CS682A Final Project Report: The Hidden Subgroup Problem

Anurag Sahay
11141/11917141
asahay@iitk.ac.in

April 21, 2016

Abstract

The Hidden Subgroup Problem is a well-known computational problem in Algebra whose efficient solution has wide-reaching consequences, including, but not limited to integer factoring, discrete logarithm, graph isomorphism and the shortest vector problem. We will consider some quantum algorithms that work for special cases of the HSP.

We will take some theorems for granted, in order to streamline our discussion with respect to the essence of the HSP. Theorems that will be used but will not be proven will be marked by a $\star$.

Contents

Chapter 1

Introduction to the HSP

Let G be a group, and suppose that $f : G \to X$ is a function, for some set X such that for $x, y \in G$, $f(x) = f(y) \implies xH = yH$ for some sugbroup $H \leq G$. In other words, $f(x) = f(y)$ implies that x and y belong to the same coset of H in G.

Given the function f as an oracle, the problem is to determine the "Hidden" subgroup H. In such a case, we say that the function f "hides" the subgroup H. To make the output computationally tractable, instead of asking for the subgroup, we instead look for a generating set of the subgroup.

The Hidden Subgroup Problem is of seminal importance in algebraic and number-theoretic problems in Quantum Computation. In particular, the famous Shor's algorithms for integer factoring and discrete logarithm both fundamentally depend on the fact that the HSP for the special case of finite abelian groups can be solved in polynomial time by a quantum computer. Further, the existence of efficient quantum algorithms for HSPs for various non-abelian or for infinite abelian groups will imply efficient algorithms for some major problems, including the Graph Isomorphism problem (which depends on HSP for symmetric groups) and the Shortest Vector Problem in certain lattices (which depends on HSP for dihedral groups).

For this project, we will focus on the known results on the HSP, beginning with the HSP for finite abelian groups, and its applications to Shor's algorithm, followed by other good quantum algorithms for groups which are close, in an exact sense, to being abelian, and then finally talking about the limitations of this proof method, and about the need for some new idea to

solve the general (as yet unsolved) nonabelian case of the HSP. In particular, we note that the Quantum Fourier Transform provides a speed up in comparison to the Fast Fourier Transform and other classical methods of computation, leading to a breakthrough with respect to solving the HSP. We will see how this speed up leads to an efficient algorithm for different groups. In fact, according to [2] all time speed-ups that have been obtained on quantum computers depend crucially on being able to quickly solve the HSP, and it is conjectured that a classical computer with an oracle for the HSP could solve all the problems in BQP in polynomial time.

Now note that given an oracle that computes $f(g)$ given $g \in G$, with $|G|$ calls to the oracle, H may be determined. However, as input G will be given by an efficient encoding, it follows that an efficient algorithm must be polynomial in $\log |G|$, which shall be the goal of our project.

All our discussion is adapted either from [2] or [3].

Chapter 2

Abelian Hidden Subgroup Problem

In this chapter, we will discuss the solution to the Hidden Subgroup Problem for finite abelian groups, which is classically known using the Quantum Fourier Transform. We will develop whatever tools are necessary, and will direct the reader towards appropriate references for any tools that we do not develop.

Before moving on, we will describe the implementation of the oracle that computes f. We will assume a "black box" operator, that operates in unit time and performs the unitary transform $U_f |g, x\rangle = |g, x \oplus f(g)\rangle$ for $g \in G$, $x \in X$ and $\oplus$ as bit-wise addition/exclusive or. This implementation will also be used for the nonabelian case, later.

In this chapter, we will first solve the problem for $G = \mathbb{Z}/N\mathbb{Z} = \mathbb{Z}_N$, and then will generalize this solution to all finite abelian groups.

2.1 The Quantum Analogue of the Discrete Fourier Transform

In this section, we describe the Quantum Fourier Transform for $\mathbb{Z}_N$.

Definition 2.1 (Cyclic Quantum Fourier Transform (QFT))**.** The Cyclic Quantum Fourier Transform F_N is an operator on a register with $n \geq \log N$ qubits given by

$$F_N = \frac{1}{\sqrt{N}} \sum_{j,k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle \langle j|$$

It is easy to see that this is a unitary transformation. The algorithm solving the Abelian HSP will crucially use the QFT, and hence its time complexity depends directly on the time complexity of the QFT. Thus, we need to discuss both what it means for QFT to be efficiently computable, and prove that it is, in fact, efficiently computable.

