Enhanced Grover's algorithm solutions for active user detection in wireless networks

Muhammad Idham Habibie

N° d'ordre NNT : 2023ISAL0126

Thèse de doctorat de l'Université de Lyon

opérée au sein de

Institut National des Sciences Appliquées de Lyon

École Doctorale 160

Électronique, électrotechnique et automatique

Spécialité / Discipline de doctorat :

Traitement du Signal et de l'Image

Soutenue publiquement le 14/12/2023, par :

Muhammad Idham Habibie

Enhanced Grover's Algorithm Solutions for Active User Detection in Wireless Networks

---

Devant le jury composé de :

Duhamel Pierre	Directeur de recherche émérite	CNRS/CentraleSupelec	Examinateur
Fawzi Omar	Directeur de Recherche	ENS Lyon	Examinateur
Burel Gilles	Professeur des Universités	Université de Bretagne Occidentale	Rapporteur
Andriyanova Iryna	Professeure des Universités	Cergy Paris University	Rapporteuse
Goursaud Claire	Directrice de Thèse	INSA Lyon	Directrice

Département FEDORA – INSA Lyon - Ecoles Doctorales

SIGLE	ECOLE DOCTORALE	NOM ET COORDONNEES DU RESPONSABLE
ED 206 CHIMIE	**CHIMIE DE LYON** https://www.edchimie-lyon.fr Sec. : Renée EL MELHEM Bât. Blaise PASCAL, 3e étage secretariat@edchimie-lyon.fr	**M. Stéphane DANIELE** C2P2-CPE LYON-UMR 5265 Bâtiment F308, BP 2077 43 Boulevard du 11 novembre 1918 69616 Villeurbanne directeur@edchimie-lyon.fr
ED 341 E2M2	**ÉVOLUTION, ÉCOSYSTÈME, MICROBIOLOGIE, MODÉLISATION** http://e2m2.universite-lyon.fr Sec. : Bénédicte LANZA Bât. Atrium, UCB Lyon 1 Tél : 04.72.44.83.62 secretariat.e2m2@univ-lyon1.fr	**Mme Sandrine CHARLES** Université Claude Bernard Lyon 1 UFR Biosciences Bâtiment Mendel 43, boulevard du 11 Novembre 1918 69622 Villeurbanne CEDEX e2m2.codir@listes.univ-lyon1.fr
ED 205 EDISS	**INTERDISCIPLINAIRE SCIENCES-SANTÉ** http://ediss.universite-lyon.fr Sec. : Bénédicte LANZA Bât. Atrium, UCB Lyon 1 Tél : 04.72.44.83.62 secretariat.ediss@univ-lyon1.fr	**Mme Sylvie RICARD-BLUM** Laboratoire ICBMS - UMR 5246 CNRS - Université Lyon 1 Bâtiment Raulin - 2ème étage Nord 43 Boulevard du 11 novembre 1918 69622 Villeurbanne Cedex Tél : +33(0)4 72 44 82 32 sylvie.ricard-blum@univ-lyon1.fr
ED 34 EDML	**MATÉRIAUX DE LYON** http://ed34.universite-lyon.fr Sec. : Yann DE ORDENANA Tél : 04.72.18.62.44 yann.de-ordenana@ec-lyon.fr	**M. Stéphane BENAYOUN** Ecole Centrale de Lyon Laboratoire LTDS 36 avenue Guy de Collongue 69134 Ecully CEDEX Tél : 04.72.18.64.37 stephane.benayoun@ec-lyon.fr
ED 160 EEA	**ÉLECTRONIQUE, ÉLECTROTECHNIQUE, AUTOMATIQUE** https://edeea.universite-lyon.fr Sec. : Philomène TRECOURT Bâtiment Direction INSA Lyon Tél : 04.72.43.71.70 secretariat.edeea@insa-lyon.fr	**M. Philippe DELACHARTRE** INSA LYON Laboratoire CREATIS Bâtiment Blaise Pascal, 7 avenue Jean Capelle 69621 Villeurbanne CEDEX Tél : 04.72.43.88.63 philippe.delachartre@insa-lyon.fr
ED 512 INFOMATHS	**INFORMATIQUE ET MATHÉMATIQUES** http://edinfomaths.universite-lyon.fr Sec. : Renée EL MELHEM Bât. Blaise PASCAL, 3e étage Tél : 04.72.43.80.46 infomaths@univ-lyon1.fr	**M. Hamamache KHEDDOUCI** Université Claude Bernard Lyon 1 Bât. Nautibus 43, Boulevard du 11 novembre 1918 69 622 Villeurbanne Cedex France Tél : 04.72.44.83.69 direction.infomaths@listes.univ-lyon1.fr
ED 162 MEGA	**MÉCANIQUE, ÉNERGÉTIQUE, GÉNIE CIVIL, ACOUSTIQUE** http://edmega.universite-lyon.fr Sec. : Philomène TRECOURT Tél : 04.72.43.71.70 Bâtiment Direction INSA Lyon mega@insa-lyon.fr	**M. Jocelyn BONJOUR** INSA Lyon Laboratoire CETHIL Bâtiment Sadi-Carnot 9, rue de la Physique 69621 Villeurbanne CEDEX jocelyn.bonjour@insa-lyon.fr
ED 483 ScSo	**ScSo**[1] https://edsciencessociales.universite-lyon.fr Sec. : Mélina FAVETON Tél : 04.78.69.77.79 melina.faveton@univ-lyon2.fr	**M. Bruno MILLY** (INSA : J.Y. TOUSSAINT) Univ. Lyon 2 Campus Berges du Rhône 18, quai Claude Bernard 69365 LYON CEDEX 07 Bureau BEL 319 bruno.milly@univ-lyon2.fr

[1] ScSo : Histoire, Géographie, Aménagement, Urbanisme, Archéologie, Science politique, Sociologie, Anthropologie

To my wife, my son,
my parents, and the future generations

Contents

List of Figures

List of Tables

List of Algorithms

Acknowledgment

I would like to extend my gratitude and sincere appreciation goes to my supervisors, Claire Goursaud and Jihad Hamie, whose invaluable guidance made this achievement possible. The experience has been truly enriching, and I am grateful for the time spent with you.

I would also like to express my heartfelt thanks to my family, particularly Pratiwi Ayunintyas, Uwais Al-Fatih Habibie, Ratu Aida Dibyakti, Sudirman Habibie, Titi Haryati, Hartono, and my brothers and sisters whose constant support has been instrumental since the inception of my PhD journey. A special acknowledgment goes to the MARACAS Team, who not only provided insightful discussions but also became my companions throughout the entire thesis process.

I want to recognize fellow PhD students, Hery Zo, Jésus, and Dango, who joined me in discussions over the course of the year. As well as my colleagues Lélio, Pierre, Antoine, Théotime, Xiao, and Benoit from the bureau, whose mutual support has been invaluable. I must also express my gratitude to Linda, Claire Sauer, and Cecillia, whose patient guidance offered support during administrative matters in France. To the members of CETHIL Lab, Ibrahim, Majid, Baqeer, and Oksana, who have consistently engaged in discussions about our experiences in France. To Ilham Naharudinsyah, who provided me with mathematical support throughout my thesis.

To the members of Ibu-Ibu pengajian Al-Hijrah Lyon, including Ibu Poppy, Ibu Neni, Mbak Eka, Mas Fuady and family and countless others that I may not mention individually. I am deeply thankful for your unwavering support during Ramadan and challenging times. To PPI Lyon, thank you so much for the sharing and care.

I extend my gratitude to my fellow Indonesian PhD students, such as Mas Endarman and Mas Ibrahim, with whom I've shared discussions about completing our PhDs together. To Mas Rohib, your companionship has been a source of strength as we navigated similar challenges.

A special thank you to the former Maracas and CITI team members, Homa

Nikbakht, Naveed Ahmed, and Safuriyawu Ahmed, your contributions are greatly appreciated.

Abstract

The key features of 5G, such as Ultra-reliable low-latency communication (URLLC) and Massive Machine Type Communication (mMTC), are designed to address the need for low latency and the ability to connect a large number of devices. To support these requirements, mobile devices can transmit messages without explicit grants from the Base Station (BS) using a scheme called Grant-Free Random Access (GFRA). This Random Access (RA) scheme allows for the reduction of data overhead , resulting in reduced latency and is particularly useful for massive networks. Thus, the GFRA scheme requires the Base Station (BS) to detect active users in real-time, a process known as Active User Detection (AUD), which becomes essential in this scheme. The Maximum Likelihood (ML) method, recognized as the optimal approach for AUD, delivers the best performance but faces challenges due to high complexity and delays in detecting active users. In an effort to mitigate this complexity, alternatives such as Conventional Correlation Receiver (CCR) and Zero Forcing (ZF) can be used, yet they struggle to match the ML performance.

To overcome this, we can exploit quantum algorithms, and in particular Grover's algorithm. Grover's algorithm appears to have the potential in reducing the complexity thanks to the superposition of states, allowing to operate on both 0 and 1 simultaneously. While Grover's approach promises lower complexity, determining the optimal solution requires knowledge of two variables: the size of the database, denoted as K and the number of solutions, denoted as S. However, the number of solutions S is usually unknown to the BS. This leads to a new problem.

The second problem is that Grover's algorithm, when applied directly, such as using the function $f(x) = \delta$, where δ is the targeted solution and x is the targeted qubits, does not perform comparably to ML, instead, it is closer to CCR and ZF. To achieve the same level of performance as ML, Grover's algorithm needs to be modified. It is worth noting that ML operates by finding the minimum distance between two variables, which also inspired Grover's algorithm for finding the minimum distance.

Hence, these two problems have led to the development of a new solution called the Quantum Minimum Searching Algorithm (QMSA), which holds promise for finding the minimum value in a database. Both the Boyer-Brassard-Høyer-Tapp (BBHT) and Durr-Hoyer Algorithm (DHA) methods have addressed these problems, which serve upper-bound of $4.5\sqrt{2^N}$ and $22.5\sqrt{2^N}$ respectively, where N is the number of users. These algorithms are limited due to with their random testing of Grover's number of iterations, denoted as L, to test which iteration is optimal. It is tested from a very small value and increases to high value with a geometric sequence, which leads to high complexity. Thus, the algorithm still raise open research questions regarding the reduction of complexity and the development of more effective methods.

In our thesis, we adapt Grover's algorithm for application in the context of AUD. We conduct an analysis of its performance, considering success probability and complexity. Additionally, we propose a new algorithm, namely Improved Iterated Minimum Searching Algorithm (IIMSA), aiming at enhancing the existing BBHT and DHA methods to reduce their complexity while maintaining high performance. The idea behind this algorithm is to utilize a random number of solution, denoted as $\hat{S}$, to predict the closest number of solutions, rather than conducting L iterations based on a geometric progression distribution. The predicted $\hat{S}$ is used to determine the L_{opt} which is believed to be faster, where L_{opt} is the ideal number of iterations. To further reduce complexity, we also incorporate classical methods such as ZF and CCR to enhance their performance by determining the correct threshold to initiate the algorithms of DHA and IIMSA. We believe this approach holds promise for our proposal.

In a crucial aspect, we introduce an Enhanced Grover's algorithm inspired by a quantum-hybrid solution that leverages both quantum and classical elements to harness quantum superiority with classical assistance. The primary goal is to enhance detection capabilities and increase the success probability of the original Grover's algorithm, taking us closer to the ideal Enhanced Grover's algorithm. The concept involves using fewer Grover's iterations than the optimal number, denoted as L_{opt}, and combining it with classical test. We show that this approach has the potential to alter the complexity behavior and significantly improve the attainment of a high success probability, denoted as P_s.

In its entirety, this thesis presents an adaptation of Grover's algorithm within the context of an AUD system. It delves into enhancing and optimizing the Grover's algorithm for this specific context.

Chapter 1

Chapter 1

Introduction

The main focus of this introduction is to highlight the motivation behind studying Active User Detection (AUD) in wireless communication systems, particularly in the context of the challenges posed by the Grant-Free (GF) scheme in Fifth-Generation (5G). This scheme allows for all-in-one messaging without handshaking between the Base Station (BS) and User Equipment (UE). In this chapter, we will provide a brief overview of the AUD problems and existing classical methods that address these issues. It is important to consider the trade-off between performance and complexity, which leads to the exploration of quantum methods.

Another important aspect to discuss in the introduction is the principle of quantum computing and its potential applications in various fields. We will delve into the origins of quantum computing, the reasons for its relevance in this field, and the fundamental principles and attributes of quantum systems, such as notation, matrices, and logic gates. Additionally, we will outline the structure and contributions of the thesis, highlighting the associated challenges.

Key Takeaways:

- Motivation for studying active user detection in wireless communication systems
- Background on quantum computing and its potential applications in various fields
- Outlining the structure and contributions of the thesis, with several challenges

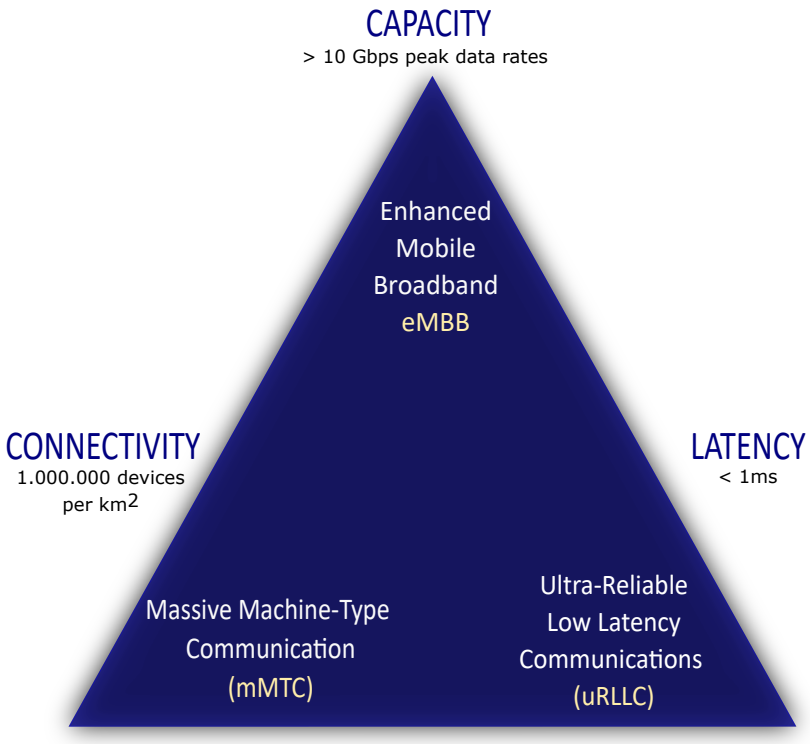


Figure 1.1: 5G Key Features

1.1 Overview of 5G Wireless Communication

The term 5G, which stands for fifth-generation, refers to the latest advancement in mobile wireless technology. It brings several key features and enhancements compared to previous generations, such as higher reliability, low-latency, and massive communication. These three key features are carried out through three primary components of 5G: Enhanced Mobile Broadband (eMBB), Ultra-reliable low-latency communication (URLLC) and Massive Machine Type Communication (mMTC) as illustrated in Fig. 1.1.

1.1.1 Enhanced Mobile Broadband (eMBB)

The first feature, eMBB, focuses on delivering a high-speed, increase bandwidth, high data-rate, compared to previous generations. The expected speed is 20 Gbps downlink (DL) and 10 Gbps for the uplink (UL), which is 20 times higher compared to Long

Term Evolution (LTE) [1]. Besides, the expected spectral efficiency is to have 30 bps/Hz for DL and 15 bps/Hz for UL [1], while the previous generation, LTE, achieves only $5-10$ bps/Hz for DL and $2-5$ bps/Hz for UL [2].

This feature is made possible through the utilization of Millimetre Wave (mmWave) technology across wider frequency bands, as discussed in references [3] and [4]. It facilitates the support of numerous real-time applications, including broadcasting, media delivery, and online gaming. The primary objective of this approach is to achieve both high reliability and high data rates, with a targeted packet loss rate of 10^{-3}, as outlined in reference [5].

1.1.2 Ultra-reliable and low-latency communication (URLLC)

On the other hand, Ultra-reliable low-latency communication (URLLC) demands exceptionally low-latency communication with a strong emphasis on reliability. The target latency for the user-plane is set as low as 1 ms, control-plane latency is aimed at 10 ms, as indicated by references [1] and [6]. Furthermore, there is a stringent requirement for high reliability, reaching 99.999%, as highlighted in [7].

User-plane latency is measured from the user device to the destination, with the objective of maintaining it at 1 ms. On the other hand, control-plane latency is measured as the time taken to transition from a power-saving state (e.g., IDLE) to the start of data transfer (e.g., ACTIVE).

In contrast to LTE, where this system is expected to achieve user-plane latencies of less than 10 ms, while control-plane latency is targeted at 100 ms, as reported in [8]. These requirements are considerably less strict compared to 5G, which demands even stricter latency requirements. These stringent requirements are driven by critical applications such as infrastructure control and industrial processes. Additionally, the future holds promise for advanced applications like augmented reality, mobile robots, and motion control centers.

1.1.3 Massive Machine Type Communication (mMTC)

The last feature is mMTC, which operates on the principle of providing scalability and efficiency for long-range, broadband machine-type communication. It caters to low-power devices such as Internet of Things (IoT) sensors, trackers, and wearable devices, which are expected to have battery lifespans of up to 10 years. This feature aligns with the goal of creating smart cities, enabling multiple low-power sensors to connect to the network. To achieve this, an architecture called Network Slicing is employed, allowing for the segmentation of different Quality of Service (QoS) levels to meet specific requirements, particularly in the context of IoT. As a result, it becomes possible to allocate lower bandwidth services to low-power sensors.

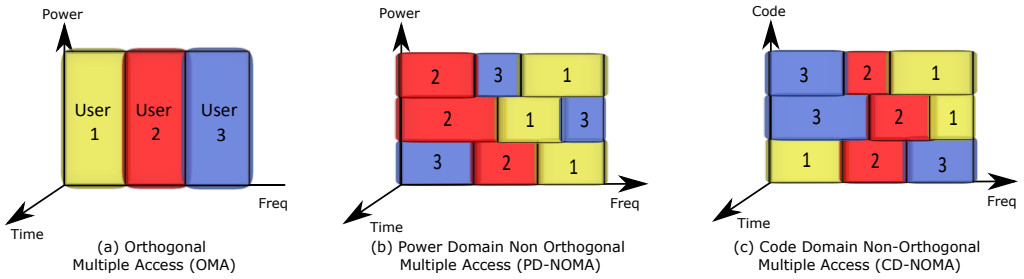


Figure 1.2: OMA vs NOMA

1.2 Multiple Access Schemes

1.2.1 Orthogonal Multiple Access vs Non-Orthogonal Multiple Access

The multiple access scheme allows several mobile users to share the same allocated spectrum. The spectrum allocation is divided into several categories: 1.) Orthogonal Multiple Access (OMA) and 2.) Non-Orthogonal Multiple Access (NOMA). The first category, OMA, divides the users into groups and shares the spectrum among them to ensure minimum interference. Some examples of this scheme are Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), and Code Division Multiple Access (CDMA). As the names explain, these schemes allow users to be distinguished by their frequency, time, and code respectively. The main concept behind these schemes is that users can share the same communication channel without causing interference to one another. In contrary, the second category, NOMA aims to increase spectral efficiency by allowing multiple users to share the same allocated spectrum simultaneously. These users are distinguished in the Power domain (PD), or the Code domain (CD). Thus, it is expected to have an inter-user interferences, which can cause errors in calculations. The OMA and NOMA (i.e PD and CD) allocation schemes are illustrated in Fig. 1.2. In this thesis, we focus more on the CD-NOMA.

In this context, 5G makes use of NOMA, which enables the simultaneous transmission of multiple signals and achieves high spectral efficiency while promising superior overall capacity and user fairness [9]. This approach allows different users to transmit using the same resource block, resulting in available resources that can be used to support additional users. The interference is managed through the use of Successive Interference Cancellation (SIC), which aims to decode the strongest signal among all users, subtract it from the received signals, and decode the remaining information until the weakest signal. This method has been demonstrated to enhance spectral efficiency while meeting the requirements of eMBB.

Several multiple access schemes which provide non-orthogonality are called Sparse Code Multiple Access (SCMA), Pattern Division Multiple Access (PDMA) and Multi-User Shared Access (MUSA). The SCMA leverages the sparse codebook which is characterized by its low-density signature to improve the system performance, by allocating each user with different codeword. The bit stream is thus transformed to different sparse codewords. By defining this codebook, it is expected to have more efficient allocated users, allowing multiple users transmit their signal simultaneously [10]. On the other hand, PDMA is the type of NOMA that leverages a given pattern to distinguish each user. It is a join design of transmitter and receiver, allowing users allocated with some resource groups which can consist of time, frequency, or any spatial resources. PDMA can effectively suppress co-channel interference, achieves low power consumption with a high spectral efficiency [11]. The last scheme is MUSA, which allows to use low-correlation spreading sequences at the transmitter. The MUSA uses the same resources for transmitting and receiving data. The idea is to use a sophisticated interference cancellation, detection, or precoding techniques [12]. It also uses the SIC and transmitter and receiver structures.

These schemes are promising to increase the spectral efficiency, which requires a more challenging system for the contention schemes especially on RACH.

1.3 Contention Schemes

In the communication network, the link established for setting up a call is done in the Random Access channel (RACH). It is used by the User Equipment (UE) to initiate communication with the Base Station (BS). Therefore, we expect collisions to occur when there are bursty transmissions in the air due to the high number of users transmitting simultaneously.

On the LTE, there are two main procedure forms: 1.) *Contention-Based* 2.) *Contention-Free*. On the first part, the UE demands an access to BS to establish the communication, namely preamble transmission [13] as indicated in Fig. 1.3. The preamble transmission is mainly used for the UE link synchronization and channel estimation. The BS should decide which UE is granted for the further communication, and later response to it within a random access response. Once the UE received it, it replies with L2/L3 messages, followed by the response of contention resolution messages. The L2/L3 message message are the messages in which the UE use the newly assigned data channel resources to communicate their connection request with a unique identifier [14].

In contrast, the *contention-free* method is a simplified version of the *contention-based* process, as described in [13]. Due to the interference caused by multiple UEs, the *contention-free* initiates the process where the BS assigns the Random Access

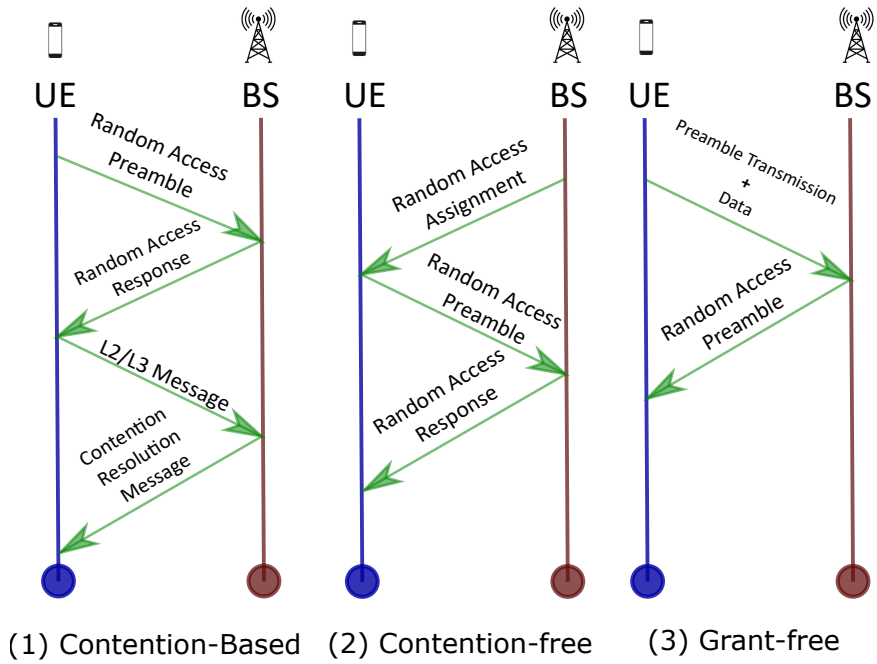


Figure 1.3: Random Access Channel Scheme

Assignment (RAA) to the users. This permits fewer delay handshakes between UE and BS and also avoid the collisions among all UEs.

On top of that, 5G proposes a different method for supporting both key features (URLLC and mMTC) with low latency and scalability, which is called the Grant-Free (GF) scheme. This scenario aims to achieve fewer delay handshakes on RACH, allowing messages to be transmitted without any granted handshake from the BS [15] [16], thereby making more resources available and enabling faster transmission. This scheme is considered as a feasible and promising technology for meeting the requirements of URLLC and mMTC. To achieve this, the preamble transmission initiated by the UE is integrated directly with the data. The general scenario is illustrated in Fig. 1.3.

The combination of the data and the preamble on GF scheme transmission leads to a new problem related to user detection, namely Active User Detection (AUD). The AUD plays a crucial role in the BS for detecting the active users among all devices, especially when GF scheme and NOMA are mainly used on BS. The following section describes the main principle of AUD with its characteristics and example.

Category	Performance-Complexity	Specific Methods
Optimal	↑ Performance, ↓ Complexity	ML, MAP
Suboptimal	↓ Performance, ↑ Complexity	AMP, CCR, OMP, ZF

Table 1.1: Comparison of Optimal and Suboptimal Methods

1.3.1 Active User Detection (AUD)

To permit all users needs when network density is high, a spectrum sharing is required to be compatible with this context. Thus, NOMA is proposed, to handle a vast connectivity with ensuring a high data rate and high spectral efficiency. This NOMA is characterized by the inter-user interference, allowing multiple transmissions to live together, which becomes challenging for detecting the active users among the network. By default, UE is configured on a sleep mode all of the time to have an energy efficiency and becomes active when there is an external events [17]. This causes a sporadic events and mostly unpredictable for being active among some users. The action of detecting the active users is called AUD.

Several existing methods have been proposed for AUD problems, with a trade-off between computation and performance. The optimal method, believed to provide the most accurate results, is Maximum Likelihood (ML). However, ML suffers from complexity issues [18]. Another promising solution within Bayesian Estimation is Maximum a posteriori (MAP), which combines likelihood and prior knowledge of user activity. However, its complexity increases with the network size [19]. Another suboptimal method aiming at reducing complexity is Approximate Message Passing (AMP), an iterative approach commonly used with limited computational resources [17] [20]. Conventional Correlation Receiver (CCR) is also categorized as a suboptimal method where its idea is to correlate the received signal with targeted codewords and return a set of active users when the correlation exceeds the threshold [21]. Last but not least, Zero Forcing (ZF) is a suboptimal method which implements the inversion of the known codewords to recover the transmitted signal. While these four methods show promise in terms of increasing user detection speed, they can lead to poor performance.

To conclude, the classical methods for AUD are summarized in Table. 1.1. The AUD problem is always a trade-off between complexity and performance. One can thus consider the solution of quantum which is promising to handle both constraints: complexity and performance [21], [22].

1.4 Overview of Quantum

1.4.1 The Advent of Quantum

Explaining quantum mechanics is somewhat rather difficult, especially, for readers who do not have a prior knowledge about it. We have been asked several times these questions:

What is Quantum? Why it becomes so important? Where does this theory came from?

First of all, we should note that understanding quantum is not easy. Richard Feynman once said *"I think I can safely say that nobody understands quantum mechanics"* [23]. As is well-known, the theory of quantum is an opposition to Newtonian (classical mechanics) and Albert Einstein's theory of general relativity [24]. Researchers have discovered quantum as a different thought from the classical theory. While classical theory is easier to handle as it corresponds to everyday life, some researchers have been able to go further than their daily vision, and adressed quantum theory. Thus, to comprehend the quantum theory, it is essential to let our glass empty before filling it with fresh theories. There is something deeply hidden out there that we have not yet discovered. The first thing we should have known is that, compared to classical computation, quantum can give us enormous benefits. It explores the undiscovered universe of the smallest scales which could be useful for all conventional computation. In this section, we explore several established theories, focusing on the key principles of quantum mechanics and the reasons for its existence.

1.4.2 What is Quantum?

The word *quantum* is derived from the Latin word *quantus* which means *how much* or *how great*, signifying the measurability and quantifiability of specific objects [25]. This terminology gained prominence when researchers observed subatomic scales in atoms, such as photons and electrons, to describe discrete and quantized energy levels [26]. Einstein and Max Planck used it to represent the fundamental units of energy packets. Consequently, photons and electrons, originally considered as particular atoms, became known as *quantum light* and *quantum electricity* respectively. So, the term *quantum* refers to a distinct branch of physics that focuses on discrete and quantized phenomena. This field of physics, which examines the properties of the subatomic scale, is known as *quantum mechanics*. Numerous experiments have substantiated this phenomenon, with further details provided in the following section.

1.4.3 Double-Slit Experiment

Several experiments have proven the existence of *quantum mechanics*. First experiment is conducted in 1801 when Thomas Young, a British polymath, demonstrates a wave-particle duality of light and matter [27]. This experiment raises the probability that a

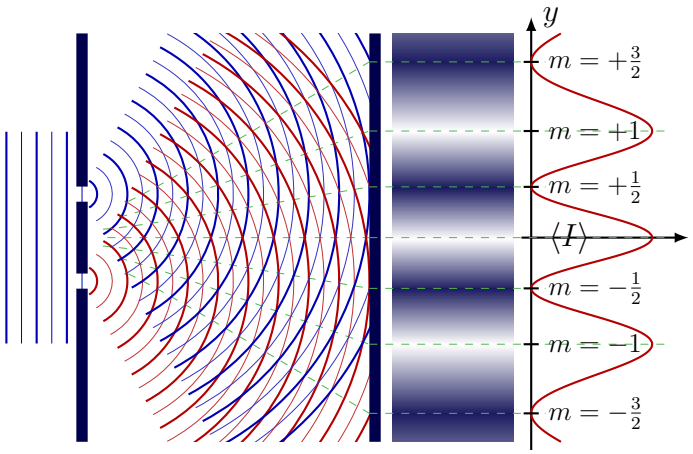


Figure 1.4: Double-Slit Experiment

light has two distinct behaviours, a *particle* and *wave*. As illustrated in Fig. 1.4, the experiment starts when light passes through double-slits. Before light passes these holes, it is observed that light is a *particle*. However, once the light passes through these slits, the light diffracts and creates a superposition (constructive interference and destructive interference). The light pattern represents the constructive one when two waves are added together, whereas the dark pattern represents the destructive interference. This signifies that light waves which pass through slits are superposed and can eliminate each other, producing bright and dark bounds on the screen. If we change the angle of slits, the constructive and destructive may be changed due to the emitted lights. In this experiment, it has been observed that when multiple light sources are combined, their behavior cannot explained by the presence of a single particle. When we send the particles one by one, the interference persists, as if each particle passed through both slits at the same time. It demonstrates attributes of multiple waves, which is why it is known as a *wave-duality experiment*.

1.4.4 Black Body Radiation

Another experiment called *Black Body Radiation* also provides the evidence supporting the theory of *quantum mechanics* [28]. It is initiated by Max Planck in 1901, where he found that the energy of the electromagnetic is rather quantized than continous. In practical terms, classical mechanics shows that if an object absorbs all incoming radiation, it is expected to re-emit it. This establishes that with increasing frequency, energy also experiences exponential growth. This phenomenon is commonly referred to as the *Ultraviolet Catastrophe* due to its consequence of infinite energy within the system.

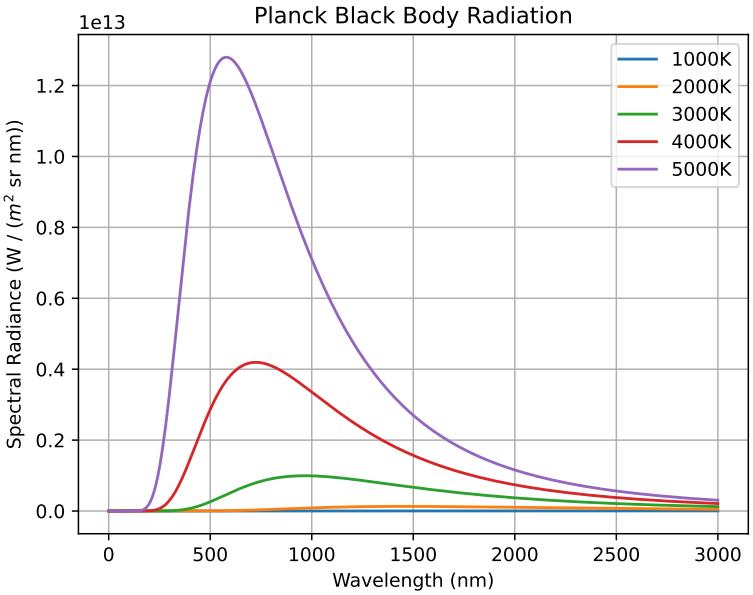


Figure 1.5: Black Body radiation

However, this catastrophe is not compliant with the real experiment. As illustrated in Fig.1.5, the energy of electromagnetic denoted by spectral radiance is quantized in a certain peak for each temperature T. Theoretically, the classical approach cannot explain this phenomenon, where high frequency f, indicated by a low wavelength λ, is always exponentially linear with variable energy. Max Planck solved this problem by proposing that the energy of the electromagnetic is *quantized* rather than *continous*. This is denoted with the equation as follows :

$$E = (n).h.f \tag{1.1}$$

where E is the electromagnetic radiation, h is a Planck constant with $6.626 \times 10^{-34} J.s$ and $n \in \{1, 2, \cdots\}$ is integer. The n signifies that this experiment is always quantized with a certain integer n. The newly proposed equation has provided evidence for the quantization of light, which ultimately led to the development of quantum mechanics.

1.4.5 Photoelectric effect

Following the phenomenon of *Black Body Radiation*, Einstein also introduced a new idea related to the *photoelectric effect*. In the early stages, classical physics thought

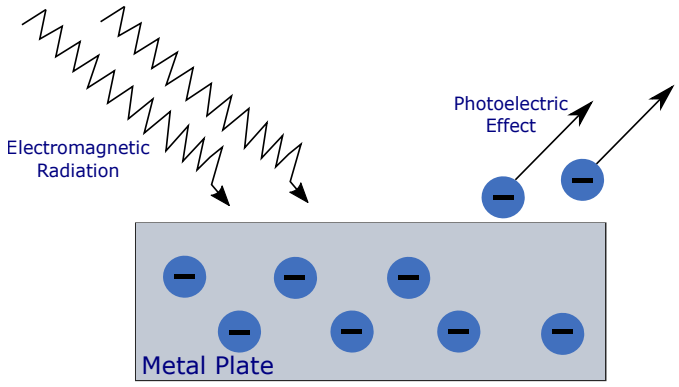


Figure 1.6: Photoelectric effect

that light purely as a wave. However, in the 20th century, it was discovered that light also behaves as particles called photons. This duality implies that light can exhibit characteristics of both particles and waves. This concept aligns with the principles observed in the double-slit experiment and black-body radiation as explained in section 1.4.3 and 1.4.4.

The effect illustrates the principle of electrons being liberated when they strike a material. Theoretically, classical mechanics cannot explain this situation because it assumes that each electron striking the material is completely transformed into energy E, which is incorrect due to the wave characteristics of light. Thus, based on this discovery, Einstein proposed that light behaves like a stream of particles called *photons* with an energy of E, which respects to the superposition of states based on dual-wave experiment as explained in section 1.4.3.

All of these phenomena have provided evidence for the existence of quantum mechanics, indicating that the photon is quantized rather than behaving solely as a particle. As a result, numerous researchers have worked on reformulating the quantum formula, as explained in the following subsection.

1.4.6 Quantum Notation

Quantum Bits

The modelization of quantum is denoted with Dirac notation, so-called *Bra-Ket notation*. $|.\rangle$ [29]. It is defined by the mathematician *Paul Dirac*, who was known as a one of the founders of quantum mechanics and quantum electrodynamics. The dirac

notation $|.\rangle$ aims to modelize the quantum qubits, as explained as follows:

$$\langle \text{bra}|\text{ket}\rangle \tag{1.2}$$

Let us assume that we have a state represented by $|\psi\rangle$. The *ket* notation, in the form of $|.\rangle$, signifies a vector matrix v within a vector space $\mathbf{V}$, which physically represents a state of a quantum system. In contrast, the *bra* notation, denoted as $\langle .|$, is used to indicate the conjugate transpose of the matrix ψ, represented as $\psi^{\intercal}$. This state $|\psi\rangle$ represents a *qubit*, a new type of bit, which is the fundamental unit of the quantum information. This qubit is modeled as follows:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.3}$$

where $\alpha, \beta \in \mathbb{C}$ are complex amplitudes which complies $|\alpha|^2 + |\beta|^2 = 1$, and $|\psi\rangle$ is the wave function that represents states in a superposition of different states, including 0 and 1. The α and β also indicate the position of the particular state in the bloch sphere 1.7. The variable $|0\rangle$ and $|1\rangle$ are the orthonormal basis for this state space, which show the probability of outcome 0 and 1 respectively, namely *computational basis states* [29]. Indeed, this notation shows merely one qubit, however, this could be extended following the *Hilbert space* with infinite-dimensional.

The probability of these outcomes depends on Born's rule, which defines that the probability of a particular measurement outcome is proportional to the square of the amplitude of the system's wavefunction [30]. Thus, if the desired value is 0, the amplitude of the system's should be $P(0) = |\alpha|^2 = 1$. On the other hand, if the desired value is 1, the amplitude of the system's is $P(1) = |\beta|^2 = 1$. The idea is that we can observe state 0 and 1. Mathematically, the Born's rule can be expressed as follows :

$$P(\alpha) = |\psi(\alpha)|^2 \tag{1.4}$$

where $P(\alpha)$ is the probability of measuring the state at position α, $\psi(\alpha)$ is the wave function or quantum state at position α, and $|\psi(\alpha)|^2$ represents the absolute value of the wave function squared. In the other words, Born's rule finds the likelihood in a particular state.

Bloch Sphere

The complex amplitudes on these two variables could be expanded to three-dimensional sphere, namely *Bloch's sphere* as illustrated in Fig.1.7. In this representation, the poles of the sphere represent the two orthogonal basis states of the qubit. For example, in a qubit system, the north pole may represent the state $|0\rangle$ and the south pole

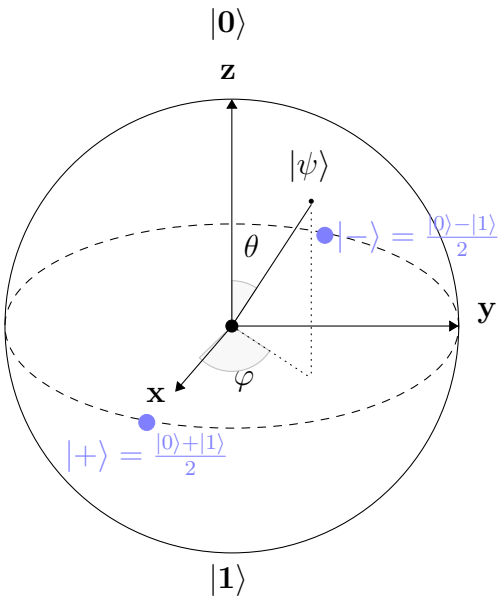


Figure 1.7: Bloch Sphere

may represent the state $|1\rangle$. The equator of the sphere represents an equiprobable superposition of these two states. The term bloch sphere is also named as *normalised sphere*, which means that each point in the Bloch sphere is limited with a unit length. In other words, the state is valid only with a total probability of 1. This respects the Born rule principle as described earlier $|\alpha|^2 + |\beta|^2 = 1$. We may re-write Eq. 1.3 as follows:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{1.5}$$

following $0 \leqslant \theta \leqslant \pi$ and $0 \leqslant \varphi \leqslant 2\pi$.

This figure shows that the qubit region consists of a sphere, which respects the amplitude sphere always equal to 1. Indeed, from this circumstance, we may also modify the direction of the point, which belongs to different computations. To the west side, we may have $|+\rangle$ which corresponds to the superposition of the states, denoted as $\frac{|0\rangle+|1\rangle}{2}$, where 0 and 1 have a same probability 50%. Similarly, on the east side, the notation is $\frac{|0\rangle-|1\rangle}{2}$ with a same probability 50% between 0 and 1.

On the other hand, it is possible to modify the phase of θ and φ to obtain a certain level following the Bloch's sphere level. For example, we may obtain that $|i\rangle$, where i is the imaginary unit, by providing $\theta = \frac{\pi}{2}$ and $\varphi = \frac{\pi}{2}$. Besides, to obtain $-|i\rangle$ by keeping the $\theta = \frac{\pi}{2}$ and changing $\varphi = \frac{3\pi}{2}$.

1.4.7 Quantum Mechanical Principles

Section 1.4.1 has shown that nature gave a different perspective on the fundamental laws of nature compared to classical mechanics. While classical mechanics is deterministic, the quantum mechanics introduces a probabilistic behavior. This quantum mechanics brings a different type of law compared to classical, which consists of several principles, as shown as follows [31]:

Entanglement

The entanglement between two states is the strangest phenomenon in quantum. Overall, it shows that two states can be maximally entangled or fully dependent between each other, which means that they are correlated 100%. If the quantum state of, let us say A is known, the other state B is deterministic. The idea of entanglement is shown as follows:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \tag{1.6}$$

From Eq. 1.6, we observe that if the first state returns $|0\rangle_A$ shows 0, the second state always be $|0\rangle_B$, and conversely. The symbol $\otimes$ defines the Kronecker product.

No-cloning Theorem

No-cloning theorem is an important principle in quantum mechanics. This theorem states that it is impossible to create an independent and identical copy of a previous quantum state. In other words, quantum states cannot be copied.

To understand this concept, let us consider the scenario where we have a quantum state denoted as $|\psi\rangle$, and we wish to create a copy of it, denoted as $|\psi'\rangle$. In order to copy the state, we need to have a precise knowledge of the components of $|\psi\rangle$, as outlined in quantum notation in subsection 1.4.6. This includes knowing the structural components of α and β associated with it. However, this knowledge is impossible to obtain. The quantum state $|\psi\rangle$, which contains the wavefunction, can only be measured if the state is collapsed into a classical state. The classical state represents a probabilistic combination of states encoded in the wavefunction. In other words, the no-cloning theorem explains that there is no single process or state in the quantum that permits the duplication of another state. This inherent probabilistic nature is one of the main reasons why an eavesdropper attempting to intercept a state on a quantum channel faces difficulties due to the *no-cloning theorem*.

Superposition

We observe that the wave-duality function exhibits a superposition of two waves, represented by a wavefunction. In classical systems, the state or value of a classical bit is deterministic, taking on either the value of 0 or 1. However, in quantum mechanics, a qubit is non-deterministic and can exist in a superposition of two or more possible states. Referring to Eq. 1.3, the state $|\psi\rangle$ is a superposition of two possible states, 0 and 1.

