The Hidden Subgroup Problem

Course Project for PHY 612: Quantum Information Science

Name: Alina Zainab Rizvi, Diya Batool, and Hassan Mehmood
IDs: 23100010, 23100267, 23100127

April 2023

Abstract

Let G be a finite abelian group and X be a finite set. Consider a function $f : G \to X$ that is periodic and distinct on each coset in G of a subgroup K of G. Does there exist a quantum algorithm to find this subgroup K? This is called the hidden subgroup problem, and can be regarded as a generalisation of a large class of computational problems that involve finding the period of a periodic function, such as Shor's factoring algorithm, discrete logarithms, order of a permutation, and so on. In this report, we discuss a solution to the hidden subgroup problem, and apply it to some specific instances.

1 Introduction

If one carefully analyzes some major quantum algorithms, it is discovered that their basic structure consists in finding a solution to a query pertaining to a function f from a finite set A to another finite set B. In general, the action of this function is typically described by means of a certain unitary operator U acting on a set of n quantum registers $|a_1\rangle, \ldots, |a_{n-1}\rangle, |b\rangle$ such that $U|a_1\rangle \cdots |a_n\rangle \to |a_1\rangle \cdots |a_{n-1}\rangle |b \oplus f(a_1, \ldots, a_{n-1})\rangle$, i.e. the last register stores the effect of applying the function to the preceding registers. The query one wishes to solve depends on the specific problem at hand. For instance, in the Deutsch algorithm, we wish to find the bias of a function on a bit-valued function on an n-bit string. In other problems, such as order-finding, factoring and discrete logarithms, one uses the quantum Fourier transform to estimate the eigenvalues of U, which, owing to the specific form of f, are directly related to the object one seeks, e.g. the order, factor or the discrete logarithm of a positive integer. What unites all of these seemingly disparate problems is the fact that in each case, the function f acts on the domain A in a manner that makes it possible to abstract from these specific problems to a much more general problem using tools from group theory. For instance, in the Deutsch algorithm,

the bias of the function depends on how the function acts on the subsets of $\{0, 1\}$, while in the other three problems mentioned above, the function is periodic, and what we seek is precisely its period, which, again, depends on how the function acts on different "parts" of its domain. These are all specific instances of a function being distinct and constant on the cosets of a subgroup of a group. Therefore, all these different problems – and many others, as we shall see – can be reduced to the problem of finding that subgroup. This is known as the hidden subgroup problem, which, in the case of a finite abelian group, is fully solvable in a polynomial amount of elementary quantum operations.

2 Mathematical Formulation

Before we can even precisely define the hidden subgroup problem, it is necessary to understand the relevant group-theoretic concepts that are used in the formulation of the problem. This section is devoted to that task.

2.1 Groups, subgroups, cosets, and all that

Definition 1. *(Group) A group is an ordered pair $(G, *)$, where $*$ is a binary operation on the set G. The binary operation must satisfy the following axioms:*

1. *associativity : $(a * b) * c = a * (b * c)$*
2. *there exists an element e, called identity, in G such that $a * e = e * a = a$ for all $a \in G$*
3. *there exists an inverse $a^{-1} \in G$ for each $a \in G$ such that $a^{-1} * a = a * a^{-1} = e$.*

For instance, the set of all invertible square matrices forms a group under matrix multiplication. Often the multiplication operation $*$ is understood from the context, and so we simply denote the group by G, and write $a * b$ as ab for any $a, b \in G$.

If G is a finite set, then G is called a *finite group*, and we denote by $|G|$ the number of elements in G. If the binary operation is commutative, i.e. $a * b = b * a$ for every $a, b \in G$, then the G is said to be *abelian*.

For example, the set of integers $\mathbb{Z}$ form a group under addition $(\mathbb{Z}, +)$. The associativity property holds for this group and identity element $e = 0$ and inverse $a^{-1} = -a$. Furthermore, since addition is commutative, $\mathbb{Z}$ is an abelian group. But this group is, of course, not finite. On the other hand, consider $\mathbb{Z}_6 := \{0, 1, 2, 3, 4, 5\}$, the set of integers defined by addition modulo 6. This is a finite abelian group.

The group action of a group $(G, \star)$ on set A can be defined as the map from $G \times A$ to A such that $a \star b$ for $a \in A$ and $g \in G$.

