Notes on Quantum Algorithms for the Finite HSP

1 Introduction

Given a finite group $(G, \circ)$ and a function $f\colon G \to X$ for some suitable set X with the property, that $f|_{gH}$ is constant and $f|_{gH} = f|_{hH} \to g = h$ for $g, h \in G$, where $H < G$ is an unknown subgroup. The problem of finding a generator for H is called the *Finite Hidden Subgroup Problem* (Finite HSP, FHSP). In these notes, we will review the generalization of the quantum algorithm for the Finite Abelian HSP to arbitrary finite groups, also known as *Quantum Fourier Sampling* (QFS), and discuss its inefficiency regarding the issue of classical reconstructibility. We will also review the information-theoretical quantum solution by Ettinger, Hoyer and Knill. Let $n, m, k \in \mathbb{N}_{\geq 1}$ throughout.

2 Representation Theory

In the case of finite Abelian groups, we were able to employ a characterization theorem [1, pp. 132-135], which allowed the use of qudit registers for storing elements. With this characterization theorem and with the help of character theory, which in turn required the characterization[1], it was possible to develop a quantum Fourier transform for finite Abelian groups with useful properties relating to the notion of orthogonal group subsets. Most of these steps required the commutativity of the group operation [2, pp. 17-20]. In the general case, we shall assume for these notes an $\mathcal{O}(\log_2(|G|))$-complex encoding of group elements as the canonical basis elements of the Hilbert space $\mathbb{C}^{|G|}$. The quantum algorithm for general finite HSPs requires another generalization of the QFT, based on representation theory, which is much different. We shall introduce the necessary definitions and facts here quickly. The following presentation of facts follows [2, pp. 25-28].

Definition 1 ([2, pp. 25-26])**.** We define the following notions.

(i) A *representation* of a group G is a group homomorphism $\rho\colon G \to \mathrm{GL}(\mathbb{C}^{d_\rho})$, $d_\rho \in \mathbb{N}$. We denote the *set of all representations* as $P(G)$.
(ii) A subspace $V \subseteq \mathbb{C}^{d_\rho}$ is said to be *invariant*, if $\rho(g)V \subseteq V$ for any $g \in G$.
(iii) If there are no invariant, nonzero and proper subspaces wrt. a representation ρ, then ρ is said to be *irreducible*.

We can always choose the trivial representation $g \mapsto E_{d_\rho}$ for any $g \in G$, allowing a zero-dimensional representation space, since any $\mathbb{C}^{d_\rho}$ would be invariant in that case, but requiring irreducibility forces a proper non-trivial representation. In the following, when we speak of subspaces, we shall speak of subspaces *up to an embedding*, i.e. when we reduce the general linear space for the values of a representation, we shall still talk of the reduced spaces as subspaces of $\mathbb{C}^{d_\rho}$.

Lemma 1 ([3, p. 6]). A representation $\rho \in P(G)$ with an invariant subspace $0 \neq V_1 \subset \mathbb{C}^{d_\rho}$ admits to an invariant subspace $0 \neq V_2 \subset \mathbb{C}^{d_\rho}$ with $\mathbb{C}^{d_\rho} = V_1 \oplus V_2$.

Corollary 2 (Decompositions of Representations). For a representation $\rho \in P(G)$, there are invariant subspaces $V_1, ..., V_k \subseteq \mathbb{C}^{d_\rho}$ with irreducible representations $\rho_i\colon G \to \mathrm{GL}(V_i)$ for any $i \in [1, k]_{\mathbb{N}}$, s.t. $\mathbb{C}^{d_\rho} = \bigoplus_{i=1}^k V_i$ and $\rho = \bigoplus_{i=1}^k \rho_i$.

Note that we use the linear-algebraic direct sum $\bigoplus$ instead of the usual sums of sets and functions, meaning that for a collection of bases $\{B_i \subseteq V_i\}_{1 \leq i \leq k}$, $\bigcup_{i=1}^k B_i$ is a basis of $\mathbb{C}^{d_\rho}$ via a natural embedding of the vectors of the subspaces. For ρ we look at the action of functions with this respect, giving the correctness of notation here. This result can be strengthened even further to the following result.

