Quantum algorithms for finding the structure of abelian and solvable groups

QIC710 Presentation

Abhibhav Garg

2021

Overview

The hidden subgroup problem for abelian groups

Finite abelian Groups

Decomposing finite abelian groups

Solvable groups

Order of solvable groups

The hidden subgroup problem for abelian groups

Problem statement

Function $f : G \to S$ hides subgroup H if

$$f(x) = f(y) \iff x - y \in H.$$

Problem statement

Function $f : G \to S$ hides subgroup H if

$$f(x) = f(y) \iff x - y \in H.$$

Given a black box for f, can you find H.

Problem statement

Function $f : G \to S$ hides subgroup H if

$$f(x) = f(y) \iff x - y \in H.$$

Given a black box for f, can you find H.

Generalises the Simon mod m problem.

Problem statement

Function $f : G \to S$ hides subgroup H if

$$f(x) = f(y) \iff x - y \in H.$$

Given a black box for f, can you find H.

Generalises the Simon mod m problem. $G = (\mathbb{Z}/m\mathbb{Z})^d$, and $H = r\mathbb{Z}$.

General solution

- Start with state $|0\rangle$, and apply F_G ($F_m^{\otimes k}$).

General solution

- Start with state $|0\rangle$, and apply F_G ($F_m^{\otimes k}$).
- Query the function f on an ancilla and measure it.

General solution

- Start with state $|0\rangle$, and apply F_G ($F_m^{\otimes k}$).
- Query the function f on an ancilla and measure it.
- Apply F_G^* to get a random character trivial on H (an element in the orthogonal complement of r).

Finite abelian Groups

The structure theorem

Theorem
Any finite abelian group is isomorphic to a direct sum of cyclic group of prime power orders.

In other words, if G is finite abelian then

$$G \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{e_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{e_k}\mathbb{Z}.$$

Sylow subgroups and decomposition.

Definition
A Sylow $p-$subgroup of G is a maximal subgroup with every element having order a power or p.

Sylow subgroups and decomposition.

Definition
A Sylow $p-$subgroup of G is a maximal subgroup with every element having order a power or p.

Theorem
Any finite abelian group is isomorphic to a direct sum of its Sylow $p-$*subgroups.*

Sylow subgroups and decomposition.

Definition
A Sylow $p-$subgroup of G is a maximal subgroup with every element having order a power or p.

Theorem
Any finite abelian group is isomorphic to a direct sum of its Sylow $p-$subgroups. If $G = \oplus G_i$ with G_i a p_i-Sylow subgroup, and if H is any subgroup of G then $H = \oplus H_i$ with H_i a subgroup of G_i.

Presentation and cyclic decomposition

Theorem

Suppose $a_1, \ldots, a_k$ *generate* G. *Suppose* M *is such that* $\prod a_i^{n_i} = e$ *if and only if* $\mathbf{n} \in \mathcal{L}(\mathrm{col}(M))$. *Then we can find* $g_1, \ldots, g_l$ *such that*

$$G \cong g_1\mathbb{Z} \oplus g_2\mathbb{Z} \oplus \cdots \oplus g_l\mathbb{Z}.$$

Decomposing finite abelian groups

Theorem Statement

Theorem ([1])
Given a finite abelian group G, we can find the decomposition of G in polynomial time.

Assumptions on G

- Unique encoding.

Assumptions on G

- Unique encoding.
- Efficiently find a generating set for G.

Assumptions on G

- Unique encoding.
- Efficiently find a generating set for G.
- Orders of generators are prime powers.

Assumptions on G

- Unique encoding.
- Efficiently find a generating set for G.
- Orders of generators are prime powers.
- Given $a \in G$ we can compute $U_a : |g\rangle \to |ag\rangle$.

Assumptions on G

- To find a generating set, just sample $\mathcal{O}(\log |G|)$ elements randomly. Each element picked doubles the size of the subgroup.

Assumptions on G

- To find a generating set, just sample $\mathcal{O}(\log|G|)$ elements randomly. Each element picked doubles the size of the subgroup.
- If $g^{pq} = e$ with $(p, q) = 1$ then g^p, g^q have order q, p and $g = (g^p)^r (g^q)^s$.

