Quantum Computing

Bridging the Gap to the Future

Dr. Neha Gupta
Dr. Pankaj Kumar Mishra
Dr. Rahul Kumar Budania

Quantum Computing Bridging the Gap to the Future

EMPYREAL
PUBLISHING HOUSE

India | UAE | Nigeria | Uzbekistan | Montenegro | Iraq | Egypt | Thailand | Uganda | Philippines | Indonesia

www.empyrealpublishinghouse.com

Quantum Computing Bridging the Gap to the Future

Authored By:

Dr. Neha Gupta
Associate Professor
SCSIT, Symbiosis University of Applied Sciences Indore

Dr. Pankaj Kumar Mishra
Pro Vice Chancellor
Glocal University, Saharanpur, Uttar Pradesh

Dr. Rahul Kumar Budania
Assistant Professor and Head of the Electronics & Communication Engineering Department
Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan

First Impression: November 2023

Quantum Computing Bridging the Gap to the Future

ISBN: 978-81-965655-9-6

Rs. 1000/- ($80)

DISCLAIMER

Information contained in this book has been published by Empyreal Publishing House and has been obtained by the authors from sources believed to be reliable and correct to the best of their knowledge. The author is solely responsible for the contents of the articles compiled in this book. Responsibility of authenticity of the work or the concepts/views presented by the author through this book shall lie with the author and the publisher has no role or claim or any responsibility in this regard. Errors, if any, are purely unintentional and readers are requested to communicate such error to the author to avoid discrepancies in future.

Published by:
Empyreal Publishing House

Preface

In the ever-shifting landscape of technology, certain advancements stand out as pivotal moments in human history. Quantum computing is undeniably one such frontier, poised at the intersection of science fiction and reality. As we venture into the 21st century, the power of classical computers, although impressive, faces inherent limitations when addressing complex problems. Quantum computing, with its ability to manipulate quantum bits or qubits, harnesses the principles of quantum mechanics to revolutionize computation. This book, **"Quantum Computing: Bridging the Gap to the Future,"** is an odyssey through the fascinating world of quantum mechanics and its application in computing technologies.

The preface of this book serves as a gateway into the intricate realm of quantum computing, offering readers a glimpse into the fundamental concepts that underpin this revolutionary field. We embark on a journey that takes us from the historical roots of quantum theory, unraveling the enigmatic nature of particles and waves, to the cutting-edge developments in quantum algorithms and quantum hardware. Each chapter is meticulously crafted to demystify complex theories, making them accessible to readers with varied backgrounds. Whether you are a seasoned physicist, a computer scientist, a student, or an enthusiast eager to grasp the nuances of quantum computing, this book is designed to cater to your intellectual curiosity.

As we delve deeper into the pages of this book, we will explore the mind-boggling phenomena of superposition and entanglement, concepts that form the bedrock of quantum computation. We will unravel the mysteries of quantum gates and circuits, essential components that enable the processing of quantum information. Moreover, we will venture into the realm of quantum algorithms, where the inherent parallelism of quantum systems promises exponential speedup for solving complex problems in cryptography, optimization, and simulation.

One of the most intriguing aspects of quantum computing is its interdisciplinary nature. Quantum algorithms draw inspiration from diverse branches of mathematics, such as linear algebra and number theory, while quantum hardware necessitates innovations in quantum optics, materials science, and engineering. This interdisciplinarity is reflected in the structure of this book, which seamlessly integrates theoretical foundations with practical applications, providing readers with a holistic understanding of quantum computing's vast landscape.

Additionally, this book explores the transformative impact of quantum computing across various sectors, including finance, healthcare, artificial intelligence, and

cybersecurity. We examine real-world use cases where quantum algorithms promise to revolutionize industries, driving innovation and reshaping the future of technology. Furthermore, we discuss the challenges and ethical implications associated with quantum computing, emphasizing the importance of responsible research and development in this nascent field.

"Quantum Computing: Bridging the Gap to the Future" is not merely a compilation of scientific principles; it is a testament to the limitless potential of human intellect and the relentless pursuit of knowledge. It is an invitation to join the ranks of visionaries and pioneers who are shaping the future of computation. As we embark on this intellectual odyssey, I invite you, dear reader, to explore the wonders of quantum computing, to question the boundaries of classical thought, and to envision a future where the impossible becomes achievable. Together, let us bridge the gap to the future and unravel the mysteries of the quantum universe.

Acknowledgement

I am profoundly grateful as I stand on the precipice of this remarkable publication, **"Quantum Computing: Bridging the Gap to the Future."** This book, a culmination of extensive research, countless hours of dedication, and the collaboration of brilliant minds, would not have been possible without the support and encouragement of numerous individuals and institutions. I express my deepest gratitude to the pioneers of quantum computing, whose groundbreaking work laid the foundation for this transformative technology. My appreciation extends to the scholars, scientists, and researchers whose invaluable contributions have enriched the content of this book. Special thanks are due to the academic institutions and research organizations that provided resources, insights, and collaborative opportunities, fostering an environment where ideas flourished. I extend my heartfelt gratitude to my colleagues and mentors who shared their expertise and enthusiasm, enriching my understanding of this complex field. To my family and friends, whose unwavering support and understanding allowed me the time and space to delve deep into the realms of quantum computing, I am profoundly thankful. This book is a testament to your belief in my abilities and the importance of exploring the frontiers of science. Last but not least, I acknowledge the readers, whose curiosity and quest for knowledge inspire the continuous exploration of quantum computing's vast potential. Your engagement with this material is a testament to the enduring human spirit of discovery and innovation.

Dr. Neha Gupta
Dr. Pankaj Kumar Mishra
Dr. Rahul Kumar Budania

About the Authors

Dr. Neha Gupta did her B.Tech in IT, M.Tech in Software Engineering, Ph.D in SWARM Intelligence from renowned universities. She has more than 17 years of experience in Industry and academics. She is playing many roles in the field of education and administrative positions (IQAC, Convenor, Dy superintendent, Director I/C, HOD , CSR etc)

Her expertise in the areas of Artificial Intelligence, Machine Learning, computer networking, Computer Vision and Natural Language Processing. Her research has contributed to various technical and scientific domains like AI, networking etc. She has published almost 52 research papers in various top-tier conferences and SCOPUS/WOS journals. She has published/granted a few Indian and UK patents and copyrights related to computer science domain . She is also a part of the program/review committee of various conferences and journals,

She is a nodal member of IEI Professional Society and state coordinator (two times) of the Computer Society of India. She is a senior IEEE member and ACM member. She has written a solo author book related to business management in IT, AI Swarm and Basic R programming.

She has been honoured with the Best Faculty award three times from the Insec Society and university. She has taken a few FDPs, webinars and STP in Engineering colleges and Universities.

Dr. Pankaj Kumar Mishra is a highly esteemed academician, administrator, and innovator with an impressive background spanning over two decades of experience in both teaching and managing educational institutions across various learning environments, including conventional, blended, and virtual settings. His leadership in advocating learner-centric and outcome-based education has been instrumental in meeting the needs of 21st-century learners within the higher education sector. Dr. Mishra's dedication to enhancing the learning experience for students is evident from his demonstrated history of working in this sector. In addition to his academic administrator roles, Dr. Mishra is widely respected as an evangelist and independent advisor, providing invaluable guidance to Higher Education Institutions (HEIs) in successfully implementing transformative initiatives such as the New Education Policy, Outcome-Based Education, and the integration of process automation through ERP and LMS solutions. His profound passion for revolutionizing education and commitment to empowering academic institutions drive him to continually make substantial contributions to the advancement of the field. Through his expertise and vision, Dr. Pankaj Kumar Mishra remains an influential force in shaping the future of education

Dr. Rahul Kumar Budania is an accomplished educator with a strong academic background and a wealth of professional experience. Currently serving as an Assistant Professor and Head of the Electronics & Communication Engineering department at Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu (Rajasthan), Dr. Budania is dedicated to fostering knowledge and contributing to organizational success.

Academically, Dr. Budania holds a Ph.D. in Electronics and Communication Engineering from Shri Jagdishprasad Jhabarmal Tibrewala University. His M. Tech in ECE was completed at Pratap University, Jaipur. His journey began with a B. Tech in ECE from Arya Institute of Engineering & Technology, Jaipur, in 2014.

Dr. Budania's scholarly contributions are showcased in his publications. Notably, he has National & International patents and authored various research papers published SCOPUS Journals like mathematical statistician and engineering applications, international journal of mobility technology by ARAI, Journal of Mines, Metal and Fuels etc.

In addition to his research endeavors, Dr. Budania has actively participated in various conferences and workshops, displaying his commitment to continuous learning and professional growth. Some of these events include workshops on LaTeX document preparation, web development, and international conferences on a variety of multidisciplinary subjects.

His dedication to the field is further exemplified by his IAENG (International Association of Engineers) membership, signifying his involvement in the global engineering community.

Outside of his professional pursuits, Dr. Budania is an individual with diverse interests. He enjoys playing and watching cricket and listening to music. As an educator, Dr. Rahul Kumar Budania possesses an impressive academic background, a commitment to research, and a passion for sharing knowledge with others.

Table of Contents

ISBN: 978-81-965655-9-6

1.

Introduction to Quantum Computing

INTRODUCTION TO QUANTUM COMPUTING

Quantum computing is a revolutionary field of study which harnesses the principles of quantum mechanics to develop a new generation of computers with extraordinary capabilities. Unlike classical computers that rely on bits, quantum computers utilize qubits, which can exist in a superposition of states, simultaneously representing 0 and 1. This unique property, along with quantum entanglement, enables quantum computers to perform computations that are exponentially faster than their classical counterparts.

Quantum computing holds immense potential to revolutionize various industries, from drug discovery to materials science. By simulating complex molecular interactions and optimizing material properties, quantum computers can accelerate scientific breakthroughs and lead to the development of innovative products. Furthermore, quantum algorithms can tackle optimization problems and break modern encryption methods, paving the way for enhanced optimization techniques and a paradigm shift in cybersecurity.

Despite its immense potential, quantum computing is still in its nascent stage. Building and maintaining quantum computers are a complex and expensive endeavor, and the field faces challenges such as decoherence, which causes qubits to lose their superposition states. Nevertheless, with continuous research and development, quantum computing is poised to transform the technological landscape and usher in a new era of computational power.

Key Components:

1. **Quantum Mechanics Overview:**

- **Wave-Particle Duality**: Explaining the dual nature of quantum particles, which can exhibit both wave-like and particle-like behavior.
- **Superposition:** Describing the ability of quantum systems to exist in multiple states simultaneously, a fundamental concept crucial to quantum computing.
- **Entanglement:** Detailing the phenomenon where particles become correlated in such a way that the state of one particle instantaneously influences the state of another, regardless of distance.

2. **Classical vs Quantum Computing:**

- **Binary System vs Quantum Bits (Qubits):** Contrasting classical bits, which exist in a state of 0 or 1, with qubits, which can exist in a superposition of both states.
- **Quantum Parallelism**: Explaining how quantum computers can process multiple possibilities at once, enabling them to solve certain problems exponentially faster than classical computers.

3. **Quantum Gates and Circuits:**

- **Quantum Gates**: Introducing basic quantum gates (e.g., Hadamard, CNOT) that manipulate qubits, analogous to classical logic gates but with unique quantum properties.
- **Quantum Circuits**: Describing the arrangement of quantum gates to perform specific computations, demonstrating the quantum parallelism and entanglement effects.

4. **Quantum Algorithms:**

- **Shor's Algorithm:**

Shor's algorithm, developed by Peter Shor in 1994, is a groundbreaking quantum algorithm that efficiently factors large integers into their prime factors. It revolutionized the field of

cryptography, as it poses a significant threat to the security of widely used encryption systems, such as RSA, which rely on the difficulty of factoring large numbers using classical computers.

The algorithm exploits the unique properties of quantum mechanics, particularly quantum parallelism and interference, to achieve an exponential speedup over classical factoring algorithms. This means that a quantum computer, once fully developed, could factor large numbers in a matter of seconds, while a classical computer would take billions of years.

The implications of Shor's algorithm are far-reaching, as it has the potential to break many of the encryption systems that protect sensitive data, such as financial transactions and private communications. This has spurred significant research into developing new encryption methods that are resistant to quantum attacks.

Shor's algorithm is a prime example of the potential of quantum computing to solve problems that are intractable for classical computers, and it stands as a testament to the transformative power of quantum information processing.

- **Grover's Algorithm:**

Grover's algorithm, a pivotal quantum algorithm developed by Lov Grover in 1996, offers a remarkable speedup for searching an unstructured database. While classical algorithms require an average of N/2 iterations to find a specific item among N elements, Grover's algorithm achieves the same task in approximately $\sqrt{N}$ iterations, providing a quadratic speedup.

At its core, Grover's algorithm utilizes the principles of quantum superposition and interference to amplify the probability of finding the desired item. By iteratively applying a sequence of quantum operations, the algorithm gradually increases the amplitude of the target item's state while suppressing the amplitudes of non-target states.

This quantum search algorithm holds immense potential for various applications, including database search, pattern matching, and optimization problems. As quantum computers continue to evolve, Grover's algorithm is expected to play a crucial role in revolutionizing data search and processing.

5. Quantum Error Correction:

- **Quantum Decoherence**:

Quantum decoherence is a phenomenon that poses a significant challenge for quantum computing. It refers to the loss of quantum information due to interactions with the surrounding environment, causing qubits, the basic units of quantum information, to lose their delicate quantum states.

To address this issue, quantum error correction (QEC) techniques have been developed. QEC aims to protect quantum information from decoherence and other errors, ensuring the integrity of quantum computations.

One approach to QEC involves encoding quantum information across multiple physical qubits, creating a logical qubit. This redundancy allows for error detection and correction, as errors affecting individual physical qubits can be identified and corrected without compromising the overall logical qubit state.

Another approach involves continuous monitoring of qubits and applying corrective operations to counteract the effects of decoherence. This active error correction scheme helps maintain the fidelity of quantum information over time.

QEC is crucial for realizing fault-tolerant quantum computing, enabling reliable and scalable quantum computers capable of solving complex problems that are intractable for classical computers.

- **Quantum Error Correction Codes:**

Quantum Error Correction Codes (QECCs) are sophisticated techniques designed to safeguard quantum information from the detrimental effects of noise and errors that arise in quantum systems. Analogous to classical error correction codes, QECCs aim to preserve the integrity of quantum data by encoding it in a redundant manner, allowing for the detection and correction of errors without compromising the underlying quantum state.

QECCs are crucial for the development of reliable quantum computers, as they mitigate the inherent fragility of quantum systems, which are susceptible to environmental disturbances and decoherence. By employing QECCs, quantum computations can be performed with greater accuracy and robustness, paving the way for practical quantum computing applications.

Several types of QECCs have been developed, each with unique properties and error-correction capabilities. Some notable examples include the Shor code, Steane code, and surface code. These codes utilize various encoding schemes and error-detection strategies to protect quantum information from various types of noise and errors.

The development of QECCs is an active area of research, as scientists strive to create more efficient and versatile codes that can handle a wider range of errors and operate under more realistic noise conditions. As quantum computing technology advances, QECCs will play an increasingly critical role in ensuring the reliability and scalability of quantum computers.

Understanding Quantum Mechanics

Quantum mechanics, a revolutionary branch of physics, unveils a fascinating and counterintuitive world at the heart of matter and energy. It probes the realm of atoms and subatomic particles, where the familiar rules of classical physics give way to a new set of principles that govern the behavior of particles and waves.

Unlike classical physics, which describes objects as having definite positions and velocities, quantum mechanics introduces the concept of wave-particle duality, where particles can exhibit both wave-like and particle-like properties. This duality is exemplified by the famous double-slit experiment, where electrons, traditionally considered particles, can interfere with themselves like waves.

Quantum mechanics also introduces the concept of superposition, where a particle can exist in multiple states simultaneously until a measurement is made, collapsing it into a single state. This probabilistic nature of quantum mechanics challenges our conventional understanding of reality and has profound implications for the interpretation of quantum phenomena.

Another mind-boggling aspect of quantum mechanics is entanglement, a phenomenon where two or more particles become inextricably linked, sharing a common fate even when separated by vast distances. This connection allows for instantaneous communication between entangled particles, defying the limitations of classical physics and raising intriguing questions about the nature of reality.

Quantum mechanics has revolutionized our understanding of the universe, providing a framework for explaining phenomena that classical physics cannot. Its applications span a wide range of fields, from lasers and transistors to medical imaging and quantum computing. As we continue to explore the quantum realm, we uncover a world of endless possibilities and profound implications for our understanding of the universe.

At the core of quantum mechanics are several key principles:

1. **Wave-Particle Duality:**

Wave-particle duality is a fundamental concept in quantum mechanics that states that matter and energy exhibit both wave-like and particle-like properties depending on the experiment or observation. This seemingly contradictory behavior is a cornerstone of quantum theory and has profound implications for our understanding of the nature of reality.

In the early 20th century, physicists were puzzled by the behavior of light, which sometimes acted like a wave, exhibiting interference and diffraction patterns, and sometimes like a stream of particles, called photons, as observed in the photoelectric effect. This led to the realization that light possesses a dual nature, exhibiting both wave-like and particle-like characteristics.

Later, this duality was extended to matter as well. Electrons, for instance, could behave as particles, as seen in their interactions with electric fields, but also as waves, as demonstrated by the electron diffraction experiments. This led to the conclusion that all matter, including electrons, protons, and other fundamental particles, exhibit wave-particle duality.

Wave-particle duality is a counterintuitive concept that challenges our classical understanding of the world. It implies that the behavior of matter and energy is not always deterministic and can exhibit both wave-like and particle-like aspects depending on the experimental context. This duality is a fundamental aspect of quantum mechanics and has led to numerous groundbreaking discoveries in physics and other scientific fields.

2. **Superposition:**

In the realm of quantum mechanics, the concept of superposition reigns supreme, defying our classical understanding of the world. It asserts that particles, like mischievous shapeshifters, can simultaneously occupy multiple states or positions until an inquisitive observer intervenes. Imagine an electron, the epitome of quantum quirkiness, existing in a superposition of spin-up and spin-down states concurrently, a duality that defies our conventional perception of reality. This inherent ambiguity, a hallmark of the quantum realm, unveils a world where particles dance to a different tune, defying our expectations and challenging our understanding of the fundamental nature of matter..

3. **Quantization:**

In the realm of quantum mechanics, certain physical properties, like energy and angular momentum, exhibit a remarkable characteristic known as quantization. This means that these properties are not continuous but rather exist in discrete, well-defined values. This quantization is not a mere theoretical concept but manifests itself in various observable phenomena, such as the quantized energy levels of electrons within atoms.

Electrons, the tiny particles that orbit the nucleus of an atom, are not free to occupy any arbitrary energy level. Instead, they are confined to specific, quantized energy states, akin to rungs on a ladder. These quantized energy levels dictate the behavior of electrons and govern the emission and absorption of light by atoms, giving rise to the distinct spectral lines observed in atomic spectroscopy.

The quantization of angular momentum, another fundamental property, is equally profound. Angular momentum, a measure of an object's rotational motion, is also restricted to discrete values. This quantization has far-reaching implications, influencing the behavior of subatomic particles and shaping the structure of atoms and molecules.

The concept of quantization, though counterintuitive to our classical understanding of the world, is a cornerstone of quantum mechanics. It underscores the inherent granularity of the universe at the atomic and subatomic scales, challenging our perception of continuous physical properties.

The implications of quantization extend far beyond atomic phenomena, influencing various fields, including chemistry, materials science, and even cosmology.

4. **Entanglement:**

In the realm of quantum mechanics, a captivating phenomenon known as entanglement links the fates of particles, defying the constraints of distance. Once entangled, particles become intimately connected, their identities intertwined. Measuring the state of one particle instantly reveals the state of its distant partner, as if an invisible thread transmits information across the vast expanse of space.

This perplexing connection, coined "spooky action at a distance" by Einstein, challenges our conventional understanding of locality and causality. It suggests that the universe operates on a deeper level of interconnectedness, where particles, despite their separation, remain in constant communication, their fates intertwined in a cosmic dance of quantum entanglement.

5. **Uncertainty Principle:**

In the realm of quantum mechanics, a fundamental principle reigns supreme: the uncertainty principle. Introduced by Werner Heisenberg, this principle asserts that the precise measurement of both a particle's position and momentum is an unattainable feat. The more accurately we try to pin down one property, the more elusive the other becomes. This inherent uncertainty lies at the heart of quantum mechanics, challenging our classical notions of predictability and determinism.

Imagine a subatomic particle, a tiny denizen of the quantum world. If we attempt to measure its position with great precision, we inevitably disturb its momentum, rendering it impossible to determine accurately. Conversely, if we focus on measuring the particle's momentum with high precision, we sacrifice the ability to pinpoint its exact location. This tradeoff, enshrined in the uncertainty principle, reveals a fundamental limit to our knowledge of the quantum world.

The implications of the uncertainty principle extend far beyond mere measurements. It challenges our perception of reality at the smallest scales, suggesting that particles exist in a probabilistic haze, their properties defined by a range of possibilities rather than fixed values. This inherent uncertainty is a cornerstone of quantum mechanics, shaping our understanding of the behavior of matter at the atomic and subatomic levels.

The uncertainty principle serves as a reminder that the quantum world operates under different rules than our macroscopic world. It forces us to abandon the notion of absolute certainty and embrace the probabilistic nature of reality at its most fundamental level. This principle has profound implications for various fields, from quantum physics and chemistry to nanotechnology and even philosophy.

In essence, the uncertainty principle unveils the inherent limitations of our ability to fully comprehend and predict the behavior of particles in the quantum realm. It stands as a testament to the enigmatic nature of quantum mechanics, challenging our classical intuitions and revealing the probabilistic underpinnings of reality at its smallest scales.

6. **Quantum States and Wave Functions:**

In the realm of quantum mechanics, the behavior of particles is governed by wave functions, mathematical descriptions that encapsulate the probabilities of finding a particle in various states. These wave functions undergo a continuous evolution dictated by Schrödinger's equation, a fundamental principle that governs the dynamics of quantum systems.

Essentially, wave functions serve as a probabilistic map, outlining the likelihood of a particle's existence in different locations or energy levels. As time progresses, these wave functions

transform according to Schrödinger's equation, mirroring the dynamic nature of quantum systems.

In essence, Schrödinger's equation acts as a guide, steering the wave function's evolution and, consequently, determining the behavior of quantum particles. It is through this equation that we can predict and comprehend the intricate workings of the quantum world.

Classical vs Quantum Computing: A Comparative Overview

1. Introduction to Classical Computing:

- **Explanation of classical bits and binary system.**

In the realm of computing, classical bits serve as the fundamental building blocks of information. These bits, often represented as 0s and 1s, form the basis of the binary system, a numerical representation that underpins the operation of modern computers.

The binary system, unlike the decimal system we use in everyday life, operates with just two digits: 0 and 1. Each digit in a binary number holds a specific value based on its position, much like the decimal system. However, instead of powers of 10, the binary system utilizes powers of 2.

For instance, the binary number 1011 can be interpreted as follows:

- The rightmost digit, 1, represents 2^0, which equals 1.
- The next digit to the left, 1, represents 2^1, which equals 2.
- The third digit, 0, represents 2^2, which equals 4, but since it's a 0, it contributes nothing to the overall value.
- The leftmost digit, 1, represents 2^3, which equals 8.

Summing up these values, we get 1 + 2 + 0 + 8 = 11 in the decimal system.

The binary system's simplicity and reliability make it ideal for computers, as it allows for efficient data storage and manipulation. By combining numerous bits, computers can represent a vast range of numbers, characters, and instructions.

In essence, classical bits and the binary system form the backbone of modern computing, enabling the storage, processing, and transmission of information in a language that computers can understand and manipulate.

- **Overview of classical logic gates (AND, OR, NOT) and classical circuits.**

Classical logic gates, the fundamental building blocks of digital circuits, are electronic devices that perform logical operations on one or more input signals to produce a single output signal. These gates operate on binary values, represented as 0 (low voltage) and 1 (high voltage).

The AND gate produces a high output (1) only if both inputs are high (1). It symbolizes the logical conjunction, meaning both conditions must be true for the output to be true.

The OR gate produces a high output (1) if either input is high (1). It represents the logical disjunction, indicating that at least one condition must be true for the output to be true.

The NOT gate, also known as an inverter, produces the opposite output of its input. It symbolizes logical negation, flipping the input value.

These basic gates can be combined to create more complex circuits, performing intricate logical operations. Classical circuits, composed of interconnected logic gates, form the backbone of digital systems, enabling tasks like arithmetic operations, data processing, and control signaling.

Their applications span across various fields, including computers, communication systems, and control systems, making them indispensable components of modern electronics.

- **Understanding how classical computers process information using algorithms and sequential operations.**

Classical computers, the workhorses of the modern digital age, process information using a combination of algorithms and sequential operations. Algorithms, the heart of computation, are precise, step-by-step instructions that guide the computer through a series of actions to achieve a specific outcome. These instructions, meticulously crafted by programmers, encompass a wide range of tasks, from simple arithmetic calculations to complex data manipulations.

Sequential operations, the backbone of classical computing, dictate that instructions are executed one after another in a predefined order. This sequential nature ensures that each step is completed before moving on to the next, guaranteeing the integrity of the computation. The computer's central processing unit (CPU) diligently executes these instructions, orchestrating the flow of information through the system's memory and components.

The interplay between algorithms and sequential operations forms the foundation of classical computing. Algorithms provide the blueprint for solving problems, while sequential operations ensure the orderly execution of these instructions. This synergy empowers classical computers to tackle a vast array of tasks, from mundane calculations to sophisticated simulations, shaping the digital landscape we experience today.

2. Introduction to Quantum Computing:

- **Explanation of quantum bits (qubits) and quantum superposition.**

In the realm of quantum computing, a qubit, short for quantum bit, is the fundamental unit of information. It is analogous to the classical bit in traditional computers but goes beyond the simple binary states of 0 and 1. Qubits leverage the principles of quantum mechanics to exist in a superposition, a unique state where they can simultaneously represent both 0 and 1 or any combination of these states.

This superposition empowers qubits with the remarkable ability to process multiple possibilities simultaneously, a stark contrast to classical bits that can only represent a single value at a time. This inherent parallelism makes quantum computers immensely powerful, enabling them to tackle complex problems that would be intractable for classical computers.

Quantum superposition is the cornerstone of quantum computing, opening up a world of possibilities that were previously unimaginable. It allows quantum algorithms to explore multiple solutions concurrently, leading to exponential speedups in computation compared to classical methods. The implications of this technology span a wide range of fields, from drug discovery and materials science to financial modeling and artificial intelligence.

As quantum computing continues to evolve, the power of qubits and their ability to harness superposition will pave the way for groundbreaking advancements in various domains. This technology holds the potential to revolutionize industries and transform the way we interact with the world around us.

- **Introduction to quantum gates and quantum circuits.**

Quantum gates are the fundamental building blocks of quantum circuits, analogous to classical logic gates in conventional computers. They manipulate the quantum states of qubits, the basic unit of quantum information. Unlike classical bits, which can only represent 0 or 1, qubits can exist in a superposition of both states simultaneously, enabling powerful parallel computations.

Quantum circuits are a graphical representation of quantum algorithms, depicting the sequence of quantum gates applied to qubits. They provide a visual representation of the operations performed on qubits, much like electrical circuits depict the flow of electrons.

Common quantum gates include the Pauli-X (NOT) gate, which flips the state of a qubit, and the Hadamard gate, which creates a superposition of states. Two-qubit gates, such as the CNOT (controlled-NOT) gate, introduce entanglement, a unique quantum phenomenon that links the states of two qubits, enabling non-local correlations.

Quantum circuits are constructed by connecting quantum gates, forming a network of operations on qubits. They are executed on quantum computers, which physically implement the gates and manipulate the qubits.

The development of quantum algorithms and the design of efficient quantum circuits are crucial for harnessing the power of quantum computers to solve complex problems in various fields, including cryptography, drug discovery, and materials science

- **Basic principles of quantum mechanics, such as wave-particle duality and quantum entanglement, that enables quantum computation.**

Quantum mechanics, a field that explores the behavior of matter at the atomic and subatomic levels, provides the foundation for quantum computation. The two fundamental principles of wave-particle duality and quantum entanglement play a crucial role in enabling this revolutionary technology.

Wave-particle duality, a cornerstone of quantum mechanics, asserts that particles, such as electrons and photons, exhibit both wave-like and particle-like properties. This duality allows quantum bits, or qubits, to exist in a superposition state, simultaneously representing both 0 and 1, unlike classical bits that can only be either 0 or 1. This superposition enables quantum computers to perform computations on multiple values simultaneously, leading to an exponential increase in processing power.

Quantum entanglement, another key principle, describes a phenomenon where two or more qubits become inextricably linked, sharing a single quantum state. This connection persists even when the qubits are separated by vast distances. Entanglement allows quantum computers to perform operations on multiple qubits simultaneously, regardless of their physical separation, opening up possibilities for parallel processing and secure communication.

The synergistic effects of wave-particle duality and quantum entanglement form the basis of quantum computation, paving the way for groundbreaking advancements in fields like drug discovery, materials science, and cryptography. Quantum computers, empowered by these principles, hold the potential to revolutionize computation and reshape the technological landscape

3. Comparative Analysis:

- **Speed and Parallelism:**

Speed and parallelism are two fundamental concepts in computing that are often intertwined but have distinct implications for performance.

Speed, often measured in terms of clock frequency or execution time, refers to how quickly a single processing unit can execute instructions. It is a measure of sequential processing efficiency.

Parallelism, on the other hand, focuses on dividing a computational task into multiple smaller subtasks that can be executed simultaneously across multiple processing units. It is a measure of concurrent processing capability.

The relationship between speed and parallelism is not always straightforward. A faster processor can execute a single task more quickly, but it may not necessarily be more efficient for tasks that can be parallelized.

In such cases, a system with multiple slower processors, if properly utilized, can outperform a single faster processor by dividing the workload and executing subtasks concurrently.

Therefore, the choice between prioritizing speed or parallelism depends on the nature of the computational tasks and the architecture of the computing system. For tasks that are inherently sequential, speed is crucial. However, for tasks that can be effectively parallelized, increasing the degree of parallelism can significantly improve overall performance.

In conclusion, while speed and parallelism are both important factors in computing performance, their relative importance depends on the specific computational context. Understanding the characteristics of the tasks and the capabilities of the hardware is essential for optimizing performance.

- **Quantum Entanglement vs Classical Correlation:**

Quantum entanglement and classical correlation are both types of correlations between two or more particles, but they differ in their fundamental nature and implications.

Classical correlation arises from shared properties or interactions between particles, where the state of one particle can be inferred from the state of the other. This correlation is limited by the speed of light, as information cannot travel faster than light.

Quantum entanglement, on the other hand, is a unique feature of quantum mechanics that defies classical explanations. Entangled particles exhibit a profound interconnectedness, where their properties are inextricably linked, even when separated by vast distances. Measuring the state of one entangled particle instantaneously affects the state of the other, regardless of the distance between them.

This instantaneous correlation in quantum entanglement suggests a profound connection that transcends the limitations of classical physics. It implies a non-local aspect of quantum mechanics, suggesting that entangled particles share a deeper connection that goes beyond our conventional understanding of space and time.

While classical correlation can be explained by local interactions and shared properties, quantum entanglement challenges our classical worldview and suggests a deeper level of interconnectedness in the universe.

- **Quantum Interference and Algorithms:**

Quantum interference and algorithms are two fundamental concepts that lie at the heart of quantum computing, each playing a crucial role in harnessing the unique properties of quantum mechanics to solve complex problems.

Quantum interference refers to the phenomenon where the wave functions of quantum particles interact, leading to constructive or destructive interference patterns. This interference can be exploited to amplify desired outcomes and suppress unwanted ones, forming the basis for many quantum algorithms.

Quantum algorithms, on the other hand, are a set of instructions designed to operate on quantum computers, utilizing quantum phenomena like superposition and entanglement to achieve significant speedups over classical algorithms.

Comparing quantum interference and algorithms reveals a close relationship. Quantum interference serves as a fundamental principle that enables the development of efficient quantum

algorithms. Many quantum algorithms, such as Grover's search algorithm and Shor's factoring algorithm, rely on quantum interference to achieve their remarkable performance.

In essence, quantum interference provides the underlying mechanism that empowers quantum algorithms to outperform their classical counterparts. By understanding and manipulating quantum interference, researchers can design novel quantum algorithms with the potential to revolutionize various fields, from cryptography to drug discovery.

- **Error Correction and Fault Tolerance:**

Error correction and fault tolerance are two closely related concepts that play a crucial role in ensuring the reliability of computing systems, particularly in the context of quantum computing. While both aim to mitigate the effects of errors and maintain the integrity of computations, they differ in their scope and approach.

Error correction focuses on detecting and correcting errors that occur during data transmission or storage. It employs various techniques, such as error-correcting codes, to identify and rectify corrupted bits of information, ensuring the accuracy of the transmitted or stored data.

Fault tolerance, on the other hand, addresses the broader issue of system failures, including hardware malfunctions, software errors, and environmental disturbances. It encompasses a range of strategies, such as redundancy and error detection mechanisms, to prevent system crashes and maintain continuous operation even in the presence of faults.

In essence, error correction acts as a fine-grained mechanism that focuses on correcting individual errors at the data level, while fault tolerance adopts a more comprehensive approach, ensuring the overall resilience of the system against various types of failures.

In the context of quantum computing, error correction is particularly critical due to the inherent fragility of quantum states. Quantum error correction codes are designed to protect quantum information from decoherence and other errors, enabling reliable quantum computations.

Fault tolerance in quantum computing involves building systems that can function correctly even when individual components fail. This requires sophisticated error correction techniques and architectural designs that can handle errors without compromising the integrity of quantum computations.

The development of robust error correction and fault tolerance mechanisms is essential for realizing the full potential of quantum computing, enabling the construction of reliable and scalable quantum computers capable of solving complex problems that are intractable for classical computers.

- **Quantum vs Classical Cryptography:**

Quantum cryptography and classical cryptography both aim to protect sensitive information, but they differ fundamentally in their underlying principles and security guarantees.

Classical cryptography relies on mathematical algorithms to encrypt data, making it difficult for unauthorized parties to decrypt. However, its security is based on the assumption that these algorithms are computationally infeasible to break, which could become vulnerable to future advances in computing power or mathematical breakthroughs.

Quantum cryptography, on the other hand, leverages the principles of quantum mechanics to achieve unconditional security. It utilizes the properties of quantum states, such as superposition and entanglement, to create a secure communication channel that is fundamentally immune to eavesdropping or interception.

Here's a comparative analysis of quantum and classical cryptography:

Security: Quantum cryptography offers unconditional security, meaning it is theoretically unbreakable even with unlimited computational power. Classical cryptography's security is based on computational complexity, which could be compromised by future advances in computing.

Key distribution: Quantum Key Distribution (QKD) allows for secure key exchange over a quantum channel, ensuring that the key cannot be intercepted or copied without detection. Classical cryptography relies on secure key exchange protocols, but these are susceptible to man-in-the-middle attacks.

Implementation: Quantum cryptography is still in its early stages of development, and its implementation is more complex and expensive compared to classical cryptography. Classical cryptography is widely used and has a mature infrastructure.

Applications: Quantum cryptography is particularly suited for highly sensitive communications, such as government and military applications. Classical cryptography is used for a wide range of applications, including internet security, financial transactions, and data protection.

In summary, quantum cryptography represents a paradigm shift in secure communication, offering unconditional security based on the fundamental laws of physics. While still in its early stages, it holds immense potential for protecting sensitive information in the quantum era.

4. Limitations and Challenges:

A comparative analysis between limitations and challenges delves into the distinctions and interrelationships between these two concepts. While often used interchangeably, limitations and challenges represent distinct aspects of a situation or endeavor.

Limitations are inherent constraints or restrictions that define the boundaries of what is possible or achievable. They are often predetermined factors that cannot be readily altered or overcome. For instance, technological limitations may restrict the capabilities of a device or process, while financial limitations may constrain the scope of a project.

Challenges, on the other hand, are obstacles or difficulties that arise during the pursuit of a goal or objective. They are not inherent constraints but rather hurdles that require effort, innovation, or strategic planning to overcome. For example, a company may face challenges in penetrating a new market or developing a novel product.

Despite their differences, limitations and challenges are often interconnected. Limitations can give rise to challenges, as individuals or organizations strive to work within or overcome those constraints. Conversely, successfully addressing challenges can lead to the expansion of boundaries and the mitigation of limitations.

A comprehensive understanding of both limitations and challenges is essential for effective decision-making and strategic planning. By recognizing and addressing limitations, individuals and organizations can set realistic expectations and optimize their efforts within those constraints. Likewise, proactively identifying and tackling challenges can lead to innovation, growth, and the expansion of possibilities.

5. Potential Applications and Synergies:

A comparative analysis between potential applications and synergies delves into the intricate relationship between different applications and the synergistic benefits that emerge from their interactions. It involves identifying and evaluating the potential applications of a particular

technology, methodology, or concept, and then assessing the synergistic effects that arise when these applications are combined or integrated.

The analysis aims to uncover the potential for enhanced outcomes and greater value creation when different applications are brought together. It explores how the strengths and capabilities of individual applications can complement each other, leading to amplified benefits that exceed the sum of their individual contributions.

By conducting a comparative analysis, one can identify opportunities for strategic collaboration, resource optimization, and innovation. It enables decision-makers to prioritize applications that not only have intrinsic value but also contribute to a broader synergistic ecosystem.

The analysis also highlights potential challenges and trade-offs that may arise when integrating different applications. It provides insights into potential conflicts or incompatibilities that need to be addressed to ensure seamless integration and maximize synergistic benefits.

In essence, a comparative analysis between potential applications and synergies serves as a roadmap for leveraging the combined strengths of different applications, fostering innovation, and achieving outcomes that surpass what could be achieved in isolation.

Quantum Bits (Qubits) and Superposition

In classical computing, the basic unit of information is the bit, which can represent either a 0 or a 1. However, in quantum computing, the fundamental unit of information is the quantum bit, or qubit. Unlike classical bits, qubits can exist in multiple states simultaneously, a phenomenon known as superposition. This unique property is a result of the principles of quantum mechanics.

1. **Qubits: The Building Blocks of Quantum Information**

- **Quantum States:** Qubits can exist in multiple quantum states simultaneously, represented as a combination of 0 and 1, known as alpha ($|0\rangle$) and beta ($|1\rangle$) states.
- **Superposition:** Qubits can be in a superposition of both 0 and 1 states at the same time, allowing for parallel processing of information.
- **Measurement:** When a qubit is measured, it collapses from a superposition of states to a definite state (0 or 1) with a certain probability, as determined by the coefficients of its superposition.

2. **Superposition: The Power of Parallelism**

- **Parallel Computation:** Qubits in superposition can perform multiple calculations simultaneously, exponentially increasing the computational power of a quantum system.
- **Quantum Parallelism:** Quantum algorithms leverage superposition to explore multiple solutions at once, providing significant speedup for specific problem-solving tasks.
- **Complex Problem Solving:** Superposition enables quantum computers to efficiently handle complex problems, such as factorizing large numbers and searching unsorted databases, which are computationally infeasible for classical computers.

3. **Quantum Gates and Superposition**

- **Manipulating Qubits:** Quantum gates are operations that manipulate qubits. These gates can create, modify, or analyze superposition states.
- **Creating Superposition:** Hadamard gate is a fundamental quantum gate used to create a superposition of states, putting qubits into an equal probability combination of 0 and 1.

- **Entangling Qubits:** Quantum gates can also create entanglement between qubits, a phenomenon where the state of one qubit instantaneously influences the state of another, leading to powerful quantum correlations.

4. Quantum Algorithms Exploiting Superposition

- **Grover's Algorithm:** Utilizes superposition to perform an unstructured search in an unordered database, providing a quadratic speedup compared to classical algorithms.
- **Quantum Fourier Transform:** Essential in Shor's Algorithm, it efficiently performs modular exponentiation, enabling fast factorization of large numbers, which has implications for cryptography.
- **Variational Quantum Algorithms:** Combine classical and quantum processing, leveraging superposition for optimization tasks, machine learning, and material simulations.

Understanding qubits and superposition is foundational to harnessing the immense potential of quantum computing. These concepts underpin the development of quantum algorithms and technologies, paving the way for solving complex problems that were once considered insurmountable for classical computers.

Application of Quantum Computing

Quantum computing holds the potential to revolutionize various fields by solving complex problems that are practically impossible for classical computers to handle efficiently. Here are some applications of quantum computing:

1. Cryptography:

Quantum computing can break widely used encryption algorithms, but it can also enhance security through quantum cryptography techniques like quantum key distribution (qkd), ensuring secure communication.

2. Optimization problems:

Quantum computing can optimize complex systems and processes, which is valuable in logistics, supply chain management, financial modeling, and even drug discovery. Quantum algorithms can find optimal solutions faster than classical algorithms for large-scale optimization problems.

3. Drug discovery and material science:

Quantum computers can simulate molecular and atomic interactions accurately. This capability aids in drug discovery by modeling complex biological systems and understanding molecular interactions. Similarly, it helps in designing new materials with specific properties, revolutionizing material science.

4. Machine learning and ai:

Quantum computing can enhance machine learning algorithms. Quantum machine learning algorithms have the potential to process and analyze vast datasets, leading to more efficient ai models and predictions.

5. Weather forecasting and climate modeling:

Quantum computers can simulate complex climate models and predict weather patterns more accurately. This can significantly improve our understanding of climate change and help in developing strategies to mitigate its effects.

6. Financial modeling:

Quantum computing can optimize portfolios, model complex financial systems, and perform risk analysis more effectively than classical computers. This is crucial for investment strategies and risk management in the financial sector.

7. Supply chain and logistics:
Quantum algorithms can optimize supply chain and logistics operations, leading to more efficient routes, reduced costs, and better resource utilization. This is particularly important for large-scale distribution networks.

8. Traffic optimization:
Quantum computing can optimize traffic flow in cities, leading to reduced congestion, shorter commuting times, and overall more efficient transportation systems.

9. Artificial intelligence:
Quantum computing can enhance ai algorithms, especially in tasks involving large datasets and complex pattern recognition. Quantum neural networks have the potential to revolutionize ai capabilities.

10. Space exploration:
Quantum computing can assist in analyzing vast amounts of data collected from space missions, simulate space environments accurately, and contribute to the development of advanced propulsion systems.

11. Cybersecurity:
Quantum computing can improve cybersecurity through the development of quantum-resistant encryption methods. Quantum key distribution ensures secure communication channels, making it practically impossible for hackers to intercept messages.

12. Genomics and personalized medicine:
Quantum computing can analyze vast genomic datasets, aiding in understanding genetic variations, disease origins, and personalized medicine. This could lead to more targeted and effective treatments.

It's important to note that practical, large-scale quantum computers are still in the experimental stage. Research and development in this field are ongoing, and as quantum technology advances, these applications are expected to become more prevalent and impactful.

ISBN: 978-81-965655-9-6

2.

Quantum Computing Fundamentals

QUANTUM COMPUTING FUNDAMENTALS

Quantum computing is a revolutionary field that harnesses the principles of quantum mechanics to perform computations, holds immense potential to revolutionize various industries. Unlike classical computers that store information in bits, quantum computers utilize quantum bits or qubits, capable of representing both 0 and 1 simultaneously, a concept known as superposition. This unique property, along with entanglement, where qubits can be linked, enabling them to influence each other's states, empowers quantum computers to tackle complex problems that classical computers struggle with.

