

Notes on the Finite Abelian HSP Algorithm

1 Introduction We quickly introduce the necessary notions, facts and the quantum algorithm, with appropriate citations. Recall the finite Abelian Hidden Subgroup Problem (HSP): Given a finite Abelian group $(G, +)$, a subgroup $H \leq G$ and some $f: G \rightarrow X$ with X an appropriate set, s.t. $f|_{gH}$ is constant and $f|_{gH} = f|_{hH} \rightarrow g = h$ for all $g, h \in G$. Our goal is to find a generator $\Gamma \subseteq H$ for H using a quantum algorithm¹.

- (i) Since the left cosets of H induce a partition of G [2, pp. 36-37], choosing X , s.t. $|X| \geq |G/H| = |G|/|H|$ [2, p. 38], e.g. via $X := \{0, 1\}^x$ for some $x \in \mathbb{N}_{\geq 1}$, $x \geq \lceil \log_2(|G/H|) \rceil$ suffices.
- (ii) How do we store group elements in G in a quantum register? We can do that using qudits, because $G \cong \bigoplus_{j=1}^k \mathbb{Z}_{N_j}$ with $k \in \mathbb{N}_{\geq 1}$ and $\{N_1, \dots, N_k\} \subseteq \mathbb{N}_{\geq 2}$ [2, pp. 132-135], where we take the direct sum of the groups, i.e. the elements of G can be taken to be tuples $G \ni g = (g_1, \dots, g_k) \in \prod_{j=1}^k \mathbb{Z}_{N_j}$ [2, pp. 53-54]. Note that we also call N_1, \dots, N_k *elementary divisors*. We take such a decomposition and appropriate qudits as given here².

To formulate the quantum algorithm, an analogon for the \mathbb{Z}_N Quantum Fourier Transform for G must be defined. This is done via characteristics.

2 Characteristics

Definition 1 ([1, p. 17]). A *characteristic* over G is a group homomorphism $(G, +) \rightarrow (\mathbb{C}^* := \mathbb{C} \setminus \{0\}, \cdot)$.

Lemma 1 ([1, p. 18]). The following statements are true.

- (i) The set of characteristics of G , $\chi(G) := \{\chi: G \rightarrow \mathbb{C}^* \mid \chi \text{ is a characteristic over } G\}$, equipped with the composition of maps, is a group.
- (ii) The map $G \hookrightarrow \chi(G), g \mapsto \chi_g$ is a group isomorphism, where we call $\chi_g: G \rightarrow \mathbb{C}^*, h \mapsto \prod_{j=1}^k \omega_{N_j}^{g_j h_j}$ the *characteristic induced by g* .

3 Orthogonal Subgroups

Definition 2 ([1, p. 18]). For $H \subseteq G$ a subgroup of a group G , we define its *orthogonal subgroup* as

$$(3.1) \quad H^\perp := \{g \in G \mid \chi_g(H) = \{1\}\}$$

Lemma 2 ([1, pp. 19-20]). The following statements hold.

- (i) $H^\perp \leq G$
- (ii) $H^\perp \cong G/H$
- (iii) $H^{\perp\perp} = H$

Note that we included statement (i) here to justify the name in the definition.

4 General Fourier Transform

Definition 3 ([1, p. 20]). We define the *Quantum Fourier Transform of the Group G* as

$$(4.1) \quad \text{QFT}_G := \frac{1}{|G|} \sum_{g, h \in G} \chi_g(h) |g\rangle\langle h| \in \mathbb{C}^{|G| \times |G|}$$

For $G = \mathbb{Z}_N$, $N \in \mathbb{N}_{\geq 1}$, we thus have $|G| = N$ and $\chi_g(h) = e^{i2\pi \frac{gh}{N}}$ for any $g, h \in G$, meaning that this corresponds to the Quantum Fourier Transform QFT_N . We further set $|H'\rangle := \frac{1}{|H'|} \sum_{h \in H'} |h\rangle$ for any subgroup $H' \leq G$. Also, we have $\text{QFT}_G |0\rangle = |G|^{-1/2} \sum_{g \in G} |g\rangle$ by definition.

Lemma 3 ([1, pp. 19-21, p. 23]). The following statements are true.

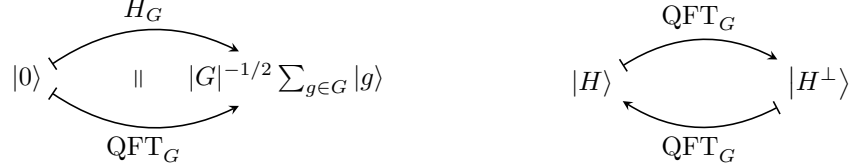
- (i) QFT_G is unitary.

