APPLICATIONS OF QUANTUM COMPUTING

Dr. Sangita Gupta, Associate Professor of Physics, Vaish College, Rohtak.

ABSTRACT

Quantum computing, an emerging field that harnesses the principles of quantum mechanics to perform complex computations, holds the promise of revolutionizing various industries and scientific domains. Its potential lies in its ability to exploit quantum phenomena such as superposition and entanglement, enabling it to solve certain problems exponentially faster than classical computers. One of the most significant applications of quantum computing is in cryptography, where it can break commonly used encryption algorithms and facilitate the development of quantum-resistant cryptographic methods. Additionally, quantum computing can significantly enhance optimization tasks, tackling challenges in supply chain management, financial modeling, and drug discovery by efficiently solving combinatorial and complex optimization problems. Moreover, quantum simulations can transform research in materials science, quantum chemistry, and particle physics, enabling the study of complex quantum systems beyond classical simulations. Furthermore, quantum machine learning offers potential advancements in pattern recognition, big data analysis, and artificial intelligence. While quantum computing is still in its infancy and faces considerable technological hurdles, its multifaceted applications hold the potential to reshape the technological landscape and drive innovations across various disciplines.

Keywords: *Quantum, Quantum Computing*

INTRODUCTION

The free flow of information and the reliability of those who protect it from possible dangers such as espionage and interference from other nations' governments are essential to the maintenance of civilized society. Before information that has been acquired and disseminated can be trusted, a variety of challenges and barriers must first be overcome. Non-repudiation, authenticity, covertness, copy-resistance, certification, authorization, and ownership protection are some examples of requirements for the efficient operation of society. Other requirements include non-repudiation and covertness. For regular social interaction to take place, the rules are necessary. Even though there are evident major parallels between these themes, it is possible to consider them as though they were separate criteria. They form the foundation of the discussion around encrypted communications when taken together. This book is built around the time-honored subject of cryptography, which also functions as the primary focus of this collection of essays. The sciences of communication and cryptography are both subfields of telecommunication and are strongly intertwined with one another. The practice of communicating thoughts and information with another person through spoken or written methods is referred to as communication. The very term "communication" conjures up thoughts of giving and receiving information openly and honestly, thus just thinking about it makes one feel more upbeat and helpful.

The verification of the message's origin is the primary purpose of the authentication process. It does not carry out the process of identifying the verification function, which is another name for the verification of the sender's identity. Using a digital signature that cannot be replicated is one method that may be utilized to give authentication. Cryptographic relationships can be created because of this necessity. Experts do study, devise, and deploy methods that fall under the category of cryptanalysis to attack and crack cryptosystems. The study of cryptography, its development, and its application are all necessities for the process of data encryption. Cryptanalysis and cryptography are two subfields that fall under the umbrella term of cryptology, which refers to the field of study. Many people who like the mental challenge of working through puzzles as a form of recreational cryptograms are already familiar with the fundamental concept behind a classical cryptosystem.

Public-key cryptography

Sending a secret key across an encrypted channel is the foundation of traditional cryptography, which is based on the idea. As things now stand, there is no method to prearrange the release of a secret key, which is a serious concern in many modern applications in which communication takes place over open public networks between people who have never met one another. The only way for these parties to speak with one another safely is if they first trade their keys over a public channel that is available to the whole public. This is conceivable and, in all honesty, rather common. To be more specific, the majority of industry experts agree that the procedure described in this chapter, which is now the one that is employed the most frequently for carrying out these actions, is risk-free. We think that it is conceivable for two parties to agree on a secret key, one that will be known only to them, through dialogues over a public channel while an opponent with adequate knowledge looks on. This will be known only to the two parties involved. We believe that this objective can be accomplished. The greatest anonymity that such a segment may offer is either computational or practical.

If someone has access to an infinite amount of processing power, they can simply crack them. A significant portion of this book is devoted to examining and refuting chapters that discuss how to carry out the activity in question. Only a one-time pad can ensure perfect secrecy or security, which was the foundation of early attempts to define the security provided by cryptography. Achieving complete secrecy or security is extremely difficult. In answer to the question "When is a cryptographic system computationally secure?" the field of cryptography has given rise to updated definitions that are more practical. Although computational security is the cornerstone of today's public-key cryptography, perfect secrecy is still seen as a more challenging and desirable criterion, and it is only very rarely achieved. Even if a system can pass the computational security test, it may do very poorly when measured against more stringent criteria.

