Abstract

Quantum Fourier Sampling, the Hidden Subgroup Problem, and Beyond

by

Sean Joseph Hallgren

Doctor of Philosophy in Computer Science

University of California, Berkeley

Professor Umesh V. Vazirani, Chair

The Hidden Subgroup Problem (HSP) provides the fundamental framework for most quantum algorithms. Until very recently, all known problems where quantum computation provides a super-polynomial speedup over classical algorithms have been variants of the HSP for particular abelian groups. Examples include factoring integers and computing the discrete log, for which Shor found efficient quantum algorithms. The algorithm for these problems may be viewed as consisting of the main HSP solution plus an ad hoc method of dealing with the particular variant. In this dissertation, we give a systematic way of dealing with all these variants. The key component of our solution is a new theorem about the robustness of Fourier sampling. The purpose of this theorem is to better understand the structure underlying existing algorithms as well as to provide an algorithmic tool for the construction of future quantum algorithms. In addition, we also derive a new algorithm for computing the quantum Fourier transform which is asymptotically faster than

any previously known algorithm.

By contrast, the nonabelian HSP is wide open. It includes as a special case the longstanding open question of graph isomorphism, where the group is the symmetric group, S_n. It is natural to carry over the abelian HSP algorithm to the nonabelian case. We show that in the case that the hidden subgroup is normal, this algorithm succeeds in reconstructing the subgroup in polynomial time. On the other hand, we give evidence that this algorithm is inadequate to even distinguish a trivial subgroup from an involution in the case of the symmetric group.

Finally, we give an algorithm for the Shifted Legendre Symbol Problem and its variants. There is some evidence that this is an intractable problem classically, and a closely related problem has been proposed as a cryptographic primitive. Perhaps the most interesting aspect of this new quantum algorithm is that it appears to go beyond the framework of the HSP.

Professor Umesh V. Vazirani
Dissertation Committee Chair

Contents

1 Introduction **1**

2 Preliminaries **6**

3 The Model **9**
3.1 Quantum Algorithms 10

4 Fourier Sampling and the HSP **20**
4.1 The Hidden Subgroup Problem 20
4.2 The General HSP 23
4.3 The Nonabelian HSP 25

5 Fourier Sampling over Abelian Groups **27**
5.1 Introduction 27
5.2 Zero-Filling 30
5.2.1 The Main Theorem 30
5.2.2 Application to the Quantum Case 30
5.2.3 The Continuous Picture 33
5.2.4 Limitations of Zero-Filling 34
5.2.5 Proof of Theorem 5.1 36
5.3 Repeating the Vector 39
5.4 Repeating and Zero-Filling 41
5.4.1 The Main Theorem 41
5.4.2 A Better Fourier Sampling Theorem 44
5.4.3 Application: Many-to-One Periodic Functions 48
5.4.4 Proof of Theorem 5.3 50

6 Fourier Sampling Coset States of Nonabelian Groups **55**
6.1 Representation Theory Background 57
6.2 The Probability Distribution over Representations 62
6.3 A Positive Result: Normal Subgroups 64
6.4 A Negative Result: Determining Triviality in the Symmetric Group 66

7 Efficient Quantum Algorithms for Shifted Quadratic Character Problems 69
7.1 Definitions and Related Work 70
7.2 An Algorithm for Prime Size Fields 72
7.3 An Algorithm for General Finite Fields 77

8 Conclusion 81

Bibliography 83