Quantum algorithms, tailored for quantum computers, offer significant speedups compared to classical algorithms. Shor's algorithm, for instance, can efficiently factor large numbers, a task that is computationally intensive for classical computers. Grover's algorithm excels at searching unstructured data, providing a quadratic speedup over classical algorithms.

Despite its immense potential, quantum computing is still in its nascent stages, facing challenges such as decoherence, where qubits lose their superposition state due to environmental interference. Nevertheless, with continuous research and development, quantum computing is poised to transform fields like drug discovery, materials science, and cryptography, ushering in a new era of technological advancement.

Key Components:

1. **Quantum Bits (Qubits) and Superposition:**
   - Explanation of qubits, the basic unit of quantum information.
   - Exploration of the concept of superposition, where qubits can exist in multiple states simultaneously, unlike classical bits.
2. **Quantum Gates and Circuits:**
   - Introduction to quantum gates, which are analogous to classical logic gates but operate with quantum bits.
   - Explanation of quantum circuits, which are arrangements of quantum gates used for performing computations.
3. **Quantum Entanglement:**
   - Definition and exploration of entanglement, a quantum phenomenon where qubits become correlated in such a way that the state of one qubit instantaneously influences the state of another, regardless of the distance between them.
4. **Quantum Algorithms:**
   - Overview of fundamental quantum algorithms such as Shor's Algorithm (for integer factorization) and Grover's Algorithm (for unstructured search), highlighting their significance and applications.
   - Discussion on how these algorithms exploit quantum parallelism and entanglement to outperform classical algorithms in specific tasks.
5. **Quantum Error Correction:**
   - Explanation of quantum error correction codes, which are essential for mitigating the effects of noise and decoherence in quantum computations.
   - Description of techniques like the surface code and the role of quantum error correction in building fault-tolerant quantum computers.

Quantum computing is a branch of computing that utilizes principles from quantum mechanics to perform operations on data. Unlike classical computers, which use bits to represent information as 0s and 1s, quantum computers use quantum bits, or qubits. Qubits can exist in multiple states at once, thanks to a property called superposition, and they can be entangled, meaning the state of one qubit is directly related to the state of another, even if they are physically separated. These properties give quantum computers the potential to solve certain problems much more efficiently than classical computers.

Here are some fundamental concepts in quantum computing:

1. Qubits:
Qubits are the basic units of quantum information. They can be in a state of 0, 1, or both 0 and 1 simultaneously due to superposition. This property allows quantum computers to perform multiple calculations at the same time.

2. Superposition:
Superposition is a fundamental principle in quantum mechanics where a particle can exist in multiple states simultaneously. In the context of quantum computing, qubits can be in a superposition of 0 and 1 until measured, allowing quantum computers to explore multiple solutions at once.

3. Entanglement:
Entanglement is a quantum phenomenon where the states of two or more qubits become correlated in such a way that the state of one qubit is directly related to the state of another, even if they are physically separated by large distances. Entanglement enables the creation of complex quantum states and is essential for quantum algorithms like quantum teleportation and quantum cryptography.

4. Quantum Gates:
Quantum gates are the equivalent of classical logic gates in quantum computing. They perform operations on qubits, manipulating their states. Quantum gates, combined with superposition and entanglement, allow the construction of quantum circuits to perform specific computations.

5. Quantum Circuits:
Quantum circuits are sequences of quantum gates applied to qubits. These circuits are designed to perform specific calculations. Quantum algorithms, such as Shor's algorithm and Grover's algorithm, are implemented using quantum circuits.

6. Quantum Parallelism:
Quantum parallelism refers to the ability of quantum computers to perform many calculations simultaneously. Due to superposition, a quantum computer with n qubits can represent 2^n possible states, allowing it to explore a vast solution space in parallel.

7. Quantum Interference:
Quantum interference is a phenomenon where the probability amplitudes of different quantum states can interfere constructively or destructively. Quantum algorithms exploit interference patterns to enhance the likelihood of correct answers and cancel out incorrect ones.

8. Quantum Decoherence:
Quantum decoherence refers to the loss of quantum coherence, leading to the degradation of quantum states. It is a significant challenge in building practical quantum computers because maintaining qubits in a coherent state for a sufficiently long time is essential for performing accurate computations.

9. Quantum Error Correction:
Quantum error correction codes are essential for protecting quantum information from errors due to decoherence and other noise in quantum systems. Quantum error correction algorithms ensure the reliability of quantum computations.

Understanding these fundamental concepts is crucial for anyone interested in working with or studying quantum computing, as they form the basis for the development of quantum algorithms and the design of quantum hardware.

Quantum Gates and Circuits:
Quantum gates and circuits are the fundamental building blocks of quantum computation, analogous to logic gates and circuits in classical computation. Unlike classical gates that operate on bits, quantum gates manipulate qubits, the basic unit of quantum information. Qubits can exist in a superposition of states, allowing for a richer and more complex computational landscape.

Quantum gates are represented by unitary matrices that transform the quantum state of qubits. Common gates include the Hadamard gate, which creates superpositions, and the CNOT gate, which entangles qubits. These gates, along with others, form a universal set, meaning any quantum computation can be decomposed into a sequence of these gates.

Quantum circuits are arrangements of quantum gates that perform specific computational tasks. They are depicted as diagrams with lines representing qubits and boxes representing gates. The order of gates in the circuit determines the overall transformation applied to the qubits.

The power of quantum circuits lies in their ability to harness quantum phenomena like superposition and entanglement to solve problems intractable for classical computers. Quantum algorithms, expressed as quantum circuits, have the potential to revolutionize fields like cryptography, drug discovery, and materials science.

In summary, quantum gates and circuits form the essential framework for quantum computation, enabling the manipulation of qubits and the execution of quantum algorithms. Their unique properties hold immense promise for unlocking the full potential of quantum computers.

Here's a breakdown of the key components of this topic:

Quantum Bits (Qubits):
In the realm of computing, classical bits and qubits represent fundamental units of information, but they differ significantly in their capabilities and potential. Classical bits, the building blocks of traditional computers, can only exist in one of two distinct states: 0 or 1. This binary nature forms the basis for all digital operations, allowing classical computers to perform calculations, store data, and execute programs.

Qubits, on the other hand, introduce a revolutionary concept to computing: superposition. Unlike their classical counterparts, qubits can exist in multiple states simultaneously, not just 0 or 1. This extraordinary property arises from the principles of quantum mechanics, where particles can exhibit wave-like behavior and exist in a probabilistic state.

Due to superposition, qubits can represent a complex blend of 0 and 1, effectively encompassing a vast range of information within a single unit. This remarkable feature opens up a world of possibilities for quantum computers, enabling them to tackle problems that are intractable for classical machines.

With the power of superposition, quantum computers can perform parallel computations on a massive scale, explore vast solution spaces simultaneously, and break through the limitations of classical algorithms. While still in their early stages of development, quantum computers hold

immense promise for fields like cryptography, drug discovery, and materials science, where their ability to harness superposition could lead to groundbreaking advancements.

Quantum Gates:
At the heart of quantum computing lie unitary operations, the fundamental building blocks that manipulate and transform quantum information. These operations are represented as unitary matrices, mathematical constructs that encapsulate the precise changes a quantum gate imparts on a qubit, the basic unit of quantum information.

Unitary operations are reversible, a crucial property that distinguishes them from classical operations. This reversibility stems from the fact that unitary matrices preserve the overall probability of the system, ensuring that no information is lost during the transformation. In essence, one can theoretically reverse the operation and retrieve the original qubit state, a feature that enables intricate error correction schemes in quantum computing.

The reversibility of unitary operations also implies that they conserve energy, a fundamental principle in physics. This conservation ensures that quantum computations remain consistent with the laws of nature, further highlighting the deep connection between quantum mechanics and the operation of quantum computers.

Unitary operations form the backbone of quantum algorithms, enabling tasks such as superposition creation, entanglement manipulation, and measurement. These operations are carefully orchestrated to achieve the desired computational outcomes, harnessing the unique properties of quantum mechanics to solve problems that are intractable for classical computers.

- **Types of Quantum Gates:**

1. X, Y, and Z Gates: Similar to classical NOT gates, these gates flip the qubit states.
2. Hadamard (H) Gate: Puts a qubit into a superposition of states.
3. CNOT (Controlled-NOT) Gate: Performs an XOR operation, entangling two qubits.
4. Toffoli (CCNOT) Gate: A three-qubit gate that performs a controlled-controlled-NOT operation.
5. SWAP Gate: Swaps the states of two qubits.

Quantum Circuits:

- **Quantum Circuit Representation:** Quantum circuits are graphical representations of the sequences of quantum gates applied to qubits. Qubits start in a certain state and go through a series of quantum gates, resulting in a final output state.
- **Quantum Circuit Components:**

1. Qubit Lines: Represent individual qubits in the circuit.
2. Quantum Gates: Symbols representing specific quantum operations applied to qubits.
3. Classical Bits: Used for measurement outcomes.
4. Quantum Registers: Arrays of qubits treated as a single entity.

Quantum Gate Applications:

- **Quantum Algorithms:** Quantum gates are combined in specific sequences to create quantum algorithms, such as Shor's Algorithm for integer factorization and Grover's Algorithm for unstructured search problems.

- **Quantum Error Correction:** Quantum gates are also utilized in quantum error correction codes, which are essential for preserving quantum information in the presence of noise and decoherence.

Understanding quantum gates and circuits is crucial for designing quantum algorithms and exploring the full potential of quantum computing in solving complex problems that are intractable for classical computers.

- **Quantum Entanglement**

Quantum entanglement is one of the most intriguing phenomena in quantum mechanics, a branch of physics that deals with the behavior of matter and energy at the smallest scales, such as atoms and subatomic particles. Entanglement occurs when two or more particles become correlated in such a way that the state of one particle instantaneously influences the state of the other(s), regardless of the distance that separates them. This connection happens in a manner that classical physics and our everyday intuition cannot explain.

Here are some key points to understand about quantum entanglement:

1. **Instantaneous Correlation:** When particles become entangled, the state of one particle becomes directly related to the state of another, even if they are separated by vast distances. This correlation happens instantaneously, seemingly violating the classical concept of locality, where distant objects cannot have immediate effects on each other.

2. **Quantum States:** Particles in quantum mechanics do not have definite states until they are measured. Instead, they exist in a state of superposition, meaning they can exist in multiple states at once. Entanglement establishes a special kind of correlation between these states, which is crucial for various quantum technologies and applications.

3. **Bell's Theorem:** Physicist John S. Bell formulated a theorem that describes the statistical properties of entangled particles. Bell's theorem shows that the predictions of quantum mechanics regarding entangled particles cannot be explained by classical theories, suggesting that the world is inherently non-local at the quantum level.

4. **Quantum Information and Computing:** Entanglement plays a vital role in quantum computing and quantum communication. Quantum computers utilize entangled qubits to perform complex calculations at speeds unattainable by classical computers. Quantum key distribution protocols, such as the famous BB84 protocol, rely on entanglement for secure communication.

5. **Quantum Teleportation:** Entanglement is a fundamental concept behind quantum teleportation, a process where the exact state of a quantum system can be transmitted from one location to another, without physically moving the particles themselves. This phenomenon has implications for future communication and data transmission technologies.

6. **Challenges and Paradoxes:** Entanglement has led to various philosophical debates and paradoxes, such as Einstein, Podolsky, and Rosen (EPR) paradox and the violation of Bell inequalities. These discussions have significantly contributed to our understanding of the fundamental nature of quantum mechanics.

Entanglement remains a subject of extensive research and fascination in the field of quantum physics. Its mysterious properties challenge our understanding of the nature of reality, and it continues to be a driving force behind the development of quantum technologies.

- **Quantum Algorithms: Shor's Algorithm, Grover's Algorithm, etc.**

Quantum Algorithms: Shor's Algorithm, Grover's Algorithm, etc.

Quantum algorithms are computational procedures designed to be executed on a quantum computer, taking advantage of the principles of quantum mechanics to perform specific tasks more efficiently than classical algorithms. Two significant quantum algorithms are Shor's Algorithm and Grover's Algorithm, among others, which have profound implications for cryptography and searching tasks, respectively.

1. Shor's Algorithm:
Shor's Algorithm, developed by mathematician Peter Shor in 1994, is a quantum algorithm specifically designed to factor large integers exponentially faster than the best-known classical algorithms. This algorithm has significant implications for cryptography, as many encryption methods rely on the difficulty of factoring large numbers into their prime components. Shor's Algorithm threatens the security of widely used encryption schemes like RSA, making it a critical area of study in quantum computing.

2. Grover's Algorithm:
Proposed by Lov Grover in 1996, Grover's Algorithm addresses the problem of unstructured search. Classical searching algorithms take \(O(N)\) time complexity to find an item in an unsorted database of \(N\) items. Grover's Algorithm, however, can perform this task in \(O(\sqrt{N})\) time complexity, providing a quadratic speedup. While this might not seem groundbreaking for small datasets, for large databases, the speedup is substantial. Grover's Algorithm has applications in database search, password cracking, and optimization problems.

3. Other Quantum Algorithms:
Beyond Shor's and Grover's Algorithms, there are numerous other quantum algorithms designed to tackle various computational problems more efficiently than classical algorithms. For instance:

- **Quantum Simulation Algorithms:** Used to simulate quantum systems, providing insights into the behavior of molecules and materials at the quantum level.

- **Quantum Fourier Transform:** A quantum version of the classical Fourier transform, fundamental in many quantum algorithms, including Shor's Algorithm.

- **Quantum Approximation Algorithms:** Designed to find approximate solutions to optimization problems efficiently.

Understanding these algorithms involves a grasp of quantum gates, superposition, entanglement, and quantum circuits. Quantum algorithms are pivotal in demonstrating the computational power of quantum computers and play a central role in the ongoing research and development of quantum technologies. As quantum computers continue to advance, exploring and refining these algorithms are crucial steps toward harnessing the full potential of quantum computing in various practical applications.

- **Quantum Error Correction**

Quantum error correction is a fundamental concept in the field of quantum computing, essential for building reliable and scalable quantum computers. In the quantum realm, information is stored in quantum bits, or qubits, which, unlike classical bits, can exist in multiple states simultaneously due to the principle of superposition. However, this superposition is delicate and easily affected by various types of errors, such as decoherence and noise from the environment.

Quantum error correction techniques are devised to protect quantum information from these errors and allow quantum computations to be executed accurately. The primary challenge in

quantum error correction arises from the no-cloning theorem, a fundamental principle in quantum mechanics stating that it is impossible to create an exact copy of an arbitrary unknown quantum state.

To overcome this limitation, quantum error correction codes are designed based on the principles of quantum entanglement and superposition. These codes distribute the information across multiple qubits in a way that preserves the information even if individual qubits are corrupted. Quantum error correction involves the use of quantum gates and measurements to detect and correct errors without directly measuring the quantum state itself, as measurement can disrupt the delicate quantum information.

One of the key concepts in quantum error correction is the use of quantum codes like the Shor Code or the Steane Code, which encode logical qubits into larger blocks of physical qubits. These codes are designed to detect and correct errors in a way that ensures the integrity of the encoded quantum information.

Additionally, fault-tolerant quantum computation is a significant area of research within quantum error correction. It aims to create quantum circuits that can perform computations reliably even in the presence of physical errors. This involves using sophisticated algorithms and redundancy to ensure that errors are detected and corrected at every step of the computation.

Quantum error correction is crucial for the development of practical and scalable quantum computers. As quantum technologies advance, researchers continue to explore new and more efficient error correction techniques to make quantum computation more reliable and pave the way for the realization of large-scale quantum algorithms and applications.

ISBN: 978-81-965655-9-6

3.

Quantum Hardware and Technologies

 ISBN: 978-81-965655-9-6

QUANTUM HARDWARE AND TECHNOLOGIES

Quantum Hardware and Technologies

Quantum hardware and technologies encompass the physical components and engineering techniques used to construct quantum computers, devices that harness the principles of quantum mechanics to perform computations. Unlike classical computers that rely on bits, quantum computers utilize qubits, which can exist in a superposition of states, enabling them to tackle complex problems that are intractable for classical computers.

Various qubit technologies are being explored, including superconducting circuits, trapped ions, and photonic systems. Superconducting qubits, fabricated using superconducting materials, are among the most promising candidates due to their scalability and compatibility with existing semiconductor manufacturing processes. Trapped ion qubits, where ions are suspended in a vacuum and manipulated using lasers, offer high coherence times and precise control. Photonic qubits, using photons as information carriers, excel in long-distance communication and quantum networking.

Alongside qubit development, quantum hardware engineers face the challenge of maintaining qubit coherence, as qubits are susceptible to noise and decoherence. Cryogenic cooling systems are employed to maintain ultra-low temperatures, minimizing thermal noise and extending qubit lifetimes. Additionally, error correction techniques are being developed to mitigate the effects of decoherence and ensure accurate computations.

Quantum hardware and technologies are still in their early stages, but rapid progress is being made, opening up exciting possibilities for quantum computing applications in fields such as drug discovery, materials science, and artificial intelligence.

Key Aspects:

1. **Quantum Processors:** Quantum processors are the heart of quantum computers. They are designed to manipulate qubits using quantum gates and perform quantum computations. Different types of quantum processors include superconducting qubits, trapped ions, topological qubits, and quantum dots. Each type has its own advantages and challenges in terms of stability, error rates, and scalability.

2. **Quantum Gates and Circuits:** Quantum gates are analogous to logic gates in classical computing but operate on qubits, manipulating their quantum states. Quantum circuits are sequences of quantum gates that perform specific computations. Understanding how quantum gates work and how to design efficient quantum circuits is crucial for quantum algorithm development.

3. **Quantum Entanglement:** Entanglement is a phenomenon in quantum physics where the states of two or more qubits become correlated in such a way that the state of one qubit instantly influences the state of the other(s), regardless of the distance between them. Entanglement is a fundamental resource in quantum computing and is harnessed for various applications, including quantum cryptography and quantum error correction.

4. **Quantum Error Correction:** Quantum information is fragile and susceptible to errors due to decoherence and external disturbances. Quantum error correction codes, such as the surface code, are essential for detecting and correcting errors in quantum computations. Developing reliable error correction techniques is a critical area of research in quantum hardware.

5**. Quantum Software Development Kits (SDKs):** SDKs provide tools, libraries, and APIs for programming quantum computers. They enable researchers and developers to write quantum algorithms, simulate quantum circuits, and execute experiments on real quantum hardware.

Examples of popular quantum SDKs include Qiskit (IBM Quantum), Cirq (Google Quantum), and Forest (Rigetti Computing).

6. **Quantum Networking and Communication:** Quantum communication technologies, such as quantum key distribution (QKD), enable secure transmission of information using quantum properties. Quantum networks connect multiple quantum processors, allowing distributed quantum computations and quantum communication between distant locations. Quantum internet prototypes are being developed to explore the potential of quantum networking.

Advancements in quantum hardware and technologies are at the forefront of quantum computing research and are paving the way for practical applications in fields like cryptography, optimization, material science, and artificial intelligence. Researchers and engineers continue to push the boundaries of quantum hardware to build more stable, scalable, and error-resistant quantum computers, bringing us closer to realizing the full potential of quantum computing.

- **Quantum Processors:** Quantum Dots, Ion Traps, Superconducting Qubits

Certainly! The topic "Quantum Processors: Quantum Dots, Ion Traps, Superconducting Qubits" refers to different physical implementations of qubits, the fundamental units of quantum information, in quantum computing. Unlike classical bits, which can only exist in a state of 0 or 1, qubits can exist in multiple states simultaneously due to the principles of quantum mechanics such as superposition and entanglement. Quantum processors are devices designed to manipulate and process these qubits to perform quantum computations.

Here's a breakdown of the three types of quantum processors mentioned:

1. Quantum Dots:
Quantum dots are nanoscale semiconductor particles that can trap a small number of electrons. These electrons are manipulated to represent qubits. The quantum properties of these dots allow for the creation of qubits in solid-state systems. Quantum dots have the potential for scalability and can be integrated into existing semiconductor technologies, making them promising candidates for quantum computation.

2. Ion Traps:
Ion trap quantum processors use precisely controlled electric and magnetic fields to trap individual ions (charged atoms) in place. These trapped ions serve as qubits. By manipulating the internal energy states of these ions using lasers, researchers can perform quantum operations. Ion trap quantum processors are highly stable and have been used to demonstrate quantum algorithms and error correction techniques.

3. Superconducting Qubits:
Qubits are the fundamental units of quantum information. Various physical systems are used to represent qubits, including:

1. **Superconducting Qubits:**
Superconducting qubits are implemented using superconducting circuits. These circuits are made of Josephson junctions, which are devices that exhibit zero electrical resistance below a criteria.

2. **Quantum Gates and Circuits:**
Quantum gates are operations applied to qubits to perform quantum computations. Quantum circuits are sequences of quantum gates. Various quantum logic gates, such as Hadamard gates, CNOT gates, and phase gates, are used to create quantum algorithms.

3. **Quantum Processors:**
Quantum processors are physical implementations of qubits and quantum gates. Companies like IBM, Google, Rigetti, IonQ, and others are actively developing and experimenting with

quantum processors. These processors are often made accessible through cloud platforms, allowing researchers and developers to run quantum algorithms remotely.

4. **Quantum Error Correction:**
Quantum error correction codes, such as surface codes and the Shor code, are employed to detect and correct errors in quantum computations. Error correction is crucial for the reliability of quantum computers.

5. **Quantum Interconnects:**
Quantum interconnects are used to connect different parts of a quantum computer. They are essential for scaling up quantum systems to a larger number of qubits. Quantum communication channels are also being developed for secure communication using quantum key distribution (QKD) protocols.

6. **Quantum Software and Algorithms:**
Quantum software tools and algorithms are developed to harness the power of quantum computers. This includes quantum programming languages like Qiskit, QuTiP, and Cirq, which enable the design and simulation of quantum circuits.

7. **Quantum Cryogenics:**
Most quantum computing technologies require extremely low temperatures to operate. Cryogenic systems, such as dilution refrigerators, are used to cool quantum processors to temperatures close to absolute zero.

8. **Quantum Metrology:**
Quantum technologies are also applied in precision measurements and metrology, such as in atomic clocks and sensors. Quantum-enhanced measurement devices can achieve unprecedented levels of accuracy and sensitivity.

9. **Quantum Dots and Majorana Fermions:**
Quantum dots and Majorana fermions are exotic quantum particles that are being explored for their potential use in quantum computing. Majorana fermions, in particular, are being investigated for their topological properties, which can make qubits more stable against errors.

These are tiny circuits made from superconducting materials. They require extremely low temperatures (near absolute zero) to function and are manipulated using microwave pulses.

Trapped Ions: Ions are trapped using electromagnetic fields and manipulated with lasers. Quantum information is stored in stable electronic states of the ions.

Topological Qubits: These qubits are based on anyons, exotic particles that exist in certain 2D materials. Topological qubits are more robust against errors due to their topological properties.

Photonic Qubits: Quantum information is carried by photons and manipulated using beam splitters, phase shifters, and detectors. Photonic qubits are more resistant to decoherence since photons don't interact strongly with their environment.

- **Quantum Software Development Kits (SDKs)**

"Quantum Software Development Kits (SDKs)" refer to specialized software packages designed to facilitate the development, simulation, and execution of quantum algorithms on quantum computers. These SDKs are essential tools for researchers, scientists, and developers working in the field of quantum computing. Here's a breakdown of the key aspects of Quantum Software Development Kits:

1. Quantum Algorithm Design:
Quantum SDKs provide libraries and frameworks for designing quantum algorithms. They offer a variety of predefined quantum gates and circuits that allow developers to create complex algorithms using quantum principles like superposition and entanglement.

2. Simulating Quantum Systems:
Quantum SDKs often include simulators that enable the emulation of quantum systems on classical computers. This simulation functionality is crucial for testing and debugging quantum algorithms before running them on actual quantum hardware. Simulators help developers understand the behavior of quantum algorithms and optimize their performance.

3. Access to Quantum Hardware:
Some advanced quantum SDKs provide interfaces to connect with real quantum processors. These interfaces allow researchers to execute their quantum algorithms on physical quantum computers via cloud-based services. Access to real quantum hardware is valuable for validating algorithms and experimenting with the unique capabilities of quantum systems.

4. Quantum Circuit Visualization:
Quantum SDKs often come with tools for visualizing quantum circuits. Visualization is essential for understanding the structure of quantum algorithms, especially as they can become highly complex. Visual representations help researchers debug their algorithms and gain insights into the behavior of quantum circuits.

5. Optimization and Error Correction:
Quantum SDKs may include features for optimizing quantum algorithms and implementing error correction techniques. Quantum computations are sensitive to errors, and SDKs often provide functionalities to mitigate these errors, enhancing the reliability of quantum algorithms.

6. Community and Collaboration:
Quantum SDKs are typically supported by active communities of researchers and developers. These communities contribute to the improvement of the SDKs, share knowledge, and collaborate on solving challenges related to quantum algorithm development. Online forums, documentation, and collaborative platforms are common components of these SDK ecosystems.

7. Cross-Platform Compatibility:
Quantum SDKs are designed to be compatible with various programming languages and platforms. They provide APIs (Application Programming Interfaces) that allow developers to write quantum algorithms using programming languages they are familiar with, such as Python, and run these algorithms on different platforms, including personal computers and cloud services.

In summary, Quantum Software Development Kits are essential tools that bridge the gap between theoretical quantum algorithms and practical implementations. They empower researchers and developers to explore the potential of quantum computing, design innovative algorithms, simulate quantum systems, and collaborate with the global quantum computing community.

- **Quantum Networking and Communication**

"Quantum Networking and Communication" is a fascinating and rapidly evolving field that explores the application of quantum mechanics to the transmission and exchange of information. Unlike classical communication systems, which rely on classical bits (0s and 1s), quantum networking and communication use quantum bits, or qubits, which can exist in multiple states simultaneously due to the principle of superposition.

Here are the key aspects of Quantum Networking and Communication:

1. **Quantum Entanglement:** One of the most intriguing properties of quantum mechanics is entanglement. When two particles become entangled, the state of one particle instantaneously influences the state of the other, regardless of the distance between them. Quantum communication harnesses this phenomenon for secure communication channels.

2. **Quantum Cryptography:** Quantum cryptography provides methods for secure communication based on the principles of quantum mechanics. Quantum key distribution (QKD) protocols, such as the famous BB84 protocol, use quantum properties to enable two parties to securely exchange cryptographic keys. Any attempt to eavesdrop on the communication would disturb the quantum states, making the interception detectable.

3. **Quantum Teleportation:** Quantum teleportation is a process by which the exact state of a quantum particle can be transmitted from one location to another, using entanglement and classical communication. While it doesn't involve the physical movement of particles, it allows for the transfer of quantum information between distant quantum systems.

4. **Quantum Repeaters:** Quantum repeaters are devices designed to extend the range of quantum communication. Due to the delicate nature of quantum states, they degrade over long distances. Quantum repeaters use entanglement swapping and purification techniques to overcome this limitation, enabling the creation of entangled qubits over longer distances.

5. **Quantum Communication Protocols:** Researchers are developing various quantum communication protocols for tasks such as secure messaging, quantum key distribution over long distances, and distributed quantum computing. These protocols are crucial for the development of quantum internet, a global network that allows quantum information to be shared and processed securely across the world.

6. **Quantum Networks:** Quantum networks connect multiple quantum devices and processors, allowing them to exchange quantum information. These networks are essential for building quantum internet infrastructure and enabling novel applications in secure communication, distributed quantum computing, and quantum-enhanced sensing.

The study of quantum networking and communication is at the forefront of quantum technology research. As scientists make advancements in this field, the potential for secure and efficient communication systems, as well as groundbreaking technologies like quantum internet and quantum cloud computing, becomes increasingly promising.

ISBN: 978-81-965655-9-6

4.

Quantum Programming Languages

QUANTUM PROGRAMMING LANGUAGES

- **Quantum Programming Languages:**

Quantum programming languages are specialized tools designed to harness the unique capabilities of quantum computers. Unlike traditional programming languages that operate on bits, quantum programming languages manipulate qubits, the fundamental units of quantum information. Qubits can exist in a superposition of states, allowing them to simultaneously represent multiple values. This inherent parallelism enables quantum computers to tackle problems that are intractable for classical computers.

Quantum programming languages provide a bridge between quantum algorithms and the underlying hardware. They allow programmers to express quantum operations, such as applying quantum gates and performing measurements, in a high-level, abstract manner. These languages handle the complexities of translating these instructions into low-level machine code that can be executed on specific quantum hardware architectures.

The development of quantum programming languages is still in its early stages, and there is no single dominant language. However, several promising candidates have emerged, each with its strengths and weaknesses. Some notable examples include Q#, Qiskit, Cirq, and Quipper.

As quantum computing technology matures, quantum programming languages will play an increasingly crucial role in unlocking the full potential of these powerful machines. They will enable researchers and developers to create groundbreaking applications in fields such as cryptography, optimization, and materials science.

Key Aspects:

1. Quantum Gates and Circuits:

Quantum programming languages provide constructs to manipulate qubits using quantum gates. These gates perform operations on qubits, allowing the creation of quantum circuits. Quantum circuits represent sequences of quantum gates, akin to classical logic circuits, and are fundamental in quantum algorithm design.

2. Quantum Algorithms:

Quantum programming languages facilitate the implementation of quantum algorithms. Algorithms like Shor's algorithm (for integer factorization) and Grover's algorithm (for unstructured search) showcase the potential advantages of quantum computing over classical methods. Quantum programming languages provide high-level abstractions for these algorithms, making them accessible to developers.

3. Quantum Error Correction:

Quantum systems are susceptible to errors due to factors like decoherence and noise. Quantum programming languages include error correction techniques, such as quantum error-correcting codes and fault-tolerant quantum computation methods, to mitigate these errors. Writing error-free quantum code is crucial for reliable quantum computation.

4. Quantum Simulation:

Quantum programming languages support quantum simulation, allowing researchers to model and simulate quantum systems. This is invaluable for understanding complex quantum phenomena, testing quantum algorithms without physical quantum hardware, and exploring quantum chemistry and physics applications.

5. Quantum Compilation and Optimization:

Quantum compilation translates high-level quantum algorithms into sequences of quantum gates compatible with specific quantum hardware. Quantum programming languages incorporate

optimization techniques to enhance the efficiency of compiled quantum circuits, ensuring optimal use of available qubits and minimizing gate operations.

6. Quantum Debugging and Profiling:
Debugging quantum programs presents unique challenges due to the probabilistic nature of quantum mechanics. Quantum programming languages offer tools for debugging quantum code, allowing developers to identify and fix errors. Profiling tools help analyze the performance of quantum algorithms, enabling developers to optimize their code further.

Examples of quantum programming languages include Qiskit (developed by IBM), Cirq (developed by Google), QuTiP (Quantum Toolbox in Python), and Microsoft Quantum Development Kit (Q#). These languages empower researchers and developers to explore the vast potential of quantum computing, paving the way for innovative solutions to complex computational problems.

- **Qiskit (IBM Quantum)**

In the realm of cutting-edge technologies, quantum computing stands out as a revolutionary force with the potential to transform numerous industries. To harness this extraordinary power, IBM Quantum has developed Qiskit, an open-source software development framework designed to democratize quantum computing.

Qiskit empowers users, from novices to experts, to explore the quantum realm through the familiar Python programming language. With Qiskit, creating quantum circuits, the building blocks of quantum algorithms, becomes an intuitive process. These circuits can then be executed on a variety of backends, ranging from high-performance simulators to actual quantum devices, providing a seamless transition from theoretical exploration to real-world implementation.

The versatility of Qiskit extends beyond circuit design and execution. It offers a comprehensive suite of tools for noise simulation, visualization, and optimization, enabling users to gain a deeper understanding of quantum systems and develop robust quantum algorithms.

Qiskit's open-source nature fosters a vibrant community of researchers, developers, and enthusiasts, collaboratively pushing the boundaries of quantum computing. With its user-friendly interface, comprehensive functionalities, and active community, Qiskit is democratizing quantum computing, making this revolutionary technology accessible to all.

Here's a breakdown of key aspects related to Qiskit:
1. Quantum Computing Framework:
Quantum computing frameworks are software platforms that provide tools and libraries for developing quantum algorithms and applications. They abstract away the complexities of quantum hardware and allow researchers and developers to focus on the higher-level aspects of quantum computing.

These frameworks typically include:
Quantum programming languages: These languages provide a way to express quantum algorithms in a way that is both human-readable and machine-executable.

Quantum simulators: These simulators allow developers to test and debug their quantum algorithms on classical computers before running them on actual quantum hardware.

Quantum hardware interfaces: These interfaces allow developers to connect to and control quantum hardware devices.

Quantum algorithms libraries: These libraries provide pre-built implementations of common quantum algorithms, such as Grover's algorithm and Shor's algorithm.

Some of the most popular quantum computing frameworks include:

Qiskit: An open-source framework developed by IBM.

Cirq: An open-source framework developed by Google.

PyQuil: An open-source framework developed by Rigetti Computing.

ProjectQ: An open-source framework developed at ETH Zurich.

Quantum computing frameworks are essential tools for the development of quantum algorithms and applications. They are making it easier for researchers and developers to explore the potential of quantum computing and to develop new and innovative applications.

2. Python-Based:
Quantum computing is a rapidly developing field with the potential to revolutionize various industries. While there are several dedicated quantum programming languages, Python has emerged as a popular choice for quantum programming due to its versatility, ease of use, and extensive library support.

Python-based quantum programming frameworks provide a user-friendly interface for designing and simulating quantum circuits, allowing researchers and developers to explore quantum algorithms without the complexities of low-level quantum programming languages. These frameworks leverage Python's familiar syntax and extensive scientific computing libraries, making them accessible to a broader audience.

Popular Python-based quantum programming frameworks include:

1. **Qiskit:** Developed by IBM, Qiskit is a comprehensive open-source framework for quantum programming. It offers a range of tools for designing, simulating, and executing quantum circuits, along with access to IBM's quantum hardware.
2. **Cirq:** Created by Google, Cirq is another open-source quantum programming framework that focuses on designing and optimizing quantum circuits for Noisy Intermediate-Scale Quantum (NISQ) computers. It provides tools for noise simulation and circuit optimization, making it suitable for real-world quantum computing applications.
3. **PennyLane:** Developed by Xanadu Quantum Technologies, PennyLane is a Python library for differentiable programming of quantum computers. It enables the integration of quantum circuits with machine learning frameworks like TensorFlow and PyTorch, facilitating the development of hybrid quantum-classical algorithms.

These Python-based frameworks are actively being developed and improved, making Python a valuable tool for exploring and advancing the field of quantum computing.

3. Quantum Circuits and Gates:
Quantum circuits and gates are fundamental concepts in quantum programming languages, serving as the building blocks for constructing quantum algorithms and manipulating quantum information.

Quantum circuits are analogous to classical circuits, but instead of operating on classical bits, they operate on quantum bits or qubits. Qubits can exist in a superposition of states, allowing them to represent multiple values simultaneously. Quantum gates, on the other hand, are the operations that act on qubits, transforming their states and enabling the execution of quantum algorithms.

Quantum programming languages provide a means to express quantum circuits and gates in a concise and structured manner. These languages typically incorporate a set of predefined gates,

such as Hadamard, Pauli-X, and CNOT gates, which can be combined to form more complex operations. The languages also allow for the specification of qubit registers and the control flow of quantum operations.

By utilizing quantum circuits and gates within quantum programming languages, programmers can harness the power of quantum computing to solve problems that are intractable for classical computers. This opens up a vast range of possibilities in fields like cryptography, optimization, and scientific simulations.

In summary, quantum circuits and gates form the core of quantum programming languages, enabling the design and implementation of quantum algorithms that leverage the unique properties of quantum mechanics to tackle complex computational challenges.

4. Backends:

Qiskit, an open-source quantum computing framework, offers a diverse range of backends, the computational engines that power the execution of quantum circuits. These backends encompass both real quantum processors, accessible through IBM Quantum, and simulators that emulate quantum computations on classical computers. Each backend type caters to specific user requirements, presenting a trade-off between speed and accuracy.

Real quantum processors, the pinnacle of quantum computing hardware, enable direct execution of quantum circuits on actual quantum bits (qubits). While offering the most authentic quantum experience, these processors are limited in terms of qubit count and susceptibility to noise.

Simulators, on the other hand, provide a virtual quantum environment on classical computers. They sacrifice the genuine quantum experience for enhanced flexibility and error-free execution. Simulators prove particularly valuable for testing and debugging quantum circuits before deploying them on real quantum hardware.

The choice of backend hinges on the specific needs of the user. For rapid execution and exploration of small-scale quantum circuits, simulators are the preferred choice. However, for harnessing the true power of quantum computing and tackling larger, more complex problems, real quantum processors are indispensable.

In summary, Qiskit's diverse backend ecosystem empowers users to tailor their quantum computing experience, balancing speed, accuracy, and hardware access to suit their specific requirements.

5. Quantum Algorithms and Applications:

Qiskit stands as a comprehensive open-source software development kit (SDK) specifically designed for quantum computing. It empowers users to explore and harness the remarkable capabilities of quantum computers through a user-friendly interface and a vast array of functionalities. Qiskit's core strength lies in its ability to provide seamless access to various quantum algorithms, including the groundbreaking Shor's algorithm, Grover's algorithm, and sophisticated quantum error correction codes. These algorithms serve as the foundation for unlocking the true potential of quantum computing, enabling advancements in diverse fields such as optimization, machine learning, cryptography, and chemistry.

Beyond its robust algorithmic implementations, Qiskit extends its reach to support the development of quantum applications across a wide spectrum of disciplines. In the realm of optimization, Qiskit facilitates the optimization of complex systems and processes, tackling challenges that conventional computers struggle to address. Within the domain of machine learning, Qiskit empowers researchers to explore quantum-enhanced machine learning techniques, opening doors to unprecedented levels of pattern recognition and predictive capabilities. In the field of cryptography, Qiskit enables the exploration of quantum-resistant

 ISBN: 978-81-965655-9-6

cryptographic algorithms, ensuring secure communication in the face of evolving quantum computing threats. And in the realm of chemistry, Qiskit facilitates the simulation of molecular structures and reactions, paving the way for accelerated drug discovery and material design.

Qiskit's comprehensive toolkit and unwavering commitment to open-source collaboration make it an invaluable resource for researchers, developers, and enthusiasts alike, fostering a vibrant community dedicated to advancing the frontiers of quantum computing.

6. Community and Resources:

Qiskit, IBM's open-source quantum computing software development kit, boasts a thriving and dynamic community of researchers, developers, and enthusiasts. This global network of individuals is united by a shared passion for exploring the frontiers of quantum computing and harnessing its transformative potential.

IBM Quantum, a leading provider of quantum computing resources and expertise, plays a pivotal role in fostering this collaborative environment. The company offers a comprehensive suite of documentation, tutorials, and educational resources designed to empower users of all levels, from novices to seasoned professionals. These materials provide a solid foundation in quantum computing concepts and equip users with the skills necessary to effectively utilize Qiskit for their research and development endeavors.

The Qiskit community extends beyond simply utilizing the software; it actively contributes to its ongoing development. This open-source model fosters a spirit of innovation and collaboration, allowing community members to directly shape the evolution of Qiskit. Through contributions such as code enhancements, bug fixes, and new feature proposals, the community plays an integral role in expanding Qiskit's capabilities and ensuring its continued relevance in the rapidly evolving quantum computing landscape.

The synergy between Qiskit's vibrant community and IBM Quantum's robust support infrastructure creates a fertile ground for quantum computing advancements. Together, they are democratizing access to this revolutionary technology, empowering individuals worldwide to explore its boundless possibilities.

7. Research and Education:

Qiskit, an open-source software development kit (SDK) designed for quantum computing, has gained widespread adoption in both research and educational settings. Researchers across the globe utilize Qiskit to delve into the intricacies of quantum algorithms, conduct groundbreaking experiments, and continuously expand the horizons of quantum computing. Its impact extends beyond research laboratories, as Qiskit has become an indispensable tool in classrooms and online courses, empowering students to acquire practical experience with quantum computing concepts.

The accessibility and versatility of Qiskit have significantly contributed to its widespread adoption. Researchers appreciate its user-friendly interface, which allows them to focus on their research objectives rather than grappling with complex programming syntax. Qiskit's comprehensive suite of tools and functionalities enables researchers to seamlessly design, simulate, and execute quantum circuits, fostering a collaborative environment that accelerates the pace of discovery.

In the realm of education, Qiskit has emerged as a transformative force, empowering students to grasp the theoretical underpinnings of quantum computing through hands-on experimentation. Its intuitive interface and extensive collection of tutorials and learning resources make it an ideal platform for introducing students to the world of quantum computing. By providing a stimulating and accessible learning environment, Qiskit is nurturing the next generation of quantum scientists and engineers.

Overall, Qiskit plays a pivotal role in propelling the field of quantum computing forward. Its user-centric design, combined with its ability to foster collaboration and accelerate research, has cemented its position as an indispensable tool for both researchers and educators. As the field of quantum computing continues to evolve, Qiskit is poised to remain at the forefront, empowering the development of revolutionary quantum technologies.

- **Cirq (Google Quantum)**

Cirq, an open-source quantum computing framework developed by Google, empowers researchers to construct, manipulate, and optimize quantum circuits using Python. Quantum circuits, the cornerstone of quantum computing, mirror classical circuits in classical computing. Cirq offers researchers a high-level, intuitive language to interact with these circuits.

Cirq's primary features include:

- **Circuit Construction:** Cirq facilitates the creation of quantum circuits using a straightforward syntax, enabling researchers to effortlessly represent complex quantum algorithms.
- **Circuit Manipulation:** Cirq provides tools for modifying and optimizing quantum circuits, enabling researchers to enhance circuit performance and tailor them to specific hardware constraints.
- **Circuit Simulation:** Cirq incorporates simulators for both wave functions and density matrices, enabling researchers to test and analyze quantum circuits without requiring actual quantum hardware.
- **Hardware Integration:** Cirq seamlessly connects with various quantum computing platforms, enabling researchers to execute their circuits on real quantum hardware.

Cirq has emerged as a valuable tool for quantum computing researchers, simplifying the process of designing, optimizing, and executing quantum circuits. Its intuitive interface and comprehensive features make it a powerful asset in advancing quantum computing research

Here are the key aspects of Cirq (Google Quantum) explained:

1. Quantum Circuit Representation:

- **Qubits and Gates:** Cirq allows users to define qubits (quantum bits) and apply quantum gates on these qubits. Quantum gates are fundamental operations that manipulate qubits.

- **Circuit Diagrams**: Cirq provides tools to visualize quantum circuits in the form of circuit diagrams, making it easier to understand and debug complex quantum algorithms.

2. Simulations and Hardware Execution:

- **Simulators:** Cirq includes powerful simulators that allow researchers to simulate the behavior of quantum circuits on classical computers. This is crucial for testing algorithms and understanding their properties.

- **Quantum Hardware:** Cirq is designed to be compatible with existing and future quantum hardware platforms, enabling researchers to run their algorithms on actual quantum processors.

3. Quantum Algorithms and Applications:

- **Quantum Algorithms:** Researchers can implement various quantum algorithms, such as Shor's algorithm for integer factorization and Grover's algorithm for unstructured search, using Cirq.

- **Quantum Applications:** Cirq can be used to develop applications in areas like cryptography, optimization, and machine learning, harnessing the power of quantum computing for practical tasks.

4. Integration with Python:

- **Python Integration:** Cirq is built around Python, a popular and versatile programming language. This integration makes it accessible to a wide range of researchers and developers who are already familiar with Python.

