Quantum computing, norms and polynomials

Escudero Gutiérrez, F.

Chapter 1

Introduction

Motivated by the necessity to perform calculations, humankind has developed *algorithms*: sequences of simple computation steps designed to perform (more) complex computations. Maybe the most basic calculation is the sum of two natural numbers, and the best-known example of an algorithm is the set of instructions we learn in primary school to perform this task. A slightly more involved algorithm is the one to multiply two natural numbers, but it is still taught at primary school. Considerably more difficult is the inverse process of *factoring*, consisting of writing a natural number as a product of *prime* numbers, which are the natural numbers that cannot be written as the product of two other natural numbers (apart from the product of 1 and themselves). The definition of factoring involves abstract concepts, and thus, understanding the algorithms for that problem requires elaborate mathematical theories. Despite what its description might suggest, factoring is a problem with practical relevance, as cybersecurity is based on the inability of current computers to factor big natural numbers efficiently. The capacities of these computers are determined by the behavior of the physical units they are composed of, which are governed by classical physics, and thus we refer to them as *classical computers*. By contrast, in the 80's Yuri Manin and Paul Benioff proposed an idea later popularized by Feynman: to build computers with quantum particles, described by the richer theory of quantum mechanics [Ben80, Man80]. This gave birth to the idea of *quantum computers*, whose capabilities would exceed those of classical computers. Notably, Peter Shor discovered a *fast* algorithm for factoring large numbers in a *quantum computer* [Sho97]. As of today, we are on the path towards realizing a fully functional quantum computer.

Factoring is not an isolated case, but rather one of many computational problems

with practical relevance whose analysis benefits from the use of mathematical structures. In this thesis, we will approach several of such problems, all related to quantum computing, from the perspective of *theoretical computer science*, i.e., establishing rigorous guarantees. The questions we will consider fall into two categories. The first is *query complexity*, a model of computation where the power and limitations of quantum and classical computers can be rigorously studied. In particular, the foundational quantum algorithms by Peter Shor, to factor large numbers, and by Lov Grover, to find a marked element in a list, belong to this model [Gro96, Sho97]. The second category is *learning theory*, where the meta-question is how to characterize an unknown object to which we have limited access. In contrast with recent breakthroughs in machine learning, such as ChatGPT, our findings do not focus on immediate applicability but instead provide rigorous performance guarantees. In other words, our results fit into the subfield of *computational learning theory* initiated by Leslie Valiant in 1984 [Val84].

To address these questions, we will borrow and develop tools of non-applied mathematical branches, especially from *functional analysis*. Functional analysis is the branch of mathematics that studies functions in a very general way, even when they depend on an unbounded number of variables. Relevant examples of functions are *polynomials*, which can be written as sums of *monomials*, that are products of numbers and variables. Thanks to their elementary definition, polynomials are ubiquitous and motivate deep mathematical questions. Some of these questions are related to the comparison of *norms* of polynomials, which are measures of the *size* of the polynomial. How these norms relate has motivated many celebrated advances of mathematics during the last century, such as the works of Alexander Grothendieck, Frederic Bohnenblust and Carl Einar Hille [Gro53, BH31].

Polynomials have found applications in theoretical computer science, like the *polynomial method* of query complexity, a tool to prove limitations of quantum computers [NS94, BBC$^+$01]. Maybe more implicitly, polynomials have also played a role in quantum mechanics, as, for instance, Hamiltonians, which model the interactions between quantum particles, can be regarded as polynomials [MO08].

In this thesis, as explained in more detail in Section 1.1, we make progress in the understanding of the polynomial method and propose new algorithms to learn quantum objects. In parallel, we will prove functional-analytic statements relating different norms of polynomials.

This thesis is a product of a four-year PhD program developed at the Centrum Wiskunde & Informatica (CWI) in Amsterdam.

1.1 Overview

This thesis is divided into three parts, preceded by a preliminary chapter (Chapter 2) where we introduce notation, definitions, and basic results.

In Part I, we study several questions related to quantum query complexity and polynomials. Query complexity is a model of computing where the aim is to approximate a known function f on a hidden input x. The algorithm can access x via queries that reveal units of information about x. The goal is to determine how many queries an algorithm needs to solve such a task. Depending on the nature of these queries, one can speak about classical or quantum query complexity.

In Chapter 3, we show that the polynomial method is complete. This method was introduced and successfully applied to show lower bounds on quantum query complexity [BBC$^+$01, AS04]. Recently, it was refined as a tool to prove upper bounds [ABP19], which also led to a classical optimization algorithm to determine quantum query complexity [GL19]. In this chapter, we review these advancements and complete this picture by proposing a constructive method to design quantum algorithms via polynomials.

In Chapter 4, we show two technical results. The first is that the Grothendieck constant, which appears in the celebrated Grothendieck inequality that relates two norms of polynomials of degree 2, can be characterized in terms of quantum algorithms that make 1 query. The second result shows that quantum algorithms that make 2 queries are not equivalent to a certain class of polynomials because of the failure of Grothendieck's inequality for polynomials of degree greater than 2, answering a question by Aaronson, Ambainis, Iraids, Kokainis, and Smotrovs [AAI$^+$16].

