Quantum Algorithm for Decomposing Black-Box Finite Abelian Groups

Yong Zhang
Department of Computer Science, Kutztown University of Pennsylvania, Kutztown, PA 19530

Abstract— *Cheung and Mosca [1] gave an efficient quantum algorithm for decomposing finite abelian groups in a unique-encoding group model. We present another efficient quantum algorithm for this problem in a more general model, the black-box group model, where each group element is not necessarily uniquely encoded.*

Keywords: quantum computation, black-box group model

1. Introduction

Any finite abelian group G can be decomposed into the direct sum of cyclic subgroups of prime power order. However, given a set of generators for G, no efficient classical algorithm is known to find the decomposition of G, i.e., find generators for the cyclic subgroups of G. This problem is at least as hard as INTEGER FACTORIZATION – finding nontrivial factors of a given integer N is equivalent to finding the decomposition of the (finite abelian) group $\mathbb{Z}_N^*$, the multiplicative group of integers modulo N.

Decomposing finite abelian groups plays an important role in quantum computation, the study of the information processing tasks that can be accomplished using quantum mechanical systems. We call an algorithm that is defined over a traditional computational model a *classical algorithm* and an algorithm that is defined over a quantum computational model a *quantum algorithm*.

In 1994 Shor [2] presented polynomial-time quantum algorithms for two important problems INTEGER FACTORIZATION and DISCRETE LOGARITHM. No efficient classical algorithms are known for these two problems. These two problems are widely believed to be hard on classical computers; their hardness are the basic assumptions for several cryptosystems including the widely used RSA public-key cryptosystem. Shor's paper is the first illustration of the practical importance of quantum computation. A key component in Shor's algorithms is the efficient implementation of the Quantum Fourier Transform (QFT), which explores the underlying algebraic structure of the problems. From this perspective, Shor's quantum algorithms, together with several other quantum algorithms, can be further generalized to a quantum algorithm for the HIDDEN SUBGROUP problem where the given group G is abelian. In the case when G is non-abelian, the HIDDEN SUBGROUP problem generalizes other well-known problems such as GRAPH ISOMORPHISM. However, the non-abelian case is much harder to solve and remains a major challenge in quantum computation.

Before one can efficiently implement QFT to solve the abelian HIDDEN SUBGROUP problem, the decomposition of the given abelian group G must be known. Cheung and Mosca [1] first studied the problem of decomposing finite abelian groups. They gave an efficient quantum algorithm for this problem. However, one of their assumptions is that each element of the input group G is *uniquely* represented by a binary string. In another word, their quantum algorithm only works for a unique-encoding group model.

In this paper we study the problem of decomposing finite abelian groups in a more general group model — the black-box group model. In the black-box group model elements of the input group G are not necessarily uniquely encoded. The black-box group model was first introduced by Babai and Szemerédi [3] as a general framework for studying algorithmic problems for finite groups. It is a widely used model in computational group theory and quantum computation [4], [5], [6], [7], [8], [9]. This non-unique encoding feature enables this model to handle factor groups [3]. A *factor group* (also known as quotient group) is a group obtained by identifying together elements of a larger group using an equivalence relation. In this paper we give an efficient quantum algorithm for decomposing finite abelian groups in the black-box group model.

2. Perliminaries

In this section we give a brief introduction of the fundamental results in group theory. We refer the readers to a classic book on group theory [10] for more details.

A set G is called a *group* if there is a binary operation $\cdot$ defined on G such that:

1) for any $x, y \in G$, $x \cdot y \in G$.
2) for any $x, y, z \in G$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

3) there is an identity element $e \in G$ such that for any $x \in G$, $x \cdot e = e \cdot x = x$.
4) for any $x \in G$, there is a unique $x^{-1} \in G$ such that $x \cdot x^{-1} = x^{-1} \cdot x = e$.

The set of integers $\mathbb{Z}$ together with the "+" operation is an example of a group. Usually if the binary operation $\cdot$ is obvious from the context, we will just write xy instead of $x \cdot y$.

A group G is *abelian* if and only if for any $x, y \in G$, $xy = yx$. Otherwise, G is *nonabelian*. A group G is *cyclic* if there exist $a \in G$ such that $G = \{a^n | n \in \mathbb{Z}\}$. Then we say a is a *generator* of G. A *subgroup* H of a group G is a subset which is also a group under the same operation in G. If H is a subgroup of a group G, then a *right coset* of H is a subset S of G such that $\exists x \in G$ for which $S = Hx = \{yx : y \in H\}$. A *left coset* of H is defined similarly. The *order* of a group G, denoted by $|G|$, is the cardinality of the set G. The order of the element a is the smallest number n such that $a^n = e$, denoted by $ord(a)$. If such $n \in \mathbb{Z}$ exists, we say a has *finite order*. In fact, the subset $\{e, a, a^2, \ldots, a^{n-1}\}$ forms a subgroup. We call this subgroup the *cyclic subgroup generated by* a and denote it by $\langle a \rangle$.

