. We will suppose that the elements of the group G are encoded by binary strings of length n for some fixed integer n, what we call the *encoding length.* The groups will be given by generators, and therefore the *input size* of a group is the product of the encoding length and the number of generators. Note that the encoding of group elements need not to be unique, a single group element may be represented by several strings. If the encoding is not unique, one also needs an oracle for identity tests. Typical examples of groups which fit in this model are factor groups G/N of matrix groups G, where N is a normal subgroup of G such that testing elements of G for membership in N can be accomplished efficiently. Also, every binary string of length n does not necessarily corresponds to a group element. If the black box is fed such a string, its behavior can be arbitrary on it.

Since we will deal with black-box groups we shall shortly describe them in the framework of quantum computing (see also [24] or [31]). For a general introduction to quantum computing the reader might consult [15] or [26]. We will work in the quantum Turing machine model. For a group G of encoding length n, the black-box will be given by two oracles U_G and V_G both operating on $2n$ qubits. For any group elements $g, h \in G$, the effect of the oracles is the following:

$$U_G|g\rangle|h\rangle = |g\rangle|gh\rangle, \quad \text{and} \quad V_G|g\rangle|h\rangle = |g\rangle|g^{-1}h\rangle.$$

The quantum algorithms we consider might make errors, but the probability of making an error should be bounded by some fixed constant $0 < \varepsilon < 1/2$.

Let us quote here two basic results about quantum group algorithms respectively in Abelian and in solvable black-box groups.

Theorem 1 (Cheung and Mosca [9]) *Assume that G is an Abelian black-box group with unique encoding. Then the decomposition of G into a direct sum of cyclic groups of prime power order can be computed in time polynomial in the input size by a quantum algorithm.*

Theorem 2 (Watrous [31]) *Assume that G is a solvable black-box group with unique encoding. Then computing the order of G and testing membership in G can be solved in time polynomial in the input size by a quantum algorithm. Moreover, it is possible to produce a quantum state that approximates the pure state $|G\rangle = |G|^{-1/2} \sum_{g \in G} |g\rangle$ with accuracy ε (in the trace norm metric) in time polynomial in the input size $+ \log(1/\varepsilon)$.*

When we address the HSP, we will suppose that a function $f : \{0,1\}^n \to \{0,1\}^m$ is given by an oracle, such that for some subgroup $H \leq G$ the function f is constant on the left cosets of H and takes different values on different cosets. We will say that f *hides* the subgroup H. The goal is to find generators for H in time polynomial in the size of G and m, that is we assume that m is also part of the input in unary. The following theorem resumes the status of this problem when the group is Abelian.

Theorem 3 (Mosca [24]) *Assume that G is an Abelian black-box group with unique encoding. Then the hidden subgroup problem can be solved in time polynomial in the input size by a quantum algorithm.*

3. Group algorithms

In [5] Beals and Babai described probabilistic Las Vegas algorithms for several important tasks related the structure of finite black-box groups. In order to state their result, we will need some definitions, in particular the definition of the parameter $\nu(G)$, where G is any group.

Let us recall that a *composition series* of a group G is a sequence of subgroups $G = G_1 \rhd G_2 \rhd \ldots \rhd G_t = 1$ such that each G_{i+1} is a proper normal subgroup in G_i, and the factor groups G_i/G_{i+1} are simple. The factors G_i/G_{i+1} are called the *composition factors* of G. It is known that the composition factors of G are – up to order, but counted with multiplicities – uniquely determined by G. Beals and Babai define the parameter $\nu(G)$ as the smallest natural number ν such that every non-Abelian composition factor of G possesses a faithful permutation representation of degree at most ν.

By definition, for a solvable group G the parameter $\nu(G)$ equals 1. Also, representation-theoretic results of [12] and [21] imply that $\nu(G)$ is polynomially bounded in the input size in many important special cases, such as permutation groups or even finite matrix groups over algebraic number fields.

The *constructive membership test in Abelian subgroups* is the following problem. Given pairwise commuting group elements $h_1, \ldots, h_r, g$ of a non necessarily commutative group, either express g as a product of powers of the h_i's or report that no such expression exists. Babai and Szemerédi have shown in [3] that under some group operations oracle this problem cannot be solved in polynomial time by classical algorithms. This test is usually required only for *elementary Abelian groups*, that is groups which are isomorphic to $\mathbb{Z}_p^n$ for some prime p and integer n.

A *presentation* of G is a sequence $g_1, \ldots, g_s$ of generator elements for G, together with a set of group expressions in variables $x_1, \ldots, x_s$, called the *relators*, such that $g_1, \ldots, g_s$ generate G and the kernel of the homomorphism from the free group $F(x_1, \ldots, x_s)$ onto G sending x_i to g_i is the smallest normal subgroup of $F(x_1, \ldots, x_s)$ containing the relators. We remark that the generators in the presentation may differ from the original generators of G.

A *nice representation* of a factor G_i/G_{i+1} means a homomorphism from G_i with kernel G_{i+1} to either a permutation group of degree polynomially bounded in the input size$+\nu(G)$ or to $\mathbb{Z}_p$ where p is a prime dividing $|G|$. Of course, if G is solvable one can insist that the representations of all the cyclic factors be of the second kind.