1.4.8 Quantum Matrix

It is noted that the *Bra-Ket* notation as presented in 1.4.6 consists of a component vector. Let us consider an example where the ket vector $|A\rangle$ represents a vector within the Hilbert space, associated with the mathematical object $\mathbf{A}$. In this context, $|A\rangle$ serves as a representation of $\mathbf{A}$ in the Hilbert space. It is noted that the $|A\rangle$ consists of a column vector, whose length is 2^n (where n is the number of qubits). Thus, an n-qubit system is represented by a 2^n-dimensional column vector. In the case of $|A\rangle$ using just one qubit, we have a column vector as follows:

$$|A\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \tag{1.7}$$

On the other work, we can expand to the bra notation, written as $\langle A|$, by representing it as a row vector:

$$\langle A| = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \tag{1.8}$$

So, conversely, the relationship between a bra and a ket can be expressed as:

$$\langle A|^\intercal = |A\rangle \tag{1.9}$$

To obtain the orthogonal basis which returns a *scalar* value, we could develop an *inner-product value*, denoted as $\langle A|A\rangle$. The Bra notation $\langle .|$ is related to the Ket $|.\rangle$ notation through the concept of the conjugate transpose. By assuming that M is the length of column vector $|A\rangle$, we can express this relationship as follows:

$$\langle A|A\rangle = \begin{pmatrix} A_1^\intercal A_2^\intercal \cdots A_M^\intercal \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ \cdots \\ A_M \end{pmatrix} = \begin{pmatrix} A_1^\intercal A_1 & A_2^\intercal A_2 & \cdots & A_M^\intercal A_M \end{pmatrix} \tag{1.10}$$

On the other hand, the quantum operation permits to operate *outer product* in the quantum state, denoted as *ket-bra*. The operation can be done by using $|\rangle.\langle .|$ as illustrated in Eq. 1.11:

$$|A\rangle\langle A| = \begin{pmatrix} A_1 \\ A_2 \\ \dots \\ A_M \end{pmatrix} \begin{pmatrix} A_1^\intercal & A_2^\intercal & \cdots & A_M^\intercal \end{pmatrix} = \begin{pmatrix} A_1A_1^\intercal & A_1A_2^\intercal & \cdots & A_1A_M^\intercal \\ A_2A_1^\intercal & A_2A_2^\intercal & \cdots & A_2A_M^\intercal \\ \dots & \dots & \dots & \dots \\ A_MA_1^\intercal & A_MA_2^\intercal & \cdots & A_MA_M^\intercal \end{pmatrix} \tag{1.11}$$

We could see the product of two quantum states, which is detained using *tensor product*. Each column vector of quantum state is presented with a column vector with length 2^n. This is shown in Eq. 1.12. Indeed, the product of quantum states can be extended to include $3, 4$, or even an infinite number of qubits, depending on the available resources. However, a high number of required qubits leads to intensive computational demands.

$$|AA\rangle = |A\rangle \otimes |A\rangle = \begin{pmatrix} A_1 \\ A_2 \\ \dots \\ A_M \end{pmatrix} \otimes \begin{pmatrix} A_1 \\ A_2 \\ \dots \\ A_M \end{pmatrix} \tag{1.12}$$

In fact, a quantum state is denoted with a vector officially to represent the elements of a vector value which is referred to a *Hilbert Space* [29]. Every state $|.\rangle$ is thus described as a vector matrix with dimension n, where n is a number of qubit. Several examples are shown as follows:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$|i\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$$

$$|-i\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$$

1.4.9 Quantum Gate

A quantum gate is a fundamental building block of quantum logic circuits designed to modify or manipulate qubits in quantum algorithms. Just as classical computing uses logic gates like XOR, OR, and AND to perform logical operations, quantum gates

serve a similar purpose in quantum computation. Let us note that quantum gate is characterized by its *reversibility*, which signifies that the origin quantum state is possible to be recovered after applying the state without lossing information. This is contrary to the classical gate. Several quantum gates are cited as follows, such as *H-gate*, *X-gate*, *Y-gate*, and *Z-gate*.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \tag{1.13}$$

$$X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \qquad Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

For example, when we apply the X-gate to the state $|0\rangle$, it results in $X|0\rangle = |1\rangle$. When we apply it again, it returns to the original state: $X|1\rangle = |0\rangle$. Similarly, if we apply the H-gate to the state $|0\rangle$, it produces a superposition of states: $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$. Applying it again brings the state back to its original form: $H.H.|0\rangle = |0\rangle$.

1.5 Quantum Advantages

1.5.1 Quantum Advantages

Due to the superposition of the states, the quantum algorithm can help reduce the complexity of several classical algorithms. For example, the Shor's algorithm is mainly used to find the prime factors of an integer. In the context of Shor's algorithm, assuming that N_i is an integer number. Normally, the classical algorithm requires $\mathcal{O}(e^{1.9(\log K)^{1/3}(\log\log N_i)^{2/3}}K)$ [32], while Shor's algorithm, in the context of quantum, can reduce to $\mathcal{O}((\log K)^2(\log\log N_i)(\log\log\log N_i))$ using fast multiplication [33]. This is what we called the *polylogarithmic time*.

The other advantages is obtained with one of the quantum algorithms, Grover's algorithm, is mainly used to do a searching engine, and proved to reduce the complexity on the database from $\mathcal{O}(K)$ to $\mathcal{O}(\sqrt{K})$ on the unsorted database, where K is the size of the database. Based on the classical computation, the linear search normally requires $\mathcal{O}(K)$ to find the correct solution. Its running time increases linearly with the size of the input. In order to move forward, the binary search aims to reduce this complexity using a half-interval search. It is proven that this method could search within $\mathcal{O}(\log K)$ merely with *sorted database* [34]. Within the unsorted database problem, a powerful Grover's algorithm came up to handle against this problem by finding a simpler way. Making it more simpler, this algorithm is based on the superposition which could reduce the complexity. Grover's algorithm has proven to handle $O(\sqrt{K})$ which is far below than the classical one.

Although quantum brings numerous benefits, it has been proven that quantum algorithm cannot solve all the non-polynomial problems (NP). However, it is shown that quantum computers have shown the potential of efficient solutions to certain specific NP problems (with using Shor's algorithm). NP problem is the complexity class for which problems that can be classified non deterministically solvable in a polynomial time. For example, the Grover's algorithm can reduce the complexity of NP-complete problem on boolean satisfiability problem (SAT). Quantum cannot reduce this complexity class from NP-complete to NP-hard, or move forward to that, however, it is capable to reduce the required time to find the underterministic solution on SAT, which leads to $\mathcal{O}(2^{n/2})$ where n is equal to the Boolean variable [35].

1.5.2 Quantum disadvantages

While quantum computing has advantages in terms of efficiency and scalability, it also comes with certain drawbacks. Firstly, it is worth mentioning that quantum computing introduces the concept of superposition, enabling the representation of multiple possibilities simultaneously. In contrast to classical computing, which deals primarily with binary states (0 and 1), quantum computing accommodates a wider range of states concurrently. This expansion of possibilities, however, necessitates more complex *error correction* mechanisms due to increased environmental susceptibility. Thus, the errors on the quantum state is relatively more vulnerable compared to the classical one.

Additionally, the second drawback is the use of quantum computing for simple calculations, which appears to be *overkill*. While classical algorithms require just one bit to perform tasks like summation and subtraction, quantum algorithms necessitate a quantum state, which is designed to solve complex problems, compared to classical methods. Quantum computing is undoubtedly much faster at solving complex problems, but it is not efficient for basic calculations such as summation and subtraction.

Another disadvantage worth mentioning is that the construction of new quantum computers necessitates very *low temperatures* for proper implementation, resulting in high energy consumption. Achieving and maintaining these low temperatures can be quite challenging when attempting to address this issue. Consequently, at this specific stage, quantum computing remains in its early phases, primarily undergoing exploration in research and various applications. Building quantum computers require expensive costs, which limit their accessibility.

The overview of pros and cons of the quantum is summarized in Table. 1.2.

Quantum Pros and Cons	
Advantages	**Disadvantages**
Quantum computing offers high security due to entanglement. However, it also poses a threat to encryption schemes, leading to the development of post-quantum cryptography.	Require advanced quantum error correction and more vulnerable to noise
Quantum offers a high speed in solving complex problems, such as searching unsorted database, SAT problem, prime numbers, etc.	Quantum computing is better suited for complex calculations rather than a simple one
Quantum can be widely used to optimize many sectors, (i.e telecommunication, finance, machine learning)	Low Temperature is necessary.
Quantum science is closely connected to our understanding of nature, revealing that nature operates through the principle of superposition	Quantum computers are high in cost.

Table 1.2: Quantum advantages and disadvantages

1.6 Contributions and Challenges

1.6.1 Contribution

A summary of the contributions of this thesis is given as follows:

1. Adapting the Grover's algorithm in context of activity users detection purposes (Chapter. 3).
2. Extending the Grover's algorithm to discover the minimum value in the context of activity users, analyzing the existing methods, and enhancing it (Chapter. 4).
3. Introducing a novel algorithm to identify the minimum value based on the enhancement of the existing method. Improving performance by employing a combination of classical methods, thereby enabling better results.(Chapter. 4).
4. Proposing an Enhanced Grover algorithm, combining the Grover's algorithm with classical methods, to enable faster speed (Chapter. 5).

1.6.2 Challenges

1. Maintaining a balance between performance and complexity for activity detection.
2. Constructing the Quantum Circuit, which demands a large number of gates.
3. Identifying an appropriate level of complexity for comparison with DHA.

4. Addressing the implementation in practical scenarios, considering that the usage of Grover's algorithm remains confined to simulation.

1.7 List of publications

This thesis is based on several publications, working with my PhD supervisor, Claire Goursaud.

1. M. I. Habibie, J. Hamie and C. Goursaud, "A Performance Comparison of Classical and Quantum Algorithm for Active User Detection," 2022 IEEE 23rd International Workshop on Signal Processing Advances in Wireless Communication (SPAWC), Oulu, Finland, 2022, pp. 1-5, doi: 10.1109/SPAWC51304.2022.9833942.

2. M. I. Habibie, J. Hamie and C. Goursaud, "Adaptation of Grover's Quantum Algorithm to Multiuser Detection in an OCDMA System," 2021 IEEE Symposium On Future Telecommunication Technologies (SOFTT), Bandung, Indonesia, 2021, pp. 88-93, doi: 10.1109/SOFTT54252.2021.9673141

3. M. I. Habibie, J. Hamie and C. Goursaud, "Adaptation de l'algorithme quantique de Grover à la détection multi-utilisateurs dans un système OCDMA", 2022 XXVIIIème Colloque Francophone de Traitement du Signal et des Images (GRETSI), Nancy, France, 2022.

4. M. I. Habibie, J. Hamie and C. Goursaud, "Comparaison des performances des algorithmes classiques et quantiques pour la détection dans un système NOMA," 2023 XXIXème Colloque Francophone de Traitement du Signal et des Images (GRETSI), Grenoble, France, 2023.

5. Quantum Minimum Searching Algorithms for Active User Detection in Wireless IoT Networks : IEEE Journal on IoT (Submitted)

Chapter 2

Chapter 2

State-of-the-art

The main focus here is to discuss the previous research conducted on Active User Detection (AUD) techniques in classical systems. We will provide a more detailed explanation of various classical methods employed, including Maximum Likelihood (ML), Conventional Correlation Receiver (CCR), and Zero Forcing (ZF). Additionally, we will compare these classical methods in terms of their complexities by employing databases searching such as linear search and binary search.

Another important aspect is to introduce quantum computing algorithms designed for solving optimization problems. We will specifically delve into the Deutsch–Jozsa algorithm, Bernstein-Vazirani algorithm, and, most importantly, Grover's algorithm. A comprehensive exploration of Grover's algorithm will be provided, along with a review of relevant studies that have applied this algorithm in communication systems. This is particularly relevant to solving problems where the solution is unknown, such as in BBHT and DHA. Furthermore, we will discuss related studies on Grover's algorithm for wireless communication.

Lastly, we will outline the system model used for AUD and the selected variables. Specifically, we will adhere to the defined plan where the observed signal is represented as $\mathbf{y} = \mathbf{b} \cdot \mathbf{C} + \mathbf{w}$, with $\mathbf{y}$ denoting the observed signal, $\mathbf{b}$ representing the set of active users, $\mathbf{C}$ representing the set of codewords, and $\mathbf{w}$ representing the noises. We will consider three types of codewords: 1) Unipolar 2) Bipolar and 3) Gaussian.

Key Takeaways :

- Previous research on active user detection techniques in classical systems
- Introduction to quantum computing algorithms for solving optimization problems

- Review of relevant studies on the application of Grover's algorithm in communication systems
- Discuss the system model used for AUD

2.1 Overview of AUD

2.1.1 System Model of AUD

We consider to have N devices connected with a BS equipped with a single antenna, where users are assumed to be by default in sleep mode and to be active when they send messages. This network adapts Code-Domain Non-Orthogonal Multiple Access (CD-NOMA) systems, where each user is distinguished by the code domain. The codewords $\mathbf{C} \in \mathbb{R}^{N \times SF}$ as an indicator in the code domain, are spread over SF, where SF is the spreading factor. The user activity model uses a set $\mathbf{b} \in \{0,1\}^N$, where $b = 1$ corresponds to an active user. We assume that $N \geq SF$ users simultaneously transmit to the BS in one transmission frame. For the sake of simplicity, it is considered that the channel is perfect by assuming $\mathbf{H} = 1$, along with the presence of Additive white Gaussian Noise (AWGN) indicated by $\mathbf{w} \in \mathbb{R}^{SF}$ following $\mathcal{N}(0, \sigma^2)$. The system model is as follows:

$$\mathbf{y} = \mathbf{b}.\mathbf{C} + \mathbf{w} \tag{2.1}$$

The received signal $\mathbf{y} \in \mathbb{R}^{SF}$ is thus composed by three variables, the user activity set of ($\mathbf{b}$) and codewords messages $\mathbf{C}$ with the additive noises ($\mathbf{w}$). For comparison purposes, three families codes will be considered in this work:

1. Unipolar $\mathbf{C} \in \{0,1\}^{N \times SF}$
2. Bipolar $\mathbf{C} \in \{-1,1\}^{N \times SF}$
3. Random Gaussian Code ($\mathbf{C}$ is normalized by dividing it by its magnitude)

Given the received signal and the set of users code, the objective is to recover the active users set $\mathbf{b} \in \{0,1\}^N$. The full scheme is given by 2.1. The full explanation of code families will be presented in the next subsection 2.1.2.

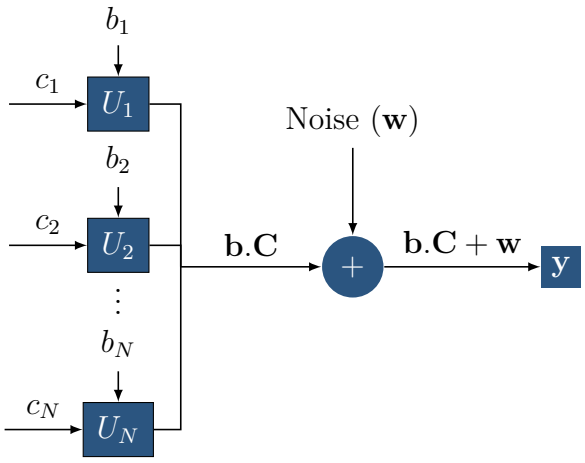


Figure 2.1: Active User Detection (AUD) system model for NOMA

2.1.2 Code Families

Unipolar Code

First, we present a simple code: Unipolar. The characteristic feature of this system lies on binary code $\mathbf{C} \in \{0,1\}^{N \times SF}$. Inspired by the concept of Optical Orthogonal Code (OOC) as presented in [36] [37] [38], the OOC codes are a family of codes consisting of $\{0,1\}$ (on/off) sequences with good auto-correlation and cross-correlation properties. The auto-correlation exhibits a narrow main lobe and adequately small side lobes, while the cross-correlation always remains small. This code is lacking *negative computation*, induced by the use of $\{0,1\}$.

In practical terms, the binary set $\{0,1\}$ is predominantly employed within optical communications, facilitating Code Division Multiple Access (CDMA) for optical fiber transmission. The **advantage** of using unipolar code is that the code is simple, as it consists only of $\{0\}$ and $\{1\}$. However, this simplicity comes at the cost of poor noise immunity, making this code vulnerable to noise and interference, which becomes this **disadvantage**. The unipolar code is mostly used in the context of OCDMA, mobile radio, spread-sectrum communications, radar and sonar signal design [36].

The unipolar code is utilized and classified as a family of non-orthogonal codes, where each code within the family maintains a non-orthogonal relationship with one or several other codes in the system to account for the non-orthogonal nature within the Non-Orthogonal Multiple Access (NOMA) system. Thus, in this thesis, we focus on the unipolar code with the non-orthogonal attribute.

Bipolar Code

The second code, namely bipolar code, utilizes $\mathbf{C} \in \{-1, 1\}^{N \times SF}$, inspired by the bipolar sequence used by [39]. The bipolar code is based on two unipolar sequences with the same period. Let us take an example, u_n and $\bar{u_n}$, which both take same values of $\{0, 1\}$. Bipolar code is obtained by operating the adder u_n with the complement $\bar{u_n}$, which leads to $\{-1, 1\}$. This code is an extension of the unipolar code, primarily utilized in OCDMA, which has also found application in Light Emitting Diode (LED) and Amplified Spontaneous Emission (ASE) from Erbium-Doped Fiber Amplifier (EDFA) [40]. The key advantage of employing this bipolar code is its bigger immunity to noise, making it robust in noisy environments.

It is important to note that quantum computing can only operate with binary representation ($\mathbb{B}$). Therefore, when representing negative integers, the closest approach is to use the one's complement ($\bar{u_n}$), which is achieved by flipping the bits to represent the negative value.

Random Gaussian Code

Real Gaussian codes are codes in which the vector $\mathbf{C}$ is randomly chosen following a normal distribution. Subsequently, this vector $\mathbf{C}$ is divided by its magnitude $\|\mathbf{C}\|$. To achieve this, let us assume that we have vector of length n_R [41]. The random codebook is generated by choosing independent identically distributed (i.i.d) random n_R-vectors, denoted as $\mathbf{C} \in \{c_1, c_2, \cdots, c_{n_R}\}$, each consisting of n_R independent Gaussian random variables with a mean of zero and a variance of σ^2. In a more extended approach, the works of [42] and [43] utilize unitary power normalization for the vectors. In this thesis, we focus on the random gaussian code.

The main point of interest regarding random Gaussian codes is that they achieve a high success probability even when the rate (R) is less than the channel capacity (W_R). This R refers to the number of bits or symbols transmitted per unit of time, measuring how quickly data is sent over a communication channel. W_R, on the other hand, represents the channel capacity, which is the maximum rate at which reliable data transmission is possible over a communication channel. However, these codewords are susceptible to noise, except there is an exceptional situation such as the vector n_R should be sufficiently large as discussed in [41]. This codebook is widely implemented in the context of image processing such as for vector quantization, [44], compressed sensing [45], etc.

2.1.3 Classical Methods for AUD problems

This section provides a detailed explanation of several classical methods that have been proposed for AUD problems. As discussed in 1, these methods have their own advantages and disadvantages, particularly in terms of performance and complexity. The subsequent section will delve into a thorough explanation of these aspects.

Maximum Likelihood

The Maximum Likelihood (ML) receiver is the optimal solution for AUD [18]. This detector identifies the most likely active users set $\mathbf{b}$, given the received sequence. For an AWGN channel and equiprobable activity, the ML is obtained by searching the active user set that minimizes the distance between its contribution and the received signal. The received sequence $\mathbf{y}$ and the set of user's signatures c_i construct the formula of ML receiver as given as follows, in an AWGN channel, and equiprobable activity :

$$\{\widehat{b}_i\}_{i\in\{0,\cdots,N\}} = \underset{\{b_i\}_{i\in\{0,\cdots,N\}}}{\arg\min} \left\| \mathbf{y} - \sum_{i=1}^{N} b_i.c_i \right\|_2^2 \tag{2.2}$$

The ML solution suffers from a high computation complexity $\mathcal{O}(2^N)$, as it is based on an exhaustive search over all the existing possibilities. Indeed, the likelihood metric has to be computed for each potential activity set. Even though this metric can be reduced to the distance between the expected received signal and the actual one (as we consider an independant, homogeneous activity, and a gaussian channel), finding the minimum among all distances depends exponentially of the number of users. Thus, the high complexity of the ML detector makes it intractable with classical processors when the number of users increases.

Conventional Correlation Receiver (CCR)

The CCR is categorized as a suboptimal method [46] and permits to slightly handle the Multiple Access Interference (MAI) [47]. Let us revoke the system model in Eq. 2.1, where $\mathbf{y}$ is observed. To construct the estimated set of activity users $\hat{\mathbf{b}} \in \{0,1\}^N$, the idea of CCR is to correlate observed signal $\mathbf{y}$ with the given codewords $\mathbf{C}$. If the correlation exceeds the given pre-defined threshold T, it is considered to be active $\hat{b} = 1$. By assuming $i \in \{1, \cdots, N\}$, the CCR equation is explained as follows:

$$\hat{b}_i = \begin{cases} 1 & \text{if } \mathbf{y} \cdot c_i \geq T \\ 0 & \text{otherwise} \end{cases} \tag{2.3}$$

Algorithm	Best Time complexity
Linear Search	$\mathcal{O}(K)$
Binary Search	$\mathcal{O}(\log_2 K)$
Ternary Search	$\mathcal{O}(\log_3 K)$
Jump Search	$\mathcal{O}(\sqrt{K})$
Interpolation Search	$O(K)$

(a) Searching Algorithm Complexity

Function	x	$f(x)$	Type
$f(x) = 0$	0	0	Constant
	1	0	
$f(x) = 1$	0	1	Constant
	1	1	
$f(x) = x$	0	0	Balanced
	1	1	
$f(x) = x \oplus 1$	0	1	Balanced
	1	0	

(b) Deutsch-Jozsa Table

Table 2.1: Table searching and Deutsch-Jozsa Algorithm

The handling of this method against interference has been studied in [47]. The level of MAI can cause errors if the interference level exceeds the given threshold T, which is considered to be high. Otherwise, the presence of MAI is considered to be canceled due to this level. Thus, the study of CCR can handle the presence of MAI.

Zero Forcing (ZF)

The Zero Forcing (ZF) receiver is categorized as a simple and effective detector, but also as a suboptimal method. While the code sequences $\mathbf{C}$ are known, we may obtain the estimation of $\hat{b}_{ZF}$ by multiplying the received signal by the inverse code sequences $\mathbf{C}$. However, due to the rectangular matrix format of $\mathbf{C}$, we should use the pseudo-inverse $\mathbf{C_C} = (\mathbf{C}^T\mathbf{C})^{-1}\mathbf{C}^T$ [48].

$$\hat{b}_{ZF} = \mathbf{y}.\mathbf{C}_C \tag{2.4}$$

The presence of noise in the context of ZF has been studied [49]. However, the ZF method, when applied using the pseudo-inverse, can introduce additional noise, a phenomenon often referred to as *noise enchancement* because noise is also amplified along with the pseudo-inverse [50]. This method is also widely known for reducing Intersymbol Interference (ISI) in a noise-free case [50].

2.1.4 Database Searching cases

Finding a value in a particular database has been an interesting subject to handle. In the context of searching for a value, several algorithms have been proposed to locate specific values within a database. Typically, these searching algorithms require a time complexity of approximately $\mathcal{O}(K)$ to find a value. The list of algorithms that have been proposed for searching a value is given in Table 2.1a.

Linear Search

The first algorithm is the *Linear Search*. This algorithm begins the search from the first index to the last index of the database sequentially [34], [51]. If the algorithm finds a match with the desired value, it will stop. Consequently, this algorithm has a worst-case complexity of $\mathcal{O}(K)$.

Binary Search

The second algorithm is called the *Binary Search*, which works efficiently on sorted elements [34], [51]. The idea is to select the middle element of the database and compare it with the desired value. If the desired value is greater or smaller than the middle element, the algorithm eliminates the remaining values. Therefore, the complexity of the binary search is $\mathcal{O}(\log_2 K)$. However, this algorithm only works effectively if the database is **sorted**.

Ternary Search

Another algorithm is known as *Ternary Search*, which shares a similar concept with the *Binary Search* [51]. While the binary search considers only one middle element, the ternary search determines two middle points. This algorithm also requires a **sorted** database and has a worst-case complexity of $\mathcal{O}(\log_3 K)$.

Jump Search

The *Jump Search* algorithm aims to find the smallest index by jumping sequentially with a certain interval instead of running linearly [51], [52]. This algorithm is only effectively applied to a *sorted* database, resulting in a complexity of $\mathcal{O}(\sqrt{K})$. Once this algorithm finds that the searched value is greater than the desired value, the jump search will move back to the last jump and proceed linearly. The jump search algorithm is recognized as being more efficient than the linear algorithm.

Interpolation Search

The *Interpolation Search* algorithm follows a similar concept to the *binary search* [34], [51]. While the binary search selects the middle element to divide the values, the interpolation search estimates the position of the target element based on the relative to the minimum and maximum elements in the array. of this algorithm is $\mathcal{O}(\log \log K)$, and the worst-case complexity is $\mathcal{O}(K)$.

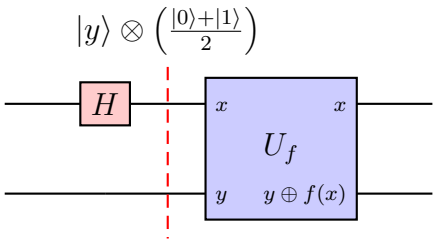


Figure 2.2: Quantum parallelism

These classical algorithms have specific requirements for their implementation. The worst complexity of each particular classical algorithm lies in having a **sorted** database, whereas real-world databases are often **unsorted**. This is why quantum search is proposed, as explained in the following section:

2.2 Quantum Algorithms

The effectiveness of quantum computing in simplifying calculations compared to classical methods has been evaluated in Chapter 1. This section explores various algorithms relevant to this thesis, specifically focusing on Grover's algorithm. The fundamental idea is to contrast it with classical search engines that entail higher levels of complexity.

2.2.1 Deutsch–Jozsa algorithm

The Deutsch-Jozsa algorithm addresses the problem of determining if a given black-box function output is *constant* or *balanced*. A *constant* function is defined as one in which the output remains constant regardless of the input applied to the black box, meaning that the input has no effect on the output. In contrast, a *balanced* function is defined as one in which different inputs produce different outputs, demonstrating that the input does affect the output. The number of outputs of a *balanced* function is consistently distributed equally between 0 and 1. This is the reason it is termed *balanced* since the count of 0s and 1s is consistently half of the total number of the input domain.

This algorithm is based on *quantum parallelism*, where two or multiple possibilities, denoted as $f(x)$, are possibly run together. Thus, let us consider an example depicted in Fig.2.2. The main concept revolves around the utilization of *black-box functions* represented by U_f, which is also known as *oracle*. This function takes an input x consisting of superposition of two states $\frac{|0\rangle+|1\rangle}{2}$. The expected output is obtained by performing an operation on $y \oplus f(x)$. Notably, since x can have two possible values,

namely $|0\rangle$ and $|1\rangle$, we can simultaneously observe the outputs of $f(|0\rangle)$ and $f(|1\rangle)$. Consequently, the output can be expressed as $y \oplus (f(0) + f(1))$. This output differs from the classical one because there is no algorithm or method that can run a *function* on two inputs simultaneously $f(0)$ and $f(1)$, a concept known as *quantum parallelism*.

Based on this principle, the Deutsch-Jozsa algorithm acts as a *black box* quantum computer, following the function:

$$f : \{0,1\}^n \rightarrow \{0,1\} \tag{2.5}$$

Where the function's goal is to take an n-bit binary input and produce an output of either 0 or 1, this can be achieved by a single oracle. However, in practical terms, classical methods necessitate evaluating the function approximately $\frac{2^n}{2} + 1$ times to determine whether it is *constant* or *balanced*. Classical methods require separate testing of 0 and 1, resulting in multiple possibilities and requiring numerous iterations [29], [53].

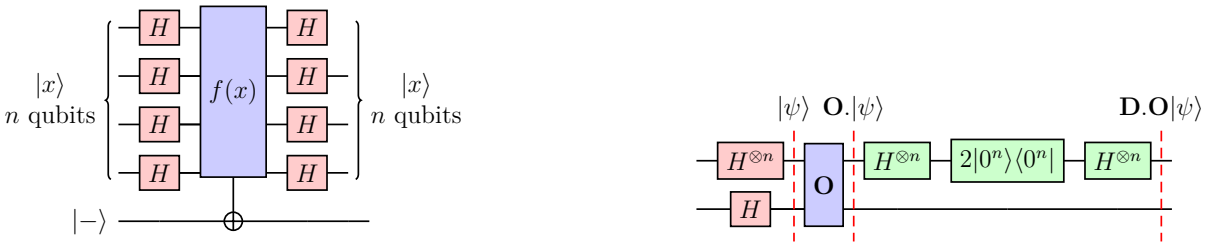
2.2.2 Bernstein-Vazirani Algorithm

While the Deutsch–Jozsa algorithm discusses the function of the *black-box*, the Bernstein-Vazirani problem delves into the hidden binary string embedded in the *black-box* [54]. The idea is to find the hidden binary string through the black-box function U_f using as few queries as possible, which is proven to achieve a significant speedup compared to classical methods. Let f be a function from bit strings of length n, and the problem is addressed as follows:

$$f : \{0,1\}^n \rightarrow \{0,1\} \tag{2.6}$$

While the Deutsch–Jozsa algorithm determines whether the final function is *constant* or *balanced*, the Bernstein-Vazirani algorithm aims to determine the output of a hidden function represented by a bit string $s \in \{0,1\}^n$. This function takes an $n-$bit string $|x\rangle$ as input and returns a single bit based on a bitwise operation. The goal is to find s where $f(x) = s \cdot x \cdot (\mod 2)$ is run multiple times as possible [55].

Let us see the picture from Fig. 2.3a. In this case, the input $|x\rangle$ has $n = 4$ where n is the number of qubits, which serves $2^n = 16$ possible cases. Classically, we should run this 16 times, to find the correspond s which permits to detect the final output. However, using the quantum solution, it is possible to reduce this multiple cases using only one call function $f(x)$.



(a) Bernstein-Vazirani Algorithm (b) Grover's Scheme

Figure 2.3: Quantum Algorithm Schemes

2.2.3 Grover's algorithm

Grover's algorithm is one of the quantum algorithm that has been proven to improve the classical searching from $\mathcal{O}(K)$ to $\mathcal{O}(\sqrt{K})$. This algorithm has been widely extended to several applications, such as quantum walk algorithm [56], quantum Grover's adaptive search [57], quantum counting [58]. This algorithm consists of two important parts: 1.) Oracle (**O**) and 2.) Diffuser (**D**). The oracle is constructed to give a mark to the qubits, by providing the negative sign. On the other hand, the diffuser (**D**) aims to reamplify the marked qubits, after marked by Oracle (**O**). Before computing the Grover's algorithm, the qubits should be initialized with the *Hadamard* (H-Gate) to have superposition of states.

Thus, the Grover's scheme is structurized as Fig. 2.3b. The first part is to develop $|\psi\rangle$ after calculating:

$$|\psi\rangle = \frac{1}{\sqrt{K}} \sum_{x=1}^{K} |x\rangle \tag{2.7}$$

where $|x\rangle$ corresponds to the index of the qubit, following $x \in \mathbb{B}^K$. Then the operation **O** selects the qubits by providing the computation in the superposition of state as written as follows:

$$\mathbf{O}|x\rangle = \begin{cases} -|x\rangle & \text{if } f(x) = \delta \\ |x\rangle & \text{otherwise} \end{cases} \tag{2.8}$$

The **O** should be compiled with the desired value δ, $f(x) = \delta$, following that $\delta \in \mathbb{C}^+$. The result should be amplified by **D**, done by the conditional phase shifter $|\psi\rangle\langle\psi|$ with the equation as follows :

$$\mathbf{D} = H^{\otimes K}(2|0\rangle\langle 0| - I)H^{\otimes K} = 2|\psi\rangle\langle\psi| - I \tag{2.9}$$

The operation of **O** and **D** can be iterated several times.

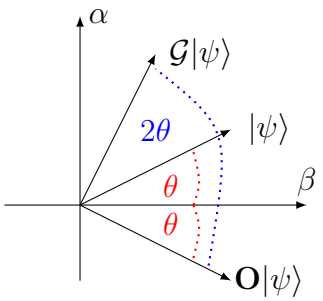


Figure 2.4: Grover's visualization

Grover's optimum iteration:known number of solution

As it is discussed in section 2.2.3, two parts of Grover's algorithm, **O** and **D** are iterated $\sqrt{K}$ times while classical requires K times. However, the iteration on Grover's algorithm can be optimized as long two variables are identified: Database size K and number of solution S.

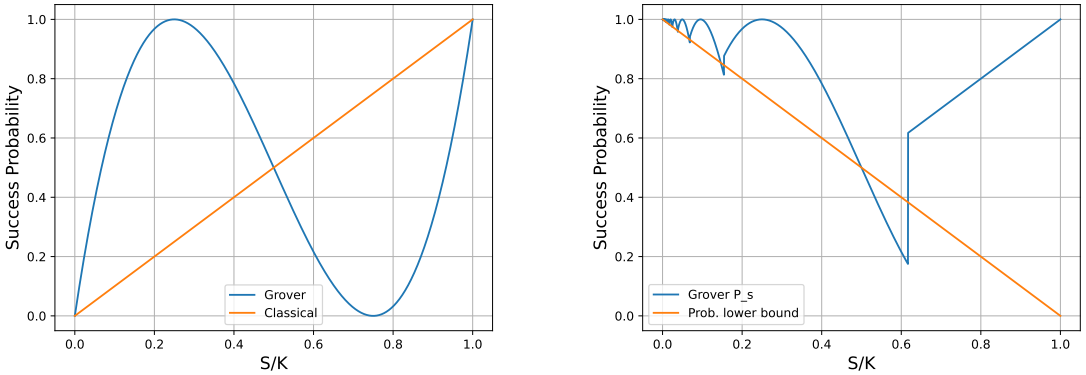
Let us consider a database U with a size K, with a sequence of $U[0, \cdots, K-1]$. Assuming that we have a solution z, which verifies $U[i_0] = z$ where i_0 is the index of our solution. Thus, α and β denote the amplitudes of $|\psi\rangle$, which satisfy $|\alpha|^2 + |\beta|^2 = 1$ in the computational basis ($|0\rangle$, $|1\rangle$), where α refers to the probability of our solutions, and β refers to the probability of other outcomes. Hence, we may write qubit $|\psi(\alpha, \beta)\rangle$ as a function of α and β:

$$|\psi(\alpha, \beta)\rangle = \sum_{i \neq i_0}^{K} \beta|i\rangle + \alpha|i_0\rangle \tag{2.10}$$

Indeed, as illustrated in Fig. 2.4, the Grover's algorithm could be visualized with 2-D dimension. Grover's algorithm changes the phase by θ once the Grover is run [29], making it closely to the solution α. From this figure, we may express (2.10) as a function of θ. Let us assume that $|\psi(\theta)\rangle = \cos\theta|i\rangle + \sin\theta|i_0\rangle$ as illustrated in Fig. 2.4, we may write as follows:

$$\begin{aligned} |\psi(\theta)\rangle &= \cos\theta|i\rangle + \sin\theta|i_0\rangle \\ \mathcal{G}|\psi(\theta)\rangle &= \cos 3\theta|i\rangle + \sin 3\theta|i_0\rangle \\ \mathcal{G}^j|\psi(\theta)\rangle &= \cos((2j+1)\theta)|i\rangle + \underbrace{\sin(2j+1)\theta}_{\alpha}|i_0\rangle \end{aligned} \tag{2.11}$$

where j refers to the number of Grover's iteration. Thus, the success probability is obtained with this equation:



(a) P_G when iteration $j = 1$ (b) P_G when iteration $j = L_{opt}$

Figure 2.5: Analysis success probability (P_G) w.r.t S/K

$$\alpha^2 = P_G = \sin^2((2j+1)\theta) \tag{2.12}$$

which corresponds to our solution, hence, we should maximise this probability.

$$\begin{aligned} \sin^2((2j+1)\theta) &= 1 \\ \sin^2((2j+1)\theta) &= \sin^2(\pi/2) \\ (2j+1)\theta &= \pi/2 \end{aligned} \tag{2.13}$$

From (2.13), we could note that the success probability is maximized if the iteration hits $j = (\pi - 2\theta)/4\theta$ [59]. The equation is simplified by taking into account the huge number of size K and the floor function's rules of equivalences, thus, we have $\lfloor \frac{\pi}{4\theta} \rfloor$. Variable $\theta = \arcsin\sqrt{S/K}$ is obtained clearly from Fig. 2.4, where S is the number of solutions. Thus, we will have : $j = \lfloor \frac{\pi}{4}\sqrt{K/S} \rfloor$ corresponds to our optimum iteration L_{opt}.

$$L_{opt} = \lfloor \frac{\pi}{4}\sqrt{\frac{K}{S}} \rfloor \tag{2.14}$$

It is important to ensure that the size of K is within the limit of $S \leq K$. In the study by [60], it is investigated that the ratio $\frac{K}{S}$ is analyzed as a function of the success probability α^2. The success probability P_G can be expressed as $P_G \geq 1 - \frac{S}{K} \geq 0$.

We have evaluated the analysis when of the ratio number of solutions S with the database size K, denoted as $\frac{S}{K}$. In Fig. 2.5a, we can observe the success probabilities of both the classical and Grover's algorithms for the given iteration $j = 1$. In the

classical algorithm, the success probability α_j shows a linear relationship with S/K. Notably, the success probability reaches 1 when the number of solutions S is equal to K, which is quite evident.

Conversely, Grover's algorithm, owing to the superposition of states, exhibits a fluctuating success probability, following a sinusoidal pattern. The disadvantage of Grover's algorithm is that when the number of solutions S becomes relatively higher, the success probability α tends to decrease significantly.

On the other hand, Fig. 2.5b illustrates the probability of success of Grover's algorithm using different identified values of j as a function of $\frac{S}{K}$. We define the j to be equal to L_{opt} which depends on the K/S. We observe that at $\frac{S}{K} = 0.5$, the algorithm achieves a success probability of 0.5 and then starts to decrease to 0.2. The reason is obvious: when the ratio of S and K is equal, Grover's algorithm searches with equiprobable probabilities, which leads to a probability of 0.5. However, as the value of S/K increases, the success probability starts to decrease again to 0.2 because Grover's algorithm may search differently, assuming that the number of solutions is the same as the number of unwanted solutions, and vice versa. An interesting observation is that at $\frac{S}{K} = 0.25$, the algorithm will succeed with a certainty of 100% after a single iteration while also note that when the $\frac{S}{K} = 0.6$, it shows a very bad success probability on the Grover's side. Furthermore, as S/K becomes high, the behavior becomes similar to classical random guessing, resulting in a high success probability P_s. In Fig. 2.5b, it is observed that the orange line represents the success probability of the lower bound of Grover's algorithm. This implies that we may experience a small success probability as a function of $\frac{S}{K}$.

It is concluded thus in these pictures, the success probability of classical and quantum shows different pattern. The strength and weakness of quantum has been shown in these pictures, which depends on the required number of solutions S and database size K.

Grover's optimum iteration : Unknown Number of Solution

Regardless of the search method, the total number of solutions S is largely unknown. which becomes challenging to find L_{opt}. As a consequence, the idea of how to determine the most effective technique in the database where S is unknown has been proposed.

Boyer, Brassard, Høyer and Tapp proposed a method called BBHT to find a certain solutions where no prior knowledge is needed [59]. The BBHT defines the upper-bound complexity of the Grover's algorithm when the number of solutions S is unknown, which leads to unknown L_{opt}. To find this way, BBHT's idea computes the average success probability P_m, derived from P_G in Eq. 2.12. The concept involves determining the the average of P_G after doing m iterations. The average of this success probability is denoted as P_m which is expressed as follows:

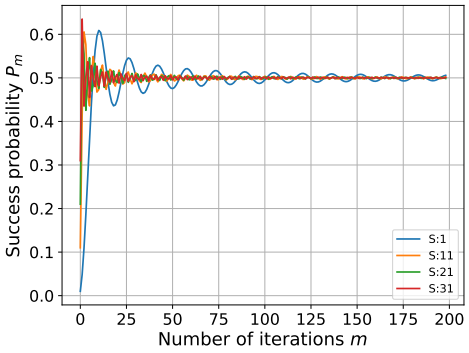
$$
\begin{aligned}
P_m &= \sum_{j=0}^{m-1} \frac{1}{m} \sin^2((2j+1)\theta) \\
P_m &= \sum_{j=0}^{m-1} \frac{1}{2m} (1 - \cos((2j+1)2\theta)) \\
P_m &= \frac{1}{2} - \frac{\sin(4m\theta)}{4m\sin(2\theta)}
\end{aligned}
\tag{2.15}
$$

where m is the maximum number of Grover iterations, P_m is the average success probability of a particular maximum iterations m. Indeed, we may note that if we have $m \geq 1/\sin(2\theta)$, then $P_m < \frac{1}{4}$.

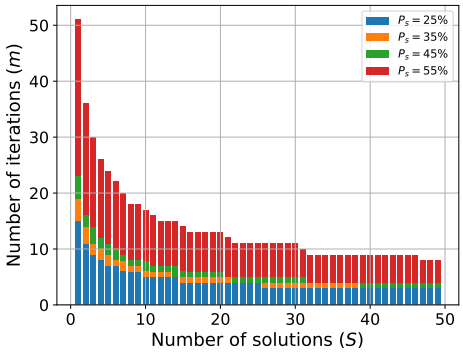
It is important to note that the success probability, represented as P_m in Fig. 2.6a, never reaches 100% although the solutions S are varied, assuming using $K = 100$. This is due to two key variables: θ and m. Firstly, the optimal iteration, denoted as L_{opt}, is achieved when m is equal to $\lfloor \frac{\pi}{4}\sqrt{\frac{K}{S}} \rfloor$. The optimum value for L_{opt} occurs when S is equal to 1, resulting in $L_{opt} = \lfloor \frac{\pi}{4}\sqrt{K} \rfloor$. On the other hand, θ is determined by $\theta = \sin^{-1}(\frac{S}{K})$. When θ is multiplied by m, the resulting value becomes 0. As a consequence, if K is relatively large, the expression $\frac{\sin(4m\theta)}{4m\sin(2\theta)}$ evaluates to 0. Thus, we can conclude that P_m should be equal to $\frac{1}{2}$.

The second reason, from Eq. 2.10, we can gain an intuitive understanding of the situation. In this equation, we have two probability amplitudes, represented by α and β. If our goal is to maximize the success probability of α, we should note that the highest achievable probability would be approximately 50%, assuming that the amplitude of β is also present. Thus, we should run the BBHT algorithm at least *twice* to obtain the best result.

In Fig. 2.6, we conducted an evaluation of the equation P_m, considering variations in both the parameter m and the number of solutions S. The results show that a smaller number of solutions S corresponded to a higher number of iterations m. In Eq. 2.14, we noticed an inverse relationship between the number of solutions S and the optimum iteration value L_{opt}. Specifically, as the number of solutions S decreased, the optimum iteration L_{opt} increased. The distinction between the red and blue bars is significant since the red bars represent instances with high success probability P_s, while the blue bars indicate lower success probability P_s. This disparity in success probabilities is primarily due to the fact that achieving a high P_s requires a certain number of iterations m_1, which is higher than the number of iterations m_2 associated with the lower success probability P_s.



(a) P_m as a function of m



(b) The number of iterations m as a function of number of solutions S

Figure 2.6: Analysis of average success probability P_s, $K = 100$

BBHT Algorithm

Let us consider the number of solutions S unknown s.t $0 \leq S \leq 3K/4$, the BBHT algorithm is fully written as follows:

Algorithm 1: BBHT Algorithm

$m \leftarrow 1$, $\lambda \leftarrow \frac{6}{5}$, and $L_{BBHT} \leftarrow 1$;
Choose j such that $0 \leq j \leq \lfloor m \rfloor$;
Initiate the superposition $|\psi\rangle = \frac{1}{\sqrt{K}} \sum_{x=0}^{K-1} |x\rangle$ as explained in Eq.(2.7);
Apply Grover's algorithm: $x_{out} = \mathcal{G}^j |\psi\rangle$;
Set $L_{BBHT} \leftarrow L_{BBHT} + 1$;
Observe the outcome of x using quantum measurement;
if $U[x_{out}] = z$ **then**
    The solution is found;
end
else
    Set $m \leftarrow \min(\lambda m, \sqrt{K})$;
end

BBHT proposes to initiate the *critical stage* of the average success probability, where its iteration is considered start from $m_0 \geq 1/\sin(2\theta)$ with $P_m = 1/4$. The analysis of critical stage is based on [61]:

$$m_0 = \frac{1}{\sin(2\theta)} = \frac{1}{2\sin\theta\cos\theta} = \frac{K}{2\sqrt{(K-S)S}} < \sqrt{K/S} \tag{2.16}$$

The critical stage is defined where Grover's algorithm starts to find large success probability while also keeping low iterations. In this case, we consider $0 \leq S \leq 3K/4$

[60]. Thus, the required iterations reaches the *critical stage* if it loops more than $\lceil \log_\lambda m_0 \rceil$. To compute the number of iteration until it achieves *critical stage*, BBHT uses λ variable as a counting variable, to control how many iterations needed. Thus, the expected number of times $\hat{E}_1$ is shown as follows :

$$\begin{aligned} \hat{E}_1 = \frac{1}{2} \sum_{s=1}^{\lceil \log_\lambda m_0 \rceil} \lambda^{s-1} &= \frac{1}{2} \frac{(1 - \lambda^{\lfloor \log_\lambda m_0 \rfloor})}{1 - \lambda} \\ \hat{E}_1 &< \frac{1}{2} . (\frac{\lambda^{\log_\lambda m_0} . \lambda^1 - 1}{\lambda - 1}) \\ \hat{E}_1 &< \frac{1}{2} (\frac{\lambda . m_0}{\lambda - 1}) \end{aligned} \tag{2.17}$$

Since $m \geq 1/\sin(2\theta)$, if the critical stage is reached, the main loop will succeed with a probability of at least $1/4$ every time around from this point on. As a result, after the critical stage has been reached, the expected number of Grover iterations required to succeed is upper-bounded $\hat{E}_2$ by:

$$\hat{E}_2 = \frac{1}{2} \sum_{u=0}^{\infty} \frac{3^u}{4^{u+1}} \lambda^{u + \lceil \log_\lambda m_0 \rceil} \tag{2.18}$$

Since, we could replace $\lceil \log_\lambda m_0 \rceil < \log_\lambda m_0 + 1$, thus, we could have :

$$\begin{aligned} \hat{E}_2 &< \frac{1}{2} \sum_{u=0}^{\infty} (\frac{3\lambda}{4})^u \lambda^1 \frac{1}{4} m_0 \\ \hat{E}_2 &< \frac{1}{2} \frac{1}{4} \lambda^1 m_0 + \frac{1}{2} \frac{1}{4} \lambda^1 (\frac{3}{4})^1 \lambda^1 m_0 + \cdots \end{aligned}$$

Let us multiply with $E_2(\frac{3}{4}\lambda)$:

$$\hat{E}_2(\frac{3}{4}\lambda) < \frac{1}{2} \frac{1}{4} \lambda^1 (\frac{3}{4})^1 \lambda^1 m_0 + \frac{1}{2} \frac{1}{4} \lambda^1 (\frac{3}{4})^2 \lambda^2 m_0 + \cdots$$

Then substract it with $E_2 - E_2(\frac{3}{4}\lambda)$:

$$\begin{aligned} \hat{E}_2 - \hat{E}_2(\frac{3}{4}\lambda) &< \frac{1}{8} \lambda m_0 \\ \hat{E}_2 &< \frac{\lambda}{8 - 6\lambda} m_0 = \frac{3}{2} m_0 \end{aligned}$$

The total number of iterations thus leads to $\hat{E}_1 + \hat{E}_2 = \frac{3}{2} m_0 + 3 m_0 = \frac{9}{2} m_0$. As we have discussed, the BBHT algorithm requires twice the number of iterations to obtain the maximum success probability. Thus, the total number of iterations should be $2m_0$.