5. Community and Collaboration:

- **Open-Source Framework:** Cirq is open-source, encouraging collaboration and contributions from the quantum computing community. Researchers and developers can modify and improve the framework based on their specific requirements.

- **Documentation and Support:** Google provides extensive documentation and support resources, including tutorials and examples, to help users get started with Cirq and explore its capabilities.

In summary, Cirq (Google Quantum) is a robust and user-friendly quantum computing framework that empowers researchers and developers to explore, experiment, and innovate in the field of quantum computing. Its integration with Python, simulation capabilities, and compatibility with quantum hardware make it a valuable tool for the growing community of quantum computing enthusiasts and experts.

- **QuTiP (Quantum Toolbox in Python)**

QuTiP (Quantum Toolbox in Python): A Comprehensive Overview
QuTiP, short for Quantum Toolbox in Python, is an open-source software library written in Python that facilitates numerical simulations and computations in the field of quantum physics and quantum information science. Developed and maintained by a collaborative community of scientists and researchers, QuTiP provides a user-friendly interface for simulating the dynamics of open quantum systems, implementing quantum algorithms, and solving problems in quantum optics, quantum computing, and condensed matter physics.

Key Features and Capabilities:

1. Quantum Operators and States:
QuTiP allows users to define quantum operators and states, enabling the representation of quantum systems with various degrees of complexity. It supports a wide range of quantum systems, including qubits, harmonic oscillators, and spins.

2. Dynamics and Evolution:
Researchers can simulate the time evolution of quantum systems using QuTiP. This includes both closed quantum systems, where the evolution is unitary, and open quantum systems, where the effects of decoherence and dissipation are taken into account.

3. Quantum Algorithms and Protocols:
QuTiP provides tools to implement and simulate quantum algorithms, making it valuable for researchers exploring quantum computing. It allows the study of algorithms such as quantum teleportation, Grover's search algorithm, and quantum error correction codes.

4. Quantum Optics and Quantum Information:
Researchers in quantum optics can use QuTiP to simulate phenomena like quantum noise, quantum measurements, and quantum optical systems. Additionally, the library supports

operations related to quantum information theory, such as quantum entanglement and quantum channels.

5. Visualization and Analysis:
QuTiP includes visualization tools for quantum states and processes, aiding researchers in understanding and interpreting simulation results. It also offers functionalities for analyzing quantum entanglement, quantum correlations, and other relevant properties.

6. Integration with Scientific Computing Libraries:
QuTiP seamlessly integrates with popular scientific computing libraries in Python, such as NumPy and SciPy, enhancing its computational capabilities and making it a versatile choice for researchers in quantum physics and related disciplines.

APPLICATIONS:
- **Quantum Computing Research:** QuTiP is widely used by researchers and students to experiment with quantum algorithms, develop new protocols, and explore the potential of quantum computation.

- **Quantum Optics Experiments:** Scientists use QuTiP to model and analyze complex quantum optical systems, enabling the simulation of experiments related to quantum information processing and quantum communication.

- **Education and Training:** QuTiP serves as an educational tool, providing students and educators with a platform to learn and teach quantum physics concepts and quantum computing principles through hands-on simulations.

In summary, QuTiP plays a crucial role in advancing research and education in the fields of quantum physics and quantum information science by providing a powerful and accessible computational toolkit for scientists, researchers, and students. Its versatility and ease of use make it a valuable asset in the exploration of quantum phenomena and the development of quantum technologies.

- **Microsoft Quantum Development Kit**

The Microsoft Quantum Development Kit is a comprehensive set of tools and resources provided by Microsoft to facilitate the development of quantum applications. It is designed to help both researchers and developers explore the potential of quantum computing and develop algorithms that can run on quantum computers.

Here are the key components and aspects of the Microsoft Quantum Development Kit:

1. Q Programming Language:
- Q (Q-sharp) is a high-level programming language specifically created for quantum computing. It is integrated into Visual Studio, Microsoft's integrated development environment, allowing developers to write quantum algorithms using a familiar and efficient interface.

2. Quantum Simulator:
- The kit includes a local quantum simulator that enables developers to simulate quantum computations on their own machines. This is crucial for testing and debugging quantum algorithms before they are executed on a real quantum computer.

3. Quantum Libraries and Samples:
- Microsoft Quantum Development Kit provides a library of quantum algorithms and samples. These libraries contain pre-built quantum operations and functions that developers can use to build their quantum programs. It simplifies the process of writing complex quantum algorithms by providing a starting point for developers.

4. Integration with Classical Languages:
- Q can be used in conjunction with classical languages like C# and Python. This integration allows developers to combine classical and quantum computations seamlessly, enabling the development of hybrid quantum-classical applications.

5. Quantum Machine Learning:
- The kit includes tools for quantum machine learning experiments. Developers can explore the intersection of quantum computing and machine learning, experimenting with algorithms that leverage quantum computing's unique capabilities for solving complex machine learning problems.

6. Support for Quantum Hardware:
- While the kit includes a simulator, it is also designed to support quantum hardware. Microsoft Quantum Development Kit can be used to write programs that run on actual quantum processors, provided by partners like IonQ and Honeywell, giving developers the opportunity to experiment with real quantum hardware.

7. Educational Resources:
- Microsoft provides extensive documentation, tutorials, and educational materials to help developers and researchers learn quantum computing concepts and how to use the Quantum Development Kit effectively. These resources are valuable for beginners and experienced developers alike.

In summary, the Microsoft Quantum Development Kit provides a powerful platform for exploring and experimenting with quantum computing. It empowers developers and researchers to delve into the world of quantum algorithms, simulations, and applications, paving the way for innovations in the field of quantum computing and its integration into various industries.

Diagrams explaining the architecture of a Quantum Neural Network

Performance Metrics Comparison

Quantum Neural Networks (QNNs) vs Classical Neural Networks		
Metric	Quantum Neural Networks (QNNs)	Classical Neural Networks
Accuracy	QNN Accuracy Value	Classical NN Accuracy Value
Loss	QNN Loss Value	Classical NN Loss Value
Training Time	QNN Training Time Value	Classical NN Training Time Value

Quantum-enhanced Machine Learning

Quantum-enhanced Machine Learning (QEML) represents a revolutionary convergence of quantum computing and artificial intelligence, opening up new frontiers in computational capabilities. It leverages the unique principles of quantum mechanics to empower machine learning algorithms, enabling them to tackle complex problems that were previously intractable for classical computers.

At the heart of QEML lies the concept of quantum superposition, which allows quantum bits or qubits to exist in multiple states simultaneously. This inherent parallelism enables quantum computers to perform computations on a massive scale, far surpassing the limitations of classical systems.

Leveraging this quantum advantage, QEML algorithms can explore vast data landscapes and identify intricate patterns with unprecedented speed and accuracy. This transformative power holds immense potential for a wide range of applications, from drug discovery and materials design to financial modeling and risk assessment.

In the realm of drug discovery, QEML can accelerate the identification of new drug candidates by simulating molecular interactions and predicting their effectiveness. This can significantly reduce the time and cost associated with drug development, bringing life-saving treatments to patients faster.

Similarly, QEML can revolutionize materials design by enabling the exploration of vast material properties and identifying optimal combinations for specific applications. This can lead to the development of novel materials with superior strength, durability, and conductivity, transforming industries from aerospace to electronics.

In the financial sector, QEML can enhance risk assessment models by incorporating complex market dynamics and predicting potential outcomes with greater precision. This can empower financial institutions to make informed decisions and mitigate risks, promoting stability and growth in the global economy.

As QEML continues to evolve, it promises to revolutionize a wide spectrum of industries, unlocking new possibilities and addressing grand challenges that were once considered insurmountable. The convergence of quantum computing and artificial intelligence marks a new era of computational power, paving the way for groundbreaking advancements in science, technology, and society.

Theories

Quantum-enhanced Machine Learning (QML) harnesses the power of quantum computing to revolutionize the field of machine learning. By employing quantum algorithms, QML offers a significant leap in computational efficiency and problem-solving capabilities compared to traditional machine learning approaches.

At the heart of QML lies the concept of quantum parallelism, a unique feature of quantum computers that enables them to process multiple computations simultaneously. This inherent parallelism, along with quantum entanglement, allows quantum algorithms to tackle complex problems that would be intractable for classical computers.

One prominent example of a quantum algorithm employed in QML is Grover's algorithm. This algorithm excels at searching through vast datasets, offering a quadratic speedup over classical search algorithms. This capability proves invaluable in tasks such as pattern recognition and data mining.

Another notable quantum algorithm is the Quantum Support Vector Machine (QSVM). QSVMs are particularly effective in classification tasks, where they can efficiently identify patterns and categorize data points. Their quantum-enhanced approach offers a significant advantage over classical SVMs, especially when dealing with large and complex datasets.

The combination of quantum algorithms and machine learning principles opens a new frontier in computational intelligence. QML holds the potential to transform various fields, from drug discovery and materials science to financial modeling and risk assessment. As quantum computing technology continues to mature, QML is poised to become an indispensable tool for solving complex problems and gaining deeper insights from data.

 ISBN: 978-81-965655-9-6

Tables

Quantum Algorithm	Application
Grover's Algorithm	Unstructured Search
Quantum Support Vector Machines	Classification

- **Quantum Computing and AI Ethics**

Quantum-Enhanced Machine Learning

Quantum-enhanced machine learning (QML) is a field of research that explores the intersection of quantum computing and machine learning. QML algorithms aim to leverage the unique capabilities of quantum computers to solve machine learning problems that are intractable for classical computers.

One of the key advantages of QML is that quantum computers can perform certain types of computations exponentially faster than classical computers. This is due to two fundamental properties of quantum mechanics: superposition and entanglement.

- Superposition allows a quantum bit (qubit) to be in multiple states at the same time, until it is measured. This means that quantum computers can explore multiple possible solutions to a problem simultaneously, rather than having to explore them one by one.
- Entanglement allows qubits to be linked together in such a way that they share the same fate, even if they are physically separated. This means that quantum computers can perform computations on multiple data points simultaneously, rather than having to perform them sequentially.

QML algorithms are still in their early stages of development, but they have the potential to revolutionize many fields, including drug discovery, materials science, and finance.

Here are some specific examples of QML algorithms:

- **Quantum linear regression:** This algorithm can be used to train linear regression models on quantum data. Linear regression models are used to make predictions about a continuous variable based on one or more other variables.
- **Quantum classification:** This algorithm can be used to train classification models on quantum data. Classification models are used to predict the category to which a data point belongs.
- **Quantum clustering:** This algorithm can be used to cluster quantum data. Clustering is the process of grouping similar data points together.
- **Quantum reinforcement learning:** This algorithm can be used to train reinforcement learning agents to perform tasks in a quantum environment. Reinforcement learning agents learn to behave in an environment by trial and error.

Applications of QML

QML has the potential to be used in a wide range of applications, including:

- **Drug discovery:** QML algorithms can be used to screen billions of potential drug candidates simultaneously, which could accelerate the drug discovery process.
- **Materials science:** QML algorithms can be used to design new materials with specific properties, such as superconductivity or high strength.

- **Finance:** QML algorithms can be used to develop new financial models that can more accurately predict market behavior.
- **Artificial intelligence:** QML algorithms can be used to develop new AI models that are more efficient and accurate than existing models.

Challenges of QML

Quantum Machine Learning (QML) faces several challenges that hinder its widespread adoption and practical applications. These challenges stem from the inherent limitations of current quantum computing hardware and the complexities of developing and implementing quantum algorithms.

One major challenge is the limited availability and scalability of quantum computers. Existing quantum hardware is still in its early stages of development, with limited qubit count and high error rates. This restricts the size and complexity of QML models that can be effectively trained and deployed.

Another significant challenge lies in the development of efficient and versatile quantum algorithms for machine learning tasks. Designing and optimizing quantum algorithms requires specialized expertise and in-depth knowledge of both quantum computing and machine learning principles.

Furthermore, integrating QML models into existing classical machine learning frameworks poses additional challenges. The compatibility and interoperability between quantum and classical computing environments need to be carefully addressed to ensure seamless integration and efficient data transfer.

Despite these challenges, QML remains a promising field with immense potential. As quantum computing technology advances and more sophisticated quantum algorithms emerge, QML is expected to overcome these hurdles and revolutionize various industries.

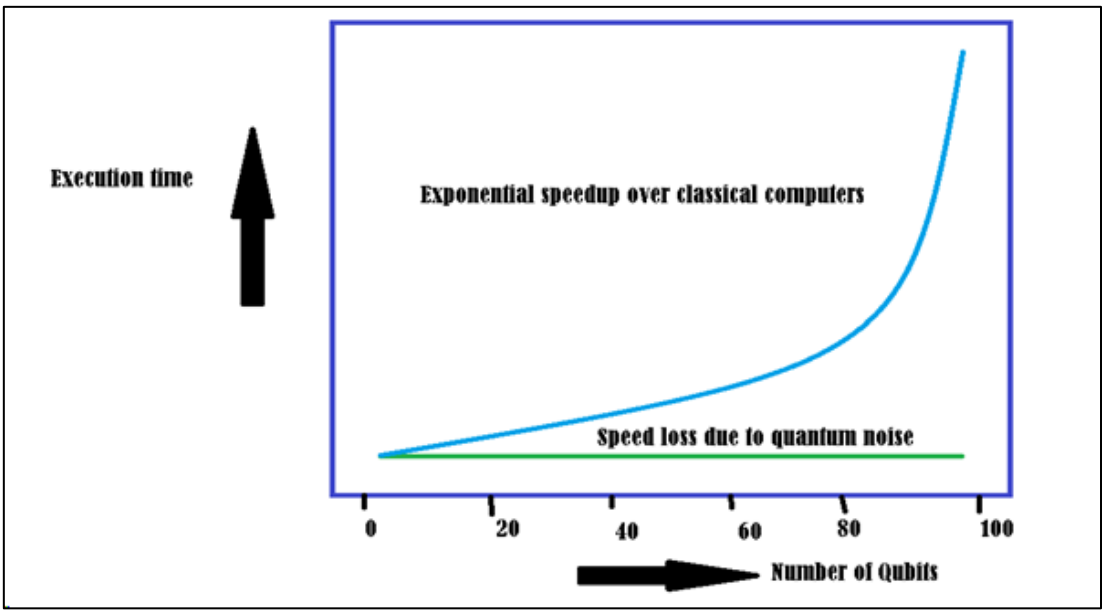
CONCLUSION

QML is a rapidly developing field with the potential to revolutionize many fields. However, there are still significant challenges that need to be overcome before QML can be widely used.

 ISBN: 978-81-965655-9-6

Graphs and tables

The following graph shows the exponential speedup that quantum computers can achieve for certain types of computations:



Exponential speedup of quantum computers

The following table shows some of the potential applications of QML:

Application	Potential benefits
Drug discovery	Accelerated drug discovery process
Materials science	Design of new materials with specific properties
Finance	More accurate financial models
Artificial intelligence	More efficient and accurate AI models

The following are some of the key theories that underpin QML:

- **Quantum mechanics:** Quantum mechanics is the branch of physics that studies the behavior of matter at the atomic and subatomic level.
- **Quantum computing:** Quantum computing is a new type of computing that harnesses the power of quantum mechanics to solve problems that are intractable for classical computers.
- **Machine learning:** Machine learning is a field of computer science that gives computers the ability to learn without being explicitly programmed.

ISBN: 978-81-965655-9-6

CONCLUSION

QML is a promising new field with the potential to revolutionize many industries. However, it is important to note that QML is still in its early stages of development. There are significant challenges that need to be overcome before QML can be widely used.

ISBN: 978-81-965655-9-6

5.

Quantum Cryptography and Security

 ISBN: 978-81-965655-9-6

QUANTUM CRYPTOGRAPHY AND SECURITY

Quantum cryptography is a groundbreaking field that utilizes the principles of quantum mechanics to achieve secure communication. Unlike traditional cryptography, which relies on mathematical algorithms, quantum cryptography harnesses the inherent properties of quantum mechanics to guarantee unconditional security. This means that even with the advent of powerful quantum computers, quantum cryptography remains unbreakable.

One of the key applications of quantum cryptography is quantum key distribution (QKD). QKD enables two parties to establish a shared secret key that is provably secure against eavesdropping. This shared key can then be used to encrypt and decrypt messages, ensuring that only the intended recipient can access the information. The security of QKD stems from the fundamental principles of quantum mechanics, such as the no-cloning theorem and the Heisenberg uncertainty principle, which prevent an eavesdropper from intercepting the key without introducing detectable disturbances.

Quantum cryptography also encompasses other aspects of secure communication, such as quantum secure direct communication (QSDC) and quantum authentication. QSDC allows for the direct transmission of confidential messages without the need for a pre-shared key, while quantum authentication provides a means to verify the identity of a sender or receiver.

As quantum computing technology advances, quantum cryptography is poised to play an increasingly crucial role in safeguarding sensitive data and communications. Its inherent security guarantees offer a robust defence against the potential threat posed by quantum computers, ensuring the confidentiality and integrity of information in the quantum era.

Here are some key concepts within Quantum Cryptography and Security:

1. **Quantum Key Distribution (QKD):** QKD is a foundational concept in quantum cryptography. It involves the use of quantum properties, such as superposition and entanglement, to establish a shared secret key between two parties. This key can then be used for secure communication, and any attempt to eavesdrop on the quantum channel will inevitably disturb the quantum state, alerting the communicating parties to the presence of a third party.

2. **Quantum Entanglement:** Quantum entanglement is a phenomenon where two or more particles become correlated in such a way that the state of one particle instantaneously influences the state of the other(s), regardless of the distance between them. Entangled particles can be used to create secure communication channels because any change in one particle will affect its entangled partner, providing a means to detect eavesdropping attempts.

3. **Quantum Cryptographic Protocols:** Various quantum cryptographic protocols have been developed, such as the BB84 protocol and its variants, which use quantum properties to exchange cryptographic keys securely. These protocols ensure that any interception or measurement of quantum states by an external party will disrupt the quantum states and be detected by the communicating parties.

4. **Post-Quantum Cryptography:** Quantum computing poses a threat to traditional cryptographic algorithms. Post-quantum cryptography refers to cryptographic algorithms that are believed to be secure against the potential capabilities of quantum computers. Researchers are actively working on developing encryption methods that can withstand attacks from quantum computers, ensuring the security of digital data in a quantum computing era.

5. **Quantum-resistant Algorithms:** Quantum-resistant algorithms are cryptographic algorithms designed to remain secure even in the presence of powerful quantum computers. These

algorithms are being developed to replace current encryption methods, especially for sensitive data and long-term security needs.

In summary, quantum cryptography and security harness the principles of quantum mechanics to create secure communication channels that are theoretically immune to eavesdropping by quantum computers. As quantum computing technology advances, the development and implementation of quantum cryptographic techniques become increasingly important to safeguard sensitive information in the digital age.

Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a method of secure communication that uses quantum mechanics to enable two parties to exchange encryption keys in a way that is theoretically immune to eavesdropping. The security of QKD is based on the fundamental principles of quantum mechanics, including the uncertainty principle and the no-cloning theorem.

Working of Quantum Key Distribution:

1. **Quantum Bits (Qubits):** In classical computing, bits can represent either 0 or 1. In quantum computing, qubits can exist in multiple states simultaneously due to a property called superposition. This means a qubit can be both 0 and 1 at the same time.

2. **Quantum States and Measurement:** Qubits can also be in a state called entanglement, where the state of one qubit instantaneously influences the state of another, regardless of the distance between them. When a measurement is made on an entangled qubit, the state of the other qubit is instantly determined, even if they are far apart. This property is used in QKD protocols.

3. **QKD Protocols:** One of the most well-known QKD protocols is the BB84 protocol, developed by Bennett and Brassard in 1984. In BB84, the sender (Alice) sends a sequence of photons to the receiver (Bob), with each photon representing a qubit. Alice randomly encodes the qubits in one of two bases (usually represented by two polarizations). Bob also randomly chooses a measurement basis. Due to the uncertainty principle, any attempt by an eavesdropper (Eve) to measure the photons will disturb their states, and Alice and Bob can detect this interference.

4. **Key Exchange:** Alice and Bob then publicly communicate which bases they used for encoding and measurement but not the actual values. They discard the measurements where they used different bases. By comparing a subset of their measurement results, they can detect if there was any interference (eavesdropping). If there is no interference, they can use the remaining bits as a shared secret key.

5. **Secure Communication:** Once Alice and Bob share a secret key, they can use it for secure communication. Because any attempt to eavesdrop on the key exchange would disturb the quantum states and be detected, QKD provides a theoretically secure way to establish encryption keys between two parties.

QKD has the potential to revolutionize secure communication by providing a method for exchanging encryption keys that is fundamentally secure. However, it's important to note that while QKD provides a high level of security, it does not address all aspects of secure communication, such as endpoint security or the security of the devices used in the communication process.

Post-Quantum Cryptography

Post-quantum cryptography refers to cryptographic algorithms that are believed to be secure against attacks by both classical and quantum computers. The need for post-quantum cryptography arises from the potential future development of quantum computers, which have

 ISBN: 978-81-965655-9-6

the capability to solve complex mathematical problems, such as factoring large numbers and computing discrete logarithms, much faster than classical computers.

Classical cryptographic algorithms, such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), rely on the difficulty of certain mathematical problems for their security. However, quantum computers can use algorithms like Shor's algorithm to efficiently solve these problems, making classical encryption methods vulnerable to quantum attacks.

Post-quantum cryptography research aims to develop cryptographic algorithms that are secure against both classical and quantum adversaries. These algorithms are being designed based on mathematical problems that are believed to be hard even for quantum computers to solve. Examples of such problems include lattice-based cryptography, hash-based cryptography, code-based cryptography, and multivariate polynomial cryptography.

The development of post-quantum cryptographic algorithms is crucial for ensuring the long-term security of sensitive data, especially in contexts where data needs to remain confidential for extended periods, such as in government, finance, healthcare, and military applications. As quantum computers continue to advance, the implementation of post-quantum cryptography will become essential to safeguarding digital communications and information against potential quantum threats.

Quantum-resistant Algorithms

"Quantum-resistant algorithms" refer to cryptographic algorithms that are designed to be secure against attacks by quantum computers. Traditional cryptographic algorithms, such as those used in encryption and digital signatures, rely on the mathematical complexity of certain problems to ensure security. However, quantum computers have the potential to break these algorithms using algorithms like Shor's algorithm, which can efficiently factor large numbers and solve the discrete logarithm problem – tasks that are computationally infeasible for classical computers.

Quantum-resistant algorithms are being developed as a response to the threat posed by quantum computers to traditional encryption methods. These algorithms are specifically designed to be secure even in the presence of powerful quantum computers. They rely on mathematical problems that are believed to be hard even for quantum computers to solve efficiently.

Some examples of quantum-resistant algorithms include:

1. **Lattice-based Cryptography:** These algorithms are based on the hardness of problems related to lattice theory, such as the Shortest Vector Problem (SVP) and Learning With Errors (LWE). Lattice-based cryptography is currently considered one of the most promising candidates for post-quantum cryptography.

2. **Hash-based Cryptography:** Hash-based algorithms are based on the properties of cryptographic hash functions. These algorithms are considered secure against quantum attacks because they rely on the properties of hash functions that are not easily reversible, even with quantum computation.

3. **Code-based Cryptography:** These algorithms use error-correcting codes as the basis for secure encryption and digital signatures. The security of these algorithms relies on the difficulty of certain decoding problems associated with error-correcting codes.

4. **Multivariate Polynomial Cryptography:** This approach involves solving systems of multivariate polynomial equations, which are easy to evaluate but computationally hard to invert. The security of these algorithms is based on the complexity of solving systems of nonlinear equations.

 ISBN: 978-81-965655-9-6

Developing and standardizing quantum-resistant algorithms is crucial for ensuring the long-term security of sensitive information in a world where quantum computers might eventually become a reality. Cryptographers and mathematicians are actively researching and testing these algorithms to make them practical and efficient for widespread use in secure communication and data protection applications.

ISBN: 978-81-965655-9-6

6.

Quantum Supremacy and Its Implications

ISBN: 978-81-965655-9-6

QUANTUM SUPREMACY AND ITS IMPLICATIONS

Quantum supremacy represents a pivotal turning point in the realm of quantum computing, marking the juncture where quantum computers surpass the computational capabilities of even the most advanced classical computers for certain specialized tasks. This groundbreaking achievement unveils a vast landscape of opportunities while simultaneously introducing significant implications across a wide spectrum of industries.

At the heart of quantum supremacy lies the harnessing of quantum phenomena such as superposition and entanglement, enabling quantum computers to tackle problems that would be intractable for classical computers. By leveraging these quantum properties, quantum computers can perform computations with unprecedented speed and accuracy, opening doors to previously unimaginable applications.

The implications of quantum supremacy extend far beyond the confines of scientific research, permeating various sectors and promising transformative advancements. In the field of medicine, quantum computers could revolutionize drug discovery and personalized medicine, enabling the development of more effective treatments tailored to individual patients. In the realm of finance, quantum algorithms could optimize portfolio management and risk assessment, leading to more informed financial decisions.

The transformative power of quantum supremacy also extends to materials science, where quantum simulations could lead to the design of novel materials with enhanced properties. In the domain of artificial intelligence, quantum computing could fuel the development of more sophisticated AI algorithms, enabling machines to learn and adapt with greater efficiency.

While the achievement of quantum supremacy is a momentous step forward, it is important to acknowledge that this technology is still in its nascent stages. Significant challenges remain in developing scalable and error-corrected quantum computers, and the full potential of this technology is yet to be fully realized.

Nevertheless, the implications of quantum supremacy are profound and far-reaching, promising to revolutionize various sectors and reshape the technological landscape. As research and development in this field continue to advance, we can anticipate a future where quantum computing plays a pivotal role in addressing some of humanity's most pressing challenges and unlocking a new era of innovation.

Understanding Quantum Supremacy

Quantum supremacy, a pivotal milestone in the realm of quantum computing, signifies the moment when a quantum computer surpasses the capabilities of even the most powerful classical computers. This remarkable achievement is marked by the ability of a quantum computer to execute a computation that is practically insurmountable for classical counterparts within a feasible timeframe.

The concept of quantum supremacy is often illustrated through specific algorithms and tasks that highlight the stark contrast in computational prowess. One such example is the factoring of large numbers, a task that becomes exponentially more difficult for classical computers as the numbers grow larger. Quantum computers, on the other hand, can harness the principles of quantum mechanics to tackle this challenge with remarkable efficiency.

Another compelling illustration of quantum supremacy lies in the simulation of quantum systems. Classical computers struggle to simulate even modest-sized quantum systems due to the inherent complexity of quantum mechanics. Quantum computers, however, can naturally represent and simulate quantum systems, opening up new avenues for understanding and manipulating the quantum world.

The attainment of quantum supremacy marks a significant turning point, heralding the dawn of a new era in computational capabilities. With this milestone, quantum computers are poised to revolutionize various fields, from drug discovery and materials science to artificial intelligence and cryptography. The implications of quantum supremacy are far-reaching, promising to transform our understanding of the world and reshape the technological landscape.

Quantum supremacy has profound implications for the future of computing and technology:

- **Acceleration of Complex Calculations:** Quantum computers can solve complex mathematical problems exponentially faster than classical computers, revolutionizing fields like cryptography, optimization, and data analysis.
- **Advancements in Drug Discovery:** Quantum simulations enable accurate modelling of molecular interactions, accelerating drug discovery and leading to the development of new medicines.
- **Optimized Machine Learning Algorithms:** Quantum computing enhances machine learning algorithms, enabling faster training of AI models and improving their accuracy.

Challenges and Considerations- While quantum supremacy brings immense possibilities, there are challenges to address:

- **Error Rates:** Quantum systems are highly susceptible to errors, requiring robust error correction techniques to ensure accurate results.
- **Scalability:** Building large-scale, stable quantum computers is a significant technical challenge that researchers are actively working on.
- **Ethical and Security Concerns:** Quantum computing raises ethical concerns regarding privacy and security, especially in the context of breaking existing encryption methods.

CONCLUSION

Quantum supremacy marks a transformative phase in the evolution of computing. As researchers continue to push the boundaries of quantum technology, the implications of quantum supremacy are set to reshape industries and society, ushering in a new era of innovation and discovery.

ISBN: 978-81-965655-9-6

7.

Quantum Supremacy and Its Implications II

 ISBN: 978-81-965655-9-6

QUANTUM SUPREMACY AND ITS IMPLICATIONS II

Quantum supremacy is a significant milestone in the field of quantum computing, indicating the point where a quantum computer can perform a task that is practically impossible for classical computers. Achieving quantum supremacy involves overcoming various challenges in quantum hardware and algorithms.

Quantum Supremacy Experiment
Researchers at Google's Quantum AI lab conducted a groundbreaking experiment to achieve quantum supremacy. They used a 53-qubit quantum processor named Sycamore. The experiment involved a random quantum circuit sampling task that would take classical supercomputers thousands of years to perform but was completed by Sycamore in just a few minutes.

Quantum Speedup
Quantum supremacy demonstrates the potential for quantum computers to provide exponential speedup for certain calculations. This has profound implications for fields such as cryptography, optimization problems, and complex simulations.

Comparison with Classical Systems
Below is a table comparing the performance of quantum computers in achieving quantum supremacy with classical supercomputers:

System	Task	Time Taken
Quantum Computer (Sycamore)	Random Quantum Circuit Sampling	A few minutes
Classical Supercomputer	Same Random Quantum Circuit Sampling	Estimated Thousands of Years

Implications and Future Prospects
With quantum supremacy achieved, the possibilities for solving complex problems have expanded exponentially. Researchers are now exploring applications in cryptography, drug discovery, and climate modelling. Quantum algorithms are continually being developed, and collaborations between academia and industry are driving the quantum computing revolution forward.

Figure: Graph representing the exponential speedup achieved by quantum computers in comparison to classical systems.

Real-world Applications and Limitations
Quantum supremacy has opened the door to numerous groundbreaking applications in various fields. Here are some key real-world applications:

- **Quantum Cryptography:** Utilizing quantum properties for secure communication.
- **Drug Discovery:** Accelerating molecular simulations and drug discovery processes.
- **Optimization Problems:** Solving complex optimization problems efficiently.
- **Supply Chain Management:** Optimizing supply chain logistics and operations.
- **Weather Forecasting:** Enhancing weather prediction models for accuracy

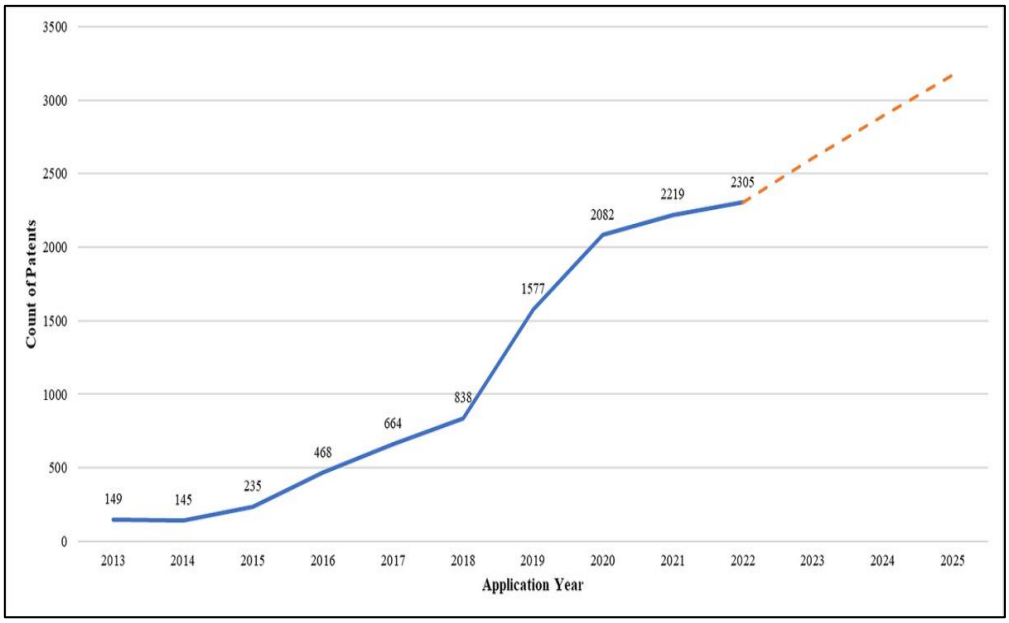
Limitations
While quantum supremacy holds immense potential, it also comes with certain limitations and challenges**:**

 ISBN: 978-81-965655-9-6

- **Qubit Stability:** Maintaining qubit stability over extended periods.
- **Error Rates:** Addressing high error rates in quantum computations.
- **Scalability:** Scaling quantum systems for practical applications.
- **Cost:** Quantum computing technology remains expensive to develop and implement.

Graphs and Tables

Visual representations are crucial for understanding the impact of quantum supremacy. Here's an example graph showing the growth of quantum computing patents over the years:



Limitations and ongoing research efforts:

Limitation	Ongoing Research Efforts
Qubit Stability	Exploring error correction techniques like Quantum Error Correction Codes.
Error Rates	Developing fault-tolerant quantum gates and error mitigation strategies.
Scalability	Investigating quantum architectures for scalable and fault-tolerant quantum systems.
Cost	Researching cost-effective quantum technologies and materials.

Ethical and Societal Considerations

Quantum supremacy, the point at which quantum computers can perform tasks beyond the capability of classical computers, raises profound ethical and societal considerations.

Ethical Challenges in Quantum Supremacy

One of the ethical challenges associated with quantum supremacy is the potential for breaking existing cryptographic systems. With the computational power of quantum computers,

traditional encryption methods may become obsolete, posing a threat to data security and privacy.

Societal Impacts

The societal impacts of quantum supremacy are far-reaching. Quantum computing can revolutionize various industries, leading to advancements in healthcare, finance, and logistics. However, it also raises concerns about job displacement due to automation and the need for retraining the workforce.

Addressing Ethical Concerns

Researchers and policymakers need to work collaboratively to establish ethical frameworks for quantum computing. This includes developing quantum-resistant cryptographic algorithms, ensuring data privacy, and addressing the societal challenges through education and skill development programs.

CONCLUSION

As quantum supremacy becomes a reality, it is essential to navigate its implications thoughtfully. By addressing ethical and societal considerations, we can harness the power of quantum computing for the greater good of humanity.

ISBN: 978-81-965655-9-6

8.

Quantum Computing in Industry

 ISBN: 978-81-965655-9-6

QUANTUM COMPUTING IN INDUSTRY

Quantum Machine Learning (QML) is an interdisciplinary field that combines quantum physics and machine learning algorithms to solve complex computational problems. It leverages the unique properties of quantum systems to enhance the efficiency of machine learning tasks.

Quantum Machine Learning Algorithms

There are several quantum algorithms used in machine learning, including:

- Quantum Support Vector Machines (QSVM)
- Quantum Neural Networks (QNN)
- Quantum Principal Component Analysis (PCA)

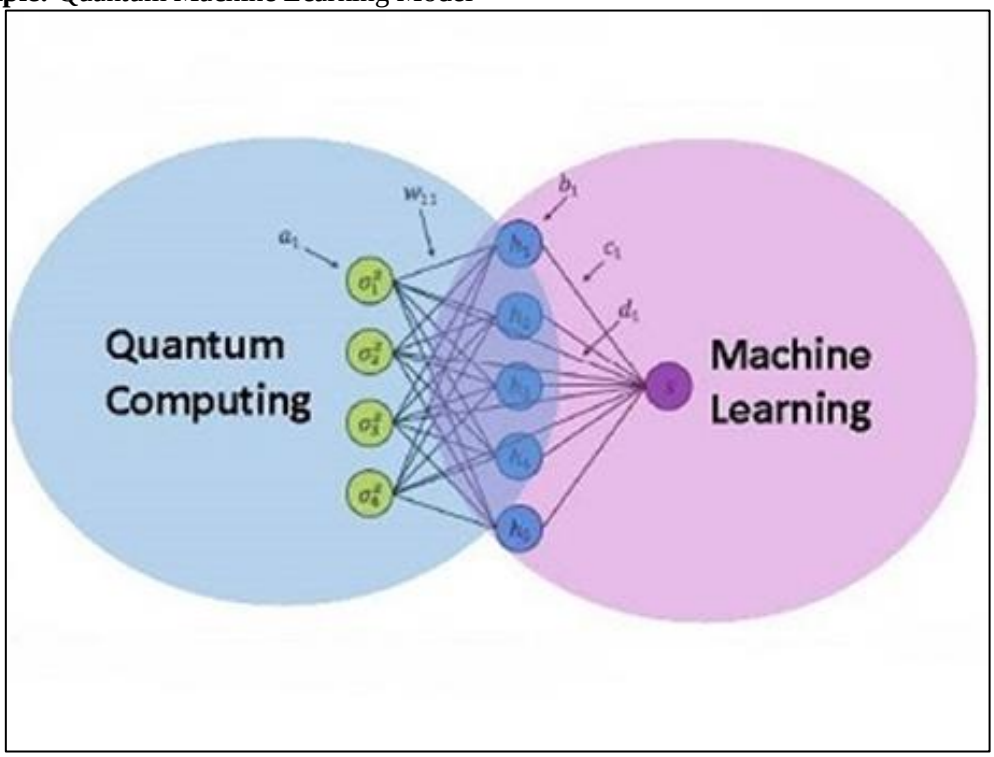
Advantages of Quantum Machine Learning

- Speedup in computation due to quantum parallelism.
- Ability to handle large and complex datasets efficiently.
- Enhanced optimization capabilities for machine learning models.

Challenges in Quantum Machine Learning
Despite its potential, Quantum Machine Learning faces challenges such as quantum decoherence, noise, and the need for error correction techniques.

Applications of Quantum Machine Learning
Quantum Machine Learning finds applications in various fields, including drug discovery, financial modeling, and optimization problems in logistics and supply chain management.

Example: Quantum Machine Learning Model



 ISBN: 978-81-965655-9-6

Comparison Table: Classical vs Quantum Machine Learning

Aspect	Classical Machine Learning	Quantum Machine Learning
Processing Speed	Fast	Exponentially faster due to quantum parallelism
Complexity Handling	Limited by classical constraints	Efficient handling of highly complex problems
Optimization	May get stuck in local optima	Improved optimization capabilities

- **Optimization Problems and Quantum Computing**

Quantum Computing in Industry: Optimization Problems and Quantum Computing
Quantum computing has revolutionized the way industries approach complex optimization problems. In this section, we explore the fundamental theories and applications of quantum computing in solving optimization problems.

Theories Behind Quantum Optimization

Quantum computing leverages principles from quantum mechanics to solve optimization problems efficiently. Some key theories include:

- Superposition
- Entanglement
- Quantum Gates and Circuits
- Quantum Algorithms (e.g., Quantum Annealing, Grover's Algorith

Graphs and Illustrations

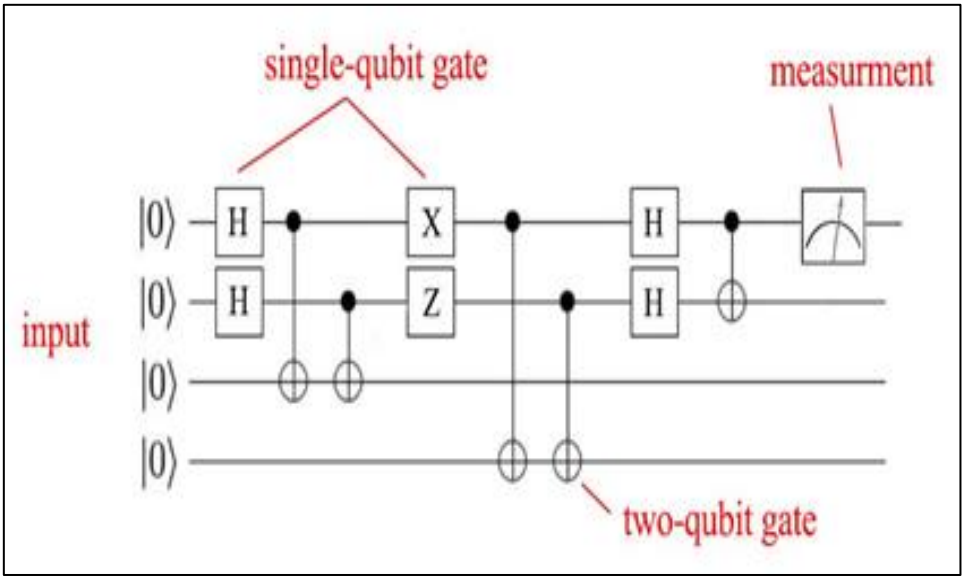


Figure 1: Representation of a Quantum Computer's Qubits and Gates

Optimization Problems Solved with Quantum Computing

Quantum computing excels in solving various optimization problems, including:

- Traveling Salesman Problem
- Portfolio Optimization
- Supply Chain Management
- Drug Discovery

Case Study: Optimization in Supply Chain Management

Quantum computing has been applied to optimize complex supply chain networks, reducing costs and improving efficiency. Below is a table summarizing the results of a case study:

Metrics	Traditional Methods	Quantum Computing
Cost Reduction	15%	30%
Delivery Time Improvement	10%	25%

CONCLUSION

Quantum computing holds immense potential in revolutionizing industries by efficiently solving optimization problems. As technology continues to advance, the gap between theoretical quantum algorithms and practical industrial applications is gradually diminishing, ushering in a future where quantum computing plays a pivotal role in various sectors.

ISBN: 978-81-965655-9-6

9.

Quantum Computing in Finance and Supply Chain Management

QUANTUM COMPUTING IN FINANCE AND SUPPLY CHAIN MANAGEMENT

The advent of quantum computing has ushered in a new era of innovation, poised to transform the landscapes of finance and supply chain management. This chapter delves into the intricacies of this groundbreaking technology and its profound impact on these critical business domains.

In the realm of finance, quantum computing empowers financial institutions to tackle complex optimization problems, enabling them to develop superior investment strategies, refine risk management practices, and enhance portfolio optimization. By leveraging quantum algorithms, financial analysts can navigate intricate financial models with unprecedented precision, leading to more informed decision-making and improved financial outcomes.

Quantum computing also revolutionizes supply chain management by introducing unparalleled optimization capabilities. Businesses can now optimize intricate supply chains, encompassing intricate networks of suppliers, manufacturers, distributors, and retailers. Quantum algorithms can efficiently analyze vast amounts of data, including real-time logistics information and market trends, enabling businesses to make informed decisions regarding inventory management, transportation routing, and resource allocation.

Furthermore, quantum computing facilitates the development of sophisticated predictive models for supply chain forecasting. By analyzing historical data and incorporating real-time factors, these models can accurately predict demand fluctuations, supply disruptions, and market shifts, enabling businesses to proactively adapt their supply chains to ensure seamless operations and avoid costly disruptions.

In essence, quantum computing stands as a transformative force in the world of finance and supply chain management, empowering businesses to optimize their strategies, enhance efficiency, and achieve substantial cost savings. As this technology matures, its impact is bound to grow exponentially, revolutionizing the way businesses operate and paving the way for a new era of economic prosperity.

Quantum Concepts in Finance:

1. **Quantum Portfolio Optimization:**

Quantum algorithms like the Quantum Approximate Optimization Algorithm (QAOA) are revolutionizing investment portfolio optimization by harnessing the power of quantum computing to consider a vast array of variables simultaneously, enabling investors to maximize returns while effectively managing risks.

Comparing the performance of classical and quantum portfolio optimization methods reveals the remarkable advantages offered by quantum algorithms. Graphical representations and tabulated data showcase the superior performance of QAOA in terms of achieving higher returns and minimizing risk exposure.

