Quantum Computation using Group Representations

Amit Jayant Deshpande*

Abstract

The abelian Hidden Subgroup Problem (HSP) and Fourier transforms form the primary ingredients of many efficient quantum algorithms. Fourier transforms are also of central importance in signal processing. The non-abelian case of HSP is still open and efficient procedures for computing generalized Fourier transforms are still not known. This is a survey of some of the recent developments in these problems which give an algebraic approach using induced group representations to propose solutions for a larger class of non-abelian groups. This will include the papers by Hallgren, Russell and Ta-Shma [6] (STOC'00) on normal subgroup reconstruction, and by Püschel, Rötteler and Beth [11] on Fourier transforms for some non-abelian groups.

1 Introduction

Quantum computation has been an important area of research in computer science as well as physics for the past few years. The ability of a quantum computer to surpass a classical one in some sense has been specifically of interest and the algorithms by Deutsch, Kitaev, Shor, Grover etc are some of the well-known examples.

1.1 Hidden Subgroup Problem

Peter Shor's article [14] presented efficient algorithms for integer factorization and discrete logarithms, problems thought hard to solve on classical computers. Quantum computational version of the discrete fourier transform and the remarkable ability of a quantum computer to efficiently determine periodicities are at the core of Shor's result. Simon's algorithm [15], which showed exponential gap between classical and quantum query complexities, is also an example of "generalized periodicities" or hidden subgroup problem. Since then it has been observed that hidden subgroup problem forms the theme of most of the efficient quantum algorithms proposed till now.

Definition 1.1 (Hidden Subgroup Problem) *Let G be a finite group with a subgroup H and S be a set. Then given an efficiently computable function $f : G \to S$ that is constant on the (left) cosets of H and takes distinct values on distinct cosets, find a set of generators for the subgroup H.*

The best place to read about the relation between quantum factoring, discrete logarithms and HSP, and the step by step progress made in the case of abelian HSP, is the survey article by Jozsa [7]. Some of the important papers include Shor [14], Kitaev [8].

It is also well known that an efficient solution for the HSP over the symmetric group S_n would give rise to an efficient algorithm for the famous graph isomorphism problem. Section

*Chennai Math Institute, Chennai, India. E-mail: amit@cmi.ac.in

3 will provide details about the result of Hallgren, Russell and Ta-Shma [6] about normal subgroup reconstruction and Section 4 presents their negative result about graph isomorphism.

1.2 Fourier Transforms

For the past few decades, Fourier transforms have been at the heart of the research in signal processing. The algorithm for fast Fourier transform rediscovered[1] by Cooley-Tuckey (1965) [4] has enormous applications in correlation analysis, polynomial interpolation, the efficient computation of convolutions and, above all, in signal processing. A deeper thought was put forward later, when DFT was considered as decomposition matrix for the regular representation. Kitaev [8] showed how to compute Fourier transform efficiently over any abelian group. It is also known how to compute Fourier transforms efficiently over some non-abelian groups, most notably over S_n (Beals [2]). Maslen and Rockmore [9] is a good survey of the recent results in generalized Fourier transforms.

Definition 1.2 (Generalized Fourier Transforms) *Every isomorphism*

$$\Phi : \mathbb{C}[G] \rightarrow \bigoplus_{i=1}^{k} M_{d_i}(\mathbb{C}) \tag{1}$$

between the group algebra $\mathbb{C}[G]$ and its Wedderburn components is called Fourier transform of the group G. A particular isomorphism is fixed by picking a system $\rho_1, \rho_2, \ldots, \rho_k$ of irreducible representations of G and defining Φ as the linear extension of the map $g \mapsto \oplus_{i=1}^{k} \rho_i(g)$ (where $deg(\rho_i) = d_i$).

Püschel's dissertation [10] on constructive representation theory is a good reference to read more about generalized Fourier transforms and their relation to representation theory. In Section 5, we present an algorithm proposed by Püschel, Rötteler and Beth [11] for computing Fourier transforms over supersolvable groups.

