FUNCTION DISCRIMINATION VIA QUANTUM SIGNAL PROCESSING WITH A NULL INPUT

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

HALIL İBRAHIM OLGUN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
PHYSICS

SEPTEMBER 2026

Approval of the thesis:

FUNCTION DISCRIMINATION VIA QUANTUM SIGNAL PROCESSING WITH A NULL INPUT

submitted by **HALIL İBRAHIM OLGUN** in partial fulfillment of the requirements for the degree of **Master of Science in Physics Department, Middle East Technical University** by,

Prof. Dr. Naci Emre Altun
Dean, Graduate School of **Natural and Applied Sciences** _____

Prof. Dr. Seçkin Kürkçüoğlu
Head of Department, **Physics** _____

Prof. Dr. Sadi Turgut
Supervisor, **Physics, METU** _____

Examining Committee Members:

Assist. Prof. Dr. Osman Barış Malcıoğlu
Physics, METU _____

Prof. Dr. Sadi Turgut
Physics, METU _____

Assist. Prof. Dr. Kıvanç Uyanık
Physics, Gazi University _____

Date:04.09.2026

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname: Halil İbrahim Olgun

Signature :

ABSTRACT

FUNCTION DISCRIMINATION VIA QUANTUM SIGNAL PROCESSING WITH A NULL INPUT

Olgun, Halil İbrahim
M.S., Department of Physics
Supervisor: Prof. Dr. Sadi Turgut

September 2026, 40 pages

This thesis applies Quantum Signal Processing (QSP) to solve a generalized Deutsch-Jozsa promise problem: distinguishing whether a Boolean function has r_1 or r_2 solutions in a search space of size N. Standard QSP suffers from two limitations: the measurement probability is symmetric under replacing the number of solutions with its complement, and the required number of evaluations is rarely an integer, introducing rounding errors that prevent deterministic success. To resolve these issues, we introduce an auxiliary null input state that remains invariant under the function evaluation. This state breaks the complement symmetry and introduces an adjustable initial amplitude coefficient. By tuning this amplitude, we can force the required number of evaluations to be an exact integer, eliminating rounding errors and achieving a deterministic algorithm with quadratic speedup.

Keywords: Quantum Singular Value Transformation, Quantum Signal Processing, Function Discrimination, Quantum Algorithm Complexity, Deterministic Quantum

Algorithms

ÖZ

BOŞ GİRDİ İLE KUANTUM SİNYAL İŞLEME YOLUYLA FONKSİYON AYIRT ETME

Olgun, Halil İbrahim
Yüksek Lisans, Fizik Bölümü
Tez Yöneticisi: Prof. Dr. Sadi Turgut

Eylül 2026 , 40 sayfa

Bu tez çalışmasında, genelleştirilmiş bir Deutsch-Jozsa vaat problemini çözmek amacıyla Kuantum Sinyal İşleme (QSP) yöntemi uygulanmıştır. İncelenen problem, toplam N girdiye sahip bir Boole fonksiyonunun çözüm sayısının (r) önceden belirlenmiş iki değerden (r_1 veya r_2) hangisine eşit olduğunu tespit etmeye dayanır. Standart QSP çerçevesi bu probleme uygulandığında iki temel kısıtla karşılaşılmaktadır: İlki, ölçüm olasılığının r ve $N - r$ sayıda çözüme sahip fonksiyonlar için aynı kalmasıdır. İkincisi ise algoritmanın gerektirdiği fonksiyon değerlendirme sayısının nadiren tam sayı çıkması ve bu durumun deterministik başarıyı engelleyen yuvarlama hatalarına yol açmasıdır. Bu kısıtlamaları aşmak için, fonksiyon uygulandığında değişmeyen yardımcı bir boş girdi durumu sisteme dahil edilmiştir. Bu durum sayesinde hem r ile $N - r$ arasındaki simetri kırılmakta hem de gereken fonksiyon değerlendirme sayısı tam bir sayıya eşitlenebilmektedir. Böylece yuvarlama hataları ortadan kaldırılarak kuadratik hızlanmaya sahip deterministik bir kuantum algoritması elde edilir.

Anahtar Kelimeler: Kuantum Tekil Değer Dönüşümü, Kuantum Sinyal İşleme, Fonksiyon Ayırt Etme, Kuantum Algoritma Karmaşıklığı, Deterministik Kuantum Algoritmaları

To my family for their never ending support

ACKNOWLEDGMENTS

I would like to start by thanking my supervisor Prof. Dr. Sadi Turgut for his guidance and support. I have always admired his approach to any subject whatsoever, and he taught me to look at problems in a much simpler and more fundamental way, which I will undoubtedly use for the rest of my life. I would also like to thank Asst. Prof. Kıvanç Uyanık and Asst. Prof. Osman Barış Malcıoğlu for their time, valuable comments and questions during my defence.

I would like to thank my family, for whom I find it hard to express all the support I felt throughout my life. They have always pushed me to follow the path that I wanted to pursue and always taught me to do the things I love. I would like to thank my sister for being such an inspiration and showing me how hard it is possible to work for the things we enjoy and love. This alone is the reason I could continue and finish this thesis.

I would like to thank Elif Varol for being such a wonderful person and for enduring this journey with me. Her vibrant personality and joy for life helped me push through whenever things got difficult. Although her field of study is completely different, her questions have enabled me to understand aspects I had overlooked. She has also taught me more than I can possibly fit into a couple of sentences here, and I will always be grateful to have such an amazing person in my life.

TABLE OF CONTENTS

ABSTRACT v

ÖZ vii

ACKNOWLEDGMENTS x

TABLE OF CONTENTS xi

LIST OF FIGURES xiii

LIST OF ABBREVIATIONS xiv

CHAPTERS

1 INTRODUCTION 1

1.1 Motivation and Background 1

1.1.1 Previous Work 3

2 QUANTUM SIGNAL PROCESSING AND POLYNOMIAL TRANSFORMATIONS 5

2.1 Quantum Signal Processing (QSP) Framework 5

2.2 Quantum Amplitude Amplification (QAA) 7

2.3 Analysis of Low-Degree Solutions 11

2.4 Chebyshev Polynomial Solutions 13

3 FUNCTION ORACLES AND PROMISE PROBLEMS 17

3.1 Formulation of the Function Oracle 17

3.1.1 Generalized Phase Oracles 17
3.1.2 Standard Phase-Kickback Oracle 18
3.2 Promise Problems 19
3.3 The Deutsch-Jozsa Problem as a Promise Problem 19
4 FUNCTION DISCRIMINATION VIA QUANTUM SIGNAL PROCESSING 23
4.1 General Formulation of Function Discrimination 23
4.2 Function Discrimination via QSP 24
4.3 Function Discrimination with a Null Input 29
4.4 Single Evaluation Discrimination from the Zero-Solution Function . . 32
4.5 Classical Query Complexity 33
5 CONCLUSION 37
REFERENCES 39

LIST OF FIGURES

FIGURES

Figure 4.1 The required number of evaluations (top) and the corresponding rounding error (bottom) for distinguishing sets separated by $\Delta r = 1$, plotted for a search space of size $N = 100$. For clarity, the discrete evaluations are marked at intervals of 5. 28

LIST OF ABBREVIATIONS

QSP	Quantum Signal Processing
QSVT	Quantum Singular Value Transformation
QAA	Quantum Amplitude Amplification

CHAPTER 1

INTRODUCTION

1.1 Motivation and Background

A promise problem consists of distinguishing between defined sets of black-box functions, with the information that the unknown function we are given is guaranteed to be in one of these sets. One of the earliest and the most fundamental promise problem in quantum information theory is Deutsch's problem [1], which was later modified to Deutsch-Jozsa problem [2]. In this problem, the objective is to determine whether a Boolean function is constant or balanced in the input space. Classically, we need to evaluate the function at least one more than half of the inputs to have a deterministic answer. Deutsch-Jozsa algorithm reduces the number of evaluations to one. This reduction in number of evaluations is the general benchmark for quantum query complexity, where the efficiency of an algorithm is defined by the number of times we evaluate the given oracle rather than the total number of operations.