Definition 2. *(Subgroup) A subgroup H of a group G is a nonempty subset of the group G that is closed under inverses and products. That is, for $x, y \in H$, the inverse $x^{-1} \in H$ and $x * y \in H$.*

We write $H \leq G$ to denote that H is a subgroup of G. It follows from the definition above that a subgroup is itself a group. For example, the set $\{0, 1, 5\}$ is a subgroup of $\mathbb{Z}_6$.

Definition 3. *(Group homomorphism) Two groups $(G, \star)$ and $(H, \diamond)$ are homomorphic if there exists a map $\phi : G \to H$ such that $\phi(a \star b) = \phi(a) \diamond \phi(b)$ for all $a, b \in G$.*

Intuitively, two groups have the same group-theoretic structure or 'look the same' if they are homomorphic. If a homomorphism also happens to be a bijection, then it is called an *isomorphism*. Isomorphic groups are completely equivalent in the sense that one can work in any one without loss of generality. If two groups G and F are isomorphic, we write $G \cong F$.

For example, the set of real numbers $\mathbb{R}$ forms a group under addition '$+$'. Similarly, the set of nonnegative real numbers $\mathbb{R}_{\geq 0}$ is a group under ordinary multiplication '$\cdot$'. These two groups are homomorphic, the homomorphism being the exponential function e^x from $\mathbb{R}$ to $\mathbb{R}_{\geq 0}$. Indeed, it is easily seen that $e^{x+y} = e^x \cdot e^y$. Furthermore, if we restrict the additive group to nonnegative real numbers only, then the map is also a bijection, as can be confirmed by drawing a graph of e^x. Thus $(\mathbb{R}_{\geq 0}, +) \cong (\mathbb{R}_{\geq 0}, \cdot)$.

Definition 4. *(Cosets) If H is a subgroup of group G, the left coset of H in G determined by $g \in G$ is the set $gH \equiv \{gh \mid h \in H\}$. The right coset is defined similarly.*

Often whether a coset is a 'left' or 'right' coset is implied by context. In the case of abelian groups, the left coset will be equal to the left coset.

Definition 5. *(Characters) Given a group G, a character is a homomorphism from G to the group of complex numbers $\mathbb{C}$ under ordinary multiplication.*

For instance, the function $f : (\mathbb{R}, +) \to (\mathbb{C}, \cdot)$ such that $f(x) = e^{ix}$ is a homomorphism. Thus it is a character of the additive group of real numbers.

Definition 6. *(Dual group) The dual $\hat{G}$ of a group G is the set of all characters of G.*

The dual of a group is itself a group under functional multiplication, i.e. for any $\alpha, \beta \in \hat{G}$, we define $\alpha \cdot \beta$ by $(\alpha \cdot \beta)(g) = \alpha(g)\beta(g)$ for all $g \in G$.

If G is a finite abelian group, then the number of characters of G is equal to the number of elements in G. In other words, $|\hat{G}| = |G|$.

2.2 Fourier transforms over groups

Given the above definitions – particularly of characters and dual groups – we can finally define Fourier transforms.

Definition 7. *(Fourier Transform) Given the characters of group G, the Fourier transform over a group G is given by*

$$|g\rangle \mapsto \frac{1}{|G|} \sum_j \chi_j(g) \, |j\rangle$$

Now that we have defined Fourier transforms, the following theorems would help us in solving the hidden subgroup problem.

Theorem 1. *For each subgroup $H \subset G$, there is a subgroup $H^\perp \subset \hat{G}$, where $H^\perp = \{k \in \hat{G} \mid k(h) = 1 \ \forall h \in H\}$. The Fourier transform over G maps an equal superposition on H to an equal superposition over $H^\perp$:*

$$\frac{1}{|H|} \sum_{h \in H} |h\rangle \mapsto \sqrt{\frac{|H|}{|G|}} \sum_{k \in H^\perp} |k\rangle$$

Theorem 2. *The Fourier transform over G maps an equal superposition on cosets of H to an equal superposition over cosets of $H^\perp$.*

$$\frac{1}{|H|} \sum_{h \in H} |hg\rangle \mapsto \sqrt{\frac{|H|}{|G|}} \sum_{k \in H^\perp} \chi_g \, |k\rangle$$

Theorem 3. *Fourier sampling on an equal superposition on a coset of H will yield a uniformly random element $k \in H$.*

2.3 The Hidden Subgroup Problem

We are now ready to formulate the hidden subgroup problem.