In Chapter 5, we make progress on the Aaronson and Ambainis (AA) conjecture. The AA conjecture asserts that certain low-degree polynomials have a very influential variable [AA09]. Although this is a functional-analytic conjecture, it implies that quantum query complexity can only be much lower than classical query complexity for functions where some structure about the hidden input is promised beforehand. Our contributions in this chapter are formulating a weaker conjecture that retains the implications for query complexity, and proving it in a particular case.

In Part II, we explore several questions related to learning quantum objects that can be understood as polynomials. This analogy was pointed out by Montanaro and Osborne, who showed that polynomials can be embedded into quantum operators while preserving relevant properties such as the degree [MO08].

In Chapter 6, we prove two new versions of the Bohnenblust-Hille inequality, which

compares two norms of polynomials. We apply the first of them to learn quantum query algorithms. Then, we use the second to learn quantum channels, which are the operations allowed in a quantum computer.

In Chapter 7, we prove some of the first results about learning quantum Hamiltonians. Due to the Schrödinger equation, Hamiltonians model the evolution of quantum systems. In this chapter, we design algorithms to infer properties of and, in some cases, fully characterize an unknown Hamiltonian by accessing the corresponding time evolution.

Part III is a *bonus* that just consists of Chapter 8, where we gather three new proofs, that we find elegant and concise, of known results related to the analysis of Boolean functions.

1.2 Relation to literature

The content of this thesis is based on the following papers.

- Section 3.4 is a quantum-oriented exposition of the following work, originally written for a non-applied mathematical audience:

  [Esc25] Francisco Escudero Gutiérrez. Christensen-Sinclair factorization via semidefinite programming. *Linear Algebra and its Applications*, 714:28–44, 2025.

- Chapter 4 is based on:

  [BE22] Jop Briët and Francisco Escudero Gutiérrez. On Converses to the Polynomial Method. In *17th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2022), volume 232 of Leibniz International Proceedings in Informatics (LIPIcs)*, pages 6:1–6:10. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022.

  [BEG24] Jop Briët, Francisco Escudero Gutiérrez, and Sander Gribling. Grothendieck inequalities characterize converses to the polynomial method. *Quantum*, 8:1526, 2024.

- Chapter 5 is based on:

  [Esc24a] Francisco Escudero Gutiérrez. Influences of Fourier completely bounded polynomials and classical simulation of quantum algorithms. *Chicago Journal of Theoretical Computer Science*, 2024.

  Also presented at the *18th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2023)*.

- Chapter 6 is based on:

  [ADEP25] Srinivasan Arunachalam, Arkopal Dutt, Francisco Escudero Gutiérrez, and Carlos Palazuelos. A cb-Bohnenblust–Hille inequality with constant one and its applications in learning theory. *Mathematische Annalen*, pages 1–30, 2025.

  A complementary version of [ADEP25] also appeared in the proceedings of ICALP'24:

  [ADEP24] Srinivasan Arunachalam, Arkopal Dutt, Francisco Escudero Gutiérrez, and Carlos Palazuelos. Learning low-degree quantum objects. In *51st International Colloquium on Automata, Languages, and Programming* (ICALP 2024), pages 13–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2024.

  Also presented at the *19th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2024)*.

- Chapter 7 is based on:

  [ADE25] Srinivasan Arunachalam, Arkopal Dutt, and Francisco Escudero Gutiérrez. Testing and learning structured quantum Hamiltonians. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, page 1263–1270, New York, NY, USA, 2025. Association for Computing Machinery.

  Also presented at the *20th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2025)*. A journal version has already been accepted in Communications in Mathematical Physics.

Additionally, this thesis contains previously unpublished work. More precisely:

- Chapter 3 contains a new exposition of the (completely bounded) polynomial method. In particular, we prove that the refinement of polynomial degree proposed in [ABP19] upper bounds quantum query complexity in an almost self-contained way. For this, we avoid the functional analytic black-boxes of the original proof, and only use tools from theoretical computer science.

- Chapter 8 contains new proofs of known results, with marginal improvements, that we find elegant and concise. All of these results are related to the analysis of Boolean functions $f : \{-1, 1\}^n \to \{-1, 1\}$.

Finally, the following papers were also completed during my PhD.

- [EFFJ+23] Francisco Escudero Gutiérrez, David Fernández-Fernández, Gabriel Jaumá, Guillermo F. Peñas, and Luciano Pereira. Hardware-efficient entangled

measurements for variational quantum algorithms. *Physical Review Applied*, 20(3), 2023.

- [EM24] Francisco Escudero Gutiérrez and Garazi Muguruza. All S_p notions of quantum expansion are equivalent. *arXiv preprint* arXiv:2405.03517, 2024.

- [BE24] Jinge Bao and Francisco Escudero Gutiérrez. Learning junta distributions, quantum junta states, and QAC^0 circuits. *arXiv preprint* arXiv:2410.15822, 2024.

  Presented at the *25th Asian Quantum Information Science Conference* (AQIS'25).

- [ACE+25] Amira Abbas, Nunzia Cerrato, Francisco Escudero Gutiérrez, Dmitry Grinko, Francesco Anna Mele, and Pulkit Sinha. Nearly optimal algorithms to learn sparse quantum Hamiltonians in physically motivated distances. *arXiv preprint* arXiv:2509.09813, 2025.

- [BCE+25] Andreas Bluhm, Matthias C. Caro, Francisco Escudero Gutiérrez, Aadil Oufkir, and Cambyse Rouzé. Certifying and learning quantum Ising Hamiltonians. *arXiv preprint* arXiv:2509.10239, 2025.