Reducing to Sylow subgroups

- We have $G = \oplus G_i$ where G_i is the p_i-Sylow subgroup.

Reducing to Sylow subgroups

- We have $G = \oplus G_i$ where G_i is the p_i-Sylow subgroup.
- Suppose g is a generator with order a power of p_1.

Reducing to Sylow subgroups

- We have $G = \oplus G_i$ where G_i is the p_i-Sylow subgroup.
- Suppose g is a generator with order a power of p_1.
- The subgroup $g\mathbb{Z}$ can be written as $g\mathbb{Z} = \oplus H_i$.

Reducing to Sylow subgroups

- We have $G = \oplus G_i$ where G_i is the p_i–Sylow subgroup.
- Suppose g is a generator with order a power of p_1.
- The subgroup $g\mathbb{Z}$ can be written as $g\mathbb{Z} = \oplus H_i$.
- It must be $H_i = \{e\}$ for $i > 1$.

Reducing to Sylow subgroups

- We have $G = \oplus G_i$ where G_i is the p_i-Sylow subgroup.
- Suppose g is a generator with order a power of p_1.
- The subgroup $g\mathbb{Z}$ can be written as $g\mathbb{Z} = \oplus H_i$.
- It must be $H_i = \{e\}$ for $i > 1$.
- Divide the generators into sets based on order.

Solving for Sylow subgroups

- Let q be the max order of $g_1, \ldots, g_k$.

Solving for Sylow subgroups

- Let q be the max order of $g_1, \ldots, g_k$.
- Define $\phi : (\mathbb{Z}/q\mathbb{Z})^k \to G$ sending basis $e_i \to g_i$.

Solving for Sylow subgroups

- Let q be the max order of $g_1, \ldots, g_k$.
- Define $\phi : (\mathbb{Z}/q\mathbb{Z})^k \to G$ sending basis $e_i \to g_i$.
- Find generators $y_1, \ldots, y_l$ of K the subgroup hidden by ϕ (equivalently $\ker(\phi)$).

Solving for Sylow subgroups

- Let q be the max order of $g_1, \ldots, g_k$.
- Define $\phi : (\mathbb{Z}/q\mathbb{Z})^k \to G$ sending basis $e_i \to g_i$.
- Find generators $y_1, \ldots, y_l$ of K the subgroup hidden by ϕ (equivalently $\ker(\phi)$).
- Output $\phi(y_1), \phi(y_2), \ldots, \phi(y_l)$.

Correctness

- We have $G \cong (\mathbb{Z}/q\mathbb{Z})^k / K$ by isomorphism theorem.

Correctness

- We have $G \cong (\mathbb{Z}/q\mathbb{Z})^k/K$ by isomorphism theorem.
- To find the generators, we can combine the matrix A of K and the matrix $M = kI$ and apply the theorem.

Solvable groups

Solvable groups

- Given G, define commutator $[G, G]$ to be the subgroup generated by $ghg^{-1}h^{-1}$ for all $g, h \in G$.

Solvable groups

- Given G, define commutator $[G, G]$ to be the subgroup generated by $ghg^{-1}h^{-1}$ for all $g, h \in G$.
- Set $G_0 := G$ and define $G_i = [G_{i-1}, G_{i-1}]$.

Solvable groups

- Given G, define commutator $[G, G]$ to be the subgroup generated by $ghg^{-1}h^{-1}$ for all $g, h \in G$.
- Set $G_0 := G$ and define $G_i = [G_{i-1}, G_{i-1}]$.
- G is solvable if $G_m = \{e\}$ for some m.

Solvable groups

- If G is finite, then G is solvable if there are $g_1, \ldots, g_m$ such that
$$\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_m = G$$
where H_i is generated by $g_1, \ldots, g_i$.

Solvable groups

- If G is finite, then G is solvable if there are $g_1, \ldots, g_m$ such that
$$\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_m = G$$
where H_i is generated by $g_1, \ldots, g_i$.
- In this case H_{i+1}/H_i is cyclic.

Solvable groups

- If G is finite, then G is solvable if there are $g_1, \dots, g_m$ such that
$$\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_m = G$$
where H_i is generated by $g_1, \dots, g_i$.
- In this case H_{i+1}/H_i is cyclic.
- Given generators for G, we can find such $g_1, \dots, g_m$ classically, although it might be $H_{i+1} = H_i$.