There have been many algorithms designed to solve problems with fewer queries than their classical counterparts. Quantum signal processing (QSP) [3], later generalized to Quantum Singular Value Transformation (QSVT) [4], is a framework that unifies many of these algorithms [5]. By composite application of two operators, one representing the oracle query and the other an arbitrary rotation, it can restrict the system's evolution to some subspace spanned by the initial and target states. The predefined sequence of these operations allows us to apply a polynomial transformation satisfying some conditions to the amplitudes of the initial state. These conditions naturally arise from the construction of these operators and the unitary condition which ensures

preservation of the information through the evolution of the system.

This thesis explores the application of QSP to solve a generalized version of the Deutsch-Jozsa problem. The problem is defined as finding the number of solutions r for a given function f with the promise that $r \in \{r_1, r_2\}$ for $r_1 \neq r_2$. Here r is the number of inputs in the domain $X = \{1, 2, \ldots, N\}$ such that $f(x) = 1$. Approaching this problem similarly to the Deutsch-Jozsa problem, we encounter two limitations. First, the final measurement probability of the target state is symmetric under the transformation $r \leftrightarrow N - r$. This is not a problem in the case of the Deutsch-Jozsa algorithm since constant functions and balanced functions remain within their respective sets under this transformation. Second, the required number of evaluations is almost never an integer, which means we do not obtain a deterministic solution as in the Deutsch-Jozsa algorithm. To address these problems, we introduce an auxiliary null state $|\star\rangle$ that is invariant under the action of the oracle. This construction leads to a deterministic solution requiring an integer number of evaluations. Furthermore, it breaks the symmetry under the $r \leftrightarrow N - r$ transformation.

The rest of this thesis is organized as follows. Chapter 2 introduces the mathematical framework of Quantum Signal Processing, shows how it can be applied to Quantum Amplitude Amplification, and discusses the mathematical conditions for achievable polynomials under the QSP framework, showing why Chebyshev polynomials are well-suited for these operations. Chapter 3 defines the theoretical framework of function oracles and promise problems, with the Deutsch-Jozsa algorithm as an example problem using the established construction. Chapter 4 presents our main contribution, where we apply QSP and the null state to solve the generalized function discrimination problem deterministically while overcoming the symmetry and rounding limitations of standard approaches. Finally, Chapter 5 concludes the thesis with a summary of our results and future research directions.

1.1.1 Previous Work

The problem of distinguishing between Boolean functions based on their number of solutions is known as the weight decision problem. Early work by Braunstein et al. [6] introduced an exact quantum algorithm for the symmetric case, distinguishing functions with r solutions from those with $N - r$ solutions by modifying phase shifts in Grover iterations. Choi and Braunstein [7] extended this framework to asymmetric solution counts ($r_1 \neq r_2$) by padding the input space to map the asymmetric problem back to a symmetric state space.

Uyanık and Turgut [8] investigated exact decision algorithms using generalized Grover iterations, deriving algebraic conditions and query limits required for deterministic function discrimination without error.

Subsequently, He et al. [9] formally connected exact quantum query complexity to Chebyshev polynomials, utilizing domain padding to address non-integer query constraints.

In this work, we adopt the Chebyshev polynomial framework within Quantum Signal Processing (QSP). Rather than padding the input domain, we introduce an invariant auxiliary state, the null input, to break complement symmetry and enable deterministic discrimination between arbitrary function sets.

CHAPTER 2

QUANTUM SIGNAL PROCESSING AND POLYNOMIAL TRANSFORMATIONS

2.1 Quantum Signal Processing (QSP) Framework

Quantum signal processing (QSP) [3] is an algorithmic framework that uses composite sequences of $\mathrm{SU}(2)$ rotations to implement a restricted class of polynomial transformations on a matrix element of some given unitary operator. It was later generalized to multi-qubit systems, known as Quantum Singular Value Transformation (QSVT) [4].

The QSP framework, as well as its extension QSVT, has been used to design quantum algorithms for many problems in the past, including Hamiltonian simulation [3] and solving linear systems of equations [4]. On the other hand, many other problems which have been solved without the use of this construction can be reduced to the QSP/QSVT framework. Consequently, it has also been called in the literature a ”unification” of quantum algorithms [5].

The idea of QSP is to use two types of unitary operations, which we can conceptually call signal operators and signal processing operators.

Let the signal operator be

$$W(x) = \begin{bmatrix} x & i\sqrt{1-x^2} \\ i\sqrt{1-x^2} & x \end{bmatrix} \tag{2.1}$$

where x is a real number between -1 and 1.

The signal processing operator is defined as

$$S(\phi) = e^{i\phi\sigma_z} = \begin{bmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{bmatrix} \tag{2.2}$$

For a set of angles $\phi_0, \phi_1, \ldots, \phi_d$, and using the operators $W(x)$ and $S(\phi)$, we can construct a sequence of operations as:

$$S(\phi_0) \prod_{j=1}^{d} W(x) S(\phi_j) \tag{2.3}$$

This unitary can be expressed in terms of some polynomials $P(x)$ and $Q(x)$.

$$S(\phi_0) \prod_{j=1}^{d} W(x) S(\phi_j) = \begin{bmatrix} P(x) & i\sqrt{1-x^2}Q(x) \\ i\sqrt{1-x^2}Q^*(x) & P^*(x) \end{bmatrix} \tag{2.4}$$

To see why the matrix elements must have this structure, consider the relation $\sigma_y A \sigma_y = A^*$. Both the signal operator and the phase rotation operators satisfy this identity:

$$\sigma_y W(x) \sigma_y = W^*(x), \tag{2.5}$$

$$\sigma_y S(\phi) \sigma_y = \sigma_y e^{i\phi\sigma_z} \sigma_y = e^{-i\phi\sigma_z} = S^*(\phi). \tag{2.6}$$

Because $\sigma_y (AB) \sigma_y = (\sigma_y A \sigma_y)(\sigma_y B \sigma_y) = A^* B^* = (AB)^*$, this property is preserved under matrix multiplication. For an arbitrary 2×2 matrix $M = \begin{bmatrix} P & R \\ S & T \end{bmatrix}$, we get the following:

$$\sigma_y M \sigma_y = \begin{bmatrix} T & -S \\ -R & P \end{bmatrix} = \begin{bmatrix} P^* & R^* \\ S^* & T^* \end{bmatrix}. \tag{2.7}$$

This implies that $T = P^*$ and $S = -R^*$. Defining the upper off-diagonal entry as $R(x) = i\sqrt{1-x^2}Q(x)$, we obtain $S(x) = -R^*(x) = i\sqrt{1-x^2}Q^*(x)$.

It can be easily shown that these polynomials satisfy the following properties:

- $\deg(P) \leq d$ and $\deg(Q) \leq d-1$,
- P has parity $d \bmod 2$ and Q has parity $(d-1) \bmod 2$,
- $|P(x)|^2 + (1-x^2)|Q(x)|^2 = 1$

The final equality is the unitarity constraint, which arises directly from the requirement that the determinant of an $\mathrm{SU}(2)$ matrix must equal 1 [10, 3].

Because the input parameter x is real-valued, $P(x)$ is an ordinary polynomial in x of degree at most d with definite parity. The definite parity reflects the physical symmetry of the alternating rotations: an even d sequence produces an even polynomial P containing only even powers of x, while an odd sequence produces an odd polynomial containing only odd powers of x in P.

There has been extensive work on QSP, and further generalization to multi-qubit systems, known as Quantum Singular Value Transformation (QSVT). For the scope of this thesis, we do not need to go into the details of QSVT. For simplicity, let us consider the multi-qubit case on quantum amplitude amplification.

2.2 Quantum Amplitude Amplification (QAA)

Amplitude amplification [11] can be accepted as a generalization of Grover's search algorithm. The idea is to amplify the amplitude of desired states (could be referred as "solutions" in Grover's analogy) in a larger Hilbert space, such that upon measurement, the probability of obtaining the desired information is increased. The main results of this thesis will be based on a similar construction of this section.