The random number is added to the secret key, which brings it up to date, and the ciphertext is appended with the random number in its original, unencrypted form. This completes the encryption process. The random number that was created specifically to encrypt and decrypt the communication is mixed with the secret key that was utilized. Even though no fresh keys are ever traded, this method nonetheless encrypts each communication with its special key. This helps to obscure any repeating user actions even more. Even if the original key is the only place where the secret may be found, this strategy can still be used to counter some attacks. Likely, the most effective method for an opponent to defeat a modern cryptosystem would be to break into either the encryptor or the decrypt or at some point before or after the process of encryption or decryption, respectively, and read the plaintext directly. This would need the adversary to have access to the encryptor or the decrypt or at the appropriate time. This is because if the plaintext is exposed, the adversary will have an easier time reading it. No matter how securely you lock the front door, it won't matter if the windows are open and unlocked. An assessment of such susceptibility to an intruder is outside the purview of the current inquiry.

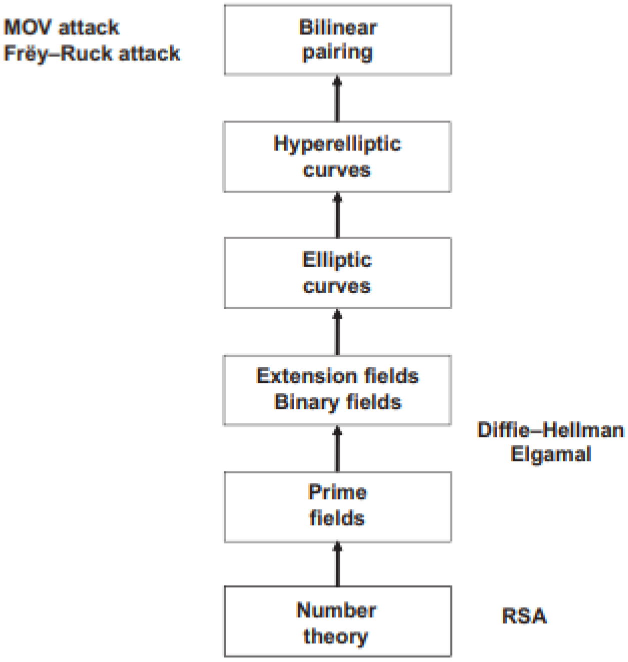


Figure 1 Mathematics in Cryptography

In conclusion, it is important to keep in mind that classical encryption, which is more common and relies on secret keys, cannot be replaced by public-key cryptography. Since public-key cryptosystems are often sluggish, and because of this, they are not ideally suited to bulk encryption, many applications make use of both secret-key and public-key cryptosystems. As a result, the primary purpose for which the public-key cryptography system is often use is for the generation of a key for the private-key cryptography system. This is because it is less difficult to crack the public-key system as opposed to the secret-key method.

QUANTUM SIMULATIONS FOR MATERIALS SCIENCE AND CHEMISTRY

Atomistic simulations, which are based on the solution of the fundamental equation of quantum mechanics, have played an increasingly important part in the prediction of the properties of functional materials over the past three decades. In the realm of materials for energy-related applications, such as catalysts and energy storage devices, quantum information science materials also have a place. The density functional theory (DFT), which is used in the majority of first-principles simulations, is accurate in theory but necessitates the use of approximations so that computations may be performed. This is especially true for materials that have a high degree of complexity as well as variety in their composition. Despite its great success in predicting many characteristics of solids, liquids, and molecules and affording important interpretations to a wide variety of experimental facts, density-functional theory (DFT) is frequently insufficient to define so-called strongly correlated electronic states. This is the case despite DFT's considerable success in predicting many features of solids, liquids, and molecules. The density-functional theory (DFT) has not only shown its value in correctly understanding a broad variety of experimental results, but it also enables several properties of solids, liquids, and molecules to be predicted with great precision.

The employment of a quantum computer to do computations on spin defects is the topic of this research, which claims an important discovery. We were able to investigate the strongly correlated electronic states of the NV center in diamond by employing a technique known as quantum phase estimation, which involved the utilization of variational quantum eigen solvers. According to the findings of our investigation, classical full configuration interaction (FCI) calculations agree with those derived from quantum simulations. The effective Hamiltonian that was developed by the quantum embedding theory served as the basis for our investigation, which allowed us to accomplish this goal. Our discoveries clear the path for the creation of quantum computers, which will make it possible to apply first-principles theories to the study of the characteristics of materials that are diverse.