Definition 2.2 (Efficiency of QFT)**.** A family of quantum circuits $\{U_i\}$ computing the quantum Fourier transform over a family of finite groups $\{G_i\}$ is called *efficient* if $|U_i| = \text{polylog}\,|G|$.

Now note that, if we have an efficient QFT algorithm for A and B such that $(A, B) = 1$, then we have an efficient QFT algorithm for $N = AB$. To see this, note that we have an (efficiently computable and reversible) isomorphism $\mathbb{Z}_N = \mathbb{Z}_A \times \mathbb{Z}_B$ given by the Chinese Remainder Theorem. Now, let U_A be the unitary transform $U_A |x \mod A\rangle = |xB \mod A\rangle$ (and conversely define U_B, then it is easy to show by the Chinese Remainder Theorem that

$$F_N = (U_B \otimes U_A)(F_A \otimes F_B)$$

which proves our claim. Hence, it is sufficient to efficiently compute QFT for $N = 2^n$ and odd N.

We now have the following theorems:

Theorem 2.1 ($\star$)**.** *The quantum Fourier transform F_N can be exactly efficiently computed for $N = 2^n$*

Theorem 2.2 ($\star$)**.** *Let $N \geq 13$ be an odd integer, and $0 < \epsilon \leq \sqrt{2}$. Then the quantum Fourier transform F_N can be computed with error bounded by ϵ using at most $13 + 3 \log \frac{\sqrt{N}}{\epsilon}$ qubits, with operational time complexity given as*

$$\mathcal{O}\left(\log \frac{\sqrt{N}}{\epsilon} \left(\log\log \frac{\sqrt{N}}{\epsilon} + \log \frac{1}{\epsilon}\right)\right)$$

Putting the above two together, it is clear that we can compute the quantum Fourier transform to arbitrary accuracy efficiently.

2.2 The Algorithm for the Cyclic Group $G = \mathbb{Z}_N$

We now present the quantum algorithm that solves the HSP for the cyclic group, show that it is efficient, and prove that the algorithm works.

Now note that, we can view the elements of G as the basis states; hence $G = \{|0\rangle, |1\rangle, \cdots, |N-1\rangle\}$. Suppose H is the hidden subgroup. Due to what we know about the structure of cyclic groups, we know that H is generated by some element and hence $H = \{|0\rangle, |d\rangle, \cdots, |(M-1)d\rangle\}$ for some M and d such that $dM = N$.

The algorithm is as follows:

1. Begin with the state $|0\rangle|0\rangle$. Applying F_N on the first register, and then calling the oracle for f, we obtain

$$\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle |f(j)\rangle$$

2. Measure the second register, to obtain some value $f(j_0)$, collapsing the state and leaving only those j in the first register which have $f(j_0)$ in the second register - that is, leaving only elements of $j_0 + H$. We can now drop the second register to get the state

$$\frac{1}{\sqrt{M}} \sum_{h \in H} |j_0 + h\rangle = \frac{1}{\sqrt{M}} \sum_{s=0}^{M-1} |j_0 + sd\rangle$$

3. Apply F_N to obtain

$$\frac{1}{\sqrt{M}} \sum_{s=0}^{M-1} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i (j_0 + sd)k}{N}} |k\rangle = \frac{1}{\sqrt{MN}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j_0 k}{N}} |k\rangle \sum_{s=0}^{M-1} e^{\frac{2\pi i s d k}{N}}$$

Using, $N = dM$, and the orthogonality of additive characters, it follows that all states except multiples of M disappear and hence we have the state

$$\frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} e^{\frac{2\pi i j_0 t M}{N}} |tM\rangle$$

4. Measure the state repeatedly (say k times, k to be determined later) to obtain $M_1, M_2, \cdots, M_k$ which are all multiples of M. Compute the GCD $M' = (M_1, \cdots, M_k)$ and output $d' = N/M'$.

It is easy to see that if we appropriately bound k (in fact, $k = 4$ works) then in each step only polynomially computations occur. Further, we need to show that the final output d' shall be d with high probability. Suppose $t_i = M_i/M$. Then it can be show that

$$P((t_1, \cdots, t_k) = 1) \geq 1 - \frac{1}{2^{k/2}}$$

Hence, we can solve the HSP for cyclic groups with high probability.