Suppose we have access to a unitary operator U and its inverse $U^\dagger$, acting on an arbitrary number of qubits. Consider two arbitrary normalized states, $|A\rangle$ and $|B\rangle$. The state $U|B\rangle$ generally has a non-zero component along $|A\rangle$ and another component perpendicular to $|A\rangle$. Defining the overlap amplitude as:

$$a = \langle A|U|B\rangle\,, \tag{2.8}$$

any relative phase in this inner product can be absorbed into the definition of $|A\rangle$ (or $|B\rangle$) without loss of generality, so we consider a to be real. We then define the normalized state perpendicular to $|A\rangle$ as:

$$|A^{\perp}\rangle = \frac{1}{\sqrt{1-a^2}}(I - |A\rangle\langle A|)U|B\rangle\,. \tag{2.9}$$

With this definition, the action of U on $|B\rangle$ is:

$$U|B\rangle = a|A\rangle + \sqrt{1-a^2}\,|A^{\perp}\rangle\,. \tag{2.10}$$

Similarly, considering the action of the adjoint operator $U^{\dagger}$ on $|A\rangle$, we can define a normalized state $|B^{\perp}\rangle$ orthogonal to $|B\rangle$ ($\langle B|B^{\perp}\rangle = 0$) such that:

$$U^{\dagger}|A\rangle = a|B\rangle + \sqrt{1-a^2}\,|B^{\perp}\rangle\,, \tag{2.11}$$

where $|B^{\perp}\rangle = \frac{1}{\sqrt{1-a^2}}(I - |B\rangle\langle B|)U^{\dagger}|A\rangle$.

Since unitarity requires $U|B^{\perp}\rangle$ to be orthonormal to $U|B\rangle$, we have

$$U|B^{\perp}\rangle = \sqrt{1-a^2}\,|A\rangle - a|A^{\perp}\rangle\,. \tag{2.12}$$

Although U is an arbitrary unitary which may act on a larger Hilbert space, its action within the two-dimensional subspaces spanned by $\{|B\rangle, |B^{\perp}\rangle\}$ and $\{|A\rangle, |A^{\perp}\rangle\}$ can be represented as[12]:

$$U = \begin{array}{c} \\ |A\rangle \\ |A^{\perp}\rangle \end{array} \begin{array}{c} \begin{array}{cc} |B\rangle & |B^{\perp}\rangle \end{array} \\ \begin{bmatrix} a & \sqrt{1-a^2} \\ \sqrt{1-a^2} & -a \end{bmatrix} \end{array}. \tag{2.13}$$

In this setting, our special interest is the state $|A\rangle$, and by applying a sequence of operations, our algorithmic goal is to amplify the amplitude a such that:

$$|a'| = |\langle A| U_{\text{algorithm}} |B\rangle| \to 1. \tag{2.14}$$

This new representation of U is a map between the subspace spanned by $\{|B\rangle, |B^{\perp}\rangle\}$ and the subspace spanned by $\{|A\rangle, |A^{\perp}\rangle\}$. With the constructed 2-dimensional representation of U, our goal is to apply the defined QSP framework to amplify the amplitude a. Now what we need is to somehow construct the signal operator $W(a)$ and the signal processing operator $S(\phi)$ in a similar fashion to the previous section.

First, observe that this two-dimensional submatrix of U can be decomposed into a sequence of standard QSP operators as:

$$\begin{aligned}
\begin{bmatrix} a & \sqrt{1-a^2} \\ \sqrt{1-a^2} & -a \end{bmatrix} &= -iS(\pi/4)W(a)S(\pi/4) \\
&= -i \begin{bmatrix} e^{i\pi/4} & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix} \begin{bmatrix} a & i\sqrt{1-a^2} \\ i\sqrt{1-a^2} & a \end{bmatrix} \begin{bmatrix} e^{i\pi/4} & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix} \\
&= -i \begin{bmatrix} e^{i\pi/2}a & i\sqrt{1-a^2} \\ i\sqrt{1-a^2} & e^{-i\pi/2}a \end{bmatrix} \\
&= -i \begin{bmatrix} ia & i\sqrt{1-a^2} \\ i\sqrt{1-a^2} & -ia \end{bmatrix} \\
&= \begin{bmatrix} a & \sqrt{1-a^2} \\ \sqrt{1-a^2} & -a \end{bmatrix}.
\end{aligned} \tag{2.15}$$

Notice that this matrix represents a reflection operator, which is chosen because amplitude amplification algorithms rely on alternating reflections to boost the target amplitude.

Now, let us assume that we also have access to some special unitary operators $S_{\mathrm{A}}(\phi) = e^{i\phi|A\rangle\langle A|}$ and $S_{\mathrm{B}}(\phi) = e^{i\phi|B\rangle\langle B|}$. It is somewhat trivial to see that the operators $S_{\mathrm{A}}(\phi)$ and $S_{\mathrm{B}}(\phi)$ are equivalent to the signal processing operator $S(\phi)$ with a global phase in the 2-dimensional subspace spanned by $\{|A\rangle, |A^{\perp}\rangle\}$ and $\{|B\rangle, |B^{\perp}\rangle\}$ respectively:

$$S_{\mathrm{A}}(\phi) = \begin{array}{c} \\ |A\rangle \\ |A^{\perp}\rangle \end{array} \begin{array}{c} \begin{array}{cc} |A\rangle & |A^{\perp}\rangle \end{array} \\ \begin{bmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{bmatrix} \end{array} = e^{i\phi/2} \begin{bmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{bmatrix} = e^{i\phi/2} S(\phi/2) \tag{2.16}$$

We now have expressed the action of U in terms of mapping between two subspaces as signal operator, and our special unitary operators $S_{\mathrm{A}}(\phi)$ and $S_{\mathrm{B}}(\phi)$ as signal processing operators.

Now, for simplicity, look at the top left block of our 2-dimensional representation. The convenience of this will be used in our result section, in which we define the initial state as $|B\rangle$ and the target state as $|A\rangle$. Therefore, for binary measurement problems it will be sufficient to look at the following amplitude:

$$a' = \langle A| S_{\mathrm{A}}(\phi_0) U S_{\mathrm{B}}(\phi_1) U^{\dagger} \dots U S_{\mathrm{B}}(\phi_{d-1}) U^{\dagger} S_{\mathrm{A}}(\phi_d) U |B\rangle \tag{2.17}$$

where the final state is in $|A\rangle$ subspace for odd d.

We can now observe that this two-dimensional submatrix is Hermitian. By using the above defined signal operator in terms of $W(a)$ and signal processing operators in terms of $S(\phi)$, we can rewrite the above amplitude similar to the previous section as:

$$a' = \langle A| S(\phi'_0) \prod_{j=1}^{d} W(a) S(\phi'_j) |B\rangle \tag{2.18}$$

Here the angles ϕ'_j are compactly defined as linear combinations of the angles ϕ_j and the phases we have extracted while rewriting the operators to show equivalence to the QSP framework.

Using Eq. (2.4), we can now express the amplitude as a polynomial transformation

of the initial amplitude a. Since we have defined U and $U^\dagger$ as a map between two subspaces, depending on which subspace we end with (assuming we start with the particular state $|B\rangle$), we need to define odd and even degree polynomials separately.

For an odd number of unitary operations:

$$\langle A| S_{\mathrm{A}}(\phi_0) \left[\prod_{j=1}^{\frac{d-1}{2}} U S_{\mathrm{B}}(\phi_{2j-1}) U^\dagger S_{\mathrm{A}}(\phi_{2j}) \right] U |B\rangle = P(a) \tag{2.19}$$

where $P(a)$ is an odd degree polynomial in $a = \langle A| U |B\rangle$, satisfying the conditions defined in the previous section.

Similarly, for an even number of operations:

$$\langle B| S_{\mathrm{B}}(\phi_0) \left[\prod_{j=1}^{\frac{d}{2}} U^\dagger S_{\mathrm{A}}(\phi_{2j-1}) U S_{\mathrm{B}}(\phi_{2j}) \right] |B\rangle = P(a) \tag{2.20}$$

where $P(a)$ is an even degree polynomial in $a = \langle A| U |B\rangle$, satisfying the conditions defined in the previous section.

2.3 Analysis of Low-Degree Solutions

To better understand how these polynomial transformations behave under alternating rotations, let us look at the simplest cases for small values of d.

For $d = 0$, no signal operator is applied, and the sequence consists only of the initial phase shift:

$$U_0(x) = S(\phi_0) = \begin{bmatrix} e^{i\phi_0} & 0 \\ 0 & e^{-i\phi_0} \end{bmatrix} \tag{2.21}$$

This gives $P(x) = e^{i\phi_0}$ and $Q(x) = 0$. Here, $P(x)$ is a constant polynomial of degree 0 with even parity, satisfying $|P(x)|^2 = 1$.