A Quantum Algorithm for Finding the Minimum

A quantum algorithm for finding the minimum locates the index of a smaller item than the value set by a predetermined threshold index. Assuming database U with size K. We should find o_x which permits to verify $U[o_x] < U[o]$, where $\forall o \in K$. This algorithm is proposed by Durr-Hoyer Algorithm [62], namely DHA algorithm, in order to find the minimum of the database, and detailled in algorithm (2). The algorithm below finds the index of the minimum value with probability at least $1/2$, while its running complexity is $\mathcal{O}(\sqrt{N})$.

Algorithm 2: DHA Algorithm

1 $L_{DHA} \leftarrow 0$;
2 Choose uniformly $0 \leq o \leq K-1$;
3 **while** $L_{DHA} \leq 22.5\sqrt{K} + 1.4\log^2 K$ **do**
4 Initialize the memory as $\sum \frac{1}{\sqrt{K}}|o_x\rangle|o\rangle$. Mark every item o for which $U[o_x] < U[o]$.;
5 Apply the BBHT algorithm;
6 Observe the register. Let o' be the outcome. If $U[o'] < U[o]$, then set threshold index o to o'.;
7 $L_{DHA} \leftarrow L_{DHA} + 1$;
8 **end**
9 Return o;

Algorithm (2) describes the full algorithm of DHA to find a certain value set by an index. Indeed, step $1-3$ do not require a high complexity, since it is computed once. Nonetheless, stage 4 requires an initialization process to initiate the index and the superposition of states. Thus, this stage is considered to be calculated as a high complexity.

Let us consider that $p(K, r)$ is the probability that the index of the element of rank r will ever be chosen when the infinite algorithm searches among K elements. The complexity can be expressed as follows :

$$\begin{aligned}\sum_{r=2}^{N} p(K,r)\log_2(K) &= \frac{1}{r}\log_2(K) \\ &\leq \ln(K)\log_2(K) \\ &\leq \ln 2\log_2(K)\log_2(K) \\ &\leq \frac{7}{10}\left(\log_2(K)\right)^2\end{aligned} \tag{2.19}$$

The initial superposition only requires N qubits to represent 2^N possibilities, which is also given by $\log_2(K)$ in this context. Afterwards, stage 5 is considered to have

high complexity since it executes the Grover's algorithm when there is an unknown number of solutions, as described in section 2.2.3 for the BBHT part. As we note that the complexity is $\frac{9}{2}\sqrt{K/S}$. Thus, the expected total time used by the infinite algorithm before y holds the index of the minimum is at most:

$$\begin{aligned}
\sum_{r=2}^{N} p(K,r)\frac{9}{2}\sqrt{\frac{K}{r-1}} &= \frac{9}{2}\sqrt{K}\sum_{r=1}^{K-1}\frac{1}{r+1}\frac{1}{\sqrt{r}} \\
&\leq \frac{9}{2}\sqrt{K}\left(\frac{1}{2}+\sum_{r=2}^{K-1} r^{-3/2}\right) \\
&\leq \frac{9}{2}\sqrt{K}\left(\frac{1}{2}+\int_{r=1}^{K-1} r^{-3/2}\mathrm{dr}\right) \\
&\leq \frac{9}{2}\sqrt{K}\left(\frac{1}{2}+\left[-2r^{-1/2}\right]_{r=1}^{K-1}\right) \\
&\leq \frac{45}{4}\sqrt{K}
\end{aligned} \tag{2.20}$$

In total, the complexity is the sum of stage 4 and 5, which is $\frac{45}{4}\sqrt{K}+0.7(\log K)^2$. However, as proposed by by [62], the probability to find the minimum is at least 0.5, thus, we may calculate the complexity of 2 iterations to obtain higher probability at 1. Then, after multiplied by two, the complexity is $\frac{45}{2}\sqrt{K}+1.4\log^2 K$.

2.3 Quantum Review Progress

This section elaborates on the concept where quantum has been explored within the context of (AUD), along with the enhancement of the DHA. It is important to highlight that quantum techniques have been employed in various aspects, including multiple access scenarios. The Grover's algorithm is particularly brought into focus with the aim of reducing complexity. We will discuss the improvement of Grover's algorithm in the context of finding the minimum, how Grover's is improved in general, and also how Grover's algorithm is applied to wireless communication.

2.3.1 Grover's algorithm for Wireless communication

This subsection discusses papers related to the utilization of Grover's algorithm in the context of wireless communication. Table 2.2 provides an overview of authors and their respective contributions that have employed Grover's algorithm within the realm of wireless communication. Primarily, it is observed that Grover's algorithm is predominantly harnessed to attain reduced complexity when compared to classical methods. It is worth recalling that Grover's algorithm exhibits the remarkable

capability of achieving a time complexity of $\mathcal{O}(\sqrt{2^N})$. Additionally, Grover's algorithm is utilized to achieve performance along with optimal ML approaches while also keeping the complexity as low as possible in the context of Multi-User Detection (MUD) and Active User Detection (AUD). This subsection will discuss several contributions related to Grover's algorithm in the field of wireless networks.

First of all, from a mathematical perspective, multiple authors have contributed to the field of mathematics, with publications such as those by [63], [64], and [65]. These authors have mathematically demonstrated the applicability of Grover's algorithm to Multi-User Detection i.e. recovering the data transmitted by several users. Their work underscores a significant reduction in complexity from $\mathcal{O}(2^N)$ to $\mathcal{O}(N)$, as highlighted.

Let us consider a simulation example from the work by the author in [66]. The proposal in this study suggests the utilization of the Quantum-Assisted Message Passing Algorithm, denoted as Q-MPA. This algorithm draws inspiration from both MUD and the traditional MPA. The superposition of states in Q-MPA enables a faster search process for maximization compared to the classical MPA. Q-MPA is essentially created by incorporating Grover's searching algorithm to expedite the message updating procedure within MPA. The outcome of this study indicates that Q-MPA effectively reduces the complexity of the total Number of Cost Functions (NCFE), with only a negligible loss in Bit Error Performance (BER) performance.

Another example of the same author [67] introduces the proposed solution known as Multiple Symbol Differential Detector (MSDD) with a quantum-assisted. The optimization process carried out by MSDD involves identifying the most probable decision candidate for transmitted multi-level symbols, and this can be effectively executed by trading off the number of iterations. This method employs Grover's algorithm to achieve this goal which is promising to reduce the number of Cost Function Evaluation (CFE). The result shows that MSDD with quantum performs better compared with the Conventional Correlation Detector (CCD) with also a reduced complexity compared to the traditional MSDD.

In another study by the same author [68], an enhancement to the quantum mean algorithm (QMA) is presented, resulting in the development of the Quantum Weight Searching Algorithm (QWSA). This QWSA is harnessed to devise a Quantum Assisted Multi-User Detection (QMUD) system that relies on soft inputs and soft outputs. To detect multi-level symbols, the DHA is implemented prior to employing the QWSA. The findings illustrate that the QWSA-based MUD has the same performance with ML MUD, while boasting significantly reduced complexity.

Furthermore, Grover's algorithm is also utilized to curtail the computational complexity of both mm-Wave-based and Visible Light Communication (VLC)-based localization algorithms, while upholding optimal performance [69]. The author utilizes DHA to find the VLC localization problems, optimizing it based on Grover's algorithm. The outcomes underscore the significant reduced made in complexity. This also applies

to [70] which centers on utilizing the QMUD on the video applications.

A similar extension work by the same author [71] where they propose the adoption of Multi-Carrier Interleave Division Multiple Access (MC-IDMA) systems, inheriting principles from Grover's algorithm. Consistent with the previously obtained results, The initial impression conveyed is that Grover's algorithm consistently leads to reduced complexity in various applications.

Expanding on his previous work, Botsinis also introduces an enhancement in locating the minimum DHA through a paper proposed by [72] in the context of Code Division Multiple Access (CDMA) and Space-Division Multiple Access (SDMA). The essence of this approach lies in improving the DHA by incorporating a semi-knowledge value that effectively mitigates certain complexities, which is denoted as Early Stopping-aided Durr-Hoyer algorithm-based QMUD. The result again shows a low complexity compared to the original DHA.

The alternative method that harnesses MUD using quantum principles is proposed by [73], which suggests incorporating quantum rotation into MUD. In addition to Grover's algorithm, this quantum rotation method has successfully reduced complexity. While the classical MUD leads to a Non-polynomial (NP) problem, QMUD is much simpler. Furthermore, its performance is compared with the Bayesian solution, demonstrating that quantum rotation exhibits superior performance with lower complexity requirements.

Grover's algorithm finds application in various routing protocols, as indicated by [74], [75], [76], and [77]. The first paper, [74], introduces Grover's algorithm in the context of Mobile Ad Hoc Networks (MANET), aiming to accommodate dynamic topology changes without the reliance on fixed infrastructure. The outcomes demonstrate that the utilization of Grover's algorithm leads to a reduction in forwarded packets among nodes, consequently lowering the computational load.

In contrast, [75] employs Grover's algorithm within an asymmetrical quantum encryption protocol. In this scenario, the sender prepares an initial private state and applies a phase shifter (Diffuser) to their bit. Assuming multiple receivers, the recipients of these states perform inversion operations. The recipient capable of deploying the searching algorithm in accordance with specific constraints becomes the recipient of the bit. This application of Grover's algorithm enhances the security and integrity of the communication protocol.

Addressing network management within communication systems, [76] and [77] apply the quantum extreme value searching algorithm as a Minimum Searching Algorithm (MSA), integrating it with the established logarithmic binary search algorithm. By comparing against random modes, this method improves resource distribution and significantly reduces computational complexity, thus effectively addressing computational resource utilization challenges.

Botsinis, in collaboration with colleagues, implemented Grover's algorithm in both

coherent and non-coherent wireless systems, as documented in [78]. Coherent symbol mapping enables accurate carrier phase and timing synchronization, whereas non-coherent mapping operates without relying on precise phase and timing synchronization. The key takeaway is that Grover's algorithm shows great promise in achieving near-optimal performance with a high Bit Error Performance (BER) but maintains low complexity. Additionally, in a study conducted by Botsinis, as described in [79], quantum technology was harnessed to outperform RWBS. The improved system is termed QRWBS. QRWBS demonstrates near-optimal performance compared to classical RWBS and maintains a low-complexity profile, thanks to quantum technology.

In another study, Wengjing Yu, as documented in [80], explored QMUD based on coherent state signals, which exhibits quantum behavior closely resembling classical state signals. The study concludes that a higher average number of photons from the users leads to smaller interference between user. Furthermore, Fei Li's work, as explained in [81], within the context of MIMO-OFDM, demonstrates a high success probability close to an optimal ML detector. This success is achieved while maintaining a low level of complexity compared to traditional ML detectors.

In conclusion, Grover's algorithm has found extensive applications in wireless communication, offering two key advantages: 1) Low complexity and 2) Near-optimal performance.

2.4 Conclusion

This chapter has discussed the system model of the AUD, along with the codetypes used (i.e., Unipolar, Bipolar, and Random Gaussian) and their motivations. We have also covered conventional approaches to address the AUD issue, spanning from the most efficient (such as ML) to less efficient methods (namely, CCR and ZF). Additionally, we have discussed a comparison of classical search algorithms in terms of finding a value and their complexity.

Furthermore, we introduced quantum algorithm as a new solution based on the superposition of states, which promises to achieve reduced complexity. One of the known algorithm to handle the complexity on the database is Grover's algorithm. We discussed Grover's algorithm and its behavior, including its success probability and complexity. We also explored how Grover's algorithm operates when there is no known number of solution in the database and how it can be used to find the minimum when the number of solution is unknown. Finally, we discussed how Grover's algorithm has been implemented in various applications within the context of wireless networks.

In conclusion, we find that Grover's algorithm is a promising approach for addressing the AUD problem, offering both high performance and low complexity. We will delve further into this topic in the next chapter.

Authors	Year	Tools	Contribution
Sándor Imre et al [63]	2002	Grover's Algorithm in QMUD	Proposes the solution to solve the MUD problem which leads to Non-polynomial (NP)-Problem using the method of Grover's algorithm (From complexity $\mathcal{O}(2^N)$ to $\mathcal{O}(N)$). It conveys how to prove it mathematically.
Sandor Imre and Laszlo Gyongyosi [64]	2012	Quantum-Assisted, Quantum-Based Solutions	Reducing the transmit power and mitigating the resultant signal-degradation imposed by the transmit-power,this is denoted by quantum-assisted which is based on Grover's algorithm.
Zhao Shang-Mei et al [65]	2006	Applying Grover's algorithm to MUD	Using the Grover Algorithm to identify the QMUD, which is promising to reduce the number of complexity by $\mathcal{O}(2^N)$.
Wenjing Ye et al [66]	2019	Quantum-Assisted Message Passing Algorithm (Q-MPA) based MUD and Quantum-Assisted Sphere Decoder-based MPA (QSD-MPA)	The Q-MPA was conceived by adopting the Durr-Hoyer Quantum Search Algorithm (DH-QSA) to accelerate the maximization search process of the classical MPA.
Botsinis et al [67]	2015	Soft-output quantum-assisted Multiple Symbol Differential Detector (MSDD))	In this treatise, we propose low-complexity hard-input hard-output, hard-input softoutput, as well as soft-input soft-output quantum-assisted MSDD that perform equivalently to the optimal, but highly complex maximum a posteriori probability MSDDs in multiuser systems, where the users are separated both in the frequency domain and in the time domain. When using an MSDD. MSDD performs better compared with the Conventional Correlation Detector (CCD). In the CCD, it performs the inverse procedure detected, differentially modulated symbol. In MSDD, make a decision.
Botsinis et al [68]	2013	Soft-input Soft-output QMUD and Quantum-domain equivalent of the QMUD	The performance of the proposed QMUD and that of the optimal classic MUD are equivalent, but the QMUD's computational complexity is significantly lower.
Botsinis et al [69]	2017	Grover's algorithm applied to mm-Wave-based and VLC-based localization algorithms	The paper demonstrates the use of Quantum Searching Algorithm (QSA) to reduce the computational complexity of both the mm-Wave-based and VLC-based local- ization algorithms while maintaining optimal performance. This approach helps to overcome the excessive computational complexity associated with searching on a virtual grid.
Botsinis et al [70]	2017	Durr-Hyer Algorithm Multi-input Approximation Forward Knowledge Transfer Quantum-Assisted Multi-User Detection (DHA-MUA-FKT QMUD)	In this paper, we demonstrate the benefits of Quantum Assisted Multi-User Detection (QMUD) in the uplink of a multi-user system, where the reference user conveys a multilayered video stream to the base station, while using adaptive modulation and different rates per video layer.
Botsinis et al [71]	2015	Multi-Carrier Interleave Division Multiple Access (MC-IDMA)	It is demonstrated that the family of Durr-Hyer Algorithm Multi-input Approximation Quantum-Assisted Multi-User Detection (DHA-MUA QMUD) is amenable to performing iterative detection, hence offering a near-optimal performance, approaching that of the Maximum a posteriori (MAP) MUD, in contrast to the DHA-Maximum Approximation (MAA).
Botsinis et al [72]	2014	Early Stopping-aided Durr-Høyer Algorithm-based Quantum Assisted	It proposes the Early Stopping-aided Durr-Hyer Algorithm-based Quantum Assisted MUD based on two techniques for achieving optimal ML solution. The idea is to improve the existing DHA where the initial chosen scenario is uniformly distributed, while using Early stopping has a semi-prior knowledge. This paper discusses the application for Soft-input Soft-output (SISO) QMUD.
Sheng-Mei Zhao et al [73]	2005	Quantum Rotation, Quantum Multi-User Detection	The simulation results illustrate that the performance of quantum multi-user detection can be improved greatly when quantum rotation algorithm is employed.
Meng Li-min et al [74]	2010	This paper puts forward a routing algorithm based on Grover searching theory for Mobile Ad Hoc Networks (MANET)	It first gives the Grover searching theory and the construction way of probability branch matrix and solution path matrix which are suitable for MANET
Luo Wenjun, Liu Guanli [75]	2014	Proposed asymmetrical quantum ecryption protocol based on Grover's QSA and trapdoor One-way quantum function (OWQF)	Introduce a new method based on Grover's QSA and trapdoot OWQF.
Sara El Gaily, Sándor Imre [76] [77]	2019	Quantum Extreme Value searching algorithm, as a Minimum Searching Algorithm (MSA)	Based on Grover's algorithm, A proposed resource distribution management model based on quantum optimization approach is introduced in this paper. The proposed quantum strategy can guarantee low computational complexity and high accuracy.
Botsinis et al [78]	2017	Grover's algorithm applied to coherent and non-coherent in wireless systems	Grover's algorithm is applied to coherent and non-coherent systems with achieving the best Bit Error Performance (BER), and low complexity.
Botsinis et al [79]	2016	Quantum-assisted repeated weighted boosting search (QRWBS) for joint Channel Estimation (CE) and MUD in MIMO-OFDM	The proposed algorithm outperforms the classical RWBS-aided CE in terms of performance, despite acquiring lack of complexity.
Wenbin Yu et al [80]	2019	Grover's Algorithm	This author presents the maximum channel capacity using a two-access quantum channel. It shows also the average interference between different users and average error probability is derived mathematically.
Fei Li et al [81]	2011	A novel signal detector based on Grover's algorithm for MIMO-OFDM	The performance of Grover's algorithm is close to the optimal ML detector when the probability of obtaining the incorrect solution P is 0.001. The Grover complexity reaches $\mathcal{O}(\sqrt{2^N})$ while ML achieves $\mathcal{O}(2^N)$.

Table 2.2: Quantum papers related to wireless communication

Chapter 3

Chapter 3

Adapting Grover's algorithm for AUD

The significant increase in the number of connected mobile devices has introduced new challenges when it comes to efficiently utilizing network resources. Typically, various multiple access schemes lead to interference issues, which, in turn, pose a challenge for the AUD problem, as described in section 1.3.1. This problem demands the ability to detect active users blindly, requiring a high level of complexity. Specifically, the ML, requires to test all possibilities of set activity users. While there are alternative methods more direct than ML like CCR, ZF, PIC, and SIC that aim to reduce this complexity, they often come at the expense of reduced performance.

Here, we employ the basic Grover's algorithm as the initial step in developing a version that can rival ML in performance while simplifying its complexity, reminding that implementing the ML principle in the quantum domain is not straightforward. We investigate the AUD problem within the framework of Grover's algorithm. We employ different codebooks and consider scenarios with and without noise. This approach is promising in addressing both performance and complexity issues. Additionally, we evaluate the adaptation of the original Grover's circuit for implementation in the AUD. Our objective is twofold: to decrease the complexity while simultaneously enhancing the performance.

Key Takeaways:

- Adapting the Grover's algorithm for AUD using multiple codes.
- Design the Grover's circuit for AUD using multiple codes
- Showing the performances and complexity between Grover's algorithm and Classical Methods in noisy and noiseless channels.

Parts of this chapter were published as part of the following articles:

- M. I. Habibie, J. Hamie and C. Goursaud, "Adaptation of Grover's Quantum Algorithm to Multiuser Detection in an OCDMA System," 2021 IEEE Symposium On Future Telecommunication Technologies (SOFTT), Bandung, Indonesia, 2021, pp. 88-93
- M. I. Habibie, J. Hamie and C. Goursaud, "A Performance Comparison of Classical and Quantum Algorithm for Active User Detection," 2022 IEEE 23rd International Workshop on Signal Processing Advances in Wireless Communication (SPAWC), Oulu, Finland, 2022, pp. 1-5.

3.1 Introduction

The increasing number of users connected to the mobile network has brought numerous challenges in efficiently utilizing available resources. This has highlighted an issue in the Active User Detection (AUD) problem, where the current approach demands significant complexity, specifically involving Maximum Likelihood (ML). While other established methods like Conventional Correlation Receiver (CCR), Zero Forcing (ZF), Successive Interference Cancellation (SIC), Parallel Interference Cancellation (PIC), hold the promise of reducing this complexity, they often result in suboptimal performance. Consequently, in this chapter, we investigate the application of Grover's algorithm, a quantum-based approach, to address both aspects: complexity and performance.

The performance of Grover's algorithm should be similar with that of ML while also keeping the complexity as low as possible. The principle of ML is to identify the most likely active set of users based on the given observed signal. Grover's algorithm proposes to achieve this by implementing the same principle. Nevertheless, applying quantum computing based on the same principle as ML is not a straightforward solution, as no existing quantum algorithm can be directly used for this problem.

Therefore, we are moving toward this goal step by step. In this chapter, we present the first step where we adapt Grover's algorithm to a specific case of the ML problem. Grover's algorithm is designed to search x such that $f(x) = \delta$ with a predefined function f and δ. In a transmission system, this corresponds to the case where there is no noise, and the channel coefficients are known. Thus, in this chapter, we consider this case.

This chapter provides a comprehensive and detailed description of a simple Grover's algorithm for AUD with the objective of solving the equation $f(x) = \delta$. We will explain and demonstrate the construction of the Grover's circuit, focusing on a simple case, and discuss how to adapt the algorithm for AUD using various code families. Our primary goal in this chapter is to examine the performance and complexity of Grover's algorithm, building upon our earlier discussions. We conduct a comparative analysis between Grover's algorithm and other classical methods such as ML, CCR, and ZF with a noiseless and noisy cases. Through this analysis, we will compare the performance and complexity of the quantum algorithm in relation to these classical methods.

3.2 Developing Grover's circuit

This section describes how to adapt the Grover's circuit into the case of AUD. As shown on sec 2.2.3, the Grover relies on oracle $\mathbf{O}$, diffuser $\mathbf{D}$, with a Hadamard gate to create a superposition of states as illustrated in Fig. 3.1. Grover consists of four registers [82]:

1. Index Register: contains the argument of the function $f(x)$ which provides the targeted results
2. Value Register: contains the value of function $f(x)$
3. Reference Register: corresponds to the targeted value $|\delta\rangle$
4. Mark Register: computes the negative sign as stated in (2.8) in order to mark the qubits.

An example of the whole Grover's circuit is shown in Fig. 3.1 where $N = 2$ is the number of qubits on the Hilbert space, allowing for four different computational basis states $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$.

The number of qubits for the value and reference registers are $Z + p$ qubits, which stand for the quantity of qubits needed to store the result of the function $|f(x)\rangle$. The last, *Mark register* occupies 1 qubits to calculate the negative computation. Here, Fig. 3.1 shows a simple circuit where implementing the Identity function $f(x) = x$,

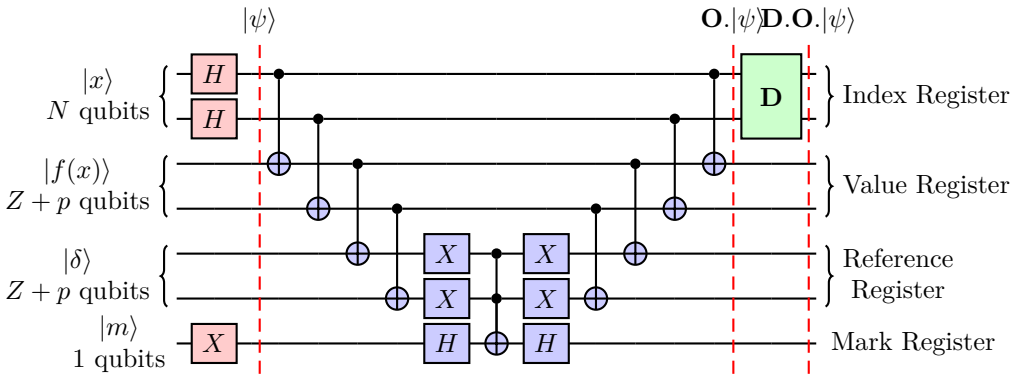


Figure 3.1: Grover's Circuit $n = 2$ qubits $f(x) = \delta$

everything provided by targeted value δ corresponds to the index of the qubit $|x\rangle$. All components of the qubits in Grover's circuit operate on a binary representation; thus, the integer value is converted to its binary representation as described in the next subsection.

3.2.1 Quantum constraint

The received signal, denoted as $\mathbf{y}$, consists of real components belonging to the positive real numbers, $\mathbf{y} \in \mathbb{R}^+$. However, as for classical digital processing, when considering the quantum aspect, quantum algorithms operate using binary representation, namely, the values 0 and 1. Therefore, to address this discrepancy, we use an approximation of $\mathbf{y}$ to the nearest discrete value. The integer part of $\mathbf{y}$ that is retained is upper bounded by $2^Z - 1$, where Z, represents the number of qubits assigned to represent the integer part of $|f(x)\rangle$. However, since we need to represent a real value in binary form on the circuit, we need p qubits to represent the decimal part, where $p \in \mathbb{N}$ denotes the precision qubits. A higher precision value p in the circuit leads to more accurate results, however, it also requires a larger memory capacity. This number of qubits $Z + p$, should have the same size qubits of $\mathbf{y}$, while $\mathbf{y}$ is obtained from Eq. 2.1. Additionally, the lower bound is strictly set to 0.

To sum up, y is converted into $\tilde{y}$, as denoted in 3.1. In Grover's algorithm, $\tilde{\mathbf{y}}$ is fed into the *reference register* as δ, as shown in Fig. 3.1:

$$\tilde{\mathbf{y}} = \min\left(\max\left(0, \frac{\text{round}(\mathbf{y} \cdot 2^p)}{2^p}\right), 2^{Z-1}\right) \tag{3.1}$$

3.2.2 Quantum Environment

It is noted that, in this context, we develop Grover's circuit under the assumption of negligible *quantum noise*. We presume the existence of a perfect gate in this scenario. The simulation is conducted using a quantum emulator, specifically the **aer simulator** with a noise-free quantum, which assumes a perfect gate without noise. This simulation is implemented on the **Qiskit** quantum platform, designed for simulating small qubit systems.

In cases where we simulate a higher number of qubits (more than 30 qubits), our simulator encounters limitations. Consequently, when dealing with more than 30 qubits, we optimize it with MATLAB to solve our problem, as it demonstrates the capability to handle a larger number of qubits [83]. It is noted that MATLAB operates only the algorithm, not based on the gate.

3.2.3 Quantum Complexity

There are several metrics that can be calculated to determine the complexity of the quantum, such as measuring the number of quantum gates, the number of qubits, the depth of the circuit, the number of queries (referred to as Query Complexity), etc. However, in this thesis, we are solely focusing on *quantum speedup*, which allows us to determine the number of iterations between the classical and quantum algorithms. This is indeed a crucial step before delving into higher levels of quantum analysis, such as analyzing the depth of complexity. Thus, we are focusing on the number of Grover's iterations speedup compared with the classical iterations [84].

3.2.4 Design Setup

As referred to 2.1.1, we consider in our work, for simplicity purpose, small Spreading Factor (SF), in order to limitate the circuit size and improving its understanding. Indeed, one may note that small circuits are easier and faster to simulate. Thus, without loss of generality, we focus in this thesis on small SF. Let us denote the codebook $\mathbf{C}$ consisting of component c_{ij} where $i \in \{1, 2, \cdots, N\}$ and $j \in \{1, 2, \cdots, SF\}$ with several code families as defined in the next subsections.

Unipolar Model

In one specific scenario, we consider $N = 4$ and $SF = 3$. Each user i sends a codeword c_i, which is spread with a factor of $SF = 3$. Given that there are four users $N = 4$, each user transmits one code taken from the codebook denoted as $\{c_1, c_2, c_3, c_4\}$ where it is chosen as follows: $c_1 = [1, 1, 0]$, $c_2 = [0, 1, 1]$, $c_3 = [0, 0, 1]$, and $c_4 = [1, 0, 1]$. Recall

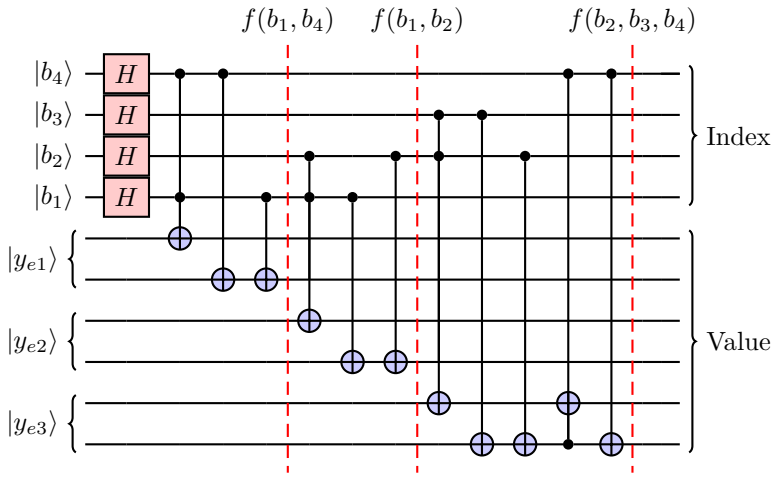


Figure 3.2: Modified Oracle: $|y_{e1}\rangle = f(b_1, b_4), |y_{e2}\rangle = f(b_1, b_2), |y_{e3}\rangle = f(b_2, b_3, b_4)$

that $\mathbf{b} \in \{0,1\}^N$ represents the set of users activity, as explained in subsection 2.1.1. The expected received sequence $\mathbf{y_e}$, which includes noise components, can be derived using the following equations:

$$\mathbf{y_e} = \mathbf{b}.\mathbf{C}$$

$$\mathbf{y_e} = \begin{bmatrix} \mathbf{y_{e1}} \\ \mathbf{y_{e2}} \\ \mathbf{y_{e3}} \end{bmatrix} = \underbrace{\begin{bmatrix} b_1 & b_2 & b_3 & b_4 \end{bmatrix}}_{\mathbf{b}} \underbrace{\begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \\ c_{41} & c_{42} & c_{43} \end{bmatrix}}_{\mathbf{C}} \tag{3.2}$$

$$\mathbf{y_e} = \begin{bmatrix} \mathbf{y_{e1}} \\ \mathbf{y_{e2}} \\ \mathbf{y_{e3}} \end{bmatrix} = \begin{bmatrix} b_1 + b_4 \\ b_1 + b_2 \\ b_2 + b_3 + b_4 \end{bmatrix}$$

After receiving $\mathbf{y}$, we should calculate the rounding function as proposed in Eq. 3.1 to obtain $\tilde{\mathbf{y}}$. Grover's algorithm is fed with $\tilde{\mathbf{y}}$, then modified by the ($\mathbf{O}$) oracle, especially the *Value Register* which refers to $|f(x)\rangle$. The change in $|f(x)\rangle$ corresponds to the value of $|\delta\rangle$, which also affects $|x\rangle$ in the end.

Since the Grover's circuit uses b as the independant variable, the notation can be expressed as $y = f(b_1, b_2, \ldots, b_N)$. Consequently, the representation of each component can be defined as follows: $\mathbf{y}_1 = f(b_1, b_4) = b_1 + b_4$, $\mathbf{y}_2 = f(b_1, b_2) = b_1 + b_2$, and $\mathbf{y}_3 = f(b_2, b_3, b_4) = b_2 + b_3 + b_4$. Thus, the designed circuit is illustrated in Fig. 3.2.

In the realm of qubits, it is important to note that the ordering of the bits is reversed compared to classical bits. This means that the Least Significant Bit (LSB)

is represented with a higher order. For instance, as shown in Fig. 3.2, we can observe that in this particular scenario, b_4 represents the LSB of the set of active users $b \in \mathbf{B}$.

Bipolar Model

Let us consider another code type, Bipolar, with an example in a small case where $N = 3$ and SF$= 3$. Let us assume a family non-orthogonal bipolar codes represented as follows: $c_1 = [-1, 1, -1], c_2 = [-1, -1, 1], c_3 = [1, -1, -1]$. Each message is carried by each user $i \in N$ and $k \in$ SF with a spreading factor SF$= 3$. The expected received sequence $\mathbf{y}$ can be derived using the following equations :

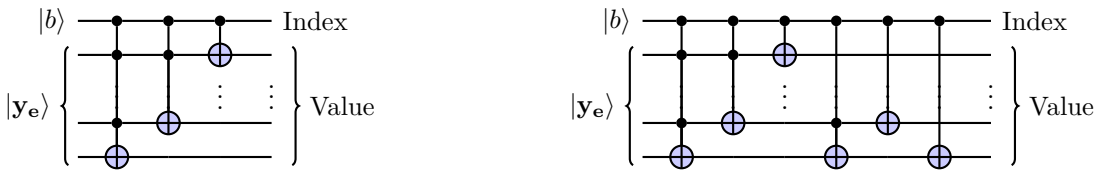
$$\begin{aligned} \mathbf{y} &= \mathbf{b}.\mathbf{C} \\ \mathbf{y} = \begin{bmatrix} \mathbf{y_1} \\ \mathbf{y_2} \\ \mathbf{y_3} \end{bmatrix} &= \underbrace{\begin{bmatrix} b_1 & b_2 & b_3 \end{bmatrix}}_{\mathbf{b}} \underbrace{\begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{bmatrix}}_{\mathbf{C}} \\ \mathbf{y} = \begin{bmatrix} \mathbf{y_1} \\ \mathbf{y_2} \\ \mathbf{y_3} \end{bmatrix} &= \begin{bmatrix} -b_1 - b_2 + b_3 \\ b_1 - b_2 - b_3 \\ -b_1 + b_2 - b_3 \end{bmatrix} \end{aligned} \tag{3.3}$$

The received signal $\mathbf{y}$ is modified to $\tilde{\mathbf{y}}$ as part of the implementation. As illustrated Fig. 3.3, the Grover's circuit should be redesigned with respect to $f(x)$. It is indeed true that when the variable $\mathbf{b}$ is multiplied by $\mathbf{C}$, which contains a negative value, the received signal may also become negative.

The Fig. 3.3 illustrates the quantum circuit when dealing with the negative and positive received signal, which is adapted based on a model 3.3. Let us assume that signal y is denoted as $\{y_1, y_2, \cdots, y_k\}$. We assume that the $|C_{p_q}\rangle$ part serves as the control bit, while $|\mathbf{y}\rangle$ serves as the target bit, where p and q denote the row and column matrix. The $|C_{p_q}\rangle$ component consists of two cases: one where $|C_{p_q}\rangle$ is positive and the other where $|C_{p_q}\rangle$ is negative. The $|C_{p_q}\rangle$ component, comprising positive numbers, is computed when the received signal consists of a component where $C_{p_q} > 0$, as shown in Fig. 3.3a. This demonstrates a simple classic quantum adder, as proposed in [85]. In contrast, the $|C_{p_q}\rangle$ component, which contains the negative number, is computed in Fig. 3.3b, illustrating a one's complement computation. Therefore, the equation we intend to adhere to is:

$$|\mathbf{y}\rangle = \begin{cases} |b\rangle + |\mathbf{y}\rangle & C_{p_q} > 0 \\ |\mathbf{y}\rangle - |b\rangle = |\mathbf{y}\rangle + |b\rangle' & C_{p_q} < 0 \end{cases} \tag{3.4}$$

The complete circuit is depicted in Figure 3.4, utilizing the model described in Eq. 3.3. Each element of $b \in \mathbf{B}$ is passed to the received sequences $|\mathbf{y}\rangle$ based on the



(a) Case $\mathbf{C_{pq}} > 0$ (b) Case $\mathbf{C_{pq}} < 0$

Figure 3.3: Two $\mathbf{C_{pq}}$ cases in bipolar operation

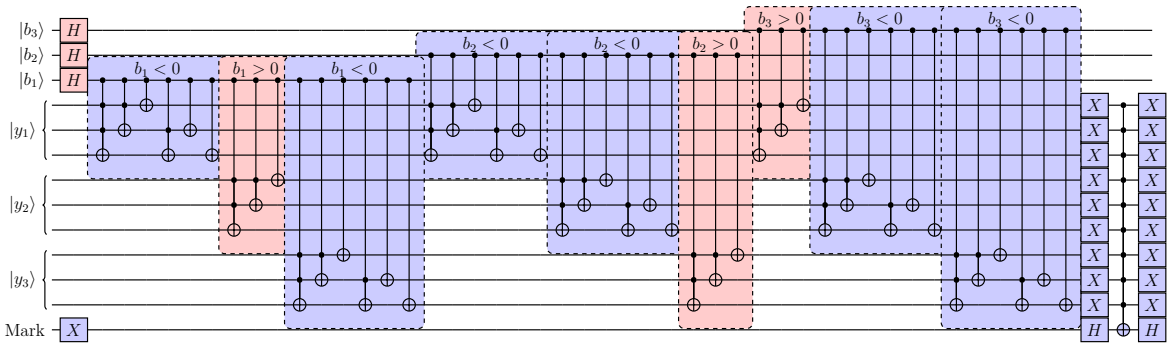
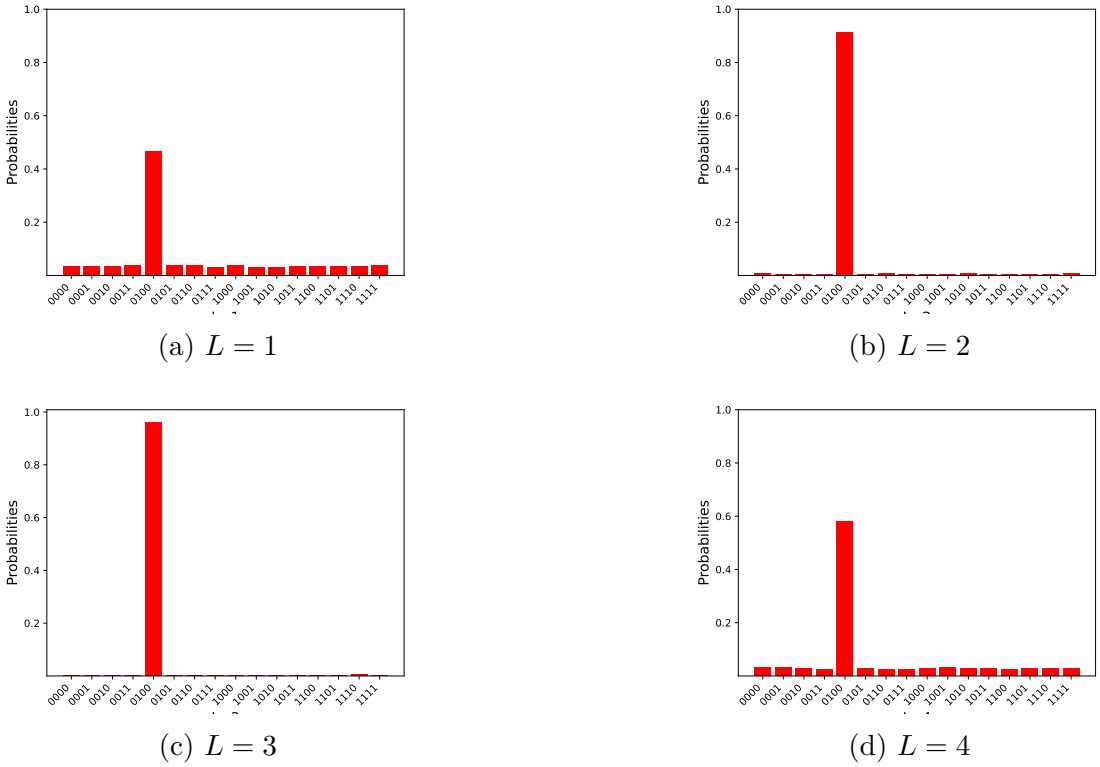


Figure 3.4: Modified Oracle: $|y_1\rangle = -b_1 - b_2 + b_3$, $|y_2\rangle = b_1 - b_2 - b_3$,$|y_3\rangle = -b_1 + b_2 - b_3$

positive or negative component of the model specified in Eq. 3.3. Once it is routed to the received signature $\mathbf{y}$, the component calculates the negative computation on the mark register, which is designed to calculate negative computation. Subsequently, the component is multiplied by the *inverse* of this circuit, with an additional *diffuser* $\mathbf{D}$ at the end.

Random Gaussian Model

In the random Gaussian model, we employ a similar approach to that proposed by Unipolar. In this case, the Gaussian model's approach is first modeled by rescaling the decimal part into a positive integer. This involves multiplying it by a factor of 2 which respects the increase of the precision p, where $p = 2$. The codebook is chosen randomly based on the distribution of gaussian model (i.i.d) divided by a unitary power as explained in 2.1.2. Here is an example of our codebook with a specific



(a) $L = 1$ (b) $L = 2$

(c) $L = 3$ (d) $L = 4$

Figure 3.5: Grover measurement results with several iterations $L \in \{1, 2, 3, 4\}$

configuration: $N = 5$ and SF $= 3$:

$$\mathbf{C} = \begin{bmatrix} 0.72442353 & -0.65608498 & 0.21157280 \\ 0.39480599 & -0.38112844 & 0.83598406 \\ 0.86927943 & -0.08977167 & -0.48610114 \\ -0.40295118 & -0.61427887 & -0.67844809 \\ -0.79661533 & 0.54067790 & 0.27031724 \end{bmatrix} \tag{3.5}$$

Therefore, a detailed explanation is provided in 3.2.4 using a similar approach as with this model. The corresponding circuit would be based on the same principle as Fig. 3.4, but with more gates to consider the non-unitary coefficients.

3.3 Classical and Quantum Performance

3.3.1 Noiseless Case

Measurement Result : Noiseless case

Let us consider as an example in the *unipolar case*, using the same codeword as presented in 3.2.4, with $N = 4$ and SF $= 3$, with a precision $p = 2$. We suppose that the set of activity users, denoted as $\{0, 1, 0, 0\}$, is active, while all others are inactive. This defines that user 3 is the only active user. The signal observed is $\mathbf{y} = [0, 1, 1]$ without noise. Fig. 3.5 illustrates the success probability outcomes of Grover's algorithm with iterations $L \in \{1, 2, 3, 4\}$. The number of users tested here is $N = 4$, with only one solution, $S = 1$. Thus, this corresponds to a total of $2^N = 2^4$ potential configurations, ranging from $\{0, 0, 0, 0\}$ to $\{1, 1, 1, 1\}$.

Upon observing Fig. 3.5, we note that $L = 3$ represents the optimal configuration since $L_{opt} = \lfloor \frac{\pi}{4}\sqrt{\frac{2^4}{1}} \rfloor = 3$. The success probability at this level is 0.966, which is significantly higher than in the other iterations. After L_{opt} iterations, the set of active users, specifically $\{0, 1, 0, 0\}$, yields a notably high success probability.

Theoretical Scenario

We first consider the ideal case where noises are not taken into account in the simulation. In this case, the classical method, ML has a success probability $P_s = 1$, thanks to the code properties which ensure that any combination of codes provides a unique signature.