Definition 2 ([2, p. 25])**.** Two representations $\rho_1, \rho_2 \in P(G)$ are called *isomorphic*, if $\exists\ \varphi\colon \mathbb{C}^{d_{\rho_1}} \hookrightarrow\!\!\!\!\rightarrow \mathbb{C}^{d_{\rho_2}}$ with $\rho_1(g) = \rho_2(g) \circ \varphi\ \forall g \in G$.

[1] See the definition of induced characteristics.

Theorem 3 ([3, p. 7])**.** For any representation $\rho \in P(G)$, there is a decomposition into invariant subspaces $V_1, ..., V_k \subseteq \mathbb{C}$, unique up to isomorphism of distinct subgroups

$$\mathbb{C}^{d_\rho} = \bigoplus_{i=1}^{k} V_i^{\oplus \alpha_i} \tag{1}$$

with $\alpha_1, ..., \alpha_k \in \mathbb{N}_{\geq 1}$ and $\rho = \bigoplus_{i=1}^{k} \rho_i^{\oplus \alpha_i}$ with $\rho_i \colon G \to \mathrm{GL}(V_i)$ being the respective irreducible representations.

The powers $\alpha_1, ..., \alpha_k$ are used here to respect the fact that some spaces in a decomposition may be isomorphic. Theorem 3 also gives the fact, that there is always a *complete* and *finite* set of irreducible representations, i.e. one, s.t. the following decomposition is respected.

Lemma 4 ([3, p. 17]). For a representation $\rho \in P(G)$ and a decomposition $\mathbb{C}^{d_\rho} = \bigoplus_{i=1}^{k} V_i^{\oplus \alpha_i}$ with $\{\alpha_i\}_{1 \leq i \leq k} \subseteq \mathbb{N}_{\geq 1}$ into invariant subspaces $\{V_i \subseteq \mathbb{C}^{d_\rho}\}_{1 \leq i \leq k}$ with irreducible representations respectively, we have

$$|G| = \sum_{i=1}^{k} \dim(V_i)^2. \tag{2}$$

Note that $\alpha_1, ..., \alpha_k$ not playing a role in the formula is not a contradiction[2], as they mostly stem from possibly too large of a dimension d_ρ.

Definition 3 ([2, p. 27])**.** Let G be a finite group, $f \colon G \to \mathbb{C}$ a function and $\rho \colon G \to \mathrm{GL}(\mathbb{C}^{d_\rho})$ with $d_\rho \in \mathbb{N}_{\geq 1}$ be an irreducible representation. Then the *Fourier transform of f wrt. ρ* (FT) is defined as

$$\hat{f}(\rho) \coloneqq \sqrt{\frac{d_\rho}{|G|}} \sum_{g \in G} f(g)\rho(g). \tag{3}$$

This is the definition of the general Fourier transform presented in the literature. In these notes we will not get deep into the intuition behind this definition besides a clear generalization wrt. the function values of characteristics as factors from the quantum fourier transform for finite Abelian groups [2, p. 20].

To finish this section, we will go over how the general FT can be expressed as a unitary matrix, reproducing [2, pp. 27-28]. We fix an ordering $G = \{g_1, ..., g_{|G|}\}$ and vectorize the function f by identifying

$$v_f \coloneqq (f(g_1), ..., f(g_{|G|})) \in \mathbb{C}^{|G|}. \tag{4}$$

Take a complete set of irreducible representations and order it to $\hat{P}'(G) \coloneqq \{\rho_1, ..., \rho_k\}$. Choose for each representation a basis, s.t. $\hat{f}(\rho_i)$, $1 \leq i \leq k$, is unitary. For that, we refer to [2, p. 28]. We set

$$v_{\hat{f}} \coloneqq (\hat{f}(\rho_1)_{11}, \hat{f}(\rho_1)_{12}, ..., \hat{f}(\rho_m)_{d_{\rho_m} d_{\rho_m}}) \in \mathbb{C}^{|G|} \tag{5}$$

due to Lemma 4. We further observe $v_f = \sum_{g \in G} f(g) \left|g\right\rangle$. The transform then boilds down to the mapping $v_f \mapsto v_{\hat{f}}$, which leads to the following definition. Note, that we denote with $\left|\rho, i, j\right\rangle \in S(\mathbb{C}^{|G|})$ the canonical state describing the position $(i, j) \in [1, d_\rho]^2_{\mathbb{N}}$ wrt. some representation $\rho \in P'(G)$.