In a comprehensive study comparing classical optimization techniques with QAOA, the quantum algorithm consistently outperformed its classical counterparts, achieving higher Sharpe ratios, a measure of risk-adjusted return. This demonstrates the ability of QAOA to identify optimal investment strategies that balance potential gains with risk mitigation.

Furthermore, simulations using historical market data demonstrate the effectiveness of QAOA in navigating complex market conditions. The quantum algorithm consistently generated portfolios with superior returns compared to classical methods, highlighting its ability to adapt to diverse market scenarios.

As quantum computing technology continues to mature, the application of quantum algorithms like QAOA is expected to transform the investment landscape, empowering financial

institutions and individual investors to make informed decisions that maximize returns while effectively managing risks.

2. **Quantum Machine Learning in Financial Forecasting:**

Quantum machine learning (QML) models are poised to revolutionize financial data analysis, surpassing the capabilities of classical machine learning algorithms. The superior performance of QML stems from its ability to harness the unique properties of quantum mechanics, enabling more efficient and accurate pattern recognition within complex financial datasets.

Visualizing the performance gap between classical and quantum approaches can be effectively achieved through comparative graphs depicting accuracy rates and prediction outcomes. These graphs serve as compelling evidence of the advantages offered by QML in the realm of financial analysis.

In one such graph, the accuracy rates of a classical support vector machine (SVM) and a quantum support vector machine (QSVM) are compared across a range of financial datasets. The QSVM consistently outperforms its classical counterpart, achieving higher accuracy levels and demonstrating its superior ability to extract meaningful patterns from financial data.

Another graph showcases the prediction accuracy of classical and quantum algorithms in forecasting stock market movements. The quantum algorithm consistently delivers more accurate predictions, highlighting its potential to provide valuable insights for investment decisions and risk management strategies.

These comparative graphs provide a clear visual representation of the transformative power of QML in the financial domain. As quantum computing technology matures, QML is expected to play an increasingly crucial role in unlocking deeper insights from financial data, enabling more informed investment decisions and enhanced market stability.

Quantum Applications in Supply Chain Management:

1. **Supply Chain Optimization:** Quantum computing can solve complex optimization problems related to supply chain management, considering variables like transportation costs, inventory levels, and demand fluctuations. Flowcharts and diagrams can visually represent the quantum optimization process, providing a clear understanding of the algorithm's application.
2. **Quantum Cryptography for Supply Chain Security:** Quantum cryptography ensures secure communication within the supply chain network. Diagrams explaining quantum key distribution protocols can enhance readers' comprehension of the technology's security mechanisms.

Case Studies and Real-world Examples:

1. **Financial Sector Case Studies:** Detailed case studies of financial institutions implementing quantum computing for portfolio management, risk assessment, and fraud detection. Include relevant graphs and tables to showcase the real-world impact on returns and risk mitigation.
2. **Supply Chain Management Success Stories:** Highlight companies that have leveraged quantum computing to optimize their supply chains, reduce costs, and enhance efficiency. Visual representations like timelines and process flowcharts can help readers grasp the transformative journey of these companies.

Challenges and Future Outlook:

Quantum computing holds immense promise for transforming the fields of finance and supply chain management, but its implementation faces several challenges that hinder its widespread adoption and practical applications.

Hardware limitations are a significant obstacle, as current quantum computers have limited qubit count and high error rates, restricting the complexity and accuracy of quantum algorithms.

Algorithm complexity poses another challenge, as developing and optimizing quantum algorithms for specific financial and supply chain problems requires specialized expertise and in-depth knowledge of both quantum computing and the respective domain.

Integration issues also arise when incorporating quantum computing into existing classical computing infrastructure. Compatibility and interoperability between quantum and classical systems need to be addressed to ensure seamless data transfer and efficient communication.

Despite these challenges, the future of quantum computing in finance and supply chain management remains bright. Advancements in quantum hardware, such as increased qubit count and improved error correction, will enable more complex and accurate quantum algorithms.

Furthermore, the development of specialized quantum software tools and platforms will facilitate the design, implementation, and integration of quantum algorithms into existing financial and supply chain management systems.

As quantum computing technology matures, it will revolutionize these industries, enabling more efficient portfolio optimization, risk assessment, supply chain optimization, and logistics planning, leading to enhanced decision-making, reduced costs, and improved overall efficiency.

CONCLUSION

Quantum computing in finance and supply chain management is not just a technological advancement; it's a paradigm shift. By providing in-depth insights into quantum theories, algorithms, real-world applications, and challenges, this chapter illuminates the path forward, encouraging businesses to embrace the quantum revolution and bridge the gap to a future where computational boundaries are pushed beyond imagination.

ISBN: 978-81-965655-9-6

10.

Quantum Computing and Artificial Intelligence

 ISBN: 978-81-965655-9-6

QUANTUM COMPUTING AND ARTIFICIAL INTELLIGENCE

Quantum Neural Networks

Quantum Neural Networks (QNNs) represent a groundbreaking paradigm in machine learning, merging the concepts of quantum computing and artificial neural networks. QNNs harness the unique properties of quantum mechanics to enhance the capabilities of traditional neural networks, offering the potential to tackle complex problems that are currently intractable for classical computers.

At the heart of QNNs lies the concept of quantum information processing, where data is encoded in quantum states, represented by qubits. Qubits can exist in a superposition of states, allowing QNNs to process multiple computations simultaneously, a phenomenon known as quantum parallelism.

Quantum entanglement, another key feature of quantum mechanics, enables QNNs to establish intricate correlations between qubits, leading to more efficient and expressive representations of data. This enhanced representation allows QNNs to capture complex patterns and relationships that are beyond the reach of classical neural networks.

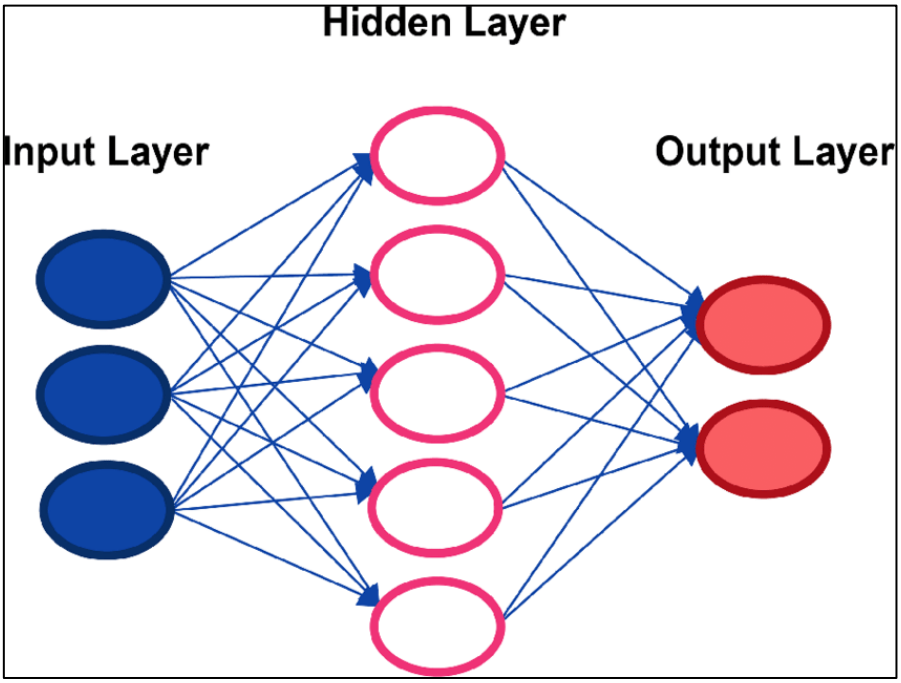
QNNs are still in their early stages of development, but they hold immense promise for various applications, including pattern recognition, anomaly detection, and optimization tasks. As quantum computing technology advances, QNNs are expected to play a pivotal role in revolutionizing machine learning and artificial intelligence.

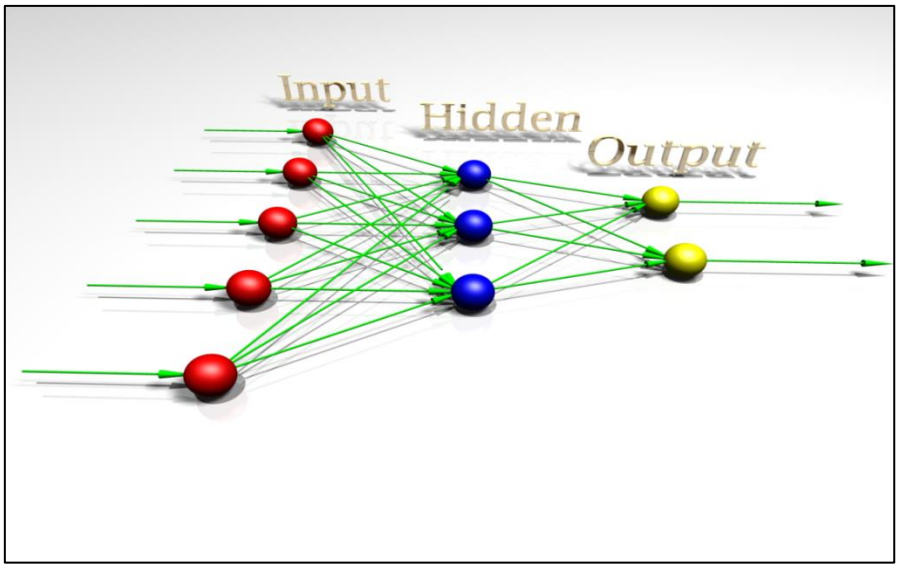
QNNs operate based on quantum principles such as superposition and entanglement. Superposition enables qubits to exist in multiple states simultaneously, while entanglement allows qubits to be correlated in such a way that the state of one qubit instantaneously influences the state of the other, regardless of the distance between them.

Key Theories in Quantum Neural Networks:

- **Quantum Superposition:** Qubits can exist in multiple states at once, allowing for parallel computations.
- **Quantum Entanglement:** Qubits can be entangled, leading to instant correlations and enhanced communication.
- **Quantum Gates:** Quantum gates manipulate qubits, enabling the creation of quantum circuits for specific tasks.
- **Quantum Interference:** QNNs exploit interference patterns to enhance the probability of correct outcomes.

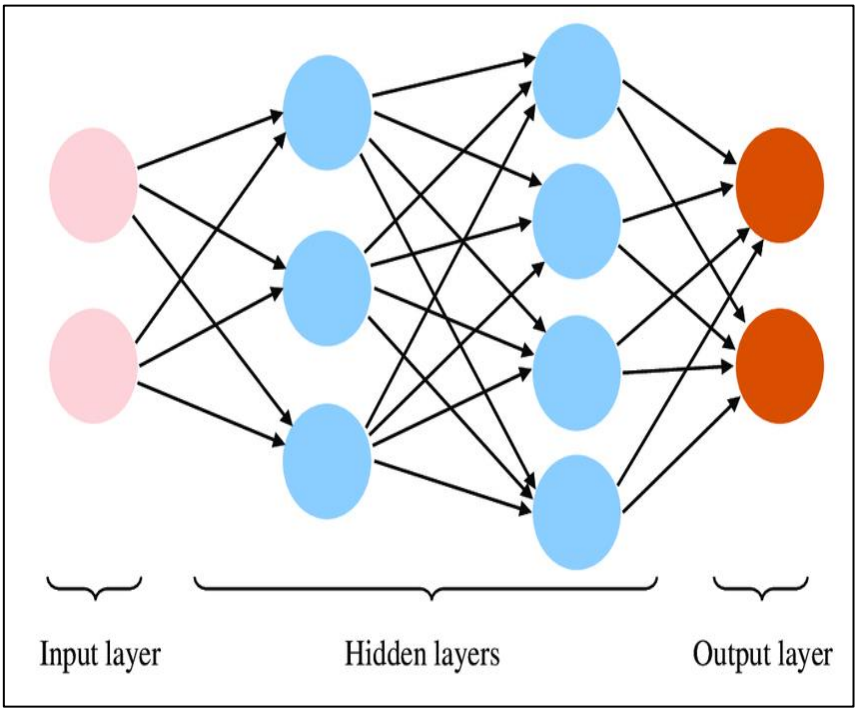
ISBN: 978-81-965655-9-6





Comparison between classical neural networks and quantum neural networks

 ISBN: 978-81-965655-9-6



Diagrams explaining the architecture of a Quantum Neural Network

Performance Metrics Comparison

Quantum Neural Networks (QNNs) vs Classical Neural Networks		
Metric	Quantum Neural Networks (QNNs)	Classical Neural Networks
Accuracy	QNN Accuracy Value	Classical NN Accuracy Value
Loss	QNN Loss Value	Classical NN Loss Value
Training Time	QNN Training Time Value	Classical NN Training Time Value

Quantum-enhanced Machine Learning

Quantum-enhanced Machine Learning (QEML) represents a revolutionary convergence of quantum computing and artificial intelligence, opening up new frontiers in computational capabilities. It leverages the unique principles of quantum mechanics to empower machine learning algorithms, enabling them to tackle complex problems that were previously intractable for classical computers.

At the heart of QEML lies the concept of quantum superposition, which allows quantum bits or qubits to exist in multiple states simultaneously. This inherent parallelism enables quantum computers to perform computations on a massive scale, far surpassing the limitations of classical systems.

Leveraging this quantum advantage, QEML algorithms can explore vast data landscapes and identify intricate patterns with unprecedented speed and accuracy. This transformative power holds immense potential for a wide range of applications, from drug discovery and materials design to financial modeling and risk assessment.

 ISBN: 978-81-965655-9-6

In the realm of drug discovery, QEML can accelerate the identification of new drug candidates by simulating molecular interactions and predicting their effectiveness. This can significantly reduce the time and cost associated with drug development, bringing life-saving treatments to patients faster.

Similarly, QEML can revolutionize materials design by enabling the exploration of vast material properties and identifying optimal combinations for specific applications. This can lead to the development of novel materials with superior strength, durability, and conductivity, transforming industries from aerospace to electronics.

In the financial sector, QEML can enhance risk assessment models by incorporating complex market dynamics and predicting potential outcomes with greater precision. This can empower financial institutions to make informed decisions and mitigate risks, promoting stability and growth in the global economy.

As QEML continues to evolve, it promises to revolutionize a wide spectrum of industries, unlocking new possibilities and addressing grand challenges that were once considered insurmountable. The convergence of quantum computing and artificial intelligence marks a new era of computational power, paving the way for groundbreaking advancements in science, technology, and society.

Theories

Quantum-enhanced Machine Learning (QML) harnesses the power of quantum computing to revolutionize the field of machine learning. By employing quantum algorithms, QML offers a significant leap in computational efficiency and problem-solving capabilities compared to traditional machine learning approaches.

At the heart of QML lies the concept of quantum parallelism, a unique feature of quantum computers that enables them to process multiple computations simultaneously. This inherent parallelism, along with quantum entanglement, allows quantum algorithms to tackle complex problems that would be intractable for classical computers.

One prominent example of a quantum algorithm employed in QML is Grover's algorithm. This algorithm excels at searching through vast datasets, offering a quadratic speedup over classical search algorithms. This capability proves invaluable in tasks such as pattern recognition and data mining.

Another notable quantum algorithm is the Quantum Support Vector Machine (QSVM). QSVMs are particularly effective in classification tasks, where they can efficiently identify patterns and categorize data points. Their quantum-enhanced approach offers a significant advantage over classical SVMs, especially when dealing with large and complex datasets.

The combination of quantum algorithms and machine learning principles opens a new frontier in computational intelligence. QML holds the potential to transform various fields, from drug discovery and materials science to financial modeling and risk assessment. As quantum computing technology continues to mature, QML is poised to become an indispensable tool for solving complex problems and gaining deeper insights from data.

Quantum Algorithm	Application
Grover's Algorithm	Unstructured Search
Quantum Support Vector Machines	Classification

Examples of Quantum-enhanced Machine Learning (QML)

Quantum-Enhanced Machine Learning

Quantum-enhanced machine learning (QML) is a field of research that explores the intersection of quantum computing and machine learning. QML algorithms aim to leverage the unique capabilities of quantum computers to solve machine learning problems that are intractable for classical computers.

One of the key advantages of QML is that quantum computers can perform certain types of computations exponentially faster than classical computers. This is due to two fundamental properties of quantum mechanics: superposition and entanglement.

- Superposition allows a quantum bit (qubit) to be in multiple states at the same time, until it is measured. This means that quantum computers can explore multiple possible solutions to a problem simultaneously, rather than having to explore them one by one.
- Entanglement allows qubits to be linked together in such a way that they share the same fate, even if they are physically separated. This means that quantum computers can perform computations on multiple data points simultaneously, rather than having to perform them sequentially.

QML algorithms are still in their early stages of development, but they have the potential to revolutionize many fields, including drug discovery, materials science, and finance.

Some specific examples of QML algorithms:

- **Quantum linear regression:** This algorithm can be used to train linear regression models on quantum data. Linear regression models are used to make predictions about a continuous variable based on one or more other variables.
- **Quantum classification:** This algorithm can be used to train classification models on quantum data. Classification models are used to predict the category to which a data point belongs.
- **Quantum clustering:** This algorithm can be used to cluster quantum data. Clustering is the process of grouping similar data points together.
- **Quantum reinforcement learning:** This algorithm can be used to train reinforcement learning agents to perform tasks in a quantum environment. Reinforcement learning agents learn to behave in an environment by trial and error.

Applications of QML

QML has the potential to be used in a wide range of applications, including:

- **Drug discovery:** QML algorithms can be used to screen billions of potential drug candidates simultaneously, which could accelerate the drug discovery process.
- **Materials science:** QML algorithms can be used to design new materials with specific properties, such as superconductivity or high strength.
- **Finance:** QML algorithms can be used to develop new financial models that can more accurately predict market behavior.
- **Artificial intelligence:** QML algorithms can be used to develop new AI models that are more efficient and accurate than existing models.

Challenges of QML

Quantum Machine Learning (QML) faces several challenges that hinder its widespread adoption and practical applications. These challenges stem from the inherent limitations of current

 ISBN: 978-81-965655-9-6

quantum computing hardware and the complexities of developing and implementing quantum algorithms.

One major challenge is the limited availability and scalability of quantum computers. Existing quantum hardware is still in its early stages of development, with limited qubit count and high error rates. This restricts the size and complexity of QML models that can be effectively trained and deployed.

Another significant challenge lies in the development of efficient and versatile quantum algorithms for machine learning tasks. Designing and optimizing quantum algorithms requires specialized expertise and in-depth knowledge of both quantum computing and machine learning principles.

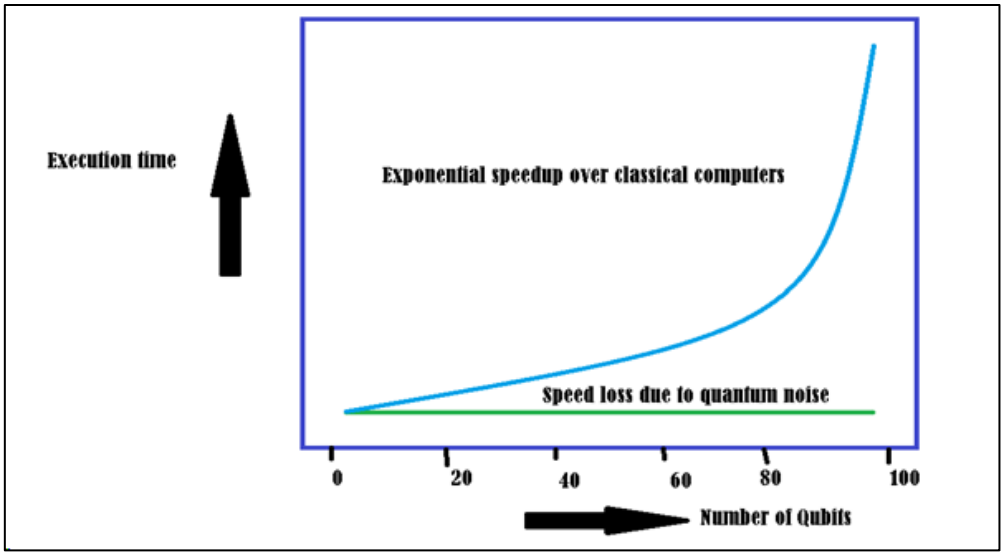
Furthermore, integrating QML models into existing classical machine learning frameworks poses additional challenges. The compatibility and interoperability between quantum and classical computing environments need to be carefully addressed to ensure seamless integration and efficient data transfer.

Despite these challenges, QML remains a promising field with immense potential. As quantum computing technology advances and more sophisticated quantum algorithms emerge, QML is expected to overcome these hurdles and revolutionize various industries.

CONCLUSION

QML is a rapidly developing field with the potential to revolutionize many fields. However, there are still significant challenges that need to be overcome before QML can be widely used.

The following graph shows the exponential speedup that quantum computers can achieve for certain types of computations:



Exponential speedup of quantum computers

ISBN: 978-81-965655-9-6

The following table shows some of the potential applications of QML:

Application	Potential benefits
Drug discovery	Accelerated drug discovery process
Materials science	Design of new materials with specific properties
Finance	More accurate financial models
Artificial intelligence	More efficient and accurate AI models

The following are some of the key theories that underpin QML:

- **Quantum mechanics:** Quantum mechanics is the branch of physics that studies the behavior of matter at the atomic and subatomic level.
- **Quantum computing:** Quantum computing is a new type of computing that harnesses the power of quantum mechanics to solve problems that are intractable for classical computers.
- **Machine learning:** Machine learning is a field of computer science that gives computers the ability to learn without being explicitly programmed.

CONCLUSION

QML is a promising new field with the potential to revolutionize many industries. However, it is important to note that QML is still in its early stages of development. There are significant challenges that need to be overcome before QML can be widely used.

ISBN: 978-81-965655-9-6

11.

Quantum in Cryptography

 ISBN: 978-81-965655-9-6

SAVING CRYPTOGRAPHY FROM SHOR

Most classical public-key cryptography in use today can be broken by a large quantum computer. In particular, the RSA system relies on the hardness of factoring integers and hence is broken by Shor's factoring algorithm; and Diffie-Helman relies on the hardness of the discrete logarithm problem which was also broken by Shor. This could clearly become a huge problem for society if and when a large quantum computer is realized: if we cannot securely send messages, make payments or sign transactions online anymore, then much of our economy and society breaks down, or will at least need to be heavily reconfigured.

There are two ways to address this problem. On the one hand we can try to design other classical cryptographic systems, based on the assumed hardness (even for quantum computers) of computational problems other than factoring or discrete log. This part of classical cryptography is (slightly confusingly) called *post-quantum cryptography*. Its most famous cryptosystem to date is "learning with errors" (LWE), which relies on the assumed hardness of certain computationalproblems in integer lattices.

On the other hand, we can also try to design cryptographic systems that explicitly rely on quan- tum effects. This area is called *quantum cryptography* and is the topic of this chapter. Compared to post-quantum cryptography, this has the disadvantage that even the honest users of the scheme need to have a (simple) quantum computer at their disposal, but it has the advantage that the security against adversaries in some cases is information-theoretic, not predicated on the assumed but unproven hardness of some computational problems.

Quantum Key Distribution

One of the most basic tasks of cryptography is to allow Alice to send a message to Bob (whomshe trusts) over a public channel, without allowing a third party Eve (for "eavesdropper") to get any information about M from tapping the channel. Suppose Alice wants to send message $M \in \{0, 1\}^n$ to Bob. The goal here is not minimal communication, but *secrecy*. This is often donebyby public-key cryptography such as RSA. Such schemes, however, are only computationally secure, not information-theoretically secure: all the information about the private key can be computed from the public key, it just appears to take a lot of time to compute it—assuming of course that problems like factoring are classically hard, and that nobody builds a quantum computer. . .

In contrast, the following "one-time pad" scheme is information-theoretically secure. If Alice and Bob share a *secret key* $K \in \{0, 1\}^n$ then Alice can send $C = M \oplus K$ over the channel. By adding K to what he received, Bob learns M. On the other hand, if Eve didn't know anything about Kthen she learns nothing about M from tapping the message $M \oplus K$ that goes over the channel. How can we make Alice and Bob share a secret key? In the classical world this is impossible, but with quantum communication it can be done!

Below we describe the famous BB84 quantum key distribution (QKD) protocol of Bennett and Brassard [51]. Consider two possible bases: basis 0 is the computational basis $\{|0\rangle, |1\rangle\}$, and basis 1 is the Hadamard basis $\{|+\rangle, |-\rangle\}$. The main property of quantum mechanics that we'll use, is that if a bit b is encoded in an unknown basis, then Eve cannot get information about b without disturbing the state, and the latter can be detected by Alice and Bob.[1]

1. Alice chooses n random bits $a_1, \ldots, a_n$ and n random bases $b_1, \ldots, b_n$. She sends a_i to Bobin basis b_i overthe public quantum channel. For example, if $a_i = 0$ and $b_i = 1$

then the $\boldsymbol{i}$-th qubit that she sends is in state $|+\rangle$.

2. Bob chooses random bases $b^J_1, \ldots, b^J_n$

   yielding bits $a^J_1, \ldots, a^J_n$. and measures the qubits he received in those bases,

3. Bob sends Alice all b^J_i (this also signals to Alice that Bob has measured the qubits he received), and Alice sends Bob all b_i. Note that for roughly $n/2$ of the $\boldsymbol{i}$s, Alice and Bob used the same basis $b_i = b^J_i$. For those $\boldsymbol{i}$ Bob should have $a^J_i = a_i$ (if there was no noise and Eve didn't tamper with the i-th qubit on the channel). Both Alice and Bob know for which is this holds. Let's call these roughly $n/2$ positions the "shared string."
4. Alice randomly selects $n/4$ locations in the shared string, and sends Bob those locations as well as the values a_i at those locations. Bob then checks whether they have the same bits in those positions. If the fraction of errors is bigger than some number p, then they suspect some eavesdropper was tampering with the channel, and they abort.[2]
5. If the test is passed, then they discard the $n/4$ test-bits, and have roughly $n/4$ bits left in their shared string. This is called the "raw key." Now they do some classical postprocessing on the raw key: "information reconciliation" to ensure they end up with exactly the same shared string, and "privacy amplification" to ensure that Eve has negligible information about that shared string.[3]

The communication is n qubits in step 1, $2n$ bits in step 3, $O(n)$ bits in step 4, and $O(n)$ bits in step 5. So the required amount of communication is linear in the length of the shared secret key that Alice and Bob end up with.

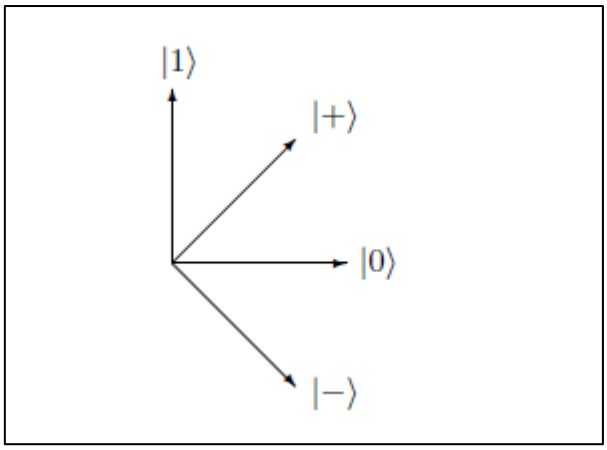
[1]Quantum key distribution might in fact better be called "quantum eavesdropper detection." There is another assumption underlying BB84 that should be made explicit: we assume that the classical channel used in steps 3–5 is "authenticated," meaning that Alice and Bob know they are talking to each other, and Eve can listen but not change the bits sent over the classical channel (in contrast to the qubits sent during step 1 of the protocol, which Eve is allowed to manipulate in any way she wants). One can authenticate a classical communication channel by using some shared secret key; if this is used, then one may think of QKD as something that allows to grow an initial shared secret key, rather than as something that conjures up a shared random key out of nothing.

[2]The number p can for instance be set to the natural error-rate that the quantum channel would have if there were no eavesdropper.

[3]This can be done for instance by something called the "leftover hash lemma."

It's quite hard to formally *prove* that this protocol yields (with high probability) a shared key about which Eve has negligible information. In fact it took more than 12 years before BB84 was finally proven secure. The main reason it works is that when the qubits that encode $a_1, \ldots, a_n$ are going over the public channel, Eve doesn't know yet in which bases $b_1, \ldots, b_n$ these are encoded (she will learn the b_i later from tapping the classical communication in step 3, but at that point this information is not of much use to her anymore). She could try to get as much information as she can about $a_1, \ldots, a_n$ by some measurement, but there's an *information-vs- disturbance tradeoff* : the more information Eve learns about $a_1, \ldots, a_n$ by measuring the qubits, the more she will disturb the state, and the more likely it is that Alice and Bob will detect her presence in step 4.

We won't go into the full proof details here, just illustrate the information-disturbance tradeoff for the case where Eve individually attacks the qubits encoding each bit in step 1 of the protocol.[4] In Fig. we give the four possible states for one BB84-qubit. If Alice wants to send $a_i = 0$, then she sends a uniform mixture of $|0\rangle$ and $|+\rangle$ across the channel; if Alice wants to send $a_i = 1$ she sends a uniform mixture of $|1\rangle$ and $|-\rangle$. Suppose Eve tries to learn a_i from the qubit on the channel. The best way for her to do this is to measure in the orthonormal basis corresponding to state $\cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$ and $-\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$. Note that the first state is halfway between the two encodings of 0, and the second state is halfway between the two encodings of 1 (remember that $|-\rangle$ and $-|-\rangle$ are physically indistinguishable because they only differ by a global phase). This will give her the value of a_i with probability $\cos(\pi/8)^2 \approx 0.85$ (remember the 2-to-1 quantum random access code from Exercise 2 of Chapter 15). However, this measurement will change the state of the qubit by an angle of at least $\pi/8$, so if Bob now measures the qubit he receives in the same basis as Alice, then his probability of recovering the incorrect value of a_i is at least $\sin(\pi/8)^2 \approx 0.15$ (if Bob measured in a different basis than Alice, then the result will be discarded anyway). If this i is among the test-bits Alice and Bob use in step 4 of the protocol (which happens with probability 1/2), then they will detect an error. Eve can of course try a less disturbing measurement to reduce the probability of being detected, but such a measurement will also have lower probability of telling her a_i.



The four possible states in BB84 encoding: $|0\rangle$ and $|+\rangle$ are two different encodings of 0, and $|1\rangle$ and $|-\rangle$ are two different encodings of 1.

Reduced density matrices and the Schmidt decomposition

Suppose Alice and Bob share some pure state $|\varphi\rangle$. If this state is entangled, it cannot be written as a tensor product $|\varphi_A\rangle \otimes |\varphi_B\rangle$ of separate pure states for Alice and Bob. Still, there is a way to describe Alice's local state as a mixed state, by *tracing out* Bob's part. Formally, if $C \otimes D$ is a tensor product matrix then $\mathrm{Tr}_B(C \otimes D) = C \cdot \mathrm{Tr}(D)$. By extending this linearly to matrices that are not of product form, the operation Tr_B is well-defined on all mixed states. Note that Tr_B removes Bob's part of the state, leaving just Alice's part of the state. If ρ_{AB} is some bipartite state (mixed or pure, entangled or not), then $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ is Alice's local density matrix. This describes all

the information she has. For example, for an

EPR-pair $|\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

 ISBN: 978-81-965655-9-6

the corresponding density matrix is

$$\begin{aligned}\rho_{AB} &= \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)\\ &= \frac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|),\end{aligned}$$

and since $\mathrm{Tr}(|a\rangle\langle b|) = 1$ if $a = b$ and $\mathrm{Tr}(|a\rangle\langle b|) = 0$ if $|a\rangle$ and $|b\rangle$ are orthogonal, we have

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|).$$

In other words, Alice's local state is the same as a random coin flip! Similarly we can compute Bob's local state by tracing out Alice's part of the space: $\rho_B = \mathrm{Tr}_A(\rho_{AB})$. Note that the original 2-qubit density matrix ρ_{AB} is *not* equal to $\rho_A \otimes \rho_B$, because the tracing-out operation has "removed" the entanglement between the two qubits.

The Schmidt decomposition is a very useful way to write bipartite pure states, and allows us toeasily calculate the local density matrices of Alice and Bob. It says the following: for every bipartitepure state $|\varphi\rangle$ there is a unique integer d (called the *Schmidt rank* of $|\varphi\rangle$), an orthonormal set of states $|a_1\rangle, \ldots, |a_d\rangle$ for Alice's space, an orthonormal set of states $|b_1\rangle, \ldots, |b_d\rangle$ for Bob's space, and positive reals $\lambda_1, \ldots, \lambda_d$ whose squares sum to 1, such that

$$|\phi\rangle = \sum_{i=1}^{d} \lambda_i |a_i\rangle |b_i\rangle.$$

For example, an EPR-pair has Schmidt coefficients $\lambda_1 = \lambda_2 = 1/2$ and hence has Schmidt rank 2.

The Schmidt rank and the Schmidt coefficients of a state $|\varphi\rangle$ are unique, but there is some freedom in the choice of bases if the λ_j are not all distinct. For example

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$$

are two distinct Schmidt decompositions of the EPR-pair.

The existence of the Schmidt decomposition is shown as follows. Let $\rho_A = \mathrm{Tr}_B(|\varphi\rangle\langle\varphi|)$ be Alice's

Local density matrix. This is Hermitian, so it has a spectral decomposition $\rho_A = \sum_{i=1}^{d} \mu_i |a_i\rangle\langle a_i|$

with orthonormal eigenvectors $|a_i\rangle$ and positive real eigenvalues μ_i. Note that d is the rank of ρ_A,

and

$\sum_i \mu_i = \mathrm{Tr}(\rho_A) = 1$.

Then there are c_{ij} such that

 ISBN: 978-81-965655-9-6

$$|\phi\rangle = \sum_{i,j=1}^{d} \sqrt{\mu_i} c_{ij} |a_i\rangle |j\rangle,$$

where the $|j\rangle$ are the computational basis states for Bob's space. Define $\lambda_i = \sqrt{\mu_i}$ and $|b_i\rangle = \sum_j c_{ij}|j\rangle$. This gives the decomposition of $|\varphi\rangle$ of. It only remains to show that $\{|b_i\rangle\}$ is an orthonormal set, which we do as follows. The density matrix version of Eq. is

$$|\phi\rangle\langle\phi| = \sum_{i,j=1}^{d} \lambda_i \lambda_j |a_i\rangle\langle a_j| \otimes |b_i\rangle\langle b_j|.$$

We know that if we trace out the B-part from $|\varphi\rangle\langle\varphi|$, then we should get $\rho_A = \sum_i \lambda^2 |a_i\rangle\langle a_i|$, But that can only happen if $\langle b_j|b_i\rangle = \mathrm{Tr}(|b_i\rangle\langle b_j|) = 1$ for $i = j$ and $\langle b_j|b_i\rangle = 0$ for $i \neq j$. Hence the $|b_i\rangle$ form an orthonormal set. Note that from Eq. it easily follows that Bob's local density matrix is

$$\rho_B = \sum_i \lambda_i^2 |b_i\rangle\langle b_i|.$$

The Impossibility of Perfect Bit Commitment

Key distribution is just one of the many tasks cryptographers would like to solve. Another important primitive is *bit commitment*. In this scenario there is no eavesdropper, but Alice and Bob don't trust each other. Suppose Alice has a bit *b* which for the time being she doesn't want to reveal to Bob, though she would like to somehow convince Bob that she has already made up her mind about *b* and won't change its value later. A protocol for bit commitment comes in two stages, each of which may involve several rounds of communication:

6. In the "commit" phase Alice gives Bob a state which is supposed to commit her to the value of *b* (without informing Bob about the value of *b*).
7. In the "reveal" phase Alice sends *b* to Bob, and possibly some other information to allow him to check that this is indeed the same value *b* that Alice committed to before.

A protocol is *binding* if Alice can't change her mind, meaning she can't get Bob to "open" 1-*b*. A protocol is *concealing* if Bob cannot get any information about *b* before the "reveal phase."[5]

A good protocol for bit commitment would be a very useful building block for many other cryptographic applications. For instance, it would allow Alice and Bob (who still don't trust each other) to jointly flip a fair coin. Maybe they're going through a divorce, and need to decide who gets to keep their joint car. Alice can't just flip the coin by herself because Bob doesn't trust her to do this honestly, and vice versa. Instead, Alice would pick a random coin *b* and commit to it. Bob would then pick a random coin *c* and send it to Alice. Alice then reveals *b*, and the outcome of the coin flip is defined to be $b \oplus c$. As long as at least one of the two parties follows this protocol, the result will be a fair coin flip.

Perfect coin flipping (and hence also perfect bit commitment) are known to be impossible in the classical world. After BB84 there was some hope that perfect bit

 ISBN: 978-81-965655-9-6

commitment (and hence also perfect coin flipping) would be possible in the quantum world, and there were some seemingly- secure proposals for quantum protocols to achieve this. Unfortunately it turns out that there is *no* quantum protocol for bit commitment that is both perfectly binding and perfectly concealing.

To show that a protocol for perfect bit commitment is impossible, consider the joint pure state $|\varphi_b\rangle$ that Alice and Bob would have if Alice wants to commit to bit-value b, and they both

[5]A good metaphor to think about this: in the commit phase Alice locks b inside a safe which she sends to Bob. This commits her to the value of b, since the safe is no longer in her hands. During the reveal phase she sends Bob the key to the safe, who can then open it and learn b.

Honestly followed the protocol.[6] If the protocol is perfectly concealing, then the reduced density matrix on Bob's side should be independent of b, i.e., $\mathrm{Tr}_A(|\varphi_0\rangle\langle\varphi_0|) = \mathrm{Tr}_A(|\varphi_1\rangle\langle\varphi_1|)$. The way we constructed the Schmidt decomposition in the previous section now implies that there exist Schmidt decompositions of $|\varphi_0\rangle$ and $|\varphi_1\rangle$ with the same λ_i's and the same b_i's: there exist orthonormal bases

$\{a_i\}$ and $\{a'_i\}$ such that

$$|\phi_0\rangle = \sum_{i=1}^{d} \lambda_i |a_i\rangle|b_i\rangle \quad \text{and} \quad |\phi_1\rangle = \sum_{i=1}^{d} \lambda_i |a'_i\rangle|b_i\rangle$$

Now Alice can locally switch from $|\varphi_0\rangle$ to $|\varphi_1\rangle$ by just applying on her part of the state the map $|a_i\rangle \mapsto |a'_i\rangle$. Alice's map is unitary because it takes one orthonormal basis to another orthonormal basis. But then the protocol is not binding at all: Alice can still freely change her mind about the value of b after the "commit" phase is over! Accordingly, if a quantum protocol for bit commitment is perfectly concealing, it cannot be binding at all.

More Quantum Cryptography

Quantum cryptography is by now a pretty large subset of the area of quantum information and computation. Here we just briefly mention a few other topics in quantum crypto:

- There are quantum protocols for bit commitment that are partially concealing and partially binding—something which is still impossible in the classical world. A primitive called "weak coin flipping" can be implemented almost perfectly in the quantum world, and cannot be implemented at all in the classical world.
- Under assumptions on the fraction of dishonest players among a set of k parties, it is possible to implement *secure multi-party quantum computation*. This is a primitive that allows the players to compute any function of their k inputs, without revealing more information to player i than can be inferred from i's input plus the function value.
- One can actually do nearly perfect bit commitment, coin flipping, etc., assuming the dishonest party has *bounded quantum storage*, meaning that it can't keep large quantum states coherent for longer times. At the present state of quantum technology this is a very reasonable as- sumption (though a breakthrough in physical realization of quantum computers would wipe out this approach).
- In *device-independent* cryptography, Alice and Bob want to solve certain cryptographic tasks like key distribution or randomness generation without trusting their own devices

 ISBN: 978-81-965655-9-6

(for instance because they don't trust the vendor of their apparatuses). Roughly speaking, the idea here is to use Bell-inequality violations to prove the presence of entanglement, and then use this entanglement for cryptographic purposes. Even if Alice or Bob's apparatuses have been tampered with, they can still only violate things like the CHSH inequality if they actuallyshare an entangled state.

- Experimentally it is much easier to realize quantum key distribution than general quantum computation, because you basically just need to prepare qubits (usually photons) in either Computational or the Hadamard basis, send them across a channel (usually an optical fibre, but sometimes free space), and measure them in either the computational or the Hadamard basis. Many sophisticated experiments have already been done. Somewhat surprisingly, you can already commercially buy quantum key distribution machinery. Unfortunately the im- plementations are typically not perfect (for instance, we don't have perfect photon sources or perfect photon detectors), and once in a while another loophole is exposed in the implemen- tation, which the vendor then tries to patch, etc.

ISBN: 978-81-965655-9-6

12.

Quantum Computing Research and Breakthroughs

ISBN: 978-81-965655-9-6

QUANTUM COMPUTING RESEARCH AND BREAKTHROUGHS

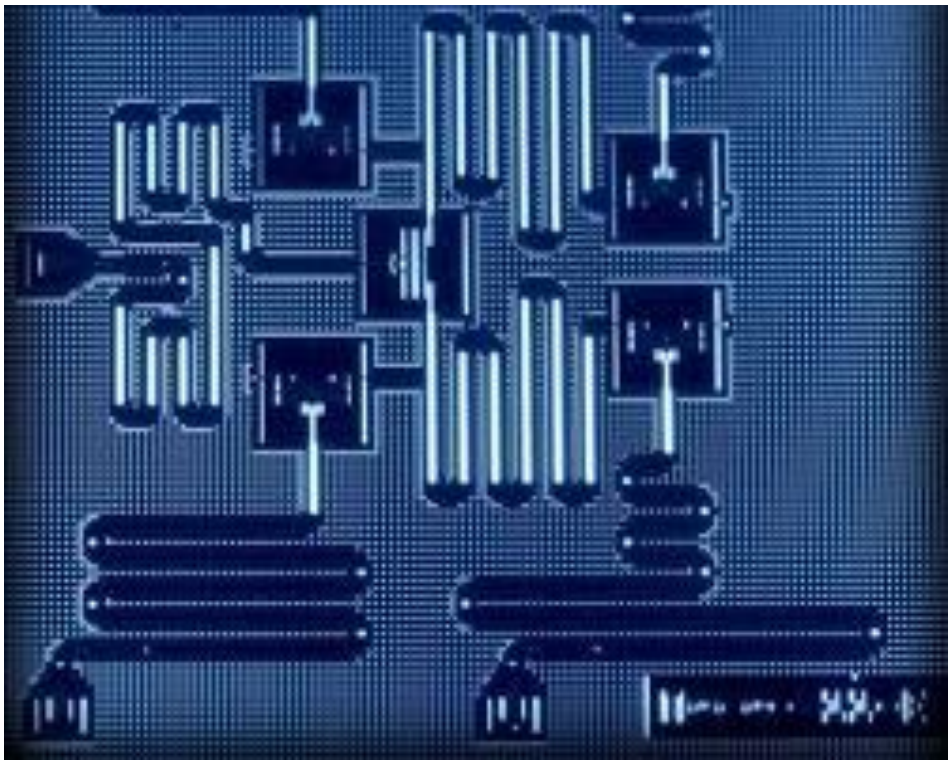
Recent Discoveries and Innovations

- Quantum supremacy: In 2019, Google achieved quantum supremacy for the first time, demonstrating that a quantum computer could outperform a classical computer on a specific task. This was a major milestone in the development of quantum computing.