¹Classically, this problem is difficult, as the prime factorization problem shows [1, p. 24].

²Finding such a decomposition is difficult, although a quantum algorithm exists [1, p. 17].

- (ii) We have $\text{QFT}_G = \bigotimes_{j=1}^k \text{QFT}_{\mathbb{Z}_{N_j}} = \bigotimes_{j=1}^k \text{QFT}_{N_j}$ for a finite Abelian group G as in Section 1, (ii).
- (iii) $\text{QFT}_G |H\rangle = |H^\perp\rangle$

Note that in Lemma 3 (ii), each quantum fourier transform acts on a single qudit. If we only allow prime qudits, we may use the decomposition of G into cyclic groups of prime power order [2, p. 136]. Statement (iii) of Lemma 3 compactly describes the action of the general fourier group on a subgroup: It flips the group into its orthogonal complement. Applying QFT_G then again gives $|H\rangle$ by Lemma 2 (iii).



In the figure, H_G denotes the Hadamard operator for G , which may be defined by the natural generalization $|h\rangle \mapsto |G|^{-1/2} \sum_{g \in G} \prod_{j=1}^k (-1)^{g_j h_j} |g\rangle$ for any $h \in G$. There is one more additional property that is useful.

Lemma 4 ([1, p. 20-21]). Setting for any $t \in G$

$$(4.2) \quad \tau_t := \sum_{g \in G} |t+g\rangle\langle g| \text{ and } \phi_t := \sum_{g \in G} \chi_g(t) |g\rangle\langle g|$$

to be its associated translation and phase shifting operators, we have the commutation

$$(4.3) \quad \text{QFT}_G \tau_t = \phi_t \text{QFT}_G$$

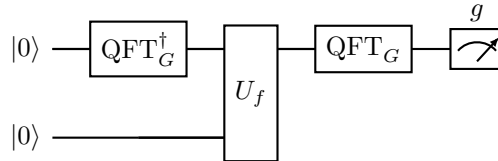
5 The Quantum Algorithm We now present the full quantum algorithm along with an analysis. The following is due to [1, pp. 22-23].

Algorithm 1 QUANTUM ALGORITHM FOR SOLVING THE FINITE ABELIAN HSP

Given: A finite Abelian group in its cyclic decomposition $G = \bigoplus_{j=1}^k \mathbb{Z}_{N_j}$ with $\{N_1, \dots, N_k\} \subseteq \mathbb{N}_{\geq 2}$, $k \in \mathbb{N}_{\geq 1}$, a function $f: G \rightarrow X$ hiding a subgroup $H \leq G$ as described in Section 1 with $X := \{0, 1\}^x$, $x \in \mathbb{N}_{\geq 1}$, $x \geq \lceil \log_2(|G|/|H|) \rceil$, a qudit register $|\Phi\rangle := |0\rangle |0\rangle \in S(\bigotimes_{j=1}^k \mathbb{C}^{N_j} \otimes \mathbb{C}^{|X|})$ 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 $g \in G, h \in X$.

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

- 1: $|\Phi\rangle \leftarrow (\text{QFT}_G^\dagger \otimes E_{|X|}) |\Phi\rangle$
 - 2: $|\Phi\rangle \leftarrow U_f |\Phi\rangle$
 - 3: $|\Phi\rangle \leftarrow (\text{QFT}_G \otimes E_{|X|}) |\Phi\rangle$
 - 4: Measure $|\Phi\rangle$ wrt. the observable $\{\text{Span}(\{|g\rangle |h\rangle \mid h \in X\} \mid g \in G)\}$ and obtain an index element $g \in G$.
 - 5: Collect $1 + \log_2(|G|) =: t_1$ elements $g^1, \dots, g^{t_1} \in G$ by repeating steps 1 to 4.
 - 6: Form the equation system $Ah := (\alpha_j g_j^i)_{\substack{1 \leq i \leq t_1 \\ 1 \leq j \leq k}} (h_j)_{1 \leq j \leq k} = 0$ with $h \in G$ and $\alpha_j := d/N_j$ for any $j \in \{1, \dots, k\}$, where $d := \text{lcm}(\{N_1, \dots, N_k\})$. Compute the SNF $D \in \mathbb{Z}_d^{t_1 \times k}$ of A , and associated unimodular matrices $U \in \mathbb{Z}_d^{t_1 \times t_1}$ and $V \in \mathbb{Z}_d^{k \times k}$.
 - 7: Sample $1 + \log_2(|G|) =: t_2$ random solutions h^1, \dots, h^{t_2} to the equation system $Dh' \equiv 0 \pmod{d}$ for $h' \in G$.
 - 8: **return** $\{Vh^1, \dots, Vh^{t_2}\}$
-



Note that we used the notation $S(\mathbb{C}^n) := \{x \in \mathbb{C}^n \mid \|x\| = 1\}$ for any $n \in \mathbb{N}$.