Lagrange's Theorem states that if H is a subgroup of a group G, then $|H|$ divides $|G|$. We say $[G : H] = |G|/|H|$ is the *index* of H in G. Let G be a group, p be a prime number, and P be a subgroup of G. If $|P| = p^r$ for some $r \in \mathbb{Z}$, we say P is a *p-subgroup* of G. If furthermore p^r divides $|G|$ but p^{r+1} does not, then we say P is a *Sylow p-subgroup* of G. Let G_1, G_2 be groups such that $G_1 \cap G_2 = \{e\}$. The set $\{(a_1, a_2) \mid a_1 \in G_1, a_2 \in G_2\}$, denoted by $G_1 \oplus G_2$, is called the *direct sum* of G_1 and G_2. $G_1 \oplus G_2$ is a group under the binary operation $\cdot$ such that $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$.

The fundamental theorem of finite abelian groups states the following.

Theorem 2.1: Given a set $\{g_1, \ldots, g_n\}$ of generators of the finite abelian group G, find a set of elements $h_1, \ldots, h_k \in G$ such that $G = \langle h_1 \rangle \oplus \cdots \oplus \langle h_k \rangle$ and $\langle h_i \rangle$ is a cyclic group of prime power order for all $1 \leq i \leq k$.

Next we introduce the black-box group model. We fix the alphabet $\Sigma = \{0, 1\}$. A *group family* is a countable sequence $\mathcal{B} = \{B_m\}_{m \geq 1}$ of finite groups B_m, such that there exist polynomials p and q satisfying the following conditions. For each $m \geq 1$, elements of B_m are encoded as strings (not necessarily unique) in $\Sigma^{p(m)}$. The group operations (inverse, product and identity testing) of B_m are performed at unit cost by black-boxes (or group oracles). The order of B_m is computable in time bounded by $q(m)$, for each m. We refer to the groups B_m of a group family and their subgroups (presented by generator sets) as *black-box groups*. Common examples of black-box groups are $\{S_n\}_{n \geq 1}$ where S_n is the permutation group on n elements, and $\{GL_n(q)\}_{n \geq 1}$ where $GL_n(q)$ is the group of $n \times n$ invertible matrices over the finite field F_q. Depending on whether the group elements are uniquely encoded, we have the *unique encoding model* and *non-unique encoding model*, the latter of which enables us to deal with factor groups [3]. In the non-unique encoding model an additional group oracle has to be provided to test if two strings represent the same group element.

3. The Algorithm

Our algorithm uses a divide-and-conquer approach. The algorithm first finds the Sylow p-subgroups of the given input group and then decomposes each Sylow p-subgroup. We start with two technical Lemmas. The first Lemma shows how to find a p-Sylow subgroup in quantum polynomial time.

Lemma 3.1: Let B = $\{B_m\}_{m>0}$ be a group family. Let $G < B_m$ be an abelian black-box group given by generating sets $S = \{g_1, \ldots, g_s\}$. For any prime number p, the generating sets for the p-Sylow subgroup of G can be computed in quantum polynomial time.

Proof: Since G is abelian, for any prime p, there is an unique p-Sylow subgroup of G. Let n be the the order of B_m. By our assumption for black-box model, we can efficiently compute n. Furthermore, we can use Shor's algorithm to compute the prime factorization $p_1^{e_1} \cdots p_r^{e_r}$ of n. If p is not a factor of n, then clearly the p-Sylow subgroup of G is trivial. If p is equal to p_k for some $1 \leq k \leq r$, then we compute the set $S_k = \{g_1', \ldots, g_s'\}$ where $g_i' = g_i^{n/p_k^{e_k}}$. Note that this can be done efficiently using modular exponetiation. We claim that S_k is the generating set for the p-Sylow subgroup. Clearly the order of g_i' is power of p for all i, so $\langle S_k \rangle$ is a p-subgroup of G. To show that $\langle S_k \rangle$ is indeed the p-Sylow subgroup it suffices to show that any $g_i \in S$ can be written as products of elements in $\langle S_1 \rangle, \ldots, \langle S_r \rangle$, i.e., $G = \langle S_1 \rangle \oplus \cdots \oplus \langle S_r \rangle$. Since $\Sigma_{l=1}^r n/p_l^{e_l}$ is coprime with n and thus the order of any elements in G, for any $g_i \in G$, $g_i^{\Sigma_{l=1}^r n/p_l^{e_l}}$, which is a product of elements in $\langle S_1 \rangle, \ldots, \langle S_r \rangle$, generates the same cyclic subgroup that g_i generates. ■