2 Preliminaries

Here is some basic background required from representation theory (Serre [13], Terras [16]), in order to undertstand the work in the following sections.

A representation of a finite group G is a homomorphism $\rho : G \rightarrow GL(V)$, where V is a (finite dimensional) vector space over $\mathbb{C}$. Fixing a basis for V, $\rho(g)$ can be realized as $d_\rho \times d_\rho$ matrix. Two representations $\rho_1 : G \rightarrow GL(V)$ and $\rho_2 : G \rightarrow GL(W)$ are equivalent if there is a linear isomorphism $\phi : V \rightarrow W$ such that $\phi \cdot \rho_1(g) = \rho_2(g) \cdot \phi$, and we write it as $\rho_1 \cong \rho_2$. And a representation is irreducible if it doesn't leave any non-trivial subspace of V invariant (i.e. $\rho(g)\ W \subseteq W$ implies that $W = V$ or the zero subspace). Moreover, in our set-up, every representation is equivalent to a direct sum of some irreducible representations, which is called its decomposition.

Definition 2.1 (Regular Representation) *Fix a vector space V with basis $\{e_g | g \in G\}$. The regular representation $\phi : G \rightarrow GL(V)$ is defined as $\phi(g)(e_x) = e_{xg}$, $\forall x \in G$. It has dimension $|G|$ and its matrix is a permutation matrix for any $g \in G$.*

[1] It was actually found in 1805 by Carl Fredrich Gauss, who used it to interpolate orbits of asteroids. It has never been published and can be found in his collected works under the title "Theoria Interpolationis Methodo Nova Tractata", Gauss (1866)

The importance of regular representation is the fact that "Regular representation is the mother of all the representations" (- Audrey Terras [16]), i.e. it contains every irreducible representation of G. If $\rho_1, \rho_2, \ldots, \rho_k$ are the irreducible representations of G with dimensions $d_1, d_2, \ldots, d_k$, respectively, then

$$\phi = d_1\rho_1 \oplus d_2\rho_2 \oplus \ldots \oplus d_k\rho_k. \tag{2}$$

which also gives that $\sum_{i=1}^{k} d_i^2 = |G|$.

Definition 2.2 (Restriction) *A representation ρ of G naturally gives a representation for H, given by $\rho\mid_H$. We denote this by $Res_H\rho$.*

Definition 2.3 (Inner Conjugates) *$\rho^t : g \mapsto \rho(t \cdot g \cdot t^{-1})$ is called the inner conjugate of ρ, a representation of H, by $t \in G$.*

But the most interesting among these all is induced representation.

Definition 2.4 (Induced Representation) *Let H be a subgroup of G and ρ be a representation of H. $T = \{t_1, t_2, \ldots, t_n\}$ be a transversal (system of coset representativesfor H). Then the representation induced by ρ on G is given by,*

$$Ind_H^G\rho(g) = \left(\tilde{\rho}(t_i \cdot g \cdot t_j^{-1})\right)_{1 \leq\ i,\ j\ \leq n} \tag{3}$$

where

$$\tilde{\rho}(x) = \begin{cases} \rho(x) & \text{if } x \in H \\ \mathbf{0}_{deg\ \rho} & \text{otherwise} \end{cases} \tag{4}$$

Induced representation is equivalent upto the choice of the transversal. And if ρ is of degree 1, then the induction is called monomial representation.

An important fact about induced representation is that $Ind_E^G\mathbf{1_E}$ is equivalent to the regular representation of G, where $\mathbf{1_E}$ is the trivial representation of the trivial subgroup E. Another useful fact, which is the theme of the result of Püschel, Rötteler and Beth [11], is the **Double Induction**: If $H \subset K \subset G$ groups and ϕ, a representation of H. Then

$$Ind_K^G(Ind_H^K\phi) \cong Ind_H^G\phi \tag{5}$$

First chapter of Püschel's dissertation [10] is about constructive representation theory where a lot of interesting observations about induced representations are listed.