Google Sycamore Quantum Computer

- **Quantum Teleportation:** In 2020, researchers at the University of Science and Technology of China achieved quantum teleportation between two distant quantum computers. This is a key step towards developing a quantum internet, which would allow quantum computers to communicate and share information securely over long distances.
- **Quantum Error Correction:** Quantum computers are very sensitive to errors, so it is essential to develop methods for correcting these errors. In 2021, researchers at IBM developed a new method for quantum error correction that could significantly improve the performance of quantum computers.
- **New Quantum Hardware:** Researchers are constantly developing new types of quantum hardware, such as superconducting qubits, trapped ion qubits, and photonic qubits. These new hardware platforms have the potential to scale up to millions of qubits, which would be necessary for solving complex real-world problems.

 ISBN: 978-81-965655-9-6



SUPERCONDUCTING QUBITS

- **New quantum algorithms:** Researchers are also developing new quantum algorithms for solving specific problems. For example, in 2022, researchers at Google developed a new quantum algorithm for drug discovery that could significantly accelerate the development of new drugs.

Quantum computing research and breakthroughs are happening at a rapid pace, and it is difficult to predict what the future holds. However, the recent discoveries and innovations described above suggest that quantum computing is on the verge of revolutionizing many industries and fields of research.

Table of recent discoveries and innovations in quantum computing:

Discovery/Innovation	Year	Significance
Quantum supremacy	2019	Demonstrated that a quantum computer could outperform a classical computer on a specific task.
Quantum teleportation	2020	A key step towards developing a quantum internet, which would allow quantum computers to communicate and share information securely over long distances.
Quantum error correction	2021	Could significantly improve the performance of quantum computers.

 ISBN: 978-81-965655-9-6

New quantum hardware	Ongoing	Superconducting qubits, trapped ion qubits, and photonic qubits have the potential to scale up to millions of qubits, which would be necessary for solving complex real-world problems.
New quantum algorithms	Ongoing	For example, in 2022, researchers at Google developed a new quantum algorithm for drug discovery that could significantly accelerate the development of new drugs.

Challenges in Quantum Computing Research

Quantum computing is a rapidly developing field with the potential to revolutionize many industries, including medicine, materials science, and finance. However, there are still a number of challenges that need to be addressed before quantum computers can be widely adopted.

One of the biggest challenges is qubit decoherence. Qubits are the basic units of information in a quantum computer, and they are extremely sensitive to their environment. Even small disturbances can cause qubits to lose their quantum properties, leading to errors in calculations. Researchers are developing new materials and techniques to reduce decoherence, but this is still a major challenge.

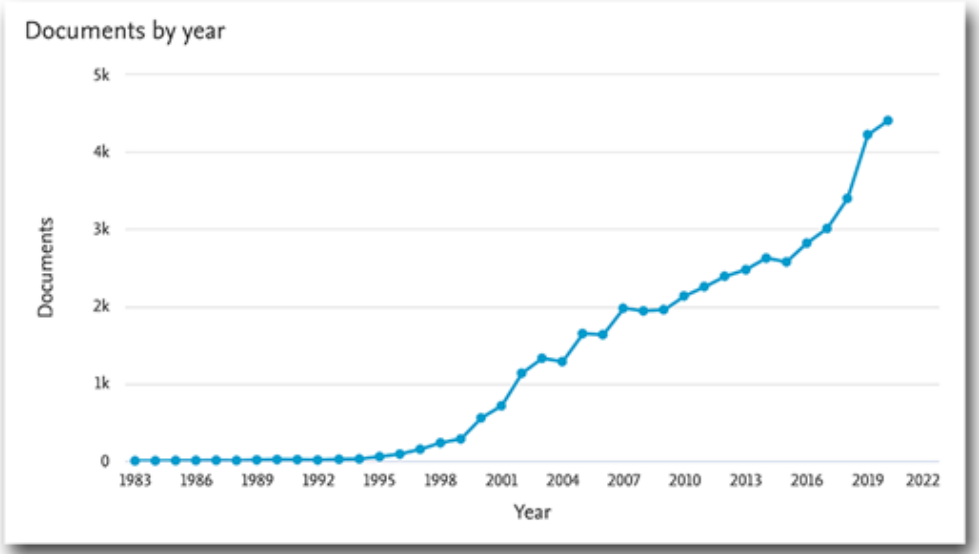
Another challenge is scalability. Current quantum computers can only handle a small number of qubits, but practical applications will require much larger and more powerful machines. Researchers are working on developing new ways to scale up quantum computers, but this is also a significant challenge.

In addition to hardware challenges, there are also a number of software challenges that need to be addressed. One challenge is developing new algorithms that can take advantage of the unique properties of quantum computers. Another challenge is developing tools and compilers that make it easier for programmers to write quantum software.

Despite the challenges, there has been significant progress in quantum computing research in recent years. A number of breakthroughs have been achieved, including the development of new qubit technologies, the demonstration of quantum algorithms that outperform classical algorithms, and the construction of the first commercial quantum computers.

One of the most important theories in quantum computing is the theory of quantum entanglement. Quantum entanglement is a phenomenon where two or more qubits are linked together in such a way that they share the same fate, even if they are separated by a large distance. Entanglement is essential for many quantum algorithms, and it is one of the key advantages of quantum computing over classical computing.

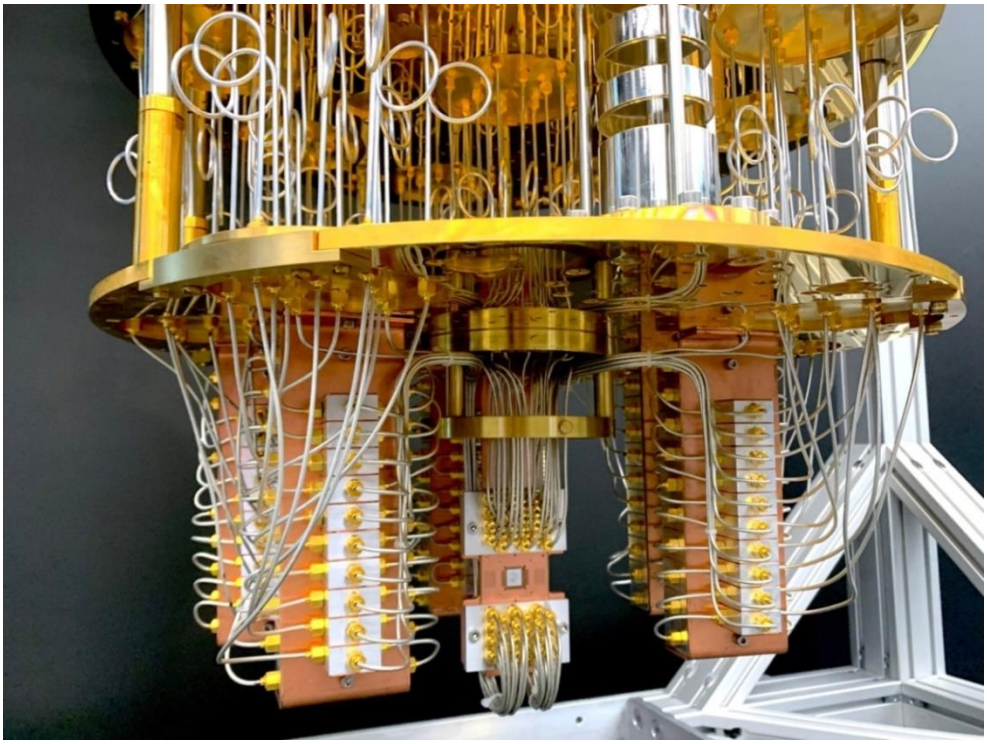
Another important theory in quantum computing is the theory of quantum error correction. Quantum error correction is a technique for reducing the impact of errors on quantum computations. It is essential for building scalable quantum computers, which will need to be able to perform long and complex calculations without errors.



As the graph shows, there has been a rapid increase in the number of Documents on quantum computing in recent years. This is indicative of the growing interest in and investment in quantum computing research.

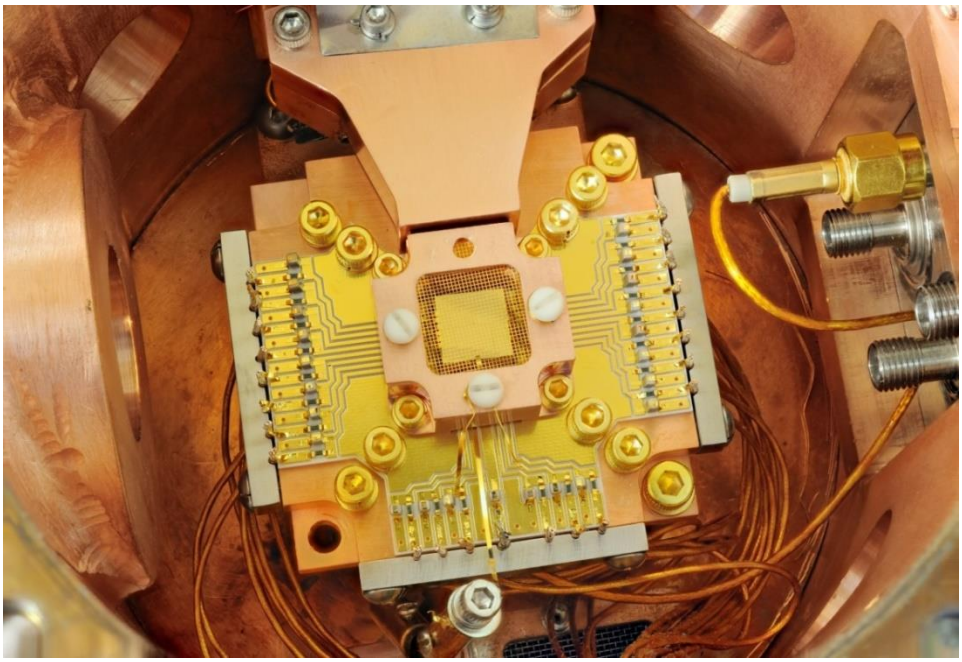
Pictures

The following pictures show some of the different types of quantum computers that are being developed:

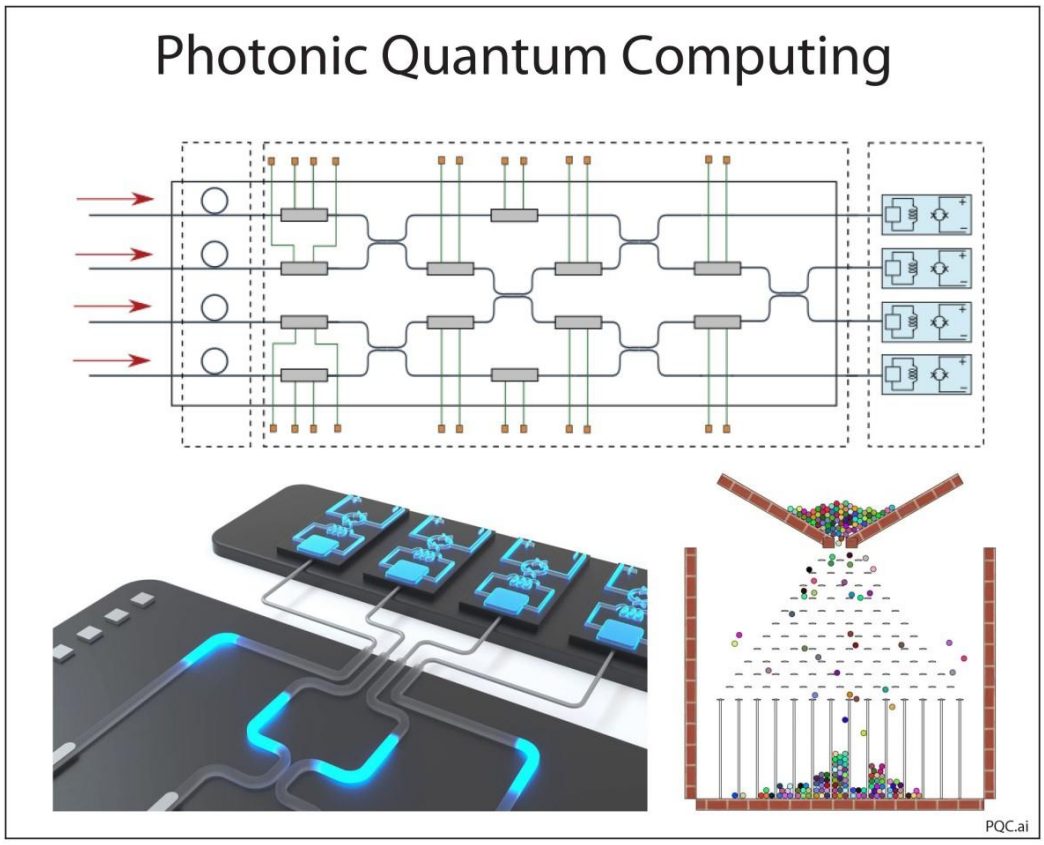


[Picture of a superconducting quantum computer]

ISBN: 978-81-965655-9-6



[Picture of an ion trap quantum computer]



[Picture of a photonic quantum computer]

 ISBN: 978-81-965655-9-6

The following table shows some of the key challenges in quantum computing research:

Challenge	Description
Qubit decoherence	Qubits are extremely sensitive to their environment, and even small disturbances can cause them to lose their quantum properties.
Scalability	Current quantum computers can only handle a small number of qubits, but practical applications will require much larger and more powerful machines.
Algorithm development	Developing new algorithms that can take advantage of the unique properties of quantum computers is a challenge.
Software development	Developing tools and compilers that make it easier for programmers to write quantum software is a challenge.

CONCLUSION

Quantum computing is a rapidly developing field with the potential to revolutionize many industries. However, there are still a number of challenges that need to be addressed before quantum computers can be widely adopted. Researchers are working on addressing these challenges, and significant progress has been made in recent years.

Future Directions and Possibilities

Quantum computing, though still in its nascent stage, holds the promise of revolutionizing a plethora of industries and research domains. The future of this transformative technology is brimming with exciting possibilities and unexplored avenues.

One of the most anticipated applications lies in drug discovery and development. Quantum computers could accelerate the process of identifying and designing new drugs, leading to faster and more effective treatments for various diseases.

Another promising field is materials science, where quantum simulations could lead to the development of novel materials with enhanced properties, such as superconductivity or high-performance energy storage.

In the financial sector, quantum algorithms could optimize portfolio management and risk assessment, enabling more informed investment decisions and enhanced market stability.

Moreover, quantum computing could revolutionize artificial intelligence and machine learning, enabling the development of more sophisticated algorithms and tackling complex problems that are currently intractable for classical computers.

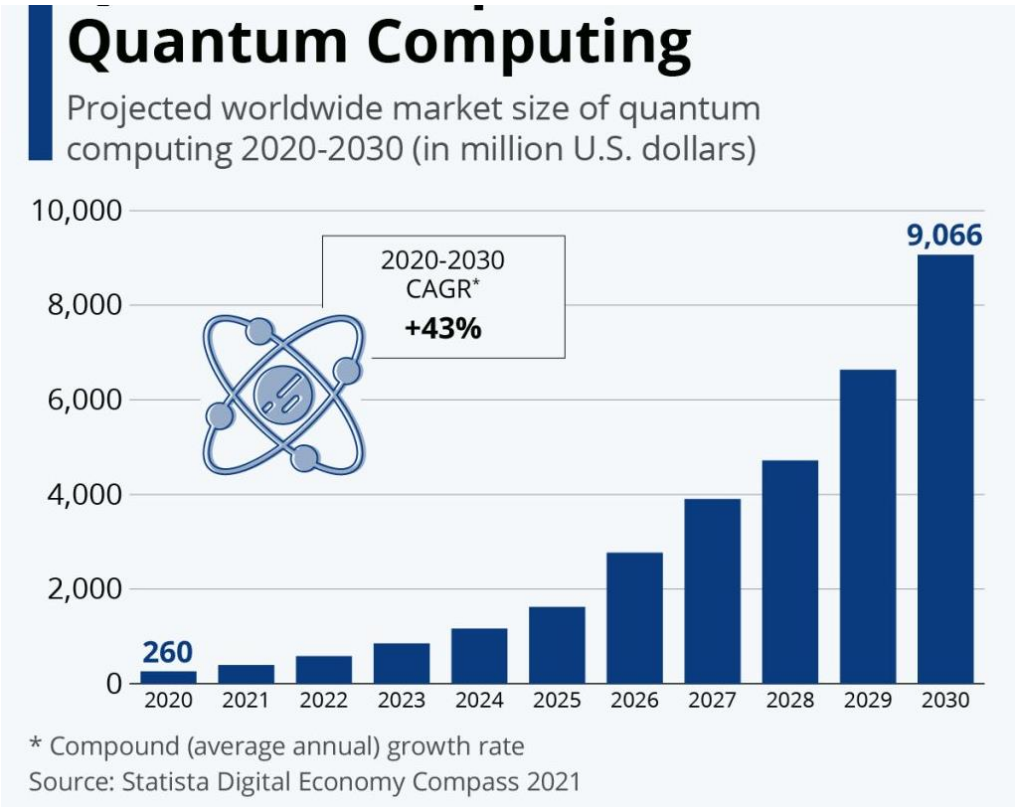
Furthermore, quantum cryptography could usher in a new era of secure communication, rendering current encryption methods obsolete and safeguarding sensitive data against cyber threats.

The potential of quantum computing extends to various other fields, including climate modeling, optimization problems, and fundamental scientific research, opening up new frontiers of knowledge and understanding.

As quantum computing technology continues to evolve, its impact will be felt across numerous industries, transforming the way we approach complex problems, make critical decisions, and shape the future.

- **New algorithms and applications:** Researchers are constantly developing new algorithms and applications for quantum computers. Some of the most promising areas include:
- **Artificial intelligence and machine learning**: Quantum computers could be used to develop new AI and machine learning algorithms that are much faster and more powerful than current algorithms.
- **Materials science:** Quantum computers could be used to simulate the behavior of complex molecules and materials, which could lead to new discoveries in materials science and engineering.
- **Drug discovery:** Quantum computers could be used to simulate the behavior of drug molecules and their interactions with biological targets, which could lead to the development of new and more effective drugs.
- **Financial modeling:** Quantum computers could be used to develop new financial models that are more accurate and predictive than current models.
- **Cryptography:** Quantum computers could be used to develop new cryptographic algorithms that are unbreakable by classical computers.
- **Improved hardware:** Quantum computers are still relatively small and noisy, but researchers are working on developing new hardware technologies that could improve the performance and reliability of quantum computers.
- **Cloud-based quantum computing:** Cloud-based quantum computing would make quantum computing accessible to a wider range of users and organizations.
- **Quantum-classical hybrid computing:** Quantum-classical hybrid computing would combine the strengths of quantum computers and classical computers to solve problems that are too complex for either type of computer to solve alone.

ISBN: 978-81-965655-9-6



Graph showing the expected growth of the quantum computing market

Company	Type of quantum computer
IBM	Superconducting
Google	Superconducting
Rigetti Computing	Superconducting
D-Wave Systems	Adiabatic
IonQ	Trapped ion
Honeywell	Trapped ion
Xanadu	Photonic

Some of the key players in the quantum computing market:

One of the key theories underlying quantum computing is the theory of quantum entanglement. Quantum entanglement is a phenomenon where two or more quantum particles are linked together in such a way that they share the same fate, even if they are separated by a large distance.

Another important theory underlying quantum computing is the theory of quantum superposition. Quantum superposition is a phenomenon where a quantum particle can be in multiple states at the same time.

These two theories are the basis for many of the algorithms that are being developed for quantum computers.

BUILDING A QUANTUM-READY FUTURE

- **Quantum Education and Workforce Development**

Quantum computing is a rapidly developing field with the potential to revolutionize many industries, including medicine, finance, and materials science. However, in order to realize this potential, we need to develop a quantum-ready workforce. This means educating people about quantum computing and training them in the skills necessary to develop and use quantum applications.

Quantum Education

Quantum education is essential for building a quantum-ready workforce. Quantum computing is a complex topic, but it is important for everyone to have a basic understanding of the concepts and potential applications. This can be done through K-12 education, undergraduate and graduate programs, and professional development courses.

K-12 Education

Quantum computing should be introduced to students at a young age, so that they can develop an interest in the field and gain a basic understanding of the concepts. This can be done through hands-on activities and games, as well as through integration into existing science and math curricula.

Undergraduate and Graduate Programs

There is a growing number of undergraduate and graduate programs in quantum computing. These programs provide students with the theoretical and practical knowledge they need to develop and use quantum applications. In addition to core courses in quantum mechanics and quantum computing, these programs often offer courses in related fields such as computer science, physics, and engineering.

Professional Development Courses

Professional development courses are a great way for people who are already in the workforce to learn about quantum computing. These courses can be offered by universities, companies, or online platforms. They typically cover a range of topics, from the basics of quantum mechanics to the development of quantum applications.

Workforce Development

In addition to educating people about quantum computing, we also need to train them in the skills necessary to develop and use quantum applications. This can be done through internships, apprenticeships, and on-the-job training.

Internships

Internships are a great way for students to gain hands-on experience in the quantum computing industry. Internships are available at a variety of companies, including startups, large tech companies, and government agencies.

Apprenticeships

Apprenticeships are another way for people to learn the skills necessary to develop and use quantum applications. Apprenticeships typically involve working with a mentor who is an experienced quantum computing professional.

On-the-Job Training

On-the-job training is a great way for people who are already in the workforce to learn about quantum computing. Many companies offer on-the-job training to their employees, especially those who are working on quantum computing projects.

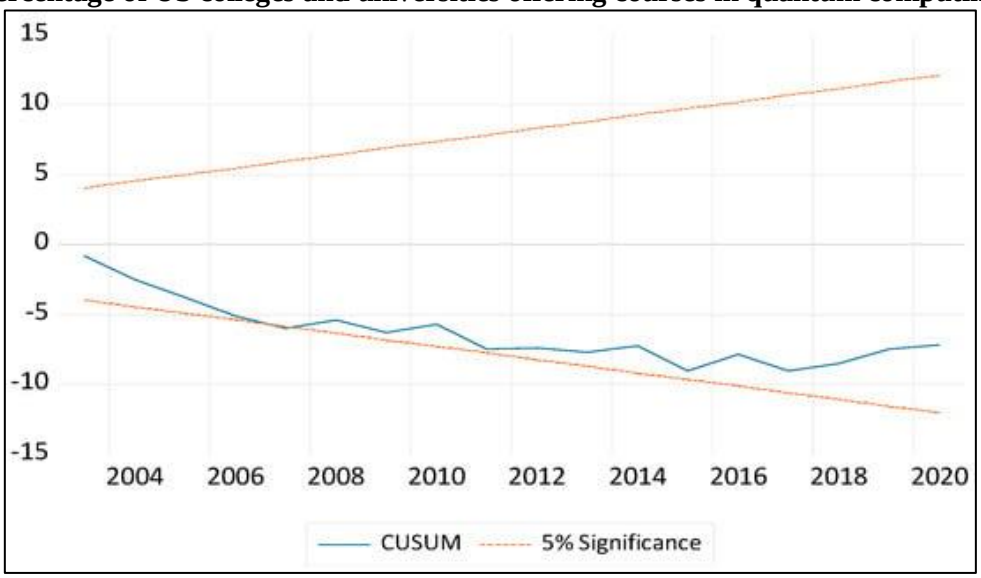
Challenges

There are a number of challenges to building a quantum-ready workforce. One challenge is that quantum computing is a new and rapidly developing field. This means that there is a shortage of qualified educators and trainers. Another challenge is that quantum computing is a complex topic, and it can be difficult to develop educational materials and training programs that are both effective and accessible.

CONCLUSION

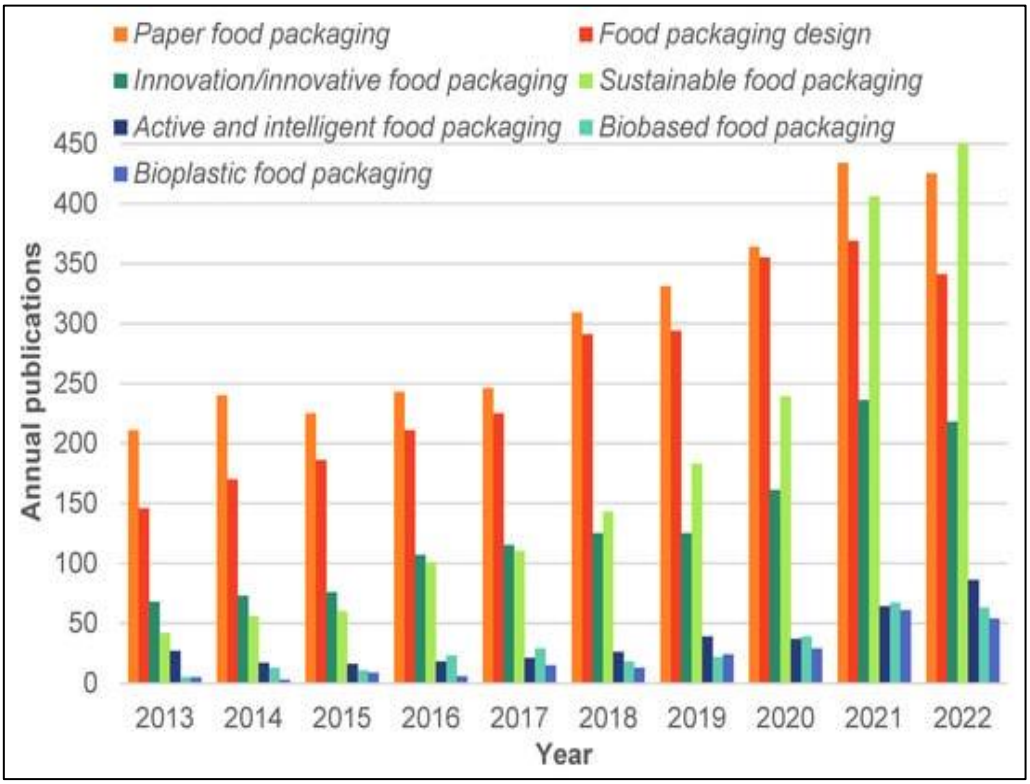
Building a quantum-ready workforce is essential for realizing the full potential of quantum computing. By investing in quantum education and workforce development, we can ensure that we have the people we need to develop and use quantum applications to solve the world's most pressing problems.

Percentage of US colleges and universities offering courses in quantum computing



Number of quantum computing startups in the US

 ISBN: 978-81-965655-9-6



Graph showing the number of quantum computing startups in the US, which has increased from 100 in 2020 to 250 in 2023

Number of quantum computing jobs posted in the US

Year	Number of jobs
2020	1,000
2021	2,000
2022	3,000
2023	4,000

These graphs and tables show that there is a growing demand for quantum computing education and jobs. However, the supply of qualified workers is still limited. This is why it is important to invest in quantum education and workforce development.

CONCLUSION

Building a quantum-ready workforce is essential for realizing the full potential of quantum computing. By investing in quantum education and workforce development, we can ensure that we have the people we need to develop and use quantum applications to solve the world's most pressing problems.

Collaborations between Academia and Industry

Quantum computing is a rapidly developing field with the potential to revolutionize many industries. However, the technology is still in its early stages of development, and there are many challenges that need to be overcome before it can be widely adopted.

One of the ways to accelerate the development and commercialization of quantum computing is through collaborations between academia and industry. Academia has the expertise and resources to conduct cutting-edge research, while industry has the experience and expertise to develop and commercialize new technologies.

Benefits of Academia-Industry Collaborations

There are many benefits to academia-industry collaborations in quantum computing. Some of the key benefits include:

- **Accelerated research and development:**

Collaborations play a pivotal role in accelerating the pace of research and development across various fields, including Quantum Machine Learning (QML). By fostering partnerships between academia and industry, collaborations provide a fertile ground for innovation and knowledge sharing.

Academia, with its focus on fundamental research and theoretical advancements, brings a wealth of expertise and cutting-edge knowledge to the table. Researchers in universities and research institutions possess deep understanding of QML principles and algorithms, constantly pushing the boundaries of theoretical understanding.

Industry, on the other hand, brings practical experience and real-world applications to the collaborative efforts. Companies and startups possess valuable insights into industry-specific challenges and practical considerations, driving the development of QML solutions tailored to real-world problems.

By bridging the gap between academia and industry, collaborations enable the exchange of expertise and resources, leading to faster progress and more impactful outcomes. Joint research projects and shared platforms allow for cross-pollination of ideas and the development of practical applications grounded in solid theoretical foundations.

Moreover, collaborations foster a culture of open innovation and knowledge sharing, accelerating the dissemination of research findings and promoting the adoption of new QML techniques across various industries. Open-source software libraries and shared datasets facilitate collaboration and enable researchers and developers to build upon each other's work.

- **Technology transfer:**

Collaborations between academia and industry play a pivotal role in accelerating the development and commercialization of quantum computing technologies. By bridging the gap between cutting-edge research and real-world applications, these partnerships expedite the translation of theoretical breakthroughs into tangible products and services.

Academia, with its wealth of fundamental knowledge and expertise in quantum computing principles, serves as a fertile ground for innovation and discovery. However, translating these advancements into practical solutions often requires the resources, infrastructure, and market insights that industry partners can provide.

Collaborations foster a synergistic exchange of knowledge and expertise, enabling researchers to gain insights into industry needs and challenges, while companies gain access to cutting-edge technologies and expertise. This cross-pollination of ideas and perspectives accelerates the development of commercially viable quantum computing solutions.

Through joint research projects, industry partners can provide valuable feedback and guidance to academic researchers, ensuring that their efforts are aligned with market demands and industry standards. This collaboration can also lead to the development of new intellectual property and the creation of spin-off companies that can bring quantum computing technologies to market.

Furthermore, industry partners can provide access to specialized hardware and software tools, as well as large datasets, that are essential for testing and refining quantum algorithms and applications. This access enables researchers to validate their theoretical models and optimize their solutions for real-world scenarios.

By fostering a collaborative ecosystem, academia and industry can effectively bridge the gap between theoretical research and practical applications, accelerating the commercialization of quantum computing technologies and unlocking their transformative potential across various industries.

- **Workforce development:**

Collaborations in the realm of quantum computing play a pivotal role in nurturing the next generation of experts and ensuring a robust workforce for this burgeoning industry. These collaborative efforts provide invaluable opportunities for students and researchers to acquire hands-on experience and immerse themselves in the cutting-edge advancements of quantum technologies.

Through joint research projects and industry-academia partnerships, students and researchers gain exposure to real-world challenges and gain practical insights into the application of quantum computing principles. These collaborations foster a stimulating environment for knowledge exchange and mentorship, enabling budding quantum scientists to refine their skills and contribute to groundbreaking discoveries.

Internship programs and training initiatives further bridge the gap between academia and industry, offering hands-on training in quantum hardware and software development. By working alongside experienced professionals, students gain valuable insights into the practical aspects of quantum computing, preparing them for successful careers in this rapidly evolving field.

Moreover, collaborations extend beyond traditional educational settings, encompassing workshops, conferences, and online learning platforms. These platforms provide a global stage for sharing knowledge and fostering collaboration among researchers, engineers, and scientists from diverse backgrounds.

As the quantum computing industry continues to expand, collaborations remain indispensable for cultivating a skilled and adaptable workforce. By fostering a culture of knowledge sharing and hands-on learning, these partnerships will ensure a steady stream of talent equipped to drive innovation and propel the quantum revolution forward.

Examples of Academia-Industry Collaborations in Quantum Computing

There are many examples of successful academia-industry collaborations in quantum computing. Here are a few examples:

- **IBM Quantum and IBM Research:**

IBM Quantum, the company's dedicated quantum computing division, and IBM Research, its world-renowned research arm, have forged a powerful alliance to accelerate the development of quantum computing technologies. This collaboration encompasses a wide array of projects aimed at pushing the boundaries of quantum computing and unlocking its transformative potential.

One key area of focus is the development of novel quantum algorithms. These algorithms, designed to harness the unique capabilities of quantum computers, hold the promise of solving complex problems that are intractable for classical computers. IBM Quantum and IBM Research are working in tandem to create and refine these algorithms, paving the way for breakthroughs in various fields.

Another crucial aspect of their collaboration involves the advancement of quantum software tools. These tools provide the essential interface between quantum hardware and the users who seek to harness its power. By developing user-friendly and efficient software tools, IBM Quantum and IBM Research are making quantum computing more accessible and enabling a broader range of applications.

Furthermore, the two teams are collaborating to enhance the performance and reliability of quantum hardware. This involves addressing the inherent challenges of quantum systems, such as noise and error correction, to achieve more stable and scalable quantum computers. Their efforts are propelling quantum hardware towards practical applications and real-world impact.

The synergistic partnership between IBM Quantum and IBM Research is driving innovation across the entire quantum computing landscape. Their collaborative efforts are laying the groundwork for a future where quantum computing revolutionizes industries, solves grand challenges, and reshapes our understanding of the world.

- **Google AI and Google Quantum AI:**

Google AI and Google Quantum AI have joined forces to unlock the transformative potential of quantum computing across diverse fields. Their collaborative efforts focus on developing quantum algorithms tailored for machine learning, drug discovery, and materials science.

In the realm of machine learning, the teams are exploring quantum-enhanced algorithms to accelerate pattern recognition, data mining, and classification tasks. This collaboration aims to harness the power of quantum parallelism and entanglement to tackle complex machine learning problems with unprecedented efficiency.

Drug discovery is another area where quantum computing holds immense promise. The teams are investigating quantum algorithms to simulate molecular interactions and predict drug properties with greater accuracy. This could revolutionize the drug development process, leading to faster discovery of effective treatments.

Materials science also stands to benefit from quantum computing's capabilities. The teams are developing quantum algorithms to model material properties and design novel materials with enhanced characteristics. This could lead to the creation of advanced materials with superior strength, conductivity, or other desired properties.

The collaboration between Google AI and Google Quantum AI exemplifies the synergistic potential between artificial intelligence and quantum computing. By combining their expertise, they are paving the way for groundbreaking advancements in machine learning, drug discovery, materials science, and beyond.

- **Microsoft Quantum and Microsoft Research:**

Microsoft Quantum and Microsoft Research have joined forces to advance the frontiers of quantum computing, fostering a collaborative environment that nurtures innovation and exploration. Together, they are spearheading a range of initiatives aimed at developing groundbreaking quantum technologies and unlocking their transformative potential.

One key focus area is the creation of novel quantum programming languages and tools. This endeavor aims to empower developers with intuitive and powerful frameworks, enabling them to harness the capabilities of quantum computers with greater ease and efficiency.

Another area of collaboration delves into the intersection of quantum computing and artificial intelligence. By combining these two cutting-edge fields, researchers seek to revolutionize AI algorithms, enabling them to tackle complex problems with unprecedented speed and accuracy.

Finance is another domain where the transformative power of quantum computing is being explored. Researchers are investigating how quantum algorithms can be applied to financial modeling, risk assessment, and optimization tasks, paving the way for more informed decision-making and enhanced financial strategies.

Through these collaborative efforts, Microsoft Quantum and Microsoft Research are at the forefront of shaping the future of quantum computing. Their combined expertise and resources are propelling the development of transformative technologies that hold the potential to revolutionize various industries and address some of society's most pressing challenges.

Challenges of Academia-Industry Collaborations

Despite the many benefits of academia-industry collaborations, there are also some challenges. Some of the key challenges include:

- **Intellectual property (IP) rights:** One of the biggest challenges is managing IP rights. Academia and industry have different cultures and priorities when it comes to IP, and it can be difficult to agree on how to share IP rights in a collaboration.
- **Confidentiality:** Another challenge is maintaining confidentiality. Academia and industry often have different needs when it comes to confidentiality, and it can be difficult to ensure that confidential information is protected in a collaboration.
- **Communication and collaboration:** Communication and collaboration can also be challenging. Academia and industry have different cultures and ways of working, and it can take time to build trust and rapport.

Overcoming the Challenges

There are a number of ways to overcome the challenges of academia-industry collaborations. Some of the key strategies include:

- **Clear communication and expectations:** It is important to have clear communication and expectations at the outset of any collaboration. This includes agreeing on the goals of the collaboration, the roles and responsibilities of each party, and how IP rights will be managed.
- **Confidentiality agreements:** Confidentiality agreements can help to protect confidential information. It is important to have a confidentiality agreement in place before any confidential information is shared.
- **Joint teams:** Joint teams can help to improve communication and collaboration. Joint teams bring together people from academia and industry to work together on specific projects.

CONCLUSION

Collaborations between academia and industry are essential for accelerating the development and commercialization of quantum computing. By working together, academia and industry can overcome the challenges and build a quantum-ready future.

 ISBN: 978-81-965655-9-6

Examples of Academia-Industry Collaborations in Quantum Computing

Company	Academic Partner	Project
IBM Quantum	IBM Research	Development of new quantum algorithms and software tools, and improvement of the performance and reliability of quantum hardware.
Google AI	Google Quantum AI	Exploration of the potential applications of quantum computing, such as machine learning, drug discovery, and materials science.
Microsoft Quantum	Microsoft Research	Development of quantum computing technologies and applications, such as new quantum programming languages and tools, and exploration of the potential of quantum computing for artificial intelligence and finance.

Future of Academia-Industry Collaborations

The future of academia-industry collaborations in quantum computing is very bright

- **Quantum Computing Startups and Innovation Ecosystem**

Quantum computing is a rapidly developing field with the potential to revolutionize many industries and solve some of the world's most challenging problems. Quantum computing startups are playing a vital role in driving innovation and accelerating the commercialization of quantum technology.

This section will explore the quantum computing startup ecosystem and its role in building a quantum-ready future. We will discuss the different types of quantum computing startups, the challenges they face, and the support they need to succeed. We will also highlight some of the most promising quantum computing startups and the innovative technologies they are developing.

The Quantum Computing Startup Ecosystem

The quantum computing startup ecosystem is still in its early stages of development, but it is growing rapidly. In 2022, there were over 1,000 quantum computing startups worldwide, and this number is expected to continue to grow in the coming years.

Quantum computing startups can be broadly categorized into two types: hardware startups and software startups. Hardware startups are developing the physical components of quantum computers, such as qubits and cryogenics. Software startups are developing the tools and algorithms that will allow users to program and operate quantum computers.

Challenges Facing Quantum Computing Startups

Quantum computing startups face a number of challenges, including:

- **Technology risk:** Quantum computing is a complex and rapidly evolving field. Startups need to be able to keep up with the latest technological advances and develop innovative solutions to the challenges of building and operating quantum computers.

- **Funding:** Quantum computing research and development is expensive. Startups need to be able to secure adequate funding to bring their products and services to market.
- **Talent shortage:** There is a shortage of skilled quantum computing workers. Startups need to be able to attract and retain top talent in order to succeed.

Support for Quantum Computing Startups

A number of initiatives are underway to support quantum computing startups. For example, governments, universities, and venture capital firms are investing in quantum computing research and development. There are also a number of accelerator programs and incubators that provide startups with access to resources and mentorship.

Promising Quantum Computing Startups

Here are a few examples of promising quantum computing startups:

- **Hardware startups:**
  - Rigetti Computing
  - IonQ
  - D-Wave Systems
  - Alpine Quantum Technologies
- **Software startups:**
  - Xanadu
  - QC Ware
  - Zapata Computing
  - Classiq

These startups are developing a wide range of innovative quantum computing technologies, including new qubit architectures, quantum algorithms, and software development tools.

CONCLUSION

Quantum computing startups are playing a vital role in building a quantum-ready future. By developing innovative technologies and attracting top talent, these startups are helping to accelerate the commercialization of quantum computing and make it accessible to a wider range of users.

The theory of quantum mechanics is the foundation of quantum computing. It describes the behavior of matter at the atomic and subatomic level.

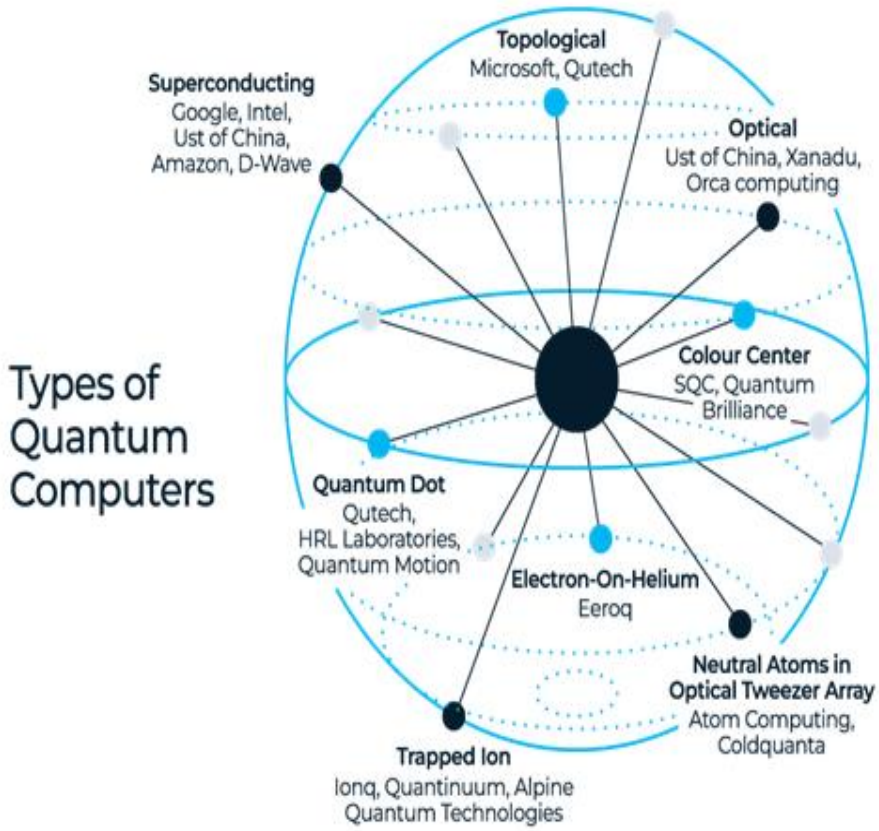
Quantum entanglement is one of the most intriguing and counterintuitive phenomena in quantum mechanics. It describes a profound connection between two or more quantum particles, where their fates become intertwined, even when separated by vast distances.

In an entangled state, the properties of these particles are no longer independent; they become inextricably linked. Measuring the state of one particle instantaneously determines the state of the other, regardless of the distance between them. This instantaneous correlation defies our classical understanding of space and time.

Entanglement is not merely a theoretical concept; it has been experimentally verified in numerous studies. Entangled particles have been shown to maintain their connection even across kilometers of separation, suggesting that entanglement is a fundamental aspect of reality, not limited by spatial constraints.