2.3 Character Theory for Finite Abelian Groups

We now develop the basics of character theory for finite abelian groups that we need for this application. Before we do that, however, note the following standard theorem:

Theorem 2.3 (Structure Theorem of Finite Abelian Group, $\star$)**.** *Every finite abelian group is isomorphic to a direct product of finite cyclic groups.*

We will use this theorem crucially in our algorithm. In particular, note that any element $g \in G$ can be written as a k-tuple if $G \sim \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_k}$, where $g = (g_1, \cdots, g_k)$ and each g_i is an integer modulo N_i.

We now delve into character theory.

Definition 2.3 (Character of a group)**.** A *character* of a group G is a group homomorphism $\chi : G \to \mathbb{C}^\times$ into the multiplicative group of complex numbers.

Writing G additively, we have that $\chi(ng) = \chi(g)^n$. Now, let $\beta_1 = (1, 0, \cdots, 0)$, $\beta_2 = (0, 1, \cdots, 0)$, $\cdots$, $beta_k = (0, 0, \cdots, 0, 1)$ all in G. Then we can write $g = (g_1, \cdots, g_k) = \sum_{j=1}^{k} g_j \beta_j$. Hence,

$$\chi(g) = \chi\left(\sum_{j=1}^{k} g_j \beta_j\right) = \prod_{j=1}^{k} \chi(\beta_j)^{g_j}$$

Hence, χ is completely determined by its values on β_j. Further, since β_j has order N_j, $\chi(\beta_j)$ must have order dividing N_j, and hence $\chi(\beta_j) = \omega_{N_j}^{h_j}$ for some integer h_j (determined only modulo N_j) where ω_N is a primitive Nth root of unity that has been fixed in the beginning. Thus, χ is determined by the k-tuple $(h_1, \cdots, h_k)$ which may be viewed as an element of of G. Thus, for each $h \in G$, we define the character χ_h given by

$$\chi_h(g) = \prod_{j=1}^{k} \omega_{N_j}^{g_j h_j}$$

It is easy to see that

$$\chi_g(h) = \chi_h(g)$$

and that

$$\chi_g(-h) = \overline{\chi_g(h)}$$

Let $\chi(G)$ be the group (under pointwise multiplication) of all such characters. Then it is easy to see that

Theorem 2.4. $\chi(G) \sim G$

Proof. Note that the map $g \mapsto \chi_g$ is an invertible homomorphism, and is hence an isomorphism. □

We can now define orthogonal subgroups as follows

Definition 2.4 (Orthogonal Subgroup)**.** Let H be a subgroup of G. Its orthogonal subgroup $H^\perp$ is given by

$$H^\perp = \{g \in G : \forall h \in H, \chi_g(h) = 1\}$$

It can be shown that

$$G/H \sim H^\perp$$

and that

$$H^{\perp\perp} = H$$

2.4 General Quantum Fourier Transform

In this section, we will define the QFT for an arbitrary finite abelian group.

Definition 2.5 (General Quantum Fourier Transform (QFT))**.** The Quantum Fourier Transform F_G over a group G is an operator on a group register defined as follows:

$$F_G = \frac{1}{\sqrt{|G|}} \sum_{g,h \in G} \chi_g(h) \left|g\right\rangle \left\langle h\right|$$

It is trivial to see that for $G = \mathbb{Z}_N$ this reduces to the cyclic QFT. We now further define the translation operation τ_t and phase-change operation ϕ_h for $t, h \in G$ as

$$\tau_t = \sum_{g \in G} \left|t + h\right\rangle \left\langle h\right|$$

$$\phi_h = \sum_{g \in G} \chi_g(h) \left|g\right\rangle \left\langle g\right|$$

Now note that we have the following identity

$$F_G \tau_t = \phi_t F_G$$

We also have that

$$F_G \left|H\right\rangle = \left|H^{\perp}\right\rangle$$

To see this, note that

$$\left|H\right\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} \left|h\right\rangle$$

Thus,

$$F_G \left|H\right\rangle = \frac{1}{\sqrt{|G||H|}} \sum_{g,h' \in G} \chi_g(h') \left|g\right\rangle \left\langle h'\right| \sum_{h \in H} \left|h\right\rangle$$