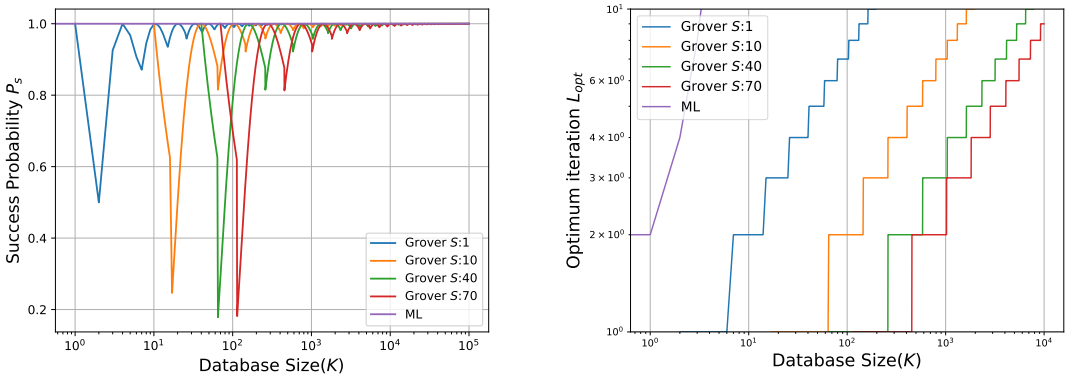
With the quantum algorithm, we observe that the optimal number of iterations in Grover's algorithm is given by $L_{opt} = \lfloor \frac{\pi}{4}\sqrt{\frac{K}{S}} \rfloor$. Let us revoke the Eq.2.13 denoted as follows:

$$P_s(j) = \sin^2\left((2j+1)\,\theta\right) \tag{3.6}$$

where $j = L_{opt}$ and $\theta = \arcsin^{-1}(\sqrt{\frac{S}{K}})$.

We plot the success probability in Fig. 3.6a, denoted as P_s, of both the ML and Grover's algorithms w.r.t the database size (K) for several numbers of solutions, denoted as S. It is noted that Grover exhibits various P_s, which depends on the number of given solutions S in the database. Grover's algorithm performs consistently for different S values $(1, 10, 40, 70)$ with a slight variation in the success probability P_s. This model achieves a 100% success rate more quickly with a small-size database when there are fewer solutions. Conversely, a high number of solutions requires a larger database size to achieve the same success rate. It should be noted that, for the noiseless channel, classical methods such as ML achieve a success probability of $P_s = 1$.

We observe that quantum has several low peaks compared to the classical ML which leads to unstable graph as a function of size database K. This is mainly



(a) P_s w.r.t K theoretical result

(b) L_{opt} w.r.t K theoretical result

Figure 3.6: The Noiseless Case Performance (Theoretical and Simulation results)

caused by the component complex amplitudes of k and l that construct a state $|\psi\rangle$ as described in Eq. 2.10. These amplitudes influence the success probability. When the size database is small, the component l has a large contribution to the state, which leads to small success probability. Mathematically, we can formulize it from Eq. 2.13 where $\theta = \arcsin\sqrt{\frac{S}{K}} \approx \frac{1}{\sqrt{K}}$ and j is the L_{opt}. The equation of P_s in Eq. 3.6 can be reformulated as follows:

$$P_s(L_{opt}) = \sin^2((2L_{opt}+1)\theta) = \sin^2\left(\frac{2\lfloor\frac{\pi}{4}\sqrt{\frac{K}{S}}\rfloor + 1}{\sqrt{K}}\right) \tag{3.7}$$

Moreover, we can assume that when K is small, the success probability might lead to $P_s \neq 1$ because the value 1 has a strong impact. While K increases, the formula will converge to $\frac{\pi}{2}$, and converges toward 1, because the large K makes the component 1 negligible.

Secondly, Fig.3.6b demonstrates the relationship between L_{opt} and the size of the database (K) in a noiseless channel. This figure serves as a continuation of the concepts introduced in Fig.3.6a, aiming to display how L_{opt} is distributed across various database sizes (K) while considering different numbers of solutions (S). It is worth noting that the distribution graph takes on a staircase pattern due to the presence of the floor function $\lfloor . \rfloor$. Additionally, the graph highlights the fact that a smaller value of S requires an increased number of Grover's iterations, which aligns with the inverse relationship existing between S and L_{opt}. In contrast, the higher value of S align with the small number of Grover's iterations needed.

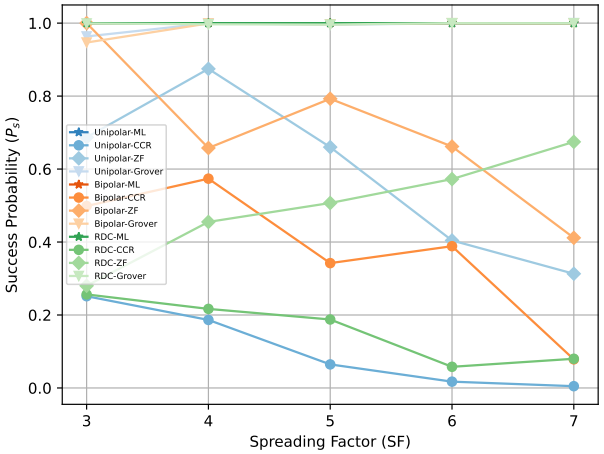


Figure 3.7: P_s w.r.t SF simulation result

Simulation Scenario

Last but certainly not least, Fig. 3.7 illustrates the comparison among various methods, namely ZF, ML, CCR, and Grover, with all code types (i.e Unipolar, Bipolar, and Random Gaussian) in a noiseless channel (i.e, $\sigma^2 = 0$). The simulation is run using for 10.000 realizations to ensure accuracy, with Precision set to $p = 2$, as explained in Section 3.2.1. Thus, the analysis is done using $\tilde{\mathbf{y}}$ to be fed into the Grover's circuit. This simulation also considers all values of SF $\in \{3, 4, 5, 6, 7\}$ with the configuration as explained in table 3.1.

The performance of classical methods (i.e., ML, CCR, ZF) and Grover have been obtained by simulation and are presented on Fig. 3.7. It is evident that in the noiseless case, all performances across all codetypes gradually decline as a function of SF across all code types. However, in exceptional cases, bipolar codes exhibit a unique trend of variation, which shows a different trend. This is attributed to the fact that each codeword's level of non-orthogonality varies depending on SF. This phenomenon is observed in all methods using bipolar.

First and foremost, it is crucial to emphasize that in all cases, ML consistently achieves a success probability of $P_s = 1$. This applies to all code types (i.e., Unipolar, Bipolar, and Random Gaussian) and all values of SF. On the other hand, the CCR exhibits a smaller P_s compared to ML, with performance declining gradually as a function of SF across all code types, except for Bipolar. The unipolar case, in particular, exhibits a low peak, approaching $P_s = 0$ in the high SF regime, specifically at SF values of 6 and 7. CCR achieves a high P_s only in the Bipolar case, ranging

Codetype	Spreading Factor SF	Number of Users N
Unipolar	3	4
	4	5
	5	7
	6	9
	7	11
Bipolar	3	3
	4	5
	5	6
	6	8
	7	10
Gaussian	3	5
	4	6
	5	7
	6	8
	7	9

Table 3.1: The configuration SF and N

from 0.58 at SF $= 4$ to 0.1 at SF $= 7$. This is because the bipolar case has a significant distance between its components.

With regard to the ZF method, it demonstrates varying performance, notably achieving variable success rates across most SF types. The trends differ among the unipolar, bipolar, and random Gaussian cases. In the unipolar case, success rates vary from $P_s = 0.88$ at SF $= 4$ to $P_s = 0.32$ at SF $= 7$, showing an increase from SF 3 to 4. In contrast, the bipolar case exhibits varying success rates, ranging from approximately 1.0 at SF $= 3$ to 0.4 at SF $= 7$. In the case of random Gaussian, the trend is upward, starting at 0.3 for SF $= 3$ and reaching 0.67 at SF $= 7$. In summary, the performance of ZF is significantly superior to that of CCR.

In contrast, Grover's algorithm delivers exceptional results for all codetypes (i.e., Unipolar, Bipolar, and Random Gaussian), nearly approaching a success rate of 1 for all SF types. The precision p in this measurement is set to a large number, which allows for high precision simulation. Thus, although Random Gaussian is characterized by a small component-to-component distance, the measurement results show that our Grover's algorithm can handle this situation, resulting in a P_s approximately equal to 1.

In conclusion, Grover's approach for this stage, $f(x) = \delta$, theoretically looks promising, with a success probability close to 1, especially when the database size is big. Regarding the effectiveness, particularly on the noiseless channel as displayed in Grover's technique has produced excellent results in Fig. 3.7, which exhibits a success rate $P_s \approx 1$. In comparison, alternative candidates like ZF and CCR have shown lower

Category	Methods	Complexity
Classical	CCR	$\mathcal{O}(N)$
	ZF	$\mathcal{O}(N)$
	ML	$\mathcal{O}(2^N)$
Quantum	Grover	$\mathcal{O}(\sqrt{2^N})$

Table 3.2: Complexity of classical and quantum methods

values of P_s compared to ML. Thus, ML remains superior to the others.

Complexity Analysis

We have evaluated the success probability for all codetype cases (i.e Unipolar, Bipolar, and Gaussian) in section 3.3.2. It is important to evaluate the complexity for both classical and quantum methods. The complexity analysis measures only the *quantum speedup* case, as explained in subsection 3.2.3.

First and foremost, it is worth noting that classical and quantum methods exhibit distinct complexities. Theoretically, CCR, based on the correlation between $\mathbf{y}$ and $\mathbf{C}$ as explained in section 7.2.2, possesses a complexity proportional to the number of users, denoted as $\mathcal{O}(N)$.

Conversely, ZF, functioning as a classical method, involves the inversion of the original code $\mathbf{C}$ with a row dimension of N. Consequently, its complexity is linked to the row dimension N, and computes with only 1 iteration. On the other hand, the optimal method, ML, necessitates an exceedingly high complexity since it exhaustively tests all possible scenarios, entailing a complexity of $\mathcal{O}(2^N)$. Grover's algorithm, in contrast, requires a complexity of $\mathcal{O}(\sqrt{2^N})$ due to the utilization of superposition of states.

The complexity starts with running oracle ($\mathbf{O}$) and diffuser ($\mathbf{D}$) with $\sqrt{K}$ times. Here, we have proven that classical ML detector requires $K = 2^N$ evaluations, while Grover's needs $\sqrt{K} = \sqrt{2^N}$. While classical complexity is significantly reduced, Grover also demonstrates a high success probability with a large database size K. This showcases the advantages of quantum for a large number of users, represented as N.

3.3.2 Noisy Case

In this part, we now take the noise into account. We assume that the noise follows a normal distribution $\mathcal{N}(0, \sigma^2)$. This subsection assesses different code types' values (i.e. Unipolar, Bipolar, and Gaussian). We also involve several classical methods, namely

(e.g., ML, CCR, and ZF), to be compared with Grover's algorithm.

Measurement Result : Noisy Case

Let us take an example of the measurement result, which shows a similar result as 3.3.1. As the number of users $N = 4$ and SF $= 3$, we can assume that we have an observed signal $\mathbf{y} = [0, 1.1, 1.2]$, after contaminated by noises, assuming that the noise variance $\sigma^2 = 0.2$. It has been shown that when we calculate the rounding function $\tilde{\mathbf{y}}$, we can obtain $\mathbf{y} = [0, 1, 1]$. In this case, the result would be the same as 3.3.1, which shows the configuration of active users that corresponds to $0, 1, 0, 0$.

P_s Unipolar Performance

The objective of this subsection is to analyze the performance of Grover's algorithm design to search for x such that $f(x) = \delta$ and compare it with classical methods (i.e., CCR, ZF, and ML) in the context of unipolar case where $\mathbf{C} \in \{0, 1\}$ is considered. The performance is denoted as P_s and ranges from 0 to 1, with 1 representing the highest success probability.

We have simulated 10000 average independent noise process realizations with a SF $= 3$ and $N = 4$. We are also considering $\mathbf{y}$ and $\tilde{\mathbf{y}}$ for all methods. To simulate $\tilde{\mathbf{y}}$, we use a precision of $p = 2$, whereas simulating $\mathbf{y}$ requires a much higher precision, approaching infinity. The optimal ML detector, the CCR, ZF and our proposed Grover algorithm are compared in Fig. 3.8. This figure shows the variation of the average probability of success in detecting the active users, as a function of the noise standard deviation σ. We can first note that the performance are degraded when the noise's variance increases. It is noted that ML provides the best accuracy as it is the optimal algorithm, as expected. On the other hand, for our proposed Grover's algorithm, the success probability goes from the maximum one in the noiseless case ($P_s = 0.7$), to a random selection with equiprobable variables ($P_s = 0.1$).

Although Grover is not as effective as ML, Grover's algorithm still leads compared to other classical methods (i.e CCR and ZF) when the noise variance is in a small regime of σ^2. This performance is followed by ZF which provides better result than Grover when the noise is relatively high. This applies to CCR but with worse performance than the ZF.

It is noted that Grover's algorithm achieves a small P_s when the noise contribution is high, the signature $\tilde{\mathbf{y}}$ leads to inappropriate value. Once we fed the Grover's algorithm with a wrong input, the outcome shows an equiprobable results, leading to equal possible outcomes. Furthermore, the rounding function also can contribute to more errors. This is a consequence of the strict application of the constraint $f(x) = \delta$ within Grover's algorithm i.e. the search is made to recover exactly this signature as if

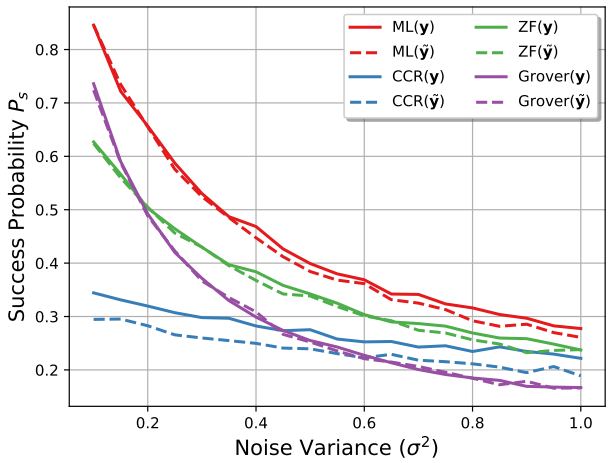


Figure 3.8: *Unipolar* : P_s as a function of σ^2

there was no noise. When the input for δ is incorrect, it leads to an inaccurate result. As depicted in Fig. 3.8, it is evident that both ZF and CCR outperform Grover's algorithm at noise levels of $\sigma^2 = 0.2$ and $\sigma^2 = 0.6$, highlighting the degradation of Grover's algorithm performance in the presence of noise. This permits to conclude that the direct use of Grover's algorithm is not highly attractive in the high-noise regimes.

Thanks to Fig. 3.6a, we can see the success probability P_s remains stable as the size database K is increased, as Grover's algorithm become more accurate. We can thus observe that our proposed solution permits to significantly reduce the computation delay at the cost of a reasonable impact on the performance.

We can also observe the impact of the quantization, where we consider $\tilde{\mathbf{y}}$ instead of $\mathbf{y}$. The performance of $\mathbf{y}$ significantly outperforms that of $\tilde{\mathbf{y}}$, primarily because the rounding function may degrade the performance of the observed signal $\mathbf{y}$. Consequently, the performance of $\tilde{\mathbf{y}}$ is lower than $\mathbf{y}$. This observation holds true for methods, namely CCR, ZF, ML. Except for Grover, whose performance is similar between $\mathbf{y}$ and $\tilde{\mathbf{y}}$, primarily due to the equiprobable probability.

P_s Bipolar Performance

On the other hand, in the *bipolar* codetype, we also compare the performance of Grover's algorithm to classical methods (i.e., CCR, ZF, and ML). It is evident that, as bipolar employs the case where $\mathbf{C} \in \{-1, 1\}$, there is a substantial gap between each component value. Consequently, we may anticipate a different range of values

for P_s across all methods. Similar to the unipolar case, the performance is denoted as P_s. We have simulated 10000 average independant noise realizations within a SF $= 3$ and $N = 3$. As illustrated in Fig. 3.9, the classical methods (ZF, CCR, and ML) and Grover's algorithm have been compared.

We may note here that ML still outperforms all classical performances and the Grover's algorithm, reminding that Grover's algorithm applies $f(x) = \delta$. This performance is followed by ZF while the incremental of noise variance σ^2 deteriorates its performance. The performance of ZF in the bipolar case is superior to that in the unipolar scenario. This is attributed to the fact that bipolar coding exhibits a greater Euclidean distance between each of its components. It is important to note that bipolar coding employs $\mathbf{C} \in \{-1, 1\}$, a range larger than that of other coding types.

We may note here that the Grover's performance is promising when the noise variance σ^2 is relatively small due to the rounding function. However, when the noise variance σ^2 is high, this leads to equiprobable probability, which leads to erroneous detection. Although bipolar is characterized by its large euclidean distance $\mathbf{C} \in \{-1, 1\}$, Grover is still uncomparable with other classical methods, especially ML and ZF. The strict requirement $f(x) = \delta$ deteriorates the Grover's performance. Thus, the success probability P_s is relatively worse than other classical methods, including the CCR in high variance σ^2.

It is noted that bipolar case has higher euclidean distance compared to unipolar. For that reason, the performances of several classical methods (i.e, ML, ZF) are increased for the same noise variance σ^2, because the detectors have a possibility to distinguish the codes better. However, Grover's algorithm seems to be degraded. The CCR also remains unchanged.

Applying the same principle with unipolar, where we want to analyze the effect of the quantized signal, denoted as $\tilde{\mathbf{y}}$. Thus, we compare the performance of $\mathbf{y}$ and $\tilde{\mathbf{y}}$ in the graph. The performance of $\mathbf{y}$ indeed outperforms that of $\tilde{\mathbf{y}}$, because the rounding function reduces the precision on $\mathbf{y}$. This applies to all methods, including CCR, ZF, ML. Nevertheless, in the case of Grover, the use or non-use of a rounding function appears to have minimal impact on performance due to the equiprobable success probability.

P_s Gaussian Performance

The final case involves random Gaussian performance, where the scenario of $\frac{\mathbf{C}}{|\mathbf{C}|}$ is considered. In this section, we present a comparative analysis of the performance of Grover's algorithm, CCR, ZF, and ML. It is important to note that this codetype exhibits a small distance between each component, making detection significantly more challenging. We may expect a lower success probability compared to other types.

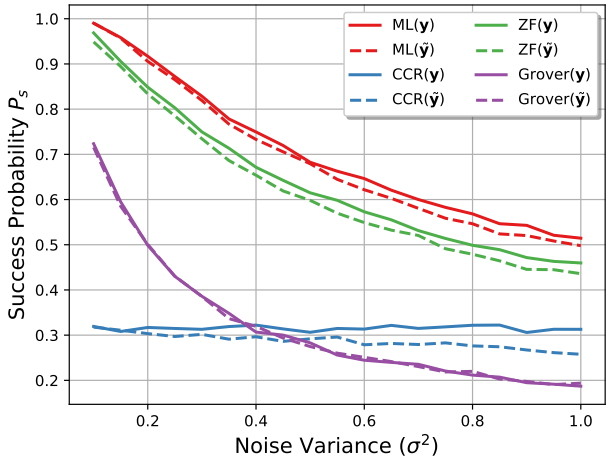


Figure 3.9: *Bipolar* : P_s as a function of σ^2

Nevertheless, our aim is to demonstrate how these methods can adapt to handle various codetype scenarios.

Similar to unipolar and bipolar, we have simulated 10.000 independent noise realizations within an SF of 3 and N equal to 5, across noise standard deviation ranging from $\sigma^2 = 0$ to $\sigma^2 = 0.1$. As illustrated in 3.10, it is noted that the maximum achieved success probability is $P_s = 0.5$ with a classical method (ML).

As expected, the ML outperforms all classical and Grover methods, leading to the highest performance. Although the achieved P_s is shown as $P_s = 0.5$, this method is still promising. This performance is followed by ZF and CCR, where both of them are comparable each other. Nonetheless, as usual, Grover's algorithm does not show promise due to its reliance on the requirement $f(x) = \delta$, which mandates an exact input. In cases where an incorrect input is provided, the algorithm yields inaccurate outcomes. Grover's algorithm's performance deteriorates further in the Gaussian context, where the proximity between each component is significant. As a result, the impact of the rounding function described in Eq. 3.1 is relatively minor. Furthermore, the equiprobable probability in high noise variance shows that Grover's algorithm maintains an unchanging success probability (P_s), rendering its performance stagnant. This principle also holds true for ZF and CCR, despite their significantly superior performances.

Applying the same principle to the unipolar and bipolar case, we compare the performance of $\mathbf{y}$ and $\tilde{\mathbf{y}}$ with the same precision p set to 2. $\mathbf{y}$ consistently outperforms $\tilde{\mathbf{y}}$ due to the performance-reducing effect of the rounding function. Additionally, in this level, the gap between $\mathbf{y}$ and $\tilde{\mathbf{y}}$ is higher than other codetypes (especially on ML) due

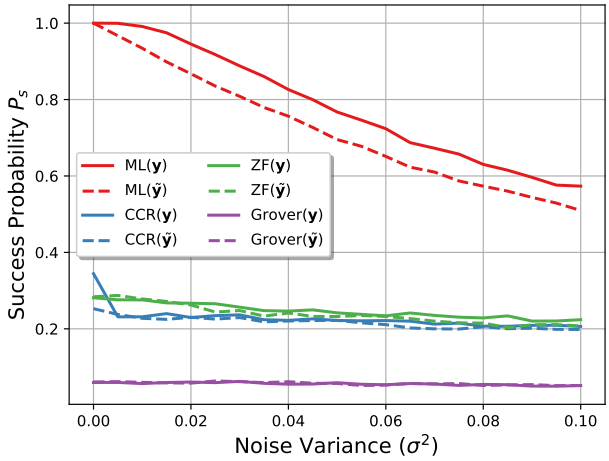


Figure 3.10: *Gaussian* : P_s as a function of σ^2

to small Euclidean Distance of each component in Random Gaussian Code. Besides, in the case of Grover, ML, and CCR, the use or non-use of a rounding function appears to have minimal impact on performance due to the equiprobable success probability.

3.3.3 Discussion

We have conducted an evaluation of both classical and quantum methods in terms of their performance and complexity across noiseless and noisy channels. The noiseless scenario involves a straightforward ideal algorithm, excluding noise effects, where we calculate the success probability (P_s). In contrast, the noisy channel introduces a range of noise levels $\mathcal{N}(0, \sigma^2)$. This assessment encompasses three distinct code types: Unipolar, Bipolar, and Gaussian.

The study expectantly shows that across all code types and variance ranges (σ^2), ML consistently exhibits superior performance compared to the others. Following closely is the performance of ZF, except in the Unipolar case where Grover's algorithm surpasses ZF under small noise variance (σ^2). On the other hand, CCR demonstrates relatively poor performance in scenarios with low variance, yet it manages to outperform Grover's algorithm as the noise variance (σ^2) increases, particularly in the Unipolar and Bipolar cases. Notably, Grover's algorithm exhibits its weakest performance in the Gaussian context.

It is evident that Grover's algorithm does not succeed on providing accurate detection performance due to the inherent constraint of utilizing $f(x) = \delta$. This constraint limits the received signal $\mathbf{y}$ to the scope of $\mathbf{b} \cdot \mathbf{C}$, leading to noise contamination of

the observed signal $\mathbf{y}$. This particular scenario seems incapable of achieving the same level of performance as achieved by other classical methods. To achieve comparable performance, a modification of the scenario, aligning with the minimum distance between $\mathbf{y}$ and $\mathbf{b} \cdot \mathbf{C}$, might be necessary. This minimum distance concept is inherently implied by ML, thereby suggesting the potential need for adapting Grover's algorithm to align with this requirement.

In terms of complexity, a clear contrast emerges. While ML calculates a complexity of $\mathcal{O}(2^N)$ in its computations, Grover's algorithm offers significantly lower complexity than both ML and other classical methods for higher user counts (N).

Key takeaways

We can take essential insights from Grover's measurements, revealing that Grover's algorithm encounters two important scenarios. *First scenario* that when noise contribution is small enough (low σ^2), the rounding function, as denoted in section 3.2.1, is applied to $\mathbf{y}$ which possibly changes the situation. Thus, the quantum has a high probability to correctly identify the users and presents the same performances as illustrated on the noiseless channels. In the *second scenario*, when the noise contribution is relatively high, applying the rounding function to the signature $\mathbf{y}$ may result in incorrect values. Thus, the Grover's searching leads to erroneous which shows an equiprobable statistics among all N possible solutions. In conclusion, our quantum algorithms faced two different situations which depend on the noise contribution that affects the P_s performances.

3.3.4 Conclusion

We observed that the original Grover's algorithm is not promising in terms of performances. The searching engine of Grover's algorithm requires an accurate inputs $f(x) = \delta$, if the input is wrong, the searching engine leads to erroneous searching. Thus, the proposed Grover's algorithm is not comparable for other classical methods.

Thus, the Grover's algorithm is promising, but it is not completely adapted to our problem. Thus, we propose to modify it by complying the minimum distance algorithm. As denoted in 7.2, the proposed modified Grover's algorithm should compute the minimum distance between $\mathbf{y}$ and $\mathbf{b} \cdot \mathbf{C}$. The subsequent section discusses more the minimum distance between $\mathbf{y}$ and $\mathbf{b}.\mathbf{C}$, with the expectation of increasing the number of Grover's iterations, subsequently leading to increased complexity. However, our goal is to increase the Grover's performance P_s. Further insights into this aspect are provided in the upcoming section. Thus, the following section is proposed to cater this needs.

Chapter 4

Chapter 4

Grover's algorithm for finding minimum in AUD

Following Chapter 3, where we considered the simplest case, in this chapter, we propose a modified version of Grover's algorithm that aims to apply the same principles as ML. Although it may require a significant amount of complexity, ML shows promise in terms of delivering the best performance. This chapter explores how Grover's algorithm can achieve comparable performance to ML while maintaining simplicity in complexity.

It is essential to modify Grover's algorithm's oracle $\mathbf{O}$, to find the minimum distance by applying $f(x) < \delta$. Afterwards, we apply the full ML algorithm on a *quantum-based approach* and compare the results as a function of variance σ^2.

As a matter of fact, applying the condition of ML for finding the minimum presents a challenge where the number of solutions, denoted as S, is unknown. This approach has been proposed by Boyer-Brassard-Høyer-Tapp (BBHT) and Durr-Hoyer Algorithm (DHA). For instance, BBHT number of iterations is an upper-bounded by $4.5\sqrt{K}$ when the number of solutions is unknown in the database, while DHA proposes an upper-bound of $22.5\sqrt{K}$ to find the minimum solution in an unknown solutions database. It is important to note that these upper-bounds are still smaller than the classical computation $\mathcal{O}(K)$. However, BBHT and DHA raise an open research question that requires improvement in terms of complexity and methods.

Our proposed solution, named Improved Iterated Minimum Searching Algorithm (IIMSA), thus aims to improve the existing DHA algorithm to enhance its performance. While DHA calculates minimum values using Grover's iteration, which follows a geometric progression for unknown solutions, IIMSA suggests an alternative algorithm. This algorithm selects an estimated solution, denoted as $\hat{S}$, based on a random $\hat{\delta}$.

In addition to both IIMSA and DHA, we integrate classical methods such as ZF and CCR into IIMSA and DHA to achieve the fastest speed. Consequently, we compare

the performances and complexities of IIMSA and DHA when classical methods are involved. This integration is achieved by determining the correct threshold, denoted as δ inspired by [72], to improve the existing performance. Our main goal thus in this chapter is to assess the performance, denoted as P_s, and complexity, denoted as nb_{it}, of IIMSA and DHA when integrated with classical methods (i.e., ZF and DHA).

- Design Grover's Quantum Circuit for AUD for $f(x) < \delta$ and implementing ML that respects $\arg\min \|\mathbf{y} - \mathbf{b} \cdot \mathbf{C}\|_2^2$.
- Propose an IIMSA algorithm as an improvement to existing BBHT and DHA.
- Elaborate more on the integration classical methods (i.e CCR and ZF) into the IIMSA and DHA.
- Compare the performances and complexity of the DHA and IIMSA algorithms, we also integrate them with classical methods (i.e. CCR and ZF) to compare both algorithms.

4.1 Introduction

This chapter begins with a literature review of DHA, highlighting that DHA establishes an upper limit for Grover's algorithm when attempting to find the minimum value in cases where the solution is unknown. The upper limit of $22.5\sqrt{2^N}$ for minimum value identification using Grover's algorithm has attracted the attention of numerous researchers, motivating them to seek ways to reduce this complexity while enhancing a straightforward method.

Furthermore, we introduce a novel solution named IIMSA to illustrate how this approach can mitigate the complexity associated with DHA. We delve into the design of the circuit and its implementation, which we explain in the subsequent section. We conduct a comparative analysis of the performance and complexity of IIMSA and DHA across various introduced parameters.

4.2 Comprehensive Review on DHA

The DHA has attracted researchers aiming to ameliorate its level of complexity. The complexity of DHA is upper-bounded by $22.5\sqrt{K}$. Consequently, researchers or

authors are exploring methods to reduce this complexity by modifying the DHA's algorithm.

First of all, the initial improvement was proposed by Long, namely, Long's algorithm [86] [87] [88], which enhances Grover's algorithm by searching for more accurate solutions (leads to $P_s = 1$). This is applied when the Grover's algorithm by using phase inversion though angle φ. The rotation angle is done with $\varphi = 2\arcsin\left(\frac{\sin\frac{\pi}{(4J+\beta)}}{\sin\beta}\right)$, where $\sin\beta = \frac{1}{\sqrt{N}}$, K is the number of items in the database, and J is an integer equal to a greater $(\frac{\pi}{2} - \beta/(2\beta))$. As an effect, an initial enhancement to the DHA is presented by the authors in [89], using the Long's algorithm. They introduce a novel algorithm, termed the Quantum Maximum or Minimum Searching Algorithm (QUMMSA), which exhibits a low failure rate when addressing the minimization of values in the DHA. Thanks to Long's algorithm, QUMMSA achieves a success probability of 100%, a notable advancement from the DHA's original success probability of 50%. This improvement stems from the utilization of the quantum exponential search algorithm, as outlined in their paper. In terms of complexity, the conventional DHA necessitates $\mathcal{O}(\log_2^2 K)$ operations each time the initial superposition of state is executed. In contrast, the proposed approach in this paper [90] requires only $\mathcal{O}(\log_2 K)$ operations. When the Grover-Long's algorithm is executed, the initial state is improved leading to a significantly reduced failure rate. An improvement of authors in [89], by the same author [90] has used QUMMSA and demonstrated the algorithm that is implemented on a circuit with an IBM superconducting processor. Yan Liu et al in [16] also proposes the improvement by optimizing the oracle circuit to reduce the number of gates.

Youngjin Seo et al [91] proposed a quantum searching algorithm (QSA) for weight solutions. This proposed algorithm is based on DHA and BBHT which aims to give a weight to a certain states $|.\rangle$ that allows to have different amplitudes for this particular state. This approach is similar to Grover's algorithm, but it allows us to adjust the weight of the state to achieve a specific desired value. This entails the same complexity as DHA, but with a higher expected reward when implemented with Graph-Coloring Problem (GCP). An alternative method is suggested by [92], wherein their approach delineates Grover's quantum circuit's construction through the utilization of Quantum Random Access Memory (QRAM).

Subhadeep Mondal et al [93] also proposes a modification of BBHT, which also applies to DHA. The modification lies on the chosen iteration L where it is based on γ distribution instead of choosing $L = \{0, \cdots, \lfloor m \rfloor\}$. It is noted that DHA chooses L with a small number of iterations, while also considering the fact that the size database is not relevant to it. Thus, the L is chosen as a function of size database, which is based on γ distribution. It has been proven that the newly proposed algorithm can reduce the complexity of DHA to $9\sqrt{K}[1 - (1/2)^{i_b+1}]$, where i_b is $1.66\log_2(\frac{K}{K_{\min}})$, and $K_{\min}$ is the threshold reached after reducing the database size K to this level.

Authors	Year	Proposed Algorithm	Contribution
Long [86] [87] [88]	1999,2001,2002	Grover's algorithm with 0 failure rate	Changing the phase of Grover's algorithm to improve the success probability P_s
Y. Chen et al [89] [90] [16]	2019, 2020, 2021	Quantum Maximum or Minimum Searching Algorithm (QUMMSA)	Modifies DHA with additional Grover's Long algorithm to observe high success probability $P_s = 1$. Also, replacing the initial circuit the initial state ($\log_2 K$)
Y. Seo et al [91]	2022	QSA Weight Solution	It has higher expeced reward than Grover's algorithm
Yujin et al [92]	2020	Grover's minimum searching algorithm with Grover's minimum circuit	Finding minimum algorithm with certain iterations. The complexity is reduced to $\mathcal{O}(\frac{5\pi}{8}\sqrt{K})$. Proposing and designing a circuit for quantum minimum searching algorithm, and applying the concept of Quantum Random Access Memory (QRAM).
S.Mondal et all [93]	2021	BBHT's modification	Changes the geometric progression of L in DHA's original algorithm to a γ-distribution. It succeed to reduce DHA's complexity to $9\sqrt{K}[1-(\frac{1}{2})^{i_b+1}]$
L.A.B Kowada et al [94]	2008	Linear Measurement (LM)	The number of measurement is reduced from $\Omega(\log_2 K)$ to $\mathcal{O}(\log K)$
K. Miyamoto et al [95]	2019	Finding k-minima	Proposes $\mathcal{O}(k \cdot K)$ speed algorithm to find the $k-$ minima

Table 4.1: Compilation of Review Papers on Enhancements to DHA

Another algorithm is proposed by Kowada in [94], where they introduce an algorithm called Linear Measurement (LM) based on BBHT. In essence, the DHA continuously applies the BBHT to theoretically identify the minimum solution. Meanwhile, the LM proposes defining the PM as a possible iteration. Unlike DHA, which stops when a potential minimum is found, LM does not follow the same approach. The objective is to decrease the number of measurements, where DHA provides an $\mathcal{O}(\log^2 K)$ complexity, while this algorithm reduces it to $\mathcal{O}(\log K)$.

Last but not least, [95] also proposes a new solution regarding the proposal to find $k-$minima which is promising in the context of machine learning. Their main contribution is to find the alternative methods to do $k-$minima with keeping the complexity holds true at $\mathcal{O}(k \cdot K)$.

Thus, DHA has undergone various improvements using different methods. In our contribution, we aim to demonstrate also a complexity reduction for DHA, which does not rely on a geometric progression but instead utilizes a random solution to determine the new threshold solution, denoted as $\hat{S}$. The following subsection describes our primary algorithm, IIMSA.

4.3 Proposed Algorithm

This section provides a detailed description of the IIMSA algorithm, its delivery, collaboration with classical methods, and its associated circuit development. Additionally, we propose a quantum-classical hybrid solution to enhance the performance of IIMSA.

4.3.1 IIMSA Algorithm

We introduce an algorithm known as the (Improved Iterated Minimum Searching Algorithm (IIMSA)). The main idea behind IIMSA is to determine the minimum value of a database with an unknown number of solution, denoted as $\hat{S}$.

Instead of employing random number of iterations, as suggested by the Durr-Hoyer Algorithm (DHA), our approach involves providing an estimated number of solution $\hat{S}$ from the random variable δ. This variable introduces uncertainty, leading to an unpredictable number of iterations. Despite this inherent inaccuracy, we persist in estimating the set of active users using Grover's algorithm $\mathcal{G}$. The proposed algorithm is given as follows 3:

Algorithm 3: IIMSA Algorithm

Input : $\mathbf{C}$, K, L_{IIMSA}, $\hat{\delta}$
Output: δ_x, $\mathbf{b}$

$i \leftarrow$ choose $(0, K-1)$ uniformly ;
Choose $\hat{\delta}(i) \leftarrow$ corresponds to i;
$\hat{S} \leftarrow \|\mathbf{y} - \mathbf{b} \cdot \mathbf{C}\|_2^2 \leq \hat{\delta}$;
$L \leftarrow 1$;
while $\hat{S} \neq 0$ *or* $L \leq L_{IIMSA}$ **do**
  $L_{opt} = \lfloor \frac{\pi}{4}\sqrt{\frac{K}{\hat{S}}} \rfloor$; $\mathbf{b} \leftarrow \mathcal{G}(L_{\text{opt}})$;
  $\delta_x \leftarrow \|\mathbf{y} - \mathbf{b} \cdot \mathbf{C}\|_2^2$;
  $\hat{S} \leftarrow \|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2 \leq \delta_x$;
  $L \leftarrow L + L_{\text{opt}}$;
  if $\delta_x < \hat{\delta}$ **then**
    $\hat{\delta} \leftarrow \delta_x$;
  end
end

Firstly, we randomly select an index i from a uniform range of values between 0 and $K-1$, where K is the size of the database. Consequently, $\hat{\delta}$ is initialized with a randomly chosen value with a uniform range. We then evaluate the number of solution $\hat{S}$ to be the squared Euclidean distance between the vector $\mathbf{y}$ and the product of $\mathbf{b}$ and $\mathbf{C}$. Then, we check if this updated value is less than or equal to the current threshold $\hat{\delta}$. The idea here is to represent the number of sets resulted by $\mathbf{y}$ and $\mathbf{b} \cdot \mathbf{C}$ whose distance is lower than the current $\hat{\delta}$. If $\hat{S} = 0$, the current $\hat{\delta}$ leads to a minimum distance. Otherwise, Grover's algorithm $\mathcal{G}$, which respects $f(x) < \hat{\delta}$ is run, to search for a lower distance. The Grover's output generates a new set, leading to find the new δ_x and solution $\hat{S}$. If this set has a distance δ_x lower than $\hat{\delta}$, we iterate by starting once again $\mathcal{G}$ but with an updated $\hat{\delta}$ by δ_x value. We thus have a smaller set

of solutions for this new iteration of $\mathcal{G}$. We note that L is measured when the number of Grover's algorithm is executed. This variable L will become the major variables on the performances which will be explained on section 4.4. This principle is applied until we obtain $S = 0$.

For each Grover's call, the algorithm runs the modified oracle for $L_{opt} = \lfloor \frac{\pi}{4}\sqrt{\frac{2^N}{\hat{S}}} \rfloor$ times, to find a lower distance. However, it is important to note that if the number of solutions is bigger than half the database size, then the unwanted cases are amplified, pushing the search in the wrong direction. Thus, we bound the number of unsuccessful trials to L_{IIMSA}.

List of important variables :

- $\hat{\delta}$ as a threshold to find the current distance
- $\hat{S}$ as an estimated number of solutions given by random δ
- L_{IIMSA} as an upper-bound of the algorithm
- δ_x as a new threshold delta to find the current distance
- L as a variable to measure the number of Grover's execution

4.3.2 Quantum-Classical Hybrid solution

To further ameliorate the previous algorithm, we propose to use classical preprocessing. The objective is to initialize accurately the quantum search algorithm, to prevent the case where the number of solutions is too high. It should also permit to accelerate the search as we start closer to the targeted solution $\hat{\delta}$. To do so, we propose to evaluate, by applying CCR (as proposed in 2.1.3) and ZF (as proposed in 2.1.3) of each case to the received signal $\mathbf{y}$. The complete algorithms (classical pre-processing and quantum search) are called CCR-DHA, ZF-DHA, CCR-IIMSA and ZF-IIMSA.

This approach requires more classical computations (N CCRs computations and 1 ZFs computation have to be classically performed), but we expect to significantly reduce the quantum complexity. CCRs and ZFs are expected to identify a *close* solution for the activity set. From this, we can initialize δ with more accurate value by computing the distance of this reference set to the received signal, which are called δ_{CCR} and δ_{ZF} respectively. If any other set is more likely, then its distance will be smaller and is likely to be retrieved by Grover's search. The full algorithm is thus using Algorithm 4, where the first executed line is changed to δ_{CCR} and δ_{ZF} respectively. The new δ proposes to find the solution correctly.

Algorithm 4: Improved IIMSA Algorithm

Input : $\mathbf{y}$, $\mathbf{b}$, $\mathbf{C}$, K, L_{IIMSA}, $\hat{\delta}$, scenario
Output : δ_x, $\mathbf{b}$

$i \leftarrow$ choose $(0, K-1)$ uniformly ;
if *scenario* $= ZF$ **then**
  Choose $\hat{\delta}_{ZF}(i) \leftarrow$ corresponds to i ;
else
  if *scenario* $= CCR$ **then**
    Choose $\hat{\delta}_{CCR}(i) \leftarrow$ corresponds to i ;
  end
  Choose $\hat{\delta}(i) \leftarrow$ corresponds to i ;
end
$\hat{S} \leftarrow \|\mathbf{y} - \mathbf{b} \cdot \mathbf{C}\|_2^2 \leq \hat{\delta}$;
$L \leftarrow 1$;
while $\hat{S} \neq 0$ *or* $L \leq L_{IIMSA}$ **do**
  $L_{opt} = \lfloor \frac{\pi}{4}\sqrt{\frac{K}{\hat{S}}} \rfloor$; $\mathbf{b} \leftarrow \mathcal{G}(L_{\text{opt}})$;
  $\delta_x \leftarrow \|\mathbf{y} - \mathbf{b} \cdot \mathbf{C}\|_2^2$;
  $\hat{S} \leftarrow \|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2 \leq \delta_x$;
  $L \leftarrow L + L_{\text{opt}}$;
  if $\delta_x < \delta$ **then**
    $\delta \leftarrow \delta_x$;
  end
end

4.3.3 Practical Implementation

The execution of the IIMSA algorithm requires a modification of the Oracle ($\mathbf{O}$) that respects the condition $f(x) < \delta$. Additionally, the implementation of finding $\arg\min \|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2$ requires a new modification of Grover's circuit. Therefore, the following subsection describes the modified Oracle along with the minimum-finding process.

Grover's circuit: Modified Oracle

When searching for the minimum in a database, it is important to modify first the oracle which complies $f(x) < \delta$ [92]. Hence, a new circuit is proposed as illustrated in Fig. 4.1.

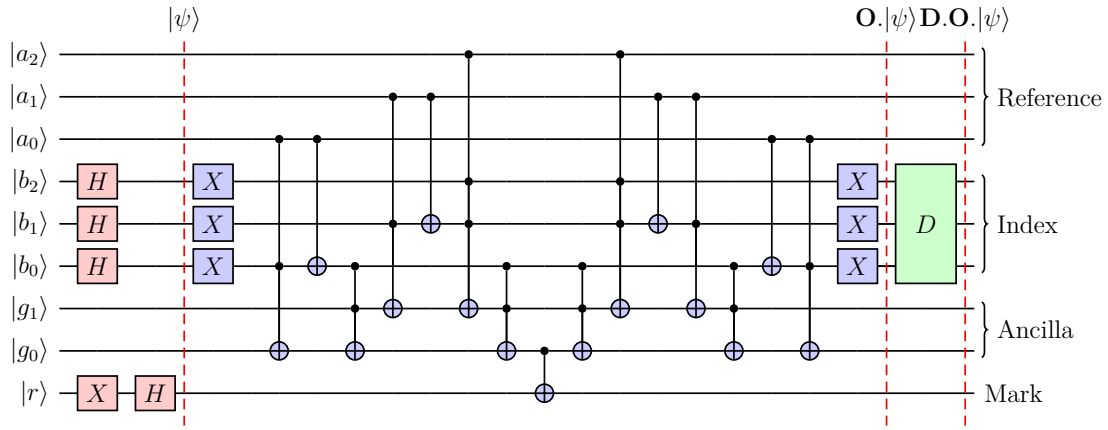


Figure 4.1: Grover's Circuit $n = 3$ qubits $f(x) < \delta$

Thus, let us assuming that we have a Grover's circuit which consists of qubits $|a\rangle$ and $|b\rangle$. In the context of our problem, $f(x) = |b\rangle$ and $\delta = |a\rangle$. The main idea of this circuit is to operate the substraction of $r = a - b$ [92] with b' which returns $r = a + b'$. To do so, a complement of b, denoted as b', is computed using *X-gate* as illustrated in Fig. 4.1. The additional qubits, denoted as g, are used for computing $a + b'$. Ultimately, the Most Significant Bit (MSB) of g contributes to the r qubits after carrying. The circuit consists of $N = 3$ qubits refers to the used bit-length, where a_0 and b_0 lead to Least Significant Bit (LSB). Then, $r = a + b'$ is operated, and will have the value 0 or 1 as follows:

$$r = \begin{cases} 1 & \text{if } a > b \\ 0 & \text{otherwise} \end{cases} \tag{4.1}$$

Then, r multiplies with $|-\rangle$ in *mark register* to provide the negative computation to the oracle. This circuit then functions well if $a > b$ is implied. Otherwise, if $a \leq b$, the circuit will not pass any information to g, which implies that no qubit is marked with negative computation.