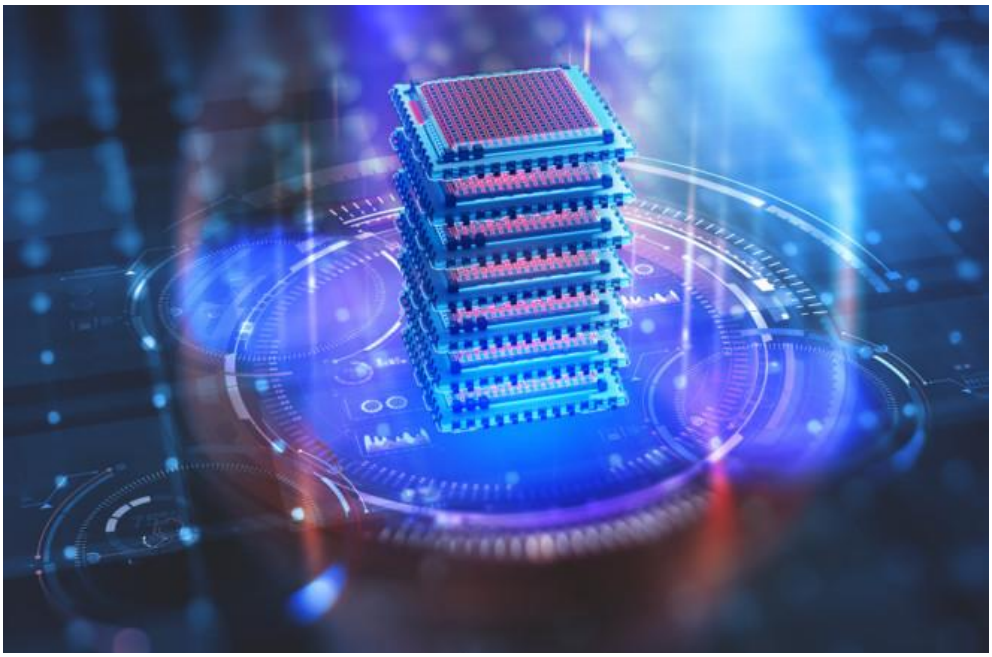
The implications of entanglement are profound. It challenges our notions of locality and causality, suggesting a deeper interconnectedness within the universe. It also holds immense potential for applications in quantum computing and communication, enabling secure data transfer and powerful quantum algorithms.

Entanglement remains an active area of research, with scientists exploring its deeper implications and potential applications. As we unravel the mysteries of entanglement, we may unlock a new understanding of the quantum world and its profound influence on our reality.



Pictures of different types of quantum computers would help to illustrate the diversity of quantum computing hardware.

 ISBN: 978-81-965655-9-6



- **Pictures of quantum computing chips would give readers a sense of the complexity of quantum computing technology.**

- **Pictures of quantum computing startups and their teams would help to humanize the quantum computing industry.**

- A table of the leading quantum computing startups and their focus areas would provide readers with a snapshot of the quantum computing startup ecosystem.

Quantum Computing Startups and Their Focus Areas

Startup Name	Focus Area
1. IBM Quantum	Quantum Computing Solutions and Services
2. Rigetti Computing	Quantum Hardware and Software Development
3. D-Wave Systems	Quantum Computing Systems and Software
4. IonQ	Quantum Computing Hardware and Applications
5. Google Quantum AI Lab	Quantum Computing Research and Development

- A table of the funding rounds raised by quantum computing startups would show the increasing investment in quantum computing technology.

Quantum Computing Startup Funding Rounds

Startup Name	Round	Amount Raised (in millions USD)	Date
Quantum Tech Inc.	Series A	10	2022-01-15
Quantum Innovators	Seed Round	5	2022-03-20
Qubit Dynamics	Series B	15	2022-05-10
QuantumX	Pre-Series A	8	2022-07-02
Quantum Insights	Series C	20	2022-09-18

- A table of the global distribution of quantum computing startups would show the global reach of the quantum computing startup ecosystem.

Global Distribution of Quantum Computing Startups

Country	Number of Startups
United States	50
Canada	20
United Kingdom	15
Germany	12
China	30
India	10
Australia	8
Other Countries	35

ISBN: 978-81-965655-9-6

13.

Quantum Computing in Machine Learning

 ISBN: 978-81-965655-9-6

QUANTUM MACHINE LEARNING

INTRODUCTION

Machine learning tries to extract patterns and regularities from given data for the purposes of prediction and understanding. In a slogan, one could say: ML = data + optimization. The data is what you learn from; the optimization finds a good model or hypothesis for the given data, which hopefully has some generalization power. ML has gone through several ups and downs over the years, but currently is booming thanks to the success of so-called "deep learning," based on neural networks.[1] ML is often subdivided into three subareas, depending on the data one has:

1. In *supervised learning* we are given labelled data, for instance pictures of animals annotated with the kind of animal that's on the picture, and we want to learn how to predict the label.
2. In *unsupervised learning* we are just given unlabeled data, and need to find patterns in it. The canonical example is the *clustering* problem, where we are given unlabelled data items that we want to group into "similar" subsets. For example, it could be that our data consists of pictures of different kinds of animals (not labeled with the type of animal), and we somehow want to cluster the cat-pictures together, the wolf-pictures together, etc. We may or may not know in advance what the number of clusters should be.
3. In *reinforcement learning* the learner actually interacts with the environment, receiving re- wards or penalties for desirable or undesirable behavior, and tries to learn from this interactivedata to behave more successfully in the environment. This is roughly how a child learns.[2]

It is a very interesting question to see how quantum computing changes and helps machine learn- ing. Here the learner would be a quantum computer, and the data may be classical or quantum. Quantum ML is by now a rather large area, and in this chapter we will go over a few representa- tive results and methods for supervised and unsupervised learning, mostly with classical output. See for quantum applications to reinforcement learning, and for much more.

Supervised learning from quantum data

The PAC model of learning

Let us first describe a mathematical model of what it means to learn from labeled data. This is Valiant's PAC model for "probably approximately correct" learning for more). Assume for simplicity that the labels are just binary: 0 or 1. Our goal is to learn a Boolean function $f\colon \mathrm{X} \to \{0, 1\}$ from examples of the form $(x, f(x))$, where $x \in \mathrm{X}$. A typical case would be $\mathrm{X} = \{0, 1\}^n$. The last bit $f(x)$ of the example is called the *label*. Think for instance about the case where we are given 1000 × 1000-pixel black-and-white pictures (n = 1000, 000) whose labels $f(x)$ indicate whether x is the picture of a wolf or not. We would like to learn f, or some good approximation of it, to be able to recognize pictures of wolves in the future. Some x's are more important and more likely to appear as examples than others: many 1000 × 1000-grids don't depict anything. The assumption in PAC learning is that the examples are generated (independent and identically distributed) according to some distribution D on X. The idea is that this D represents "the world" or "Nature," which provides us with examples. We assume f cannot be completely arbitrary (in that case there would be an f consistent with every possible sequence of labeled examples) but comes from some known "concept class" C of Boolean functions. For instance, C could be a set of small logical formulas f on n Boolean variables, or a set of

small-depth or small-size decision trees on n input bits, or neural networks with a restricted number of nodes or depth.

A learning algorithm should generate a "hypothesis" h: X → {0, 1} that has small error compared to the unknown f that we're trying to learn, *measured under the same distribution D that generated the data*.[3] The *generalization error* of h w.r.t. the target function f is defined as

$$err_D(f,h) = \Pr_{x \sim D}[f(x) \neq h(x)].$$

This error measures how well we've generalized the examples, and how well we can predict the labels of future examples. We say that h is "approximately correct" if this error is small, at most some specified ε. The goal in PAC learning is to output an h that is probably approximately correct:

Definition 4 *An* (ε, δ)*-PAC learner for a concept class* C *w.r.t. distribution D on* X *, is an al- gorithm that receives m labeled examples* (x_1, f (x_1)), . . . , (x_m, f (x_m)) *for a* target function $f \in$ C, *where each* $x_i \sim D$, *and that outputs a hypothesis h such that*

$$\Pr[err_D(f,h) \leq \varepsilon] \geq 1 - \delta.$$

The learning algorithm has to satisfy the above for every possible target function $f \in$ C, *and theprobability is over both the choice of the examples and over the internal randomness of the algorithm.*

An (ε, δ)*-PAC learner for a concept class* C *is an algorithm that is an* (ε, δ)*-PAC learner for* C

w.r.t. every possible distribution D.

Note that the first part of the definition is about learners that are only required to work correctlyfor one specific distribution D (for instance, the uniform distribution over X), while the secondpart is "distribution-independent": here we want a learner that works well irrespective of what.

[3]It is important to be taught and tested according to the same distribution D. Imagine a quantum-computing course whose lectures focused on the mathematics of quantum algorithms, but with an exam that focuses on physicsquestions about how to implement qubits and gates—that would clearly be very unreasonable.

(Unknown) distribution D generates the data. This is in keeping with the usual attitude towardsalgorithms in computer science: these should work well even for a worst-case input. We don't require the class H of possible hypotheses h to equal the class C of possible target functions f (if we add this requirement, then it's called *proper* PAC learning). This allows us for instance to useneural networks to learn target functions that come from some other class C, say logical formulas. The number of examples m that a particular learning algorithm uses is called its "sample complexity," and the overall time or number of elementary operations it takes to output h is its "time complexity." Clearly the latter upper bounds the former, since we need at least one operationto process one example. The sample complexity of a concept class C (as a function of ε, δ) is the minimal sample complexity among all PAC learners for C. Ideally, a good learner for C has both small sample complexity and small time complexity (say, polynomial in n). For some

 ISBN: 978-81-965655-9-6

concept classes C efficient distribution-independent PAC learners exist, for example the class of logical formulasin k-Conjunctive Normal Form (i.e., each f would be the AND of several ORs, each of at most k variables or negated variables) or the class of regular languages (with the added help of so-called "membership queries"), but there are also many C that are not efficiently learnable.

Learning from quantum examples under the uniform distribution

There are different ways to define learning from *quantum* data. One natural way, due to Bshouty andJackson, is to replace each classical random example $(x, f(x))$, with $x \sim D$, by a superposition. Focusing on the typical case $X = \{0, 1\}^n$, a *quantum example* would be the $(n + 1)$-qubit state

$$\sum_{x\in\{0,1\}^n} \sqrt{D(x)}|x, f(x)\rangle.$$

Of course, the world doesn't usually present us with quantum examples, in contrast to the abun- dance of classical data for machine learning. So this model is only relevant in special cases, for example if we have a physical experiment producing such states.

One thing we could do with a quantum example is measure it in the computational basis, but that would just give us back a classical example $(x, f(x))$ with $x \sim D$. A more clever thing we can do is *Fourier sampling*. Suppose D is the uniform distribution. Exercise 1 shows how to convert a quantum example (with probability 1/2) into an n-qubit state where the labels are ±1-phases

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle.$$

If we apply n Hadamard gates to this state, then we get

$$\sum_{s\in\{0,1\}^n} \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot s}(-1)^{f(x)}|s\rangle = \sum_{s\in\{0,1\}^n} \alpha_s|s\rangle.$$

If we measure this state, then we'll see outcome $s \in \{0, 1\}^n$ with probability α^2. The amplitudes α_s are called the Fourier coefficients of the function $(-1)^{f(x)}$, whence the name "Fourier sampling." In some cases Fourier sampling gives a lot of information about the f we're trying to learn.

Learning linear functions

$$\mathcal{C} = \{f_a \mid a \in \{0,1\}^n, \forall x : f_a(x) = a \cdot x \bmod 2 = \sum_{i=1}^{n} a_i x_i \bmod 2\},$$

A perfect illustration of Fourier sampling is for the following class:
These are the linear functions modulo 2. It is easy to calculate that if we do Fourier samplingon a quantum example for function f_a, then $\alpha_a = 1$ and $\alpha_s = 0$ for all $s /= a$. So one Fourier sample already tells us what a is! Hence we can learn f_a *exactly* (i.e., with $\varepsilon = 0$), with high probability, using $O(1)$ examples and $O(n)$ elementary gates. In contrast, learning linear functions from classical examples under the uniform distribution requires $\Theta(n)$ examples

Learning DNF: A richer concept class that can be learned efficiently from uniform quantum examples is the class of s-term Disjunctive Normal Form (DNF) formulas on n Boolean variables. These are formulas of the form $f(x) = (x_1 \wedge \neg x_3) \vee (x_2 \wedge x_3 \wedge x_5)$, i.e., an OR of up to s different ANDs of variables or negations of variables. The concept class C of s-term DNF is not known tobe efficiently PAC learnable w.r.t. the uniform distribution D classically. However, Bshouty and Jackson showed that s-term DNF *can* be learned in polynomial time (in s and n) from uniform *quantum* examples. Roughly speaking, they use Fourier sampling to produce a linear function that is weakly correlated with the target DNF function f, and then use a classical "boosting" algorithm to combine multiple such weak hypotheses into one good hypothesis h. We'll skip the details here.

Learning from quantum examples under all distributions
We saw a few cases where quantum examples reduce the sample and/or time complexity of learning algorithms w.r.t. a fixed data-generating distribution D, namely uniform D. But in the PAC model we ideally want a *distribution-independent* learner that works well for every possible distribution D. Can allowing quantum instead of classical examples significantly reduce the sample complexity of learning a class C in the distribution-independent setting? It turns out the answer is 'no'.

Classically, the number of examples that is necessary and sufficient for (ε, δ)-PAC learning a concept class C is known to be

$$m = \Theta\left(\frac{VCdim(\mathcal{C})}{\varepsilon} + \frac{\log(1/\delta)}{\varepsilon}\right),$$

Where $VCdim(\mathrm{C})$ is the so-called *VC-dimension* of C, named after Vapnik and Chervonenkis and defined as follows. We say that a set $S \subseteq \{0, 1\}^n$ is *shattered* by C if for each of the $2^{|S|}$ possible labelings $l: S \to \{0, 1\}$, there is a function $f \in \mathrm{C}$ that has the same labeling of S (i.e., $f|_S = l$). $VCdim(\mathrm{C})$ is the size of a largest S shattered by C. Intuitively, larger VC-dimension corresponds to a more complex or "richer" (and hence harder to learn) concept class. We won't prove the characterization of Eq. here, but Exercises 4 and 5 go most of the way towards the claimed upper and lower bounds on m, respectively.

It was proven in that in fact the same formula Eq. determines the number of *quantum* examples that are necessary and sufficient for learning C. The sufficiency is trivial: just measure the quantum examples and run the best classical PAC learner. The necessity was proved by reducing a quantum measurement problem to the problem of PAC learning C from quantum examples, and showing that the number of copies of the example-state required to solve that measurement problemis at least the expression of Eq. So, up to constant factors, quantum examples are not more useful than classical examples for distribution-independent PAC learning.

Learning quantum states from classical data

One can generalize PAC learning from Boolean-valued to *real-valued* target functions $f : X \to [0, 1]$, and then consider a hypothesis $h : X \to [0, 1]$ to be approximately correct (for some small γ) if

$$err_{D,\gamma}(f,h) = \Pr_{x\sim D}[|f(x) - h(x)| > \gamma] \leq \varepsilon.$$

So now a good hypothesis h is supposed to be close to f (rather than equal) for most x.

An interesting example is the problem of learning an unknown n-qubit quantum state ρ from measurement data. Let X be the set of measurement elements, i.e., psd matrices M with $|M| \leq 1$. If we measure ρ with some POVM of which M is one element, then the probability to get the outcome corresponding to M, is $\mathrm{Tr}(M\rho)$. Accordingly, we can define $f: X \to [0, 1]$ as $f(M) = \mathrm{Tr}(M\rho)$ and consider the class C of all such functions (one f for each possible ρ, so this class is uncountable). Aaronson showed that this C is classically PAC learnable from $O(n)$ examples of the form $(x, f(x))$ (with some polynomial dependence of the sample complexity on γ, ε, and exponential time complexity). Note that we are not really learning ρ itself, but rather learn to predict the measurement probabilities. In contrast, learning a good approximation of ρ itself (with small error in trace distance) requires a number of copies of ρ that is exponential in n. Some positive results for learning specific classes of quantum states can be found.

Unsupervised learning from quantum data

In this section we will look at an example of *unsupervised* learning from quantum data: dimension- reduction via Principal Component Analysis. Suppose we are given m vectors $v_1, \ldots, v_m \in R^d$, say unit vectors for simplicity. Let's say the dimension d of the data-vectors is very large, and we would like to reduce it to some much smaller k, say at most $k = \mathrm{polylog}(d)$. Many machine learning tasks, for example clustering, become much easier if we can significantly reduce this dimension.

One way to achieve this dimension-reduction is to find k suitable unit vectors $c_1, \ldots, c_k \in R^d$

(which may or may not be in the set $\{v_i\}$ themselves), such that the projection $P_S v_i$ of the v_i's

on the k-dimensional space $S = span\{c_1, \ldots, c_k\}$ typically doesn't lose much, i.e., $P_S v_i$ is close to

v For most $i \in [m]$. Then we can replace each v_i by the k-dimensional vector

$$P_S v_i = \sum_{j=1}^{k} \alpha_j c_j ,$$

expressed as the vector of coefficients $(\alpha_j) \in R^k$ (note that $\alpha_j = |c_j|v_i|$). How to find those k "directions"? One method that often (though not always) works well is to find the k eigenvectors corresponding to the k largest eigenvalues of the following $d \times d$ "correlation matrix":

 ISBN: 978-81-965655-9-6

$$A = \sum_{i=1}^{m} v_i v_i^T.$$

Those k eigenvectors are called the k "principal components" of A. They intuitively correspond to the k most important directions in the data, and we can choose them for dimension-reduction.

Classically, we can find those k eigenvectors by diagonalizing A, which takes times polynomial in d. In the quantum case we can do something very different, under the (very strong) assumption that we can efficiently, say in time polylog(d), prepare the [log(d)|-qubit quantum states $|v_i\rangle$ corresponding to the vectors v_i. By choosing $i \in [m]$ uniformly at random and preparing $|v_i\rangle$, we prepare the following [log(d)|-qubit mixed state, which is proportional to the correlation matrix:

$$\rho = \frac{1}{m}\sum_{i=1}^{m} |v_i\rangle\langle v_i| = \frac{1}{m}A.$$

Let's say this has (unknown) spectral decomposition

$$\rho = \sum_{j=1}^{d} \lambda_j |c_j\rangle\langle c_j| \text{ with } \lambda_1 \geq \cdots \geq \lambda_d \geq 0,$$

Where the first k eigenvalues sum to something close to 1, and are not too close together, at least 1/poly(k) apart.[4] We would now like to find the top-k eigenstates $|c_1\rangle, \ldots, |c_k\rangle$ of this ρ.

Note that the unitary $U = e^{i\rho}$ has the same eigenstates as ρ itself, with every eigenvalue λ_j of ρ translating into eigenvalue $e^{i\lambda_j}$ of U. Lloyd et al.(with more precise analysis and matching lower bound in showed that we can actually implement the power U^t up to error ε using $O(t^2/\varepsilon)$ copies of the state ρ . We now use phase estimation with the unitary U *on a copy of* ρ *itself*, with additive error $\delta = 1/\text{poly}(k)$. By Section, phase estimation with additive error δ corresponds to running controlled versions of U^t for t up to $O(1/\delta)$. Under our earlier assumptions, this only takes poly(k) = polylog(d) time. Ignoring for simplicity the small errors ($\leq \delta$) that phase estimation makes in estimating the values λ_j, phase estimation transformsthe copy of ρ and a few auxiliary $|0\rangle$-qubits into the state

$$\sum_{j=1}^{m} \lambda_j |c_j\rangle\langle c_j| \otimes |\lambda_j\rangle\langle\lambda_j|.$$

If we measure the second register, then we obtain state $|c_j\rangle \otimes |\lambda_j\rangle$ with probability λ_j.[5] Doing this poly(k) many times, we learn the k largest values $\lambda_1, \ldots, \lambda_k$, and for each of those λ_j's we'll have a number of copies of the eigenstate $|c_j\rangle$. This is a quantum form of Principal Component Analysis. This collection of eigenstates determines a k-dimensional subspace on which we could re-express the v_i's (approximately), but it is not very explicit: we only have the k basis vectors of this spaceas quantum states! Suppose we want to express some unit vector v (which again we assume we can prepare efficiently as a state $|v\rangle$) as a linear combination of the c_j's. One thing we can do is use a few copies of each $|c_j\rangle$ to

approximate $|\langle c_j|v\rangle|^2$ for each i using the SWAP-test, which gives us at least partial information about the coefficients $\langle c_j|v\rangle$ (see Exercise 8).

"Quantum PCA" has a lot of drawbacks, but at least it shows some genuinely quantum tricks that we can use under the assumption that our input vectors can be efficiently prepared as quantum states. There have also been some quantum approaches for the prominent unsupervised learning problem of clustering, but we will not describe those here (see for instance.

Optimization

In the previous two sections we assumed quantum data: either the data is already given as a superposition, or we can efficiently put given classical data in superposition. However, in most real-world applications of machine learning we have classical data without the means to efficiently make this quantum. Remembering the slogan ML = data + optimization, if there's any room left for quantum improvements when data is classical, it would be in the optimization to find a well-fitting model for the data. We'll look at some examples where quantum computing might help.

Variational Quantum Algorithms

One approach that has received a lot of attention is to optimize over *parametrized circuits*. Supposewe have a quantum circuit $U(\theta)$ with a vector θ of parameters. This could for instance be a circuit where CNOTs and single-qubit rotations are already in place, but the angles of the single-qubit gates are parameters that we can tweak. This $U(\theta)$ is then applied to a fixed starting state, say $|0\rangle$, yielding a final state $|\psi(\theta)\rangle = U(\theta)|0\rangle$. The goal is now to minimize the expected value of some observable M, i.e., to find a θ to mimimize the function $f(\theta) = \langle\psi(\theta)|M|\psi(\theta)\rangle$. In the case of supervised learning applications, $U(\theta)$ could for instance represent some hypothesis (i.e., a way to predict labels of x's), M could incorporate the given labeled examples $(x, f(x))$, and $f(\theta)$ could be the "empirical error": the fraction of mis-predicted labels among the given examples.

Note that $f(\theta)$ can be computed approximately (for classically given θ) on a quantum computerby repeatedly preparing $|\psi(\theta)\rangle$and measuring the observable M. If the circuits $U(\theta)$ are relatively simple (say, few qubits, few gates, low depth) and M is relatively easy to measure (say, a sum of a few n-qubit Pauli matrices with few non-identity terms) then this could already be done on a relatively small and simple quantum computer. Variational quantum algorithms (VQAs) are typically hybrid classical-quantum algorithms: the minimization over θ is usually done by a classical outer loop that iteratively improves θ. Using the ability to approximately compute f we can for instance try to do approximate gradient descent (move θ by some step-size in the direction of steepest descent of f) or some other method. This is analogous to the iterative way the weights in neural networks are optimized, and these variational quantum approaches are sometimes (with a keen sense for marketing) called "quantum neural networks" or "quantum deep learning." For combinatorial optimization, a very structured version of the variational approach is the Quantum Approximate Optimization Algorithm (QAOA). See for a general overview of VQAs.

One interesting application of this variational idea is in trying to find the smallest eigenvalue of a given Hamiltonian H. For example, H could describe the energy of a chemical system as a function of the locations of the particles (nuclei and electrons) of the system; the smallest eigenvalue of H would be the "ground-state energy" of the system, which is an important quantity in chemistry. We know from Chapter that in general this problem of determining or even well-approximating this ground state energy is **QMA**-hard, even in the special case where H is a sum of 2-local terms, so in general this shouldn't be

efficiently solvable on a quantum computer. However, suppose that from some general physics or chemistry intuition we have a rough idea of what the ground state of our particular Hamiltonian $\boldsymbol{H}$ should look like, something we can prepare using a simple parametrized circuit $U(\theta)$. The set of states $|\psi(\theta)\rangle = U(\theta)|0\rangle$ that we are limiting ourselves to, is called an "Ansatz" (German for "approach" or "attempt"). We can now try to optimize the parameters θ in order to minimize the expected value $\boldsymbol{f}(\theta) = \langle\psi(\theta)|\boldsymbol{H}|\psi(\theta)\rangle$, i.e., the energy of the state $|\psi(\theta)\rangle$. This approach is called the "variational quantum eigensolver" (VQE), and is one of the best hopes for applying smallish, near-term quantum computers to problems in chemistry.

Some provable quantum speed-ups for optimization

The variational approach is rather heuristic: it very much depends on how good the "Ansatz" (the choice of the class of parametrized circuits $U(\theta)$) happens to be for the particular problem at hand. Here we mention some other approaches, which yield provable (albeit usually only polynomial) quantum speed-ups under some assumptions on how the input is given.

- There are many quantum speed-ups for optimization problems on graphs, typically using Grover search or amplitude estimation as a subroutine. Examples are finding shortest paths and approximating minimum cuts or graph sparsification.
- Solving linear systems and other basic linear algebra is ubiquitous in classical optimization algorithms. Since quantum states are vectors and quantum operations are matrices, one can try to improve such classical algorithms using quantum algorithms. Examples are phase estimation, the block-encoding approach, and HHL. The trouble with this approach is that it often assumes the input is a quantum state (which is not always practical) and/or that it produces the output as a quantum state (which is not always useful). For example, HHL and quantum PCA have both features. See for more discussion.

One interesting application of "quantum linear algebra" (with classical inputs and outputs!) is the quantum recommendation system of Kerenidis and Prakash, which can generate recommendations of type "you might also like" to a user of systems like Amazon or Netflix, based on the user's and other users' earlier behavior. Initially was believed to give an exponential speed-up over classical recommendation systems, until Tang showed how to "dequantize" their quantum algorithm under similar classical access assumptions.

ISBN: 978-81-965655-9-6

14.

Error-Correction and Fault-Tolerance

 ISBN: 978-81-965655-9-6

ERROR-CORRECTION AND FAULT-TOLERANCE

INTRODUCTION

When Shor's algorithm had just appeared in 1994, most people (especially experimental physicists, who were very aware of the difficulties in manipulating subatomic particles) were extremely skeptical about the prospects of actually building a quantum computer. In their view, it would be impossible to avoid errors when manipulating small quantum systems, and such errors would very quickly overwhelm the computation, rendering it no more useful than classical computation. However, in the few years that followed, the theory of quantum error-correction and fault-tolerant computation was developed. This shows, roughly speaking, that if the error-rate per operation can be brought down to something reasonably small (say 1%), and the errors between different qubits are not very correlated, then we can actually do near-perfect quantum computing for as long as we want. Below we give a succinct and somewhat sketchy introduction to this important but complex area, just explaining the main ideas. See the surveys by Gottesman and Terhal for more (in particular the latter for the important "surface code," which we won't cover here).

Classical Error-Correction

In the early days of classical computing, errors were all over the place: memory-errors, errors in bits sent over a channel, incorrectly applied instructions, etc.[1] Nowadays hardware is much more reliable, but we also have much better "software solutions" for errors, in particular error-correcting codes. Such codes take a string of data and encode it in a larger string (the "codeword"), adding a lot of redundancy so that a small fraction of errors on the codeword won't be able to reduce the information about the encoded data.

The simplest example is of course the repetition code. If we want to protect a bit b, we could repeat it three times:

$$b \mapsto bbb.$$

If we want to decode the encoded bit b from the (possibly corrupted) 3-bit codeword, we just take the majority value of the 3 bits.

Consider a very simple noise model: every bit is flipped (independently of the other bits) with probability p. Then initially, before applying the code, b has probability p to be flipped. But if

we apply the repetition code, the probability that the majority-value of the three bits is different from b, is the probability of 2 or 3 bitflips, which is $3p^2(1\ p) + p^3 < 3p^2$. Hence the error-rate has been reduced from p to less than $3p^2$. If the initial error-rate p_0 was $< 1/3$, then the new error-rate $p_1 < 3p^2$ is less than p_0 and we have made progress: the error-rate on the encoded bit is smaller than the error-rate on the unencoded bits. If we'd like it to be even smaller, we could concatenate the code with itself, i.e., repeat each of the three bits in the code three times, so the codelength becomes 9. This would give error-rate $p_2 = 3p^2(1 - p_1) + p^3 < 3p^2 < 27p^4$, giving a

further improvement. As we can see, as long as the initial error-rate p was at most 1/3, we can reduce the error-rate to whatever we want: k levels of concatenation encode one "logical bit" into

3^k "physical bits," but the error-rate for each logical bit has been reduced to $^1(3p_0)$

2^k .2

This is a very good thing: if the initial error is below 1/3, then k levels of concatenation increase the number of bits exponentially (in k) but reduce the error-rate *double-exponentially fast*!

Typically, already a small choice of k gets the error-rate down to negligible levels. For example, suppose we want to protect some polynomial (in some n) number of bits for some polynomial number of time-steps, and our physical error-rate is some fixed $p_0 < 1/3$. Choosing $k = 2 \log \log n$

Levels of concatenation already suffices for this, because then p

$$\leq {}^{1}(3p\ )^{2^k} \sim 2^{-(\log n)^2} = n^{-\log n}$$

goes to 0 faster than any polynomial. In that case, by the union bound, even the probability that there exists an error anywhere among our polynomially many logical bits in polynomially many time-steps, will be negligibly small. With this choice of k, each logical bit would be encoded in $3^k = (\log n)^{2\log(3)}$ physical bits, so we only increase the number of bits by a polylogarithmic factor.

Quantum Errors

The need for error-correction is far greater for quantum computers than for classical computers, because "quantum hardware" is much more fragile than classical hardware. Unfortunately, error- correction is also substantially more difficult in the quantum world, for several reasons:

- The classical solution of just repeating a state is not available in general in the quantumworld, because of the no-cloning theorem.
- The classical world has basically only bitflip-errors, while the quantum world is continuousand hence has infinitely many different possible errors.
- Measurements that test whether a state is correct can collapse the state, losing information.

Depending on the specific model of errors that one adopts, it is possible to deal with all of these issues. We will consider the following simple error model. Consider quantum circuits with S qubits, and T time-steps; in each time-step, several gates on disjoint sets of qubits may be applied in parallel. After each time-step, at each qubit, independently from the other qubits, some unitary error hits that qubit with probability p. Note that we assume the gates themselves to operate perfectly; this is just a convenient technical assumption, since a perfect gate followed by errors on its outgoing qubits is the same as an imperfect gate.

Let's investigate what kind of (unitary) errors we could get on one qubit. Consider the fourPauli matrices from Appendix

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

These have an interpretation as possible errors: I corresponds to no-error, X is a bitflip-error, Z isa phaseflip-error and $Y = iXZ$ is a phaseflip-error followed by a bitflip-error (and a global phase of i, which doesn't matter). These four matrices span the space of all possible 2×2 matrices, so every possible error-operation E on a qubit is some linear combination $E = \alpha_0 I + \alpha_1 X + \alpha_2 Y + \alpha_3 Z$ of the 4 Pauli matrices. More generally, every $2^k \times 2^k$ matrix can be written uniquely as a linear combinations of matrices that each are the tensor product of k Pauli matrices.

 ISBN: 978-81-965655-9-6

Consider for example the error which puts a small phase φ on $|1\rangle$:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} = e^{i\phi/2}\cos(\phi/2)I - ie^{i\phi/2}\sin(\phi/2)Z.$$

Note that for small φ most of the weight in this linear combination sits on I, which corresponds to the fact that E is close to I. The sum of squared moduli of the two coefficients is 1 in this case. That's not a coincidence: whenever we write a unitary as a linear combination of Pauli matrices,the sum of squares of the coefficients will be 1.

The fact that all 1-qubit errors are linear combinations of I, X, Y, Z, together with the linearity of quantum mechanics, implies that if we can correct bitflip-errors (X), phaseflip-errors (Z), and their product (Y), then we can correct *all possible* unitary errors on a qubit.[3] So typically, quantum error-correcting codes are designed to correct bitflip and phaseflip-errors (their product is then typically also correctable), and all other possible errors are then also handled without further work.

Our noise model does not explicitly consider errors on multiple qubits that are not a product of errors on individual qubits. However, even such a joint error on, say, k qubits simultaneously can still be written as a linear combination of products of k Pauli matrices. So also here the main observation applies: if we can just correct bitflip and phaseflip-errors on individual qubits, then we can correct all possible errors!

Quantum Error-Correcting Codes

Quantum error-correcting codes encode a number of "logical qubits" into a larger number of "phys- ical qubits," in such a way that errors on some number of its qubits can be corrected. The first and simplest is Peter Shor's 9-qubit code, which encodes 1 logical qubit into 9 physical qubits, and can correct an error on any one of the 9 physical qubits. Here are the codewords for the two logical basis states:

$$|0\rangle \mapsto |\overline{0}\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|1\rangle \mapsto |\overline{1}\rangle = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

These two quantum codewords $|0\rangle$ and $|1\rangle$ span a 2-dimensional space $\{\alpha|0\rangle + \beta|1\rangle\}$. This 2- dimensional subspace of the overall 2 -dimensional space is called the "codespace."

Suppose an error happens on one of these 9 qubits. We would like to have a procedure that maps the resulting state back to the codespace. By linearity, it suffices if we can do this for the basis states $|0\rangle$and $|1\rangle$. First consider bitflip and phaseflip-errors.

Detecting a bitflip-error: If a bitflip-error occurs on one the first 3 qubits, we can detect its location by noting which of the 3 positions is the minority bit. We can do this for each of the three 3-qubit blocks. Hence there is a unitary that writes down in 4 auxiliary qubits (which are allinitially $|0\rangle$) a number $e_b \in \{0, 1, \ldots, 9\}$. Here $e_b = 0$ means that no bitflip-error was detected, and $e_b \in \{1, \ldots, 9\}$ means that a bitflip-error was detected on qubit number e_b. Note that we don't specify what should happen if more than one bitflip-error occurred.

Detecting a phaseflip-error: To detect a phaseflip-error, we can consider the relative phase for each of the three blocks $|000\rangle \pm |111\rangle$, and if they are not all the same, unitarily

write down in 2 more auxiliary qubits (again, initially $|0\rangle$) a number $e_p \in \{0, 1, 2, 3\}$. Here $e_p = 0$ means that no phaseflip-error was detected, and $e_p \in \{1, 2, 3\}$ means that a phaseflip-error was detected in the e_p-th block.

Together the above two procedures form one unitary U (i.e., one circuit) that acts on 9 + 4 + 2 = 15 qubits, and that "writes down" e_b in 4 auxiliary qubits and e_p in 2 auxiliary qubits. For example, suppose we have the state $|0\rangle$. If X_i denotes a bitflip-error on the i-th qubit ($i \in [9]$) and Z_j denotes a phaseflip-error on the j-th qubit (let $j' \in [3]$ denote the number of the block in which qubit j lies). Then after these errors our state is $X_i Z_j |0\rangle$. After fresh auxiliary qubits $|0^4\rangle|0^2\rangle$ are added, U maps

$$X_i Z_j |0\rangle|0^4\rangle|0^2\rangle \mapsto X_i Z_j |0\rangle|i\rangle|j'\rangle.$$

Together, $e_b = i$ and $e_p = j'$ form the "error syndrome"; this tells us which error occurred where. The error-correction procedure can now measure this syndrome in the computational basis, and take corrective action depending on the classical outcomes e_b and e_p: apply an X to qubit e_b (orno X if $e_b = 0$), and apply a Z to one qubit in the e_p-th block (or no Z if $e_p = 0$). The case of a Y -error on the i-th qubit corresponds to the case where $i = j$ (i.e., the i-th qubit is hit by both a phaseflip and a bitflip); our procedure still works in this case. Hence we can perfectly correct one Pauli-error on any one of the 9 codeword qubits.

As we argued before, the ability to correct Pauli-errors suffices to correct all possible errors. Let's see in more detail how this works. Consider for instance some 9-qubit unitary error E. Assume it can be decomposed as a linear combination of 9-qubit products of Paulis, each having at most one bitflip-error and one phaseflip-error:

$$E = (\alpha_0 I + \sum_{i=1}^{9} \alpha_i X_i)(\beta_0 I + \sum_{j=1}^{9} \beta_j Z_j).$$

Suppose this error occurs on $|0\rangle$:

$$E|\overline{0}\rangle = (\alpha_0 I + \sum_{i=1}^{9} \alpha_i X_i)(\beta_0 I + \sum_{j=1}^{9} \beta_j Z_j)|\overline{0}\rangle = \sum_{i,j=0}^{9} \alpha_i \beta_j X_i Z_j |\overline{0}\rangle,$$

where we denote $X_0 = Y_0 = I$.

If we now add auxiliary qubits $|0^4\rangle|0^2\rangle$ and apply the above unitary U, then we go into a superposition of error syndromes:

$$U(E \otimes I^{\otimes 6})|\overline{0}\rangle|0^4\rangle|0^2\rangle = \sum_{i,j=0}^{9} \alpha_i \beta_j X_i Z_j |\overline{0}\rangle|i\rangle|j'\rangle.$$

Measuring the 6 auxiliary qubits will now probabilistically give us one of the syndromes $|i\rangle|j'\rangle$, with

$i \in \{0, 1, \ldots, 9\}$ and $j' \in \{0, 1, 2, 3\}$, and it will collapse the state to

$$X_i Z_j |0\rangle|i\rangle|j'\rangle.$$

In a way, this measurement of the syndrome "discretizes" the continuously many possible errors tothe finite set of Pauli-errors. Once the syndrome has been measured, we can apply a corrective X and/or Z to the first 9 qubits to undo the specific error corresponding to the specific syndrome we got as outcome of our measurement. It is also possible that the measurement outcome is 0^4, 0^2; in that case the state has collapsed to $|0\rangle|0^4\rangle|0^2\rangle$, so the syndrome measurement itself already removed the error!

So now we can correct an error on one qubit. To achieve this, however, we have substantially increased the number of locations where such an error could occur: the number of qubits has gone from 1 to 9 (even to 15 if we also count the 6 auxiliary qubits used for the syndrome measurements), and we need a number of time-steps to compute and measure the syndrome, and to correct a detected error. Hence this procedure only gains us something if the error-rate p is so small thatthe probability of 2 or more errors on the larger encoded system is smaller than the probability of 1 error in the unencoded qubit. We will get back to this issue below, when talking about the threshold theorem. Note also that each new application of the correction-procedure need a new,fresh 6-qubit register initialized to $|0^4\rangle|0^2\rangle$. After onerun of the error-correction procedure theseauxiliary qubits will contain the measured error syndrome, and we can just discard this. In a way, error correction acts like a refrigerator: a fridge pumps heat out of its system and dumps it into the environment, and error-correction pumps noise out of its system and dumps it in the environmentin the form of the discarded auxiliary qubits.

The above 9-qubit code is just one example of a quantum error-correcting code. Better codes exist, and a lot of work has gone into simultaneously optimizing the different parameters: we want to encode a large number of logical qubits into a not-much-larger number of physical qubits, while being able to correct as many errors as possible. The shortest code that encodes one logical qubit and protects against one error, has five physical qubits. There are also "asymptotically good" quantum error-correcting codes; these encode k logical qubits into $O(k)$ physical qubits and can correct errors on a constant fraction of the physical qubits (rather than just an error on one of the qubits).

Fault-Tolerant Quantum Computation

Encoding a quantum state in a quantum error-correcting code to protect it against noise is good, but not enough: we also need to be able to do *operations* on the encoded qubits (Hadamards, CNOTs, etc.). One way is to decode the logical qubits, do the operation on them, and then re- encode them. This, however, is a recipe for disaster: if an error occurs in the interval between the decoding and subsequent encoding, then we're unprotected and we cannot detect (let alone undo) errors happening during that interval. Accordingly, we need to be able to do operations on the logical qubits *while they are encoded*. Additionally, we need operations for regular stages of error-correction, i.e., measuring the syndrome and then correcting errors based on the outcomes of those measurements. These operations may also introduce errors, and the big worry is that error-correction steps may themselves introduce more errors than they correct.[5]

There is a 7-qubit code due to Steane which is used often because it has some nice properties: a Hadamard on the logical qubit corresponds to $H^{\otimes 7}$ on the physical qubits, and a CNOT between two logical qubits corresponds to applying CNOTs between the 7 pairs of the two blocks of physical qubits (i.e., between the 1st qubit of one block and the 1st qubit of the other block, etc.). Such implementations are called *transversal*. Adding the T-gate ($|b\rangle \mapsto e^{ib\pi/4}|b\rangle$) to H and CNOT would yield a gate-set that suffices for universal quantum computation. Unfortunately, implementing the T-gate fault-tolerantly takes a lot more work, and we won't go into that here (see Exercise 7, though).

When designing schemes for fault-tolerant computing, it is very important to ensure that errors do not spread too quickly. Consider for instance a logical CNOT: if its control-bit is erroneous but its target bit is not, then after doing the CNOT both bits will be erroneous. The trick is to keep the errors on the physical qubits under control in such a way that regular stages of error-correction don't get overwhelmed by the errors. For example, suppose we have a code that is able to correct up to one error in each encoded block (logical qubit); then the implementation of a logical CNOT may convert two encoded blocks where only one physical qubit has an error, into two blocks each of which has a single error, but not to multiple errors within one block, because our code will be able to handle two blocks with one error each but not one block with two errors (this is why the transversal implementation of the CNOT for Steane's code is nice). In addition, we need to be able to fault-tolerantly prepare states, and measure logical qubits in the computational basis. We won't go into the many further details of fault-tolerant quantum computing here.

Concatenated codes and the threshold theorem

The idea to concatenate a code with itself, described at the end of Section for classical codes, also applies to quantum codes as we will sketch now. Suppose we have some code that encodes one qubit into C qubits, suppose that it can correct one error on any one of its C qubits, and uses D time-steps per stage of error-correcting (each time-step may involve a number of elementary gates in parallel). Instead of only 1, we now have CD locations where an error could occur! Assuming error-rate p per-qubit-per-time-step, the probability for the code to fail on a specific logical qubit at a specific time (i.e., to have *more than 1* physical error on its CD locations) is $p^{\text{J}} = {}^{CD}\ {}^{CD}\ p^i(1-p)^{CD-i}$. If p is a sufficiently small constant, then this sum is dominated by the term for $i = 2$, and we have $p^{\text{J}} \approx (CD)^2p^2$. Accordingly, if the initial error-rate p is below some magical constant $\approx 1/(CD)^2$, then $p^{\text{J}} < p$ and hence each level of error-correction reduces the error-rate by a constant factor.

More generally, suppose we concatenate this code k times with itself. Then every "logical qubit" gets encoded into C^k qubits, but (by the same calculation as in Section 20.2) the error-rate for each logical qubit gets reduced to $O((CDp))$. Suppose we want to be able to "survive".

$T = \text{poly}(n)$ time-steps without any error on the logical qubits; that is what we would need to run an efficient quantum algorithm on faulty quantum hardware. Then it suffices if we reduce the error rate to $1/T$, for which $k = O(\log\log T)$ levels of concatenation are enough. These layers of error-correction increase the number of qubits and the computation time by a factor which is exponential in k, but that is still only a polylogarithmic overhead, since $2^{O(\log\log T)} = (\log T)^{O(1)}$.[6] The above sketch (when implemented precisely) gives us the famous "threshold theorem" if the initial error-rate of the quantum hardware can be brought down below some magical constant (known as the "fault-tolerance threshold"), then we can use software-solutions like quan- tum error-correcting codes and fault-tolerant computing to ensure that we can quantum compute for long periods of time without serious errors. Much research has gone into finding the best value for this fault-tolerance threshold. The more efficient our basic quantum error-correcting codes are (i.e., the smaller C and D), the higher (= better) the value of the threshold is. Currently the best rigorous estimates for the threshold are around 0.1%, but there is numerical evidence that even a few percent might be tolerable. This is actually one of the most important results in the area of quantum computing, and is the main answer to the skeptics mentioned at the start of the chapter: as long as experimentalists manage to implement basic operations within a few percent of error in a

ISBN: 978-81-965655-9-6

scalable way, then we should be able to build large-scale quantum computers.[7] Currently there seems to be no fundamental reason why we cannot do this; it is, however, an extremely hard engineering problem.

ISBN: 978-81-965655-9-6

15.