Definition 2.5 (Characters and Frobenius Reciprocity) *The character $\chi_\rho : G \to \mathbb{C}$ of a representation ρ is defined as $\chi_\rho(g) = trace(\rho(g))$. It is basis independent and moreover, is a class function, i.e. fixed on conjugacy classes. There is a natural notion for inner product of two characters as,*

$$\langle\chi_\rho|\chi_\sigma\rangle_G = \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g)\chi_\sigma(g^{-1}). \tag{6}$$

Frobenius reciprocity theorem says that,

$$\langle\chi_{1_H}|\chi_{Res_H^G\rho}\rangle_H = \langle\chi_{Ind_H^G 1_H}|\chi_\rho\rangle_G. \tag{7}$$

We know that two inequivalent irreducible characters are orthogonal and therefore inner product of a representation with an irreducible representation gives the number of occurences of that irreducible representation in its decomposition.

We also need the following important theorem from representation theory:

Theorem 2.6 (Mackey's Subgroup Theorem) *G be a group and H and K be its two subgroups. Then,*

$$Res_K^G Ind_H^G \phi = \bigoplus_{g \in H \backslash G / K} Ind_{H_g}^K Res_{H_g \cap K}^{H_g} \phi^g \tag{8}$$

The generalized Fourier transform defined already can also be thought of as the following:

Definition 2.7 (Fourier Transform) *Let $f : G \to \mathbb{C}$. The Fourier transform of f at the irreducible representation ρ, denoted by $\hat{f}(\rho)$ is the $d_\rho \times d_\rho$ matrix*

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{|G|}} \sum_{g \in G} f(g)\rho(g). \tag{9}$$

3 Normal Subgroup Reconstruction

The paper of Hallgren, Russell and Ta-Shma [6] fully analyzes a natural generalization of the abelian HSP algorithm to the non-abelian case. This algorithm finds the normal core of the hidden subgroup, and therefore, in particular, normal subgroups can be found.

The folklore algorithm for abelian HSP is as follows:

Algorithm 3.1 (Algorithm for the abelian HSP)

1. *Compute $\sum_{g \in G} |g, f(g)\rangle$ and measure the second register $f(g)$. The resulting superposition is $\sum_{h \in H} |ch\rangle \otimes |f(ch)\rangle$ for some coset cH of H. Furthermore, c is uniformly distributed over G.*

2. *Compute the Fourier transform of the coset state, resulting in*

$$\sum_{\rho \in \hat{G}} \sqrt{\frac{1}{|G|}} \sqrt{\frac{1}{|H|}} \sum_{h \in H} \rho(ch)|\rho\rangle \tag{10}$$

   where $\hat{G}$ denotes the character group, $\{\rho | \rho : G \to \mathbb{C}$ homomorphism$\}$.

3. *Measure the first register and observe a homomorphism ρ.*

A key fact about this procedure is that the resulting distribution over ρ is independent of the coset arising after the first stage. Thus, we can repeat the experiment many times, each time inducing the same distribution over $\hat{G}$.

Consider the natural generalization of Algorithm 3.1 to non-abelian groups,

Algorithm 3.2 (Potential Algorithm for the General HSP)

1. *Compute $\sum_{g \in G} |g, f(g)\rangle$ and measure the second register $f(g)$. The resulting superposition is $\sum_{h \in H} |ch\rangle \otimes |f(ch)\rangle$ for some coset cH of H. Furthermore, c is uniformly distributed over G.*