Any finite abelian p-group can be expressed as a direct sum of m cyclic groups with order $p^{e_1}, \ldots, p^{e_m}$ and $e_1 \leq \cdots \leq e_m$. We say that $(e_1, \ldots, e_m)$ is the *type* of the p-group. In the second lemma we describe a method to decompose a finite abelian p-group.

Lemma 3.2: Let G be a finite abelian p-group of type

$(m_1, m_2, \ldots, m_s)$. Let $g_1, \ldots, g_i$ be elements of G of orders $p^{m_1}, \ldots, p^{m_i}$ and for any $j \neq k$ and $1 \leq j, k \leq i$ the cyclic groups $\langle g_j \rangle$, $\langle g_k \rangle$ have trivial intersection. Given $a\langle g_1, \ldots, g_i \rangle$ as an element in the factor group $G/\langle g_1, \ldots, g_i \rangle$ of order $p^{m_{i+1}}$ with $a^{p^{m_{i+1}}} = g_1^{x_1} \cdots g_i^{x_i}$, we can efficiently find another element g_{i+1} of order $p^{m_{i+1}}$ where $\langle g_{i+1} \rangle$ and is $\langle g_1, \ldots, g_i \rangle$ have trivial intersection.

Proof: First we show that x_j is a multiple of $p^{m_{i+1}}$ for all $1 \leq j \leq i$.

$$\begin{aligned} a^{p^{m_i}} &= (a^{p^{m_{i+1}}})^{p^{m_i - m_{i+1}}} \\ &= (g_1^{x_1} \cdots g_i^{x_i})^{p^{m_i - m_{i+1}}} \\ &= g_1^{x_1 p^{m_i - m_{i+1}}} \cdots g_i^{x_i p^{m_i - m_{i+1}}}. \end{aligned}$$

But $a^{p^{m_i}}$ is clearly in $\langle g_1, \ldots, g_{i-1} \rangle$, so $g_i^{x_i p^{m_i - m_{i+1}}}$ is also in $\langle g_1, \ldots, g_{i-1} \rangle$, therefore x_i is a multiple of $p^{m_{i+1}}$. Similarly we have

$$\begin{aligned} a^{p^{m_{i-1}}} &= (a^{p^{m_{i+1}}})^{p^{m_{i-1} - m_{i+1}}} \\ &= g_1^{x_1 p^{m_{i-1} - m_{i+1}}} \cdots g_i^{x_i p^{m_{i-1} - m_{i+1}}} \\ &= g_1^{x_1 p^{m_{i-1} - m_{i+1}}} \cdots g_{i-1}^{x_{i-1} p^{m_{i-1} - m_{i+1}}}. \end{aligned}$$

By the same reasoning x_{i-1} is also a multiple of $p^{m_{i+1}}$. Clearly this inductive procedure can go down to $i = 1$. Thus x_j is a multiple of $p^{m_{i+1}}$ for all $1 \leq j \leq i$. Let $y_j = x_j / p^{m_{i+1}}$ for $1 \leq j \leq i$ and $g_{i+1} = a g_1^{-y_1} \cdots g_i^{-y_i}$. Then

$$\begin{aligned} g_{i+1}^{p^{m_{i+1}}} &= (a g_1^{-y_1} \cdots g_i^{-y_i})^{p^{m_{i+1}}} \\ &= a g_1^{-x_1} \cdots g_i^{-x_i} \\ &= e \end{aligned}$$

It is also easy to verify that $\langle g_{i+1} \rangle$ and $\langle g_1, \ldots, g_i \rangle$ have trivial intersection. ∎

Now we describe the whole algorithm. Given a generating set $\{g_1, \ldots, g_s\}$ of a finite abelian group $G \subseteq B_m$, we want to output a set of elements $\{d_1, \ldots, d_l\}$ such that $G = \langle d_1 \rangle \oplus \cdots \oplus \langle d_l \rangle$. The algorithm uses a divide-and-conquer approach. It first computes the generating set of each p-Sylow subgroup, and then convert each generating set into an "indepedent generating set". We say a generating set S of a group is *indepedent* if for any two element $s_i, s_j \in S$, $\langle s_i \rangle$ and $\langle s_j \rangle$ has trivial intersection. Note that in a p-group an independent generating set is exactly the decomposition of the p-group.