This circuit relies on four registers, 1.) *Index Register* 2.) *Reference Register* 3.) *Ancilla register* and 4.) *Mark Register*. *Index register* contains the argument of the function $f(x)$ while *reference register* contains function δ. The *ancilla register* helps to operate the *index* and *reference registers*, in order to pass the qubits to the *mark register*. Then, the last register, *mark register*, computes the negative computation in the circuit.

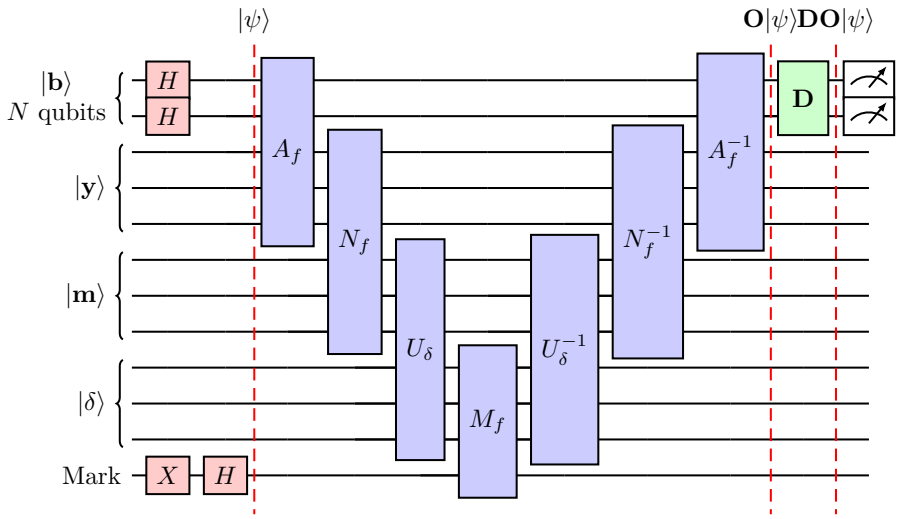


Figure 4.2: Quantum Circuit of $\|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2 < \delta$

Grover's circuit: Finding the minimum

This new Grover's circuit expands the functionality of $f(x) < \delta$ to include a novel feature algorithm. It is designed to perform an optimization task where it seeks to find the minimum $\arg\min \|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2 < \delta$ on the quantum circuit. Overall, the full Grover's circuit is illustrated in Fig. 4.2. It consists of four component qubits, which are:

1. $|\mathbf{b}\rangle \in \{0, 1\}^N$ as a set of activity users qubits
2. $|\mathbf{y}\rangle \in \mathbb{R}^{SF}$ as a received signal qubits
3. $|\mathbf{m}\rangle \in \mathbb{R}$ as a multiplication qubits
4. $|\delta\rangle \in \mathbb{R}$ as a threshold qubits

First of all, the primary target value, denoted as $|\mathbf{b}\rangle$, is the central focus of this circuit which is measured at the end of this circuit. Conversely, $|\mathbf{y}\rangle$ represents the observed signal that is fed into the Grover's algorithm, playing a crucial role in calculating the minimum distance. The parameter $|\delta\rangle$ serves as a reference point for determining the minimum distance and is also included in the circuit. It is important to note that this circuit takes both $|\mathbf{y}\rangle$ and $|\delta\rangle$ as inputs to compute the minimum distance, which is different from Fig. 4.1 because in that figure, we only taking account for $|\mathbf{y}\rangle$. The qubit $|\mathbf{m}\rangle$ serves as a passing qubits which carries the result of minimum distance calculation.

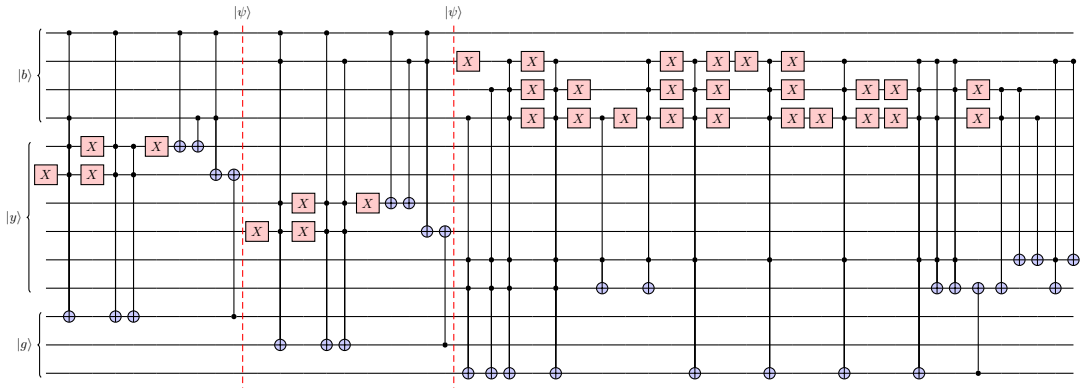


Figure 4.3: The A_f block

We also introduce the Oracle (**O**), which composes of four key components, to facilitate the execution of this function, as described below:

- A_f : stands for *adder function*, it computes $\mathbf{y} - \mathbf{b}.\mathbf{C}$
- N_f : stands for *norm function*, it computes the norm $\|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2$
- U_δ : is the oracle part,identifying the states where the norm is lower than $f(b) < \delta$
- M_f : marks the previous identified states

These blocks are followed by a Diffuser (**D**) and then repeated to amplify the wanted solutions.

Designing A_f

The block A_f consists of an *adder function*, which aims to compute $\mathbf{y} - \mathbf{b}.\mathbf{C}$ reminding that variables $\mathbf{y}$ and $\mathbf{b}$ consist of vectors, while $\mathbf{C}$ is a rectangular matrix. The b_i qubit, represents the activity of user i. With the same principle in Fig. 4.1, the implementation is done with the principle LSB which is represented with a higher order. The size of $\mathbf{b}$ is N qubits.

On the other hand, $\mathbf{y}$ is represented with a size of SF as $\mathbf{y} \in \{y_i | i \in \{1, 2, \cdots, \mathrm{SF}\}\}$ where each component y_i represents two bit-length, thus, we may have y_{01} and y_{11} where first value represents the bit index. Thus, the total required number of qubits to represent $\mathbf{y}$ is $N \cdot SF$. The qubit $|g\rangle$ is used to represent the carry qubits to help the operation of $|\mathbf{y}\rangle$ and $|\mathbf{b}\rangle$.

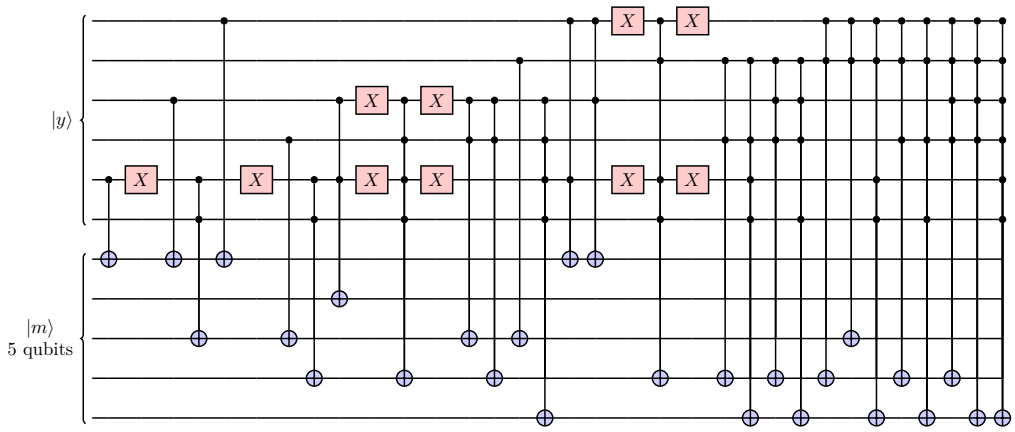


Figure 4.4: The N_f block

Designing N_f

The block denoted as N_f contains a *norm function* that is designed to calculate the norm $|.|$. Specifically, this norm corresponds to $\arg\min \|\mathbf{y} - \mathbf{b} \cdot \mathbf{C}\|_2^2$. The outcome of this computation is stored in $|\mathbf{m}\rangle$ qubits, which represents the result of the norm calculation. In this context, the size of the $|\mathbf{m}\rangle$ qubits aligns with the bit-length required to accurately represent the norm value itself. Thus, the required qubits to represent $|\mathbf{m}\rangle$ is 5 for our chosen system with dimension SF $= 3$.

Designing U_δ

In this part, specifically in U_δ, we introduce the idea of utilizing quantum computing to find the minimum. The goal is to check a condition where $f(b) < \delta$, and the value of δ is determined using the associated qubits.

Here, we are executing Grover's circuit, aiming to identify the minimum value, as indicated in Eq. 4.1. The concept involves the computation of $|\delta\rangle + |\mathbf{m}\rangle'$. It is important to mention that we utilize the one's complement notation for $|\mathbf{m}\rangle$, which is denoted by the X-gate. If $|\mathbf{m}\rangle$ is less than $|\delta\rangle$, the marked qubits will be set to 1; otherwise, they will be set to 0. Thus, the computation can be written as follows:

$$g = \begin{cases} 1 & \text{if } m < \delta \\ 0 & \text{otherwise} \end{cases} \tag{4.2}$$

Since we are working with Z qubits, as a result of $\arg\min \|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2$, the size of the qubits representing $|\delta\rangle$ is also the same. It is worth noting that we must employ

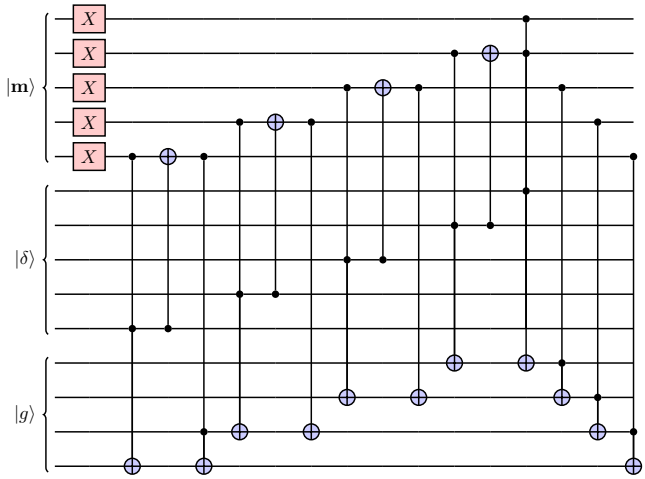


Figure 4.5: The U_δ block

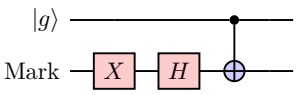


Figure 4.6: The M_f block

$|g\rangle$ qubits to assist in the carry computation of both $|\delta\rangle$ and $|g\rangle$. Thus, the result of qubits are carried through the mark register, as explained in the next subsection.

Designing M_f

Within this block, the concept is to mark the states with a negative computation $|-\rangle$ after being computed with $f(b) < \delta$. This is an extension of the work presented in Fig. 4.1. The required qubits to represent this are only 1 qubit, which is modified using the X-gate and the H-gate. Continuing from Fig.4.5, the idea is to pass the last carry qubit $|g\rangle$ to the Mark qubits, as shown in Fig.4.6. It is important to note that this does not require an inverse gate M_f^{-1} at the end of the computation.

4.4 A Comparative Analysis of DHA and IIMSA Performance

This section discusses the comparison performances between DHA and IIMSA with the contribution of non-quantum methods (CCR and ZF). This section is divided into five subsections:

1. IIMSA vs mixed algorithm (e.g ZF, CCR and ML):
   We assess the performance of IIMSA and classical methods (i.e., ZF, CCR, and ML). We also evaluate Grover's algorithm performance with respect to $f(x) = \delta$.

2. DHA + mixed algorithm:
   We assess the performance of DHA integrated with the classical methods (i.e ZF, CCR) as a function of variance σ^2 and SF.

3. IIMSA + mixed algorithm:
   We compare the performance of IIMSA integrated with the classical methods (i.e ZF, CCR) as a function of variance σ^2 and SF.

4. The L_{max} analysis for both IIMSA and DHA:
   Performance analysis is conducted to compare IIMSA and DHA as a function of L_{max}.

5. IIMSA and DHA integrated with (CCR-DHA, CCR-IIMSA, ZF-DHA and ZF-IIMSA):
   Performance analysis is conducted to compared CCR-DHA, CCR-IIMSA, ZF-DHA, and ZF-IIMSA.

This measurement phase examines two parameters:

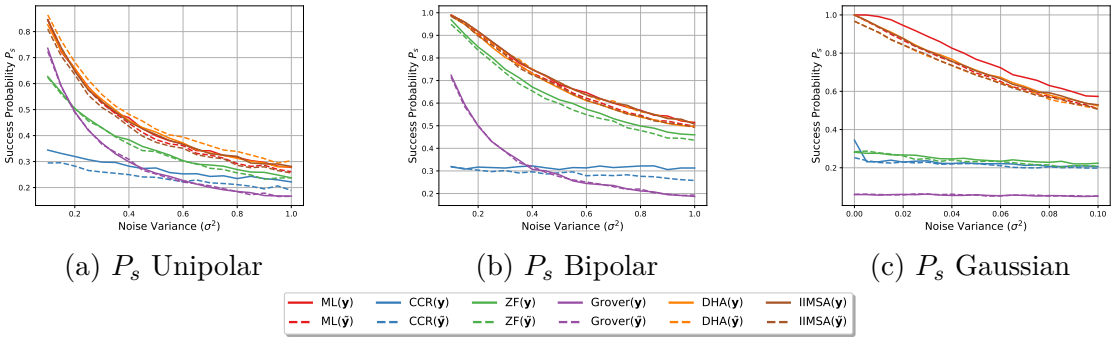
1. The success probability (P_s)

2. The accumulation of Grover's iterations (nb_{it})

The variable nb_{it} represents the total number of Grover's iterations. The nb_{it} involves an accumulation evaluation identical to that of L_{DHA} and L_{IIMSA}. The optimal performance is achieved when there is a high success probability (P_s) along with a low count of Grover's iterations (nb_{it}). In this chapter, we consider small-size code families so as to be able to simulate the proposed quantum algorithms with classical processors, as proof of concept. The simulation is conducted in a noise-free circuit, assuming that noise on the Grover algorithm is not taken into account, as explained in 3.2.2. Additionally, the complexity analysis considers solely on quantum speedup part, which compares the speed between the classical and quantum algorithm, as explained in 3.2.3. The used configuration of SF and the corresponding number of users along with code types is summarized in Table. 3.1 in Chapter 3.

4.4.1 IIMSA vs Mixed Algorithm (e.g ZF , CCR and ML)

As explained in Chapter 3, Grover's algorithm has not yet achieved optimal performance in solving the AUD problem, in contrast to classical methods. Therefore, this



(a) P_s Unipolar (b) P_s Bipolar (c) P_s Gaussian

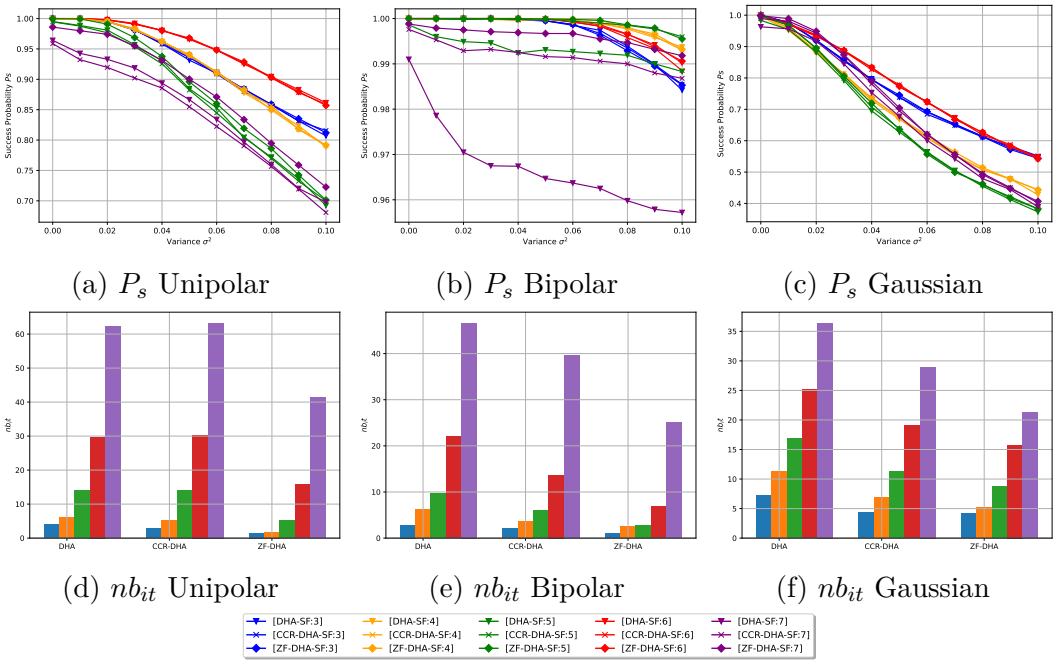
Figure 4.7: P_s classical (i.e ZF, CCR, ML) and Grover's algorithm with IIMSA

subsection aims to reevaluate its performance against classical methods. The context of Grover's algorithm is modified to execute $f(x) < \delta$ which permits to identify the minimum distance of $\arg\min ||\mathbf{y} - \mathbf{b} \cdot \mathbf{C}||_2^2$, as proposed by our new algorithm IIMSA.

First of all, let us compare our proposed algorithm, IIMSA, with ML, CCR and ZF. Using the same configuration as proposed in section 3.3.2, we simulated $10,000$ realizations with a precision of $p = 2$ to obtain the observed signal $\tilde{y}$ and code types with the following configuration:

1. Unipolar Model: $N = 4$ and SF$= 3$
2. Bipolar Model: $N = 3$ and SF$= 3$
3. Random Gaussian Model: $N = 5$ and SF$= 3$

We compare the use of classical methods with IIMSA, where the SF configuration is set to 3 for all code types, and L_{IIMSA} and L_{DHA} are configured to $22.5\sqrt{2^N}$. The corresponding N changes as a function of SF because each specific code type exhibits a different level of non-orthogonality, resulting in varying values for N. The result is shown in Fig. 4.7, which presents a comparison between the performance of classical and quantum algorithms, along with the incorporation of IIMSA, across Unipolar, Bipolar, and Gaussian scenarios. The results illustrate that our proposed IIMSA algorithm is comparable with ML techniques, applied to all codetypes, although IIMSA has a lower P_s compared to ML. This observation underscores the significant advantages of the IIMSA algorithm compared to Grover's algorithm, as our approach aims to locate the minimum algorithm, applying that $\arg\min ||\mathbf{y} - \mathbf{b} \cdot \mathbf{C}||_2^2$. It also demonstrates a very promising solution in terms of performance when compared with classical methods (i.e., CCR, ZF) for all code types (i.e., Unipolar, Bipolar, and Gaussian). We also compare the case where precision is $p = 2$, (denoted as $\tilde{y}$) and



(a) P_s Unipolar (b) P_s Bipolar (c) P_s Gaussian

(d) nb_{it} Unipolar (e) nb_{it} Bipolar (f) nb_{it} Gaussian

Figure 4.8: P_s and nb_{it} w.r.t variance σ^2 (DHA, CCR-DHA, ZF-DHA)

the case without precision, (denoted as y). This shows a similar behavior. It shows that $\tilde{y}$ has a lower success probability due to the rounding function, which applies to all codetypes. Indeed, when the quantized signal $\hat{y}$ is used, we loose the information contained in the removed part. However, this operation is needed as explained in section 3.2.1.

This section concludes that IIMSA is a promising solution in terms of performance, far superior to the other classical methods. The subsequent subsection delves into IIMSA's capabilities in addressing challenges beyond those tackled by the DHA, exploring how our algorithm can reduce the complexity of the DHA while increasing its performance. Besides, we also incorporate them with the classical methods (i.e., CCR, ZF) which may be promising to increase the success probability P_s.

4.4.2 DHA + Mixed Algorithm

As a function of variance σ^2

We conducted a comparison between DHA and a mixed algorithm (ZF and CCR) to assess their efficiency in determining the correct value of $\hat{\delta}$. Our expectation is to minimize the number of iterations (nb_{it}) when the classical algorithm could accurately identify $\hat{\delta}$. By analyzing results from different code types (Unipolar, Bipolar, and

Gaussian) as shown in 4.8a-4.8c, we observe interesting patterns.

In this case, P_s and nb_{it} are evaluated as a function of variance σ^2 and code types. The configuration is established with an upper-bound for nb_{it}, set as $L_{DHA} = 22.5\sqrt{2^N}$. We evaluate the values of nb_{it} for all codetype cases to facilitate a comparison between different methods, namely DHA, CCR-DHA, and ZF-DHA. Our objective here focuses on comparing different types of DHA in conjunction with classical methods.

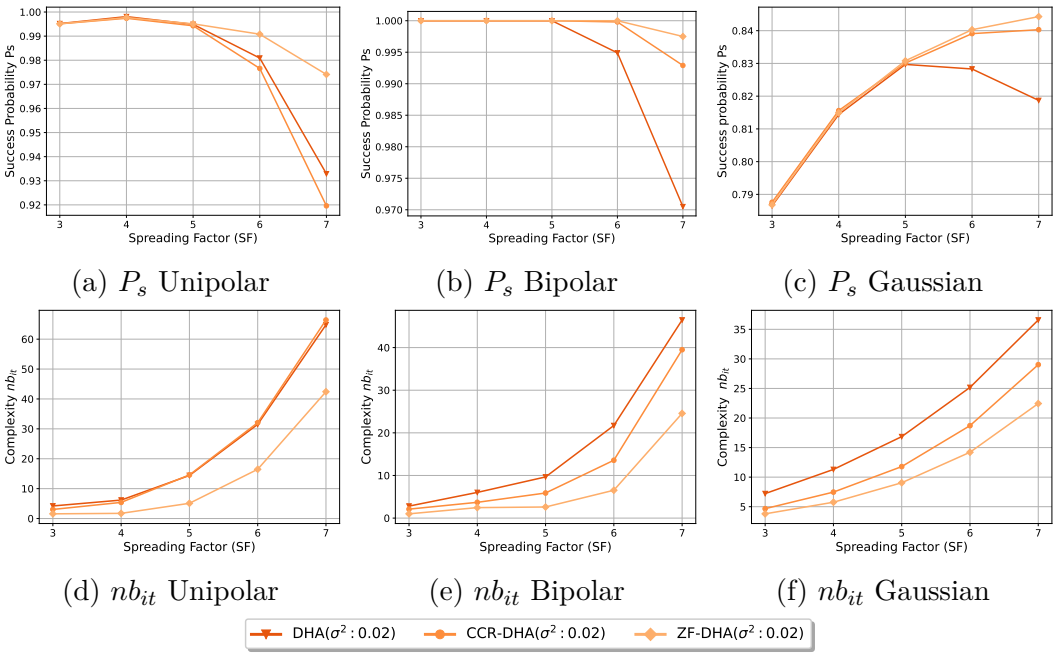
We can compare the performance of the first three methods, namely DHA, CCR-DHA, and ZF-DHA, using Fig. 4.8a-4.8c. When SF is set to 3, 4, and 6, the comparison of DHA and IIMSA shows similar performance. However, when SF is set to 5 and 7, the success probability P_s exhibits notable differences. It is observed that ZF-DHA demonstrates a superior success probability compared to the others, followed by CCR-DHA. This trend is observed specifically in the unipolar and bipolar scenarios at SF levels of 6 and 7, while the remaining scenario exhibits similarity.

It is worth noting that on the Gaussian part, the success probability (P_s) is low due to the closer proximity between components, making it susceptible to noise contamination (σ^2). Interestingly, all mixed types (DHA, CCR-DHA, ZF-DHA) show similar P_s despite higher variance (σ^2) in this case. Notably, even with a high number of users (N) at $SF = 7$, the performance of P_s remained in the middle range compared to other code types.

To analyze the number of iterations (nb_{it}), we examined Fig. 4.8d - 4.8f, which displayed the relationship between code types, SF, and nb_{it}. It is evident that DHA consistently required a higher number of Grover iterations compared to other methods for all code types. We observe that ZF-DHA outperforms all performances, since it leads to accurate detection $\hat{\delta}$ which may reduces the time. This performance is followed by CCR-DHA, which is promising to reduce the complexity as well. This applies to all codetypes and all SF.

Furthermore, surprisingly, CCR-DHA exhibits lower complexity than the standard DHA in the Unipolar case. This occurs when SF is set to $5, 6, 7$. However, in the Bipolar and Gaussian cases, CCR-DHA still proves to be a promising solution. On the other hand, CCR-DHA outperforms ZF-DHA in a specific scenario, namely, the Gaussian case with a small SF. This outcome arises because, when SF $= 3$, the active user set is relatively small, resulting in CCR-DHA having a higher probability of accurate detection compared to ZF-DHA.

In summary, ZF-DHA exhibits a high success probability while maintaining simplicity with fewer iterations (nb_{it}). It is followed by CCR-DHA and the original DHA. Our approach proves the efficiency of both parameters: performance P_s and complexity nb_{it}.



(a) P_s Unipolar (b) P_s Bipolar (c) P_s Gaussian

(d) nb_{it} Unipolar (e) nb_{it} Bipolar (f) nb_{it} Gaussian

Figure 4.9: P_s and nb_{it} w.r.t SF (DHA, CCR-DHA, ZF-DHA)

As a function of SF

In this section, we now consider the performances of the classically-aided DHA algorithms. We present a comparison between DHA and a mixed classical algorithm (ZF and CCR) to evaluate their efficiency in determining the correct value of $\hat{\mathbf{b}}$.

In this case, we consider the same three code types (i.e Unipolar, Bipolar, and Gaussian). P_s and nb_{it} are evaluated as a function of SF as a function of SF for the different algorithms, namely DHA, CCR-DHA, and ZF-DHA. The configuration is established with an upper-bound for $L_{DHA} = 22.5\sqrt{2^N}$ with a noise variance $\sigma^2 = 0.02$. Results are presented in Fig. 4.9.

First, we can observe that across all codetypes, all algorithms (DHA, CCR-DHA, and ZF-DHA) demonstrate similar P_s values when SF is small. Interestingly, as the SF value is higher than 6, ZF-DHA outperforms the other DHA types (DHA and CCR-DHA). Then, we can notice that the use of CCR degrades the performances for unipolar code, while it brings improvement for Bipolar and Gaussian codes. This can be explained by the fact that the CCR detects the users activity in a less accurate way in the Unipolar codes case, due to the accumulation of positive interference over all chips, thus leading oftenly to an *active* decision. Meanwhile, Bipolar and Gaussian decoding leads to both positive and negative interference, which reduces the risk of false alarm.

Secondly, we have also observed that the success probability (P_s) is lower in the Gaussian part due to the closer proximity between components, which makes it more susceptible to noise contamination (σ^2). Despite the lower P_s in the Gaussian part, it exhibits a distinct trend when compared to Unipolar and Bipolar components. This difference can be attributed to the fact that as SF increases, two codes are less likely to be confused. However, as the number of users increases, the random generation might lead to have two close codewords, thus reducing the performances. The curve shape thus shows the compromise between these two effects.

In addition, Fig. 4.9d - 4.9f, focus on the evolution of nb_{it} as a function of SF. It shows that DHA consistently required a higher number of iterations compared to other methods for all code types. We observe that ZF-DHA outruns other DHA types (i.e DHA, CCR-DHA). This is due to the fact that its accurate detection permits to stop the search sooner.

Finally, the trend indicates that at low SF values, the number of iterations (nb_{it}) is quite competitive among all algorithms. Particularly, when SF is set to 3, the nb_{it} values are very close to each other. This closeness in values can be attributed to the fact that with a small SF, the number of Grover's iterations in each step is small, resulting in a closely aligned comparison graph. Moreover, in the Unipolar scenario, CCR-DHA is still less efficient than DHA when the SF value is high. The reason behind this can be attributed to the fact that as seen before, the CCR suffers from high interference in the Unipolar case.

In summary, ZF-DHA exhibits a high success probability while maintaining simplicity with fewer iterations (nb_{it}). It is followed by CCR-DHA and the original DHA.

4.4.3 IIMSA + mixed algorithm

As a function of variance σ^2

Similar to Section 4.4.2, this subsection assesses the performance and complexity of IIMSA, CCR-IIMSA, and ZF-IIMSA as a function of variance σ^2. The main objective is to determine whether the mixed classical algorithm is efficient in handling the IIMSA algorithm while maintaining a high success probability P_s with fewer iterations nb_{it} required.

In this case, we considered three code types (i.e Unipolar, Bipolar, and Gaussian), and evaluate P_s and nb_{it} as a function of variance σ^2 and code types. As explained in section 4.4.2, the upper-bound of IIMSA is set as $L_{IIMSA} = L_{DHA} = 22.5\sqrt{2^N}$. It is worth noting that the success probabilities P_s with all evaluated performances (i.e IIMSA, CCR-IIMSA and ZF-IIMSA) have a similar performance. As described in section 4.4.1, from Fig. 4.10a-4.10c, the unipolar case tends to yield a relatively

low success probability, achieving $P_s = 0.7$, while the bipolar case exhibits higher success probabilities with $P_s \geq 0.9825$, and the Gaussian case has the lowest success probability with $P_s = 0.4$. These differences in success probabilities can be attributed to the varying distances between each component among all code types. Bipolar, in particular, has a significantly larger Euclidean distance between each component $\mathbf{C} \in \{-1, 1\}$, making it easier to detect and more resistant to noise contamination. On the other hand, Gaussian coding features a smaller Euclidean distance, making it more susceptible to being adversely affected by noise σ^2. Overall, the P_s among all evaluated methods (IIMSA, CCR-IIMSA, and ZF-IIMSA) exhibits similar performance, except for the bipolar scenario where SF is used. In this case, ZF-IIMSA outperforms all other methods.

Concerning the number of iterations nb_{it}, as illustrated in Fig. 4.10d-4.10f there is a difference among all IIMSA types. We conclude that ZF-IIMSA outperforms other IIMSA types (i.e IIMSA and CCR-IIMSA) for all codetypes cases (i.e Unipolar, Bipolar, Random Gaussian) and also all SF types. It has been shown that the higher SF, the more distinct the complexity is among all methods. This signifies that ZF-IIMSA has an accurate detection, making the Grover requires fewer iterations. This performance is followed by CCR-IIMSA with less accurate detection but which can still outperform the original IIMSA.

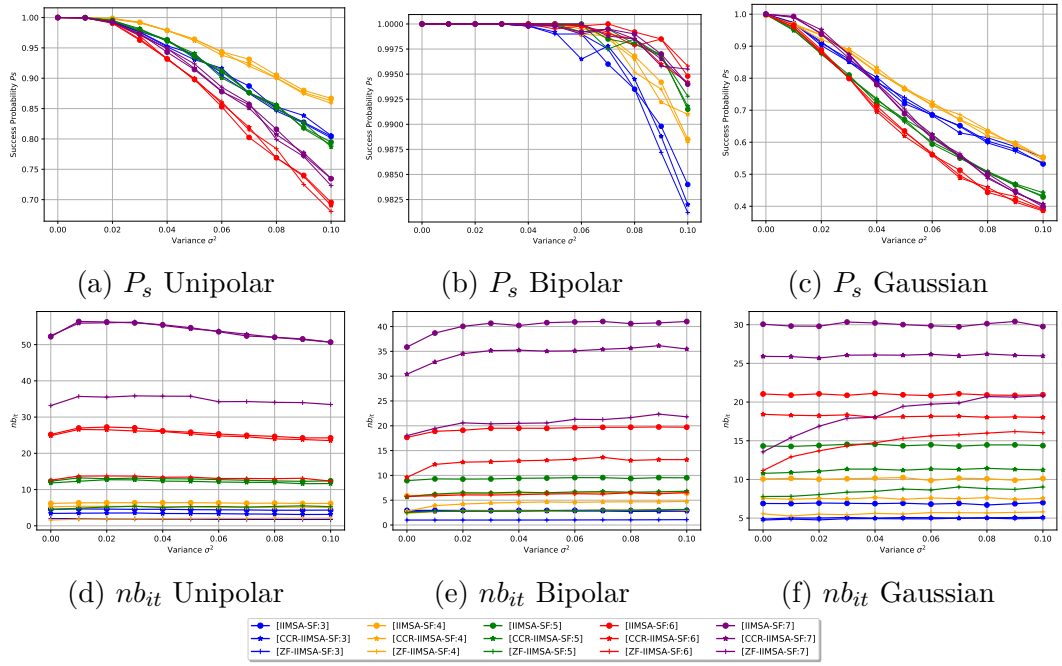
In summary, ZF-IIMSA exhibited a good success probability while maintaining simplicity with fewer iterations (nb_{it}). However, the ZF-IIMSA performance has a similar behavior with other methods. It is followed by CCR-IIMSA and the original IIMSA. The success probability remains the same among all IIMSA types (i.e IIMSA, CCR-IIMSA and ZF-IIMSA), except for bipolar case with SF = 7. The complexity nb_{it} shows that ZF-IIMSA outperforms other methods, followed by CCR-IIMSA and IIMSA which denotes less complexity.

As a function of SF

Similiar with Section 4.4.2, this section discusses the performances between IIMSA, CCR-IIMSA, and ZF-IIMSA as a function of SF. The main objective is to address if the previous conclusions for DHA also apply for IIMSA.

We evaluate the performances of P_s and nb_{it} for the same three code types. As explained in section 4.4.2, the upper-bound is set to $L_{IIMSA} = L_{DHA} = 22.5\sqrt{N}$, Results are presented for a noise variance $\sigma^2 = 0.02$.

First, as illustrated in Fig. 4.11a-4.11c, we can note that the success probability P_s with all evaluated performances (i.e IIMSA, CCR-IIMSA and ZF-IIMSA) are similar. The Unipolar and Bipolar SFs tend to have $P_s = 1$ among all SFs, while the Gaussian SF exhibits a wider range across different SF. This is related to the random choice of the Gaussian codes.



(a) P_s Unipolar (b) P_s Bipolar (c) P_s Gaussian

(d) nb_{it} Unipolar (e) nb_{it} Bipolar (f) nb_{it} Gaussian

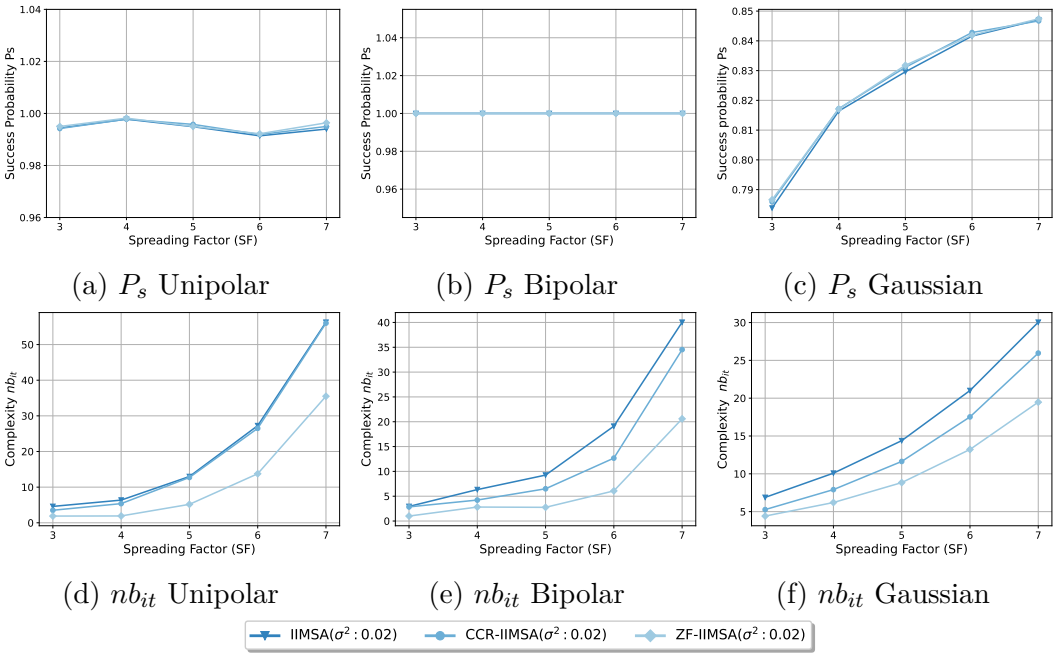
Figure 4.10: P_s and nb_{it} w.r.t variance σ^2 (IIMSA, CCR-IIMSA, and ZF-IIMSA)

Meanwhile, when considering the number of iterations nb_{it}, as we have seen in Fig. 4.11d-4.11f, there is a difference among all IIMSA types. We can observe that ZF-IIMSA outperforms the 2 other IIMSA types (i.e IIMSA and CCR-IIMSA) for all SF. This signifies that the classical ZF has a more accurate detection, making the Grover requires fewer iterations. This performance is followed by CCR-IIMSA with less accurate detection but still can outperform the original IIMSA. The CCR-IIMSA however has a similar performance with IIMSA in unipolar case, but it does outperform the IIMSA on other cases such as Bipolar and Gaussian.

In summary, ZF-IIMSA also exhibits an high success probability while maintaining simplicity with fewer iterations (nb_{it}). Despite the success probability has a similarity with other methods, the ZF-IIMSA is still outperforming IIMSA and CCR-IIMSA the nb_{it} case. This ZF-IIMSA advantage is more important for the high SF range, which is promising for dense IoT networks.

4.4.4 IIMSA and DHA integrated with (CCR-DHA, CCR-IIMSA, ZF-DHA and ZF-IIMSA)

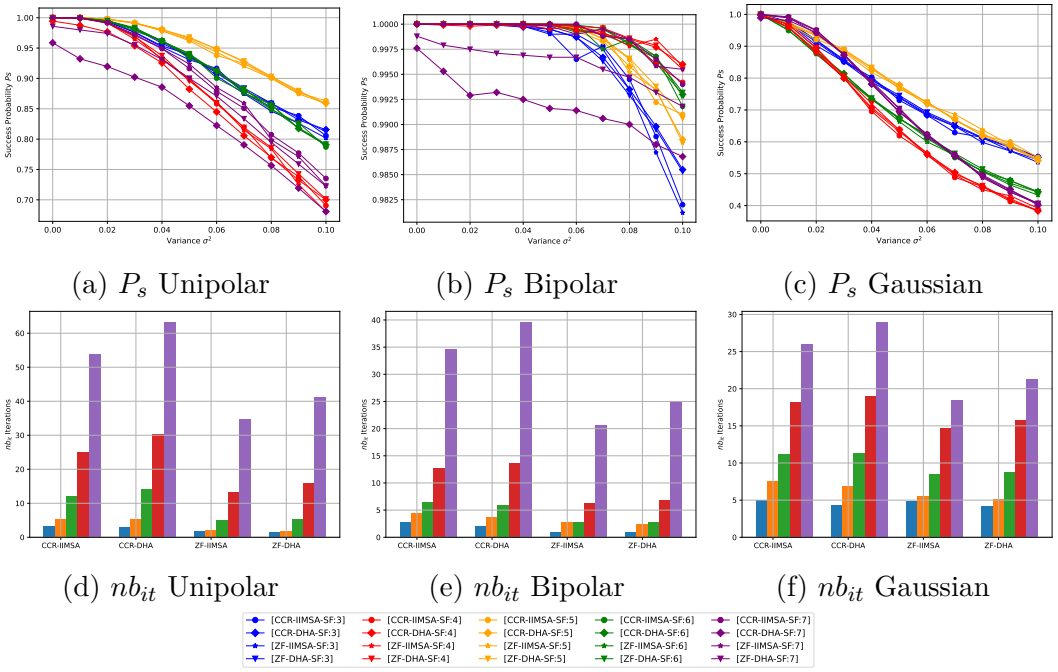
This section focuses on the impact of using the classical detectors (i.e. CCR and ZF) to be integrated with both DHA and IIMSA and compares both impacts when applied



(a) P_s Unipolar (b) P_s Bipolar (c) P_s Gaussian

(d) nb_{it} Unipolar (e) nb_{it} Bipolar (f) nb_{it} Gaussian

Figure 4.11: P_s and nb_{it} w.r.t SF (IIMSA, CCR-IIMSA, and ZF-IIMSA)



(a) P_s Unipolar (b) P_s Bipolar (c) P_s Gaussian

(d) nb_{it} Unipolar (e) nb_{it} Bipolar (f) nb_{it} Gaussian

Figure 4.12: P_s and nb_{it} w.r.t σ^2 (CCR-IIMSA, ZF-IIMSA, CCR-DHA, ZF-DHA)

to all code types (i.e Unipolar, Bipolar, Random Gaussian), where some of them are already done in sections 4.4.3 and 4.4.2. Here, the objective is to find the algorithm which which has the highest success probability P_s and low complexity nb_{it}. As used in previous subsection 4.4.2, 4.4.3, the upper-bound is set to DHA and IIMSA are L_{DHA} and L_{IIMSA} where both of them respect $22.5\sqrt{2^N}$.

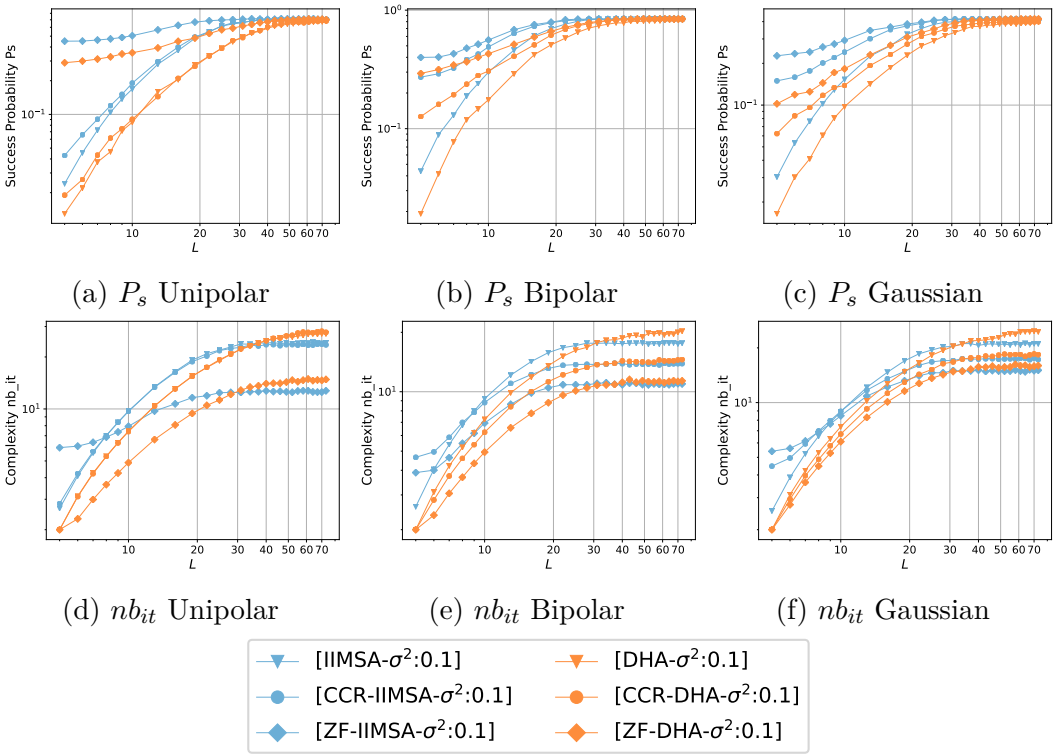
Let us analyze Fig. 4.12a - 4.12c where several evaluations have been assessed. It can be observed that the high SF range exhibits a low probability of success P_s due to the presence of a large number of users N, as indicated by both unipolar and bipolar scenarios. However, as explained in the previous subsection, the SF= 6 is exceptionally higher because of its family non-orthogonal codes. The Gaussian, as usual, due to the closest distance between each code component, is hard to detect active users. Thus, the result among all SFs is the same. On the small regime of ZF, the behavior of IIMSA types (i.e. CCR-IIMSA, ZF-IIMSA, CCR-DHA, and ZF-DHA) remains similar.