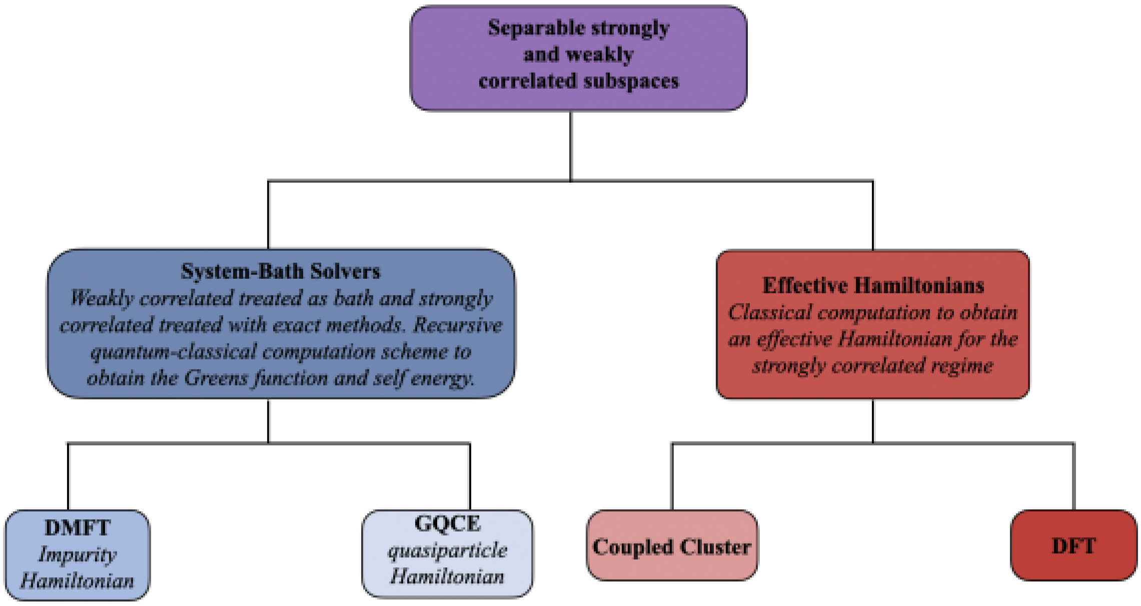

Separable strongly and weakly correlated subspaces
System-Bath Solvers
Weakly correlated treated as bath and strongly correlated treated with exact methods. Recursive quantum-classical computation scheme to obtain the Greens function and self energy.
Effective Hamiltonians
Classical computation to obtain an effective Hamiltonian for the strongly correlated regime
DMFT
Impurity Hamiltonian
GQCE
quasiparticle Hamiltonian
Coupled Cluster
DFT

Figure 2. Embedding Schemes for Hybrid Quantum-Classical Computation Of Materials.

(According to the definition), and because of this, it has the potential to be readily converted into a quantum circuit and carried out by a quantum computer. On the other hand, evolution may also be constructed with the aid of something called "imaginary time." Determining the value of this non-unitary operator, which may be beneficial in many circumstances, such as transitioning between the ground and excited states of a Hamiltonian system or creating thermal states, is how this is done. This operator may also be useful in other contexts as well. Since it is not possible to create non-unitary gates on the qubits of a quantum computer, an approximation of this operator needs to be accomplished by using the recently developed quantum imaginary time-evolution (QITE) approach. This technique may be found here. The QITE method makes perfect sense from a theoretical standpoint; nonetheless, several issues prevent it from being implemented on a large scale. The correlation length in the system must always be maintained at a level that is lower than the specified limit to avoid the algorithm from becoming inexecutable. The correlation length is used to establish the number of operators that need to be monitored to construct the QITE circuit. This number increases exponentially in proportion to the length of the correlation. Although raising the correlation length makes the QITE approximation more accurate, doing so also brings about an increase in the amount of overhead that must be incurred to generate the circuit. Through the utilization of symmetry, it is possible to cut down on the number of operators that need to be measured to produce the QITE.

The second problem of using QITE is that it frequently produces very big circuits that are incompatible with NISQ. This is the case because of how QITE works. While this is one approach for lowering circuit depths, many others have been detailed as well. The best chance for quantum processing to develop materials simulations is presented by highly correlated systems, for which perturbative techniques are unable to capture the correlation energy or the dynamical repercussions of those correlations. This presents the greatest promise for quantum processing. The portion of the system that is strongly correlated is typically small (and is typically the primary area of interest), while the remaining portion of the system is only weakly correlated. This is the case with many of the important materials. Calculations of a less exact kind are often adequate for describing the zone of low correlation, in contrast to the highly correlated region, which requires calculations of a very precise nature to be characterized. The goal of the quantum embedding theories is to combine these two levels of computing to accurately simulate a greater quantity of quantum materials using fewer computer resources. This will be possible if the theories are successful.