Definition 4. For a finite group G, the *General Quantum Fourier Transform* (QFT) is defined as

$$\mathrm{QFT}_G \coloneqq \sum_{g \in G} \sum_{\rho \in P'(G)} \sum_{1 \leq i,j \leq d_\rho} \sqrt{\frac{d_\rho}{|G|}} \rho(g)_{ij} \left|\rho, i, j\right\rangle\!\left\langle g\right| . \tag{6}$$

Lemma 5 ([2, pp. 27-28]). The map QFT_G for any finite group G, if constructed as above, is a linear and unitary map.

The citation for Lemma 5 is incomplete as it lacks the actual proof, but it gives the hint to look into [3].
DONE

[2] At least by intuition for the way it is written down in these notes here.

3 The Generalized Finite Abelian HSP Algorithm

We now discuss the generalization of the quantum algorithm for solving finite Abelian HSPs. The procedure is also called *Quantum Fourier Sampling* (QFS) in literature. We present the algorithm as a schema, since in contrast to the aforementioned algorithm and the more general structure of non-Abelian groups we need to leave out some steps. We further assume access to some Hadamard matrix $H_G \in U(|G|)$ with the action $|g_1\rangle \mapsto 1/\sqrt{|G|} \sum_{g \in G} |g\rangle$, if $g_1 \in G$ is the neutral element.

Algorithm 1 Quantum Fourier Sampling Schema

Require: A finite group G in some order $G = \{g_1, ..., g_{|G|}\}$, with g_1 being the neutral element, with an $\mathcal{O}(\log_2(|G|))$-complex representation in a $\mathbb{C}^{|G|}$-based quantum register, a complete set of irreducible representations $P'(G)$; omitting isomorphy; a function $f\colon G \to X$ hiding a subgroup $H \leq G$ as described in Section 1 with $X \coloneqq \{0,1\}^x$, $x \in \mathbb{N}_{\geq 1}$ and an oracle $U_f \in \mathbb{C}^{|G||X| \times |G||X|}$ with $|g\rangle |h\rangle \mapsto |g\rangle |h \oplus f(g)\rangle$ for all $g \in G, h \in X$.

Ensure: A generator $\Gamma \subseteq G$ for H.

1: $|\Phi\rangle \coloneqq (H_G \otimes E_{|X|}) |g_1\rangle |0\rangle \in S(\mathbb{C}^{|G||X|})$
2: $|\Phi\rangle \leftarrow U_f |\Phi\rangle$
3: Measure $|\Phi\rangle$ wrt. the observable $\{\mathrm{Span}(\{|g\rangle |x\rangle \mid g \in G\}) \mid x \in X\}$ and observe an index $x \in X$.
4: Drop the second register of $|\Phi\rangle =: |\Psi\rangle |x\rangle$ to obtain $|\Psi\rangle \in S(\mathbb{C}^{|G|})$.
5: $|\Psi\rangle \leftarrow \mathrm{QFT}_G |\Psi\rangle$
6: Measure $|\Psi\rangle$ wrt. the observable $\{\mathrm{Span}(\{|\rho, i, j\rangle \mid 1 \leq i, j \leq d_\rho\}) \mid \rho \in P'(G)\}$ and observe a part of a representation $\rho \in P'(G)$.
7: Collect some m representation parts $\{\rho'_i\}_{1 \leq i \leq m}$ and construct a generator $\Gamma \subseteq H$ for H using them.
8: **return** Γ

We quickly compute the result of Algorithm 1. Steps 1 and 2 give the state

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle = \sqrt{\frac{|H|}{|G|}} \sum_{c \in T} \frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch\rangle |f(c)\rangle , \tag{7}$$

where $T \subseteq G$ is some transversal wrt. H, i.e. a set of representatives for the sets from the factor group G/H. Measuring the second register and dropping it gives

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch\rangle \tag{8}$$

for some $c \in T$. Applying QFT_G then gives the state

$$\sum_{\rho \in P'(G)} \sum_{1 \leq i,j \leq d_\rho} \sqrt{\frac{d_\rho}{|G||H|}} \left(\sum_{h \in H} \rho(ch) \right)_{ij} |\rho, i, j\rangle . \tag{9}$$

Performing the measurement in step 6 then corresponds to measuring a part of a representation, as claimed.