We first compute $|B_m|$. Recall that in the black-box model, $|B_m|$ is computable in time bounded by $q(m)$, for each m. In some cases, we will also obtain the prime factorization of $|B_m|$. If not, we can always use Shor's quantum algorithm for INTEGER FACTORIZATION to get the prime factorization $p_1^{e_1} \cdots p_r^{e_r}$. For $1 \leq i \leq s$, compute the order of g_i. This can be done using Watrous's quantum procedure for computing order of an group element in any solvable group [4]. Then, by Lemma 3.1 we can compute the generating set of each p_i-Sylow subgroup, $1 \leq i \leq r$.

Let X_i be the generating set for the p_i-Sylow subgroup. For each $1 \leq i \leq r$, we use Lemma 3.2 to compute an independent generating set S_i of the p_i-Sylow subgroup. We will construct S_i in steps. Initially S_i is empty. We add one element to S_i at each step. Suppose after the $(j-1)$'th step, $S_i = \{s_1, \ldots, s_{j-1}\}$. At the j'th step, first compute an element $h \in X_i$ such that $h\langle S_i \rangle$ has the maximum possible order in the factor group $\langle X_i \rangle / \langle S_i \rangle$. This can be done by the constructive group membership test described in [11], i.e., we will get $x_1, \ldots, x_{j-1}$ such that $h^{ord(h\langle S_i \rangle)} = \Pi_{k=1}^{j-1} s_k^{x_k}$. By Lemma 3.2, we will add the element $s_j = h \Pi_{k=1}^{j-1} s_k^{-x_k / ord(h\langle S_i \rangle)}$ to the set S_i. We then test if X_i is a subset of $\langle S_i \rangle$. If yes, we can stop and return S_i as the independent generating set. Otherwise, we will go to the $j+1$'th step.

Once we compute the independent generating set S_i for each p_i-Sylow subgroup, the decomposition of G is obtained as $\cup_{i=1}^{r} S_i$.

4. Discussion

In this paper we present an efficient quantum algorithm to decompose finite-abelian groups in a more general group model — black-box group model. Comparing to Cheung and Mosca's algorithm [1], our algorithm is conceptually simpler and only uses elementary results in group theory. Components of our algorithm may be used to construct quantum algorithms for HIDDEN SUBGROUP problem over certain non-abelian finite groups.

References

[1] K. Cheung and M. Mosca, "Decomposing finite abelian groups," *Quantum Information and Computation*, vol. 1, no. 3, 2001.

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, pp. 1484–1509, 1997.

[3] L. Babai and E. Szemerédi, "On the complexity of matrix group problems I." in *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science*, 1984, pp. 229–240.

[4] J. Watrous, "Quantum algorithms for solvable groups," in *Proceedings of the 33rd ACM Symposium on the Theory of Computing*, 2001, pp. 60–67.

[5] ——, "Succinct quantum proofs for properties of finite groups," in *Proceedings of the 41st IEEE Symposium on Foundations of Computer Science*, 2000.

[6] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen, "Hidden translation and orbit coset in quantum computing," in *Proceedings of the 35th ACM Symposium on the Theory of Computing*, 2003, pp. 1–9.

[7] S. Fenner and Y. Zhang, "Quantum algorithms for a set of group-theoretic problems," in *Proceedings of the Ninth IC-EATCS Italian Conference on Theoretical Computer Science, Siena, Italy*, 2005, pp. 215–227, lecture notes in computer science No. 3701.

[8] L. Babai, R. Beals, and A. Seress, "Polynomial-time theory of matrix groups," in *Proceedings of the 41st annual ACM symposium on Theory of computing*, ser. STOC '09, 2009, pp. 55–64.

[9] P. Holmes, S. Linton, E. O'Brien, A. Ryba, and R. Wilson, "Constructive membership in black-box groups," *Jounal of Group Theory*, vol. 11, pp. 747–763, 2008.

[10] W. Burnside, *Theory of Groups of Finite Order*. Dover Publications, Inc, 1955.

[11] G. Ivanyos, F. Magniez, and M. Santha, "Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem," in *Proceedings of 13th ACM Symposium on Parallelism in Algorithms and Architectures*, 2001, pp. 263–270.