For $d = 1$, we apply a single signal operator:

$$\begin{aligned} U_1(x) &= S(\phi_0)W(x)S(\phi_1) \\ &= \begin{bmatrix} e^{i\phi_0} & 0 \\ 0 & e^{-i\phi_0} \end{bmatrix} \begin{bmatrix} x & i\sqrt{1-x^2} \\ i\sqrt{1-x^2} & x \end{bmatrix} \begin{bmatrix} e^{i\phi_1} & 0 \\ 0 & e^{-i\phi_1} \end{bmatrix} \\ &= \begin{bmatrix} e^{i(\phi_0+\phi_1)}x & i\sqrt{1-x^2}e^{i(\phi_0-\phi_1)} \\ i\sqrt{1-x^2}e^{-i(\phi_0-\phi_1)} & e^{-i(\phi_0+\phi_1)}x \end{bmatrix} \end{aligned} \tag{2.22}$$

Here, $P(x) = e^{i(\phi_0+\phi_1)}x$, which is a degree 1 polynomial with odd parity, while $Q(x) = e^{i(\phi_0-\phi_1)}$ has degree 0 with even parity. The unitarity condition is satisfied since $|P(x)|^2 + (1-x^2)|Q(x)|^2 = x^2 + (1-x^2) = 1$.

For $d = 2$, we have two signal operators separated by an intermediate phase shift:

$$U_2(x) = S(\phi_0)W(x)S(\phi_1)W(x)S(\phi_2) \tag{2.23}$$

First evaluating the product $W(x)S(\phi_1)W(x)$:

$$\begin{aligned} W(x)S(\phi_1)W(x) &= \begin{bmatrix} x & i\sqrt{1-x^2} \\ i\sqrt{1-x^2} & x \end{bmatrix} \begin{bmatrix} e^{i\phi_1} & 0 \\ 0 & e^{-i\phi_1} \end{bmatrix} \begin{bmatrix} x & i\sqrt{1-x^2} \\ i\sqrt{1-x^2} & x \end{bmatrix} \\ &= \begin{bmatrix} x^2e^{i\phi_1} - (1-x^2)e^{-i\phi_1} & i\sqrt{1-x^2}x(e^{i\phi_1} + e^{-i\phi_1}) \\ i\sqrt{1-x^2}x(e^{i\phi_1} + e^{-i\phi_1}) & x^2e^{-i\phi_1} - (1-x^2)e^{i\phi_1} \end{bmatrix} \end{aligned} \tag{2.24}$$

Multiplying by the outer phase shifts $S(\phi_0)$ and $S(\phi_2)$, the polynomial $P(x)$ becomes:

$$P(x) = e^{i(\phi_0+\phi_2)}\left[x^2e^{i\phi_1} - (1-x^2)e^{-i\phi_1}\right] \tag{2.25}$$

Since x is real-valued, $P(x)$ is an even polynomial in x of degree 2.

If we choose the phases as $\phi_1 = \pi$ and $\phi_0 + \phi_2 = 0$, this simplifies to:

$$P(x) = -x^2 + (1 - x^2) = 1 - 2x^2 = -(2x^2 - 1) \tag{2.26}$$

which is the second Chebyshev polynomial of the first kind, $P(x) = -T_2(x)$. This shows that specific choices of phase angles directly yield Chebyshev polynomials, which we examine for general d in the next section.

2.4 Chebyshev Polynomial Solutions

In the literature, polynomial approximations are usually used to design quantum algorithms for various problems, which we have called $P(x)$ in previous sections. In this work, we will not be using any approximations, but rather exact solutions. We will show that there exists a second polynomial, $Q(x)$, which satisfies the constraints in Section 2.1.

The Chebyshev polynomials of the first kind $T_n(x)$ and second kind $U_n(x)$ are defined [13] for $x \in [-1, 1]$ using sine and cosine functions as:

$$T_n(\cos\theta) = \cos(n\theta) \tag{2.27}$$

and

$$U_n(\cos\theta)\sin\theta = \sin((n+1)\theta) \tag{2.28}$$

These polynomials have several properties that match our requirements:

- $T_d(x)$ has degree d and parity $d \bmod 2$.
- $U_{d-1}(x)$ has degree $d - 1$ and parity $(d - 1) \bmod 2$.

- For all $x \in [-1, 1]$, $|T_d(x)| \leq 1$.

To show that Chebyshev polynomials provide an exact solution, we set $P(x) = T_d(x)$ and $Q(x) = U_{d-1}(x)$. Substituting these into the unitarity condition from Section 2.1:

$$\begin{aligned} |P(x)|^2 + (1 - x^2)|Q(x)|^2 &= 1 \\ T_d^2(x) + (1 - x^2)U_{d-1}^2(x) &= 1 \end{aligned} \tag{2.29}$$

Using the substitution $x = \cos\theta$, so that $1 - x^2 = \sin^2\theta$, the left-hand side becomes:

$$\begin{aligned} \cos^2(d\theta) + \sin^2\theta \left(\frac{\sin(d\theta)}{\sin\theta}\right)^2 &= \cos^2(d\theta) + \sin^2(d\theta) \\ &= 1 \end{aligned} \tag{2.30}$$

which holds identically for all $x \in [-1, 1]$ and all integers $d \geq 1$.

Therefore, choosing $P(x) = T_d(x)$ satisfies the degree, parity, and unitarity conditions without requiring any approximation.

Setting all intermediate phase angles to zero ($\phi_j = 0$) sets $S(0) = I$, reducing the sequence to $W(x)^d$. Writing $W(x) = e^{i\theta\sigma_x}$ where $x = \cos\theta$, we have:

$$W(x)^d = e^{id\theta\sigma_x} = \begin{bmatrix} \cos(d\theta) & i\sin(d\theta) \\ i\sin(d\theta) & \cos(d\theta) \end{bmatrix} = \begin{bmatrix} T_d(x) & i\sqrt{1-x^2}U_{d-1}(x) \\ i\sqrt{1-x^2}U_{d-1}(x) & T_d(x) \end{bmatrix}. \tag{2.31}$$

Thus, setting $\vec{\phi} = \vec{0}$ directly generates the Chebyshev polynomial $T_d(x)$ [5]. More generally, the fundamental theorem of QSP guarantees that a valid phase sequence exists for any target polynomial satisfying the parity and unitarity constraints, which can be computed efficiently using numerical phase-finding algorithms [14, 15, 16].

Chebyshev polynomials are also well-suited for our algorithmic purpose because they oscillate strictly between -1 and $+1$ on the interval $x \in [-1, 1]$. In the following

chapters, we will use this property to map the solution counts of Boolean functions directly to the roots and extrema of $T_d(x)$, allowing us to achieve deterministic function discrimination.

CHAPTER 3

FUNCTION ORACLES AND PROMISE PROBLEMS

3.1 Formulation of the Function Oracle

The use of function oracles allows us to abstract and generalize the problem. By treating the evaluation of a function as a black-box operation, we can study the fundamental query complexity of an algorithm independently of the specific physical implementation of the function itself.

Throughout this thesis, we consider a two-valued, or binary-valued, Boolean function:

$$f : \{1, 2, \ldots, N\} \to \{0, 1\} \tag{3.1}$$

where N is a positive integer representing the size of the input domain.

3.1.1 Generalized Phase Oracles

In the quantum computing literature [17], an oracle is typically implemented as a unitary operator acting on two registers: an input register $|x\rangle$ and an auxiliary result register $|y\rangle$. The standard oracle U_f acts as:

$$U_f \, |x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle \tag{3.2}$$

where $\oplus$ denotes addition modulo M, and the auxiliary register has dimension M.