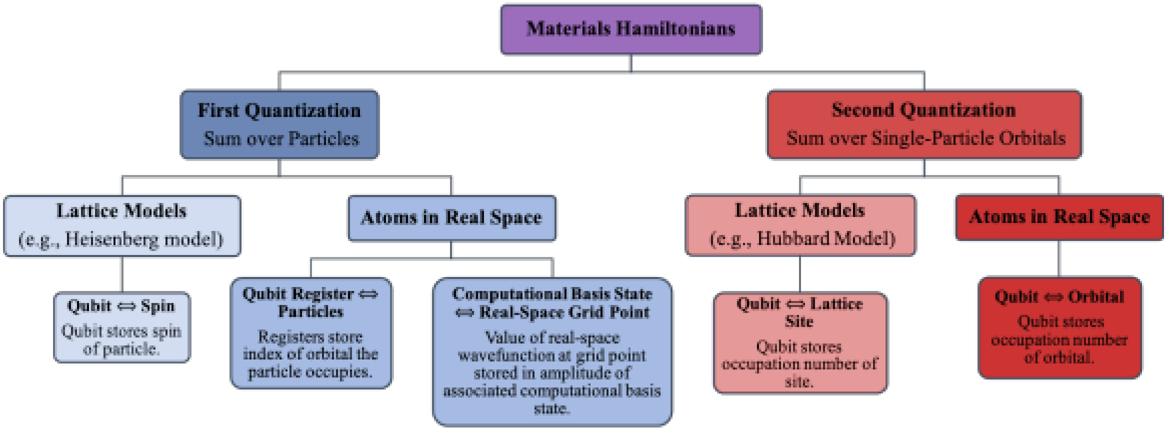

Materials Hamiltonians
First Quantization
Sum over Particles
Second Quantization
Sum over Single-Particle Orbitals
Lattice Models
(e.g., Heisenberg model)
Atoms in Real Space
Lattice Models
(e.g., Hubbard Model)
Atoms in Real Space
Qubit ⇔ Spin
Qubit stores spin of particle.
Qubit Register ⇔ Particles
Registers store index of orbital the particle occupies.
Computational Basis State ⇔ Real-Space Grid Point
Value of real-space wavefunction at grid point stored in amplitude of associated computational basis state.
Qubit ⇔ Lattice Site
Qubit stores occupation number of site.
Qubit ⇔ Orbital
Qubit stores occupation number of orbital.

Figure 3 Tree Diagram for Hamiltonians and Qubit Mappings That Have Been Used for Simulating Quantum Materials on Quantum Computers.

Quantum Information and Shor's Algorithm

Imagine there is a collection of n bits, and that each bit represents a traditional two-state system. You could explain it to me by saying.

$$b_1, b_2, \ldots b_n, \text{ ....(1)}$$

where bi = 0 or 1. Obviously, n classical bits of information can be stored in a single integer in the range (0, 2n).

The next thing that you need to do is think about n independent quantum two-state systems, sometimes known as qubits. The wave function of the entire system looks like this:

$$|\psi\rangle = a_1|0\ldots00\rangle + a_2|0\ldots01\rangle + a_3|0\ldots10\rangle + \ldots + a_k|1\ldots11\rangle. \text{ ....(2)}$$

For this system, you will need 2n complex numbers (minus two real numbers for the respective purposes of normalization and overall phase), so that you can describe any arbitrary state. This point exemplifies the primary distinction that can be seen between classical and quantum systems. As their sizes, n, get larger, quantum systems are able to store an exponentially greater amount of information than classical ones. Because obtaining information from a quantum system is a probabilistic process that lacks precision, putting this assumption into practice calls for a certain amount of leeway. However, in theory, a quantum computer with only 50 qubits might hold the same amount of information as the most powerful contemporary supercomputers. A similar quantum computer with 70 qubits may potentially store almost a million times as much information as its classical counterpart.