It is noted that ZF-IIMSA has better performances when SF is 7 for unipolar. This is due to the fact the ZF-IIMSA has more accurate detection prior to CCR-IIMSA and also other DHA types. Both of them outperform the DHA part, followed by CCR-DHA and ZF-DHA. On the bipolar side, when SF is 7, the CCR-IIMSA and ZF-IIMSA have competitive values. However, on other SF, this does not apply to other SFs cases where the performance results a random value.

Regarding the nb_{it} aspect, which evaluates the number of iterations, it is evident that the mixed classical ZF algorithm has shown superior performance compared to the CCR contribution for all code types. Additionally, we observe that the original DHA algorithm requires more iterations (nb_{it}) in comparison to IIMSA, our proposed algorithm designed to reduce the number of iterations for DHA. This observation holds true across all SF. In conclusion, ZF-IIMSA emerges as a promising solution, especially considering that ZF has low complexity when combined with our new algorithm IIMSA. To sum up, this section demonstrates that ZF-IIMSA outperforms all classical and DHA algorithm. Although the success probability P_s does not show significant changes, ZF-IIMSA succeeds in reducing the number of iterations (nb_{it}) compared to the original DHA, with or without the classical CCR algorithm. To conclude, ZF (and CCR to a lesser extent) is an effective classical method, which permits, when combined with quantum algorithms to achieve fewer Grover's iterations.

4.4.5 The L_{IIMSA} analysis for both IIMSA and DHA

This section focuses on examining the influence of analyzing the number of iterations denoted by $L \in \{1, \cdots, L_{IIMSA}\}$, where $L_{IIMSA} = 22.5\sqrt{2^N}$. This analysis is conducted for all code types and for a noise variance $\sigma = 0.1$. DHA based curves are plotted in red, and IIMSA ones in blue, to keep the same aspect than Fig. 4.9 and



(a) P_s Unipolar (b) P_s Bipolar (c) P_s Gaussian

(d) nb_{it} Unipolar (e) nb_{it} Bipolar (f) nb_{it} Gaussian

Figure 4.13: P_s and nb_{it} w.r.t L

Fig. 4.11.

First of all, we can observe in Fig. 4.13, that as L increases, P_s increases, but nb_{it} also increases. This due to the fact that, as we allow for more trials within the algorithms, it is more likely to find the solution, but at the cost of more iterations in average.

Secondly, we can observe that in Fig. 4.12a to Fig. 4.12c, the success probability (P_s) of IIMSA surpasses the DHA's one, when they are both used in the original version, but also when improved with CCR or ZF. This is due to the fact that IIMSA exploits the estimation of the number of solutions at each step to be more efficient in the search. Besides, ZF-IIMSA outperforms all the other algorithms. This trend can be observed for all codetypes.

On the other hand, we observe a distinct performance trend concerning nb_{it}. In Fig. 4.12d - 4.12f, it can be seen that DHA with the additional classical algorithm (ZF and CCR) outperforms IIMSA, especially when L is small. This is due to the fact that in IIMSA, the algorithm starts with a higher number of iterations as defined by L_{opt}, while DHA starts with a random value taken in an interval $L \in \{0, \cdots, \lfloor m \rfloor\}$ as explained in Algo. 2, with m gradually increasing from 1. As the *while* loop stops when the number of iterations has exceeded the level, DHA cross this limits sooner than IIMSA. However, this behavior disappears when L increases. Indeed, in this case, the *while* loop is more likely to stop because the minimum has been found. Thus, the previous small scale behavior is not dominant anymore. This pattern holds true for all mixed classical algorithms (ZF and DHA).

In addition, it is worth noting that among all code types, Bipolar shows a high success probability (P_s) compared to the others. Specifically, for small $L_{max} \in \{7, \cdots, 10\}$, some methods achieve $P_s = 1$, which significantly surpasses the performance of Unipolar, where only one method reaches this level at this range. In contrast, Gaussian does not achieve $P_s = 1$. This difference can be attributed to the fact that Bipolar code type has higher Euclidean distance $\mathbf{C} \in \{-1, 1\}$, leading to more accurate detections and lower susceptibility to noise contamination. This also applies to the required number of Grover's iterations (nb_{it}), where Bipolar requires fewer nb_{it} compared to other code types. This signifies that Bipolar is faster at detecting accurate detections. This is logical since being less vulnerable to noise allows the algorithm to detect targets more easily. The maximum nb_{it} reached by Bipolar is 18, while Unipolar and Gaussian achieve 30 and 25, respectively.

While CCR seems to struggle to compete with ZF, it exhibits a higher success probability (P_s) compared to the original algorithm. This indicates that CCR contributes positively to the calculations, leading to a small number of iterations (nb_{it}) required for accurate detections. Consequently, CCR performs well and outperforms the original DHA and IIMSA.

Furthermore, it is important to emphasize the significant impact of the classical

algorithm (ZF and CCR) in these results. These algorithms notably enhance both the success probability (P_s) and the number of iterations (nb_{it}). Specifically, for $L > 20$, the results demonstrate that ZF-IIMSA exhibits similar performance, but with a smaller nb_{it} compared to other methods. Following closely is ZF-DHA, which also demonstrates a considerable impact on nb_{it}. Thus, we can conclude that ZF serves as an excellent method for providing accurate initialization set for the quantum minimum searching algorithms.

To conclude, ZF (and CCR to a lesser extent) is an effective classical method, which permits, when combined with quantum algorithms to achieve fewer Grover's iterations.

4.5 Conclusion

We have designed the Grover's quantum circuit which allows to have $f(x) < \delta$ and also the implementation to find the minimum $\arg\min \|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2$. We have evaluated and assessed the proposed algorithm IIMSA to improve the existing method DHA, with also the integration of classical methods (i.e, CCR and ZF) which is proven to increase the performance of DHA and IIMSA.

It has been demonstrated that our proposed algorithm, IIMSA, outperforms DHA, resulting in reduced complexity and superior performance. Moreover, its integration with classical methods is considered effective, especially when combined with ZF, as it enables more accurate detection with minimal complexity. The most efficient combination is achieved when our proposed algorithm is integrated with ZF, referred to as ZF-IIMSA, which delivers superior performance with low complexity.

The complexity is mathematically demonstrated, where IIMSA is proposed based on a random solution. We observe that IIMSA achieves a complexity better than that of DHA, denoted as $22.5\sqrt{2^N}$. Future work will involve improving IIMSA, including the verification of whether $\hat{S} < \frac{K}{2}$, otherwise, the algorithm should find new index i. This is primarily because our IIMSA algorithm may run when $\hat{S}$ that satisfy all conditions, which is *not* accurate due to the unwanted solution $\hat{S} \geq \frac{K}{2}$. Another aspect of future work is to investigate the complexity of IIMSA.

Chapter 5

Chapter 5

Enhanced Grover's algorithm

After dealing with IIMSA, in this chapter, we propose the Enhanced Grover's algorithm. This is an improved version of Grover's algorithm designed to ameliorate its performance. In this case, we aim to improve the Grover's algorithm by combining differently with the classical methods. We discuss the underlying theory, the main motivation behind its development, the proposed equation, the implications and insights derived from our findings, and also provide a simulation of our algorithm. The goal is to achieve a high success probability with a reduced number of Grover's iterations.

The main motivation is referred to as the quantum-hybrid solution, primarily used to harness quantum superiority along with classical assistance in solving multiple problems. The idea is to test Grover's algorithm with a small number of iterations, assumably less than the optimal L_{opt}, and verifying if the returned solution is valid. We compare the performance and complexity of the original Grover's algorithm with our Enhanced Grover's algorithm. We expect to observe smaller iterations in our algorithm compared to the original one while also keeping the performance better.

Therefore, the **key points** to be addressed are as follows:

- Explain and elaborate on the principles of the Enhanced Grover's algorithm, including the proposed theory, equation, implications, simulation, and experimental results.
- Discuss how the Enhanced Grover's algorithm can improve the performance of Grover's algorithm.
- Provide evidence, through simulations and mathematical analysis, that the proposed algorithm is superior to the original Grover's algorithm.

5.1 Introduction

In *Enhanced Grover's algorithm*, the idea is to enhance the existing Grover's algorithm that is proposed by Grover [96] by combining it with a classical test. Our proposed idea is to mix the classical and quantum algorithm, which aims to achieve higher success probability for a given number of iterations. We evaluate the expectation of the number of iterations to be compared with the original Grover. The following section discusses the principle theory of our proposed algorithm along with the performance.

5.2 Quantum Hybrid Solution

The primary motivation behind this research is the utilization of a *hybrid solution*, commonly referring to a program that simultaneously operates both classical and quantum components [97]. This terminology signifies the execution of quantum operations on quantum bits (*qubits*), typically on a quantum device, while classical computations are carried out using traditional algorithms or programming languages.

This terminology has been established within the realm of classical computing in conjunction with Microsoft's Quantum Cloud Service. In this setup, the classical computer handles standard execution tasks, while more complex tasks are offloaded to the Quantum Cloud Service, promising reduced computational complexity. It is essential to note that quantum cloud execution is exclusively conducted online, specifically for tasks of significant complexity. As a result, the Quantum Cloud Service leverages Quantum Processing Units (QPU) and delivers results directly to the classical computer. This approach holds significant promise as an alternative to employing an entire quantum computer. Fig 5.1 describes the concept where classical computer demands the cloud service to run several jobs, with the aid of the quantum processing units.

Inspired by this work, we propose an algorithm to enhance Grover's algorithm. This algorithm leverages the classical algorithm after performing a quantum measurement during the test. Our aim is to improve the performance and reduce complexity of Grover's algorithm in the realm of using both classical and quantum processors. We execute Grover's algorithm using qubits and analyze the results in terms of classical bits at the end. The success probability is determined through the classical algorithm, as illustrated in the following section.

5.3 Proposed algorithm

In this section, we delve into the foundational theory of the Enhanced Grover's algorithm, including its objectives and the detailed algorithm it encompasses. The

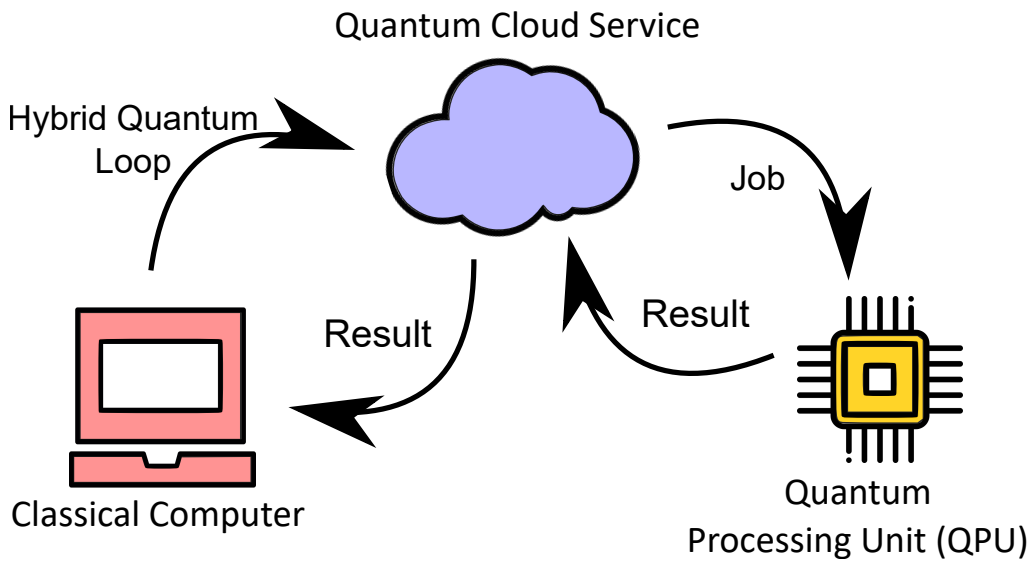


Figure 5.1: Quantum Hybrid Solution

primary goal of this proposed algorithm is to accelerate the basic Grover's algorithm. Indeed, the basic and natural approach is to run Grover algorithm with the optimum number of iterations as defined in Eq. 2.14 [29]. The number of iterations can be reduced to speed up the computation but at the cost of performances degradation Eq. 2.12. Nonetheless, we propose an algorithm which permits to keep similar performances while reducing the number of Grover iterations. The full algorithm is explained in Algo. 7.12 and Fig. 5.2.

The principle is to make several trials with Grover's algorithm (with j iterations) and test the outcoming solution, as illustrated by Fig. 5.2. Our primary objective is to minimize the total number of iterations of the Grover's algorithm while aiming to achieve a high success probability and low complexity. This is different with the proposed algorithm in IIMSA, where the number of iterations is chosen based on L_{opt} as cited in Eq. 2.14.

The algorithm is explained as follows. We define $T_{\max}$ as the maximum number of trials, and we aim to run j iterations, ideally fewer than $T_{\max}$. Assuming that we know the constraint that the solution has to verify what we want to find, denoted as S_{en}, once we run Grover's algorithm ($\mathcal{G}$) multiple times, we check if the returned solution S_{en} satisfies the constraint. If it does not, we run a new trial and increment

Algorithm 5: Enhanced Grover Algorithm

Data: Define T_{max}, $P_{en}^{j} = 0$, $targPs$, $j < L_{opt}$, $nb_{\text{trial}} = 0$

```
while nb_trial < T_max do
    Perform Grover G with j-iterations;
    if Solution verifies the constraint then
        Exit while Loop;
    else
        nb_trial = nb_trial + 1;
        Run P_en^j based on Eq. 5.2.
```

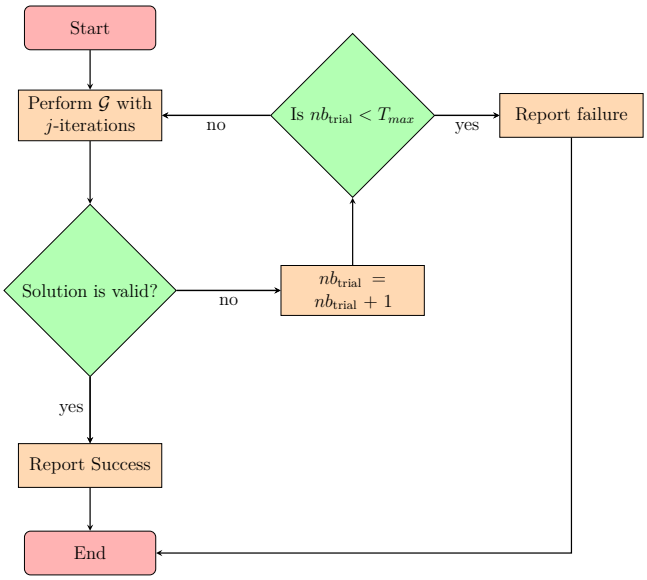


Figure 5.2: Proposed searching scheme for reducing the number of iterations

the number of trials, represented by nb_{trial}. The algorithm will stop when one of the following conditions is met: 1.) If the solution S_{en} is valid, or 2.) nb_{trial} reaches the value of T_{max}.

A maximum number of trials (T_{max}) is set to bound the algorithm resource consumption. It must be noted that, to provide an output for the classical algorithm, the quantum part makes a measurement which suppresses the states superposition. Hence, at each new trial, one can not exploit the previous trials, and the Grover algorithm has to start from scratch.

Let us recall the success probability of Grover's algorithm as denoted in 2.12. The success probability is the same for each trial and is denoted by P_G^j, where j denotes the number of Grover iterations and G denotes the probability given by Grover, thus, it is represented as follows:

$$P_G^j = \sin^2((2j+1)\theta) \tag{5.1}$$

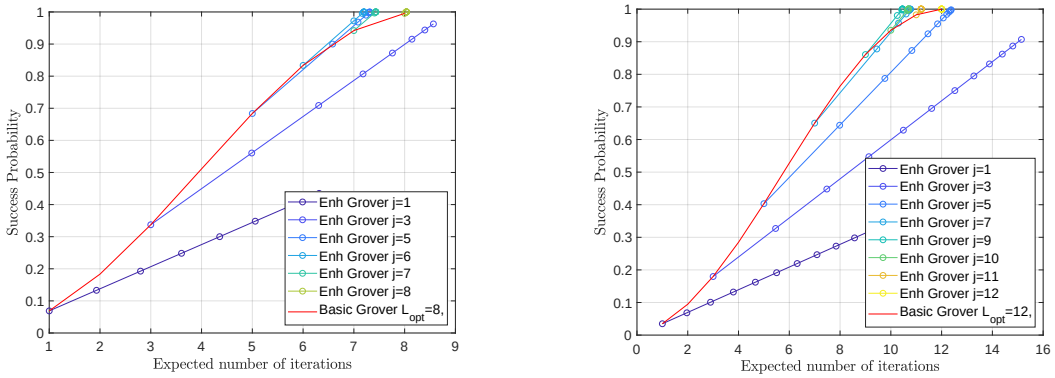
In our Enhanced Grover algorithm, we derive the new success probability expression based on bernouli distribution which is mainly used to describe the *yes/no* distribution. This probability is given by $\left(P_G^j\right) \cdot \left(1 - P_G^j\right)^{t-1}$ which defines the success probability of finding an actual solution after exactly t trials, where P_G^j is the Grover's success probability for j iteration. Consequently, the success probability P_{en}^j, obtained after at most T_{max} trials of this mixed algorithm can be expressed as:

$$\begin{aligned} P_{en}^j &= \sum_{t=1}^{T_{max}} \left(P_G^j\right) \cdot \left(1 - P_G^j\right)^{t-1} \\ &= 1 - (1 - P_G^j)^{T_{max}} \\ &= 1 - (1 - \sin^2((2j+1)\theta))^{T_{max}} \end{aligned} \tag{5.2}$$

If $T_{\max}$ is ∞, then P_{en}^j will be 1. However, we want to ensure that $T_{\max}$ should be as small as possible. In addition, we can evaluate the expected number of iterations performed within the Grover algorithm which also count the number of trial $nb_{\text{trial}} \in \{1, \cdots, T_{max}\}$:

$$\begin{aligned} E_{en}^j = &\left(\sum_{t=1}^{T_{max}-1} t \cdot j \cdot \left(P_G^j\right) \cdot \left(1 - P_G^j\right)^{t-1} \right) \\ &+ \left(T_{max} \cdot j\right)(1 - P_G^j)^{T_{max}-1} \end{aligned} \tag{5.3}$$

In the end, we evaluate the performance of Grover's algorithm success probability P_{en}^j with respect to P_G^j. Additionally, we assess the expectations represented by E_{en}.



(a) $N = 7, T_{max} = 9$ (b) $N = 8, T_{max=16}$

Figure 5.3: Average P_{en} vs Success probability P_G

5.3.1 Enhanced Grover Performances

Success Probability Enhanced Grover

In this section, we compare the performance of our proposal, denoted as *Enhanced Grover*, with the initial Grover's algorithm, denoted as *Basic Grover*. We have plotted on Fig. 5.3, the success probability as a function of the average number of iterations for the two approaches, where we consider $N = 7$ and $N = 8$ users. We assume that for both scenario, the number of solution is $S = 1$. Thus, Grover's optimum number of iteration for both scenario would be $L_{opt} = 8$ for $N = 7$ and $L_{opt} = 12$ for $N = 8$, respectively. It is true that the iteration of Grover's algorithm follows the distribution of $j \in \{1, \cdots, L_{opt}\}$ while the Enhanced Grover algorithm consists of several j-iterations, each of which belongs to different Grover trials. This Enhanced Grover's algorithm depicted in the Fig. 5.3 relies on the concept of P_{en}^{j} vs E_{en}.

Fig. 5.3a illustrates the scenario with seven users, denoted as $N = 7$, and an optimal value of $L_{opt} = 8$. The success probability of the Enhanced Grover's algorithm, denoted as P_{en}^{j}, is notably high when j is in the set $\{6, 7, 8\}$, matching the expected number of iterations. In contrast, Grover's success probability follows the distribution described by Eq. 5.1. Notably, for j values in $\{6, 7\}$, it holds that $E_{en} < L_{opt}$, indicating promising performance without the need for eight iterations, as required by L_{opt}.

From Fig.5.3b, on the other hand, with more users $N = 8$ and $L_{opt} = 12$, we observe several iterations. It is worth noting that within the range of $j \in \{10, 11, 12\}$, there is a demonstration of high success probability of the Enhanced Grover's algorithm. Similar to Fig.5.3a, when E_{en} does not reach L_{opt}, we can achieve a higher success

probability, which is promising.

For the *Basic Grover* case, the number of iterations is the only degree of freedom and we retrieve the previous shape given by 2.12. Contrarily, for the *Enhanced Grover*, we have 2 degrees of freedom : (j, T_{max}). Interestingly, we can observe that there exists some sets which permit *Enhanced Grover* to reach a better compromise success probability P_G^j vs P_{En}^j. This proves that our *Enhanced Grover* permits to further improves Grover algorithm efficiency.

Mathematically speaking, we are searching for a value of j such that $P_G < P_{En}$. It is evident that the Grover's algorithm is running one trial always. Thus, to be comparable, we should compare the best outcome for both algorithm. The P_G represents the best outcome, as denoted by L_{opt}. Assuming that $j < L_{opt}$, in this context, we can satisfy the following condition:

$$\begin{aligned} P_G &< P_{En} \\ \sin^2\left(\frac{(2 \cdot L_{opt}+1)}{\sqrt{K}}\right) &< 1 - \left(1 - \sin^2\left(\frac{2 \cdot j+1}{\sqrt{K}}\right)\right)^{T_{max}} \end{aligned} \tag{5.4}$$

Let us denote $\sin^2\left(\frac{(2 \cdot L_{opt}+1)}{\sqrt{K}}\right) = x_1$ and $\sin^2\left(\frac{(2 \cdot j+1)}{\sqrt{K}}\right) = x_2$. Since we assume that $j < L_{opt}$, we can observe that $x_2 < x_1$ (due to their sinusoidal nature), and that $x_1 \approx 1$ because the optimal one. Therefore, we can represent them as follows:

$$\begin{aligned} P_G &< P_{En} \\ x_1 &< 1 - (1 - x_2)^{T_{max}} \\ x_1 + (1 - x_2)^{T_{max}} - 1 &< 0 \end{aligned} \tag{5.5}$$

In here, we know that the $0 < x_1 < 1$ and $0 < x_2 < 1$, due to the sinusoidal model. We also state that $x_1 = 1$ is the optimal one, thus we obtain:

$$(1 - x_2)^{T_{max}} < 0 \tag{5.6}$$

It is evident that the equation above depends on two degrees of freedom: the number of trials, denoted as T_{max}, and the Grover's iteration, denoted as j. However, this inequality is never satisfied since the result will always be greater than 0 with assuming that $x_1 = 1$. Thus, we can make this vary by assuming that $x_1 = x_2$ with the equation as follows :

$$\begin{aligned} P_G &< P_{En} \\ \sin^2\left(\frac{(2 \cdot j+1)}{\sqrt{K}}\right) &< 1 - \left(1 - \sin^2\left(\frac{2 \cdot j+1}{\sqrt{K}}\right)\right)^{T_{max}} \end{aligned} \tag{5.7}$$

while assuming that $x_1 = x_2$. We can change as follows :

$$\begin{aligned} P_G &< P_{En} \\ x_1 &< 1 - (1 - x_1)^{T_{max}} \\ x_1 + (1 - x_1)^{T_{max}} - 1 &< 0 \end{aligned} \tag{5.8}$$

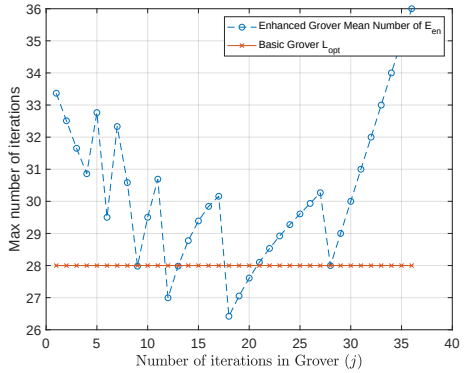
If we consider $x_1 = 0$ and $x_1 = 1$, neither condition satisfies the equation. Therefore, we should seek a middle-ground solution, such as $x_1 = 0.5$. In this case, it becomes evident that j can satisfy this equation when x_1 is in the midpoint. Consequently, with x_1 in the middle range, we can expect that the value of j will also fall within a middle range. This is the primary reason why our proposed solution surpasses Grover's algorithm with not exceeding the L_{opt}. While the optimal number of iterations L_{opt} reaches the maximum success probability with $x_1 = 1$, our goal j requires less than L_{opt}.

Expectation Enhanced Grover

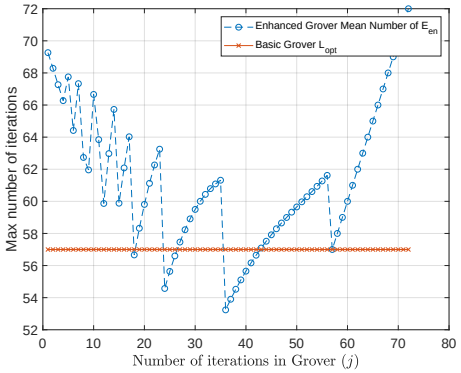
Here, we aim to introduce the mean number of iterations and trials required to achieve a target success probability, assuming a target of $P_s = 0.9$. To achieve this target success probability, there is no need to run L_{opt} times as the standard procedure for the basic grover. Instead, we can use a suboptimal approach denoted as $L_{s\text{-}opt}$ since the success probability is less than 0.99. We plot two variables: 1) the mean number of Enhanced Grover's algorithm (E_{en}) and 2) the Basic Grover algorithm ($L_{s\text{-}opt}$) with respect to Grover's iteration j. We illustrate the result for different number of users, first with $N = 11$, as shown in Fig.5.4a, second with $N = 13$, as illustrated in Fig.5.4b.

We begin by observing that the Basic Grover algorithm, with a fixed success probability of $P_s = 0.9$, achieves results of $L_{s\text{-}opt} = 28$ when $N = 11$ and $L_{s\text{-}opt} = 57$ when $N = 13$. It is noteworthy that these results fall short of the ideal value, denoted as L_{opt}, Where each L_{opt} corresponds to 35 and 71 for $N = 11$ and $N = 13$, respectively. This is unsurprising because reaching a success probability of $P_s = 0.9$ does not necessarily require the ideal L_{opt}. In contrast, our proposed algorithm exhibits variation relative to Grover's iterations, denoted as j. Notably, our approach sometimes outperforms the traditional Grover algorithm. For instance, when $N = 11$, our algorithm surpasses Grover's performance at iterations $j = 12$ and $j = 18$, yielding outstanding results. Similarly, when considering $N = 13$, our proposed algorithm displays variation across Grover's iterations. Consistent with the case of $N = 11$, our approach surpasses Grover's performance at iterations $j = 22$ and $j = 38$. This underscores the promising nature of our results.

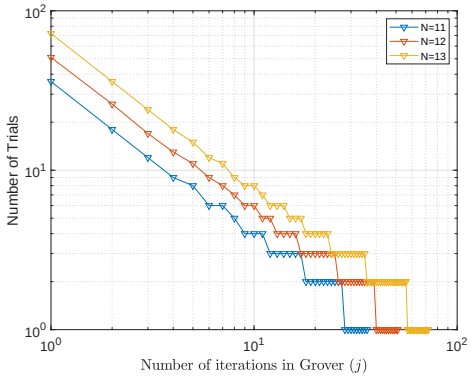
We have evaluated the number of trials w.r.t the Grover's iteration j as illustrated in Fig. 5.4c. We first note that as j increases, the required number of trials decreases. To be balanced with the Grover's iterations, our nb_{trial} is also decreases as well.



(a) $N = 11, L_{opt} = 28$



(b) $N = 13, L_{opt} = 57$



(c) Number of Trials for $N \in \{11, 12, 13\}$

Figure 5.4: Mean number E_{en}, Basic Grover $L_{s\text{-}opt}$ and number of trials with target $P_s = 0.9$

Conclusion

We have assessed both the Enhanced Grover's algorithm and the original Grover's algorithm, focusing on performance and complexity. Initially, it is worth noting that our Enhanced Grover's algorithm consistently outperforms the original Grover's algorithm, particularly in achieving or even surpassing the same L_{opt} values. This superiority has been verified for user counts of both $N = 7$ and $N = 8$. Furthermore, our proposed algorithm has consistently met performance expectations across different iterations of Grover (j), thereby demonstrating the existence of a point below the baseline Grover levels. It is worth noting that there is a negative relationship between the number of trials and Grover iterations.

Chapter 6

Chapter 6

Conclusion

This chapter discusses the brief summary of what we have contributed and also the future work to the research especially for the Grover's algorithm in the context of detecting the Active User Detection in Wireless networks.

6.1 Contribution

In **Chapter 1**, we discussed the case of wireless communication in the context of 5G, which enables shorter communication protocol between the BS (Base Station) and UE (User Equipment). This communication paradigm is referred to as the GF scheme. The Grant-Free (GF) scheme introduces a new challenge in AUD (Active User Detection), where multiple UEs can transmit messages simultaneously, each with its unique user identifier. This poses a significant challenge for the BS in detecting active and inactive users. We explored several classical methods to address this issue; however, they resulted in high computational complexity or limited performances. Consequently, we introduced quantum computing as a potential solution. We also delved into the principles of quantum mechanics, which describe the fundamental physics and properties that underlie these phenomena. We discussed the characteristics of quantum mechanics and how they can be harnessed. Additionally, we highlighted the advantages and disadvantages of using quantum computing in this context. We discussed more in details about quantum and the classical methods that have been harnessed to solve the AUD in the next chapter.

In **Chapter 2**, we emphasized the current state of the art in this thesis regarding the utilized model of the Active User Detection system, the historical development of codetypes, and the significance of Grover's algorithm as a promising approach for executing the Active User Detection. We also explored the origins of quantum superposition, often referred to as quantum parallelism, within the context of the Deutsch-Jozsa and Bernstein algorithms. Furthermore, we delved extensively into

Grover's algorithm, examining the necessary number of iterations and identifying the optimal iteration. Additionally, when it comes to scenarios where finding a solution is unknown, Grover's algorithm remains highly promising, especially in the context of locating the minimum in search algorithms, which is denoted by Boyer-Brassard-Høyer-Tapp (BBHT) and Durr-Hoyer Algorithm (DHA). We have previously discussed this, particularly in terms of establishing the upper bound, referred to as DHA. Furthermore, we conducted a thorough review of Grover's algorithm, highlighting its primary applications in wireless communication. We conclude that Grover's algorithm holds promise for wireless communication, particularly in the context of addressing the complexity of the AUD perspective.

In **Chapter 3**, we have highlighted that Grover's algorithm is a promising method as a searching engine, that permits to have $\mathcal{O}(\sqrt{K})$. We have designed the Grover's circuit with a constraint of $f(x) = \delta$, by analysing how to develop the Grover's algorithm in the context of AUD as well as how to be adapted with our codetypes (i.e unipolar, bipolar, and random gaussian). We also found that when Grover's algorithm using a strict ideal Grover is implemented in the AUD, which permits to have $f(x) = \delta$, is not achieving the best result. The complexity still follows the principle $\sqrt{K}$ but at cost of the performances. Thus, we seek to new algorithm to achieve better result but at cost of the complexity.

In **Chapter 4**, we introduce a new solution by designing Grover's algorithm to find the minimum solution. This approach leverages BBHT and DHA, with the primary objective being the development of a minimum searching algorithm. This chapter delves into various aspects, such as modifying the Grover's circuit to meet the condition $f(x) < \delta$ and optimizing it for creating a minimum searching algorithm that fulfills the criteria $\arg\min \|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2$. Within the scope of this objective, we also propose a new solution, named IIMSA, which holds promise for reducing the complexity introduced by DHA. We integrate it with classical methods (specifically, ZF and CCR) to enhance both DHA and IIMSA. We assess performance across various code types (Unipolar, Bipolar, and Random Gaussian) with multiple variances and slots represented by σ^2 and SF. Furthermore, we conduct a complexity comparison between IIMSA and DHA. In conclusion, our evaluation reveals that our proposed algorithm, IIMSA, outperforms DHA in terms of both complexity and performance. The complexity of IIMSA is proposed to be $9\sqrt{2^N}$, whereas DHA requires $22.5\sqrt{2^N}$.

The final contribution, discussed in **Chapter 5**, focuses on enhancing Grover's algorithm, namely Enhanced Grover's algorithm. This concept combines elements of both quantum and classical approaches to improve the success probability, denoted as P_s. We anticipate that our proposed algorithm will increase this success probability. We provide evidence that our success probability, denoted as P_e, exhibits higher success rates after several trials (nb_{trial}). Additionally, we demonstrate that the complexity of the Enhanced Grover's algorithm decreases as the number of Grover's iterations (k)

decreases.

6.2 Future Work

This work has opened up several avenues for future work. The list of future works have been addressed in the following :

1. **Evaluate Additional Classical Methods on Grover's algorithm**.
   We should consider including Approximate Message Passing (AMP), Successive Interference Cancellation (SIC), Parallel Interference Cancellation (PIC) or even the bayesian estimation in the evaluation to compare their performance and complexity with Grover's algorithm. This will provide a Comprehensive understanding of Grover's algorithm's position in this context.

2. **Investigate the specific scenario in Active User Detection (AUD)**.
   The channel information should be unknown, thus, we should have a channel estimation scenario. This allows our method to execute the channel more improved since the channel is counted.

3. **Considering the possibilities of many codebooks (i.e Optical Orthogonal Codes, Polar Codes etc)**.
   While we are currently assuming the use of only three codebooks (Unipolar, Bipolar, and Random Gaussian), it is worth noting that several other codebooks exist in wireless communication that could be explored to identify the most suitable one.

4. **Finding the minimum algorithm for** $\arg\min \|\mathbf{y}-\mathbf{b}\cdot\mathbf{C}\|_2^2$ **may be achieved without the use of Grover's algorithm**.
   There is a possibility of finding a minimum searching algorithm without using Grover's algorithm, which may be a promising alternative to running *numerous gates and computations* that require extensive memory resources. This may be addressed using Quantum Euclidean Distance, addressed by [98].

5. **The DHA's minimum has been improved to find its success probability**.
   The success probability of DHA only reaches 50%. It requires execution twice to reach 100%. However, there is a possibility of using the Grover-long algorithm, as explained in section 4, which is a promising method to achieve 100%. At this stage, we may enhance the already improved version rather than improving the original DHA.

6. **Calculating the IIMSA complexity**.
   Indeed, we have proven that the simulations of IIMSA have outperformed the complexity of DHA. This should be demonstrated mathematically, while also keeping in mind that the complexity of DHA is $22.5\sqrt{K}$.

7. **The limited number of quantum simulation (i.e Qiskit) in the classical processing**.
   For the current work, we have simulated quantum circuit using Qiskit, a python's library to run the quantum emulation over classical processing. However, there is a limited number of qubits that can be used in this simulation (maximum 30 qubits) [83]. Thus, we shall wait the future technology to cater more qubits.

Résume

Chapter 7

Resumé En Français

7.1 Introduction

Dans cette introduction nous mettons en évidence la motivation qui sous-tend l'étude de Détection des l'utilisateurs Actifs (AUD) dans les systèmes de communication sans fil, en particulier dans le contexte des défis posés par le schéma Système sans accord préalable (GF) dans la 5G. Ce schéma permet d'envoyer des messages est un accord préalable entre la Station de Base (BS) et l'Équipement Utilisateur (UE). Dans ce chapitre, nous donnerons un bref aperçu des problèmes liés à AUD et des méthodes classiques existantes qui traitent ces questions. Il est important de prendre en compte le compromis entre performances et complexité, ce qui nous a amenés à l'exploration de méthodes quantiques.

Nous montrerons que l'algorithme quantique est prometteur pour résoudre la complexité de la détection d'utilisateur actif dans les systèmes de communication sans fil. Nous allons dans la section suivante discuter du modèle système utilisé pour simuler notre algorithme quantique et le comparer à l'algorithme classique.

7.2 État De L'art

7.2.1 Introduction

L'objectif principal est ici d'examiner les recherches antérieures menées sur les techniques Détection des l'utilisateurs Actifs (AUD) dans les systèmes classiques. Nous fournirons une explication plus détaillée des diverses méthodes classiques employées, y compris Maximum de Vraisemblance (ML), Récepteur de Corrélation Conventionnel (CCR), et Zéro forcing (ZF). En outre, nous comparerons ces méthodes classiques en termes de complexité en utilisant des bases de données de recherche telles que la

recherche linéaire et la recherche binaire.

Un autre aspect important est l'introduction d'algorithmes d'informatique quantique conçus pour résoudre les problèmes d'optimisation. Nous nous pencherons plus particulièrement sur l'algorithme de Grover, une exploration complète de l'algorithme de Grover. Cet algorithme est particulièrement utile pour résoudre des problèmes dont la solution est inconnue, comme dans BBHT et DHA.

Enfin, nous décrirons le modèle de système utilisé pour AUD et les variables sélectionnées. Plus précisément, nous respecterons le plan défini où le signal observé est représenté par $\mathbf{y} = \mathbf{b} \cdot \mathbf{C} + \mathbf{W}$, avec $\mathbf{y}$ représentant le signal observé, $\mathbf{b}$ représentant l'ensemble des utilisateurs actifs, $\mathbf{C}$ représentant l'ensemble des mots codés, et $\mathbf{W}$ représentant les bruits gaussien. Nous considérerons trois types de mots de codes:

1. Unipolar, où $\mathbf{C} \in \{0, 1\}$;

2. Bipolar, où $\mathbf{C} \in \{-1, 1\}$; et

3. Gaussien, où $\frac{\mathbf{C}}{\|\mathbf{C}\|}$.

Nous considérons avoir N appareils connectés à une BS équipée d'une seule antenne, où les utilisateurs sont supposés être en mode veille par défaut et devenir actifs lorsqu'ils envoient des messages. Ce réseau utilise des systèmes Accès Multiple Non Orthogonal en Domaine de Code (CD-NOMA), où chaque utilisateur est identifié par mot du code. Les mots de code $\mathbf{C} \in \mathbb{R}^{N \times SF}$ sont répartis sur SF puces, où SF est le facteur d'étalement. Nous supposons que $N \geq SF$ utilisateurs transmettent simultanément vers la BS dans une trame de transmission. Le modèle d'activité de l'utilisateur utilise un ensemble $\mathbf{b} \in \{0, 1\}^N$, où $b = 1$ correspond à un utilisateur actif. Pour simplifier, nous considérons que le canal est parfait en supposant $\mathbf{H} = 1$, en plus de la présence d'un Bruit Blanc Additif Gaussien (AWGN) indiqué par $\mathbf{w} \in \mathbb{R}^{SF}$ suivant une distribution $\mathcal{N}(0, \sigma^2)$ pour chaque composante. Le modèle du système est le suivant:

$$\mathbf{y} = \mathbf{H}.\mathbf{b}.\mathbf{C} + \mathbf{w} \tag{7.1}$$

Le signal reçu $\mathbf{y} \in \mathbb{R}^{SF}$ est donc composé de trois variables; l'ensemble d'utilisateurs actifs ($\mathbf{b}$) et les messages codés $\mathbf{C}$ avec les bruits additifs ($\mathbf{w}$). Dans un but de comparaison, trois familles de codes sont utilisées, Unipolar, Bipolar, et Gaussien. Étant donné le signal reçu et l'ensemble des codes des utilisateurs, l'objectif est de retrouver quels sont les utilisateurs actifs $\mathbf{b} \in \{0, 1\}^N$. Le schéma complet est présenté dans la Fig. 7.1.

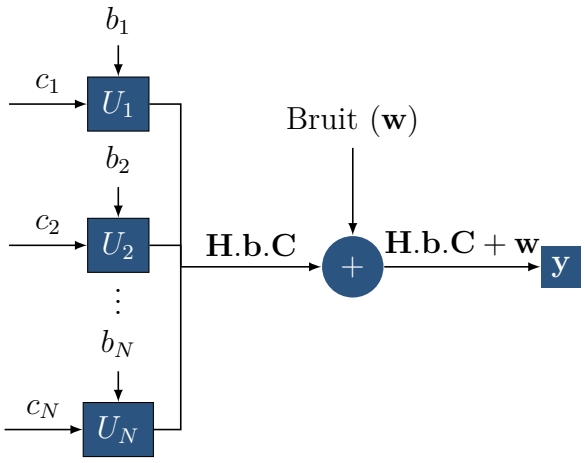


Figure 7.1: Modèle de système pour la Détection des l'utilisateurs Actifs (AUD) dans le contexte de NOMA

7.2.2 Méthodes classiques pour les problèmes d'AUD

Cette section fournit une explication détaillée de plusieurs méthodes classiques qui ont été proposées pour les problèmes d'AUD. Ces méthodes ont leurs propres avantages et inconvénients, notamment en termes de performances et de complexité. La section suivante plongera dans une explication approfondie de ces aspects.

Maximum de vraisemblance

Le récepteur de maximum de vraisemblance (ML) est la solution optimale pour l'AUD [18]. Ce détecteur identifie l'ensemble d'utilisateurs actifs le plus probable $\mathbf{b}$, compte tenu de la séquence reçue.

$$\{\widehat{b}_i\}_{i\in\{0,\cdots,N\}} = \underset{\{b_i\}_{i\in\{0,\cdots,N\}}}{\arg\min} \|\mathbf{y} - \mathbf{b.c}\|_2^2 \tag{7.2}$$

La solution du ML souffre d'une complexité de calcul élevée $\mathcal{O}(2^N)$, car elle repose sur une recherche exhaustive de toutes les possibilités existantes. En effet, la métrique de vraisemblance doit être calculée pour chaque ensemble d'activités potentiel.

Récepteur de corrélation classique (CCR)

Le CCR est classé comme une méthode sous-optimale [46] et promet de traiter le problème d'interférence multiple (MAI) [47]. L'équation du CCR s'explique comme suit :

$$\hat{b}_i = \begin{cases} 1 & \text{if } \mathbf{y} \cdot c_i \geq T \\ 0 & \text{otherwise} \end{cases} \tag{7.3}$$

où T est le seuil préalablement défini et i est un indice utilisateur.

Zero Forcing (ZF)

Le Zero Forcing (ZF) est classé comme un détecteur simple et efficace, ainsi qu'une méthode sous-optimale. Lorsque les séquences de codes $\mathbf{C}$ sont connues, nous pouvons observer l'estimation de $\hat{b}_{ZF}$ en multipliant les séquences de codes inverses de $\mathbf{C}$. Cependant, en raison du format matriciel rectangulaire de $\mathbf{C}$, nous devons utiliser la pseudo-inverse $C_C = (\mathbf{C}^T\mathbf{C})^{-1}\mathbf{C}^T$ [48].

$$\hat{b}_{ZF} = \mathbf{y}.\mathbf{C}_C \tag{7.4}$$

L'algorithme de Grover

L'algorithme de Grover est l'un des algorithmes quantiques qui a été démontré pour améliorer la recherche classique de $\mathcal{O}(N)$ à $\mathcal{O}(\sqrt{N})$. Cet algorithme se compose de deux variables importantes : 1.) Oracle ($\mathbf{O}$) et 2.) Diffuseur ($\mathbf{D}$). L'oracle est construit pour marquer les qubits en fournissant la signe négatif. D'autre part, le diffuseur ($\mathbf{D}$) vise à réamplifier les qubits marqués, après avoir été calculés par l'oracle ($\mathbf{O}$). Avant de calculer l'algorithme de Grover, la structure doit être calculée avec la porte de Hadamard (porte H) pour obtenir une superposition d'états.

Ainsi, le schéma de Grover est structuré comme le montre la Fig. 7.2. La première partie consiste à développer $|\psi\rangle$ après avoir calculé:

$$|\psi\rangle = \frac{1}{\sqrt{K}} \sum_{x=1}^{K} |x\rangle \tag{7.5}$$

où x correspond à l'indice du qubit, avec $x \in \mathbb{B}^N$. Ensuite, l'opération $\mathbf{O}$ sélectionne les qubits en effectuant le calcul dans la superposition d'états, comme indiqué ci-dessous:

$$\mathbf{O}|x\rangle = \begin{cases} |x\rangle & f(x) = \delta \\ -|x\rangle & \text{otherwise} \end{cases} \tag{7.6}$$

L'opération $\mathbf{O}$ doit être exécutée avec la valeur souhaitée δ, c'est-à-dire $f(x) = \delta$, en tenant compte du fait que $\delta \in \mathbb{C}^+$, où δ représente la valeur souhaitée. En effet, ce

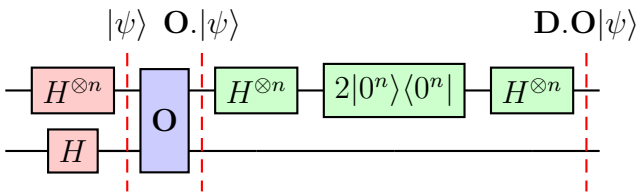


Figure 7.2: Grover's Scheme

résultat doit être amplifié par **D**, car il traite du déphaseur conditionnel $|\psi\rangle\langle\psi|$ avec l'équation suivante:

$$\mathbf{D} = H^{\otimes N}(2|0^N\rangle\langle 0^N| - I)H^{\otimes N} = 2|\psi\rangle\langle\psi| - I \tag{7.7}$$

Les opérations de **O** et **D** sont itérées L_{opt} fois, bien moins que dans le cas classique. Dans ce cas là, L_{opt} est defini par le suivant:

$$L_{opt} = \lfloor \frac{\pi}{4}\sqrt{\frac{K}{S}} \rfloor \tag{7.8}$$

Et pour trouver la probabilité de succès P_G, nous pouvons la définir comme suit:

$$P_G = \sin^2((2j+1)\theta) \tag{7.9}$$

où j est le nombre d'iterations et $\theta = \arcsin\left(\sqrt{\frac{S}{K}}\right)$.