To encode the function values into the relative phases of the input register, we prepare the auxiliary register in a Fourier basis state. Let $|y_0\rangle$ be a computational basis state of

the M-dimensional auxiliary space. The discrete Fourier transform of $|y_0\rangle$ is defined as:

$$F_t |y_0\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} e^{i\frac{2\pi}{M} y_0 j} |j\rangle \tag{3.3}$$

Applying the oracle U_f to the state $|x\rangle \otimes F_t |y_0\rangle$:

$$\begin{aligned} U_f \left(|x\rangle \otimes F_t |y_0\rangle\right) &= U_f \left(|x\rangle \otimes \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} e^{i\frac{2\pi}{M} y_0 j} |j\rangle \right) \\ &= |x\rangle \otimes \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} e^{i\frac{2\pi}{M} y_0 j} |j \oplus f(x)\rangle \\ &= e^{-i\frac{2\pi}{M} y_0 f(x)} |x\rangle \otimes F_t |y_0\rangle \end{aligned} \tag{3.4}$$

This transformation demonstrates the standard phase-kickback mechanism: the evaluation of the function on the auxiliary register induces a state-dependent phase shift on the input register, while the auxiliary state $F_t |y_0\rangle$ remains unchanged.

3.1.2 Standard Phase-Kickback Oracle

For binary Boolean functions ($M = 2$), the auxiliary register consists of a single qubit with basis states $\{|0\rangle, |1\rangle\}$. Choosing the initial auxiliary state as $F_t |1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, the action of the oracle becomes:

$$\begin{aligned} U_f |x\rangle \otimes |-\rangle &= |x\rangle \otimes \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \\ &= (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ &= (-1)^{f(x)} |x\rangle \otimes |-\rangle \end{aligned} \tag{3.5}$$

Since the auxiliary qubit remains invariant in the state $|-\rangle$, it can be factored out of the subsequent analysis. We therefore represent the oracle solely by its action on the input space:

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle \quad \text{for } x \in \{1, 2, \ldots, N\} \tag{3.6}$$

This is the standard phase oracle formulation used throughout algorithms such as Grover's search and the Deutsch-Jozsa problem.

3.2 Promise Problems

The problem of function discrimination can be framed as a promise problem. In a promise problem, we are given black-box oracle access to an unknown function f, with the guarantee (or "promise") that f belongs to a specific subset of all possible functions. Our algorithmic goal is to determine which of these predefined sets f belongs to using as few oracle queries as possible.

Let our search space be $X = \{1, 2, \ldots, N\}$. For any Boolean function $f : X \to \{0, 1\}$, we define its solution set S_f as the collection of inputs for which the function evaluates to 1:

$$S_f = \{x \in X \mid f(x) = 1\} \tag{3.7}$$

The total number of solutions is given by the cardinality $r = |S_f|$.

In this thesis, we focus on the promise problem where the function is guaranteed to belong to one of two predefined families characterized by their solution counts:

$$\mathcal{F}_1 = \{f : X \to \{0, 1\} \mid |S_f| = r_1\} \tag{3.8}$$

$$\mathcal{F}_2 = \{f : X \to \{0, 1\} \mid |S_f| = r_2\} \tag{3.9}$$

where $r_1, r_2 \in \{0, 1, \ldots, N\}$ and $r_1 \neq r_2$. The promise is that $f \in \mathcal{F}_1 \cup \mathcal{F}_2$, and our objective is to determine whether $f \in \mathcal{F}_1$ or $f \in \mathcal{F}_2$.

3.3 The Deutsch-Jozsa Problem as a Promise Problem

The Deutsch-Jozsa algorithm [2] is the earliest example of a quantum promise problem admitting an exact, deterministic speedup over classical algorithms. In our notation, the problem is defined over an input domain of size N, with the promise that the

function is either constant or balanced:

$$r = \begin{cases} 0 \text{ or } N & \text{if } f \text{ is constant} \\ N/2 & \text{if } f \text{ is balanced} \end{cases} \tag{3.10}$$

The standard algorithm solves this problem using a single evaluation of the oracle U_f:

- Initialize the system in an equal superposition state:

$$|B\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle \tag{3.11}$$

- Apply the phase oracle U_f.

- Measure the state in the basis $\{|A\rangle, |A^{\perp}\rangle\}$, where $|A\rangle = \frac{1}{\sqrt{N}} \sum_{j=1}^{N} |j\rangle$.

- If the outcome is $|A\rangle$, the function is constant; if the outcome is in the orthogonal subspace, it is balanced.

To see why this single query succeeds deterministically, we evaluate the overlap amplitude $a = \langle A| U_f |B\rangle$:

$$\begin{aligned} a &= \langle A| U_f |B\rangle \\ &= \left(\frac{1}{\sqrt{N}} \sum_{j=1}^{N} \langle j| \right) U_f \left(\frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle \right) \\ &= \frac{1}{N} \sum_{j=1}^{N} \sum_{i=1}^{N} \langle j|i\rangle \, (-1)^{f(i)} \\ &= \frac{1}{N} \sum_{i=1}^{N} (-1)^{f(i)} \\ &= \frac{1}{N}(N - 2r) = 1 - 2\frac{r}{N} \end{aligned} \tag{3.12}$$

Evaluating this amplitude under the Deutsch-Jozsa promise yields:

$$a = \begin{cases} 1 & \text{if } r = 0 \text{ (constant 0)} \\ -1 & \text{if } r = N \text{ (constant 1)} \\ 0 & \text{if } r = N/2 \text{ (balanced)} \end{cases} \tag{3.13}$$

Because the overlap amplitude a already takes the extremal values ± 1 (measurement probability $|a|^2 = 1$) or 0 (measurement probability $|a|^2 = 0$), no amplitude amplification is required. The single query ($d = 1$) distinguishes the two sets with 100% certainty.

For arbitrary r_1 and r_2, the amplitude $a = 1 - 2r/N$ is generally not equal to 0 or ± 1. Therefore, a single query cannot determine which set the function belongs to deterministically. In this case, we need to amplify the amplitude so that we can distinguish the two sets with certainty. In the next chapter, we show how this can be achieved using Quantum Signal Processing and Chebyshev polynomials.

CHAPTER 4

FUNCTION DISCRIMINATION VIA QUANTUM SIGNAL PROCESSING

4.1 General Formulation of Function Discrimination

Let us first set up the function discrimination problem within our quantum framework. As formulated in Chapter 3, we consider the promise problem where an unknown Boolean function f, accessed via the phase oracle $U_f |x\rangle = (-1)^{f(x)} |x\rangle$, is guaranteed to belong to either $\mathcal{F}_1$ (with r_1 solutions) or $\mathcal{F}_2$ (with r_2 solutions).

We define the initial state $|B\rangle$ and measurement state $|A\rangle$ in an arbitrary complete orthonormal basis, abstracted into the computational basis:

$$|A\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle , \quad |B\rangle = \sum_{i=1}^{N} \beta_i |i\rangle . \tag{4.1}$$

Let us look at the amplitude we are interested in under the action of the oracle U_f:

$$\begin{aligned} a &= \langle A| U_f |B\rangle \\ &= \sum_i \alpha_i^* \beta_i (-1)^{f(i)} \\ &= \sum_i c_i (-1)^{f(i)}, \end{aligned} \tag{4.2}$$

where $c_i = \alpha_i^* \beta_i$.

Here we have the freedom to choose c_i depending on the problem. Since we consider distinguishing between two sets of functions with fixed numbers of solutions, we

choose $c_i = c$ such that it is constant for each input. The reason is that we need the algorithm to be permutation symmetric with respect to solutions. Therefore, we can rewrite the amplitude as:

$$\begin{aligned} a &= c\sum_{i=1}^{N}(-1)^{f(i)} \\ &= c(N-2r). \end{aligned} \tag{4.3}$$

Since each promise set contains all combinations of functions with r_1 and r_2 solutions respectively, we have two possible values for our amplitude of interest:

$$a_1 = c(N-2r_1), \quad a_2 = c(N-2r_2). \tag{4.4}$$

Our goal is to construct and execute an algorithm $U_{\text{algorithm}}$ using the function oracle U_f acting on the initial state $|B\rangle$ and measure in the basis $\{|A\rangle, |A^{\perp}\rangle\}$ such that we can distinguish between a_1 and a_2:

$$\begin{aligned} P_1 &= |\langle A| U_{\text{algorithm}} |B\rangle|^2 \to 1, \\ P_2 &= |\langle A| U_{\text{algorithm}} |B\rangle|^2 \to 0, \end{aligned} \tag{4.5}$$

where P_1 corresponds to the probability if the function is in $\mathcal{F}_1$ and P_2 corresponds to the probability if the function is in $\mathcal{F}_2$.

