# Chapter 4

# Fourier Sampling and the HSP

In this chapter we will discuss the problems that can be efficiently solved by quantum computers but cannot be solved efficiently by classical probabilistic algorithms. The main primitive is Fourier sampling, which is the process of computing the Fourier transform over a group $G$ and measuring. It will be the main step in the algorithm below. Along with providing background, this chapter will motivate the contributions of this thesis, which start in the next chapter.

## 4.1 The Hidden Subgroup Problem

**Definition 4.1 (The Hidden Subgroup Problem (HSP))** *Given a finite group $G$, and a function $f : G \to S$ that is constant and distinct on cosets of some unknown subgroup $H$ of $G$, where $S$ is any set. Find a set of generators for $H$.*

The main transformation in the algorithm for the HSP is the quantum Fourier transform, which can be efficiently computed over any abelian group. The Fourier transform

is a change of basis of $\mathbb{C}^{|G|}$ from the basis indexed by group elements $\{|g\rangle : g \in G\}$, to the basis indexed by the characters of the group $\{|\chi\rangle : \chi \in \hat{G}\}$. The group of characters is the group $\hat{G} = \{\chi : G \to \mathbb{C}^*\}$, where $|\chi\rangle = \sum_{g \in G} \chi(g)|g\rangle$. The algorithm for solving the HSP uses two known properties [47] of the Fourier transform over $G$. The first is that a state that is uniform on a subgroup $H$ is mapped to the perp subgroup $H^\perp = \{\chi : H \subseteq \ker \chi\}$. That is, we have the map

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |h\rangle \xrightarrow{F_G} \frac{1}{\sqrt{|H^\perp|}} \sum_{\chi \in H^\perp} |\chi\rangle.$$

Fourier sampling a subgroup state would give a uniform distribution over the perp group, from which we could compute $H$. The second property is that the Fourier transform of the convolution "$*$" of two vectors is the pointwise product "$\bullet$" of the Fourier transform of each vector. Strictly speaking, this is only true without the normalization factors, which we will now leave out. Consider a coset state $\sum_{h \in H} |gh\rangle$:

$$\sum_{h \in H} |gh\rangle = |g\rangle * \sum_{h \in H} |h\rangle \xrightarrow{F_G} \left( \sum_{\chi \in \hat{G}} \chi(g)|\chi\rangle \right) \bullet \left( \sum_{\chi \in H^\perp} |\chi\rangle \right) = \sum_{\chi \in H^\perp} \chi(g)|\chi\rangle.$$

Therefore, Fourier sampling treats all coset states the same, i.e. the identity of the coset does not matter. We can now describe the algorithm. In the algorithm $M_i$ denotes a measurement of the $i^{th}$ register. In particular, $M_2$ measures the value of $f(g)$, and $M_1$ measures the character name.

**Algorithm 4.1 (Abelian Hidden Subgroup Problem Algorithm)**

**Input:** *A group $G$, a function $f$ that is constant and distinct on cosets of unknown $H$.*

**Output:** *A set of generators for $H$.*

1. *Repeat $k = poly(\log |G|)$ times:*

*(a) Create a random coset state* $\sum_{h\in H}|gh\rangle$*:*

$$|0\rangle \xrightarrow{F_G} \frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle \xrightarrow{U_f} \frac{1}{\sqrt{|G|}}\sum_{g\in G}|g,f(g)\rangle \xrightarrow{M_2} \frac{1}{\sqrt{|H|}}\sum_{h\in H}|gh,f(g)\rangle$$

*(b) Fourier sample the coset state:*

$$\frac{1}{\sqrt{|H|}}\sum_{h\in H}|gh\rangle \xrightarrow{F_G} \frac{1}{\sqrt{|H^\perp|}}\sum_{\chi\in H^\perp}\chi(g)|\chi\rangle \xrightarrow{M_1} |\chi_i\rangle$$

*2. Classically compute* $H=\bigcap_{i=0}^{k-1}\ker\chi_i$

Since we are sampling from a uniform distribution on the subgroup $H^\perp$, a polynomial number of samples is enough to know $H^\perp$, and then the intersection of the kernels can be efficiently computed from the set of modular linear equations they define.

Simon [46] gave the first example of such a problem. The instance given is $G=\mathbb{Z}_2^n$, and a function satisfying the HSP, and the problem is to decide whether the hidden subgroup is trivial or has order two.

One problem that is not directly an instance of the HSP, but still uses the same properties, is the recursive Fourier sampling problem of Bernstein and Vazirani [8]. The recursive Fourier sampling problem is the only known example of a problem that is not in NP that can be efficiently solved by a quantum computer. In one level of the recursion, a function $f_s:\mathbb{Z}_2^n\to\{0,1\}$ is given such that $f_s(x)=(x,s)$ mod 2, the inner product mod 2 of $x$ and $s$. The goal is to find $s$. The quantum algorithm is to Fourier sample the state with $f$ in the phases:

$$\sum_{x\in\{0,1\}}(-1)^{f(x)}|x\rangle \xrightarrow{F_{\mathbb{Z}_2^n}} |s\rangle.$$

Notice that this step can be viewed as the HSP algorithm in reverse, where $|s\rangle$ is the coset state and the subgroup is trivial.