Algorithm Analysis of the Quantum Part Let $T \subseteq G$ be a transversal wrt. G/H , i.e. a set of representatives of the induced partition. Applying the first steps yields

$$(5.1) \quad |0\rangle |0\rangle \xrightarrow{\text{QFT}_G^\dagger \otimes E_{|X|}} \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |0\rangle$$

$$(5.2) \quad \xrightarrow{U_f} \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle = \frac{1}{\sqrt{|T|}} \sum_{t \in T} |t + H\rangle |f(t)\rangle = \frac{1}{\sqrt{|T|}} \sum_{t \in T} \tau_t |H\rangle |f(t)\rangle$$

$$(5.3) \quad \xrightarrow{\text{QFT}_G \otimes E_{|X|}} \frac{1}{\sqrt{|T|}} \sum_{t \in T} \text{QFT}_G \tau_t |H\rangle |f(t)\rangle \stackrel{(1)}{=} \frac{1}{\sqrt{|H^\perp|}} \sum_{t \in T} \phi_t |H^\perp\rangle |f(t)\rangle$$

(1) Use the commutation relation from Lemma 4, apply Lemma 3 (iii) and then use the fact that $|T| = |G/H| = |H^\perp|$ by Lemma 2 (ii).

Note the phase shifting operator ϕ_t for any $t \in T$ in the resulting state does not influence measurements, so we have successfully, using the general QFT and the oracle, stored a uniform superposition of the elements in $|H^\perp\rangle$ in the first register. This suggests that we may repeatedly measure on this register to obtain random elements from H^\perp . We will apply the following lemma on random generators.

Lemma 5 ([1, pp. 76-77]). Let G be a finite group and $t \in \mathbb{N}$. Then for $t + \lceil \log_2(|G|) \rceil$ uniformly randomly chosen elements $g_1, \dots, g_{t + \lceil \log_2(|G|) \rceil} \in G$, we have

$$(5.4) \quad \Pr(\langle g_1, \dots, g_{t + \lceil \log_2(|G|) \rceil} \rangle = G) \geq 1 - \frac{1}{2^t}$$

Better results for this exist [1, p. 77], but this lemma suffices. However, it is still not clear how to obtain a generator for H .

Obtaining a Generator Assume for now that we have obtained elements $g^1, \dots, g^\ell \in G$ with some $\ell \in \mathbb{N}_{\geq 1}$, s.t. $\langle g^1, \dots, g^\ell \rangle = H^\perp$. Since $H = H^{\perp\perp}$, we have by definition for any $h \in G$, that $h \in H$, iff $\chi_h(g^j) = 1$ for any $j \in \{1, \dots, \ell\}$, as annihilating a generator suffices for the definition of being in the orthogonal complement. We first reformulate the solution condition via the orthogonal complement in terms of a linear system by norming the complex roots we consider. Let $d := \text{lcm}(\{N_1, \dots, N_k\})$ be the least common multiple of the elementary divisors of G . Fix for now some $j' \in \{1, \dots, \ell\}$. Let $\alpha_{j'} := d/N_{j'}$. Then $\omega_{N_j} = e^{i2\pi/N_j} = \omega_d^{\alpha_{j'}}$. Furthermore, $\chi_h(g^{j'}) = \prod_{j=1}^k \omega_d^{\alpha_{j'} h_j g_j^{j'}} = 1$, iff $\sum_{j=1}^k \alpha_{j'} h_j g_j^{j'} \equiv 0 \pmod{d}$. Letting j' be loose now, giving the system of congruences

$$(5.5) \quad \begin{aligned} \sum_{j=1}^k \alpha_j g_j^1 h_j &\equiv 0 \pmod{d} \\ \sum_{j=1}^k \alpha_j g_j^2 h_j &\equiv 0 \pmod{d} \\ &\vdots \\ \sum_{j=1}^k \alpha_j g_j^\ell h_j &\equiv 0 \pmod{d} \end{aligned}$$

or in matrix notation $(\alpha_j g_j^i)_{\substack{1 \leq i \leq \ell \\ 1 \leq j \leq k}} (h_j)_{1 \leq j \leq k} = 0 =: Ah$ over \mathbb{Z}_d , where we now interpret h as a column vector. If we are able to obtain enough solutions to this system of congruences, we can generate H with high probability. The necessary solution technique is the *Smith Normal Form*. Let R be a principal ideal ring and $m, n, d \in \mathbb{N}_{\geq 1}$ for the following few definitions and theorems.