2. *Let $\hat{G}$ denote the set of all irreducible representations of G and, for each $\rho \in \hat{G}$, fix a basis for the space on which $\rho(g)$ act. Let d_ρ denote the dimension of ρ. Compute the Fourier transform of the coset state, which gives the superposition*

$$\sum_{\rho \in \hat{G}} \sum_{i=1}^{d_\rho} \sum_{j=1}^{d_\rho} \sqrt{\frac{d_\rho}{|G|}} \sqrt{\frac{1}{|H|}} \left(\sum_{h \in H} \rho(ch) \right)_{i,j} |\rho, i, j\rangle \tag{11}$$

3. *Measure the first register and observe a representation ρ.*

As expected, the resulting distribution is independent of the actual coset cH (and thus depends only on H). This is guarateed by measuring only the name of the representation ρ and leaving the matrix entries (i and j) unobserved. But the crucial question is whether this procedure retains enough information to determine H, or more precisely, are $O(\log |G|)$ samples of this distribution sufficient to determine H with high probability.

Let f be the indicator function for a particular left coset cH of H, given by

$$f(g) = \begin{cases} \sqrt{\frac{1}{|H|}} & \text{if } g \in cH, \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

Now consider the probability of observing ρ according to the Algorithm 3.2. Let $\mathcal{D}_H$ be the distribution on the representations ρ given by the algorithm 3.2. It's easy to see that the probability of observing ρ, $\mathcal{D}_H(\rho)$, is $\|\hat{f}(\rho)\|^2 = \frac{d_\rho}{|G|}\frac{1}{|H|}\|\sum_{h \in H} \rho(h)\|^2 = \frac{d_\rho}{|G|}\frac{1}{|H|}|H|^2\langle \chi_\rho, \chi_{\mathbf{1}_H}\rangle_H$. Therefore $\mathcal{D}_H(\rho) = d_\rho \frac{|H|}{G}\langle \chi_\rho, \chi_{\mathbf{1}_H}\rangle_H$.

Thus, from now onwards we can assume w.l.o.g. that our function f is constant and positive on subgroup H itself and zero elsewhere.

Now, applying Frobenius Reciprocity to the above value calculated of $\mathcal{D}_H(\rho)$, we get the following result:

Proposition 3.1 *the probability of measuring the representation ρ in Algorithm 3.2 is the product of d_ρ, $|H|/|G|$ and the number of occurences of the $\mathbf{1}_H$, the trivial representation of H, in ρ (which, due to Frobenius reciprocity, is the same as the number of occurences of ρ in the representation induced by $\mathbf{1}_H$).*

Now, let H be a subgroup of G and by H^G we denote the core of H, the largest normal subgroup of G contained in H. Our aim is to reconstruct H in general. Right now, we will try to see if H^G can be reconstructed. Thus, in the case when H is a normal subgroup, $H = H^G$ and the same procedure works. So let us consider the following algorithm:

Consider the following algorithm:

Algorithm 3.3 (Normal Subgroup Reconstruction)

1. *For $i = 1, 2, \ldots, m = 4\log|G|$, run Algorithm 3.2 and measure an irreducible representation ρ.*

2. *Let $N_i = \cap_{j=1}^{i} \ker(\rho_j)$, and finally output N_m.*

Following is the theorem which will prove the reconstruction of the core:

Theorem 3.2 *Algorithm 3.3 returns H^G with probability $1 - 2e^{\frac{-\log|G|}{8}}$.*

Proof: Here we present the proof using induced representations. For interesting aliters, see [6]. It is easy to see that $\ker(Ind_H^G \mathbf{1}_H) = H^G$. Therefore, whenever an irreducible representation ρ_i is sampled in algorithm 3.3, it must appear in $Ind_H^G \mathbf{1}_H$ and thus $H^G \subseteq \ker(Ind_H^G \mathbf{1}_H) \subseteq \ker(\rho_i)$.