We can now quote part of the main results of [5].

Theorem 4 (Beals and Babai [5], Theorem 1.2) *Let G be a finite black-box group with not necessarily unique encoding. Assume that the followings are given:*

(a) a superset of the primes dividing the order of G,

(b) an oracle for taking discrete logarithms in finite fields of size at most $|G|$,

(c) an oracle for the constructive membership tests in elementary Abelian subgroups of G.

Then the following tasks can be solved by Las Vegas algorithms of running time polynomial in the input size $+ \nu(G)$:

(i) test membership in subgroups of G,

(ii) compute the order of G and a presentation for G,

(iii) find generators for the center of G,

(iv) construct a composition series $G = G_1 \rhd G_2 \rhd \ldots \rhd G_t = 1$ for G, together with nice representations of the composition factors G_i/G_{i+1},

(v) find Sylow subgroups of G.

In the following paragraphs, first we sketch the brief outline of the Beals-Babai algorithm and then, using standard results, from quantum computing we rewrite it in the quantum model. In addition, we remark that the algorithm for testing membership can be understood in a stronger, *constructive* sense, (see Section 5.3 in [4]), which is the proper generalization of the constructive membership test in the Abelian case. For this we need the notion of a *straight line program* on a set of generators. This is a sequence of expressions $e_1, \ldots, e_s$ where each e_i is either of the form $x_i := h$ where h is a member of the generating set or of the form $x_i = x_j x_k^{-1}$ where $0 < j, k < i$. It turns out that for elements g of G one can also require that a straight line program expressing g in terms of the generators be returned.

Before starting the description of the Beals-Babai algorithm, we argue that task (iv) is the crucial part of Theorem 4. Actually if we have a composition series with nice factor representations the solutions of all of the other tasks can be solved using standard techniques of computational group theory not requiring calls to the oracle (c). Also, assumption (a) can be eliminated as the list of large prime factors of $|G|$ can be read from the non-permutation factor representations. (The other prime factors are of magnitude polynomial in $\nu(G)$.)

We briefly outline below how the task of oracle (c) can be solved using a series $G = G_1 \rhd G_2 \rhd \ldots \rhd G_t = 1$ with nice factor representations. Actually we solve the more general task of testing membership constructively in arbitrary subgroups of G in time polynomial in input size $+\,\nu(G)$. The technique, called sifting is a standard tool of computational group theory. Its origins go back to basic permutation group algorithms.

Let g be an element of G and H be a subgroup of G given by generators $h_1, \ldots, h_r$. Let $G = G_1 \rhd G_2 \rhd \ldots \rhd G_t = 1$ be a composition series and let ϕ be a nice representation of G/G_2. Then the constructive membership test of g in H is reduced to the constructive membership of $\phi(g)$ in $\phi(H)$ and a constructive membership test of another element in $H \cap G_2$. Indeed, if $\phi(G)$ is not in $\phi(H)$ then g is not in H. Otherwise, substituting $h_1, \ldots, h_r$ in the straight-line program for $\phi(g)$ gives an element $g' \in H$ such that $\phi(g) = \phi(g')$. Here $gg'^{-1} \in G_2$ and g is in H if and only if $gg'^{-1} \in G_2 \cap H$. Finally, provided that we have straight line programs for generators for $G_2 \cap H$ and a straight line program for gg'^{-1} in terms of these elements then a straightforward combination gives a straight line program for g in terms of the generators for H.

If ϕ is a representation of G/G_2 into the additive group of the integers modulo the prime p then the membership test in $\phi(H)$ can be accomplished by solving a linear congruence modulo p. If $\phi : G \to S_\nu$ is a permutation representation then sifting along a stabilizer chain can be applied. First we enumerate the H-orbit of 1 and for every element j of the orbit we construct an element x_j of H such that $\phi(x_j)1 = j$. Next, a system of generators for the stabilizer H_1 of 1 in H is given by $x_{j_i}^{-1} h_i$ $(i = 1, \ldots, r)$ where $j_i = \phi(h_i)1$. Also set $g_1 = x_{j_g}^{-1} g$ where $j_g = \phi(g)1$. Now $g \in H$ if and only if $g_1 \in H_1$; and both H_1 and g_1 acts on the smaller set $\{2, \ldots, \nu\}$. Repeating this at most ν times and maintaining straight line program representations carefully we can solve the constructive membership test in $\phi(H)$ in time polynomial in ν (and the input size). Note that generators for $H \cap G_2$ can be obtained by a similar procedure.

Now we proceed with the description of the main part of Beals-Babai algorithm which solves task (iv). Of course, we have to omit many important details.

The algorithm builds a composition series together with the nice factor representations downward from the top. Assume that we have a series $G = G_1 \rhd G_2 \rhd \ldots \rhd G_d =: K$, together with nice factor representations, such that the factors G_i/G_{i+1} are simple. For keeping track of intermediate progress the method also maintains an auxiliary subgroup Z of the center of K which is set to $\{1\}$ in every step when the descending chain is extended and increased in certain other steps.