Solvable groups

- If G is finite, then G is solvable if there are $g_1, \ldots, g_m$ such that
$$\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_m = G$$
where H_i is generated by $g_1, \ldots, g_i$.
- In this case H_{i+1}/H_i is cyclic.
- Given generators for G, we can find such $g_1, \ldots, g_m$ classically, although it might be $H_{i+1} = H_i$.
- We have $|G| = \prod |H_{i+1}/H_i|$.

Order of solvable groups

Order finding revisited

- We saw how to do order finding by reducing to phase estimation.

Order finding revisited

- We saw how to do order finding by reducing to phase estimation.
- Alternatively, hidden subgroup problem on $\mathbb{Z}$.

Order finding revisited

- We saw how to do order finding by reducing to phase estimation.
- Alternatively, hidden subgroup problem on $\mathbb{Z}$.
- Subgroup is generated by $r := \mathtt{ord}(a)$.

Order finding revisited

- We saw how to do order finding by reducing to phase estimation.
- Alternatively, hidden subgroup problem on $\mathbb{Z}$.
- Subgroup is generated by $r := \mathtt{ord}(a)$.
- The function f is $f(x) = a^x$.

Alternative method for order finding.

- Pick $N > r^2$.

Alternative method for order finding.

- Pick $N > r^2$.
- Do the same steps as hsp on $\mathbb{Z}/N\mathbb{Z}$ with f.

Alternative method for order finding.

- Pick $N > r^2$.
- Do the same steps as hsp on $\mathbb{Z}/N\mathbb{Z}$ with f.
- Whp, we get the closest integer to jN/r for some j.

Alternative method for order finding.

- Pick $N > r^2$.
- Do the same steps as hsp on $\mathbb{Z}/N\mathbb{Z}$ with f.
- Whp, we get the closest integer to jN/r for some j.
- Use the continued fraction based method to find r.

Theorem statement

Theorem ([2])
Given generators $g_1, \ldots, g_k$ *of a solvable group, there exists an algorithm that outputs the order of* G *with high probability. The algorithm also produces a pure state that is* ϵ *close to* $|G\rangle = \sum_{g \in G} |g\rangle$.

Some definitions and assumptions

- For any $a \in G$ and subgroup H of G, define $\mathrm{ord}_H(a)$ to be the smallest r such that $a^r \in H$.

Some definitions and assumptions

- For any $a \in G$ and subgroup H of G, define $\mathrm{ord}_H(a)$ to be the smallest r such that $a^r \in H$.
- For any subgroup H of G define $|H\rangle = |H|^{1/2} \sum_{a \in H} |a\rangle$.

Some definitions and assumptions

- For any $a \in G$ and subgroup H of G, define $\mathrm{ord}_H(a)$ to be the smallest r such that $a^r \in H$.
- For any subgroup H of G define $|H\rangle = |H|^{1/2} \sum_{a \in H} |a\rangle$.
- We assume that we have a unitary performing $U : |g\rangle|h\rangle \to |g\rangle|gh\rangle$.

Two step process for finding the order of solvable groups

- Use $|H_i\rangle$ to find $\mathrm{ord}_{H_i}(g_{i+1})$.

Two step process for finding the order of solvable groups

- Use $|H_i\rangle$ to find $\mathrm{ord}_{H_i}(g_{i+1})$.
- Use $\mathrm{ord}_{H_i}(g_{i+1})$ to construct $|H_{i+1}\rangle$.

Step 1

- Do the same steps as order finding, with second qubit set to $|H\rangle$.