In theory, the promise of general-purpose quantum computers was first realized when Peter Shor suggested a method to use a limited set of gates on a digital quantum computer to factor numbers. This was the first step towards realizing the promise of general-purpose quantum computers. The reason for this was due to the scalability of quantum information. The general number field sieve (GNFS) is the factorization algorithm for classical computers that has received the most attention in recent years. Over time, there is a steadily increasing amount of it.

$$O\left(\exp\sqrt[3]{\frac{64}{9}b\,(\log b)^2}\right) \text{........(3)}$$

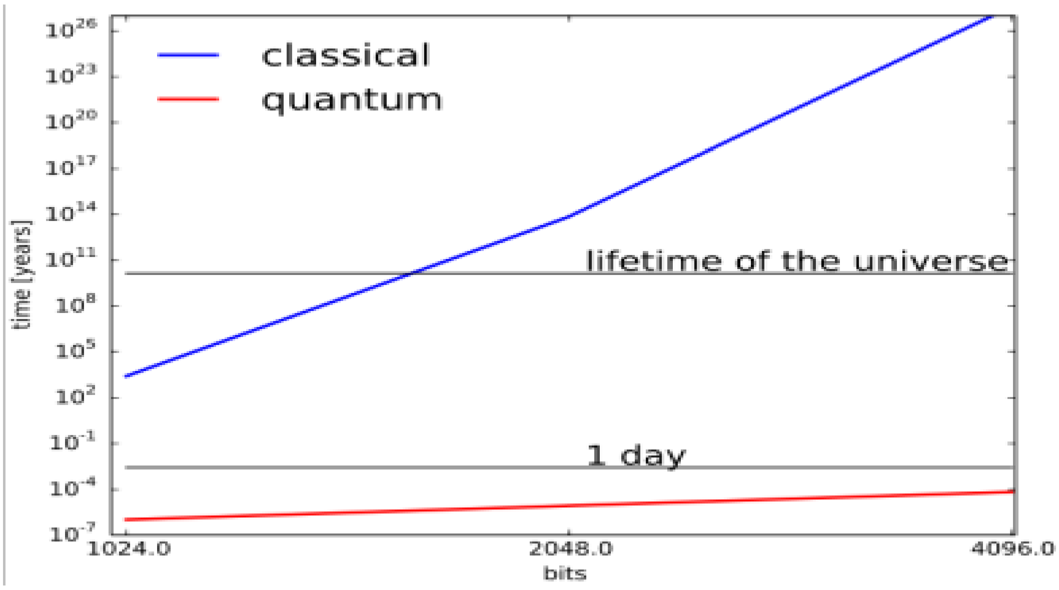


Figure 2. conventional and quantum algorithms to factor a number of size 2bits

Table 1. Shor's algorithm has high resource needs.

number size	1024 bits	2048 bits	4096 bits
qubits	5,124	10,244	20,484
gates	3×10^{10}	2×10^{11}	2×10^{12}

for factoring numbers of b bits. Shor's algorithm, on the other hand, scales as

$$O\left(b^2 \log b \log\log b\right), \text{..........(4)}$$

When compared to GNFS, the amount of time saved here is on the order of a super polynomial. Because there are currently no quantum computers that are in a position to factor large numbers utilizing Shor's algorithm, it is difficult to make a practical prediction of the speed at which the approach runs. On the other hand, if we are willing to make a few assumptions, we might be able to calculate how long it would take conventional computers and quantum computers, respectively, to factor an important number. The results of the calculations that were carried out are presented in Figure 4. The required quantum resources are shown in Table 1. The possibilities illustrated in Figure 4 are responsible for a significant portion of the excitement that has been generated by quantum computing. If a problem could be solved in less than a day when it would ordinarily take longer than the length of the universe to do it, this would have significant repercussions.

The following logical line of inquiry is to determine if or not there are further quantum algorithms that yield equivalent speedups over their classical analogues. The reality is that a good many of them have been discovered by this point. The pursuit of innovative quantum algorithms is an active area of research now. The "Quantum Algorithm Zoo" is a website that provides an overview of the most recent developments in the field of quantum computing.