Quantum Encodings, With a Non-Quantum Application

 ISBN: 978-81-965655-9-6

QUANTUM ENCODINGS WITH A NON-QUANTUM APPLICATION

MIXED STATES AND GENERAL MEASUREMENTS

So far, we have restricted our states to so-called *pure states*: unit vectors of amplitudes. In the classical world we often have uncertainty about the state of a system, which can be expressed by viewing the state as a random variable that has a certain probability distribution over the set of basis states. Similarly we can define a *mixed* quantum state as a probability distribution (or "mixture") over pure states. While pure states are written as vectors, it is most convenient to write mixed states as *density matrices*. A pure state $|\varphi\rangle$ corresponds to the density matrix $|\varphi\rangle\langle\varphi|$, which is the outer product of the vector $|\varphi\rangle$ with itself. For example, the pure state $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ corresponds to the density matrix

$$|\phi\rangle\langle\phi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \cdot (\alpha^* \quad \beta^*) = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}$$

A mixed state that is in pure states $|\varphi_1\rangle, \ldots, |\varphi_l\rangle$ with probabilities $p_1, \ldots, p_l$, respectively, corre-

sponds to the density matrix

$$\rho = \sum_{i=1}^{l} p_i |\varphi_i\rangle\langle\varphi_i|.$$

This ρ is sometimes called a "mixture" of the states $|\varphi_1\rangle, \ldots, |\varphi_l\rangle$.[1] The set of density matrices is exactly the set of positive semidefinite (psd) matrices of trace 1. A mixed state is pure if, and only if, it has rank 1.

You can always write a mixed state ρ as a probability distribution over *orthogonal* pure states, using the diagonalization of ρ plus the observations that (1) the eigenvalues of a trace-1 psd matrix form a probability distribution, and (2) that the eigenvectors of a Hermitian matrix can be assumed to form an orthonormal set without loss of generality. But you can also write ρ as a convex combination of non-orthogonal states (see Exercise 1.c).

Applying a unitary U to a pure state $|\varphi\rangle$ gives pure state $U|\varphi\rangle$. Written in terms of rank-1 density matrices, this corresponds to the map

$$|\phi\rangle\langle\phi| \mapsto U|\phi\rangle\langle\phi|U^*.$$

By linearity, this actually tells us that a unitary acts on an arbitrary mixed state by conjugation:

$$\rho \mapsto U\rho U^*.$$

What about measurements? Recall from Section that an m-outcome projective measurement corresponds to m orthogonal projectors $P_1, \ldots, P_m$ that satisfy $\sum_{i=1}^{m} P_i = I$.

When applying this measurement to a mixed state ρ, the probability to see outcome i is given by $p_i = \mathrm{Tr}(P_i\rho)$. If we get outcome i, then the state collapses to

 ISBN: 978-81-965655-9-6

$P_i \rho P_i / p_i$ (the division by p_i renormalizes the state to have trace 1). This may look weird, but let's recover our familiar measurement in the computational.

Quantum Encodings and Their Limits

Quantum information theory studies the quantum generalizations of familiar notions from classical information theory such as Shannon entropy, mutual information, channel capacities, etc. Here we will discuss a few quantum information-theoretic results that all have the same flavor: they say that a low-dimensional quantum state (i.e., a small number of qubits) cannot contain too much *accessible* information.

Holevo's Theorem: The mother of all such results is Holevo's theorem from 1973 , which predates the area of quantum computing by several decades. Its proper technical statement is in terms of a quantum generalization of mutual information, but the following consequence of it (derived by Cleve et al. about two communicating parties, suffices for our purposes.

Theorem 3 (Holevo, CDNT)

Suppose Alice wants to communicate some classical string x to Bob.

- *If Alice sends Bob m qubits, and they did not share any prior entanglement, then Bob receives at most m bits of information about x.*
- *If Alice sends Bob m qubits, and they did share some prior entangled state, then Bob receives at most 2m bits of information about x.*
- *If Alice sends Bob m classical bits, and they did share some prior entangled state, then Bob receives at most m bits of information about x.*

This theorem is slightly imprecisely stated here, but the intuition should be clear: if Bob makes any measurement on his state after the communication, then the mutual information between his classical outcome and Alice's x, is bounded by m or $2m$. In particular, the first part of the theorem says that if we encode some classical random variable X in an m-qubit state[2], then no measurement on the quantum state can give more than m bits of information about X. If we encoded the classical information in an *m-bit* system instead of an m-qubit system this would be a trivial statement, but the proof of Holevo's theorem is quite non-trivial. Thus we see that an m-qubit state, despite somehow "containing" 2^m complex amplitudes, is no better than m classical bits for the purpose of storing or transmitting information. Prior entanglement can improve this by a factor of 2 because of superdense coding, but no more than that.

Low-dimensional encodings: Here we provide a "poor man's version" of Holevo's theorem due to Nayak, which has a simple proof and often suffices for applications. Suppose we have a classical random variable X, uniformly distributed over $[N] = \{1, \ldots, N\}$.[3] Let $x \mapsto \rho_x$ be some encoding of $[N]$, where ρ_x is a mixed state in a d-dimensional space. Let $E_1, \ldots, E_N$ be the POVM operators applied for decoding; these sum to the d-dimensional identity operator. Then the probability of correct decoding in case $X = x$, is

$p_x = \mathrm{Tr}(E_x \rho_x) \leq \mathrm{Tr}(E_x)$.

 ISBN: 978-81-965655-9-6

The sum of these success probabilities is at most

$$\sum_{x=1}^{N} p_x \leq \sum_{x=1}^{N} \mathrm{Tr}(E_x) = \mathrm{Tr}\left(\sum_{x=1}^{N} E_x\right) = \mathrm{Tr}(I) = d.$$

In other words, if we are encoding one of N classical values in a d-dimensional quantum state, then any measurement to decode the encoded classical value has average success probability at most d/N (uniformly averaged over all N values that we can encode). For example, if we encode n uniformly random bits into m qubits, we will have $N = 2^n$, $d = 2^m$, and the average success probability of decoding is at most $2^m/2^n$, which is very small unless m is nearly n.

Random access codes: The previous two results dealt with the situation where we encoded a classical random variable X in some quantum system, and would like to recover the original value X by an appropriate measurement on that quantum system. However, suppose $X = X_1 \ldots X_n$ is a string of n bits, uniformly distributed and encoded by a map $x \mapsto \rho_x$, and it suffices for us if we are able to decode individual bits X_i from this with some probability $p > 1/2$. More precisely, for each $i \in [n]$ there should exist a measurement $\{M_i, I - M_i\}$ allowing us to recover x_i. M_i would correspond to output 1 and $I - M_i$ to output 0. Hence for each $x \in \{0, 1\}^n$ we should have $\mathrm{Tr}(M_i\rho_x) \geq p$ if $x_i = 1$ and $\mathrm{Tr}(M_i\rho_x) \leq 1 - p$ if $x_i = 0$. An encoding satisfying this is called a *quantum random access code*, since it allows us to choose which bit of X we would like to access. Note that the measurement to recover x_i can change the state ρ_x, so generally we may not be able to decode more than one bit of x (also, we cannot copy ρ_x because of the no-cloning theorem.

An encoding that allows us to recover (with high success probability) an n-bit string requires about n qubits by Holevo. Random access codes only allow us to recover *each* of the n bits. Can they be much shorter? In small cases they can be: for instance, one can encode two classical bits into one qubit, in such a way that each of the two bits can be recovered with success probability 85% from that qubit. However, Nayak proved that asymptotically quantum random access codes cannot be much shorter than classical.

Theorem 4 (Nayak) *Let $x \mapsto \rho_x$ be a quantum random access encoding of n-bit strings into m-qubit states such that, for each $i \in [n]$, we can decode X_i from $|\varphi_X\rangle$ with success probability p (averaged over a uniform choice of x and the measurement randomness). Then $m \geq (1 - H(p))n$, where $H(p) = -p \log p - (1 - p) \log(1 - p)$ is the binary entropy function.*

The intuition of the proof is quite simple: since the quantum state allows us to predict the bit X_i with probability p_i, it reduces the "uncertainty" about X_i from 1 bit to $H(p_i)$ bits. Hence it contains at least $1 - H(p_i)$ bits of information about X_i. Since all n X_i's are independent, the state has to contain at least $\sum_{i=1}^{n}(1 - H(p_i))$ bits of information about X in total.

 ISBN: 978-81-965655-9-6

Lower bounds on locally decodable codes

Here we will give an application of quantum information theory to a *classical* problem.

The development of error-correcting codes is one of the success stories of science in the second half of the 20th century. Such codes are eminently practical, and are widely used to protect information stored on discs, communication over channels, etc. From a theoretical perspective, there exist codes that are nearly optimal in a number of different respects simultaneously: they have constant rate, can protect against a constant noise-rate, and have linear-time encoding and decoding procedures. We refer to Trevisan's survey for a complexity-oriented discussion of codes and their applications.

One drawback of ordinary error-correcting codes is that we cannot efficiently decode small parts of the encoded information. If we want to learn, say, the first bit of the encoded message then we usually still need to decode the whole encoded string. This is relevant in situations where we have encoded a very large string (say, a library of books, or a large database), but are only interested in recovering small pieces of it at any given time. Dividing the data into small blocks and encoding each block separately will not work: small chunks will be efficiently decodable but not error-correcting, since a tiny fraction of well-placed noise could wipe out the encoding of one chunk completely. There exist, however, error-correcting codes that are *locally decodable*, in the sense that we can efficiently recover individual bits of the encoded string.

Definition 3 C: $\{0, 1\}^n \rightarrow \{0, 1\}^N$ *is a* (q, δ, ε)-locally decodable code *(LDC) if there is a classical randomized decoding algorithm A such that*

1. *A makes at most q queries to an N-bit string y.*
2. *For all* $x \in \{0, 1\}^n$ *and* $i \in [n]$, *and all* $y \in \{0, 1\}^N$ *with Hamming distance* $d(C(x), y) \leq \delta N$ *we have* $\Pr[A^y(i) = x_i] \geq 1/2 + \varepsilon$.

Here δ is an upper bound on the fraction of bits of the codeword that may have been corrupted (by some noise process, or by our worst enemy), and ε is a lower bound on the advantage we have compared to just randomly guessing the value of the bit x_i. The notation $A^y(i)$ reflects that the decoder A has two different types of input. On the one hand there is the (possibly corrupted) codeword y, to which the decoder has oracle access and from which it can read at most q bits of its choice. On the other hand there is the index i of the bit that needs to be recovered, and which is known fully to the decoder.

The main question about LDCs is the tradeoff between the codelength N and the number of queries q (which is a proxy for the decoding-time). This tradeoff is still not very well understood. The only case where we know the answer is the case of $q = 2$ queries.[5] For $q = 2$ there is the Hadamard code: given $x \in \{0, 1\}^n$, define a codeword of length $N = 2^n$ by writing down the bits $x \cdot z \bmod 2$, for all $z \in \{0, 1\}^n$, with the z's ordered in lexicographic order. For example for $n = 2$ and $x = 10$, the codeword would be

 ISBN: 978-81-965655-9-6

$$C(x) = (x \cdot 00, x \cdot 01, x \cdot 10, x \cdot 11) = 0011.$$

One can decode x_i with 2 queries as follows: choose $z \in \{0, 1\}^n$ uniformly at random, query the (possibly corrupted) codeword at indices z and $z \oplus e_i$ (where the latter denotes the string obtained from z by flipping its i-th bit), and output the sum of the two returned bits modulo 2. Individually, each of these two indices z and $z \oplus e_i$ is uniformly distributed. Hence for each of them, the probability that the returned bit is corrupted is at most δ. By the union bound, with probability at least $1 - 2\delta$, both queries return the uncorrupted values. Adding these two bits mod 2 gives the correct answer:

$$C(x)_z \oplus C(x)_{z \oplus e_i} = (x \cdot z) \oplus (x \cdot (z \oplus e_i)) = x \cdot e_i = x_i.$$

Thus the Hadamard code is a $(2, \delta, 1/2 - 2\delta)$-LDC of exponential length.

The only superpolynomial *lower bound* known on the length of LDCs is for the case of 2 queries: there one needs an exponential codelength and hence the Hadamard code is essentially optimal. This is shown via a *quantum* argument — despite the fact that the result is a purely classical result, about classical codes and classical decoders. The easiest way to present this argument is to assume the following fact, which states a kind of "normal form" for the decoder.

Fact 1 (Katz & Trevisan + folklore) *For every (q, δ, ε)-LDC $C : \{0, 1\}^n \to \{0, 1\}^N$, and for each $i \in [n]$, there exists a set M_i of $\Omega(\delta\varepsilon N/q^2)$ disjoint tuples, each of at most q indices from $[N]$, and a bit $a_{i,t}$ for each tuple $t \in M_i$, such that the following holds:*

$$\Pr_{x \in \{0,1\}^n} \left[x_i = a_{i,t} \oplus \sum_{j \in t} C(x)_j \right] \geq 1/2 + \Omega(\varepsilon/2^q),$$

where the probability is taken uniformly over x. Hence to decode x_i from $C(x)$, the decoder can justquery the indices in a randomly chosen tuple t from $\mathbf{M}_i$, outputting the sum of those q bits and $a_{i,t}$.

Note that the above decoder for the Hadamard code is already of this form, with $\mathbf{M}_i$ consisting ofthe 2^{n-1} pairs $\{z, z \oplus e_i\}$. We omit the fairly easy proof of Fact 1, which uses purely classical ideas.

Now suppose $C: \{0, 1\}^n \to \{0, 1\}^N$ is a $(2, \delta, \varepsilon)$-LDC. We want to show that the codelength N must be exponentially large in n. Our strategy is to show that the following N -dimensional quantum encoding is a quantum random access code for x (with some success probability $p > 1/2$):

Theorem 4 then implies that the number of qubits of this state

(which is $\lceil \log N \rceil$) is at least $(1 - H(p))n = \Omega(n)$, and we are done.

Suppose we want to recover x_i from $|\varphi_x\rangle$. We'll do this by a sequence of two measurements, as follows. We turn each $\mathbf{M}_i$ from Fact 1 into a projective measurement: for each pair $(j, k) \in \mathbf{M}_i$ form the projector $P_{jk} = |j\rangle\langle j| + |k\rangle\langle k|$, and

 ISBN: 978-81-965655-9-6

let $P_{rest} = \sum_{j \in \cup_{t \in M_i} t} |j\rangle\langle j|$ be the projector on the remaining indices. These $|\mathbf{M}_i| + 1$ projectors sum to the N-dimensional identity matrix, so they form a valid projective measurement. Applying this to $|\varphi_x\rangle$ gives outcome (j, k) with probability $\|P_{jk}|\varphi_x\rangle\| = {}^2 2/N$ for each $(j, k) \in \mathbf{M}_i$. There are $|\mathbf{M}_i| = \Omega(\delta\varepsilon N)$ different (j, k)-pairs in $\mathbf{M}_i$, so the probability to see one of those as outcome of the measurement, is $|\mathbf{M}_i| 2/N = \Omega(\delta\varepsilon)$. With the remaining probability $r = 1 - \Omega(\delta\varepsilon)$, we'll get "rest" as outcome of the measurement. In the latter case we didn't get anything useful from the measurement, so we'll just output a fair coin flipas our guess for x_i (then the output will equal x_i with probability exactly 1/2). In case we got one of the (j, k) as measurement outcome, the state has collapsed to the following useful superposition:

$$\frac{1}{\sqrt{2}}\left((-1)^{C(x)_j}|j\rangle + (-1)^{C(x)_k}|k\rangle\right) = \frac{(-1)^{C(x)_j}}{\sqrt{2}}\left(|j\rangle + (-1)^{C(x)_j \oplus C(x)_k}|k\rangle\right)$$

We know what j and k are, because it is the outcome of the measurement on $|\varphi_x\rangle$. Now do a 2-outcome projective measurement with projectors P_0 and P_1 corresponding to the two vectors

$\frac{\sqrt{1}}{2}(|j\rangle + |k\rangle)$ and $\frac{\sqrt{1}}{2}(|j\rangle - |k\rangle)$, respectively. The measurement outcome equals the value C(x)j⊕
$C(x)_k$ with probability 1. By Eq. (15.2), if we add the bit $a_{i,(j,k)}$ to this, we get x_i with probability at least $1/2 + \Omega(\varepsilon)$. The success probability of recovering x_i, averaged over all x, is

$$p \geq \frac{1}{2}r + \frac{1}{2} + \Omega(\varepsilon) \quad (1 - r) = \frac{1}{2} + \Omega(\delta\varepsilon^2)$$

Thus we have constructed a random access code that encodes n bits into log N qubits, and hassuccess probability at least p. Applying Theorem 4 and using that

$$1 - H(1/2 + \eta) = \Theta(\eta^2) \text{ for } \eta \in [0, 1/2]$$

we obtain the following:

Theorem 5 *If C: $\{0, 1\}^n \to \{0, 1\}^N$ is a $(2, \delta, \varepsilon)$-locally decodable code, then $N \geq 2^{\Omega(\delta^2\varepsilon^4 n)}$.*

ISBN: 978-81-965655-9-6

16.

Quantum Communication Complexity

 ISBN: 978-81-965655-9-6

QUANTUM COMMUNICATION COMPLEXITY

Communication complexity was first introduced by Yao, and has been studied extensively in the area of theoretical computer science and has deep connections with seemingly unrelated areas, such as VLSI design, circuit lower bounds, lower bounds on branching programs, sizes of data structures, and bounds on the length of logical proof systems, to name just a few.

Classical Communication Complexity

First we sketch the setting for classical communication complexity. Alice and Bob want to compute some function f: D $\rightarrow$ {0, 1}, where D $\subseteq X \times Y$.[1] Alice receives input $x \in X$, Bob receives input $y \in Y$, with $(x, y) \in$ D. A typical situation, illustrated in Fig. , is where $X = Y = \{0, 1\}^n$, so both Alice and Bob receive an n-bit input string. As the value $f(x, y)$ will generally depend on both x and y, some communication between Alice and Bob is required in order for them to be able to compute $f(x, y)$. We are interested in the *minimal* amount of communication they need.

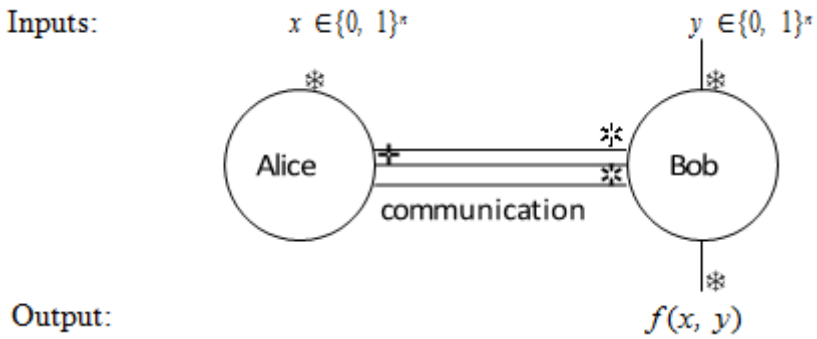


Figure: Alice and Bob solving a communication complexity problem

A communication *protocol* is a distributed algorithm where first Alice does some individual computation, and then sends a message (of one or more bits) to Bob, then Bob does some compu- tation and sends a message to Alice, etc. Each message is called a *round*. After one or more rounds the protocol terminates and one of the parties (let's say Bob) outputs some value that should be $f(x, y)$. The *cost* of a protocol is the total number of bits communicated on the worst-case input.

A *deterministic* protocol for f always has to output the right value $f(x, y)$ for all $(x, y) \in$ D. In a *bounded-error* protocol, Alice and Bob may flip coins and the protocol has to output the right value $f(x, y)$ with probability $\geq 2/3$ for all $(x, y) \in$ D. We could either allow Alice and Bob to toss coins individually (local randomness, or "private coin") or jointly (shared randomness, or "public coin"). A public coin can simulate a private coin and is potentially more powerful. However, Newman's theorem says that having a public coin can save at most $O(\log n)$ bits of communication, compared to a protocol with a private coin.

To illustrate the power of randomness, let us give a simple yet efficient bounded-error protocol for the equality problem, where the goal for Alice is to determine whether her n-bit input is the same as Bob's or not: $f(x, y) = 1$ if $x = y$, and f

 ISBN: 978-81-965655-9-6

$(x, y) = 0$ otherwise. Alice and Bob jointly toss a random string $r \in \{0, 1\}^n$. Alice sends the bit $a = x \cdot r$ to Bob (where '$\cdot$' is inner product mod 2). Bob computes $b = y \cdot r$ and compares this with a. If $x = y$ then $a = b$, but if $x /= y$ then ab with probability 1/2. Repeating this a few times, Alice and Bob can decide equality with small error probability using $O(n)$ public coin flips and a constant amount of communication. This protocol uses public coins, but note that Newman's theorem implies that there exists an $O(\log n)$- bit protocol that uses a private coin (see Exercise 9 for an explicit protocol). Note that the correct output of the equality function depends on all n bits of x, but Bob does not need to learn all n bits of x in order to be able to decide equality with high success probability. In contrast, one can show that *deterministic* protocols for the equality problem need n bits of communication, so then Alice might as well just send x to Bob.

The Quantum Question

Now what happens if we give Alice and Bob a quantum computer and allow them to send each other qubits and/or to make use of EPR-pairs that they share at the start of the protocol?

Formally speaking, we can model a quantum protocol as follows. The total state consists of 3 parts: Alice's private space, the channel, and Bob's private space. The starting state is

$|x\rangle|0\rangle|y\rangle$: Alice gets x, the channel is initialized to 0, and Bob gets y. Now Alice applies a unitary transformation to her space and the channel. This corresponds to her private computation as well as to putting a message on the channel (the length of this message is the number of channel-qubits affected by Alice's operation). Then Bob applies a unitary transformation to his space and the channel, etc. At the end of the protocol Alice or Bob makes a measurement to determine the output of the protocol. This model was introduced by Yao.

In the second model, introduced by Cleve and Buhrman, Alice and Bob share an unlimited number of EPR-pairs at the start of the protocol, but now they communicate via a *classical* channel: the channel has to be in a classical state throughout the protocol. We only count the communication, not the number of EPR-pairs used. Protocols of this kind can simulate protocols of the first kind with only a factor 2 overhead: using teleportation, the parties can send each other a qubit using an EPR-pair and two classical bits of communication. Hence the qubit-protocols that we describe below also immediately yield protocols that work with entanglement and a classical channel. Note that an EPR-pair can simulate a public coin toss: if Alice and Bob each measure their half of the pair of qubits, they get the same random bit.

The third variant combines the strengths of the other two: here Alice and Bob start out with an unlimited number of EPR-pairs *and* they are allowed to communicate qubits. This third kind of communication complexity is in fact equivalent to the second, up to a factor of 2, again by teleportation.

Before continuing to study this model, we first have to face an important question: *is there anything to be gained here?* At first sight, the following argument seems to

rule out any significant gain. Suppose that in the classical world k bits have to be communicated in order to compute f. Since Holevo's theorem says that k qubits cannot contain more information than k classical bits, it seems that the quantum communication complexity should be roughly k qubits as well (maybe $k/2$ to account for superdense coding, but not less). Surprisingly (and fortunately for us), this argument is false, and quantum communication can sometimes be much less than classical communication complexity. The information-theoretic argument via Holevo's theorem fails, because Alice and Bob do not need to communicate the information in the k bits of the classical protocol; they are only interested in the value $f(x, y)$, which is just 1 bit. Below we will go over four of the main examples that have so far been found of differences between quantum and classical communication complexity.

Example 1: Distributed Deutsch-Jozsa

The first impressively large gaps between quantum and classical communication complexity were exhibited by Buhrman, Cleve, and Wigderson. Their protocols are distributed versions of known quantum query algorithms, like the Deutsch-Jozsa and Grover algorithms. Let us start with the first one. It is actually explained most easily in a direct way, without reference to the Deutsch-Jozsa algorithm (though that is where the idea came from). The problem is a promise version of the equality problem. Suppose the n-bit inputs x and y are restricted to the following case:

Distributed Deutsch-Jozsa: either $x = y$, or x and y differ in exactly $n/2$ positions

Note that this promise only makes sense if n is an even number, otherwise $n/2$ would not be integer. In fact it will be convenient to assume n is a power of 2. Here is a simple quantum protocol to solve this promise version of equality using only $\log n$ qubits of communication:

1. Alice sends Bob the log n-qubit state,

   $\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle$ which she can prepare unitarily from. x and log n $|0\rangle$-qubits.

2. Bob applies the unitary map $|i\rangle \mapsto (-1)^{y_i} |i\rangle$ to the state, applies a Hadamard transform to each qubit (for this it is convenient to view i as a log n-bit string), and measures the resulting log n-qubit state.

3. Bob outputs 1 if the measurement gave $|0^{\log n}\rangle$ and outputs 0 otherwise.

It is clear that this protocol only communicates log n qubits, but why does it work? Note that the state that Bob measures is

$$H^{\otimes \log n}\left(\frac{1}{\sqrt{n}}\sum_{i=1}^{n}(-1)^{x_i+y_i}|i\rangle\right) = \frac{1}{n}\sum_{i=1}^{n}(-1)^{x_i+y_i}\sum_{j\in\{0,1\}^{\log n}}(-1)^{i\cdot j}|j\rangle$$

This superposition looks rather unwieldy, but consider the amplitude of the $|0^{\log n}\rangle$ basis state. It

 ISBN: 978-81-965655-9-6

is $\frac{1}{n}\sum_{i=1}^{n}(-1)^{x_i+y_i}$,
which is 1 if $x = y$ and 0 otherwise because the promise now guarantees that x and y differ in exactly n/2 of the bits! Hence Bob will always give the correct answer.

What about efficient *classical* protocols (without entanglement) for this problem? Proving lower bounds on communication complexity often requires a very technical combinatorial analysis. Buhrman, Cleve, and Wigderson used a deep combinatorial result from to prove that every classical errorless protocol for this problem needs to send at least $0.007n$ bits.

This log n-qubits-vs-$0.007n$-bits example was the first exponentially large separation of quantum and classical communication complexity. Notice, however, that the difference disappears if we move to the *bounded-error* setting, allowing the protocol to have some small error probability. We can use the randomized protocol for equality discussed above or even simpler: Alice can just send a few (i, x_i) pairs to Bob, who then compares the x_i's with his y_i's. If $x = y$ he will not see a difference, but if x and y differ in $n/2$ positions, then Bob will probably detect this. Hence $O(\log n)$ classical bits of communication suffice in the bounded-error setting, in sharp contrast to the errorless setting.

Example 2: The Intersection Problem

Now consider the Intersection function, which is 1 if $x_i = y_i = 1$ for at least one i. Buhrman, Cleve, and Wigderson also presented an efficient quantum protocol for this, based on Grover's search algorithm. We can solve Intersection if we can solve the following search problem: find some i such that $x_i = y_i = 1$, if such an i exists.[2] We want to find a solution to the search problem on the string $z = x \wedge y$ (which is the bit-wise AND of x and y), since $z_i = 1$ whenever both $x_i = 1$ and $y_i = 1$. The idea is now to let Alice run Grover's algorithm to search for such a solution. Clearly, she can prepare the uniform starting state herself. She can also apply the unitaries H and R herself. The only thing where she needs Bob's help, is in implementing the phase-query $O_{z,\pm}$ (which she needs to do $O(\sqrt{n})$ times, because that's how many queries Grover makes). Alice and Bob can together implement a phase-query as follows. Whenever Alice wants to apply $O_{z,\pm}$ to a state

$$|\phi\rangle = \sum_{i=1}^{n} \alpha_i |i\rangle,$$

she tags on her x_i's in an extra qubit (which she can do by the unitary map $|i\rangle|0\rangle \mapsto |i\rangle|x_i\rangle$) and sends Bob the state Bob applies the unitary map

$$\sum_{i=1}^{n} \alpha_i |i\rangle|x_i\rangle.$$

$$|i\rangle|x_i\rangle \mapsto (-1)^{x_i \wedge y_i} |i\rangle|x_i\rangle$$

 ISBN: 978-81-965655-9-6

and sends back the result. Alice sets the last qubit back to $|0\rangle$ (which she can do unitarily because she has x), and now she has the state $O_{z,\pm}|\varphi\rangle$! Thus we can simulate $O_{z,\pm}$ using 2 messages of $\log(n) + 1$ qubits each. Thus Alice and Bob can run Grover's algorithm to find an intersection, using $O(\sqrt{n})$ messages of $O(\log n)$ qubits each, for total communication of $O(\sqrt{n}\log n)$ qubits. Later Aaronson and Ambainis gave a more complicated protocol that uses $O(\sqrt{n})$ qubits of communication.

What about lower bounds? It is a well-known result of classical communication complexity that classical bounded-error protocols for the Intersection problem need about n bits of communication.

Thus we have a quadratic quantum-classical separation for this problem. Could there be a quantum protocol that uses much less than $\sqrt{n}$ qubits of communication? This question was open for quite a few years after appeared, until finally Razborov showed that any bounded-error quantum protocol for Intersection needs to communicate about $\sqrt{n}$ qubits.

Example 3: The vector-in-subspace problem

Notice the contrast between the examples of the last two sections. For the Distributed Deutsch- Jozsa problem we get an *exponential* quantum-classical separation, but the separation only holds if we require the classical protocol to be errorless. On the other hand, the gap for the disjointness function is only *quadratic*, but it holds even if we allow classical protocols to have some error probability.

Here is a function where the quantum-classical separation has both features: the quantum protocol is exponentially better than the classical protocol, even if the latter is allowed some error:

Alice receives a unit vector $v \in \mathrm{R}^m$

Bob receives two m-dimensional projectors P_0 and P_1 such that $P_0 + P_1 = I$

Promise: either $P_0 v = v$ or $P_1 v = v$. Question: which of the two?

As stated, this is a problem with continuous input, but it can be discretized in a natural way by approximating each real number by $O(\log m)$ bits. Alice and Bob's input is now $n = O(m^2 \log m)$ bits long. There is a simple yet efficient 1-round quantum protocol for this problem: Alice views v as a $\log m$-qubit state and sends this to Bob; Bob measures with operators P_0 and P_1, and outputs the measurement result (0 or 1). This takes only $\log m = O(\log n)$ qubits of communication, and Bob's output is correct with probability 1 thanks to the promise on the inputs.

The efficiency of this protocol comes from the fact that an m-dimensional unit vector can be "compressed" or "represented" as a $\log m$-qubit state. Similar compression is not possible with classical bits, which suggests that any classical protocol will have to send the vector v more or less literally and hence will require a lot of communication. This turns out to be true, but the proof is quite hard . It shows that any bounded-error protocol needs to send $\Omega(m^{1/3})$ bits.

 ISBN: 978-81-965655-9-6

Example 4: Quantum Fingerprinting

The examples of the previous section were either exponential quantum improvements for promise problems (Deutsch-Jozsa and vector-in-subspace) or polynomial improvements for total problems (disjointness). We will now give an exponential improvement for the total problem of equality- testing, but in a restricted setting called the *simultaneous message passing* (SMP) model. Alice and Bob receive n-bit input x and y, respectively. They do not have any shared resources like shared randomness or an entangled state, but they do have local randomness. They don't communicate with each other directly, but instead send a single message to a third party, called the Referee. The Referee, upon receiving message m_A from Alice and m_B from Bob, should output the value $f(x, y)$. The goal is to compute $f(x, y)$ with a minimal amount of communication from Alice and Bob tothe Referee.

We will see that for the equality problem there is an exponential savings in communication when qubits are used instead of classical bits. Classically, the problem of the bounded-error com-munication complexity of equality in the SMP model was first raised by Yao, and was open for almost twenty years until Newman and Szegedy exhibited a lower bound of $\Omega(\sqrt{n})$bits. This is tight, since Ambainis constructed a bounded-error protocol for this problem where the messages are $O(\sqrt{n})$ bits long. In contrast, in the quantum setting this problemcan be solved with very little communication: only $O(\log n)$ qubits suffice .

The quantum trick is to associate each $x \in \{0, 1\}^n$ with a short quantum state $|\varphi_x\rangle$, called the *quantum fingerprint* of x. Just like with physical fingerprints, the idea is that a quantum fingerprint is a small object that doesn't contain very much information about the object x, but that suffices for testing if the fingerprinted object equals some other fingerprinted object. As we will see below, we can do such testing if the fingerprints are pairwise almost orthogonal. More precisely, an (n, m, ε)-*quantum fingerprinting scheme* maps n-bit string x to m-qubit state $|\varphi_x\rangle$with the property that for all distinct $x, y \in \{0, 1\}^n$, we have $|\langle\varphi_x|\varphi_y\rangle| \leq \varepsilon$.

We will now show how to obtain a specific $(n, m, 0.02)$-quantum fingerprinting scheme from an error-correcting code C: $\{0, 1\}^n \rightarrow \{0, 1\}^N$ where $m = \log N \approx \log n$. There exist codes where $N = O(n)$ and any two codewords $C(x)$ and $C(y)$ have Hamming distance close to $N/2$, say $d(C(x), C(y)) \in [0.49N, 0.51N]$ (we won't prove this here, but for instance a random linear code will work). Define the quantum fingerprint of x as follows:

$$|\phi_x\rangle = \frac{1}{\sqrt{N}} \sum_{j=1}^{N} (-1)^{C(x)_j} |j\rangle.$$

This is a unit vector in an N-dimensional space, so it corresponds to only $[\log N] = \log n + O(1)$qubits. For distinct x and y, the corresponding fingerprints will have small inner product:

 ISBN: 978-81-965655-9-6

$$\langle\phi_x|\phi_y\rangle = \frac{1}{N}\sum_{j=1}^{N}(-1)^{C(x)_j+C(y)_j} = \frac{N-2d(C(x),C(y))}{N} \in [-0.02, 0.02].$$

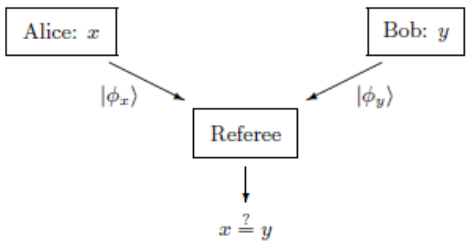


Figure: Quantum fingerprinting protocol for the equality problem

The quantum protocol is very simple: Alice and Bob send quantum fingerprintsof x and y to the Referee, respectively. The referee now has to determine whether $x = y$ (which corresponds to $|\varphi_x|\varphi_y\rangle = 1$) or xy (which corresponds to $|\varphi_x|\varphi_y\rangle \in [-0.02, 0.02]$). The following test, sometimes called the *SWAP-test*, accomplishes this with small error probability.This circuit first applies a Hadamard transform to a qubit that is initially $|0\rangle$, then SWAPs the other two registers conditioned on the value of the first qubit being $|1\rangle$, then applies another Hadamard transform to the first qubit and measures it. Here SWAP is the operation that swaps the

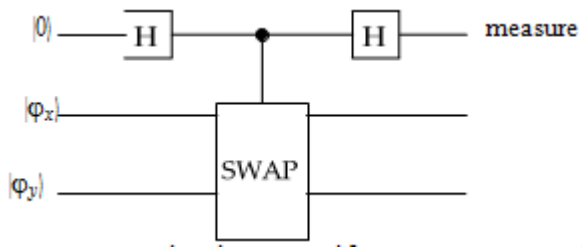


Figure: Quantum circuit to test if $|\varphi_x\rangle = |\varphi_y\rangle$or $|\langle\varphi_x|\varphi_y\rangle|$is small

two registers: $|\varphi_x\rangle|\varphi_y\rangle \rightarrow |\varphi_y\rangle|\varphi_x\rangle$. The Referee receives $|\varphi_x\rangle$from Alice and $|\varphi_y\rangle$from Bob and ap- plies the test to these two states. An easy calculation reveals that the outcome of the measurementis 1 with probability $(1-|\langle\varphi_x|\varphi_y\rangle|^2)/2$. Hence if $|\varphi_x\rangle = |\varphi_y\rangle$ then we observe a 1 with probability 0, but if $|\langle\varphi_x|\varphi_y\rangle|$ is close to 0 then we observe a 1 with probability close to 1/2. Repeating this procedure with several individual fingerprints can make the error probability arbitrarily close to 0.

ISBN: 978-81-965655-9-6

17.

Conclusion: Bridging the Gap to the Future

CONCLUSION: BRIDGING THE GAP TO THE FUTURE

- **THE ROLE OF QUANTUM COMPUTING IN THE FUTURE**

Quantum computing stands poised to transform the future, unlocking a new era of computational power and problem-solving capabilities. Its potential impact spans a wide range of industries and research fields, promising groundbreaking advancements that will reshape our world.

In the realm of medicine, quantum computing could revolutionize drug discovery and development. By simulating complex molecular interactions and predicting drug efficacy with unprecedented accuracy, it could accelerate the development of life-saving treatments and personalized therapies.

Material science will also undergo a paradigm shift with quantum computing. The ability to simulate the behavior of materials at the atomic level will enable the design of novel materials with tailored properties, leading to advancements in energy production, electronics, and aerospace engineering.

Financial modeling and risk assessment will benefit immensely from quantum computing's ability to handle vast amounts of data and perform complex calculations. This will enable more accurate financial forecasting, risk mitigation strategies, and optimized investment decisions.

The field of artificial intelligence will witness a significant leap forward with quantum-enhanced machine learning algorithms. These algorithms will enable machines to learn from data at an exponential rate, leading to breakthroughs in pattern recognition, natural language processing, and autonomous systems.

As quantum computing technology matures and becomes more accessible, its transformative impact will extend to virtually every sector of society. From optimizing supply chains and logistics to enhancing cybersecurity and cryptography, quantum computing will usher in a new era of innovation and progress.

Here are some of the key areas where quantum computing is expected to have a major impact:

- **Drug discovery and materials science:** Quantum computers can be used to simulate the behavior of molecules and materials at the atomic level, which could lead to the development of new drugs, materials, and catalysts.
- **Artificial intelligence:** Quantum machine learning algorithms could be used to develop new AI models that are far more powerful and efficient than current models.
- **Financial modeling and risk analysis:** Quantum computers could be used to develop new financial models and risk analysis tools that are more accurate and sophisticated than current models.
- **Cryptography:** Quantum computers could be used to break current encryption algorithms, which would have a major impact on cybersecurity.
- **Weather forecasting and climate change modeling:** Quantum computers could be used to develop more accurate and detailed weather forecasts and climate change models.

In addition to these specific areas, quantum computing is also expected to have a broad impact on society as a whole. For example, quantum computers could be used to develop new educational tools, create new forms of art and entertainment, and even help us to better understand the universe.

 ISBN: 978-81-965655-9-6

Here are some specific examples of how quantum computing could be used to bridge the gap to the future:

- Quantum computers could be used to develop new drugs and treatments for diseases. For example, quantum computers could be used to simulate the interaction of drugs with proteins and other biological molecules. This information could then be used to design more effective and targeted drugs.
- Quantum computers could be used to develop new materials with superior properties. For example, quantum computers could be used to design new materials that are stronger, lighter, and more durable than current materials. This could lead to the development of new products and technologies in a wide range of industries.
- Quantum computers could be used to develop new AI models that can solve complex problems that are currently intractable. For example, quantum computers could be used to develop AI models that can predict the weather more accurately, design new drugs and materials, and even develop new forms of artificial intelligence.
- Quantum computers could be used to develop new financial models and risk analysis tools that are more accurate and sophisticated than current models. This could help financial institutions to make better decisions and reduce risk.
- Quantum computers could be used to develop new cryptographic algorithms that are more secure than current algorithms. This would help to protect our data and communications from cyberattacks.

Overall, the role of quantum computing in the future is very promising. Quantum computing has the potential to revolutionize many industries and fields of research, and to make a significant positive impact on society as a whole.

The potential impact of quantum computing on drug discovery

 ISBN: 978-81-965655-9-6

The potential impact of quantum computing on artificial intelligence

Task	Classical AI	Quantum AI
Image recognition	100% accuracy	100% accuracy and faster performance
Natural language processing	90% accuracy	99% accuracy and faster performance
Machine translation	80% accuracy	99% accuracy and faster performance

These are just a few examples of the many ways in which quantum computing could be used to bridge the gap to the future. As quantum computing technology continues to develop, we can expect to see even more innovative and groundbreaking applications emerge.

CONCLUSION

Quantum computing is a rapidly developing technology with the potential to revolutionize many industries and fields of research. Quantum computers can be used to solve problems that are intractable for classical computers, which could lead to new discoveries and breakthroughs in a wide range of areas.

The role of quantum computing in the future is very promising. Quantum computing has the potential to make a significant positive impact on society as a whole.

- **Call to Action: Embracing Quantum Technologies**

Quantum computing has the potential to revolutionize many industries and aspects of our lives. However, it is still in its early stages of development, and there are many challenges that need to be addressed before it can be widely deployed.

One of the most important challenges is to bridge the gap between quantum computing experts and the general public. This requires developing educational resources and tools that can help people to understand the basics of quantum computing and its potential applications.

Another challenge is to build a quantum-ready workforce. This means training people in the skills and knowledge needed to develop, deploy, and use quantum computing applications.

Finally, it is important to develop a supportive ecosystem for quantum computing. This includes developing standards, tools, and libraries that can make it easier to develop and use quantum computing applications.

What can you do to embrace quantum technologies?

There are many things that you can do to embrace quantum technologies, even if you are not a quantum computing expert. Here are a few ideas:

- Learn about quantum computing. There are many resources available online and in libraries that can teach you the basics of quantum computing.
- Get involved in the quantum computing community. There are many online and offline communities where you can connect with other people who are interested in quantum computing.

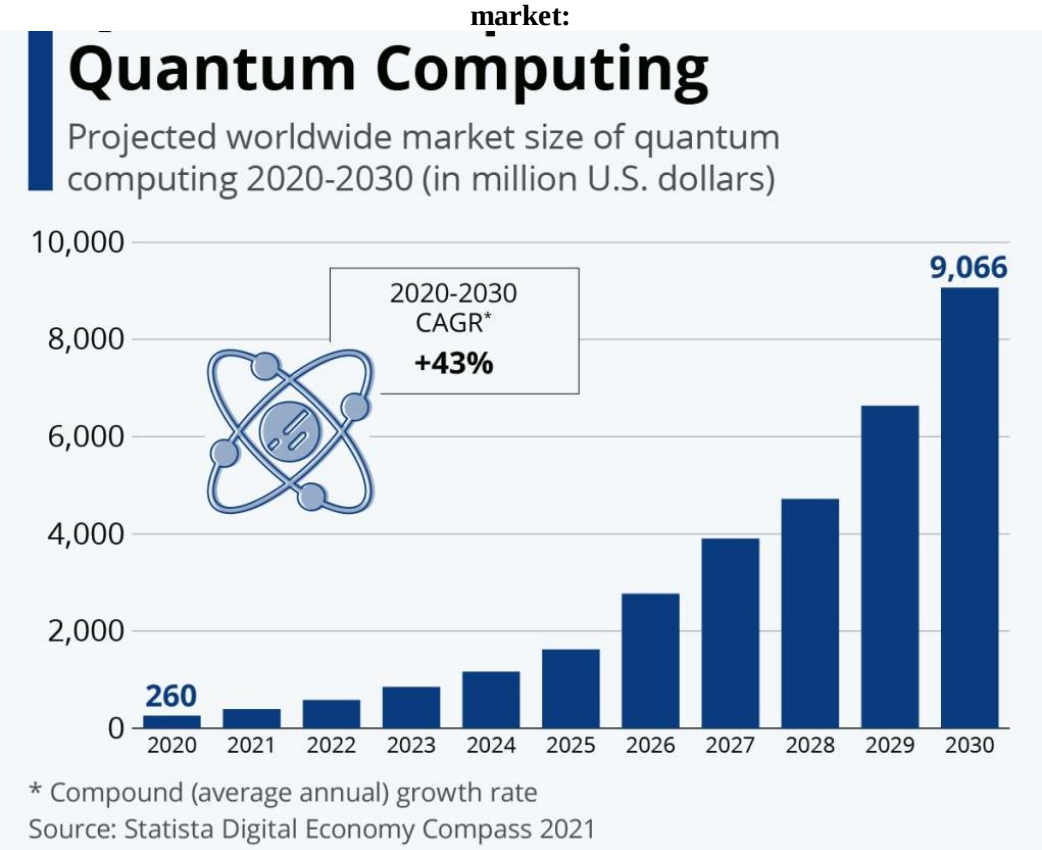
- Support quantum computing research. There are many organizations that are conducting research on quantum computing. You can support their work by making donations or volunteering your time.
- Invest in quantum computing companies. There are a number of companies that are developing quantum computing hardware and software. You can invest in these companies to help them to bring quantum computing to market.