The construction of QFT_G and the construction of a generator of H from the representation parts are what Lomont presents as some of the main theoretical issues with the description and complexity of this algorithm [2, pp. 29-30]:

(1) The QFT must be efficiently implemented, which depends on multiple aspects. A complete set of representations must be explicitely given, and that depends on the group. There are a lot of results on existing groups, such as cyclic, symmetric, dihedral groups and others [2, p. 29] [4, pp. 3-4]. Furthermore, the bases making the matrices of the irreducible representations in the complete set unitary can impact the efficiency of the implementation, as the example for symmetric groups demonstrates [2, pp. 29-30].
(2) We obtain representation parts, from which we need to compute a generator for the hidden subgroup. This is generally difficult, as the dihedral group demonstrates. A small introduction to the characterization of subgroups of the dihedral group and some intuition on the hardness is given by one of the papers leading to the best known algorithm for the dihedral HSP in [5], with the former on pp. 1-2.

4 An Information-Theoretical Solution to the Finite HSP

Despite the issues of Algorithm 1, a different quantum algorithm has been found, which proves, that it is information-theoretically possible to determine a hidden subgroup using a large quantum register with a possibly exponential algorithm. Algorithm 2 is due to [6, pp. 2-3]. Wrt. the setting for the HSP algorithm as in the input of Algorithm 1, denote with $U_{f,m}$ the modified oracle

$$U_{f,m} \in \mathbb{C}^{|G|^m|X|^m \times |G|^m|X|^m}, |g'_1, ..., g'_m\rangle |x_1, ..., x_m\rangle \mapsto |g'_1, ..., g'_m\rangle |x_1 \oplus f(g_1), ..., x_m \oplus f(g'_m)\rangle . \tag{10}$$

Also denote for any $G' \subseteq G$ the state $|G'\rangle \coloneqq 1/\sqrt{|G'|} \sum_{g' \in G'} |g'\rangle$ and for some $K \leq G$ and $\{b_i\}_{1 \leq i \leq m} \subseteq G$ the ket $|\Psi_K^{\{b_i\}_{1 \leq i \leq m}}\rangle \coloneqq \bigotimes_{i=1}^m |b_i K\rangle$.

Algorithm 2 Information Theoretical HSP Solver

Require: A finite group G in some order $G = \{g_1, ..., g_{|G|}\}$, with g_1 being the neutral element, with an $\mathcal{O}(\log_2(|G|))$-complex representation in a $\mathbb{C}^{|G|}$-based quantum register, a function $f\colon G \to X$ hiding a subgroup $H \leq G$ as described in Section 1 with $X \coloneqq \{0,1\}^x$, $x \in \mathbb{N}_{\geq 1}$ and an oracle $U_f \in \mathbb{C}^{|G||X| \times |G||X|}$ with $|g\rangle |h\rangle \mapsto |g\rangle |h \oplus f(g)\rangle$ for all $g \in G, h \in X$.

Ensure: A generator $\Gamma \subseteq G$ for H.

1: Set $m \coloneqq 4 \log_2(|G|) + 2$.
2: $|\Phi\rangle \coloneqq |g_1\rangle^{\otimes m} |0\rangle^{\otimes m} \in S(\mathbb{C}^{|G|^m|X|^m})$
3: $|\Phi\rangle \leftarrow (H_{|G|}^{\otimes m} \otimes E_{|X|}^{\otimes m}) |\Phi\rangle$
4: $|\Phi\rangle \leftarrow U_{f,m} |\Phi\rangle$
5: Measure $|\Phi\rangle$ wrt. the observable $\{\mathrm{Span}(\{|g'_1, ..., g'_m\rangle |x_1, ..., x_m\rangle \mid g'_1, ..., g'_m \in G\}) \mid x_1, ..., x_m \in X\}$ and observe an index $X' \in X^m$.
6: Drop the second register of $|\Phi\rangle =: |\Psi\rangle |X'\rangle$ to obtain $|\Psi\rangle \in S(\mathbb{C}^{|G|^m})$.
7: $\Gamma \coloneqq \emptyset$
8: **for** $i \in \{1, ..., |G|\}$ **do**
9: Let $\mathcal{H}_{\langle g_i \rangle} \coloneqq \mathrm{Span}(\{ |\Psi_{\langle g_i \rangle}^{\{b_j\}_{1 \leq j \leq m}}\rangle \mid \{b_j\}_{1 \leq j \leq m} \subseteq G\})$.
10: Measure $|\Psi\rangle$ wrt. the observable $\{\mathcal{H}_{\langle g_i \rangle}, \mathcal{H}_{\langle g_i \rangle}^\perp\}$ and obtain an index $z \in \{0,1\}$ in this order.
11: **if** $z = 0$ **then**
12: $\Gamma \leftarrow \Gamma \cup \{g_i\}$
13: **return** Γ