4.2 Function Discrimination via QSP

Let us first look at the states $|A\rangle$ and $|B\rangle$. We know that

$$\langle A|A\rangle = \sum_{i=1}^{N} |\alpha_i|^2 = 1 \quad \text{and} \quad \langle B|B\rangle = \sum_{i=1}^{N} |\beta_i|^2 = 1 \tag{4.6}$$

We can use Cauchy-Schwarz Inequality to bound $c_i = \alpha_i^* \beta_i$ such that

$$\begin{aligned}\sum_{i=1}^{N}|c_i| &= \sum_{i=1}^{N}|\alpha_i^*\beta_i| \\ &= \sum_{i=1}^{N}|\alpha_i||\beta_i| \\ &\leq \sqrt{\sum_{i=1}^{N}|\alpha_i|^2}\sqrt{\sum_{i=1}^{N}|\beta_i|^2} = 1\end{aligned} \tag{4.7}$$

For the problem at hand we have explained previously that we chose c_i such that it is constant for all inputs i.e $c_i = c$. Then for the bound on c we have

$$|c| \leq \frac{1}{N} \tag{4.8}$$

Let us first consider that we have prepared the states $|A\rangle$ and $|B\rangle$ the same way in Deutsch-Jozsa algorithm. We choose $c = 1/N$ to maximize a. In that case we have equal superposition for both states. Looking at the amplitude of interest a we have

$$a = \frac{1}{N}(N - 2r) = 1 - 2\frac{r}{N} \tag{4.9}$$

Now we have our amplitude of interest as well as the initial and measurement states. Let us now construct the problem in the framework of QSP. Previously, we have proved that there exists $\vec{\phi}$ such that through consecutive applications of U_f and $S(\phi)$ we can apply a Chebyshev polynomial transformation on a.

Let the number of function evaluations be t and transformed amplitude be a'. Since the problem is essentially a decision problem between two possible sets, we set the target amplitude to be ± 1 for one case and 0 for the other one.

$$a'_1 = T_t(\cos(\theta_1)) = \pm 1 \quad \text{and} \quad a'_2 = T_t(\cos(\theta_2)) = 0 \tag{4.10}$$

where $\cos(\theta_i) = a_i$ and $\sin^2(\frac{\theta_i}{2}) = \frac{r_i}{N}$.

Start by the amplitude we want to amplify to ± 1. i.e. $a'_1 = \pm 1$

$$\begin{aligned} T_t(\cos(\theta_1)) &= \cos(t\theta_1) = \pm 1 \\ t\theta_1 &= k\pi \end{aligned} \tag{4.11}$$

where $k = 0, 1, 2, \ldots$

Looking at the other amplitude

$$\begin{aligned} T_t(\cos(\theta_2)) &= \cos(t\theta_2) = 0 \\ t\theta_2 &= \frac{\pi}{2} + k'\pi \end{aligned} \tag{4.12}$$

We want to know the lowest number of function evaluations to distinguish between two sets. Substitute Eq. (4.11) into Eq. (4.12)

$$\begin{aligned} t\theta_2 - t\theta_1 &\geq \frac{\pi}{2} \\ t(\theta_2 - \theta_1) &\geq \frac{\pi}{2} \\ t &\geq \frac{\pi}{2(\theta_2 - \theta_1)}. \end{aligned} \tag{4.13}$$

Therefore, the minimum number of queries required scales as:

$$t = \left\lceil \frac{\pi}{2(\theta_2 - \theta_1)} \right\rceil. \tag{4.14}$$

We have defined t to be the number of evaluations, which is naturally a positive integer. Therefore, we can simply take the absolute value of the difference between the angles θ_1 and θ_2:

$$t = \left\lceil \frac{\pi}{2|\theta_2 - \theta_1|} \right\rceil \tag{4.15}$$

From our earlier definition, we know that $\sin^2(\frac{\theta_i}{2}) = \frac{r_i}{N}$. Let us define the fraction of solutions in the search space as $p_i = \frac{r_i}{N}$. The exact relation for the phase angle is then:

$$\theta_i = 2\arcsin\left(\sqrt{p_i}\right) = 2\arcsin\left(\sqrt{\frac{r_i}{N}}\right) \tag{4.16}$$

Substituting this relation back into Eq. (4.15), we obtain the exact analytical bound for the required number of function evaluations to distinguish the two sets:

$$t = \left\lceil \frac{\pi}{4\left|\arcsin\left(\sqrt{\frac{r_2}{N}}\right) - \arcsin\left(\sqrt{\frac{r_1}{N}}\right)\right|} \right\rceil \tag{4.17}$$

Let us examine this result in two limits. First, consider the case where the number of solutions is very small ($r_i \ll N$). Here, p_i is close to zero, so we can use the approximation $\arcsin(x) \approx x$. The number of evaluations simplifies to:

$$t \approx \frac{\pi\sqrt{N}}{4|\sqrt{r_2} - \sqrt{r_1}|} \tag{4.18}$$

If we distinguish a function with no solutions ($r_1 = 0$) from a function with exactly one solution ($r_2 = 1$), this yields $t \approx \frac{\pi}{4}\sqrt{N}$. This exactly matches the $\mathcal{O}(\sqrt{N})$ query complexity of Grover's algorithm [18].

Next, let us look at the limit where the two sets have a nearly identical number of solutions ($r_2 = r_1 + \Delta r$, with $\Delta r \ll r_1$). We can approximate the denominator using a first-order Taylor expansion:

$$\begin{aligned} \arcsin\left(\sqrt{p + \Delta p}\right) - \arcsin\left(\sqrt{p}\right) &\approx \frac{d}{dp}\Big(\arcsin(\sqrt{p})\Big)\Delta p \\ &= \frac{\Delta p}{2\sqrt{p(1-p)}} \end{aligned} \tag{4.19}$$

Substituting this approximation and translating back to r and N, the query complexity becomes:

$$t \approx \frac{\pi\sqrt{r(N-r)}}{2|\Delta r|} \tag{4.20}$$

Because the number of solutions is discrete, the minimum possible difference between the two sets is $|\Delta r| = 1$. Looking at Eq. (4.20), the maximum number of evaluations occurs when the search space is half-filled ($r = N/2$). In this worst-case scenario, the required number of evaluations scales as $\mathcal{O}(N)$. This shows that when the sets are dense and highly similar, the algorithm loses its quadratic speedup.

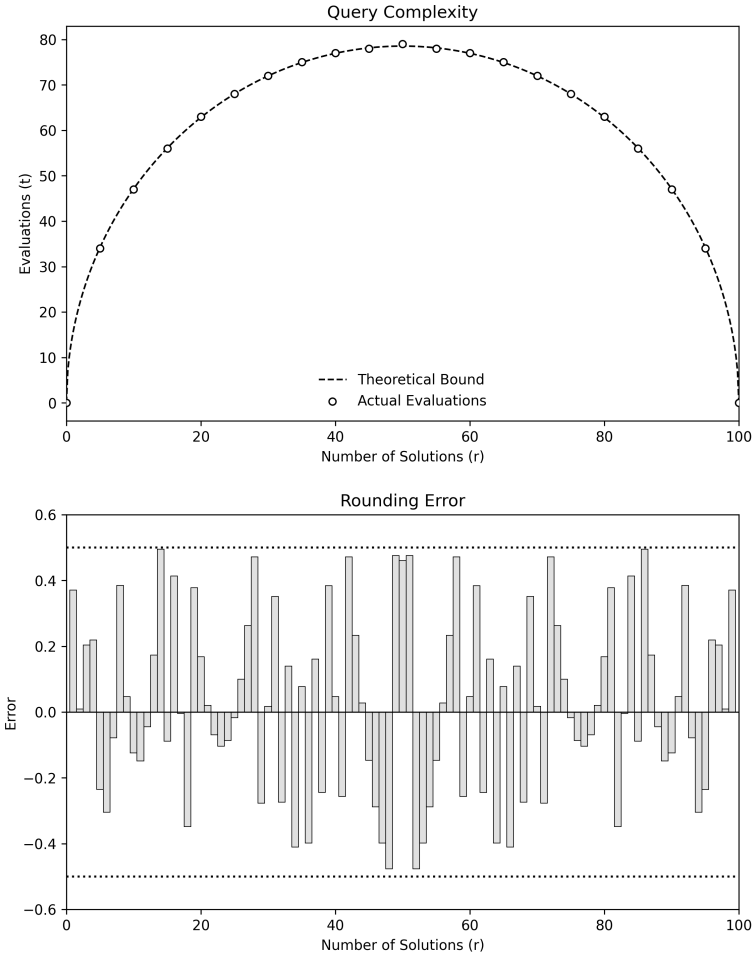

Figure 4.1: The required number of evaluations (top) and the corresponding rounding error (bottom) for distinguishing sets separated by $\Delta r = 1$, plotted for a search space of size $N = 100$. For clarity, the discrete evaluations are marked at intervals of 5.