Current and Near-term Hardware

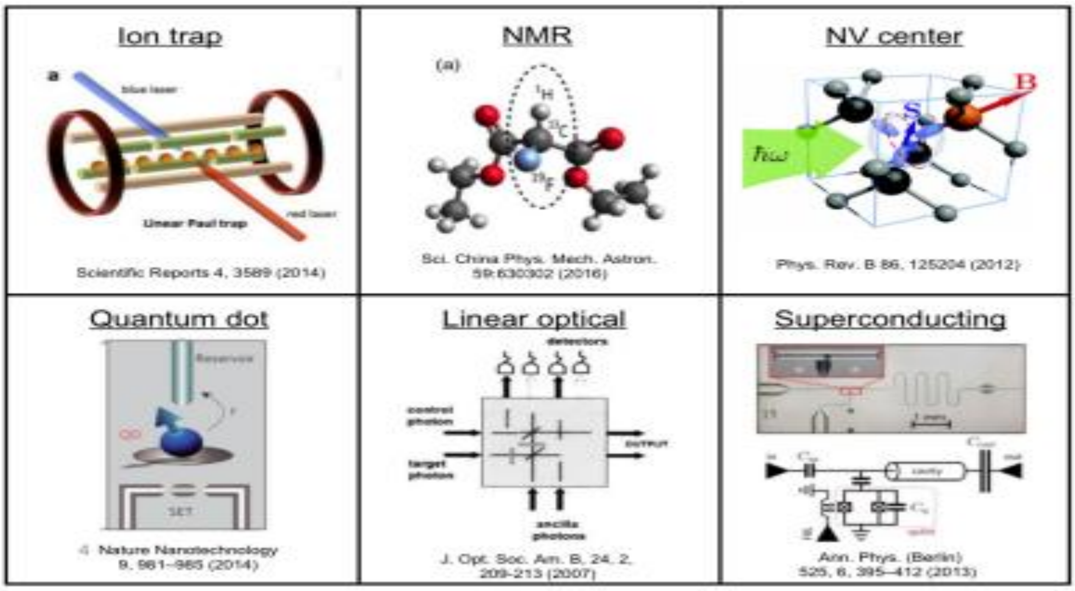

Ion trap
a
blue laser
Linear Paul trap
red laser
Scientific Reports 4, 3589 (2014)
NMR
(a)
1H
13C
19F
Sci. China Phys. Mech. Astron. 59:630302 (2016)
NV center
B
S
ħω
Phys. Rev. B 86, 125204 (2012)
Quantum dot
Reservoir
SET
Nature Nanotechnology 9, 981–985 (2014)
Linear optical
detectors
control photon
target photon
OUTPUT
ancilla photons
J. Opt. Soc. Am. B, 24, 2, 209-213 (2007)
Superconducting
1 mm
cavity
qubit
Ann. Phys. (Berlin) 525, 6, 395–412 (2013)

Figure 3. The study of qubit technology is ongoing. While superconducting qubits are the technology of choice right now, other methods still have a chance.

Multi-qubit systems are only just now starting to have their first significant realizations of their potential. study into possible quantum computer technology is illustrated in Figure 3, which shows a few examples of this study. As at the time that this article was written, Google, IBM, Intel, and Rigetti have all developed many-qubit machines that are based on superconducting technologies. IonQ is conducting research on ion-trap technology, however the company has not yet built a prototype that is operational. The range of eight to twenty-two qubits is now covered by devices that are made available to the public by Google, IBM, and Rigetti. Google, IBM, and Intel have all introduced machines with fifty qubits or more, and Google has also claimed that they would be releasing a computer with seventy qubits. These computer systems are not currently available to the public at this time.

Although progress is being made in the competition to expand qubit production, this is only one aspect of the whole picture. If we take a second look at Table 1, we can see that the best efforts that have been made so far are still a factor of 100–1000 away from the number of qubits that are required by Shor's method to factor enormous integers. However, the limitation that currently exists is the number of operations (gate count) that may be carried out on the qubits before the system loses both its coherence and its capacity for processing due to the presence of a variety of different types of noise. In real application, the number of gates that contemporary technologies can employ ranges anywhere from the low tens to the high hundreds. These requirements are substantially higher than what is needed for Shor's algorithm. Increasing the gate count will necessitate the use of quantum error correction, which is not yet feasible and would call for a system to include an extremely high number of qubits.

Quantum Efforts at Fermilab

There are four subfields of quantum science that are receiving consistent attention from researchers and developers at Fermilab. Quantum computing for high energy physics, quantum technology for high energy physics experiments, quantum networking, and HEP technology for quantum computing are these four areas of research. The final three points are important, but we won't get into them because they go beyond the scope of this article. In a nutshell, Fermilab implements superconducting RF technology to produce superior qubits and utilizes cutting-edge cold instrumentation electronics in order to collect data for usage in quantum information systems. Utilizing ultra-sensitive quantum technology that was initially developed for quantum computers, we are working on the development of a Matter-wave Atomic Gradiometer Interferometric Sensor (MAGIS-100) and a detector for Axion Dark Matter. Both projects are at the forefront of experimental high-energy physics. In the realm of quantum networking, our objective is to make it possible to transmit a quantum state over a distance equivalent to that which encompasses Chicago and its surrounding suburbs. The applications of quantum computing in high energy physics are the focus of all the quantum activities that take place at Fermilab, which we highlight in this article. These activities are either specifically designed to facilitate these applications or can do so. We have formed a partnership with Google to take advantage of Fermilab's HEPCloud effort to give users access to Google's current quantum computing test equipment. This will make it easier for HEP to carry out operations using quantum computing. Because of this endeavor, HEP physicists will be able to utilize the same interface for quantum computing workflows as they use for classical computing workflows. This will allow them to transition between the two types of computing more easily. The creation of quantum algorithms for high-energy physics is where most of our quantum efforts are currently being concentrated. The three key subjects that we have found thus far are optimization, machine learning, and quantum simulation.