Nombre de Solutions inconnu par Grover

Indépendamment de la méthode de recherche, le nombre total de solutions S est souvent inconnu, ce qui rend difficile la recherche de L_{opt}. Boyer, Brassard, Høyer et Tapp ont proposé une méthode appelée BBHT pour trouver certaines solutions sans nécessiter de connaissances préalables [59]. Cela conduit à une limite supérieure de recherche de $4.5\sqrt{K}$. L'idée de l'algorithme BBHT est de procéder par itérations, le nombre d'itérations étant basé sur des progressions géométriques. D'autre part, il est possible de trouver la solution minimale lorsque le nombre de solutions de la base de données est inconnu, ce qui est abordé par l'algorithme Durr-Hoyer (DHA). Pour ce faire, cet algorithme nécessite une limite supérieure de $22.5\sqrt{K}$ pour trouver le minimum de la recherche dans la base de données.

7.2.3 Conclusion

Ce chapitre a discuté du modèle de système de l'AUD, ainsi que des types de codes utilisés (c'est-à-dire Unipolar, Bipolar et Random Gaussian) et de leurs motivations.

Nous avons également abordé les approches conventionnelles pour résoudre le problème de l'AUD, allant des plus efficaces (comme le ML) aux méthodes moins efficaces (à savoir, le CCR et le ZF). De plus, nous avons discuté d'une comparaison des algorithmes de recherche classiques en termes de recherche de valeur et de leur complexité.

De plus, nous avons introduit l'algorithme quantique comme une nouvelle solution basée sur la superposition d'états, qui promet de réduire la complexité. L'un des algorithmes connus pour gérer la complexité de la base de données est l'algorithme de Grover. Nous avons discuté de l'algorithme de Grover et de son comportement, notamment sa probabilité de succès et sa complexité. Nous avons également exploré comment fonctionne l'algorithme de Grover lorsqu'il n'y a pas de solution connue dans la base de données et comment il peut être utilisé pour trouver le minimum lorsque la solution est inconnue.

En conclusion, nous constatons que l'algorithme de Grover est une approche prometteuse pour résoudre le problème de l'AUD, offrant à la fois des performances élevées et une faible complexité. Nous approfondirons davantage ce sujet dans le chapitre suivant.

7.3 En adaptant l'algorithme de Grover pour AUD

7.3.1 Introduction

Le nombre croissant d'utilisateurs connectés au réseau mobile a entraîné de nombreux défis en matière d'utilisation efficace des ressources disponibles. Cela a mis en évidence dans le problème Détection des l'utilisateurs Actifs (AUD), où l'approche actuelle exige une complexité importante, en particulier impliquant Maximum de Vraisemblance (ML). Alors que d'autres méthodes établies comme Récepteur de Corrélation Conventionnel (CCR), Zéro forcing (ZF), Annulation Successive des Interférences (SIC), Annulation des Interférences en Parallèle (PIC), promettent de réduire cette complexité, mais elles se traduisent souvent par des performances sous-optimales. Par conséquent, dans ce chapitre, nous étudions l'application de l'algorithme de Grover, une approche quantique, pour traiter ces deux aspects: Complexité et performance.

Les performances de l'algorithme de Grover doivent être similaires à celles de ML tout en conservant une complexité aussi simple que possible. Le principe de ML est d'identifier l'ensemble d'utilisateurs actifs le plus probable sur la base des données de l'utilisateur. L'algorithme de Grover propose d'y parvenir en appliquant le même principe. Néanmoins, l'application de l'informatique quantique basée sur le même principe que ML n'est pas une solution simple, car aucun algorithme ne peut être utilisé directement pour ce problème. C'est pourquoi nous n'avançons pas vers cet objectif. Dans ce chapitre, nous présentons la première étape où nous adaptons l'algorithme de Grover à un cas spécifique du problème ML. En effet, l'algorithme de Grover est conçu pour rechercher x tel que $f(x) = \delta$ avec une fonction prédéfinie f et δ.

Ce chapitre fournit une description complète et détaillée d'un simple algorithme de Grover pour AUD dans le but de résoudre l'équation $f(x) = \delta$. Nous expliquerons et démontrerons en détail la construction du circuit de Grover, en nous concentrant sur un cas spécifique, et nous discuterons de la façon d'adapter l'algorithme pour AUD en utilisant diverses familles de codes.

L'objectif principal de ce chapitre est d'examiner les performances et la complexité de l'algorithme de Grover, en nous appuyant sur nos discussions précédentes. Nous effectuons une analyse comparative entre l'algorithme de Grover et d'autres méthodes classiques telles que ML, CCR, et ZF dans des cas avec bruit et sans bruit. Grâce à cette analyse, nous évaluerons les performances et la complexité de l'algorithme par rapport à ces méthodes classiques.

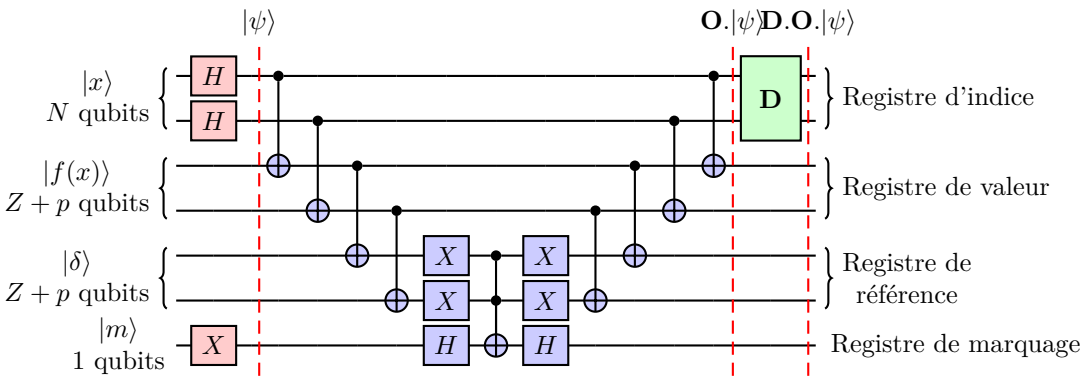


Figure 7.3: Circuit de Grover $n = 2$ qubits $f(x) = \delta$

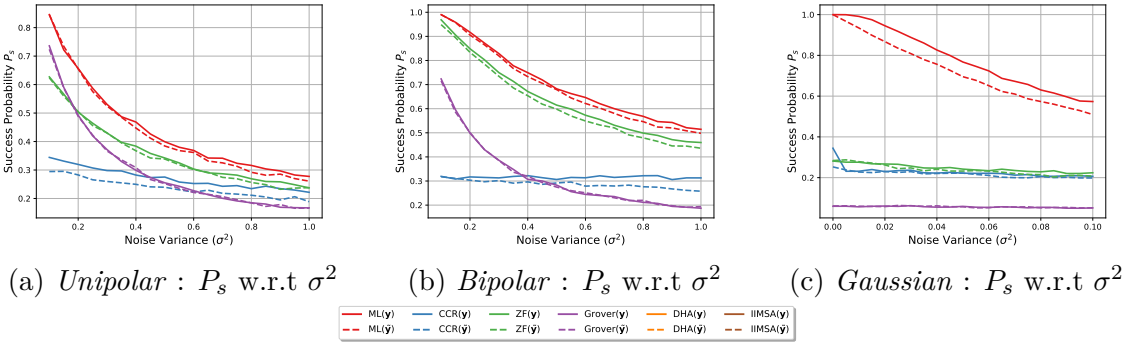
7.3.2 Développement du circuit de Grover

Cette section décrit comment adapter le circuit de Grover au cas de l'AUD. Grover s'appuie sur un oracle **O**, un diffuseur **D** et une porte de Hadamard pour créer une superposition d'états, comme illustré à la Fig 7.3. Grover se compose de quatre registres [82]:

- Registre d'indice : contient l'argument de la fonction $f(x)$ qui fournit les résultats ciblés.
- Registre de valeur : contient la valeur de la fonction $f(x)$.
- Registre de référence : correspond à la valeur ciblée $|\delta\rangle$.
- Registre de marquage : contient le signe négatif afin de marquer les qubits.

Un exemple du circuit de Grover complet est présenté à la Fig. 7.3, où $N = 2$ est le nombre de qubits dans l'espace de Hilbert, permettant quatre états de base computationnels différents $|00\rangle, |01\rangle, |10\rangle$ et $|11\rangle$.

Le nombre de qubits pour les registres de valeur et de référence est de $Z + p$ qubits, ce qui correspond à la quantité de qubits nécessaires pour stocker le résultat de la fonction $|f(x)\rangle$. Enfin, le registre de marquage occupe 1 qubit pour effectuer l'inversion du signe. Dans la Fig. 7.3, un circuit simple est présenté où $|x\rangle = |\delta\rangle$, tout est fourni par la valeur ciblée δ correspondant à l'indice du qubit $|x\rangle$. Tous les composants des qubits dans le circuit de Grover fonctionnent avec une représentation binaire; ainsi, le nombre entier est converti en binaire comme décrit dans la section suivante.



(a) *Unipolar* : P_s w.r.t σ^2 (b) *Bipolar* : P_s w.r.t σ^2 (c) *Gaussian* : P_s w.r.t σ^2

Figure 7.4: AUD performance with classical method and Grover's algorithm $f(x) = \delta$

Performances

La Fig. 7.4 présente une comparaison des performances des méthodes classiques, à savoir ML, ZF, CCR, par rapport à l'algorithme de Grover en fonction de la variance du bruit (σ^2) dans des scénarios bruités. Il est important de souligner que l'algorithme ML surpasse les autres méthodes, y compris l'algorithme de Grover. Notre observation révèle que l'algorithme de Grover donne des résultats prometteurs uniquement lorsque la variance du bruit est faible. Plus précisément, dans le cas unipolaire, il peut surpasser toutes les méthodes classiques, à l'exception de ML. En revanche, cet algorithme ne peut pas surpasser les performances de ZF dans le cas bipolaire pour tous les niveaux de variance du bruit. Cependant, dans le cas gaussien, l'algorithme de Grover semble produire des erreurs pour toutes les variances de bruit. Il est à noter que l'algorithme de Grover n'est pas adapté au cas gaussien en raison d'une faible distance entre chaque composante.

D'autre part, dans le cas unipolaire avec une variance de bruit de $\sigma^2 = 0.2$, l'algorithme ZF a la capacité de surpasser l'algorithme de Grover, devenant ainsi la deuxième meilleure option après ML dans tous les cas, qu'il s'agisse du scénario unipolaire, bipolaire ou gaussien. En contraste, l'algorithme CCR affiche généralement des performances inférieures par rapport aux autres méthodes. Ainsi, dans le contexte unipolaire avec une variance de bruit de $\sigma^2 = 0.5$, l'algorithme de Grover devient moins performant que CCR. Cette tendance se maintient également dans le cas bipolaire, où le CCR dépasse les performances de l'algorithme de Grover au même niveau de variance (σ^2).

Ce phénomène découle du fait que le code gaussien présente une faible séparation entre ses composantes, rendant l'algorithme de Grover inefficace pour la détection appropriée des utilisateurs. Nous concluons que l'algorithme de Grover ne semble pas prometteur dans ce cas, où $f(x) = \delta$ est mis en œuvre. Nous devrions modifier l'oracle

pour améliorer les performances.

7.3.3 Conclusion

Comme nous l'avons observé, l'algorithme original de Grover n'est pas prometteur en termes de performances. Le moteur de recherche de l'algorithme de Grover nécessite une entrée précise $f(x) = \delta$, si l'entrée est erronée, le moteur de recherche conduit à une recherche erronée. L'algorithme de Grover proposé n'est donc pas comparable aux autres méthodes classiques.

L'algorithme de Grover est donc prometteur, mais il n'est pas complètement adapté à notre problème. Nous proposons donc de le modifier en appliquant l'algorithme de la distance minimale. Comme indiqué dans 7.2, l'algorithme de Grover modifié proposé doit respecter la distance minimale entre $\mathbf{y}$ et $\mathbf{b}. \cdot \mathbf{C}$. La section suivante traite plus en détail de la distance minimale entre $\mathbf{y}$ et $\mathbf{b}.\mathbf{C}$, dans l'espoir d'augmenter le nombre d'itérations de Grover, ce qui conduit à une complexité accrue. Cependant, notre objectif est d'augmenter la performance de Grover P_s. D'autres aperçus sur cet aspect sont fournis dans la section suivante. La section suivante a donc pour objectif de répondre à ce besoin.

7.4 Adaptation de l'algorithme de Grover pour trouver le minimum

7.4.1 Introduction

Après le chapitre 7.3, où nous avons considéré le cas le plus simple, nous proposons dans ce chapitre une version modifiée de l'algorithme de Grover qui vise à appliquer les mêmes principes que ML. Bien qu'elle puisse nécessiter un degré de complexité important, cette version de l'algorithme de Grover est la plus simple et la plus efficace, ML est prometteur en termes de performances. Ce chapitre étudie comment l'algorithme de Grover peut atteindre des performances comparables à celles de ML, tout en restant simple.

Tout d'abord, nous fournissons une explication et une démonstration de la construction de l'algorithme de Grover. En mettant l'accent sur un cas particulier. Nous expliquons également comment adapter l'algorithme pour AUD en utilisant différentes familles de codes. Il est essentiel de modifier l'oracle de l'algorithme de Grover $\mathbf{O}$, afin de trouver la distance minimale en appliquant $f(x) < \delta$. Ensuite, nous appliquons l'algorithme complet ML avec une *approche quantique* et comparons les résultats en fonction de la variance σ^2.

En fait, l'application de la condition de ML avec la recherche du minimum présente un défi lorsque le nombre de solutions, noté S, est inconnu. Cette approche a été proposée par Boyer-Brassard-Høyer-Tapp (BBHT) et Algorithme Durr-Hoyer (DHA). Par exemple, BBHT possède une limite supérieure de $4.5\sqrt{K}$ lorsque le nombre de solutions est inconnu dans la base de données, tandis que DHA possède une borne supérieure de $22.5\sqrt{K}$ pour trouver la solution minimale lorsque le nombre de solutions est inconnu. Il est important de noter que ces bornes supérieures sont toujours inférieures au calcul classique $\mathcal{O}(K)$. Cependant, BBHT et DHA soulèvent une question de recherche ouverte qui nécessite des améliorations en termes de complexité et de méthodes.

La solution que nous proposons, à savoir Algorithme Amélioré de Recherche de Minimum par Itération (IIMSA), vise donc à améliorer l'algorithme DHA afin d'améliorer ses performances. Tandis que DHA calcule les valeurs minimales à l'aide de l'itération de Grover, qui suit une progression géométrique pour les solutions inconnues, IIMSA propose un autre algorithme. Cet algorithme sélectionne un nombre de solutions estimé appelé $\hat{S}$, sur la base d'un $\hat{\delta}$ aléatoire.

En plus de IIMSA et de DHA, nous intégrons des méthodes classiques telles que ZF et CCR dans IIMSA et DHA pour atteindre une vitesse plus rapide. Par conséquent, nous comparons les performances et la complexité de IIMSA et DHA pour des méthodes classiques. Cette intégration est réalisée en déterminant un seuil pertinent, dénoté par δ inspiré de [72], afin d'améliorer la performance existante. Notre objectif principal dans ce chapitre est donc d'évaluer la performance, notée P_s, et la complexité, notée nb_{it}, de IIMSA et de DHA lorsqu'elles sont intégrées aux méthodes classiques (c'est-à-dire ZF et DHA).

7.4.2 L'algorithme d'IIMSA

Nous introduisons un algorithme connu sous le nom d'Algorithme Amélioré de Recherche de Minimum par Itération (IIMSA). L'idée principale derrière IIMSA est d'exploiter la connaissance a priori des systèmes pour évaluer le nombre de solutions à chaque étape, dénommé $\hat{S}$.

Au lieu d'employer des itérations aléatoires, comme suggéré par le Algorithme Durr-Hoyer (DHA), notre approche consiste à trouver $\hat{S}$ à partir de δ. Cette variable introduit de l'incertitude, entraînant un nombre d'itérations imprévisible. Malgré cette imprécision inhérente, nous estimons l'ensemble des utilisateurs actifs en utilisant l'algorithme de Grover. L'algorithme proposé est donné comme suit Algo. 6:

Tout d'abord, nous sélectionnons aléatoirement un indice i dans une plage uniforme de valeurs entre 0 et $K-1$, où K est la taille de la base de données. En conséquence, $\hat{\delta}$ est initialisé avec un indice i choisi au hasard et uniformément distribué. Ensuite, nous évaluons le nombre de solutions $\hat{S}$, c'est-à-dire le nombre d'ensembles dont la distance

Algorithm 6: L'algorithme d'IIMSA

Input : $\mathbf{C}$, K, L_{IIMSA}, $\hat{\delta}$
Output : δ_x, $\mathbf{b}$

$i \leftarrow$ choose $(0, K-1)$uniformly ;
Choose $\hat{\delta}(i) \leftarrow$ corresponds to i ;
$\hat{S} \leftarrow \|\mathbf{y} - \mathbf{b} \cdot \mathbf{C}\|_2^2 \leq \hat{\delta}$;
$L \leftarrow 1$;
while $\hat{S} \neq 0$ *or* $L \leq L_{IIMSA}$ **do**
    $L_{opt} = \lfloor \frac{\pi}{4} \sqrt{\frac{K}{S}} \rfloor$;
    $\mathbf{b} \leftarrow \mathcal{G}(L_{\text{opt}})$;
    $\delta_x \leftarrow \|\mathbf{y} - \mathbf{b} \cdot \mathbf{C}\|_2^2$;
    $\hat{S} \leftarrow \|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2 \leq \delta_x$;
    $L \leftarrow L + L_{\text{opt}}$;
    if $\delta_x < \hat{\delta}$ **then**
        $\hat{\delta} \leftarrow \delta_x$;
    end
end

est inférieure à la valeur actuelle de $\hat{\delta}$ grâce à une analyse statistique du système. Si $\hat{S} = 0$, cela signifie que la valeur actuelle de $\hat{\delta}$ conduit à une distance minimale. Sinon, l'algorithme de Grover $\mathcal{G}$, qui cherche x tel que $f(x) < \hat{\delta}$, est exécuté pour rechercher une distance inférieure. La sortie de Grover génère un nouvel ensemble, ce qui permet de trouver la nouvelle valeur de δ_x et le nombre de solutions $\hat{S}$. Si cet ensemble a une distance δ_x inférieure à $\hat{\delta}$, nous itérons en relançant $\mathcal{G}$ avec la valeur de $\hat{\delta}$ mise à jour par la valeur de δ_x. Nous obtenons ainsi un ensemble de solutions plus restreint pour cette nouvelle itération de $\mathcal{G}$. Notons que L est mesuré lorsque l'algorithme de Grover est exécuté. Cette variable L deviendra la principale variable affectant les performances. Ce principe est appliqué jusqu'à ce que nous obtenions $S = 0$.

Pour chaque appel à Grover, l'algorithme exécute l'oracle modifié $L_{opt} = \lfloor \frac{\pi}{4} \sqrt{\frac{2^N}{\hat{S}}} \rfloor$ fois pour trouver une distance inférieure. Cependant, il est important de noter que si le nombre de solutions est plus grand que la moitié de la taille de la base de données, alors les cas non souhaités sont amplifiés, poussant la recherche dans la mauvaise direction. Ainsi, pour identifier et réduire l'impact d'une telle situation, nous limitons le nombre de tentatives infructueuses à L_{IIMSA}.

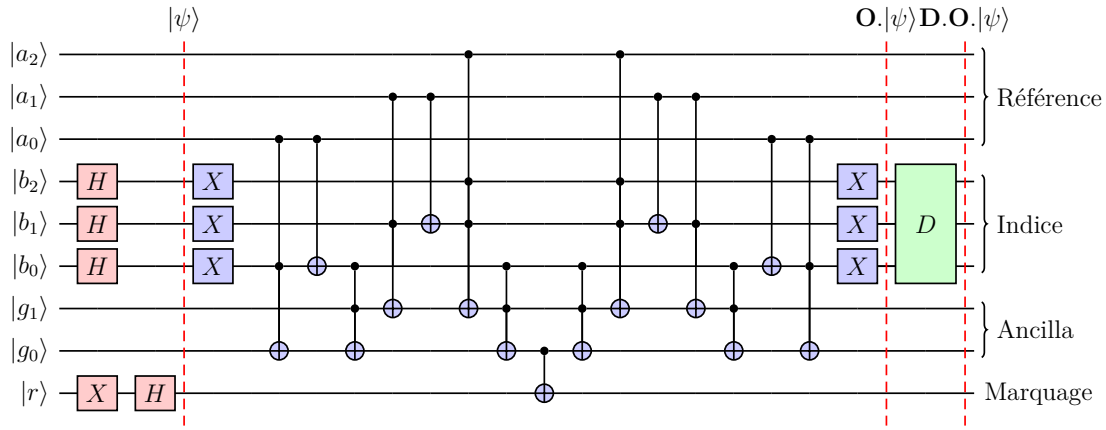


Figure 7.5: Circuit de Grover pour $n = 3$ qubits $f(x) < \delta$

Liste des variables importantes :

- $\hat{\delta}$ en tant que seuil pour trouver la distance actuelle
- $\hat{S}$ les solutions estimées données par un δ aléatoire
- L_{IIMSA} la limite supérieure de l'algorithme
- δ_x un nouveau seuil δ pour trouver la distance actuelle
- L une variable pour mesurer le nombre d'exécutions de Grover

En effet, l'exécution de l'algorithme IIMSA nécessite une modification de l'Oracle ($\mathbf{O}$) qui respecte la condition $f(x) < \delta$. De plus, la mise en œuvre de la recherche de $\arg\min \|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2$ nécessite une nouvelle modification du circuit de Grover. Par conséquent, la sous-section suivante décrit l'Oracle modifié ainsi que le processus de recherche du minimum.

7.4.3 Circuit de Grover : Oracle Modifié

Lors de la recherche du minimum dans une base de données, il est important de modifier d'abord l'oracle qui satisfait $f(x) < \delta$. Par conséquent, un nouveau circuit est proposé comme illustré dans la Fig. 7.5.

Ainsi, supposons que nous ayons un circuit de Grover composé de qubits $|a\rangle$ et $|b\rangle$. Dans le contexte de notre problème, $f(x) = |b\rangle$ et $\delta = |a\rangle$. L'idée principale

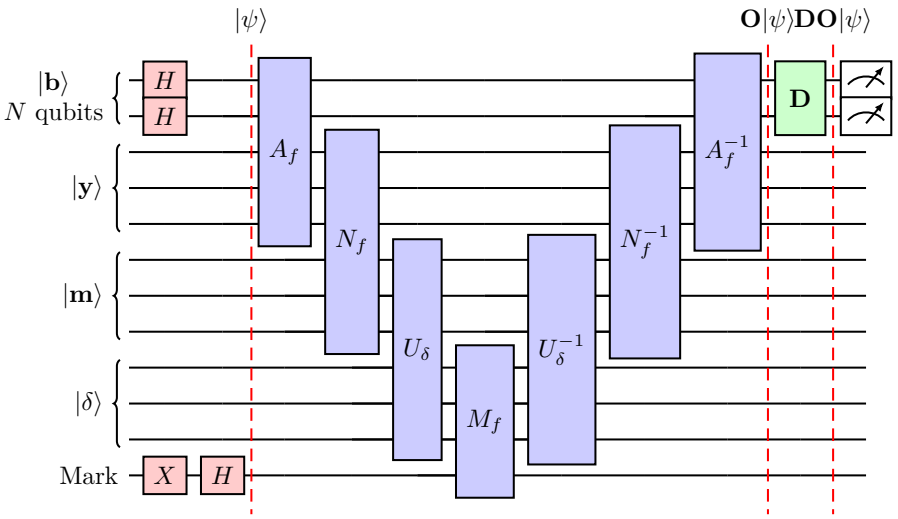


Figure 7.6: Quantum Circuit of $\|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2 < \delta$

de ce circuit est de réaliser la soustraction de $r = a - b$ [92] avec un complément b' qui retourne $r = a + b'$. Pour ce faire, le complément de b' est calculé à l'aide de la porte *X-gate*, comme illustré dans la Fig. 7.5. Le qubit supplémentaire, désigné par g, est utilisé pour calculer $a + b'$ et est appelé qubit de retenue. En fin de compte, il contribue aux qubits r après la retenue. Le circuit est composé de $N = 3$ qubits, ce qui correspond à la longueur binaire utilisée, où a_0 et b_0 correspondent au bit de poids faible. Ensuite, une fois que $r = a + b'$ est calculé, le qubit r agit comme une retenue, avec la condition suivante :

$$r = \begin{cases} 1 & a > b \\ 0 & \text{otherwise} \end{cases} \tag{7.10}$$

Ensuite, r est multiplié par $|-\rangle$ dans le *registre de marquage* pour fournir le signe négatif à la ou les solutions. Ce circuit fonctionne donc bien lorsque $a > b$ est implicite. Ce circuit repose sur quatre registres : 1.) *Registre d'indice* 2.) *Registre de référence* 3.) *Registre auxiliaire* et 4.) *Registre de marquage*. Le *registre d'indice* contient l'argument de la fonction $f(x)$ tandis que le *registre de référence* contient la fonction δ. Le *registre auxiliaire* aide à effectuer les opérations sur les *registres d'indice* et de *référence*, afin de transmettre les qubits au *registre de marquage*. Ensuite, le dernier registre, le *registre de marquage*, effectue le calcul négatif dans le circuit.

Circuit de Grover : Recherche du minimum

Ce nouveau circuit de Grover étend la fonctionnalité de $f(x) < \delta$. Il est conçu pour effectuer une tâche d'optimisation où il cherche à trouver le minimum $\arg\min \|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2 < \delta$ sur le circuit quantique. Globalement, le circuit de Grover complet est illustré dans la Fig. 7.6. Il se compose de quatre principales variables, à savoir :

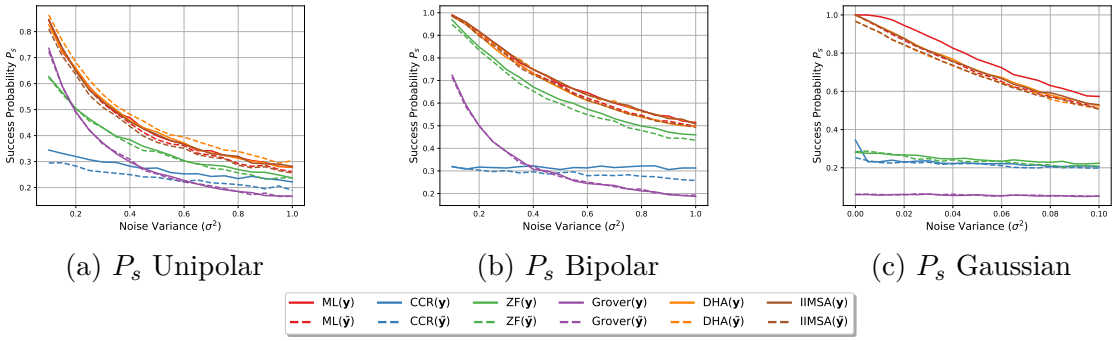
1. $|\mathbf{b}\rangle \in \{0,1\}^N$ en tant qu'ensemble de qubits d'utilisateurs actifs
2. $|\mathbf{y}\rangle \in \mathbb{R}^{SF}$ en tant que qubits de signal reçu
3. $|\mathbf{m}\rangle \in \mathbb{R}$ en tant que qubits de multiplication
4. $|\delta\rangle \in \mathbb{R}$ en tant que qubits de seuil

Tout d'abord, la valeur cible principale, désignée par $|\mathbf{b}\rangle$, est le point central de ce circuit qui est mesuré à la fin de ce circuit. En revanche, $|\mathbf{y}\rangle$ représente le signal observé qui est introduit dans l'algorithme de Grover, jouant un rôle crucial dans le calcul de la distance minimale. Le paramètre $|\delta\rangle$ sert de point de référence pour déterminer la distance minimale et est également inclus dans le circuit. Il est important de noter que ce circuit prend à la fois $|\mathbf{y}\rangle$ et $|\delta\rangle$ en tant qu'entrées pour calculer la distance minimale, ce qui est différent de la Fig. 7.5. Le qubit $|\mathbf{m}\rangle$ sert de registre de stockage temporaire qui transporte le résultat du calcul de la distance minimale.

Nous introduisons également l'Oracle ($\mathbf{O}$), qui se compose de quatre composants clés, pour faciliter l'exécution de cette fonction, comme décrit ci-dessous :

- A_f : signifie *fonction d'addition*, elle calcule $\mathbf{y} - \mathbf{b}.\mathbf{C}$
- N_f : signifie *fonction de norme*, elle calcule la norme $\|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2$
- U_δ : est la partie de l'oracle, identifiant les états où la norme est inférieure à $f(b) < \delta$
- M_f : marque les états précédemment identifiés

Ces blocs sont suivis d'un diffuseur ($\mathbf{D}$) et sont ensuite répétés pour amplifier les solutions souhaitées.



(a) P_s Unipolar (b) P_s Bipolar (c) P_s Gaussian

Figure 7.7: P_s des méthodes classiques (c'est-à-dire ZF, CCR, ML) et de l'algorithme de Grover avec IIMSA

IIMSA contre Algorithme Mixte (ZF, CCR et ML)

Comme expliqué dans la section 7.3, l'algorithme de Grover n'a pas encore atteint des performances optimales pour résoudre le problème de l'AUD, contrairement aux méthodes classiques discutées dans le même chapitre. Par conséquent, cette sous-section vise à réévaluer ses performances par rapport aux méthodes classiques. Le contexte de l'algorithme de Grover est modifié pour exécuter $f(x) < \delta$, ce qui permet d'identifier la distance minimale de $\arg\min ||\mathbf{y} - \mathbf{b} \cdot \mathbf{C}||_2^2$, comme le propose notre nouvel algorithme IIMSA.

Tout d'abord, comparons notre algorithme proposé, IIMSA, avec ML, CCR et ZF. Nous avons simulé 10.000 réalisations avec une précision de $p = 2$ pour obtenir le signal observé $\tilde{y}$ et les types de codes avec la configuration suivante :

- Modèle unipolaire : $N = 4$ et SF$= 3$
- Modèle bipolaire : $N = 3$ et SF$= 3$
- Modèle gaussien aléatoire : $N = 5$ et SF$= 3$

Nous comparons l'utilisation des méthodes classiques avec IIMSA, où la configuration de SF est fixée à 3 pour tous les types de codes, et L_{IIMSA} et L_{DHA} sont configurés à $22.5\sqrt{2^N}$. Le résultat est présenté dans la Fig. 4.7, qui présente une comparaison entre les performances des algorithmes classiques et quantiques, ainsi que l'intégration de IIMSA, dans les scénarios unipolaires, bipolaires et gaussiens. Les résultats montrent que notre algorithme IIMSA proposé est comparable aux techniques ML, appliquées à tous les types de codes, bien que IIMSA ait un P_s plus faible par rapport à ML. Cette observation souligne les avantages significatifs de l'algorithme IIMSA par rapport à l'algorithme de Grover, car notre approche vise à localiser

l'algorithme minimum en appliquant $\arg\min ||\mathbf{y} - \mathbf{b} \cdot \mathbf{C}||_2^2$. Il démontre également une solution très prometteuse en termes de performances par rapport aux méthodes classiques (c'est-à-dire CCR, ZF) pour tous les types de codes (unipolaire, bipolaire et gaussien). Nous comparons également le cas où la précision est $p = 2$ (indiqué par $\tilde{y}$) et le cas sans précision (indiqué par y). Cela montre un comportement similaire. Il montre que $\tilde{y}$ a une probabilité de succès plus faible en raison de la fonction d'arrondi, qui s'applique à tous les types de codes. En effet, lorsque le signal quantifié $\tilde{y}$ est utilisé, nous perdons les informations contenues dans la partie supprimée. Cependant, cette opération est nécessaire comme expliqué dans la section 3.2.1.

Cette section conclut que IIMSA est une solution prometteuse en termes de performances, bien supérieure aux autres méthodes classiques. La sous-section suivante se penche sur les capacités de l'IIMSA à relever des défis au-delà de ceux abordés par le DHA, explorant comment notre algorithme peut réduire la complexité du DHA tout en améliorant ses performances. De plus, nous les incorporons également avec les méthodes classiques (c'est-à-dire CCR, ZF), ce qui peut être prometteur pour augmenter la probabilité de succès P_s.

7.4.4 L'analyse de Lmax pour à la fois IIMSA et DHA

Cette section se concentre sur l'examen de l'influence de l'analyse du nombre d'itérations noté par $L \in \{1, \cdots, L_{max}\}$, où $L_{max} = 22.5\sqrt{2^N}$. Cette analyse est réalisée pour tous les types de codes et pour une variance de bruit $\sigma = 0.1$. Les courbes basées sur le DHA sont tracées en rouge, et celles de l'IIMSA en bleu.

Tout d'abord, nous pouvons observer dans la Fig. 7.8 que lorsque L augmente, P_s augmente également, mais nb_{it} augmente aussi. Cela est dû au fait que, en permettant davantage d'essais au sein des algorithmes, il est plus probable de trouver la solution, mais au prix de davantage d'itérations en moyenne.

Deuxièmement, nous pouvons observer dans la probabilité de succès (P_s) de l'IIMSA dépasse celle de le DHA, lorsqu'ils sont tous deux utilisés dans la version d'origine, mais aussi lorsqu'ils sont améliorés avec CCR ou ZF. Cela est dû au fait qu'IIMSA exploite l'estimation du nombre de solutions à chaque étape pour être plus efficace dans la recherche. De plus, ZF-IIMSA surpasse tous les autres algorithmes. Cette tendance peut être observée pour tous les types de codes.

D'autre part, nous observons une tendance de performance distincte concernant nb_{it}. Dans la Fig.7.8d à la Fig.7.8f, il peut être observé que le DHA avec l'algorithme classique supplémentaire (ZF et CCR) surpasse l'IIMSA, en particulier lorsque L est faible. Cela est dû au fait qu'avec IIMSA, l'algorithme commence avec un nombre plus élevé d'itérations défini par L_{opt}, tandis que le DHA commence avec une valeur aléatoire prise dans un intervalle $L \in \{0, \cdots, \lfloor m \rfloor\}$ comme expliqué dans Algo. 2, avec m augmentant progressivement à partir de 1. Comme la boucle *while* s'arrête

lorsque le nombre d'itérations a dépassé le niveau, le DHA dépasse cette limite plus tôt que l'IIMSA. Cependant, ce comportement disparaît lorsque L augmente. En effet, dans ce cas, la boucle *while* a plus de chances de s'arrêter car le minimum a été trouvé. Ainsi, le comportement précédent à petite échelle ne prédomine plus. Ce schéma est valable pour tous les algorithmes classiques mixtes (ZF et DHA).

De plus, il est important de noter que parmi tous les types de codes, le code bipolaire présente une probabilité de succès (P_s) élevée par rapport aux autres. Plus précisément, pour de petits $L_{max} \in \{7, \cdots, 10\}$, certaines méthodes atteignent $P_s = 1$, ce qui dépasse significativement les performances de l'unipolaire, où seule une méthode atteint ce niveau dans cette plage. En revanche, le gaussien n'atteint pas $P_s = 1$. Cette différence peut être attribuée au fait que le type de code bipolaire a une distance euclidienne plus élevée $\mathbf{C} \in \{-1, 1\}$, ce qui permet des détections plus précises et une moindre susceptibilité à la contamination par le bruit. Cela s'applique également au nombre d'itérations de Grover requis (nb_{it}), où le bipolaire nécessite moins de nb_{it} par rapport aux autres types de codes. Cela signifie que le bipolaire est plus rapide pour détecter des détections précises. Ceci est logique, car étant moins vulnérable au bruit, l'algorithme peut détecter plus facilement les cibles. Le nombre maximum de nb_{it} atteint par le bipolaire est de 18, tandis que l'unipolaire et le gaussien atteignent respectivement 30 et 25.

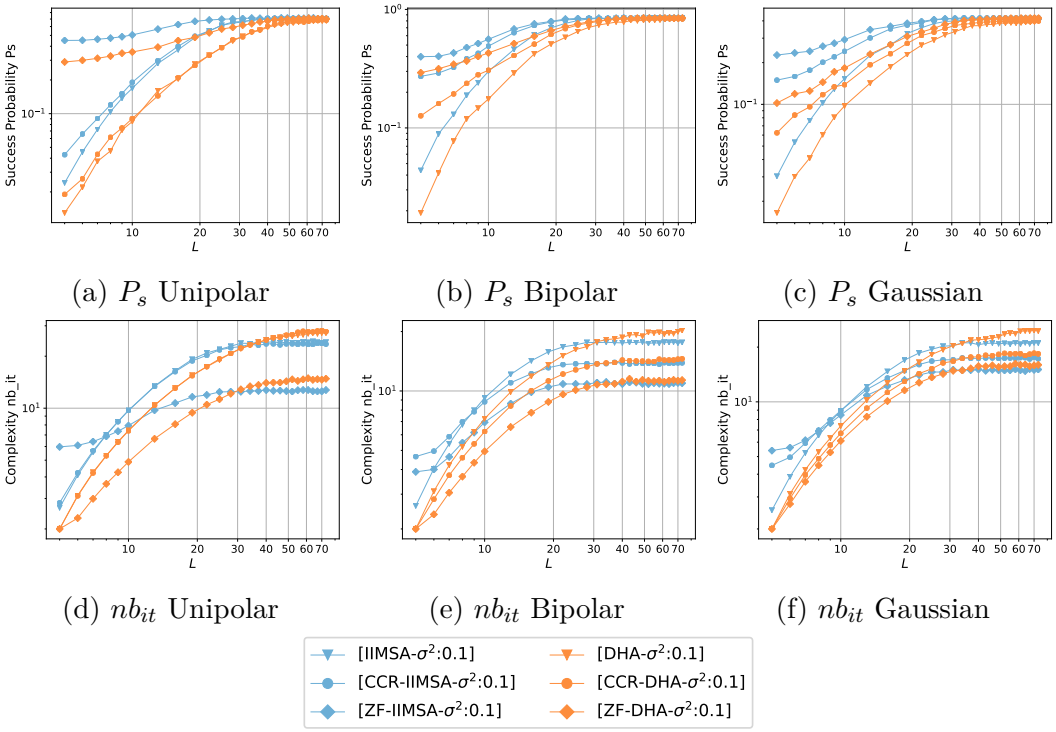
Bien que le CCR semble avoir du mal à rivaliser avec le ZF, il présente une probabilité de succès (P_s) plus élevée par rapport à l'algorithme original. Cela indique que le CCR contribue positivement aux calculs, conduisant à un faible nombre d'itérations (nb_{it}) nécessaires pour des détections précises. Par conséquent, le CCR se comporte bien et surpasse le DHA original et l'IIMSA.

De plus, il est important de souligner l'impact significatif de l'algorithme classique (ZF et CCR) dans ces résultats. Ces algorithmes améliorent notablement à la fois la probabilité de succès (P_s) et le nombre d'itérations (nb_{it}). Plus précisément, pour $L > 20$, les résultats montrent que ZF-IIMSA présente des performances similaires, mais avec un nb_{it} plus faible par rapport à d'autres méthodes. Suit de près ZF-DHA, qui a également un impact considérable sur nb_{it}. Ainsi, nous pouvons conclure que ZF sert d'excellent moyen pour fournir un ensemble d'initialisation précis pour les algorithmes quantiques de recherche du minimum.

Pour conclure, ZF (et CCR dans une moindre mesure) est une méthode classique efficace, qui permet, lorsqu'elle est combinée avec des algorithmes quantiques, d'atteindre moins d'itérations de Grover.

7.4.5 Conclusion

Nous avons conçu le circuit quantique de Grover qui permet d'avoir $f(x) < \delta$ et aussi l'implémentation pour trouver le minimum $\arg\min \|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2$. Nous avons évalué



(a) P_s Unipolar (b) P_s Bipolar (c) P_s Gaussian

(d) nb_{it} Unipolar (e) nb_{it} Bipolar (f) nb_{it} Gaussian

Figure 7.8: P_s et nb_{it} par rapport à L

l'algorithme proposé IIMSA pour améliorer la méthode existante DHA, avec également l'intégration de méthodes classiques (c'est-à-dire CCR et ZF) ce qui permet d'accroître les performances de DHA et de IIMSA.

Il a été démontré que l'algorithme que nous proposons, IIMSA, est plus performant que DHA et IIMSA. DHA, ce qui se traduit par une complexité réduite et des performances supérieures. En outre, son intégration aux méthodes classiques est considérée comme efficace, surtout lorsqu'elle est combinée avec ZF, car elle permet une détection plus précise avec une complexité minimale. La combinaison la plus efficace est obtenue lorsque l'algorithme est intégré à ZF, appelé ZF-IIMSA, qui offre des performances supérieures avec une faible complexité.

Nous observons que IIMSA atteint une complexité de moins que DHA, ce qui est nettement mieux que DHA, dont la complexité est de $22.5\sqrt{2^N}$. Les travaux futurs consisteront à améliorer IIMSA, en vérifiant notamment si $\hat{S} < \frac{K}{2}$, sinon, l'algorithme algorithme peut trouver un nouvel indice i. Cela s'explique principalement par le fait que notre algorithme IIMSA peut s'exécuter lorsque $\hat{S}$ qui satisfont toutes les conditions, ce qui est n'est pas précis en raison de la solution indésirable $\hat{S} \geq \frac{K}{2}$.

7.5 Algorithme de Grover amélioré

7.5.1 Introduction

Après avoir traité de IIMSA, dans ce chapitre, nous proposons l'algorithme de Grover amélioré, Dans ce cas, nous visons à améliorer la théorie de l'algorithme de Grover en le combinant différemment avec les méthodes classiques. Nous discutons de la théorie sous-jacente, la motivation principale de son développement, l'équation proposée, les implications et les enseignements tirés de nos résultats, et fournissons également une simulation de notre algorithme. L'objectif est d'obtenir une probabilité de succès élevée avec un nombre réduit d'itérations de Grover.

La principale motivation est la solution hybride quantique, principalement utilisée pour exploiter la supériorité quantique avec l'aide classique dans la résolution de problèmes multiples.

L'idée est de tester l'algorithme de Grover avec un petit nombre d'itérations, vraisemblablement moins que l'optimal L_{opt}, et de manipuler la probabilité de succès en utilisant une distribution de Bernoulli. Nous comparons les performances et la complexité de l'algorithme de Grover original avec notre algorithme de Grover amélioré. Nous nous attendons à observer des itérations plus petites dans notre algorithme par rapport à l'algorithme original, tout en conservant le même nombre d'itérations.

7.5.2 L'algorithme de Grover amélioré

Nous plongeons dans la théorie fondamentale de l'algorithme de Grover amélioré, y compris ses objectifs et l'algorithme détaillé qu'il englobe. L'objectif principal de cet algorithme proposé est d'accélérer l'algorithme de base de Grover. Nous proposons un algorithme qui permet de maintenir des performances similaires tout en réduisant le nombre d'itérations de Grover. L'algorithme complet est expliqué dans l'Algo. 7.

Rappelons la probabilité de succès de l'algorithme de Grover telle que définie dans 2.12. La probabilité de succès est la même pour chaque essai et est notée P_G^j, où j désigne le nombre d'itérations de Grover et G représente la probabilité donnée par Grover, donc elle est représentée comme suit :

$$P_G^j = \sin^2((2j+1)\theta) \tag{7.11}$$

Pour caractériser notre algorithme Grover amélioré, nous estimons théoriquement la probabilité de succès. Notre objectif principal est de minimiser le nombre d'itérations de l'algorithme de Grover tout en visant à obtenir une probabilité de succès élevée et une faible complexité. Cette probabilité est structurée comme suit : $\left(P_G^j\right) \cdot \left(1 - P_G^j\right)^{t-1}$ après exactement t essais, où P_G^j est la probabilité de succès de Grover pour j itérations.