For testing membership in Z a basis of Z consisting of elements of prime power orders is computed. This can be relatively easily accomplished using the oracle for the constructive elementary Abelian membership test and a list of primes possibly occurring in the orders of the elements. Note that such a basis immediately provides us with a composition series of Z together with nice factor representations.

The basic tool in non-Abelian groups is trying to find permutation representations of K of moderate size using the conjugation action of K either on certain elements or on certain subgroups, and, using the extensive permutation group algorithm library, extend the chain fro G to K to a chain reaching the kernel of this representation. Recall that for $x, u \in K$ the conjugate of u by x is $u^x := x^{-1}ux$. The K-conjugates of u are the elements of the form u^x for some $x \in K$. The group K acts as a transitive permutation group on the set of the K-conjugates of u where the action of an element $x \in K$ is given by $v \mapsto v^x$. Similarly, if U is a subgroup of K then the x-conjugate of U is the subgroup $U^x = \{u^x | u \in U\}$. Again, K permutes transitively the K-conjugates of an arbitrary subgroup.

The algorithm proceeds as follows. First it finds a subnormal subgroup U of K (a subgroup reachable from K by a chain of subgroups where each element is normal in its predecessor) containing Z such that U/Z is a nontrivial simple group using a so-called one-way random walk technique of Beals and Seress ([6]). Note that the probability of that this procedure successfully gets down depends on the assumption on the composition factors of G.

If U/Z is non-Abelian and not normal in K then the conjugation action of K on the conjugates of U gives a nontrivial permutation representation of K of moderate size and by standard permutation group algorithms (essentially the sifting technique outlined above) the chain can be extended down to the kernel of this representation.

If U/Z is non-Abelian but normal in K then, by theorems depending on the classification of simple groups, with sufficiently high probability, for a random element u of U there is a prime p dividing the order of u such that the number of the K-conjugates of u^p is bounded by a polynomial in $\nu(U) \leq \nu(G)$. The prime can be selected from the set (a). (And, of course it must be tested that the number of conjugates of u^p does not exceed the limit.) This gives a permutation representation of K of degree polynomial in $\nu(G)$ and again, the chain can be extended down to the kernel of this representation.

If U/Z is Abelian then it is a cyclic group of prime order p and group theoretic facts imply that the K-conjugates of U generate a group P such that P/Z is a p-group. The prime p can be made explicit using the set of possible primes membership tests in Z. By descending along the lower central series of P ($P_0 = P$, $P_{i+1} = [P, P_i]$), i.e, iteratively taking commutators with generators from P one can find an element of $v \in P \setminus Z$ such that vZ is in the center of P/Z. Taking an appropriate power one can further achieve that $v^p \in Z$. Then the K-conjugates of v together with Z generate a subgroup V of such that V/Z is a vector space over the field $\mathbb{Z}_p$ and this gives a linear representation of K over $\mathbb{Z}_p$ with kernel containing V. If this representation is trivial, i.e., $v^x = x^{-1}vx \in vZ$, or, equivalently, $[x, v] = x^{-1}v^{-1}xv \in Z$ for every $x \in K$, one can see that the mapping $x \mapsto [x, v]$

is a homomorphism from K to the Abelian group Z. If this homomorphism is also trivial then v is in the center of K and Z can be increased by adding v to it. Otherwise composing this map with the top factor representation of Z one obtains a homomorphism of K into the additive group of a prime field. If this is a trivial map one can go on with the next-to-top factor representation and so on. Eventually one finds a nontrivial homomorphism from K to the additive group of a prime field and hence extend the chain to the kernel.

If the conjugation action of K on V/Z is nontrivial, then, provided that matrices for the generators of K can be computed efficiently, by a recursive call of the whole procedure (considering a matrix group as a black box group) one can extend the chain down to the kernel. An oracle for testing membership in elementary Abelian matrix groups can be implemented by using an oracle for computing discrete logarithms in finite extensions of the ground field. This explains the role of the oracle for task (b) in Theorem 4.

Calculating a basis of V/Z and matrices for actions of the generators for K, using the constructive elementary Abelian membership oracle, is immediate in the case when Z is trivial. Even in the general case when Z is possibly nontrivial one can see that for every fixed element $u \in V$ the map $x \mapsto [u, x]$ is a homomorphism from V to Z with kernel V_0 containing Z. If u is not in the center of V (at least one of the elements of a generator set for V is such provided that V is non-Abelian) then V_0 is a proper subgroup of V. Furthermore, the inverse image of the chain for Z at this map gives a chain from V down to V_0 with factors of order p and factor representations in $\mathbb{Z}_p$. If V_0 is non-Abelian then one can repeat this procedure. Finally, for an Abelian subgroup $V_0 \geq Z$ it is not difficult to produce a chain from V_0 down to Z using Abelian techniques. Selecting appropriate elements of V from the subsequent members of the chain of subgroups between V and Z gives a basis of V/Z over $\mathbb{Z}_p$ and the nice factor representations give an efficient procedure for expressing any element of V/Z in terms of this basis and hence a way to construct the desired matrix representation of K.