Simplifiying, we get that

$$F_G \left|H\right\rangle = \frac{1}{|G||H|} \sum_{g \in G} \left(\sum_{h \in H} \chi_g(h) \right) \left|g\right\rangle$$

Now, the sum in the bracket does not disappears if and only if H is orthogonal to g, and hence we can see that

$$F_G \left|H\right\rangle = \frac{1}{|G||H|} \sum_{g \in H^{\perp}} |H| \left|g\right\rangle = \sqrt{\frac{|H|}{|G|}} \sum_{g \in H^{\perp}} \left|g\right\rangle = \left|H^{\perp}\right\rangle$$

2.5 The Algorithm for the general Finite Abelian Group G

We now present the quantum algorithm that solves the HSP for the general finite abelian group and show that it is efficient. The proof of correctness of the algorithm is not presented, and can be seen in [2]

As with the cyclic group, we can view the elements of G as the basis states; hence $G = \{|g\rangle : g \in G\}$. Suppose H is the hidden subgroup.

The algorithm is as follows:

1. Begin with the state $|0\rangle |0\rangle$. Applying F_G on the first register, and then calling the oracle for f, we obtain

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle$$

   Now let T be a set of representatives of the cosets of H. We can simplify our state as

$$\frac{1}{\sqrt{|T|}} \sum_{t \in T} |t + H\rangle |f(t)\rangle = \frac{1}{\sqrt{|T|}} \sum_{t \in T} \tau_t |H\rangle |f(t)\rangle$$

2. Applying the Fourier transform F_G again on the first register, and applying the results we have shown, we get

$$\frac{1}{\sqrt{|T|}} \sum_{t \in T} F_G \tau_t |H\rangle |f(t)\rangle = \frac{1}{\sqrt{|T|}} \sum_{t \in T} \phi_t F_G |H\rangle |f(t)\rangle = \frac{1}{\sqrt{|H^\perp|}} \sum_{t \in T} \phi_t |H^\perp\rangle |f(t)\rangle$$

$$\frac{1}{\sqrt{M}} \sum_{h \in H} |j_0 + h\rangle = \frac{1}{\sqrt{M}} \sum_{s=0}^{M-1} |j_0 + sd\rangle$$

3. Measure the first register obtaining a random element of $H^\perp$. Note that ϕ_t does not affect the amplitude, and hence does not affect the probability.

It can now be shown that, at least $t + \log |G|$ uniformly random elements of a group G generate it with probability greater than $1 - 1/2^t$. Further, with a generating set of $H^\perp$, one can efficiently compute a generating set of $H^{\perp\perp} = H$. Please see [2] for the details.

Chapter 3

Nonabelian Hidden Subgroup Problem

In this chapter, we will develop the representation theory machinery that we need to adequately solve the HSP for certain finite nonabelian groups. We will explicitly solve the problem for the following two cases:

- If the hidden subgroup H of an arbitrary finite nonabelian group G is normal in G.
- The finite nonabelian group is "almost" abelian in a very precise sense.

Finally, we will discuss the applicability of this proof method to the general finite nonabelian case.

3.1 Representation Theory

Representation theory plays an analogous role for nonabelian groups as character theory does for abelian groups. This is natural - the representation theory of an abelian group reduces to its character theory. In this section, we will develop the requisite knowledge we need about representation theory.

Definition 3.1 (Representation of a group)**.** A representation ρ of a group G is a group homomorphism $\rho : G \to GL(V)$ where V is a vector space over a field $\mathbb{F}$ and d_ρ is the dimension of V.

For our application, the field $\mathbb{F}$ shall be the field of complex number $\mathbb{C}$, and d_ρ shall always be finite.

We say that a representation is reducible if there exists a vector subspace W of V such that $(0) \neq W \neq V$ and such that $\rho(g)$ fixes W for all $g \in G$. If a representation is not reducible, we call it irreducible. It can be shown that for any reducible representation, the complement $W^\perp$ of W in V is also fixed by $\rho(g)$ for all g, and hence the representation ρ can be written as the direct sum of $\rho_W \oplus \rho_{W^\perp}$, where ρ_W is ρ restricted onto W. Hence, any finite dimensional reducible representation may in fact be written as $\rho = \rho_1 \oplus \cdots \oplus \rho_k$ where each ρ_i is irreducible.