We quickly analyze this algorithm. The steps 1 to 6 give a state

$$\bigotimes_{i=1}^m |a_i H\rangle \tag{11}$$

for some $a_1, ..., a_m \in G$. Let $P_{\langle g_i \rangle}$ be the canonical projector onto $\mathcal{H}_{\langle g_i \rangle}$ for any $i \in [1, m]_\mathbb{N}$ and analogously $P_{\langle g_i \rangle}^\perp$ be the canonical projector onto $\mathcal{H}_{\langle g_i \rangle}^\perp$. We look at the measurement in step 10. Defining $|\Psi_0\rangle \coloneqq |\Psi\rangle$ for the state in step 6, we can set unnormalized states

$$|\Psi_i\rangle \coloneqq \begin{cases} P_{\langle g_i \rangle} |\Psi_{i-1}\rangle & g_i \in H \\ P_{\langle g_i \rangle}^\perp |\Psi_{i-1}\rangle & g_i \neq H \end{cases} \tag{12}$$

for any $i \in [1, |G|]_\mathbb{N}$. We then have the following Lemma.

Lemma 6 ([6, pp. 3-4]). For any $i \in [1, |G|]_\mathbb{N}$, it holds, that

$$\langle \Psi_i | \Psi_i \rangle \geq 1 - \frac{2i}{2^{m/2}} \geq 1 - \frac{1}{|G|}. \tag{13}$$

We can summarize the result as a Theorem.

Theorem 7. Algorithm 2 solves the problem of determining a generator for an arbitrary FHSP using $\mathcal{O}(|G|)$ measurements and $\mathcal{O}(\log_2(|G|))$ oracle calls with a probability of at least $1 - 1/|G|$.

Whilst the algorithm uses a subexponential number of oracle calls, the number of measurement it requires lies between 1 and $|G|$ with the minimal example being any cyclic group and the maximal example requiring a group, s.t., e.g., every generator has $O(|G|)$ elements. It could be improved by using characterizations of generators of the group to systematically cross out group elements from the testing loop from step 8 to step 12, as suggested in [6, p. 3].

5 Some Further Notes

We further list some more intruiging results on these problems.

• Besides the reduction of the SVP to the DHSP, there is also a reduction of the graph isomorphism to the symmetric HSP, see [2, pp. 61-64].

• Gogioso and Kissinger [7] have modelled the quantum algorithm for Finite Abelian HSPs using abstract diagrams and proved the correctness. Figure (5.2) in [7, p. 12] illustrates the main proof diagram. Some notes on infinite HSPs, which may get attacked in the future by quantum computers under employment of quantum states modelled using infinite-dimensional Hilbert spaces such as $\mathcal{L}_2(\mathbb{R})$, can also be found [7, p. 19].

References

[1] Fischer, G., *Lehrbuch der Algebra*, ISBN: 978-3-658-19365-2.

[2] Lomont, C., "The Hidden Subgroup Problem - Review and Open Problems." DOI: 10.48550/arXiv.quant-ph/0411037.

[3] Fulton, W. and Harris, J., *Representation Theory*, ISBN: 978-0-387-97495-8.

[4] Chen, I. and Sun, D., "The dihedral hidden subgroup problem." DOI: 10.48550/arXiv.2106.09907.

[5] Kuperberg, G., "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem." DOI: 10.48550/arXiv.quant-ph/0302112.

[6] Ettinger, M. and Hoyer, P. and Knill, E., "Hidden Subgroup States are Almost Orthogonal." DOI: 10.48550/arXiv.quant-ph/9901034.

[7] Gogioso, S. and Kissinger, A., "Fully graphical treatment of the quantum algorithm for the Hidden Subgroup Problem," DOI: 10.48550/ARXIV.1701.08669.