After the description of the Beals-Babai algorithm, we now put the result in the context of quantum computing. It turns out that for some of the tasks in the hypotheses of Theorem 4 there are efficient quantum algorithms. By Shor's results [29], the oracle for computing discrete logarithms can be implemented by a polynomial time quantum algorithm. Also, a superset of the primes dividing $|G|$ can be obtained in polynomial time by quantum algorithms in the most natural cases. For example, if G is a matrix group over a finite field, say $G \leq \mathrm{GL}(n, q)$ then such a superset can be obtained by factoring the number $(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$, the order of the group $GL(n, q)$. The same method works even for factors of matrix groups over finite fields. If G is (a factor of) a finite matrix group of characteristic zero, then the situation is even better because in that case the prime divisors of G are of polynomial size. But in any case, one can note that the superset of the primes dividing the order of G is only used in Theorem 4 to compute (and factorize) the orders of elements of G as well as those of matrices over finite fields of size at most $|G|$. This latter task can also be achieved by a quantum algorithm in polynomial time. Therefore, one can immediately derive from Theorem 4 the following result.

Corollary 1 *Let G be a finite black-box group with not necessarily unique encoding. Assume that the following are given:*

(a) an oracle for computing the orders of elements of G,

(b) an oracle for the constructive membership tests in elementary Abelian subgroups of G.

Then the following tasks can be solved by quantum *algorithms of running time polynomial in the input size $+ \nu(G)$:*

(i) constructive membership test in subgroups of G,

(ii)–(v) as in Theorem 4.

4. Quantum implementations

In this section we will discuss several cases when the remaining tasks in the hypotheses of Corollary 1 can also be efficiently implemented by quantum algorithms.

4.1. Unique encoding

If we have a unique encoding for the elements of the black-box group G then we can use Shor's order finding method. As we will show, in that case there is also an efficient quantum algorithm for the constructive membership test in elementary (and non-elementary) Abelian subgroups. Therefore we will get the following result.

Theorem 5 *Assume that G is a black-box group with unique encoding. Then, each of the tasks listed in Corollary 1 can be solved in time polynomial in the input size$+ \nu(G)$ by a quantum algorithm..*

Proof. Let us prove that task *(b)* in Corollary 1 can be solved efficiently by a quantum algorithm. In fact, we can reduce the test to an instance of the Abelian hidden subgroup problem as follows. First, we compute the orders of the underlying elements (see [24] for example). Let the orders of $h_1, \ldots, h_r$ and g be $s_1, \ldots, s_r$ and s, respectively. Then for a tuple $(\alpha_1, \ldots, \alpha_r, \alpha)$ from $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r} \times \mathbb{Z}_s$, set $\phi(\alpha_1, \ldots, \alpha_r, \alpha) = h_1^{\alpha_1} \cdots h_r^{\alpha_r} g^{-\alpha}$. Clearly ϕ is a homomorphism from $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r} \times \mathbb{Z}_s$ into G, therefore this is an instance of the Abelian hidden subgroup problem, and its kernel can be found in polynomial time by a quantum algorithm. The kernel contains an element the last coordinate of which is relatively prime to s if and only if g is representable as a product of powers of h_i's. Also, from such an element an expression for g in the desired form can be constructed efficiently. □

This result generalizes the order finding algorithm of Watrous (Theorem 2 in [31]) for solvable groups. Also note that, even if G is solvable, the way how quantum algorithms are used here is slightly different from that of Watrous.

4.2. Hidden normal subgroup

Assume now that G is a black-box group with an encoding which is not necessarily unique, and N is a normal subgroup of G given as a hidden subgroup via the function f. We use the encoding of G for that of G/N. The function f gives us a secondary encoding for the elements of G/N. Although we do not have a machinery to multiply elements in the secondary encoding, Shor's order-finding algorithm and even the treatment of the constructive membership test outlined above are still applicable.

Theorem 6 *Assume that G is a black-box group with not necessarily unique encoding. Suppose that N is a normal subgroup given as a hidden subgroup of G. Then all the tasks listed in Corollary 1 for G/N can be solved by quantum algorithms in time polynomial in the input size $+ \nu(G/N)$.*

Proof. The proof is similar to the one of Theorem 5, where $\phi(\alpha_1, \ldots, \alpha_r, \alpha) = f(h_1^{\alpha_1} \cdots h_r^{\alpha_r} g^{-\alpha})$ is taken. □

Let us now turn back to the original hidden subgroup problem. We are able to solve it completely when the hidden subgroup is normal. Hallgren Russell and Ta-Shma [16] have already given a solution for that case under the condition that one can efficiently construct the quantum Fourier transform on G. Note that such an efficient construction is not known in general. The algorithm presented here does not require such a hypothesis, on the other hand its complexity depends also on the additional parameter $\nu(G/N)$.

Theorem 7 *Assume that G is a black-box group with not necessarily unique encoding. Suppose that N is a normal subgroup given as a hidden subgroup of G. Then generators for N can be found by a quantum algorithm in time polynomial in the input size$+\nu(G/N)$. In particular, we can find hidden normal subgroups of solvable black-box groups and permutation groups in polynomial time.*

Proof. We use the presentation of G/N obtained by the algorithm of Theorem 6 to find generators for N. Let T be the generating set from the presentation. If T generates G then it is easy to find generators for N. Let R_0 denote the set of elements obtained by substituting the generators in T into the relators, and let N_0 stand for the normal closure (the smallest normal subgroup containing) of R_0. Then $N = N_0$ since $N_0 \leq N$ and $G/N_0 = G/N$ by definition of T and R_0.