Definition 4 ([3, p. 267]). We define the following notions.

(i) An invertible square matrix $A \in R^{n \times n}$, $n \in \mathbb{N}_{\geq 1}$, is called *unimodular*.

(ii) Let $A \in R^{m \times n}$ be some matrix, $r := \text{rk}(A)$ in the associated R -module and let $U \in R^{m \times m}$, $V \in R^{n \times n}$ be unimodular. A matrix $D \in R^{m \times n}$, s.t.

$$(5.6) \quad D = UAV = \begin{pmatrix} s_1 & & & & & \\ & \ddots & & & & \\ & & s_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

where the omitted entries in either width or height, depending on $m \leq n$ or $m > n$, are zero and $s_i | s_{i+1}$ for any $i \in \{1, \dots, r-1\}$, is called the *Smith Normal Form* (SNF) of A .

Theorem 6 ([4, pp. 1073-1074]). Any matrix $A \in \mathbb{Z}^{m \times n}$ admits to a SNF, which can be computed in time $\tilde{O}(m^3 n \log_2(m))$, additionally obtaining the similarity matrices.

With \tilde{O} , we denote a looser version of the O -notation, in this case omitting a few logarithmic factors. This is not the best possible result, see e.g. [3, pp. 273-274], but it is one of the simpler algorithms recovering the unimodular similarity matrices as well in the general, thus possibly singular, case.

Remark 7. In [1, p. 23], it is stated that [3] gives algorithms for computing both the SNF of a matrix over \mathbb{Z} , as well as the equivalence matrices, but the latter is contradicted in [3, p. 268].

Let $t_1, t_2 \in \mathbb{N}_{\geq 1}$ be loose. We first obtain $t_1 + \log_2(|G|)$ elements generating H^\perp with probability $\geq 1 - 1/2^{t_1}$. After computing the SNF $D = UAV$, we have $U^{-1}DV^{-1} = A$, where we interpret first A over \mathbb{Z}_d and then \mathbb{Z} , assuming $d \in O(1)$ in our runtime considerations. Afterwards, we interpret all matrices over \mathbb{Z}_d again. We obtain a uniformly random solution to the diagonal inversion problem $Dh' \equiv 0 \pmod{d}$ and set $h := Vh'$, yielding $Ah = U^{-1}DV^{-1}Vh' = 0$. Thus, we may obtain $t_2 + \log_2(|G|)$ elements of H this way, which form a generator with probability $\geq 1 - 1/2^{t_2}$. In total, we obtain a generator of H with probability $\geq (1 - 1/2^{t_1})(1 - 1/2^{t_2})$. Letting $t_1 = t_2 = 1$, this is $\geq 1/4$, which means that we may execute the algorithm four times in expectation.

Runtime Analysis We apply $2k \in O(\log_2(N))$ QFT gates and use an oracle call in the first three steps of the algorithm. Note that we assume efficient implementations for the qudit unitaries $\text{QFT}_{N_1}, \dots, \text{QFT}_{N_k}$, as these operations are local. The main cost thus stems from the computation of the SNF. Since $t_1 \in O(\log_2(|G|))$, we require a runtime of $\tilde{O}(\log_2^3(|G|) \log_2^{(2)}(|G|))$, where $\log_2^{(2)} := \log_2 \circ \log_2$.

Theorem 8. Algorithm 1 solves the HSP for a finite Abelian group with probability $\geq 1/4$ in time $\tilde{O}(\log_2^3(|G|) \log_2^{(2)}(|G|))$.

References

- [1] Lomont, Chris, “The Hidden Subgroup Problem - Review and Open Problems,” DOI: <https://doi.org/10.48550/arXiv.quant-ph/0411037>.
- [2] Fischer, Gerd, *Lehrbuch der Algebra*, ISBN: 978-3-658-19365-2.
- [3] Storjohann, Arne, “Near optimal algorithms for computing Smith normal forms of integer matrices,” DOI: 10.1145/236869.237084.
- [4] L. Hafner, James and S. McCurley, Kevin, “Asymptotically Fast Triangularization of Matrices over Rings,” DOI: 10.1137/0220067.