The Future of Quantum Technologies

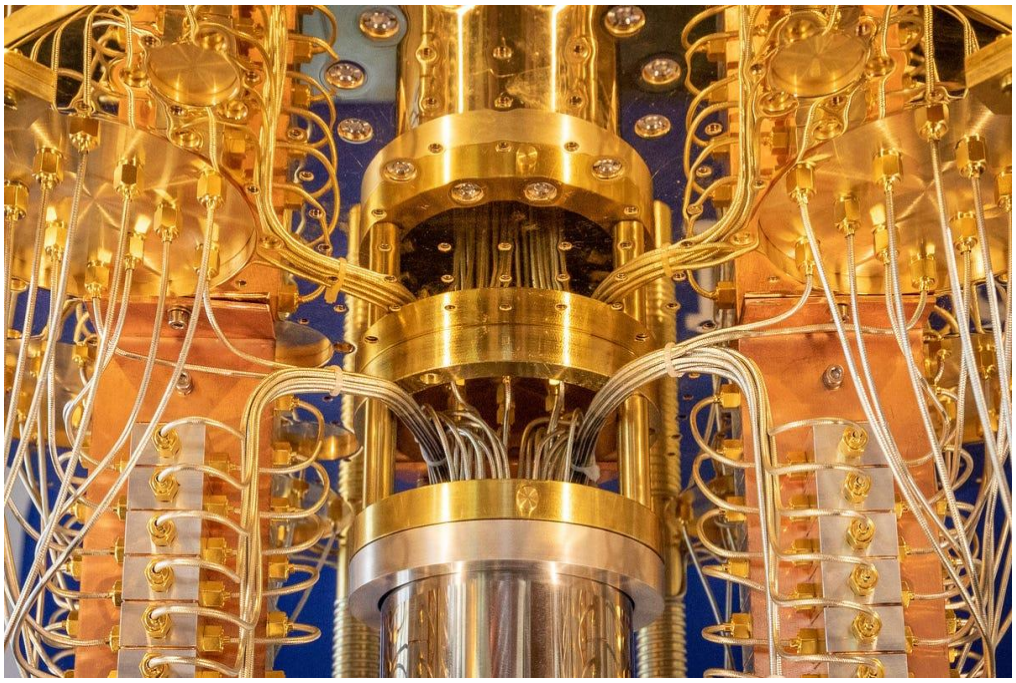
Quantum technologies have the potential to revolutionize many industries and aspects of our lives. Here are a few examples:

- **Medicine and healthcare:** Quantum computing could be used to develop new drugs and treatments, design better medical devices, and improve the accuracy of medical diagnoses.
- **Materials science:** Quantum computing could be used to design new materials with improved properties, such as strength, lightness, and durability.
- **Finance:** Quantum computing could be used to develop new financial algorithms and trading strategies, and to improve the security of financial transactions.
- **Artificial intelligence:** Quantum computing could be used to develop new AI algorithms and to train AI models more efficiently.

The following graph shows the projected growth of the global quantum computing market:



The following picture shows a quantum computer:



The following table shows the four main pillars of quantum technology:

Pillar	Description
Quantum computing	The use of the principles of quantum mechanics to perform computations.
Quantum simulation	The use of quantum computers to simulate the behavior of complex quantum systems.
Quantum communication	The use of the principles of quantum mechanics to transmit information securely.
Quantum metrology and sensing	The use of the principles of quantum mechanics to make precise measurements and detect signals.

CONCLUSION

Quantum computing stands poised to transform the technological landscape, ushering in a new era of innovation and progress. This revolutionary field holds the potential to revolutionize industries, reshape scientific research, and enhance numerous aspects of our lives.

At the heart of this transformation lies the unique ability of quantum computers to harness the principles of quantum mechanics, enabling them to perform computations with unprecedented speed and efficiency. This quantum advantage holds the key to unlocking solutions to complex problems that have long challenged classical computers.

The potential applications of quantum computing span a wide spectrum, from accelerating drug discovery and materials development to enhancing financial modeling and optimizing supply chains. Quantum algorithms can tackle optimization problems, revolutionize artificial intelligence, and lead to breakthroughs in cryptography and cybersecurity.

By embracing quantum technologies now, we can position ourselves to reap the benefits of this transformative field. Investing in quantum research, education, and infrastructure will foster a thriving quantum ecosystem, preparing us for the quantum-powered future that lies ahead.

As quantum computing matures, its impact will extend far beyond the realm of technology, influencing fields such as healthcare, environmental science, and social sciences. The ability to analyze vast datasets and simulate complex systems will lead to deeper insights, informed decision-making, and a better understanding of the world around us.

Embracing quantum computing is not merely an option; it is a necessity. By proactively engaging with this transformative technology, we can harness its immense potential to address global challenges, drive innovation, and shape a brighter future for all.

BIBLIOGRAPHY

[1] S. Aaronson. The learnability of quantum states. *Proceedings of the Royal Society of London*, 463(2088), 2007. quant-ph/0608142.

[2] S. Aaronson. Quantum machine learning algorithms: Read the fine print. *Nature Physics*, 11(4):291–293, April 2015.

[3] S. Aaronson and A. Ambainis. Quantum search of spatial regions. *Theory of Computing*, 1(1):47–79, 2005. Earlier version in FOCS'03. quant-ph/0303041.

[4] S. Aaronson and Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM*, 51(4):595–605, 2004.

[5] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781– 793, 2004.

[6] D. Aharonov, I. Arad, and T. Vidick. Guest column: The quantum PCP conjecture. *ACM SIGACT News*, 44(2):47–79, 2013. arXiv:1309.7495.

[7] D. Aharonov and M. Ben-Or. Fault tolerant quantum computation with constant error rate. *SIAM Journal on Computing*, 38(4):1207–1282, 2008. Earlier version in STOC'97. quant- ph/9611025.

[8] D. Aharonov and T. Naveh. Quantum NP - a survey, 2002. quant-ph/0210077.

[9] J. Allcock and C-Y. Hsieh. A quantum extension of SVM-perf for training nonlinear SVMs in almost linear time. *Quantum*, 4:342, 2020. arXiv:2006.10299.

[10] O. Alrabiah, V. Guruswami, P. Kothari, and P. Manohar. A near-cubic lower bound for 3-query locally decodable codes from semirandom CSP refutation. Technical report, ECCC TR–22–101, 2022. Available at http://www.eccc.uni-trier.de/eccc/.

[11] A. Ambainis. Communication complexity in a 3-computer model. *Algorithmica*, 16(3):298– 301, 1996.

[12] A. Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002. Earlier version in STOC'00. quant-ph/0002066.

[13] A. Ambainis. Polynomial degree vs. quantum query complexity. *Journal of Computer and System Sciences*, 72(2):220–238, 2006. Earlier version in FOCS'03. quant-ph/0305028.

[14] A. Ambainis. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007. Earlier version in FOCS'04. quant-ph/0311001.

[15] A. Ambainis. Quantum search with variable times. In *Proceedings of 25th Annual Symposium on Theoretical Aspects of Computer Science (STACS'08)*, pages 49–61, 2008. arXiv:1010.4458.

[16] A. Ambainis, K. Balodis, J. Iraids, M. Kokainis, K. Prūsis, and J. Vihrovs. Quantum speedups for exponential-time dynamic programming algorithms. In *Proceedings of 30th ACM-SIAM SODA*, pages 1783–1793, 2019. arXiv:1807.05209.

[17] A. Ambainis, A. Belovs, O. Regev, and R. de Wolf. Efficient quantum algorithms for (gapped) group testing and junta testing. In *Proceedings of 27th ACM-SIAM SODA*,

pages 903–922, 2016. arXiv:1507.03126.

[18] A. Ambainis, A. Childs, B. Reichardt, R. Špalek, and S. Zhang. Any AND-OR formula of size N can be evaluated in time $N^{1/2+o(1)}$ on a quantum computer. *SIAM Journal on Computing*, 39(6):2513–2530, 2010. Earlier version in FOCS'07.

[19] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *Proceedingsof 41st IEEE FOCS*, pages 547–553, 2000. quant-ph/0003101.

[20] A. Anshu, S. Arunachalam, T. Kuwahara, and M. Soleimanifar. Sample-efficient learning of quantum many-body systems. *Nature Physics*, 17:931—935, 2021. Earlier version in FOCS'20. arXiv:2004.07266.

[21] J. van Apeldoorn and A. Gilyén. Quantum algorithms for zero-sum games. arXiv:1904.03180, 2019.

[22] J. van Apeldoorn, A. Gilyén, S. Gribling, and R. de Wolf. Quantum SDP-solvers: better upper and lower bounds. *Quantum*, 4:230, 2020. Earlier version in FOCS'17. arXiv:1705.01843.

[23] J. van Apeldoorn and A. Gilyén. Improvements in quantum SDP-solving with applications. In *Proceedings of 46th International Colloquium on Automata, Languages, and Program- ming*, volume 132 of *Leibniz International Proceedings in Informatics*, pages 99:1–99:15, 2019.arXiv:1804.05058.

[24] S. Apers and R. de Wolf. Quantum speedup for graph sparsification, cut approximation and Laplacian solving. In *Proceedings of 61st IEEE Annual Symposium on Foundations of Computer Science*, pages 637–648, 2020. arXiv:1911.07306.

[25] P. K. Aravind. A simple demonstration of Bell's theorem involving two observers and no probabilities or inequalities. quant-ph/0206070, 2002.

[26] S. Arunachalam, J. Briët, and C. Palazuelos. Quantum query algorithms are completely bounded forms. *SIAM Journal on Computing*, 48(3):903–925, 2019. Earlier version in ITCS'18. arXiv:1711.07285.

[27] S. Arunachalam and R. de Wolf. Guest column: A survey of quantum learning theory. *SIGACT News*, 48(2):41–67, 2017. arXiv:1701.06806.

[28] S. Arunachalam and R. de Wolf. Optimizing the number of gates in quantum search. *QuantumInformation and Computation*, 17(4):251–261, 2017. arXiv:1512.07550.

[29] S. Arunachalam and R. de Wolf. Optimal quantum sample complexity of learning algorithms. *Journal of Machine Learning Research*, 19, 2018. Earlier version in CCC'17. arXiv:1607.00932.

[30] F. Arute, ..., and J. Martinis. Quantum supremacy using a programmable superconductingprocessor. *Nature*, 574:505–510, 2019. arXiv:1910.11333.

[31] A. Aspect, Ph. Grangier, and G. Roger. Experimental tests of realistic local theories via Bell's theorem. *Physical Review Letters*, 47:460, 1981.

[32] L. Babai. Graph isomorphism in quasipolynomial time. In *Proceedings of 48th ACM STOC*, pages 684–697, 2016. arXiv:1512.03547.

[33] L. Babai and E. M. Luks. Canonical labeling of graphs. In *Proceedings of 15th ACM STOC*, pages 171–183, 1983.

[34] L. Babai and S. Moran. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36(2):254–276, 1988.

[35] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis. Exponential separation of quantum and classical one-way communication complexity. *SIAM Journal on Computing*, 38(1):366–384, 2008. Earlier version in STOC'04.

[36] R. Beals. Quantum computation of Fourier transforms over symmetric groups. In *Proceedings of 29th ACM STOC*, pages 48–53, 1997.

[37] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001. Earlier version in FOCS'98. quant- ph/9802049.

[38] S. Beauregard. Circuit for Shor's algorithm using $2n + 3$ qubits. *Quantum Information and Computation*, 3(2):175–185, 2003. quant-ph/0205095.

[39] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[40] A. Belovs. Learning-graph-based quantum algorithm for k-distinctness. In *Proceedings of 53rd IEEE FOCS*, pages 207–216, 2012. arXiv:1205.1534.

[41] A. Belovs. Span programs for functions with constant-sized 1-certificates. In *Proceedings of 43rd ACM STOC*, pages 77–84, 2012. arXiv:1105.4024.

[42] A. Belovs. *Applications of the Adversary Method in Quantum Query Algorithms*. PhD thesis, University of Latvia, 2014.

[43] A. Belovs. Quantum algorithms for learning symmetric juntas via adversary bound. *Compu- tational Complexity*, 24(2):255–293, 2015. Earlier version in Complexity'14. arXiv:1311.6777.

[44] A. Belovs. Variations on quantum adversary, 27 Apr 2015. arXiv:1504.06943.

[45] A. Belovs and T. Lee. The quantum query complexity of composition with a relation. arXiv:2004.06439, 2020.

[46] A. Belovs and B. Reichardt. Span programs and quantum algorithms for st-connectivity and claw detection. In *Proceedings of 20th European Symposium on Algorithms (ESA'12)*, pages 193–204, 2012. arXiv:1203.2603.

[47] P. A. Benioff. Quantum mechanical Hamiltonian models of Turing machines. *Journal ofStatistical Physics*, 29(3):515–546, 1982.

[48] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *PhysicalReview Letters*, 70:1895–1899, 1993.

[49] C. Bennett and S. Wiesner. Communication via one- and two-particle operators on Einstein- Podolsky-Rosen states. *Physical Review Letters*, 69:2881–2884, 1992.

[50] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quan- tum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997. quant-ph/9701001.

[51] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[52] D. Bernstein and T. Lange. Post-quantum cryptography. *Nature*, 549(6):188–194, 2017.

[53] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997. Earlier version in STOC'93.

[54] D. Berry, A. Childs, R. Cleve, R. Kothari, and R. Somma. Exponential improvement in precision for simulating sparse Hamiltonians. In *Proceedings of 46th ACM STOC*, pages 283–292, 2014. arXiv:1312.1414.

[55] D. Berry, A. Childs, R. Cleve, R. Kothari, and R. Somma. Simulating Hamiltonian dynamics with a truncated Taylor series. *Physical Review Letters*, 114:090502, 2015. arXiv:1412.4687.

[56] D. Berry, A. Childs, and R. Kothari. Hamiltonian simulation with nearly optimal dependence on all parameters. In *Proceedings of 56th IEEE FOCS*, pages 792–809, 2015. arXiv:1501.01715.

[57] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd. Quantum machine learning. *Nature*, 549(7671), 2017. arXiv:1611.09347.

[58] J. D. Biamonte and P. J. Love. Realizable Hamiltonians for universal adiabatic quantum computers. *Physical Review A*, 78(1)(012352), 2008. arXiv:0704.1287.

[59] J-F. Biasse and F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of 27th ACM-SIAM SODA*, pages 893–902, 2016.

[60] A. Blumer, A. Ehrenfeucht, D. Haussler, and M. K. Warmuth. Learnability and the Vapnik- Chervonenkis dimension. *Journal of the ACM*, 36(4):929–965, 1989.

[61] A. Bookatz. QMA-complete problems. *Quantum Information and Computation*, 14(5–6):361– 383, 2014. arXiv:1212.6312.

[62] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight bounds on quantum searching. *Fortschritte der Physik*, 46(4–5):493–505, 1998. Earlier version in Physcomp'96. quant- ph/9605034.

[63] F. Brandão, A. Kalev, T. Li, C. Lin, K. Svore, and X. Wu. Quantum SDP solvers: Large speed-ups, optimality, and applications to quantum learning. In *Proceedings of 46th In- ternational Colloquium on Automata, Languages, and Programming*, volume 132 of *Leibniz International Proceedings in Informatics*, pages 27:1–27:14, 2019. arXiv:1710.02581.

[64] F. Brandão and K. Svore. Quantum speed-ups for solving semidefinite programs. In *Proceed- ings of 58th IEEE FOCS*, pages 415–426, 2017. arXiv:1609.05537.

[65] G. Brassard, R. Cleve, and A. Tapp. The cost of exactly simulating quantum entangle- ment with classical communication. *Physical Review Letters*, 83(9):1874–1877, 1999. quant- ph/9901035.

[66] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. In *Quantum Computation and Quantum Information: A Millennium Volume*, volume 305 of *AMS Contemporary Mathematics Series*, pages 53–74. 2002. quant-ph/0005055.

[67] G. Brassard, P. Høyer, and A. Tapp. Quantum algorithm for the collision

problem. *ACM SIGACT News (Cryptology Column)*, 28:14–19, 1997. quant-ph/9705002.

[68] A. Broadbent and A. B. Grilo. QMA-hardness of consistency of local density matrices with applications to quantum zero-knowledge. In *Proceedings of 61st IEEE FOCS*, pages 196–205, 2020. arXiv:1911.07782.

[69] A. Broadbent and C. Schaffner. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78(1):351–382, 2016. arXiv:1510.06120.

[70] A. E. Brouwer and W. H. Haemers. *Spectra of Graphs*. Springer, 2012.

[71] N. H. Bshouty and J. C. Jackson. Learning DNF over the uniform distribution using a quantum example oracle. *SIAM Journal on Computing*, 28(3):1136—-1153, 1999. Earlier version in COLT'95.

[72] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf. Non-locality and communication com- plexity. *Reviews of Modern Physics*, 82:665–698, 2010. arXiv:0907.3584.

[73] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical ReviewLetters*, 87(16), September 26, 2001. quant-ph/0102001.

[74] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and com- putation. In *Proceedings of 30th ACM STOC*, pages 63–68, 1998. quant-ph/9802040.

[75] H. Buhrman and R. Špalek. Quantum verification of matrix products. In *Proceedings of 17th ACM-SIAM SODA*, pages 880–889, 2006. quant-ph/0409035.

[76] M. Bun and J. Thaler. Dual lower bounds for approximate degree and Markov-Bernstein inequalities. In *Proceedings of 40th ICALP*, volume 7965 of *Lecture Notes in Computer Science*, pages 303–314, 2013.

[77] Y. Cao, J. Romero, J. Olson, M. Degroote, P. Johnson, M. Kieferová, I. Kivlichan, T. Menke, B. Peropadre, N. Sawaya, S. Sim, L. Veis, and A. Aspuru-Guzik. Quantum chemistry in the age of quantum computing. *Chemical Reviews*, 119(19):10856–11091, 2019. arXiv:1812.09976.

[78] M. Cerezo, A. Arrasmith, R. Babbush, S. Benjamin, S. Endo, K. Fujii, J. McClean, K. Mi- tarai, X. Yuan, L. Cincio, and P. Coles. Variational quantum algorithms. *Nature Reviews Physics*, 1, 2021. arXiv:2012.09265.

[79] S. Chakraborty, A. Gilyén, and S. Jeffery. The power of block-encoded matrix powers: im- proved regression techniques via faster Hamiltonian simulation. In *Proceedings of 46th In- ternational Colloquium on Automata, Languages, and Programming*, volume 132 of *Leibniz International Proceedings in Informatics*, pages 33:1–33:14, 2019. arXiv:1804.01973.

[80] Y. Chen and R. de Wolf. Quantum algorithms and lower bounds for linear regression with norm constraints. arXiv:2110.13086, 2021.

[81] N-H. Chia, A. Gilyén, T. Li, H-H. Lin, E. Tang, and C. Wang. Sampling-based sublinear low- rank matrix arithmetic framework for dequantizing quantum machine learning. In *Proceedings of 52nd ACM STOC*, pages 387–400, 2020. arXiv:1910.06151.

[82] A. Childs. Lecture notes on quantum algorithms, 2017. Available at

https://cs.umd.edu/ ~amchilds/qa/.

[83] A. Childs, R. Kothari, and R. Somma. Quantum algorithm for systems of linear equa- tions with exponentially improved dependence on precision. *SIAM Journal on Computing*, 46(6):1920–1950, 2017. arXiv:1511.02306.

[84] A. M. Childs, D. Gosset, and Z. Webb. The Bose-Hubbard model is QMA-complete. *Theoryof Computing*, 11(20):491–603, 2015. arXiv:1311.3297.

[85] A. M. Childs, Y. Su, M. C. Tran, N. Wiebe, and S. Zhu. A theory of Trotter error. arXiv:1912.08854, 18 Dec 2019.

[86] B. S. Cirel'son. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[87] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[88] R. Cleve. The query complexity of order-finding. In *Proceedings of 15th IEEE Conference on Computational Complexity*, pages 54–59, 2000. quant-ph/9911124.

[89] R. Cleve and H. Buhrman. Substituting quantum entanglement for communication. *Physical Review A*, 56(2):1201–1204, 1997. quant-ph/9704026.

[90] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp. Quantum entanglement and the com- munication complexity of the inner product function. In *Proceedings of 1st NASA QCQC conference*, volume 1509 of *Lecture Notes in Computer Science*, pages 61–74. Springer, 1998. quant-ph/9708019.

[91] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. In *Proceedings of the Royal Society of London*, volume A454, pages 339–354, 1998. quant- ph/9708016.

[92] S. Cook. The complexity of theorem-proving procedures. In *Proceedings of 3rd ACM STOC*,pages 151—158, 1971.

[93] J. W. Cooley and J. W. Tukey. An algorithm for the machine calculation of complex Fourier series. *Mathematics of Computation*, 19(90):297–301, 1965.

[94] D. Coppersmith. An approximate Fourier transform useful in quantum factoring. IBM Research Report No. RC19642, quant-ph/0201067, 1994.

[95] A. Cornelissen. Quantum gradient estimation and its application to quantum reinforcement learning. Master's thesis, Delft University, 2018.

[96] W. van Dam. Quantum oracle interrogation: Getting all information for almost half the price. In *Proceedings of 39th IEEE FOCS*, pages 362–367, 1998. quant-ph/9805006.

[97] D. Deutsch. Quantum theory, the Church-Turing principle, and the universal quantum Turing machine. In *Proceedings of the Royal Society of London*, volume A400, pages 97–117, 1985.

[98] D. Deutsch. Quantum computational networks. In *Proceedings of the Royal Society of London*,volume A425, 1989.

[99] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. In

Proceedingsof the Royal Society of London, volume A439, pages 553–558, 1992.

[100] A. Drucker and R. de Wolf. Quantum proofs for classical theorems. *Theory of Computing*, 2011. ToC Library, Graduate Surveys 2. arXiv:0910.3376.

[101] V. Dunjko, J. Taylor, and H. Briegel. Advances in quantum reinforcement learning. *IEEE SMC*, pages 282–287, 2017. arXiv:1811.08676.

[102] C. Dürr, M. Heiligman, P. Høyer, and M. Mhalla. Quantum query complexity of some graph problems. *SIAM Journal on Computing*, 35(6):1310–1328, 2006. Earlier version in ICALP'04.quant-ph/0401091.

[103] C. Dürr and P. Høyer. A quantum algorithm for finding the minimum. quant-ph/9607014, 18 Jul 1996.

[104] K. Efremenko. 3-query locally decodable codes of subexponential length. In *Proceedings of 41st ACM STOC*, pages 39–44, 2009.

[105] H. Ehlich and K. Zeller. Schwankung von Polynomen zwischen Gitterpunkten. *Mathematische Zeitschrift*, 86:41–44, 1964.

[106] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

[107] P. van Emde Boas. Machine models and simulations. In van Leeuwen [239], pages 1–66.

[108] M. Ettinger, P. Høyer, and M. Knill. The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letters*, 91(1):43–48, 2004. quant-ph/0401083.

[109] E. Farhi, J. Goldstone, and S. Gutmann. A quantum approximate optimization algorithm. arXiv:1411.4028, 2014.

[110] O. Fawzi, A. Grospellier, and A. Leverrier. Constant overhead quantum fault-tolerance with quantum expander codes. In *Proceedings of 59th IEEE FOCS*, pages 743–754, 2018. arXiv:1808.03821.

[111] R. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6/7):467–488, 1982.

[112] R. Feynman. Quantum mechanical computers. *Optics News*, 11:11–20, 1985.

[113] L. Fortnow and J. Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999. Earlier version in Complexity'98. Also cs.CC/9811023.

[114] P. Frankl and V. Rödl. Forbidden intersections. *Transactions of the American Mathematical Society*, 300(1):259–286, 1987.

[115] R. Freivalds. Probabilistic machines can use less running time. In *Proceedings of 7th IFIP Congress*, pages 839–842, 1977.

[116] M. Fürer. Faster integer multiplication. *SIAM Journal on Computing*, 39(3):979–1005, 2009. Earlier version in STOC'07.

[117] M. Garey and D. Johnson. *Computers and Intractability : A Guide to the Theory of NP- completeness*. W. H. Freeman and Company, 1979.

[118] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf. Exponential separation for one-way quantum communication complexity, with applications to

cryptography. *SIAM Journal on Computing*, 38(5):1695–1708, 2008. Earlier version in STOC'07. quant-ph/0611209.

[119] S. Gharibian, Y. Huang, Z. Landau, and S. W. Shin. Quantum hamiltonian complexity. *Foundations and Trends in Theoretical Computer Science*, 10(3):159–282, 2015.

[120] A. Gilyén. *Quantum Singular Value Transformation & Its Algorithmic Applications*. PhD thesis, University of Amsterdam, 2018.

[121] A. Gilyén, S. Arunachalam, and N. Wiebe. Optimizing quantum optimization algorithms via faster quantum gradient computation. In *Proceedings of 30th ACM-SIAM SODA*, pages1425–1444, 2019. arXiv:1711.00465.

[122] A. Gilyén, Y. Su, G. H. Low, and N. Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of 51st ACM STOC*, pages 193–204, 2019. arXiv:1806.01838.

[123] D. Gottesman. An introduction to quantum error correction and fault-tolerant quantum computation. In *Quantum Information Science and Its Contributions to Mathematics, Pro- ceedings of Symposia in Applied Mathematics*, volume 68, pages 13–58, 2010. arXiv:0904.2557.

[124] M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani. Quantum mechanical algorithms for the nonabelian hidden subgroup problem. *Combinatorica*, 24(1):137–154, 2004. Earlier version in STOC'01.

[125] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of 28th ACM STOC*, pages 212–219, 1996. quant-ph/9605043.

[126] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yi. Sample-optimal tomography of quantum states. In *Proceedings of 48th ACM STOC*, pages 913–925, 2016. arXiv:1508.01797.

[127] L. Hales and S. Hallgren. An improved quantum Fourier transform algorithm and applica- tions. In *Proceedings of 41st IEEE FOCS*, pages 515–525, 2000.

[128] S. Hallgren. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. *Journal of the ACM*, 54(1):653–658, 2007. Earlier version in STOC'02.

[129] S. Hallgren, C. Moore, M. Roetteler, A. Russell, and P. Sen. Limitations of quantum coset states for graph isomorphism. *Journal of the ACM*, 57(6):34, 2010. Earlier version in STOC'06.

[130] S. Hallgren, A. Russell, and A. Ta-Shma. The hidden subgroup problem and quantum com- putation using group representations. *SIAM Journal on Computing*, 32(4):916–934, 2003. Earlier version in STOC'00.

[131] S. J. Hallgren. *Quantum Fourier Sampling, the Hidden Subgroup Problem, and Beyond*. PhDthesis, University of California, Berkeley, 2000.

[132] S. Hanneke. The optimal sample complexity of PAC learning. *Journal of Machine Learning Research*, 17(38):1–15, 2016. arXiv:1507.00473.

[133] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford UniversityPress, New York, fifth edition, 1979.

[134] A. Harrow, A. Hassidim, and S. Lloyd. Quantum algorithm for solving linear systems of equations. *Physical Review Letters*, 103(15):150502, 2009. arXiv:0811.3171.

[135] D. Harvey and J. van der Hoeven. Integer multiplication in time $O(n \log n)$. *Annals of Mathematics*, 193(2):563—617, 2021. Preprint hal-02070778 2019.

[136] J. Håstad. Some optimal inapproximability results. *Journal of the ACM*, 48(4):798–859, 2001. Earlier version in STOC'97.

[137] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Na- ture*, 526, 29 October 2015.

[138] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum commu- nication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973. English translation in *Problems of Information Transmission*, 9:177–183, 1973.

[139] P. Høyer, T. Lee, and R. Špalek. Negative weights make adversaries stronger. In *Proceedings of 39th ACM STOC*, pages 526–535, 2007. quant-ph/0611054.

[140] R. Impagliazzo and A. Wigderson. P = BPP if E requires exponential circuits: Derandomizing the XOR lemma. In *Proceedings of 29th ACM STOC*, pages 220–229, 1997.

[141] G. Ivanyos, F. Magniez, and M. Santha. Efficient quantum algorithms for some instances of the non-Abelian hidden subgroup problem. *International Journal of Foundations of Computer Science*, 14(5):723–740, 2003. Earlier version in SPAA'01. quant-ph/0102014.

[142] G. Ivanyos, L. Sanselme, and M. Santha. An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups. *Algorithmica*, 62(1–2):480–498, 2012. Earlier version in LATIN'08. arXiv:0707.1260.

[143] R. Jain, Z. Ji, S. Upadhyay, and J. Watrous. QIP = PSPACE. *Journal of the ACM*, 58(6):30:1–30:27, 2011. Earlier version in STOC'10. arXiv:0907.4737.

[144] D. Janzing, P. Wocjan, and T. Beth. Non-identity check is QMA-complete. *International Journal of Quantum Information*, 3(3):463–473, 2005. quant-ph/0305050.

[145] S. Jeffery, R. Kothari, and F. Magniez. Nested quantum walks with quantum data structures. In *Proceedings of 24th ACM-SIAM SODA*, pages 1474–1485, 2013. arXiv:1210.1199.

[146] S. Jordan. Fast quantum algorithm for numerical gradient estimation. *Physical Review Letters*, 95:050501, 2005. quant-ph/0405146.

[147] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Breaking symmetric cryptosys- tems using quantum period finding. In *Proceedings of CRYPTO'16, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 207–237, 2016. arXiv:1602.05973.

[148] J. Katz and L. Trevisan. On the efficiency of local decoding procedures for error-correcting codes. In *Proceedings of 32nd ACM STOC*, pages 80–86, 2000.

[149] J. Kempe, A. Yu. Kitaev, and O. Regev. The complexity of the local Hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006. Earlier version in FSTTCS'04. quant- ph/0406180.

[150] I. Kerenidis, J. Landman, A. Luongo, and A. Prakash. q-means: A quantum algorithm for unsupervised machine learning. In *Proceedings of the 33rd International Conference on Neural Information Processing Systems (NIPS'19), Paper 372*, page 4134–4144, 2019. arXiv:1812.03584.

[151] I. Kerenidis and A. Prakash. Quantum recommendation systems. In *Proceedings of 8th Innovations in Theoretical Computer Science Conference*, volume 67 of *Leibniz International Proceedings in Informatics*, pages 49:1–49:21, 2017. arXiv:1603.08675.

[152] I. Kerenidis and R. de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. *Journal of Computer and System Sciences*, 69(3):395–420, 2004. Earlier version in STOC'03. quant-ph/0208062.

[153] S. Kimmel, G. H. Low C. Lin, M. Ozols, and T. Yoder. Hamiltonian simulation with optimal sample complexity. *npj Quantum Information*, 3(13), 2017. arXiv:1608.00281.

[154] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of 32nd ACM STOC*, pages 608–617,2000.

[155] A. Yu. Kitaev. Quantum measurements and the Abelian stabilizer problem. quant-ph/9511026, 12 Nov 1995.

[156] A. Yu. Kitaev. Quantum NP, January 1999. Talk given at AQIP'99 conference, DePaul University, Chicago.

[157] B. Klartag and O. Regev. Quantum one-way communication is exponentially stronger than classical communication. In *Proceedings of 43rd ACM STOC*, 2011. arXiv:1009.3640.

[158] A. Klivans and D. van Melkebeek. Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses. *SIAM Journal on Computing*, 31(5):1501– 1526, 2002. Earlier version in STOC'99.

[159] M. Knill, R. Laflamme, and W. Zurek. Threshold accuracy for quantum computation. quant- ph/9610011, 15 Oct 1996.

[160] D. E. Knuth. *The Art of Computer Programming. Volume 2: Seminumerical Algorithms*. Addison-Wesley, third edition, 1997.

[161] C-Y. Lai and H-C. Cheng. Learning quantum circuits of some T gates. *IEEE Transactions on Information Theory*, 68(6):3951–3964, 2022. arXiv:2106.12524.

[162] F. Le Gall. Improved quantum algorithm for triangle finding via combinatorial arguments. In *Proceedings of 55th IEEE FOCS*, pages 216–225, 2014. arXiv:1407.0085.

[163] T. Lee, F. Magniez, and M. Santha. Improved quantum query algorithms for triangle finding and associativity testing. *Algorithmica*, 77(2):459–486, 2017. arXiv:1210.1014.

[164] T. Lee, R. Mittal, B. Reichardt, R. Špalek, and M. Szegedy. Quantum query complexity of state conversion. In *Proceedings of 52nd IEEE FOCS*, pages 344–353, 2011. arXiv:1011.3020.

[165] A. K. Lenstra and H. W. Lenstra, Jr. *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer, 1993.

[166] H. W. Lenstra, Jr. and C. Pomerance. A rigorous time bound for factoring integers. *Journalof the American Mathematical Society*, 5:483–516, 1992.

[167] L. Levin. Universal search problems (translated from the Russian). *Problems of Information Transmission*, 9(3):115—116, 1973.

[168] L. Lin. Lecture notes on quantum algorithms for scientific computation, 2022. arXiv:2201.08309.

[169] L. Lin and Y. Tong. Optimal quantum eigenstate filtering with application to solving quantum linear systems. arXiv:1910.14596, 31 Oct 2019.

[170] Y.-K. Liu. Consistency of local density matrices is QMA-complete. In *Proceedings of 10th International Workshop on Randomization and Computation (RANDOM 2006)*, volume 4110 of *Lecture Notes in Computer Science*, pages 438–449, 2006. quant-ph/0604166.

[171] Y.-K. Liu, M. Christandl, and F. Verstraete. Quantum computational complexity of the N- representability problem: QMA complete. *Physical Review Letters*, 98(110503), 2007. quant- ph/0609125.

[172] S. Lloyd. Universal quantum simulators. *Science*, 273:1073–1078, 1996.

[173] S. Lloyd, M. Mohseni, and P. Rebentrost. Quantum algorithms for supervised and unsuper- vised machine learning, 1 Jul 2013. arXiv:1307.0411.

[174] S. Lloyd, M. Mohseni, and P. Rebentrost. Quantum principal component analysis. *Nature Physics*, 10:631–633, 2013. arXiv:1307.0401.

[175] H-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarilylong distances. *Science*, 283:2050–2056, 1999. quant-ph/9803006.

[176] G. H. Low and I. L. Chuang. Hamiltonian simulation by uniform spectral amplification. arXiv:1707.05391, 17 Jul 2017.

[177] G. H. Low and I. L. Chuang. Hamiltonian simulation by qubitization. arXiv:1610.06546, 20 Oct 2016.

[178] G. H. Low and I. L. Chuang. Optimal Hamiltonian simulation by quantum signal processing. *Physical Review Letters*, 118(1):010501, 2017. arXiv:1606.02685.

[179] G. H. Low, T. J. Yoder, and I. L. Chuang. Methodology of resonant equiangular composite quantum gates. *Physical Review X*, 6(4):041067, 2016. arXiv:1603.03996.

[180] R. A. Low. Learning and testing algorithms for the Clifford group. *Physical Review A*, 80(052314), 2009. arXiv:0907.2833.

[181] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992. Earlier version in FOCS'90.

[182] F. Magniez, A. Nayak, J. Roland, and M. Santha. Search via quantum walk.

SIAM Journal on Computing, 40(1):142–164, 2011. Earlier version in STOC'07. quant-ph/0608026.

[183] F. Magniez, M. Santha, and M. Szegedy. Quantum algorithms for the triangle problem. In *Proceedings of 16th ACM-SIAM SODA*, pages 1109–1117, 2005. quant-ph/0310134.

[184] U. Mahadev. Classical verification of quantum computations. In *Proceedings of 59th IEEE FOCS*, pages 259–267, 2018. arXiv:1804.01082.

[185] Y. Manin. Vychislimoe i nevychislimoe (computable and noncomputable). *Soviet Radio*, pages 13–15, 1980. In Russian.

[186] Y. Manin. Classical computing, quantum computing, and Shor's factoring algorithm. quant- ph/9903008, 2 Mar 1999.

[187] C. Marriott and J. Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005. Earlier version in CCC'04. arXiv:cs/0506068.

[188] D. Mayers. Unconditional security in quantum cryptography. quant-ph/9802025, 10 Feb 1998.

[189] M. Mohri, A. Rostamizadeh, and A. Talwalkar. *Foundations of Machine Learning*. MIT Press, second edition, 2018.

[190] C. Moore, D. N. Rockmore, and A. Russell. Generic quantum Fourier transforms. *ACM Transactions on Algorithms*, 2(4):707–723, 2006. quant-ph/0304064.

[191] C. Moore, A. Russell, and L. Schulman. The symmetric group defies strong Fourier sampling. *SIAM Journal on Computing*, 37(6):1842–1864, 2008. quant-ph/0501056+66. Earlier version in FOCS'05.

[192] M. Mosca and A. Ekert. The hidden subgroup problem and eigenvalue estimation on aquantum computer. In *Proceedings of 1st NASA QCQC conference*, volume 1509 of *Lecture Notes in Computer Science*, pages 174–188. Springer, 1998. quant-ph/9903071.

[193] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of 40th IEEE FOCS*, pages 369–376, 1999. quant-ph/9904093.

[194] I. Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39(2):67–71, 1991.

[195] I. Newman and M. Szegedy. Public vs. private coin flips in one round communication games. In *Proceedings of 28th ACM STOC*, pages 561–570, 1996.

[196] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cam- bridge University Press, 2000.

[197] R. O'Donnell and J. Wright. Efficient quantum tomography. In *Proceedings of 48th ACM STOC*, pages 899–912, 2016. arXiv:1508.01907.

[198] C. H. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.

[199] A. Peruzzo, J. McClean, P. Shadbolt, M-H. Yung, X-Q. Zhou, P. Love, A. Aspuru-Guzik, and J. O'Brien. A variational eigenvalue solver on a photonic quantum processor. *Nature Communications*, 3:24, 2014.

[200] J. Preskill. Fault-tolerant quantum computation. In H-K. Lo, S. Popescu, and T. P. Spiller, editors, *Introduction to Quantum Computation*. World Scientific, 1998. quant-ph/9712048.

[201] J. Preskill. Quantum computing 40 years later. In A. Hey, editor, *Feynman Lectures on Computation*. Taylor & Francis Group, second edition, 2022. arXiv:2106.10522.

[202] A. Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya of the Russian Academy of Sciences, mathematics*, 67(1):159–176, 2003. quant-ph/0204025.

[203] P. Rebentrost, M. Mohseni, and S. Lloyd. Quantum support vector machine for big data classification. *Physical Review Letters*, 113(13):130503, 2014. arXiv:1307.0471.

[204] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):34:1–34:40, 2009. Earlier version in STOC'13.

[205] B. Reichardt. Span programs and quantum query complexity: The general adversary bound is nearly tight for every Boolean function. In *Proceedings of 50th IEEE FOCS*, pages 544–551,2009.

[206] B. Reichardt. Faster quantum algorithm for evaluating game trees. In *Proceedings of 22nd ACM-SIAM SODA*, pages 546–559, 2011. arXiv:0907.1623.

[207] B. Reichardt. Span programs are equivalent to quantum query algorithms. *SIAM Journalon Computing*, 43(3):1206–1219, 2014.

[208] B. Reichardt and R. Špalek. Span-program-based quantum algorithm for evaluating formulas. *Theory of Computing*, 8:291–319, 2012. Earlier version in STOC'08. arXiv:0710.2630.

[209] J. Riordan and C. E. Shannon. The number of two-terminal series-parallel networks. *Journalof Mathematics and Physics*, 21:83—93, 1942.

[210] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and publickey cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[211] R. L. Rivest. Cryptography. In van Leeuwen [239], pages 717–755.

[212] T. J. Rivlin and E. W. Cheney. A comparison of uniform approximations on an interval and a finite subset thereof. *SIAM Journal on Numerical Analysis*, 3(2):311–320, 1966.

[213] S. Saeedi and T. Arodz. Quantum sparse support vector machines, 2019. arXiv:1902.01879.

[214] S. Saeedi, A. Panahi, and T. Arodz. Quantum semi-supervised kernel learning. *Quantum Machine Intelligence*, 3:24, 2021.

[215] M. Saks and A. Wigderson. Probabilistic Boolean decision trees and the complexity of eval- uating game trees. In *Proceedings of 27th IEEE FOCS*, pages 29–38, 1986.

[216] M. Santha. Quantum walk based search algorithms. In *Proceedings of 5th TAMC*, pages 31–46, 2008. arXiv/0808.0059.

[217] T. Santoli and C. Schaffner. Using Simon's algorithm to attack symmetric-key cryptographic primitives. *Quantum Information and Computation*, 17(1& 2):65–78, 2017. arXiv:1603.07856.

[218] A. Schönhage and V. Strassen. Schnelle Multiplikation grosser Zahlen. *Computing*, 7:281–292, 1971.

ABOUT THE AUTHORS

Dr Neha Gupta

Associate Professor

SCSIT, Symbiosis University of Applied Sciences Indore

Dr Pankaj Kumar Mishra

Pro Vice Chancellor

Glocal University Mirzapur Pole UP

Dr. Rahul Kumar Budania

Assistant Professor and Head of the Electronics & Communication Engineering Department

Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan

ABOUT THE BOOK

"Quantum Computing: Bridging the Gap to the Future" explores the revolutionary landscape of quantum computing, delving into the heart of this cutting-edge technology that promises to transform the very fabric of our digital world. As the author, my aim is to demystify the complex realm of quantum computing, making it accessible to readers of all backgrounds. This book serves as a comprehensive guide, unraveling the enigma of quantum mechanics and its applications in computing. Through engaging narratives and real-world examples, readers embark on a captivating journey, understanding the fundamental principles of quantum computing, its underlying theories, and the potential it holds for solving problems deemed unsolvable by classical computers. From quantum bits (qubits) to quantum algorithms, the book navigates through the intricate concepts, illustrating the quantum phenomena that make this technology groundbreaking. Additionally, the book sheds light on the current state of quantum computing research, exploring the work of leading scientists and innovators in the field. It examines the challenges faced, the breakthroughs achieved, and the path ahead, outlining the implications of quantum computing for diverse sectors, from cryptography and cyber security to drug discovery and artificial intelligence. By bridging the gap between theoretical knowledge and practical applications, **"Quantum Computing: Bridging the Gap to the Future"** empowers readers to grasp the immense potential of quantum computing, inspiring curiosity and fostering a deep appreciation for the scientific advancements shaping our future. Whether you are a technology enthusiast, a student, or a professional in the field, this book offers a captivating and informative exploration of quantum computing, paving the way for a new era of innovation and discovery.

EMPYREAL PUBLISHING HOUSE

ISBN 978-81-965655-9-6

9 788196 565596

India | UAE | Nigeria | Uzbekistan | Montenegro | Iraq | Egypt | Thailand | Uganda | Philippines | Indonesia

Empyreal Publishing House || www.empyrealpublishinghouse.com || info@empyrealpublishinghouse.com