Still some care has to be taken since it is possible that T generates G only modulo N, that is it might generate a proper subgroup of G. Therefore some additional elements should be added to R_0. Let S be the generating set for G. Using the constructive membership test for G/N, we express the original generators from S modulo N with straight line programs in terms of the elements of T. For each element $x \in S$ we form the quotient $y^{-1}x$ where y is the element obtained by substituting the generators from T into the straight line program for x modulo N. Let S_0 be the set of all the quotients formed this way. Note that T and S_0 generate together G. Then one can verify that the normal closure of $R_0 \cup S_0$ in G is N.

Thus, from R_0 and S_0 we can find generators for N in time polynomial in the input size $+ \nu(G/N)$ using the normal closure algorithm of [2]. We obtained the desired result. □

4.3. Unique encoding and solvable normal subgroup

We conclude this section with some results obtained as combination of the ideas presented above with those of Watrous described in [31]. Assume that the encoding of the elements of G is unique and a normal solvable subgroup N of G is given by generators. We use the encoding of G for that of G/N. The identity test in G/N can be implemented by an efficient quantum algorithm for testing membership in N due to Watrous (Theorem 2). We are also able to produce (approximately) the uniform superposition $|N\rangle = \frac{1}{\sqrt{|N|}} \sum_{x \in N} |x\rangle$ efficiently. For solvable subgroups N, we can again apply the result of Watrous (Theorem 2) to produce $|N\rangle$ in polynomial time. We will now show that having sufficiently many copies of $|N\rangle$ at hand, we can use ideas of Watrous for computing orders of elements of G/N and even for performing the constructive membership test in Abelian subgroups of G/N. Thus, we will have an efficient quantum implementation of the Beals-Babai algorithms for G/N. We will first state a lemma which says that we can efficiently solve the HSP in an Abelian group if we have an appropriate quantum oracle.

Lemma 1 *Let A be an Abelian group, and let X be a finite set. Let $H \leq A$, and let $f : A \to \mathbb{C}^X$ (given by an oracle) such that:*

1. *For every $g \in A$, $|f(g)\rangle$ is a unit vector,*
2. *f is constant on the left cosets of H, and maps elements from different cosets into orthogonal states.*

Then there exists a polynomial time quantum algorithm for finding the hidden subgroup H.

Proof. First we extend naturally f to G/H: on a coset of H, it takes the value $f(h)$ for an arbitrary member h of the coset. The algorithm is the standard quantum algorithm for the Abelian hidden subgroup problem. We repeat several times the following steps to find a set of generators for H.

- Prepare the initial superposition: $|1_G\rangle|0^m\rangle$.
- Apply the Abelian quantum Fourier transform in A on the first register: $\sum_{g\in A} |g\rangle|0^m\rangle$.
- Call f: $\sum_{g\in A} |g\rangle|f(g)\rangle$.
- Apply again the Fourier transform in A: $\sum_{g\in A/H, h\in H^\perp} \chi_h(g)|h\rangle|f(g)\rangle$.
- Observe the first register.

By hypothesis, the states $|f(g)\rangle$ are orthogonal for distinct $g \in A/H$, therefore an observation of the first register will give a uniform probability distribution on $H^\perp$. After sufficient number of iterations, this will give a set of generators for $H^\perp$, which leads then to a set of generators for H.

Note that in the above steps it is sufficient to compute only the approximate quantum Fourier transform on A which can be done in polynomial time. □

Theorem 8 *Assume that G is a black-box group with a unique encoding of group elements. Suppose that N is a normal subgroup given by generators. Assume further that N is either solvable or of polynomial size. Then all the tasks listed in Corollary 1 for G/N can be solved by a quantum algorithm in running time polynomial in the input size $+\,\nu(G/N)$.*

Proof. For applying Corollary 1, one has to verify that we can perform tasks *(a)–(b)* of the corollary. If N is of polynomial size, it is trivial. Therefore we suppose that N is solvable. We will closely follow the approach indicated by Watrous in [31] for dealing with factor groups.

First, let $g \in G$. To compute the order of g in G/N, we compute the period of the quantum function $f(k) = |g^k N\rangle$, where $k \in \{1, \ldots, m\}$ for some multiple m of the order. This function can be computed efficiently since one can prepare the superposition $|N\rangle$ by Theorem 2, and for example we can take m as the order of g in G. Therefore by Lemma 1 one can find this period.