Similar to the decomposition theorem for the regular representation, we can show that $Ind_{N_i}^G \mathbf{1}_{N_i} = \bigoplus_{\rho \in \hat{G}, N_i \subseteq \ker(\rho)} d_\rho \rho$. Also let, $Ind_H^G \mathbf{1}_H = \bigoplus_{\rho \in \hat{G}} m_\rho \rho$. Then we have

$$\Pr_{\rho \in \mathcal{D}_H}[N_i \subseteq \ker(\rho)] = \frac{|H|}{|G|} \sum_{\rho \in \hat{G}, N_i \subseteq \ker(\rho)} m_\rho d_\rho = \frac{|H|}{|G|} \langle \chi_{Ind_H^G \mathbf{1}_H}, \chi_{Ind_{N_i}^G \mathbf{1}_{N_i}} \rangle_G \tag{13}$$

$$= \frac{|H|}{|G|} \langle \chi_{\mathbf{1}_H}, \chi_{Res_H^G Ind_{N_i}^G \mathbf{1}_{N_i}} \rangle_H \tag{14}$$

$$= \frac{|H|}{|G|} \bigoplus_{g \in H \backslash G / N_i} \langle \chi_{\mathbf{1}_H}, \chi_{Ind_{H \cap N_i}^H \mathbf{1}_{H \cap N_i}} \rangle_H \tag{15}$$

$$= \frac{|H|}{|G|} \bigoplus_{g \in H \backslash G / N_i} \langle \chi_{\mathbf{1}_{H \cap N_i}}, \chi_{\mathbf{1}_{H \cap N_i}} \rangle_{H \cap N_i} \tag{16}$$

$$= \frac{|H|}{|G|} \frac{|G|}{|HN_i|} = \frac{|H|}{|HN_i|} \tag{17}$$

$$\leq \frac{1}{2} \; if \; N_i \not\subseteq H. \tag{18}$$

where (14) is due to Frobenius Reciprocity and (15) is due to Mackey's Subgroup Theorem.

Let $X_i \in 0, 1$ be the indicator random variable such that $X_i = 1$, if $N_i \subseteq H$ or $N_{i+1} \neq N_i$; and 0 otherwise. Thus from above, $\Pr[X_i = 0 | X_1, \ldots, X_{i-1}] \leq 1/2$ and also $\sum_{j=0}^{i} X_i$ satisfies Lipschitz condition, i.e. $|\sum_{j=0}^{i+1} X_i - \sum_{j=0}^{i} X_i| \leq 1$. Thus applying Azuma's inequality ([1]) for Martingale Bounds, we finally get that $\Pr[|\sum_{i=0}^{m} X_i - \frac{m}{2}| \geq \lambda] \leq 2e^{-\lambda^2/2m}$. So putting $\lambda = \log_2 |G|$ we have $\Pr[\sum_{i=0}^{m} X_i \leq log_2 |G|] \leq 2e^{-\log_2 |G|/8}$.

Therefore with high probability, $1 - 2e^{-\log_2 |G|/8}$, we have $N_m \subset H$. But we already know that $H^G \subset \ker(\rho_i) \subset N_i, \forall i$ and therefore $N_m = H^G$, which means that the algorithm actually gives H^G with high probability. □

Using this result, HSP can be solved efficiently for Hamiltonian Groups. These are the groups in which every subgroup is normal. All abelian groups are Hamiltonian and the only non-abelian Hamiltonian groups are of the form $G \cong \mathbb{Z}_2^k \times B \times Q$, where Q is the quaternion group and B is an abelian group with exponent b coprime to 2. Using the irreducible representations for Q and B, efficient QFT's were constructed in [6] which making use of the same algorithm solve HSP over Hamiltonian Groups.

4 Negative result: triviality in S_n

As we have already seen, an efficient solution to HSP over S_n would give rise to an efficient algorithm for the Graph Isomorphism Problem. Here is a negative result from [6] which says that the proposed algorithm doesn't give any help to solve Graph Isomorphism.