There are two important limitations to this result. First, the derived number of evaluations t is rarely an exact integer. Because we must round t to the nearest integer to run the algorithm, the final measurement probability will be slightly less than 1, scaling with the fractional rounding error [19].

Second, due to our choice of states $|A\rangle$ and $|B\rangle$, the algorithm is symmetric. If a function has r_1 solutions, its amplitude is a_1. If a function has $r_{1,m} = N - r_1$ solutions, its amplitude becomes:

$$a_{1,m} = 1 - 2\frac{N - r_1}{N} = -1 + 2\frac{r_1}{N} = -a_1 \tag{4.21}$$

Because the QSP transformation yields the same measurement probability for symmetric amplitudes ($|P(-a_1)|^2 = |P(a_1)|^2$), the algorithm cannot distinguish between r_1 and $N - r_1$ solutions. Therefore, we require an additional promise that the number of solutions is restricted to either $r \leq N/2$ or $r \geq N/2$.

4.3 Function Discrimination with a Null Input

To overcome these two limitations, we introduce a null input state $|\star\rangle$, which is invariant under the action of the function oracle U_f. This state acts as an auxiliary state that is not evaluated by the oracle:

$$U_f |\star\rangle = |\star\rangle \tag{4.22}$$

We then prepare the initial state $|B\rangle$ and the measurement state $|A\rangle$ within this enlarged Hilbert space:

$$|B\rangle = \beta_\star |\star\rangle + \sum_{i=1}^{N} \beta_i |i\rangle \quad \text{and} \quad |A\rangle = \alpha_\star |\star\rangle + \sum_{i=1}^{N} \alpha_i |i\rangle \tag{4.23}$$

where the normalization conditions are:

$$|\alpha_\star|^2 + \sum_{i=1}^{N} |\alpha_i|^2 = 1 \quad \text{and} \quad |\beta_\star|^2 + \sum_{i=1}^{N} |\beta_i|^2 = 1 \tag{4.24}$$

Now, let us evaluate the initial amplitude of interest:

$$
\begin{aligned}
a &= \langle A| U_f |B\rangle \\
&= \left(\alpha_\star^* \langle\star| + \sum_{i=1}^{N} \alpha_i^* \langle i|\right) U_f \left(\beta_\star |\star\rangle + \sum_{j=1}^{N} \beta_j |j\rangle\right) \\
&= \alpha_\star^* \beta_\star + \sum_{i=1}^{N} \alpha_i^* \beta_i (-1)^{f(i)} \\
&= c_\star + \sum_{i=1}^{N} c_i (-1)^{f(i)}
\end{aligned}
\tag{4.25}
$$

where $c_\star = \alpha_\star^* \beta_\star$ and $c_i = \alpha_i^* \beta_i$.

As before, we require permutation symmetry across all computational inputs, so we choose $c_i = c$ for all $i \in \{1, 2, \ldots, N\}$. Using the Cauchy-Schwarz inequality, the sum of all product coefficients is bounded by:

$$
|c_\star| + \sum_{i=1}^{N} |c_i| = |\alpha_\star^* \beta_\star| + \sum_{i=1}^{N} |\alpha_i^* \beta_i| \leq \sqrt{|\alpha_\star|^2 + \sum_{i=1}^{N} |\alpha_i|^2} \sqrt{|\beta_\star|^2 + \sum_{i=1}^{N} |\beta_i|^2} = 1 \tag{4.26}
$$

Since we have chosen $c_i = c$ to be constant for all inputs, this directly yields $|c_\star| + |Nc| \leq 1$.

To maximize the overlap and preserve deterministic behavior, we saturate the inequality by choosing identical real and positive coefficients for state preparation ($\alpha_\star = \beta_\star$ and $\alpha_i = \beta_i = \sqrt{c}$). This fixes the relationship between the coefficients:

$$
c_\star + Nc = 1 \implies c_\star = 1 - Nc \tag{4.27}
$$

Notice that if $c = 1/N$, we have $c_\star = 0$, which corresponds to having no amplitude on the null state $|\star\rangle$, returning us to the standard QSP case. Because we assume a non-zero amplitude for the null state ($c_\star > 0$), the bound on c is strictly:

$$
c < \frac{1}{N} \tag{4.28}
$$

Substituting Eq. (4.27) back into the amplitude expression:

$$\begin{aligned} a &= c_\star + c(N - 2r) \\ &= (1 - Nc) + cN - 2rc \\ &= 1 - 2rc \end{aligned} \tag{4.29}$$

Now, let us examine how the null input resolves the two limitations of standard QSP.

First, consider the symmetry between r_1 and $N - r_1$. Under the modified amplitude $a = 1 - 2rc$, the amplitude for the complementary function with $N - r_1$ solutions is:

$$a_{1,m} = 1 - 2(N - r_1)c = 1 - 2Nc + 2r_1c \tag{4.30}$$

This is no longer equal to $-a_1 = -(1 - 2r_1c) = -1 + 2r_1c$, unless $c = 1/N$. For any choice of $c < 1/N$, the symmetry is broken:

$$a_{1,m} \neq -a_1 \tag{4.31}$$

Therefore, by preparation of the states such that $c < 1/N$, the algorithm can distinguish between r and $N - r$ solutions without requiring any additional promise.

Second, the parameter c can be continuously tuned within the interval $c \in (0, 1/N]$ to eliminate rounding errors. Recall from Section 4.2 that the required number of function evaluations to distinguish two angles θ_1 and θ_2 is:

$$t = \frac{\pi}{2|\theta_2 - \theta_1|} \tag{4.32}$$

where $\cos(\theta_i) = a_i = 1 - 2r_ic$. Using the trigonometric identity $1 - \cos(\theta_i) = 2\sin^2(\frac{\theta_i}{2})$, we have:

$$2\sin^2\left(\frac{\theta_i}{2}\right) = 2r_ic \implies \sin^2\left(\frac{\theta_i}{2}\right) = r_ic \tag{4.33}$$

Thus, the angles are directly parameterized by c:

$$\theta_i = 2\arcsin\left(\sqrt{r_i c}\right) \tag{4.34}$$

Substituting this relation back into the expression for t, we obtain:

$$t = \frac{\pi}{4\left|\arcsin\left(\sqrt{r_2 c}\right) - \arcsin\left(\sqrt{r_1 c}\right)\right|} \tag{4.35}$$

Because c is a continuous parameter that can be chosen freely in the range $(0, 1/N]$, the resulting query count $t(c)$ is a continuous function of c. Consequently, for any pair of solution counts r_1 and r_2, we can always select an exact value of c such that t is identically an integer:

$$t \in \mathbb{Z}^+ \tag{4.36}$$

This completely eliminates the rounding error, ensuring that the measurement probabilities $P_1 = 1$ and $P_2 = 0$ are exact. Thus, the algorithm distinguishes between the sets $\mathcal{F}_1$ and $\mathcal{F}_2$, which contain all combinations of functions with number of solutions r_1 and r_2 respectively, with deterministic certainty.

4.4 Single Evaluation Discrimination from the Zero-Solution Function

It is instructive to examine the regime where the quantum algorithm performs only a single evaluation of the function, $t = 1$. Consider the promise problem where one of the candidate sets has no solutions, i.e., $r_1 = 0$ and $r_2 > 0$. Using the null input construction, the amplitude is given by:

$$a_i = 1 - 2r_i c \tag{4.37}$$

where $c < \frac{1}{N}$ ensures a non-zero amplitude for the auxiliary null state $|\star\rangle$. For this problem, the amplitudes evaluate to $a_1 = 1$ and $a_2 = 1 - 2r_2 c$.