Second, let $g \in G$ and let $h_1, \ldots, h_r \in G$ be pairwise commuting elements modulo N. generating some Abelian subgroup $H \leq G/N$. We compute the orders of the underlying elements on G/N using the previous method. Let the orders of $h_1, \ldots, h_r$ and g be $s_1, \ldots, s_r$ and s, respectively. Then for a tuple $(\alpha_1, \ldots, \alpha_r, \alpha)$ from $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r} \times \mathbb{Z}_s$, set $\phi(\alpha_1, \ldots, \alpha_r, \alpha) = |h_1^{\alpha_1} \cdots h_r^{\alpha_r} g^{-\alpha} N\rangle$. Then ϕ is a homomorphism from $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r} \times \mathbb{Z}_s$ into $\mathbb{C}^{G/N}$. From Lemma 1, the kernel of ϕ can be computed in polynomial time by a quantum algorithm. Moreover it contains an element the last coordinate of which is relatively prime to s if and only if g is representable as a product of powers of h_is. Also, from such an element an expression for g in the desired form can be constructed efficiently using elementary number theory. □

5. Groups with small commutator subgroups

Assume that G is a black-box group with unique encoding of elements, and suppose that a subgroup H is hidden by a function f. Our next result states that one can solve the HSP in time polynomial in the input size $+\,|G'|$, where G' is the commutator subgroup of G. Let us recall the *commutator subgroup* is the smallest normal subgroup of G containing the commutators $xyx^{-1}y^{-1}$, for every $x, y \in G$.

Theorem 9 *Let G be a black-box group with unique encoding of elements. The hidden subgroup problem in G can be solved by a quantum algorithm in time polynomial in the input size $+\,|G'|$.*

Proof. Let H be a hidden subgroup of G defined by the function f. We start with the following observation. If N is a normal subgroup of G and $H_1 \leq H$ is such that $H_1 \cap N = H \cap N$ and $H_1 N = HN$, then by the isomorphism theorem, $H_1/(H \cap N) \cong H_1 N/N \cong H/(H \cap N)$ which implies $H_1 = H$. We will generate such a subgroup $H_1 \leq H$ for $N = G'$.

As the commutator subgroup G' of G consists of products conjugates of commutators of the generators of G we can enumerate G', and therefore also $G' \cap H$, in time polynomial in the input size $+\,|G'|$. We consider the function $F : x \mapsto \{f(xG')\} = \{f(xg) | g \in G'\}$ which can be computed by querying $|G'|$ times the function f.

The function F hides the subgroup HG'. Note that HG' is normal since G/G' is Abelian. Thus by Theorem 7, we can find generators for HG' by a quantum algorithm in time polynomial in the size of the input + $|G'|$ since $\nu(G/HG') = 1$, because G/HG' is Abelian.

For each generator x of HG', we enumerate all the elements of coset xG' and select an element of $xG' \cap H$. The cost of this step is again polynomial in the input size + $|G'|$. We take for H_1 the subgroup of G generated by the selected elements and $H \cap G'$. We get $H_1 \cap G' = H \cap G'$, and by the definition of the selected elements $H_1 G' = HG'$. □

A group G is an *extra-special p-group* if its commutator subgroup G' coincides with its center, $|G'| = p$, and moreover G/G' is an elementary Abelian p-group. Therefore we get the following corollary from the previous theorem.

Corollary 2 *The hidden subgroup problem in extra-special p-groups can be solved by a quantum algorithm in time polynomial in input size $+\, p$.*

6. Groups with a large elementary Abelian normal 2-subgroup

The purpose of this section is to introduce a few ideas which, in some cases, can reduce the HSP in G to the HSP in a normal subgroup N of G. The HSP in N is firstly used to compute $H \cap N$. To simplify the following discussion let us suppose that the hidden subgroup H has trivial intersection with N. If we have at our disposal a representative element of HN/N, then finding the unique element of H in this coset is reducible to the Hidden Translation Problem (HTP) in N. Moreover deciding if a coset of N is an element of HN/N can also be reduced to it. The HTP was implicitly defined by Ettinger and Høyer [10]. We are given two injective functions f_0 and f_1 from a finite group to some finite set such that, for some group element u, the equality $f_1(xu) = f_0(x)$ holds for every x. The task is to find the translation u. In elementary Abelian 2-groups, it is immediate that the HTP can be efficiently solved since it is an instance of the Abelian HSP. Also, when G/N is either small or cyclic, we can construct efficiently a small set $V \subseteq G$ which, when its elements are considered as coset representatives, every subgroup of G/N contains a generator set consisting of some elements of V. For our purpose, we will only use this property for the subgroup HN/N.

In the rest of this section, we assume that N is an elementary Abelian normal 2-subgroup of a group G, which is given by generators as part of the input, and that G/N is either small or cyclic. Typical examples of groups of the latter type are matrix groups over a field of characteristic 2 of degree $k+1$ generated by a single matrix of type *(a)*, where the $k \times k$ sub-matrix in the upper left corner is invertible, together with several matrices of type *(b)*:

$$\textit{(a)} \begin{pmatrix} * & * & * & * & 0 \\ * & * & * & * & 0 \\ * & * & * & * & 0 \\ * & * & * & * & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \textit{(b)} \begin{pmatrix} 1 & 0 & 0 & 0 & * \\ 0 & 1 & 0 & 0 & * \\ 0 & 0 & 1 & 0 & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that the class of groups of this kind include the wreath products $\mathbb{Z}_2^k \wr \mathbb{Z}_2$ in which the hidden subgroup problem has been shown to be solvable in polynomial time by Rötteler and Beth in [28].