## 4.2 The General HSP

In the General HSP, less information is given. The input in this case is a function $f : \mathbb{Z}^k \to S$ and integers $q_1, \ldots q_k$. The guarantee is that the hidden subgroup is contained in a finite size group contained in $\mathbb{Z}^k$, and that the values $q_i$ are estimates of the size of the group in each component. We cannot immediately apply the HSP algorithm in this case since we do not know the group.

This variant arises in Shor's algorithm for factoring. In the algorithm, the idea is to reduce factoring to the HSP over a cyclic group, but in this case the group size is necessarily unknown. Using ad hoc techniques, he showed that it is possible to Fourier sample over a group of a different size and still reconstruct the subgroup. We will now outline the algorithm: given an odd integer $N$ to factor, suppose for the moment that we can find the order of $x \in \mathbb{Z}_N$, i.e., the least $r$ such that $x^r \equiv 1 \bmod N$. The following algorithm factors $N$. Choose a random $x \in \mathbb{Z}_N$, and find its order $r$. If $r$ is even then compute $\gcd(x^{r/2} - 1, N)$, otherwise try a new $x$. Since with probability at least $1/2$, the order $r$ is even, and $x^{r/2} \not\equiv \pm 1 \bmod N$ [38], we get a factor of $N$.

We will now show how to find $r$. Note that the order of $x \bmod N$ divides $\phi(N)$, where $\phi(N)$ is Euler's phi function, since the exponent of $x$ acts as addition mod $\phi(N)$. Define the function $f : \mathbb{Z}_{\phi(N)} \to \mathbb{Z}_N$ by $f(x) = x^r \bmod N$. This is an instance of the HSP. The problem is that $\phi(N)$ is unknown, and indeed it could not be known since the factors of $N$ can be computed in polynomial time from knowledge of $\phi(N)$. Shor showed that nevertheless Fourier sampling over a larger size group $\mathbb{Z}_q$, where $q > \phi(N)$, results in a distribution similar to the original, and $r$ can be found using continued fractions.

In Chapter 5 we give new results generalizing Shor's ideas to arbitrary quantum states and arbitrary abelian groups. In Chapter 5 we characterize the behavior of the Fourier transform over different cyclic groups for arbitrary input vectors. The conclusion is that this process is possible in general for abelian groups whose decomposition into cyclic groups has at most a constant number of such factors. We also extend these results to all abelian groups. We first show that repeating the input superposition, combined with computing the Fourier transform over a larger modulus, leads to a new Fourier transform algorithm over abelian groups. The algorithm is asymptotically faster than the previous one, and is extremely simple. Due to the simplicity of the algorithm, we can conclude a new Fourier sampling theorem that works for all abelian groups.

Boneh and Lipton [11] solve a variant of the HSP in certain cases where the function is not distinct on all cosets. We solve this in general, and give necessary and sufficient conditions describing when this is possible.

Kitaev [36] defines the Abelian Stabilizer problem, which seems quite general. It is defined as follows: given positive integers $k$ and $n$, an element $a \in \{0,1\}^n$, and a blackbox $F$ defining an action of $G = \mathbb{Z}^k$ on the set $M \subseteq \{0,1\}^n$, find the stabilizer of $a$. The stabilizer of $a$ is the subset of $G$ that fixes $a$ under the action, and is a subgroup of $G$. This problem includes factoring and discrete log, and if the group is nonabelian, then it also includes graph isomorphism. It is not clear if the problem is equivalent to the HSP, but it does reduce to the General HSP, by defining the function $f$ by $f(g) = F(g,a)$. Then $f$ is an instance of the hidden subgroup problem, the hidden subgroup being the stabilizer.

There is another approach to efficient quantum algorithms that involves eigenvalue

estimation [36]. However, a link has been found between that method and the HSP algorithm presented here [14], and there are no known problems that it can solve that cannot be solved using Fourier sampling.

## 4.3 The Nonabelian HSP

Ettinger and Hoyer [24] give an algorithm for the HSP for the dihedral group. Their algorithm is close to the HSP algorithm, except they Fourier sample over a different group. While the dihedral group is the semi-direct product $\mathbb{Z}_N \rtimes \mathbb{Z}_2$, their algorithm Fourier samples over the abelian group $\mathbb{Z}_N \times \mathbb{Z}_2$. They show that a polynomial number of queries (i.e. samples in the HSP algorithm) is enough to reconstruct the hidden subgroup, with exponential classical post-processing time.

In [23, 22, 25], they address the question of whether or not any algorithm is possible at all. They show that the tensor products of coset states for different subgroups are almost orthogonal. This shows a polynomial query complexity, but requires an exponential number of samples (quantum measurements) from the quantum step.

Rötteler and Beth [44] give an example of a nonabelian group where the HSP can be solved. Zalka [51] has shown how to solve the problem using the HSP algorithm over $\mathbb{Z}_2^n$.

In this thesis we give the first characterization of the distribution sampled in the HSP algorithm for nonabelian groups. We use this to show that for normal subgroups the distribution has a particularly nice form, and that a polynomial number of samples is enough to reconstruct hidden normal subgroups. We then analyze the reduction of graph isomorphism to the HSP over $S_n$ and show that the HSP algorithm does not work, by

showing that the trivial subgroup cannot be distinguished from order two subgroups.

Our result about $S_n$ is based on only sampling the group representation $\rho$, and not the rows and columns of the matrices (group representations are homomorphisms into matrix groups). Independently, Grigni, Schulman, and Vazirani [28] have shown that this approach does not work, and in addition show that measuring the row of the matrix in addition does not work.