A graph G is called rigid if its automorphism group $Aut(G)$ is trivial. Note that if a graph consists of two connected components G_1, G_2 which are themselves rigid graphs then either $Aut(G)$ is trivial (when $G_1 \ncong G_2$) or it is $\{e, \tau\}$, where $\tau \in S_n$ is a permutation with $n/2$ disjoint 2-cycles.

Theorem 4.1 *Let G_1 and G_2 be two rigid, connected graphs with n vertices. Let $\mathcal{D}_I$ and $\mathcal{D}_N$ be the distributions on ρ in algorithm 3.3 for the cases, $G_1 \cong G_2$ and $G_1 \ncong G_2$ respectively. Then $|\mathcal{D}_I - \mathcal{D}_N|_1 \leq 2^{\Omega(n)}$.*

Proof: First of all, as we know $\mathcal{D}_H(\rho) = d_\rho \frac{|H|}{G} \langle \chi_\rho, \chi_{\mathbf{1}_H} \rangle_H$. And therefore, $\mathcal{D}_N(\rho) = d_\rho^2/n!$ as H is trivial, whereas $\mathcal{D}_I(\rho) = \frac{|H|}{|G|} d_\rho \langle \chi_{\mathbf{1}_H}, \chi_\rho \rangle_H = \frac{d_\rho}{n!}(d_\rho + \chi_\rho(\tau))$.

Therefore,

$$\sum_\rho |\mathcal{D}_I(\rho) - \mathcal{D}_N(\rho)| = \frac{1}{n!} \sum_\rho d_\rho |\chi_\rho(\tau)| \tag{19}$$

$$\leq \frac{1}{n!} \sqrt{\sum_\rho d_\rho^2} \sqrt{\sum_\rho |\chi_\rho(\tau)|^2} \leq \frac{1}{\sqrt{n!}} \sqrt{\sum_\rho |\chi_\rho(\tau)|^2} \tag{20}$$

by Cauchy-Schwarz inequality. Now using orthogonality of second kind ([12], thm 1.10.3) we get

$$\sum_\rho |\mathcal{D}_I(\rho) - \mathcal{D}_N(\rho)| \leq \frac{1}{\sqrt{n!}} \sqrt{\frac{n!}{|conjugacy\ class\ of\ \tau|}} = \sqrt{\frac{2^{(n/2)}(n/2)!}{n!}} \leq 2^{\Omega(n)}. \tag{21}$$

□

Grigni, Schulman, Vazirani, Vazirani ([5], STOC'2000) independently showed that measuring the representation alone is not enough for graph isomorphism, and gave stronger negative results. This involves some bound even when the row i (similarly column j) of the representation is also measured, under the assumption thet random bases are selected for each representation. They also showed that the problem can be solved if the normalizers of all subgroup have a large intersection.

5 Fourier transforms on non-abelian groups

The result of Püschel, Rötteler and Beth is a new approach to solve the problem of the construction of Fourier transforms on non-abelian groups. The main theme is to construct efficient Fourier transforms for a group G once we know how to construct efficient Fourier transforms for N, a normal subgroup of G, and have some special information about the quotient group G/N.

Here are the main lemmas from constructive representation theory which occupy a considerable part of the chapter 1 of Püschel's dissertation [10]. He considered a case when G/N is cyclic, moreover of prime index. From here onwards ϕ^A means matrix of the representation ϕ conjugated by the matrix A and an extension of a representation ϕ of N to G means a representation $\bar{\phi}$ of G such that $Res_N^G \bar{\phi} = \phi$. We also denote the matrix of the representation $Ind_N^G \phi$ using transversal T, by $(\phi \uparrow_T G)$.

Now, since Fourier transforms are nothing but the matrix decomposing the regular representation, we can use the recursion formula of double induction.