The reduction idea was further extended and generalized in [13] where it is shown that the problem Orbit Coset (see definition in [13]) generalizing both HTP and HSP, has the powerful self-reducibility property: Orbit Coset in a finite group G, is reducible to Orbit Coset in G/N and subgroups of N, for any solvable normal subgroup N of G.

Theorem 10 *Let G be a black-box group with unique encoding of elements and N be a normal elementary Abelian 2-subgroup of G given by generators. Then the hidden subgroup problem in G can be solved by a quantum algorithm in time polynomial in the input size $+ |G/N|$. If G/N is cyclic then the hidden subgroup problem can be solved in polynomial time.*

Proof. Let H be a subgroup of G hidden by the function f. The main line of the proof is like in Theorem 9: we will generate $H_1 \leq H$ which satisfies $H_1 \cap N = H \cap N$ and $H_1N/N = HN/N$ (or equivalently $H_1N = HN$). Again we start the generation of H_1 with $H \cap N$ which can be computed in polynomial time in the input size by Theorem 3 since N is Abelian. The additional generators of H_1 will be obtained from a set $V \subseteq G$ which, for every subgroup $\overline{M} \leq G/N$ (in particular, for $\overline{M} = HN/N$), contains some generator set for $\overline{M}$. For each $z \in V$, we will verify if $zN \in HN$ (equivalently $zH \cap N \neq \emptyset$ or also $zN \cap H \neq \emptyset$), and in the positive case we will find some $u \in N$ such that $u^{-1}z \in H$. Both of these tasks will be reduced to the Abelian hidden subgroup problem, and the elements of the form $u^{-1}z$ will be the additional generators of H_1.

If G/N is cyclic, we use Theorem 8 to find generators for the Sylow subgroups of G/N (note that $\nu(G/N) = 1$). Each Sylow will be cyclic (and unique), therefore a random element of the Sylow p-subgroup will be a generator with probability $1 - 1/p \geq 1/2$. Note that one can check if the chosen element is really a generator by using the order finding procedure of Theorem 8. Then, for each p we choose a generator x_pN for the Sylow p-subgroup after iterating the previous random choice. The p-subgroups of G/N are $\langle x_pN\rangle, \ldots, \langle x_p^{p^{h_p}}N\rangle = N/N$, where p^{h_p} is the order of the Sylow p-subgroup of G/N. Let V stand for the union of the sets $\{1, x_p, \ldots, x_p^{p^{h_p}}\}$ over all primes p dividing $|G/N|$. Note that $|V| = O(\log |G/N|)$, and the cost of constructing V is polynomial in the input size. V contains a generating set for an arbitrary subgroup $\overline{M}$ of G/N because for each p, it contains a generator for the Sylow p-subgroup of $\overline{M}$ (namely $x_p^{p^{l_p}}$ where l_p is the smallest positive integer l such that $x_p^{p^l}N \in \overline{M}$).

In the general case, let V be a complete set of coset representatives of G/N. V can be constructed by the following standard method. We start with the set $V = \{1\}$. In each round we adjoin to V a representative vg of a new coset, for each $v \in V$ and each generator g of G, if $vg \notin wN$, for all $w \in V$. This membership test can be achieved using a quantum algorithm for testing membership of $w^{-1}vg$ in the commutative group N. The procedure stops if no new element can be added.

Then, for each $z \in V \setminus \{1\}$, we consider the function defined on $\mathbb{Z}_2 \times N$ as follows. For every $x \in N$, let $F(0,x) = f(x)$ and let $F(1,x) = f(xz)$. Obviously, for $i \in \{0,1\}$ and $x, y \in N$, $F(i,x) = F(i,y)$ if and only if $y^{-1}x \in H \cap N$, while $F(0,x) = F(1,y)$ if and only if $y^{-1}x \in zH \cap N$.

We claim that $zH \cap N$ is either empty or a coset of $H \cap N$ in N. Indeed, if $zH \cap N$ contains zh for some $h \in H$, then $zh(H \cap N) \subseteq zH \cap N$, and conversely for all $h' \in H$ such that $zh' \in N$, we have $(zh)^{-1}zh' = h^{-1}h' \in H \cap N$. It follows that in the group $\mathbb{Z}_2 \times N$, F hides either $\{0\} \times (H \cap N)$ or $\{0\} \times (H \cap N) \bigcup \{1\} \times u(H \cap N)$ for some $u \in zH \cap N$ depending on whether $zH \cap N$ is empty or not. Note that this set is indeed a subgroup because N is an elementary Abelian 2-group. We remark that u is determined only modulo $H \cap N$.