We say that $\rho_1 \sim \rho_2$ (in words, ρ_1 is isomorphic to ρ_2, if there exists an isomorphism $\phi : V_1 \to V_2$ of their underlying vector spaces such that, for all $g \in G$ and $v \in V_1$, $\phi(\rho_1(g)v) = \rho_2(g)\phi(v)$. There are only finitely many non-isomorphic irreducible representations (the set of which is denoted as $\hat{G}$), and in fact,

$$|G| = \sum_{\rho \in \hat{G}} d_\rho^2$$

Further, for any representation ρ, one can define a character χ_ρ as $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$.

We now describe the analogue of the Fourier transform in the nonabelian context. To do this, we first map elements g of G to vectors v_g in a vector space of dimension $|G|$ indexed by (ρ, i, j) where ρ runs over all non-isomorphic irreducible characters and i, j run from 1 to d_ρ. The previous result shows that this index gives a vector space of the right dimension. v_g is now given as

$$(v_g)_{\rho,i,j} = \frac{\sqrt{d_\rho}\rho_{ij}(g)}{|G|}$$

where $\rho_{ij}(g)$ is the (i,j)th entry of $\rho(g)$. Now, elements of G act as a basis of the $\mathbb{C}$-algebra given by the complex linear combinations of elements of G. Hence, we can extend this to a linear map of this $\mathbb{C}$-algebra. This linear map is known as the Fourier Transform.

Now define, for any subset S of G,

$$\rho(S) = \rho(|S\rangle) = \frac{1}{\sqrt{|S|}} \sum_{g \in S} \rho(g)$$

Then it is easy to see from the orthogonality of representations that $\rho(G)$ is the scalar matrix $\sqrt{|G|}$ if ρ is trivial, and the zero matrix otherwise.

3.2 The "Standard Method"

In this section, we describe what is called the "Standard Method" for solving the HSP by the authors of [3], which is essentially the same algorithm which is used for all known solved cases of the HSP (including the abelian case, and the nonabelian cases that we will consider in this chapter).

The method is as follows:

1. Form the uniform superposition over a random coset gH (that is $|gH\rangle$ of the hidden subgroup H. This is done by taking the uniform distribution $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |0\rangle$, applying f, and then measuring and discarding the second register. Thus, we have

$$|gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$$

2. Apply the nonabelian Fourier transform on this vector to obtain

$$\frac{1}{sqrt|G||H|} \sum_{\rho,i,j} \sqrt{d_\rho} \sum_{h \in H} \rho_{ij}(gh) |\rho, i, j\rangle$$

   Now note that this gives a probability distribution over the representation ρ and its indices.

3. Sample the Fourier transform polynomially many times by performing a measurement. Do some post-processing

For the above described method to work, polynomially samples of the Fourier transform should be sufficient to reconstruct H with high probability - for the abelian case, this is true, and something similar holds for the two cases

described in the beginning of this chapter. The question now arises as to whether this is possible.

In both the nonabelian applications, a "weak form" of the method suffices whereby we only obtain the probability distribution of ρ and discard the indices.

3.3 Maximal Normal Subgroup and Solving the HSP for H normal subgroup of G

We will now state a theorem that we will use without proof. Please see [3] for a proof. This theorem encapsulates the special nature of normal subgroups which allow the HSP to be solved in that case.

Theorem 3.1 (Maximal Normal Subgroup contained in H, $\star$)**.** *Let H be the hidden subgroup of a group G. Further, suppose ρ is sampled $\mathcal{O}(\log |G|)$ times from the Fourier transform. Further, let $N = \cap_\rho \ker \rho$. Then, with high probability N is the maximal normal subgroup of G which is contained in H.*

It is now easy to see that if G is any nonabelian group, and H is a hidden subgroup such that H is normal in G, then $H = N$ from the theorem, and H can be computed with high probability in an efficient manner.

3.4 "Almost" Abelian Groups

Using the results of the previous section, we can now solve the HSP for a general class of nonabelian subgroups which are "almost" abelian in a very precise sense. To describe this solution, we first describe "almost" abelian groups.