There is currently a vibrant branch within the subject of quantum computing that is dedicated to applying quantum mechanics to solve optimization problems. Concerns pertaining to reconstruction and data analysis are relevant to HEP applications respectively. Researchers in high energy physics have developed a program called the Quantum Approximate Optimization Algorithm (QAOA), which is responsible for some of the most innovative work in the area. We are actively studying the usage of quantum optimization approaches by making advantage of the quantum technology that is already available. Quantum machine learning is yet another active area of research in the quantum world that has direct applicability to high-energy physics. Image processing in astrophysics and reconstruction in a wide variety of detector types are two examples of possible applications. To explore these uses, Fermilab is working along with other businesses, such as Lockheed Martin and Google. The idea of quantum computing was initially developed and tested within the context of the field of quantum simulation. This very concept was the focus of the Feynman quotation that appeared at the beginning of this article. Quantum computing seems like it would be a natural fit for simulating quantum systems, and it's not hard to understand how that could work. This area of research has been responsible for some of the most important and groundbreaking developments in quantum computing to date. Quantum algorithms for quantum chemistry have been developed to describe generic Hamiltonian problems including interactions between fermions. Given the importance of fermion-boson interactions to a wide variety of HEP issues, we have recently released two papers that extend our earlier work on fermion-fermion algorithms to consider these interactions as well. These papers are a result of our efforts.

Goals of Machine Learning Chapter

The development of general-purpose algorithms that may be applied in real-world settings is the fundamental objective of this machine learning component. It is anticipated that these algorithms would perform well. As is standard practice for computer scientists, one of our primary concerns is maximizing the efficiency with which both time and space are utilized. However, when it comes to learning, we also worry about another valuable resource, and that is the quantity of data that the learning algorithm requires. This is because knowledge being a limited resource makes it extremely valuable. In addition to this, it is recommended that learning algorithms be as general as is practically practicable. We are on the lookout for algorithmic methods that have the potential to be applied to a wide range of learning challenges, including the ones that have been discussed in the previous paragraphs. We place a high value on the fact that the learning process will provide a prediction rule that will produce results that are almost as close to perfect as can be achieved under the given conditions. The interpretability of the learnt prediction rules may be also an important factor in some circumstances. When we use the computer for things like medical diagnosis, one of the things we want it to be able to do is come up with prediction rules that are simple enough for human specialists to comprehend.

Considering what has been said so far, it is useful to think about machine learning as a type of "programming by example." Why should one choose machine learning over more conventional forms of programming? To begin, the results that can be reached using machine learning have the potential to be more exact than those that can be achieved via the use of direct programming. This is because the algorithms used in machine learning are data-driven and capable of processing vast volumes of information. On the other hand, human experts may have skewed perspectives since they have only researched a limited number of cases, which might lead to bias in their findings. Because humans are fallible and prone to making mistakes.

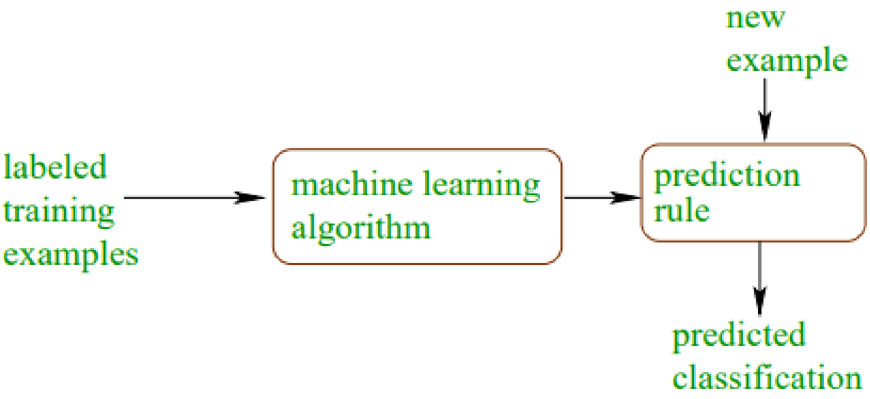
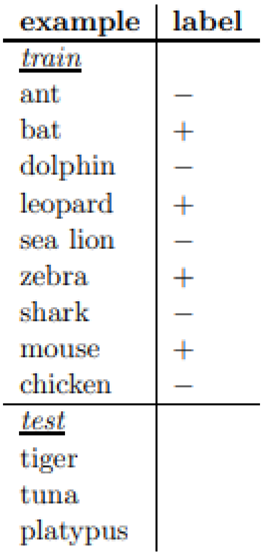


Figure 5: Diagram of A Typical Learning Problem.