Lemma 5.1 *Let $N \trianglelefteq G$ be a normal subgroup of prime index p with transversal (group of coset representatives) $T = (t^0, t^1, \ldots, t^{(p-1)})$ and ϕ be a representation of N of degree d such that it has an extension (careful ! this may not exist in general) $\bar{\phi}$ to G. Now if A is the*

matrix decomposing ϕ into irreducibles, say $\phi^A = \rho = \rho_1 \oplus \ldots \oplus \rho_k$, and $\bar{\rho}$ be an extension of ρ to G, then the matrix for the decomposition of $(\phi \uparrow_T G)$ is the following:

$$B = (\mathbf{1}_p \otimes A) \cdot D \cdot (DFT_p \otimes \mathbf{1}_d), where D = \bigoplus_{i=0}^{p-1} \bar{\rho}(t^i). \tag{22}$$

Moreover, the decomposition is

$$(\phi \uparrow_T G)^B = \bigoplus_{i=0}^{p-1} \lambda_i \cdot \bar{\rho}, \tag{23}$$

where $\lambda_i : t \mapsto \omega_p^i$ for $i = 0, 1, \ldots, (p-1)$, are the 1-dimensional representations of G arising from the factor group G/N.

The matrix D is called the generalized Twiddle factor, which vanishes in the case when $G \cong N \times G/N$. And when G is abelian, above formula gives the well-known Cooley-Tuckey decomposition.

Since we are considering Fourier transforms as the matrix decompositions of regular representations, it is interesting to know if we can apply this lemma for regular representation.

Lemma 5.2 *G and N as above and let ϕ be a regular representation of N. Then ϕ has an extension $\bar{\phi}$ to G (and hence all conjugates of ϕ, too). Furthermore $\phi \cong \phi^t$, $\forall t \in G$, i.e. all its inner conjugates are equivalent.*

This lemma says that G/N operated on the set of irreducible representations via inner conjugation. Now, according to Clifford's theorem ([10], thm 1.71) exactly one of following two cases occurs for each summand ρ_i:

1. $\rho_i \cong \rho_i^t$, $\forall t \in G$ and ρ_i can be extended to G. The extension can be explicitly calculated by Minkwitz' formula (an elementary proof can be found in [3]).

2. $\rho_i \ncong \rho_i^t$, $\forall t \in G$ and $\rho_i \uparrow_T G$ is irreducible and hence the whole direct sum $\rho_i \oplus \rho_i^t \oplus \ldots \oplus \rho_i^{t^{(p-1)}}$ can be extended to G by $\rho_i \uparrow_T G$.

Another problem is to fix up the direct sum $\oplus_{i=0}^{p-1} \lambda_i \cdot \bar{\rho}$ with the equivalent summands being equal. These arise from the ρ_i's falling in the second case of Clifford's theorem. This can be fixed up by conjugating them with a blockdiagonal matrix $diag(1, \omega_p, \ldots, \omega_p^{(p-1)})^i$.

Putting this all together, we get a procedure to construct Fourier transform on G, once we know how to construct Fourier transforms on its subgroup N which is of prime index.

Algorithm 5.1 (Recursive Fourier transforms) *Our goal is to get a decomposition matrix B for $(\phi \uparrow_T G)$ from the matrix A that decomposes ϕ, regular representation of N.*

1. *Determine the permutation matrix P which rearranges ρ_i's such that the extendable ones (first case of Clifford's theorem) come first followed by the others, also ordered into sequences of p-blocks equivalent to $\rho_i, \rho_i^t, \ldots, \rho_i^{t^{(p-1)}}$.*

2. *Calculate matrix M which is identity on the extendables but conjugates the p-block sequences to make them equal to $\rho_i, \rho_i^t, \ldots, \rho_i^{t^{(p-1)}}$, instead of just equivalent.*

3. *Now extend $\phi^{A \cdot P \cdot M}$ summandwise. Use Minkwitz formula for the extendables and use $\rho_i \uparrow_T G$ for the p-block sequences.*

4. *Evaluate $= \bigoplus_{i=0}^{(p-1)} \bar{\rho}(t^i)$ and also construct the blockdiagonal matrix C as in the discussion above.*