Let G be a finite abelian group and X be a finite set. Suppose that there exists a function $f : G \to X$ that is distinct and constant on each coset of a subgroup H of G. Thus $f(g) = f(g')$ if and only if $g' = hg$ for some $h \in H$. Suppose that we possess a unitary operator U that performs the operation $|g\rangle|x\rangle \to |g\rangle|x \oplus f(g)\rangle$, where $g \in G$, $x \in X$ and $\oplus$ is an appropriately chosen binary operation on X. Find the subgroup H.

As we outlined in the Introduction, many textbook quantum algorithms can be regarded as specific instances of the hidden subgroup problem. For example, consider the problem of finding the period r of a periodic function $f : \mathbb{Z} \to X$, where X is any finite set. In other words, we wish to find r such that $f(z + r) = f(z)$ for all $z \in \mathbb{Z}$. Now $\mathbb{Z}$

is a group under addition '+'. Consider $H = \{0, r, 2r, \ldots\} \leq \mathbb{Z}$. It is not difficult to see that f is constant and distinct on each coset $z + H := \{z, z + r, z + 2r, \ldots\}$ of H. Thus, finding the period r is equivalent to finding the subgroup H. Fig 1 lists several other well-known problems that are specific cases of the hidden subgroup problem; in each case, the relevant groups, functions and subgroups are identified.

Name	G	X	K	Function
Deutsch	$\{0,1\}, \oplus$	$\{0,1\}$	$\{0\}$ or $\{0,1\}$	$K = \{0,1\} : \begin{cases} f(x) = 0 \\ f(x) = 1 \end{cases}$ $K = \{0\} : \begin{cases} f(x) = x \\ f(x) = 1 - x \end{cases}$
Simon	$\{0,1\}^n, \oplus$	any finite set	$\{0, s\}$ $s \in \{0,1\}^n$	$f(x \oplus s) = f(x)$
Period-finding	$\mathbf{Z}, +$	any finite set	$\{0, r, 2r, \ldots\}$ $r \in G$	$f(x + r) = f(x)$
Order-finding	$\mathbf{Z}, +$	$\{a^j\}$ $j \in Z_r$ $a^r = 1$	$\{0, r, 2r, \ldots\}$ $r \in G$	$f(x) = a^x$ $f(x + r) = f(x)$
Discrete logarithm	$\mathbf{Z}_r \times \mathbf{Z}_r$ + (mod r)	$\{a^j\}$ $j \in Z_r$ $a^r = 1$	$(\ell, -\ell s)$ $\ell, s \in \mathbf{Z}_r$	$f(x_1, x_2) = a^{kx_1 + x_2}$ $f(x_1 + \ell, x_2 - \ell s) = f(x_1, x_2)$
Order of a permutation	$\mathbf{Z}_{2^m} \times \mathbf{Z}_{2^n}$ + (mod 2^m)	$\mathbf{Z}_{2^n}$	$\{0, r, 2r, \ldots\}$ $r \in X$	$f(x, y) = \pi^x(y)$ $f(x + r, y) = f(x, y)$ π = permutation on X
Hidden linear function	$\mathbf{Z} \times \mathbf{Z}, +$	$\mathbf{Z}_N$	$(\ell, -\ell s)$ $\ell, s \in X$	$f(x_1, x_2) =$ $\pi(sx_1 + x_2 \bmod N)$ π = permutation on X
Abelian stabilizer	(H, X) H = any Abelian group	any finite set	$\{s \in H \mid$ $f(s, x) = x,$ $\forall x \in X\}$	$f(gh, x) = f(g, f(h, x))$ $f(gs, x) = f(g, x)$

Figure 1: Specific examples of the hidden subgroup problem. Credits: Nielsen and Chuang

References

[1] Nielsen, Michael A., and Isaac L. Chuang. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2022.

[2] Dummit, David Steven, and Richard M. Foote. Abstract Algebra. Danvers: John Wiley amp; Sons, 2004

[3] Umesh Vazirani. Home Page For Umesh Vazirani. Accessed April 7, 2023. https://people.eecs.berkeley.edu/ vazirani/.