Also, individuals often struggle to articulate what they know yet have little problem assigning names to what they encounter. For example, although it is simple for any of us to assign a name to a picture of a letter based on the person or thing that it depicts, we would have a hard time expressing how exactly we do this task using precise language.

The theoretical underpinnings of machine learning are the primary emphasis of this class. The aims of theoretical machine learning are essentially the same. We are still interested in developing algorithms for machine learning, but first, we want to study them mathematically to have a better understanding of how effective they are. It is intended that theoretical research may yield useful insights and intuitions, if not actual algorithms, that will be of assistance in the process of building practical algorithms. We have high hopes that theory will allow us to comprehend the inherent complexity of a particular learning challenge. In addition to this, we try to describe phenomena that were seen in real-world trials using learning algorithms. The study of mathematical models of machine learning, as well as the construction and analysis of machine learning algorithms, is the primary focus of this course.



example	label
train	
ant	−
bat	+
dolphin	−
leopard	+
sea lion	−
zebra	+
shark	−
mouse	+
chicken	−
test	
tiger	
tuna	
platypus	

Figure 6: A Tiny Learning Problem.

Consider the following subjects:

- The theoretical understanding of practical algorithms, including boosting and support vector machines.
- The required number of random examples for learning.
- Reinforcement Learning or Game Theory (Probably Not Time for Both)
- On-Line Learning from Non-Random Examples (Including Portfolio Selection)
- Estimating A Probability Distribution from Samples
- On-Line Learning from Non-Random Examples (Including Portfolio Selection)

The two computer science courses at Princeton that are most closely connected are 402 (which focuses on fundamental aspects of artificial intelligence) and 424 (which focuses on strategies for making efficient use of data, such as machine learning, statistics, and data mining). Both courses give a more comprehensive and general introduction to machine learning compared to 511, which focuses only on the theoretical aspects of machine learning. These courses are more comprehensive not just in terms of the subjects that are covered, but also in terms of the balance that is maintained between theory and applications.

CONCLUSION

In conclusion, quantum computing holds tremendous promise and potential to revolutionize various fields and industries. Its ability to harness the principles of quantum mechanics, such as superposition and entanglement, allows it to perform complex calculations and tasks exponentially faster than classical computers. One of the most exciting applications of quantum computing lies in cryptography, where it can break current encryption algorithms and offer more secure solutions. Additionally, quantum computing can significantly advance drug discovery and materials science by simulating molecular interactions and optimizing chemical processes. It also has the potential to transform optimization problems in logistics, finance, and transportation, leading to more efficient resource allocation and cost savings.

REFERENCES

1. Aspect, A. (2017). From Huygens' waves to Einstein's photons: weird light. ComptesRendus Physique, 18:498–503.
2. Bell, J. S. (1964). On the Einstein Podolsky Rosen paradox. Physics Physique Fizika, 1:195–200.
3. Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. Journal of Statistical Physics, 22:563–591.
4. Bernstein, E. S. and Vazirani, U. V. (1993). Quantum complexity theory. Proceedings of the twenty-fifth annual ACM symposium on Theory of Computing.
5. Bloch, F. (1946). Nuclear Induction. Phys. Rev., 70:460–474.
6. Born, M. (1926). ZurQuantenmechanik der Stovorg¨ange. Zeitschrift fur Physik, 37(12):863–867.
7. Burgisser, P. (2000). Completeness and Reduction in Algebraic Complexity Theory. Springer Berlin Heidelberg.

8. Clarke, J. and Wilhelm, F. K. (2008). Superconducting quantum bits. Nature, 453:1031–1042.
9. de Broglie, L. (1924). Recherches sur la th´eorie des Quanta. Theses, Migration - university'sandcourseaffectation.
10. Feynman, R. P. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21:467–488.
11. Fleisch, D. and Kinnaman, L. (2015). A Student's Guide to Waves. Student's Guides. Cambridge University Press.
12. Herbert, S. (2018). On the depth overhead incurred when running quantum algorithms on near-term quantum computers with limited qubit connectivity. Quantum Inf. Comput., 20:787–806.