Algorithm 7: L'algorithme de Grover amélioré

Data: Define T_{max}, $P_{en}^{j} = 0$, $targPs$, $j < L_{opt}$
while $nb_{trial} < T_{max}$ **do**
  Perform Grover $\mathcal{G}$ with j-iterations;
  if $P_{en}^{j} < targPs$ **then**
    $nb_{trial} = nb_{trial} + 1$;
    Run P_{en}^{j} based on Eq. 7.12.
  else
    $nb_{trial} = 0$;
    Finish;

En conséquence, la probabilité de succès P_{en}^{j}, obtenue après au plus T_{max} essais de cet algorithme mixte, peut être exprimée comme suit :

$$\begin{aligned} P_{en}^{j} &= \sum_{t=1}^{T_{max}} \left(P_G^j\right) \cdot \left(1 - P_G^j\right)^{t-1} \\ &= 1 - (1 - P_G^j)^{T_{max}} \\ &= 1 - (1 - \sin^2((2j+1)\theta))^{T_{max}} \end{aligned} \tag{7.12}$$

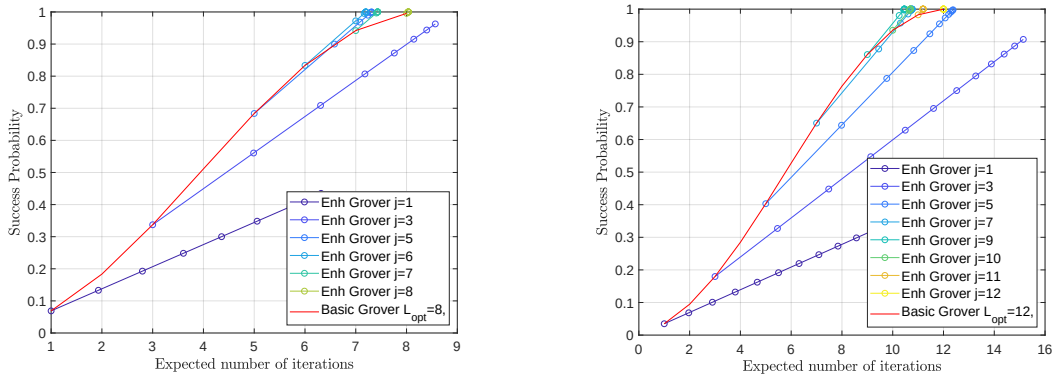
Si $T_{\max}$ est ∞, alors P_{en}^{j} sera égal à 1. Cependant, nous voulons nous assurer que $T_{\max}$ soit aussi petit que possible, beaucoup plus petit que le nombre d'itérations de l'oracle j lui-même.

De plus, nous pouvons évaluer le nombre attendu d'itérations effectuées dans l'algorithme de Grover, qui compte également le nombre d'essais $nb_{trial} \in \{1, \cdots, T_{max}\}$:

$$\begin{aligned} E_{en} = &\left(\sum_{t=1}^{T_{max}-1} t \cdot j \cdot \left(P_G^j\right) \cdot \left(1 - P_G^j\right)^{t-1} \right) \\ &+ \left(T_{max} \cdot j\right)(1 - P_G^j)^{T_{max}-1} \end{aligned} \tag{7.13}$$

En fin de compte, nous évaluons la performance de la probabilité de succès de l'algorithme de Grover P_{en}^{j} par rapport à P_G^j. De plus, nous évaluons les attentes représentées par E_{en}.

7.5.3 Enhanced Grover Performances



(a) $N = 7, T_{max} = 9$ (b) $N = 8, T_{max=16}$

Figure 7.9: Average P_{en} vs Success probability P_G

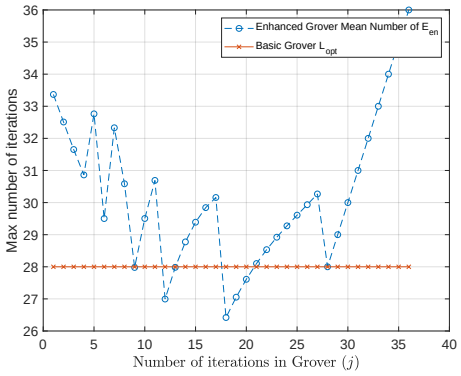
Probabilité de réussite améliorée de Grover

Dans cette section, nous comparons les performances de notre proposition, dénommée *Grover amélioré*, avec l'algorithme Grover initial, dénommé *Grover de base*. Nous avons tracé sur la Fig.7.9, la probabilité de réussite en fonction du nombre moyen d'itérations pour les deux approches, où nous considérons $N = 7$ et $N = 8$ utilisateurs. Nous supposons que pour les deux scénarios, nous utilisons un nombre de solutions $S = 1$. Ainsi, le nombre optimal d'itérations de Grover pour les deux scénarios serait de $L_{opt} = 8$ pour $N = 7$ et de $L_{opt} = 12$ pour $N = 8$, respectivement. Cet algorithme Grover amélioré, illustré dans la Fig.7.9, repose sur le concept de P_{en}^{j} par rapport à E_{en}.

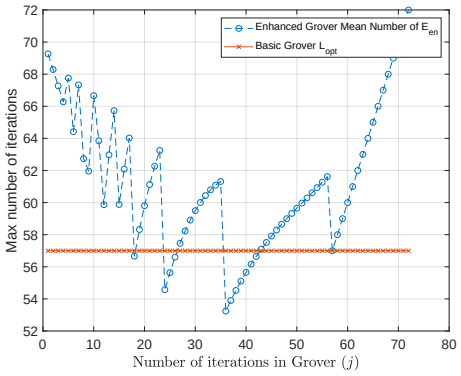
La Fig. 7.9a illustre le scénario avec sept utilisateurs, désigné par $N = 7$, et une valeur optimale de $L_{opt} = 8$. La probabilité de réussite de l'algorithme Grover amélioré, désignée par P_{en}^{j}, est notablement élevée lorsque j est dans l'ensemble $\{6, 7, 8\}$, correspondant au nombre attendu d'itérations. En revanche, la probabilité de réussite de Grover suit la distribution décrite par l'équation 7.11. Il est à noter que pour les valeurs de j dans $\{6, 7\}$, on a $j < L_{opt}$, ce qui indique une performance prometteuse sans nécessiter huit itérations, comme le requiert L_{opt}.

D'autre part, à partir de la Fig.7.9b, avec plus d'utilisateurs $N = 8$ et $L_{opt} = 12$, nous observons plusieurs itérations. Il est à noter qu'à l'intérieur de l'intervalle $j \in 10, 11, 12$, il y a une démonstration d'une probabilité de réussite élevée de l'algorithme Grover amélioré. De manière similaire à la Fig.7.9a, lorsque j n'atteint pas L_{opt}, nous pouvons atteindre une probabilité de réussite plus élevée, ce qui est prometteur.

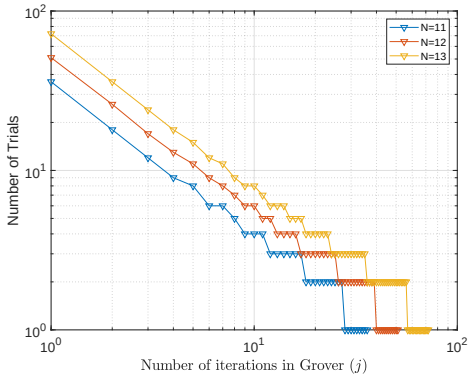
Pour le cas du *Grover de base*, le nombre d'itérations est le seul degré de liberté, et nous retrouvons la forme précédente donnée par 2.12. Au contraire, pour le



(a) $N = 11, L_{opt} = 28$



(b) $N = 13, L_{opt} = 57$



(c) Nombre d'Essais pour $N \in 11, 12, 13$

Figure 7.10: Nombre moyen E_{en}, Grover de Base $L_{s\text{-}opt}$ et nombre d'essais avec une cible $P_s = 0.9$

Grover amélioré, nous avons 2 degrés de liberté : (j, T_{max}). De manière intéressante, nous pouvons observer qu'il existe certains ensembles qui permettent au *Grover amélioré* d'atteindre un meilleur compromis entre la probabilité de réussite P_G^j et P_{En}^j. Cela prouve que notre *Grover amélioré* permet d'améliorer davantage l'efficacité de l'algorithme de Grover.

Nombre moyen d'itération pour Grover Amélioré

Ici, notre objectif est d'introduire le nombre moyen d'itérations et d'essais nécessaires pour atteindre une probabilité de réussite cible, en supposant une cible de $P_s = 0.9$. Pour atteindre cette probabilité de réussite cible, il n'est pas nécessaire d'exécuter L_{opt}

fois comme dans la procédure standard. Au lieu de cela, nous pouvons utiliser une approche sous-optimale, désignée par $L_{s\text{-}opt}$, car la probabilité de réussite est inférieure à 0.99. Nous traçons deux variables : 1) le nombre moyen d'itérations de Grover amélioré (E_{en}) et 2) l'algorithme Grover de base ($L_{s\text{-}opt}$) par rapport à l'itération de Grover j. Nous illustrons les résultats pour différents nombres d'utilisateurs, d'abord avec $N = 11$, comme indiqué dans la Fig.7.10a, puis avec $N = 13$, comme illustré dans la Fig.7.10b.

Nous commençons par observer que l'algorithme Grover de base, avec une probabilité de réussite fixe de $P_s = 0.9$, atteint des résultats de $L_{s\text{-}opt} = 28$ lorsque $N = 11$ et $L_{s\text{-}opt} = 57$ lorsque $N = 13$. Il est à noter que ces résultats sont en deçà de la valeur idéale, désignée par L_{opt}. Cela n'est pas surprenant car atteindre une probabilité de réussite de $P_s = 0.9$ ne nécessite pas nécessairement le nombre idéal L_{opt}. En revanche, notre algorithme proposé présente des variations par rapport aux itérations de Grover, désignées par j. Notamment, notre approche dépasse parfois l'algorithme Grover traditionnel. Par exemple, lorsque $N = 11$, notre algorithme surpasse la performance de Grover aux itérations $j = 12$ et $j = 18$, ce qui donne d'excellents résultats. De même, en considérant $N = 13$, notre algorithme proposé présente des variations à travers les itérations de Grover. Conformément au cas de $N = 11$, notre approche dépasse la performance de Grover aux itérations $j = 22$ et $j = 38$, ce qui souligne la nature prometteuse de nos résultats.

Nous avons évalué le nombre d'essais par rapport à l'itération de Grover j, comme illustré dans Fig. 7.10c. Nous notons d'abord que lorsque j augmente, le nombre d'essais requis diminue. Pour être en équilibre avec les itérations de Grover, notre nb_{trial} diminue également.

7.5.4 Conclusion

Nous avons effectué des simulations et des évaluations de l'algorithme de Grover amélioré et de l'algorithme de Grover original, en nous concentrant sur les performances et la complexité. Tout d'abord, il convient de noter que notre algorithme de Grover amélioré est toujours plus performant que l'algorithme de Grover original, en particulier lorsqu'il s'agit d'atteindre ou de dépasser les limites de la complexité. l'algorithme de Grover original, en particulier en atteignant ou même en dépassant les mêmes valeurs de L_{opt}. Cette supériorité a été vérifiée pour des nombres d'utilisateurs de $N = 7$ et $N = 8$. En outre, l'algorithme proposé a toujours répondu aux attentes en matière de performances pour diverses itérations de Grover (j), ce qui démontre une similitude fondamentale entre les deux algorithmes. Ce chapitre souligne l'importance de discuter du potentiel des solutions hybrides dans les recherches futures.

Bibliography

[1] Ericsson, "5g wireless access : An overview," *Ericsson White Paper*, no. 1/28423-FGB1010937, 2020. [Online]. Available: https://www.ericsson.com/4ac666/assets/local/reports-papers/white-papers/whitepaper-5g-wireless-access.pdf.

[2] "Spectral efficiency:5g-nr and 4g-lte." (), [Online]. Available: https://www.techplayon.com/spectral-efficiency-5g-nr-and-4g-lte/ (visited on 06/21/2023).

[3] T. S. Rappaport, Y. Xing, G. R. MacCartney, A. F. Molisch, E. Mellios, and J. Zhang, "Overview of millimeter wave communications for fifth-generation (5g) wireless networks—with a focus on propagation models," *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 12, pp. 6213–6230, 2017. DOI: 10.1109/TAP.2017.2734243.

[4] B. Jijo, S. Zeebaree, R. Zebari, *et al.*, "A comprehensive survey of 5g mm-wave technology design challenges," *Asian Journal of Computer Science and Information Technology*, vol. 8, pp. 1–20, Apr. 2021. DOI: 10.9734/AJRCOS/2021/v8i130190.

[5] P. Popovskii, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5g wireless network slicing for embb, urllc, and mmtc: A communication-theoretic view," 2018.

[6] E. Kahuha. "5 real life use cases of 5g ultra-reliable low-latency communication (urllc)." (2021), [Online]. Available: https://www.section.io/engineering-education/five-real-life-use-cases-of-5g-ultra-reliable-low-latency-communication-urllc/.

[7] T. Electronic. "How to test the ultra-reliability and low latency of 5g networks according to urllc requirements?" (2022), [Online]. Available: https://www.temcom.com/how-to-test-the-ultra-reliability-and-low-latency-of-5g-networks-according-to-urllc-requirements/.

[8] "Lte control plane and user plane latency calculation (fdd)." (), [Online]. Available: https://www.techplayon.com/lte-control-plane-and-user-latency-calculation-fdd/#:~:text=LTE%2D%20is%20designed%20to%20support,the%20reception%20of%20an%20acknowledgment (visited on 06/21/2023).

[9] Z. Xiao, L. Zhu, Z. Gao, D. O. Wu, and X.-G. Xia, "User fairness non-orthogonal multiple access (noma) for millimeter-wave communications with analog beamforming," *IEEE Transactions on Wireless Communications*, vol. 18, no. 7, pp. 3411–3423, 2019. DOI: 10.1109/TWC.2019.2913844.

[10] S. Chaturvedi, Z. Liu, V. A. Bohara, A. Srivastava, and P. Xiao, "A tutorial to sparse code multiple access," 2021. arXiv: 2105.06860 [cs.IT].

[11] X. Dai, Z. Zhang, B. Bai, S. Chen, and S. Sun, "Pattern division multiple access: A new multiple access technology for 5g," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 54–60, 2018. DOI: 10.1109/MWC.2018.1700084.

[12] B. Wang, K. Wang, Z. Lu, T. Xie, and J. Quan, "Comparison study of non-orthogonal multiple access schemes for 5g," in *2015 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*, 2015, pp. 1–5. DOI: 10.1109/BMSB.2015.7177186.

[13] P. Bertrand and J. Jiang, "Random access," in *LTE – The UMTS Long Term Evolution*. John Wiley and Sons, Ltd, 2011, ch. 17, pp. 371–406, ISBN: 9780470978504. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470978504.ch17. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9780470978504.ch17.

[14] D. Magrin, C. Pielli, Č. Stefanović, and M. Zorzi, "Enabling lte rach collision multiplicity detection via machine learning," in *2019 International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOPT)*, 2019, pp. 1–8. DOI: 10.23919/WiOPT47501.2019.9144126.

[15] A. Celik, "Grant-Free NOMA: A Low Complexity Power Control Through User Clustering," May 2022. [Online]. Available: https://www.techrxiv.org/articles/preprint/Grant-Free_NOMA_A_Low_Complexity_Power_Control_Through_User_Clustering/19688019.

[16] W. Liu, W. Qingshan, J. Shen, J. Zhao, M. Zidan, and L. Tong, "An optimized quantum minimum searching algorithm with sure-success probability and its experiment simulation with cirq," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 1–10, Nov. 2021. DOI: 10.1007/s12652-020-02840-z.

[17] J. Jiang and H. Wang, "Massive random access with sporadic short packets: Joint active user detection and channel estimation via sequential message passing," *CoRR*, vol. abs/2102.10779, 2021. arXiv: 2102.10779. [Online]. Available: https://arxiv.org/abs/2102.10779.

[18] B. C. Levy, *Principles of Signal Detection and Parameter Estimation*, 1st ed. Springer Publishing Company, Incorporated, 2008, ISBN: 0387765425.

[19] G. Wunder, Č. Stefanović, P. Popovski, and L. Thiele, "Compressive coded random access for massive mtc traffic in 5g systems," in *2015 49th Asilomar Conference on Signals, Systems and Computers*, 2015, pp. 13–17. DOI: 10.1109/ACSSC.2015.7421050.

[20] Z. Chen and W. Yu, "Massive device activity detection by approximate message passing," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2017, pp. 3514–3518. DOI: 10.1109/ICASSP.2017.7952810.

[21] M. I. Habibie, J. Hamie, and C. Goursaud, "A performance comparison of classical and quantum algorithm for active user detection," in *2022 IEEE 23rd International Workshop on Signal Processing Advances in Wireless Communication (SPAWC)*, 2022, pp. 1–5. DOI: 10.1109/SPAWC51304.2022.9833942.

[22] M. I. Habibie, J. Hamie, and C. Goursaud, "Adaptation of grover's quantum algorithm to multiuser detection in an ocdma system," in *2021 IEEE Symposium On Future Telecommunication Technologies (SOFTT)*, 2021, pp. 88–93. DOI: 10.1109/SOFTT54252.2021.9673141.

[23] S. Carrol. "Even Physicists Don't Understand Quantum Mechanics." (), [Online]. Available: Even%20Physicists%20Don't%20Understand%20Quantum%20Mechanics.

[24] C. Rovelli, *Reality Is Not What It Seems*. 2014.

[25] G. Wright. "Quantum." (), [Online]. Available: https://www.techtarget.com/whatis/definition/quantum.

[26] L. Chemistry. "Quantized energy and photons." (), [Online]. Available: https://chem.libretexts.org/Bookshelves/General_Chemistry/Map%3A_Chemistry_-_The_Central_Science_(Brown_et_al.)/06%3A_Electronic_Structure_of_Atoms/6.02%3A_Quantized_Energy_and_Photons.

[27] D. Dobrijevic. "The double-slit experiment: Is light a wave or a particle?" (2022), [Online]. Available: https://www.space.com/double-slit-experiment-light-wave-or-particle.

[28] W. K. Xiaoming Lu Qishan Tang, *Research and verification of blackbody radiation law*, 2018. [Online]. Available: https://www.researchgate.net/publication/335655740_Research_and_Verifi_cation_of_Blackbody_Radiation_Law/fulltext/5d72539192851cacdb23f1a0/Research-and-Verifi-cation-of-Blackbody-Radiation-Law.pdf.

[29] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[30] N. Zettili, *Quantum Mechanics Concepts and Applications*, Wiley, Ed. John Wiley and Sons, Ltd, 2009.

[31] C. Wang and A. Rahman, "Quantum-enabled 6g wireless networks: Opportunities and challenges," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 58–69, 2022. DOI: 10.1109/MWC.006.00340.

[32] D. Harvey and J. van Der Hoeven, "Integer multiplication in time O(n log n)," *Annals of Mathematics*, Mar. 2021. DOI: 10.4007/annals.2021.193.2.4. [Online]. Available: https://hal.science/hal-02070778.

[33] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, "Efficient networks for quantum factoring," *Physical Review A*, vol. 54, no. 2, pp. 1034–1063, Aug. 1996. DOI: 10.1103/physreva.54.1034. [Online]. Available: https://doi.org/10.1103%2Fphysreva.54.1034.

[34] A. Irmayana, H. SY, Y. T. Paulus, N. Aini, and K. Aryasa, "A systematic comparative study of linear, binary and interpolation search algorithms," in *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2021, pp. 1–5. DOI: 10.1109/ICORIS52787.2021.9649479.

[35] V. Portilheiro, "Applying grover's algorithm to unique-k-sat," Sep. 2018.

[36] F. Chung, J. Salehi, and V. Wei, "Optical orthogonal codes: Design, analysis and applications," *IEEE Transactions on Information Theory*, vol. 35, no. 3, pp. 595–604, 1989.

[37] G.-C. Yang, "Variable-weight optical orthogonal codes for cdma networks with multiple performance requirements," *IEEE Transactions on Communications*, vol. 44, no. 1, pp. 47–55, 1996.

[38] S. Maric, M. Hahm, and E. Titlebaum, "Construction and performance analysis of a new family of optical orthogonal codes for cdma fiber-optic networks," *IEEE Transactions on Communications*, vol. 43, no. 2/3/4, pp. 485–489, 1995. DOI: 10.1109/26.380066.

[39] B. L.Nguyen and J. Young, "All-optical cdma with bipolar codes," *Electronic Letters*, vol. 31, no. 6, 1995.

[40] A. Farhat, M. Menif, C. Lepers, H. Rezig, and P. Gallion, "Performance comparison of coherent versus incoherent direct sequence optical code division multiple access system," vol. 7099, Jun. 2008. DOI: 10.1117/12.806880.

[41] T. M. Cover, "Multiple user information theory for the gaussian channel," *New Concepts in Multi-User Communication*, vol. 43, pp. 53–61, 1981.

[42] D. Duchemin, J.-M. Gorce, and C. Goursaud, "Code domain non orthogonal multiple access versus aloha: A simulation based study," in *2018 25th International Conference on Telecommunications (ICT)*, 2018, pp. 445–450. DOI: 10.1109/ICT.2018.8464836.

[43] D. Duchemin, L. Chetot, J.-M. Gorce, and C. Goursaud, "Coded random access for massive mtc under statistical channel knowledge," in *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2019, pp. 1–5. DOI: 10.1109/SPAWC.2019.8815491.

[44] M. Khataie, M. Soleymani, and M. Ahmad, "Use of gaussian codebooks for residual vector quantizers," in *Proceedings 2000 International Conference on Image Processing (Cat. No.00CH37101)*, vol. 2, 2000, 179–182 vol.2.

[45] A. Kipnis, G. Reeves, and Y. C. Eldar, "Single letter formulas for quantized compressed sensing with gaussian codebooks," in *2018 IEEE International Symposium on Information Theory (ISIT)*, 2018, pp. 71–75. DOI: 10.1109/ISIT.2018.8437761.

[46] E. V. Rogozhnikov, K. V. Savenko, A. K. Movchan, and E. M. Dmitriyev, "The study of correlation receivers," in *2019 20th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM)*, 2019, pp. 155–159.

[47] C. Goursaud, A. Julien-Vergonjanne, C. Aupetit-Berthelemot, J.-P. Cances, and J.-M. Dumas, "Ds-ocdma receivers based on parallel interference cancellation and hard limiters," *IEEE Transactions on Communications*, vol. 54, no. 9, pp. 1663–1671, 2006. DOI: 10.1109/TCOMM.2006.881252.

[48] K. B. Petersen and M. S. Pedersen, *The Matrix Cookbook*. Technical University of Denmark, Nov. 2012, Version 20121115. [Online]. Available: http://www2.compute.dtu.dk/pubdb/pubs/3274-full.html.

[49] J. Xiao, X. Ma, and S. W. McLaughlin, "Quantifying information rate losses with zero-forcing and maximum-likelihood detectors," in *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2010, pp. 3342–3345. DOI: 10.1109/ICASSP.2010.5496010.

[50] F. C. Vilar, "Implementation of zero forcing and mmse equalization techniques in ofdm," [Online]. Available: https://upcommons.upc.edu/bitstream/handle/2117/78037/Implementation%20of%20Zero%20Forcing%20and%20MMSE%20equalization%20techniques%20in%20OFDM.pdf.

[51] geeksforgeeks. "Searching algorithms." (), [Online]. Available: https://www.geeksforgeeks.org/searching-algorithms/ (visited on 08/23/2023).

[52] W. Janko, "Variable jump search: The algorithm and its efficiency.," *Angewandte Informatik*, vol. 23, pp. 6–11, Jan. 1981.

[53] U. of Cambridge, *Quantum computing (cst part ii) - lecture 7 deutsch-jozsa algorithm*, 2023.

[54] F. H. Azka Rafey Khan Bismah Rizwan, *Bernstein-vazirani algorithm*, 2023.

[55] P. Young, *The bernstein-vazirani algorithm*, 2019.

[56] A. Ambainis, "Quantum walks and their algorithmic applications," 2004. arXiv: quant-ph/0403120 [quant-ph].

[57] D. Bulger, W. Baritompa, and G. Wood, "Implementing pure adaptive search with grover's quantum algorithm," *Journal of Optimization Theory and Applications*, vol. 116, pp. 517–529, Mar. 2003. DOI: 10.1023/A:1023061218864.

[58] G. Brassard, P. HØyer, and A. Tapp, "Quantum counting," in *Automata, Languages and Programming*, Springer Berlin Heidelberg, 1998, pp. 820–831. [Online]. Available: https://doi.org/10.1007%2Fbfb0055105.

[59] 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, Jun. 1998.

[60] A. Younes, *Strength and weakness in grover's quantum search algorithm*, 2008. arXiv: 0811.4481 [quant-ph].

[61] F. Song, *Early days following grover's quantum search algorithm*, 2017. arXiv: 1709.01236 [quant-ph].

[62] C. Durr and P. Hoyer, "A quantum algorithm for finding the minimum," 1996.

[63] S. Imre and F. Balazs, "Non-coherent multi-user detection based on quantum search," in *2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No.02CH37333)*, vol. 1, 2002, 283–287 vol.1.

[64] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless myths, realities, and futures: From 3g/4g to optical and quantum wireless," *Proceedings of the IEEE*, vol. 100, pp. 1853–1888, May 2012. [Online]. Available: https://doi.org/10.1109%2Fjproc.2012.2189788.

[65] S. Zhao, J. Yao, and B. Zheng, "Multiuser detection based on grover's algorithm," May 2006. DOI: 10.1109/ISCAS.2006.1693688.

[66] W. Ye, W. Chen, X. Guo, C. Sun, and L. Hanzo, "Quantum search-aided multi-user detection for sparse code multiple access," *IEEE Access*, vol. 7, pp. 52 804–52 817, 2019.

[67] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Noncoherent quantum multiple symbol differential detection for wireless systems," *IEEE Access*, vol. 3, pp. 569–598, 2015.

[68] P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design," *IEEE Access*, vol. 1, pp. 94–122, 2013.

[69] P. Botsinis, D. Alanis, S. Feng, *et al.*, "Quantum-assisted indoor localization for uplink mm-wave and downlink visible light communication systems," *IEEE Access*, vol. 5, pp. 23 327–23 351, 2017. DOI: 10.1109/ACCESS.2017.2733557.

[70] P. Botsinis, Y. Huo, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Quantum search-aided multi-user detection of idma-assisted multi-layered video streaming," *IEEE Access*, vol. 5, pp. 23 233–23 255, 2017. DOI: 10.1109/ACCESS.2017.2732358.

[71] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Iterative quantum-assisted multi-user detection for multi-carrier interleave division multiple access systems," *IEEE Transactions on Communications*, vol. 63, no. 10, pp. 3713–3727, 2015.

[72] P. Botsinis, S. X. Ng, and L. Hanzo, "Fixed-complexity quantum-assisted multi-user detection for cdma and sdma," *IEEE Transactions on Communications*, vol. 62, no. 3, pp. 990–1000, 2014.

[73] S.-m. Zhao and B.-y. Zheng, "Quantum multi-user detection," vol. 1, Feb. 2005, pp. 371–374, ISBN: 0-7803-9243-4. DOI: 10.1109/ISSPA.2005.1580273.

[74] M. Li-min, S. Xin-yu, and Z. Kai, "Research on routing algorithm for manet based on grover searching theory," in *2010 IEEE International Conference on Wireless Information Technology and Systems*, 2010, pp. 1–4.

[75] W. Luo and G. Liu, "Asymmetrical quantum encryption protocol based on quantum search algorithm," *China Communications*, vol. 11, no. 9, pp. 104–111, 2014. DOI: 10.1109/CC.2014.6969775.

[76] S. E. Gaily and S. Imre, "Quantum resource distribution management in multi-task environment," in *2019 14th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)*, 2019, pp. 364–367. DOI: 10.1109/TELSIKS46999.2019.9002340.

[77] S. E. Gaily and S. Imre, "Quantum optimization in large resource management systems," in *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2019, pp. 1–5. DOI: 10.1109/SPAWC.2019.8815470.

[78] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Coherent versus non-coherent quantum-assisted solutions in wireless systems," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 144–153, 2017.

[79] P. Botsinis, D. Alanis, Z. Babar, S. Ng, and L. Hanzo, "Joint quantum-assisted channel estimation and data detection," Jul. 2016.

[80] W. Yu, Y. Xu, W. Liu, A. Liu, and B. Zheng, "Quantum multi-user detection based on coherent state signals," *Journal of Quantum Computing*, vol. 1, pp. 81–88, Jan. 2019. DOI: 10.32604/jqc.2019.07324.

[81] F. Li, L. Zhou, L. Liu, and H. Li, "A quantum search based signal detection for mimo-ofdm systems," in *2011 18th International Conference on Telecommunications*, 2011, pp. 276–281. DOI: 10.1109/CTS.2011.5898934.

[82] P. Botsinis, Z. Babar, D. Alanis, *et al.*, "Research data: Quantum error correction protects quantum search algorithms against decoherence," 2016. [Online]. Available: https://api.semanticscholar.org/CorpusID:13039291.

[83] qiskit. "Maximum number of qubits supported by the qasm simulator." (), [Online]. Available: https://quantumcomputing.stackexchange.com/questions/14927/maximum-number-of-qubits-supported-by-the-qasm-simulator#:~:text=You%20can%20also%20play%20with,everything%20there%20is%20to%20know!&text=If%20you%20use%20ibmq_qasm_simulator%20then,of%20qubit%20supported%20is%2032.

[84] C. E. community. "How can you measure complexity quantum algorithms." (), [Online]. Available: https://www.linkedin.com/advice/3/how-can-you-measure-complexity-quantum-algorithms-eycae#:~:text=The%20complexity%20of%20a%20quantum,the%20depth%20of%20the%20circuit.

[85] X. Lu, N. Jiang, H. Hu, and Z. Ji, "Quantum adder for superposition states," *International Journal of Theoretical Physics*, vol. 57, Sep. 2018. DOI: 10.1007/s10773-018-3779-2.

[86] G. L. Long, Y. S. Li, W. L. Zhang, and L. Niu, "Phase matching in quantum searching," *Physics Letters A*, vol. 262, no. 1, pp. 27–34, Oct. 1999.

[87] G. L. Long, "Grover algorithm with zero theoretical failure rate," *Physical Review A*, vol. 64, no. 2, Jul. 2001. DOI: 10.1103/physreva.64.022307.

[88] G.-L. Long, X. Li, and Y. Sun, "Phase matching condition for quantum search with a generalized initial state," *Physics Letters A*, vol. 294, no. 3, pp. 143–152, 2002, ISSN: 0375-9601.

[89] Y. Chen, S. Wei, X. Gao, C. Wang, J. Wu, and H. Guo, "An optimized quantum maximum or minimum searching algorithm and its circuits.," *arXiv: Quantum Physics*, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:201124776.

[90] Y. Chen, S. Wei, X. Gao, *et al.*, "A low failure rate quantum algorithm for searching maximum or minimum," *Quantum Information Processing*, vol. 19, Aug. 2020.

[91] Y. Seo, Y. Kang, and J. Heo, "Quantum search algorithm for weighted solutions," *IEEE Access*, vol. 10, pp. 16 209–16 224, 2022. DOI: 10.1109/ACCESS.2022.3149351.

[92] Y. Kang and J. Heo, "Quantum minimum searching algorithm and circuit implementation," in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, 2020, pp. 214–219.

[93] S. Mondal, M. R. Laskar, and A. K. Dutta, "Ml criterion based signal detection of a mimo-ofdm system using quantum and semi-quantum assisted modified dha/bbht search algorithm," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1688–1698, 2021. DOI: 10.1109/TVT.2021.3055537.

[94] L. A. B. Kowada, C. Lavor, R. Portugal, and C. M. H. de Figueiredo, "A new quantum algorithm for solving the minimum searching problem," *International Journal of Quantum Information*, vol. 06, pp. 427–436, 2008. [Online]. Available: https://api.semanticscholar.org/CorpusID:120938723.

[95] K. Miyamoto, M. Iwamura, and K. Kise, *A quantum algorithm for finding k-minima*, 2019. arXiv: 1907.03315 [quant-ph].

[96] L. K. Grover, *A fast quantum mechanical algorithm for database search*, 1996. arXiv: quant-ph/9605043 [quant-ph].

[97] G. Prawiroatmodjo. "Hybrid quantum-classical computing models." (2021), [Online]. Available: https://devblogs.microsoft.com/qsharp/hybrid-quantum-classical-models/.

[98] Qiskit, *Calculate quantum euclidean distance with qiskit*. [Online]. Available: https://medium.com/qiskit/calculate-quantum-euclidean-distance-with-qiskit-df85525ab485.

Acronyms

5G	Fifth-Generation. 3, 4, 5, 6, 8, 111, 158
5G	Cinquième Génération. 117
AMP	Approximate Message Passing. 9, 113
ASE	Amplified Spontaneous Emission. 28
AUD	Active User Detection. IX, X, XVII, XVIII, 3, 8, 9, 25, 27, 29, 42, 43, 45, 49, 50, 51, 72, 83, 111, 112, 113, 119, 125, 132, 158
AUD	Détection des l'utilisateurs Actifs. X, 117, 118, 119, 121, 122, 123, 124, 126, 158
AWGN	Additive white Gaussian Noise. 26, 29
AWGN	Bruit Blanc Additif Gaussien. 118
BBHT	Boyer-Brassard-Høyer-Tapp. XVIII, 25, 37, 38, 39, 40, 41, 42, 71, 72, 73, 74, 112, 118, 121, 127, 158
BER	Bit Error Performance. 43, 45, 46
BS	Base Station. XVII, 3, 7, 8, 26, 111, 158
BS	Station de Base. 117, 118
CCD	Conventional Correlation Detector. 43, 46
CCR	Conventional Correlation Receiver. X, XVII, XVIII, 9, 25, 29, 30, 45, 49, 50, 51, 60, 61, 62, 63, 64, 65, 66, 67, 71, 72, 76, 82, 83, 84, 85, 87, 88, 90, 92, 94, 95, 112, 119, 125, 132, 133, 134, 158

CCR	Récepteur de Corrélation Conventionnel. 117, 122, 123, 127, 134, 136, 158
CCR-IIMSA	Conventional Correlation Receiver Improved Iterated Minimum Searching Algorithm. 76, 83, 88, 89, 90, 92
CCR-DHA	Conventional Correlation Receiver Durr-Hoyer. 76, 83, 86, 87, 88, 92
CD	Code domain. 6
CD-NOMA	Accès Multiple Non Orthogonal en Domaine de Code. 118
CD-NOMA	Code-Domain Non-Orthogonal Multiple Access. 6, 26
CDMA	Code Division Multiple Access. 6, 27, 44
CE	Channel Estimation. 46
CFE	Cost Function Evaluation. 43
DHA	Algorithme Durr-Hoyer. 118, 127, 134, 136
DHA-MUA QMUD	Durr-Hyer Algorithm Multi-input Approximation Quantum-Assisted Multi-User Detection. 46
DHA-MUA-FKT QMUD	Durr-Hyer Algorithm Multi-input Approximation Forward Knowledge Transfer Quantum-Assisted Multi-User Detection. 46
DH-QSA	Durr-Hoyer Quantum Search Algorithm. 46
DHA	Durr-Hoyer Algorithm. XVIII, 21, 25, 41, 42, 43, 44, 46, 71, 72, 73, 74, 75, 82, 83, 85, 86, 87, 88, 89, 90, 92, 94, 95, 112, 113, 114, 121, 133, 134, 158
DL	downlink. 4, 5
EDFA	Erbium-Doped Fiber Amplifier. 28
eMBB	Enhanced Mobile Broadband. 4, 6
FDMA	Frequency Division Multiple Access. 6
GCP	Graph-Coloring Problem. 73
GF	Grant-Free. 3, 8, 111
GF	Système sans accord préalable. 117
GFRA	Grant-Free Random Access. XVII

IBM	International Business Machines Corporation. 73
IIMSA	Improved Iterated Minimum Searching Algorithm. X, XVIII, 71, 72, 74, 75, 77, 82, 83, 84, 85, 86, 88, 89, 90, 92, 94, 95, 99, 101, 112, 114, 132, 133, 134, 158
IIMSA	Algorithme Amélioré de Recherche de Minimum par Itération. 127, 129, 136, 137, 158
IoT	Internet of Things. 5, 90
ISI	Intersymbol Interference. 30
LED	Light Emitting Diode. 28
LM	Linear Measurement. 74
LSB	Least Significant Bit. 54, 55, 78, 80
LTE	Long Term Evolution. 4, 5, 7
MAA	Maximum Approximation. 46
MAI	Multiple Access Interference. 29, 30, 119
MANET	Mobile Ad Hoc Networks. 44, 46
MAP	Maximum a posteriori. 9, 46
MC-IDMA	Multi-Carrier Interleave Division Multiple Access. 44, 46
MIMO	Multiple-Input Multiple-Output. 45, 46
ML	Maximum Likelihood. X, XVII, 9, 25, 29, 43, 45, 46, 49, 50, 51, 58, 60, 62, 63, 64, 65, 66, 67, 68, 71, 72, 83, 84, 119, 125, 132, 158
ML	Maximum de Vraisemblance. 117, 122, 123, 126, 127, 158
mMTC	Massive Machine Type Communication. XVII, 4, 5, 8, 158
mMTC	Massives entre machines. 158
mmWave	Millimetre Wave. 5
MPA	Message Passing Algorithm. 43, 46
MSA	Minimum Searching Algorithm. 44, 46
MSB	Most Significant Bit. 78
MSDD	Multiple Symbol Differential Detector. 43, 46
MUD	Multi-User Detection. 43, 44, 46
MUSA	Multi-User Shared Access. 7
NCFE	Number of Cost Functions. 43

NOMA	Non-Orthogonal Multiple Access. IX, X, 6, 7, 8, 9, 27, 119
NP	Non-polynomial. 44, 46
OCDMA	Optical Code Division Multiple Access. 27, 28
OFDM	Orthogonal Frequency-Division Multiplexing. 45, 46
OMA	Orthogonal Multiple Access. 6
OMP	Orthogonal Matching Pursuit. 9
OOC	Optical Orthogonal Code. 27
OWQF	One-way quantum function. 46
PD	Power domain. 6
PDMA	Pattern Division Multiple Access. 7
PIC	Parallel Interference Cancellation. 49, 50, 113
PIC	Annulation des Interférences en Parallèle. 123
PM	Potential Minimum. 74
Q-MPA	Quantum-Assisted Message Passing Algorithm. 43, 46
QMSA	Quantum Minimum Searching Algorithm. XVIII
QMUD	Quantum Assisted Multi-User Detection. 43, 44, 45, 46
QoS	Quality of Service. 5
QPU	Quantum Processing Units. 100
QRAM	Quantum Random Access Memory. 73, 74
QRWBS	Quantum-assisted repeated weighted boosting search. 45, 46
QSA	Quantum Searching Algorithm. 46
QSD-MPA	Quantum-Assisted Sphere Decoder-based MPA. 46
QUMMSA	Quantum Maximum or Minimum Searching Algorithm. 73, 74
QWSA	Quantum Weight Searching Algorithm. 43
RA	Random Access. XVII
RAA	Random Access Assignment. 7
RACH	Random Access channel. 7, 8
RWBS	Repeated Weighted Boosting Search. 45, 46

SCMA	Sparse Code Multiple Access. 7
SDMA	Space-Division Multiple Access. 44
SF	Spreading Factor. IX, 26, 53, 57, 58, 60, 61, 63, 81, 83, 84, 86, 87, 88, 89, 90, 92, 112, 118, 132
SIC	Successive Interference Cancellation. 6, 7, 49, 50, 113
SIC	Annulation Successive des Interférences. 123
SISO	Soft-input Soft-output. 46
TDMA	Time Division Multiple Access. 6
UE	User Equipment. 3, 7, 8, 9, 111
UE	Équipement Utilisateur. 117
UL	uplink. 4, 5
URLLC	Ultra-reliable low-latency communication. XVII, 4, 5, 8, 158
URLLC	Ultra-fiables à faible latence. 158
VLC	Visible Light Communication. 43, 46
ZF	Zero Forcing. X, XVII, XVIII, 9, 25, 30, 45, 49, 50, 51, 60, 61, 62, 63, 64, 65, 66, 67, 71, 72, 76, 82, 83, 84, 85, 87, 90, 92, 94, 95, 112, 120, 125, 132, 133, 134
ZF	Zéro forcing. 117, 122, 123, 127, 134, 136, 158
ZF-IIMSA	Zero Forcing Receiver Improved Iterated Minimum Searching Algorithm. 76, 83, 88, 89, 90, 92, 94, 95, 133, 134, 136
ZF-DHA	Zero Forcing Durr-Hoyer. 76, 83, 86, 87, 88, 92, 134

FOLIO ADMINISTRATIF

THÈSE DE L'UNIVERSITÉ DE LYON OPERÉE AU SEIN DE L'INSA LYON

NOM : Habibie
Prénoms : Idham

Date de soutenance : 14/12/2023

Titre : Solutions améliorées de l'algorithme de Grover pour la détection d'utilisateurs actifs dans les réseaux sans fil

Nature : Doctorat

Numéro d'ordre : 2023ISAL0126

École doctorale : EEA, n°160

Spécialité : Traitement du signal et des images

Résumé :
5G comprend des fonctionnalités telles que Ultra-fiables à faible latence (URLLC) et Massives entre machines (mMTC) pour minimiser les délais et connecter de nombreux appareils. Cela nécessite un schéma Détection des l'utilisateurs Actifs (AUD), nécessitant une détection en temps réel par Base Station (BS). Maximum de Vraisemblance (ML) est le plus performant pour AUD mais il est complexe. Pour simplifier, des alternatives comme CCR et ZF ont été introduites mais mais ne peuvent égaler les performances de ML. Pour y remédier, nous explorons l'algorithme de Grover, connu pour ses capacités de superposition (travail avec 0 et 1). superposition (travailler avec 0 et 1 en même temps). Cependant, l'algorithme de Grover, lorsqu'il est contraint par la fonction $f(x) = \delta$, n'est pas aussi performant que ML ; il est plus proche de CCR et de ZF. Pour atteindre les performances de ML, l'algorithme de Grover doit être modifié pour trouver la distance minimale, comme ML. la distance minimale, comme le fait ML.
Nous proposons un nouvel algorithme, à savoir Algorithme Amélioré de Recherche de Minimum par Itération (IIMSA), visant à améliorer les algorithmes existants Boyer-Brassard-Høyer-Tapp (BBHT) et Durr-Hoyer Algorithm (DHA), qui sont les méthodes prometteuses pour trouver le minimum à l'aide de l'algorithme de Grover. afin de réduire leur complexité tout en maintenant des performances élevées. L'idée est d'utiliser n'importe quelle solution aléatoire plutôt que d'effectuer L itérations aléatoires comme le suggère DHA. Nous incorporons également des méthodes classiques telles que ZF et CCR pour améliorer leurs performances et réduire la complexité. Nous adaptons également l'algorithme de Grover dans le contexte de AUD dans cette thèse.
Nous présentons également un algorithme de Grover amélioré inspiré d'une solution hybride quantique qui exploite à la fois des éléments quantiques et classiques. solution hybride quantique qui exploite à la fois des éléments quantiques et classiques. L'objectif principal est d'augmenter la probabilité de succès P_s et de réduire la complexité de l'algorithme original de Grover. de l'algorithme de Grover original. Le concept consiste à utiliser moins d'itérations de Grover que le nombre optimal, dénommé P_s. que le nombre optimal, noté L_{opt}, et de le combiner avec la probabilité de succès classique. Nous pensons que cette approche a le potentiel de modifier le comportement de la complexité et d'obtenir une probabilité de succès élevée. et d'atteindre une probabilité de succès élevée.

Mots-clés : URLLC, mMTC, AUD, ML, CCR, IIMSA, BBHT, DHA

Laboratoire(s) de recherche : Centre of Innovation in Telecommunications and Integration of Service (CITI)

Directeur de thèse : Claire Goursaud

Président du jury : Pierre Duhamel

Composition du jury : Omar Fawzi, Iryna Andriyanova, Gilles Burel