As $\mathbb{Z}_2 \times N$ is Abelian, we can find generators for this hidden subgroup in quantum polynomial time. From any generator of type $(1, u)$ we obtain an element $u^{-1}z \in zN \cap H$. Repeating this, we collect elements in $zN \cap H$ for each of $z \in V \setminus \{1\}$ such that $zN \cap H \neq \emptyset$. Let H_1 be the subgroup of G generated by the collected elements and by $H \cap N$. Then by construction H_1 is a subgroup of H which satisfies the claimed properties. □

References

1. L. Babai and R. Beals, A polynomial-time theory of black-box groups I., *Groups St. Andrews 1997 in Bath, I*, London Math. Soc. Lecture Notes Ser., vol. 260, Cambridge Univ. Press, 1999, 30–64.
2. L. Babai, G. Cooperman, L. Finkelstein, E. M. Luks and Á. Seress, Fast Monte Carlo algorithms for permutation groups, *J. Computer and System Sciences*, vol. 50, 1995, 263–307.
3. L. Babai and E. Szemerédi, On the complexity of matrix group problems I., *Proc. 25th IEEE Foundations of Computer Science*, 1984, 229–240.
4. R. Beals, Towards polynomial time algorithms for matrix groups, *Groups and Computation Proc. 1991 DIMACS Workshop,* L. Finkelstein, W. M. Kantor (eds.), DIMACS Ser. in Discr. Math. and Theor. Comp. Sci., vol. 11, AMS, 1993, 31–54.
5. R. Beals and L. Babai, Las Vegas algorithms for matrix groups, *Proc. 34th IEEE Foundations of Computer Science*, 1993, 427–436.
6. R. Beals and Á. Seress, Structure forest and composition factors for small base groups in nearly linear time, *Proc. 24th ACM Symposium on Theory of Computing*, 1992, 116–125.
7. D. Boneh and R. Lipton, Quantum cryptanalysis of hidden linear functions, *Proc. Crypto'95*, LNCS vol. 963, 1995, 427–437.
8. G. Brassard and P. Høyer, An exact quantum polynomial-time algorithm for Simon's problem, *Proc. 5th Israeli Symposium on Theory of Computing Systems*, 1997, 12–23.
9. K. Cheung and M. Mosca, Decomposing finite abelian groups, *J. Quantum Inf. Comp.*, 1(3), 2001, 26–32.
10. M. Ettinger and P. Høyer, On quantum algorithms for noncommutative hidden subgroups, *Proc. 16th Symposium on Theoretical Aspects of Computer Science*, LNCS vol. 1563, 1999, 478–487.
11. M. Ettinger, P. Høyer, and E. Knill, Hidden subgroup states are almost orthogonal, preprint available at `http://xxx.lanl.gov/abs/quant-ph/9901034`.

12. W. Feit and J. Tits, Projective representations of minimum degree of group extensions, *Canadian J. Math.*, vol. 30, 1978, 1092–1102.
13. K. Friedl, G. Ivanyos, F. Magniez, M. Santha and P. Sen, Hidden translation and orbit coset in quantum computing, to appear in *Proc. 35th ACM Symposium on Theory of Computing*, 2003. Preprint available at `http://xxx.lanl.gov/abs/quant-ph/0211091`.
14. M. Grigni, L. Schulman, M. Vazirani and U. Vazirani, Quantum mechanical algorithms for the nonabelian hidden subgroup problem, *Proc. 33rd ACM Symposium on Theory of Computing*, 2001, 68–74.
15. J. Gruska, *Quantum Computing*, McGraw Hill, 1999.
16. S. Hallgren, A. Russell and A. Ta-Shma, Normal subgroup reconstruction and quantum computation using group representations, *Proc. 32nd ACM Symposium on Theory of Computing*, 2000, 627–635.
17. R. Jozsa, Quantum algorithms and the Fourier transform, preprint available at `http://xxx.lanl.gov/abs/quant-ph/9707033`.
18. R. Jozsa, Quantum factoring, discrete logarithms and the hidden subgroup problem, preprint available at `http://xxx.lanl.gov/abs/quant-ph/0012084`.
19. W. M. Kantor and Á. Seress, Black box classical groups, Manuscript.
20. A. Kitaev, Quantum measurements and the Abelian Stabilizer Problem, preprint available at `http://xxx.lanl.gov/abs/quant-ph/9511026`.
21. V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* vol. 32, 1974, 418–443.
22. E. M. Luks, Computing in solvable matrix groups, *Proc. 33th IEEE Foundations of Computer Science, 1992, 111–120.*
23. C. Moore, D. Rockemore, A. Russell and L. Schulman, The hidden subgroup problem in affine groups: basis selection in Fourier sampling, preprint available at `http://xxx.lanl.gov/abs/quant-ph/0211124`.
24. M. Mosca, *Quantum Computer Algorithms*, PhD thesis, University of Oxford, 1999.
25. M. Mosca and A. Ekert, The hidden subgroup problem and eigenvalue estimation on a quantum computer, *Proc. 1st NASA International Conference on Quantum Computing and Quantum Communication*, LNCS vol. 1509, 1999.
26. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
27. J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag, Series: Graduate Texts in Mathematics, vol. 148, 4th ed. 1995 (corr. 2nd printing 1999).
28. M. Rötteler and T. Beth, Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups, preprint available at `http://xxx.lanl.gov/abs/quant-ph/9812070`.
29. P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. on Computing*, vol. 26(5), 1997, 1484–1509.
30. D. Simon, On the power of quantum computation, *SIAM J. on Computing*, vol. 26(5), 1997, 1474–1483.
31. J. Watrous, Quantum algorithms for solvable groups, *Proc. 33rd ACM Symposium on Theory of Computing*, 2001, 60–67.