Definition 3.2 (Baer Norm)**.** For any subgroup H of G, define the normalizer $N(H)$ as the largest subgroup of G containing H in which H is normal. In other words,

$$N(H) = \{g \in G : gH = Hg\}$$

Then the Baer norm of G is the subgroup $\kappa(G)$ given by

$$\kappa(G) = \bigcap_{H \subset G} N(H)$$

where the intersection runs over all subgroups of G.

It is easy to see that $\kappa(G) = G$ for any abelian group. Hence, the size of $\kappa(G)$ can be seen as a measure of how abelian a group is - the larger it is, the more abelian the group. In other words, the size of $[G : \kappa(G)]$ can be seen as a similar measure: the closer it is to 1, the more abelian the group is.

Definition 3.3 ("Almost" Abelian)**.** We say a group G is "almost" abelian if

$$[G : \kappa(G)] = \exp(\mathcal{O}(\sqrt{\log |G|}))$$

Theorem 3.2. *$\kappa(G)$ is normal in G.*

Proof. Let $g \in \kappa(G)$ and $a \in G$. We need to show that $aga^{-1} \in N(H)$ for all subgroups H.

Fix an H, and let $h \in H$. Then,

$$(aga^{-1})h(aga^{-1})^{-1} = aga^{-1}hag^{-1}a^{-1}$$

Now, $a^{-1}ha \in a^{-1}Ha$, and $g \in \kappa(G) \subset N(a^{-1}Ha)$. Hence,

$$ga^{-1}hag^{-1} \in a^{-1}Ha$$

But then $aga^{-1}hag^{-1}a^{-1} \in H$ as required.

□

Now we consider the following question: how many subgroups of G are there which contain $\kappa(G)$. By one of the isomorphism theorems of groups, this is the same as the number of subgroups of $G/\kappa(G)$. However, if m is the size of a group, the group has at most $2^{(\log_2 m)^2}$ subgroups. Hence, for an "almost" abelian group, there at most polynomially many (in $\log |G|$) subgroups containing $\kappa(G)$.

Thus, the algorithm for solving an "almost" abelian group HSP is essentially brute force. Let G be the group and H a hidden subgroup. Let J be a subgroup such that $\kappa(G) \subset J \subset G$. Define $H_J = H \cap J$. Then, clearly, the same function f hides the subgroup H_J in J. Using the algorithm described in the previous section, we can efficiently compute, with high probability, the maximal normal subgroup N_J of J which is contained in H_J. Let $N = \cup_J N_J$ where the union runs over all subgroups J described above. Then, $N = H$. To see this, note that $N_J \subset H_J \subset H$. Furthermore, for $J = N(H)$ ($\kappa(G) \subset N(H)$ by the definition of the Baer norm), it is clear that N_J is, in fact, equal to H. Hence we are done.

Chapter 4

Conclusion

As shown in this report, using what is known as the (weak form of the) standard method, one can solve the HSP for a fairly large class of groups. However, the HSP for the general nonabelian group is still open, and it is unknown if there is any quantum speed-up in this case. Furthermore, note that there is an inherent ambiguity in the definition of the nonabelian Fourier transform: for a given representation ρ, we can fix the basis of its vector space, and each choice for the basis gives a different transform. It is known that if we randomly choose this basis, then the standard method is likely to fail - for sufficiently small hidden subgroup H and sufficiently nonabelian (in the sense of the Baer norm, and other senses) group G, a random basis will not provide sufficient information to reconstruct H even if we use the strong form of the standard method. See [3] for the details.

Bibliography

[1] W. V. Dam and Y. Sasaki, *Quantum Algorithms for Problems in Number Theory, Algebraic Geometry, and Group Theory* (2012), arxiv *preprint* `http://arxiv.org/pdf/1206.6126v1.pdf`

[2] C. Lomont, Cybernet, *The Hidden Subgroup Problem - Review and Open Problems* (2004), arxiv *preprint* `http://arxiv.org/pdf/quant-ph/0411037v1.pdf`

[3] M. Grigni, L. J. Schulman, M. Vazirani, U. Vazirani, *Quantum Mechanical Algorithms for the Nonabelian Hidden Subgroup Problem*, COMBINATORICA **24 (1) (2004), 137-154** `https://www.math.ucdavis.edu/~vazirani/Papers/hidden.subgroup.pdf`