Then the decomposition matrix for $\phi \uparrow_T G$ is given by,

$$B = (\mathbf{1}_p \otimes A \cdot P \cdot M) \cdot D \cdot (DFT_p \otimes \mathbf{1}_{|N|}) \cdot C \tag{24}$$

Using this recursive technique, Püschel, Rötteler and Beth have constructed quantum circuits that construct Fourier transforms efficiently on non-abelian 2-groups. This involves explicit calculations of the above matrices in terms of quantum circuits on explicit class of groups. They used the classification theorem for 2-groups which says that, for $n \geq 3$ there are four classes of non-abelian groups of order $2^(n+1)$ upto isomorphism.

1. Dihedral group $D_{2^{(n+1)}} = \langle x, y \mid x^{2^n} = y^2 = 1, yxy^{-1} = x^{-1} \rangle$.
2. Quaternion group $Q_{2^{(n+1)}} = \langle x, y \mid x^{2^n} = y^4 = 1, yxy^{-1} = x^{-1} \rangle$.
3. $QP_{2^{(n+1)}} = \langle x, y \mid x^{2^n} = y^2 = 1, yxy^{-1} = x^{2^{(n-1)}+1} \rangle$.
4. Quasidihedral group $QD_{2^{(n+1)}} = \langle x, y \mid x^{2^n} = y^2 = 1, yxy^{-1} = x^{2^{(n-1)}-1} \rangle$.

6 Conclusion and Open Problems

This opens up a new approach towards non-abelian HSP as well as the construction of non-abelian Fourier transforms. An important open problem is to try and apply the procedure of Püschel et al to construct Fourier transforms over solvable groups. Even extending their procedure to supersolvable groups would also be very interesting.

7 Acknowledgements

I sincerely thank my advisor, Prof. Miklos Santha for introducing these problems to me. Some references suggested by Frédéric Magniez were also helpful.

References

[1] N. Alon and J. Spencer, *The probabilistic method*, Wiley, 1992.

[2] R. Beals, *Quantum computation of Fourier transforms over symmetric groups*, STOC'1997.

[3] M. Clausen, *A direct proof of Minkwitz extension theorem*, AAECC Vol.8 (4), 1997.

[4] J. W. Cooley and J. W. Tuckey, *An algorithm for machine calculation of complex Fourier series*, Math. Comp. 19 (1965).

[5] M. Grigni, L. Schulman, M. Vazirani and U. Vazirani, *Quantum mechanical algorithms for the non-abelian hidden subgroup problem*, STOC'2000.

[6] S. Hallgren, A. Russell and A. Ta-Shma *Normal subgroup resonstruction and quantum computation using group representations*, STOC'2000.

[7] R. Jozsa, *Quantum algorithm and Fourier transform*, Proc. Royal Society London A, 1998.

[8] A. Kitaev, *Quantum measurements and abelian stabilizer problem*, Technical report quant-ph/9511026, 1995.

[9] D.Maslen and D. Rochmore, *Generalized FFT: A survey of some recent results*, DIMACS series in Discrete Math and Theoretical Computer Science, 28 (1997).

[10] M. Püschel, *Constructive representation theory and generation of algorithms*, Ph.D. dissertation, Universität Karlsruhe, 1998.

[11] M. Püschel, M. Rötteler and T. Beth, *Fast quantum Fourier transforms for a class of non-abelian group*, Proc. AAECC 1999.

[12] B. E. Sagan, *The symmetric group: Representations, combinatorial algorithms, and symmetric functions.*

[13] J. P. Serre, *Linear representations of finite groups*, 42: Grad texts in Math, Springer-Verlag, 1977.

[14] P. Shor, *Polynomial time algorithm for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal of Computing, 1997.

[15] D. Simon, *On the power of quantum computation*, SIAM Journal of Computing, 1997.

[16] A. Terras, *Fourier analysis of finite groups and applications*, Cambridge Univ. Press, 1999.