Step 1

- Do the same steps as order finding, with second qubit set to $|H\rangle$.
- Pick N. Start with $|0\rangle|H\rangle$ and apply F_N to the first register to get

$$\sum_{a \in \mathbb{Z}/N\mathbb{Z}} |a\rangle|H\rangle.$$

Step 1

- Do the same steps as order finding, with second qubit set to $|H\rangle$.
- Pick N. Start with $|0\rangle|H\rangle$ and apply F_N to the first register to get
$$\sum_{a \in \mathbb{Z}/N\mathbb{Z}} |a\rangle|H\rangle.$$
- Use a multiplicity controlled gate to compute
$$\sum_{a \in \mathbb{Z}/N\mathbb{Z}} |a\rangle|g_{i+1}^{a}H\rangle.$$

Step 1

- Apply F_N^* to get

$$\sum_{a,b \in \mathbb{Z}/N\mathbb{Z}} \omega_N^{ab} |b\rangle |g_{i+1}^a H\rangle.$$

Step 1

- Apply F_N^* to get

$$\sum_{a,b \in \mathbb{Z}/N\mathbb{Z}} \omega_N^{ab} |b\rangle |g_{i+1}^a H\rangle.$$

- Measure first register, with high probability the result is an integer closest to jN/r.

Step 2

- We use k copies of $|H_i\rangle$ to construct $k-1$ copies of $|H_{i+1}\rangle = |g_{i+1}H_i\rangle$.

Step 2

- We use k copies of $|H_i\rangle$ to construct $k-1$ copies of $|H_{i+1}\rangle = |g_{i+1}H_i\rangle$.
- Using the same as before, prepare l copies of state

$$\sum_{a,b \in \mathbb{Z}/r\mathbb{Z}} \omega_r^{ab} |b\rangle |g_{i+1}^a H\rangle.$$

Step 2

- We use k copies of $|H_i\rangle$ to construct $k-1$ copies of $|H_{i+1}\rangle = |g_{i+1}H_i\rangle$.
- Using the same as before, prepare l copies of state

$$\sum_{a,b \in \mathbb{Z}/r\mathbb{Z}} \omega_r^{ab} |b\rangle |g_{i+1}^a H\rangle.$$

- Measure the first register, let $b_1, \ldots, b_l$ be the outcome and $|\psi_i\rangle$ the residual state.

Step 2

- We use k copies of $|H_i\rangle$ to construct $k-1$ copies of $|H_{i+1}\rangle = |g_{i+1}H_i\rangle$.
- Using the same as before, prepare l copies of state

$$\sum_{a,b \in \mathbb{Z}/r\mathbb{Z}} \omega_r^{ab} |b\rangle |g_{i+1}^a H\rangle.$$

- Measure the first register, let $b_1, \ldots, b_l$ be the outcome and $|\psi_i\rangle$ the residual state.
- whp, say b_1 is relatively prime to r.

Step 2

- Pick c so that $c \cong b_2 b_1^{-1} \pmod{r}$.

Step 2

- Pick c so that $c \cong b_2 b_1^{-1} \pmod{r}$.
- Apply U_G^c to the state $|\psi_2\rangle|\psi_1\rangle$ to get $|H_{i+1}\rangle|\psi_1\rangle$.

Applications

- Membership testing

Applications

- Membership testing
- Subgroup testing

Applications

- Membership testing
- Subgroup testing
- Normality testing

Applications

- Membership testing
- Subgroup testing
- Normality testing
- We can use $|gH\rangle$ instead of $|g\rangle$ and use algorithms that work on abelian groups.

References

[1] K. K. Cheung and M. Mosca. Decomposing finite abelian groups. *arXiv preprint cs/0101004*, 2001.

[2] J. Watrous. Quantum algorithms for solvable groups. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 60–67, 2001.

Proof Details

- Let $M_{g^j h}$ denote multiplication by $g^j h$.

Proof Details

- Let $M_{g^j h}$ denote multiplication by $g^j h$.
- We have

$$\begin{aligned} M_{g^j h}|\psi_1\rangle &= \sum_a \omega_r^{a b_1} |g^{j+a} H\rangle \\ &= \sum_a \omega_r^{(a-j) b_1} |g^a H\rangle \\ &= \omega_r^{-j b_1} |\psi_1\rangle. \end{aligned}$$

Proof Details

- We have

$$
\begin{aligned}
U_G^c |\psi_2\rangle|\psi_1\rangle &= \sum_a \sum_{h \in H} \omega_r^{ab_2} |g^a h\rangle M_{(g^a h)^c} |\psi_1\rangle \\
&= \sum_a \sum_{h \in H} \omega_r^{ab_2 - acb_1} |g^a h\rangle |\psi_1\rangle \\
&= \sum_a \sum_{h \in H} |g^a h\rangle |\psi_1\rangle
\end{aligned}
$$