For a single query ($t = 1$), deterministic discrimination requires setting the transformed amplitude of the second set to zero ($a_2 = 0$), yielding:

$$\begin{aligned} 1 - 2r_2c &= 0 \\ r_2 &= \frac{1}{2c} > \frac{N}{2} \end{aligned} \tag{4.38}$$

where the strict inequality follows directly from the normalization constraint $c < \frac{1}{N}$.

This implies that any function with more than half of its domain evaluating to one ($r_2 > N/2$) can be deterministically distinguished from the zero-solution function in a single quantum evaluation. At the boundary where the null state amplitude vanishes ($c = 1/N$), this condition recovers $r_2 = N/2$, corresponding to the balanced function case resolved by the standard Deutsch-Jozsa algorithm.

4.5 Classical Query Complexity

To benchmark the algorithm with its classical counterpart, we determine the number of queries required to distinguish whether a Boolean function $f : \{1, 2, \ldots, N\} \to \{0, 1\}$ belongs to a set with r_1 solutions or a set with r_2 solutions. The deterministic classical solution is to evaluate f at every input. There could be cases where the answer would be achieved earlier, but we focus on the worst-case scenario for the query complexity. Therefore, the classical deterministic algorithm to distinguish between r_1 and r_2 takes $\mathcal{O}(N)$ queries.

To evaluate this, we consider a probabilistic sampling strategy. We assume that each query is independent and identically distributed (i.i.d.), meaning the function inputs are sampled with replacement. While a practical algorithm would remember previous evaluations and sample without replacement, this i.i.d. assumption simplifies the analysis. Furthermore, since our complexity analysis is concerned with large search space N, the probability of evaluating the same input twice is almost zero.

Suppose we evaluate t random samples $x_1, \ldots, x_t \in X$. Let p be the fraction of solutions in the search space:

$$p = \frac{r}{N}. \tag{4.39}$$

The fraction of solutions observed in our sample is:

$$p' = \frac{1}{t}\sum_{j=1}^{t} f(x_j), \tag{4.40}$$

which has variance:

$$\sigma'^2 = \frac{p(1-p)}{t}. \tag{4.41}$$

To distinguish between the two function sets with high probability (about 97.5%), the difference between the two possible fractions, Δ, must be at least $4\sigma'$:

$$\Delta = \frac{|r_1 - r_2|}{N}. \tag{4.42}$$

This gives:

$$\Delta \geq 4\sigma' = 4\sqrt{\frac{p(1-p)}{t}}. \tag{4.43}$$

Solving for the number of queries t:

$$t \geq \frac{16p(1-p)}{\Delta^2}. \tag{4.44}$$

Since $p(1-p) \leq \frac{1}{4}$ for any $p \in [0,1]$, the worst case gives:

$$t \geq \frac{4}{\Delta^2} = \frac{4N^2}{(r_1 - r_2)^2}. \tag{4.45}$$

This random sampling approach is only useful if the required number of queries t is strictly less than checking the entire space of size N. Therefore, sampling is effective only when:

$$\frac{N^2}{(r_1 - r_2)^2} < N \implies |r_1 - r_2| > \sqrt{N}. \tag{4.46}$$

If this condition does not hold (i.e., $|r_1 - r_2| \leq \sqrt{N}$), sampling requires more queries than simply checking all N inputs deterministically in the worst case.

CHAPTER 5

CONCLUSION

In this thesis, we have investigated a generalized version of the Deutsch-Jozsa promise problem through the framework of Quantum Signal Processing (QSP), formulating function discrimination as an amplitude amplification task. After establishing the QSP operator algebra and the unitary polynomial constraints, we showed that Chebyshev polynomials of the first kind naturally satisfy these requirements without relying on polynomial approximations. Consequently, we demonstrated that Chebyshev polynomials provide an exact algebraic foundation for constructing a deterministic algorithm.

When applying standard QSP to this generalized problem, two fundamental limitations arise. First, the theoretical number of oracle queries is rarely an exact integer, introducing rounding errors that prevent deterministic success. Second, the measurement probability is symmetric under the transformation $r \leftrightarrow N - r$, meaning that a standard QSP sequence cannot distinguish between a function with r solutions and its complement with $N - r$ solutions.

To resolve both limitations, we introduced an auxiliary null input state $|\star\rangle$ that remains invariant under the action of the function oracle. We showed that including this state breaks the $r \leftrightarrow N - r$ reflection symmetry whenever $c < 1/N$. Furthermore, the parameter c acts as a continuously tunable coefficient that allows us to set the required query count t to an exact integer, completely eliminating rounding errors and ensuring deterministic measurement outcomes. Because our investigation is formulated within the query complexity model, the analysis is centered on the number of oracle evaluations, while the detailed physical gate count for state preparation remains outside the primary scope of this work.

Finally, we derived the classical query complexities for both deterministic and probabilistic approaches to establish a baseline. Comparing these limits demonstrates that our quantum algorithm speeds up the function discrimination problem quadratically, achieving a query complexity equivalent to Grover's search algorithm. Ultimately, this study shows that we can lift the limitations of standard QSP while maintaining this optimal quadratic speedup.

Future research could explore the quantum circuits required to prepare the null state superposition on specific quantum hardware. Additionally, generalizing this framework to promise problems involving more than two solution sets presents an interesting direction for further study.

REFERENCES

[1] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, vol. 400, no. 1818, pp. 97–117, 1985.

[2] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, vol. 439, no. 1907, pp. 553–558, 1992.

[3] G. H. Low and I. L. Chuang, "Optimal Hamiltonian simulation by quantum signal processing," *Physical Review Letters*, vol. 118, no. 1, p. 010501, 2017.

[4] A. Gilyén, Y. Su, G. H. Low, and N. Wiebe, "Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pp. 193–204, 2019.

[5] J. M. Martyn, Z. M. Rossi, A. K. Tan, and I. L. Chuang, "Grand unification of quantum algorithms," *PRX Quantum*, vol. 2, no. 4, p. 040203, 2021.

[6] S. L. Braunstein, B.-S. Choi, S. Ghosh, and S. Maitra, "Exact quantum algorithm to distinguish boolean functions of different weights," *Journal of Physics A: Mathematical and Theoretical*, vol. 40, no. 29, p. 8441, 2007.

[7] B.-S. Choi and S. L. Braunstein, "Quantum algorithm for the asymmetric weight decision problem and its generalization to multiple weights," *Quantum Information Processing*, vol. 10, no. 2, pp. 177–188, 2011.

[8] K. Uyanık and S. Turgut, "Sure-success quantum algorithms on weight decision problem," 2013.

[9] X. He, X. Sun, G. Yang, and P. Yuan, "Exact quantum query complexity of weight

decision problems via chebyshev polynomials," *Science China Information Sciences*, vol. 66, no. 2, p. 129503, 2023.

[10] G. H. Low, V. Kliuchnikov, and I. L. Chuang, "Methodology of resonant transitions for implementing arbitrary unitary transformations of an arbitrary single qubit," *Physical Review A*, vol. 94, no. 5, p. 052314, 2016.

[11] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," *Contemporary Mathematics*, vol. 305, pp. 53–74, 2002.

[12] G. H. Low and I. L. Chuang, "Hamiltonian simulation by qubitization," *Quantum*, vol. 3, p. 163, 2019.

[13] J. C. Mason and D. C. Handscomb, *Chebyshev Polynomials*. Boca Raton, FL: Chapman and Hall/CRC, 2002.

[14] J. Haah, "Product decomposition of periodic functions in quantum signal processing," *Quantum*, vol. 3, p. 119, 2019.

[15] R. Chao, D. Ding, A. Gilyén, C. Huang, and M. Szegedy, "Finding angles for quantum signal processing with machine precision," *arXiv preprint arXiv:2003.02831*, 2020.

[16] Y. Dong, X. Meng, K. B. Whaley, and L. Lin, "Efficient phase-factor evaluation in quantum signal processing," *Physical Review A*, vol. 103, no. 4, p. 042419, 2021.

[17] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 10th anniversary ed., 2010.

[18] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC)*, pp. 212–219, 1996.

[19] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," *Fortschritte der Physik*, vol. 46, no. 4-5, pp. 493–505, 1998.