A Study into the Development and  
Uses of Quantum Mechanics with Proposed  
Future Directions for Research

**Assessment number: J107790**

**INTRODUCTION**

The discovery of quantum physics by Max Planck and Niels Bohr in 1900 has changed physics as we know it. By applying the laws of quantum mechanics to computation, scientists have discovered the capabilities to improve communication protocols, create faster algorithms and novel cryptographic mechanisms (Rieffel & Polak, 2011). Quantum computing is a relatively new concept which uses the science behind quantum mechanics to vastly increase its capabilities in comparison to conventional computing. It is a physical system, much like conventional computing, but does not adhere to the rules of classical physics, but rather quantum physics (Adeh, 2018). Quoted from Rieffel and Polak (2011), “Quantum computing is not about changing the physical substrate on which computation is done from classical to quantum, but rather changing the notion of computation itself”. Conventional computing uses classical mechanics which extends from using macroscopic bodies, known as macrocosm, as opposed to quantum computing which uses quantum mechanics, known as microcosm (Sakho, 2019).

Rieffel & Polak (2011) states that quantum computing is a combination of quantum physics, quantum science and quantum information theory. Quantum computing uses quantum bits, also known as qubits, as opposed to the standard bits used in conventional computing (Gill et al, 2022). Conventional computing converts information to bits which represent the data as a 0 or 1, also known as binary, creating a string of binary values and uses integrated circuits to manipulate the binary information obtained to carry out everyday computing tasks such as processing text documents, the ability to generate or play videos and graphics, use of the internet and much more (Horowitz & Grumbling, 2019). Similarly to bits, qubits represent information as 0 or 1, but using the fundamental principle of superposition, qubits can be in a state where it is 0 and 1 at the same time. The superposition of these qubits allowing all possible binary states to be used is the advantage quantum computing has over conventional computing (Horowitz & Grumbling, 2019). This significant increase in computational power makes quantum computing more recourse- and time- efficient than conventional computing. It is anticipated that quantum computing, when fully developed, will help solve complex problems in a variety of fields including solution to complex algorithms, chemical development and quantum chemistry, secure communications, drug design, data science, clean energy and finance (Gill et al, 2022).

Quantum computation is one of three branches of the quantum information sciences, along with quantum communication and quantum sensing. All three of these fields are showing advancements at an accelerating rate due to advancements in one field providing information and insight into both other fields, rapidly advancing all three (Hidary, 2021).

Quantum physics as a whole is still in its infancy with very limited understanding thus far, meaning more research is needed before being able to use this field to carry out any form of quantum computation to its full potential (fingerhuth et al, 2018).

**FOUR PARADIGMS OF QUANTUM COMPUTING**

There are four proposed paradigms to quantum computing, the first being discrete variable gate-model quantum computing, or discrete gate model for short. This model is where qubits are used as a replacement for bits and logical transformations are used to solve (or approximate) arbitrary unitary operations (Fingerhuth et al, 2018).

The second paradigm is called continuous variable gate-model quantum computing, or continuous gate model for short. Rather than using qubits, this model uses qumods which can take in continuous vales and is conceptually follows the laws of quantum physics (in particular quantum optics) much closer than the other models (Fingerhuth et al, 2018).

The third paradigm is called adiabatic quantum computation which is a model primarily used by quantum annealing devices. This method is used to solve discrete optimization problems by utilizing the adiabatic theorem, which is able to find global optimums, and has proven to be particularly effective in sampling Boltzmann distributions (Fingerhuth et al, 2018).

The fourth and final paradigm is called quantum simulators which was the original reason for the theory of quantum mechanics proposed by Richard Feynman (Feynman, 1982). This model is used in application-specific devices and primarily used in the study of quantum main-body physics (Fingerhuth et al, 2018).

**USES OF QUANTUM COMPUTING**

In 2019, Google developed a quantum computer which utilised a fully programmable 54-qubit processor which was able to solve a sampling problem within 200 seconds. This would normally take a modern supercomputer close to 100,000 years to solve, proving the exponential speed at which quantum computers are able to computationally solve problems (Gururaj, 2023).

In 2022, a milestone in the development of the quantum internet was achieved by Alain Aspect, John Clauser and Anton Zeilinger as they demonstrated quantum enlargement which shows the ability of teleporting quantum information between photons (Gururaj, 2023). This allows the distribution of entanglement over greater distances and is a milestone in the development of the quantum internet (Brassard, 2023). Quantum teleportation gives rise to the possibility of the quantum internet being zero latency, a massive improvement to the internet as we know it (Rohde, 2021). Qubits are not able to be copied and is easily detected when attempted to do so, giving the quantum internet better security and protection (Rohde, 2021). The laws of quantum entanglement state qubits at remote nodes are correlated with each other at such a strength that no other qubit is able to entangle with these, because of a process called no-cloning, which further increases the potential security of the quantum internet (Singh et al, 2020).

Quantum computing poses a threat to anything that uses cryptography as a means to protect data for online security, vehicle security and medical devices (Bernstein & Lange, 2017). Quantum cryptography is the means of applying the laws of quantum mechanics to perform cryptographic tasks which also includes quantum money and randomness generation, as well as secure two- and multiparty computation and delegated quantum computation (Broadbent, 2016). Modern cryptography currently employs Shor’s algorithm which uses the multiplication of specific prime factors as a method of protection (Joseph et al, 2022). For the last 40 years, this method of encryption has been successful as even the most modern super computers would take up to 16 million years to decode Shor’s algorithm, quantum computers would be able to decode Shor’s algorithm within minutes (Joseph et al, 2022). The threat of the development of quantum computers for this reason is causing scientists to develop post-quantum cryptography which are methods of securing and protecting data from conventional and quantum computation (Bernstein & Lange, 2017).

Quantum information processing is a field which focuses on using the laws of quantum mechanics to model information and its processing. Quantum information can be split into quantum cryptography, quantum gaming and quantum communications (Rieffel & Polak, 2011). Quantum gaming is having an increasing effect on the framework for game theory, known as “quantizing the game”, and being implemented for a variety of gaming types including both non-cooperative and cooperative games (Faisal & Phoenix, 2012). Unlike classical communication, quantum communication has the potential to provide an error-free rate for the transmission of digital information (Mishra, 2016).

**LIMITATIONS OF QUANTUM COMPUTING**

The rules of the quantum world make is difficult to implement many of the features talked about so far as they do not follow the laws of conventional physics (Horowitz & Grumbling, 2019). Little is known about the laws of the quantum world which makes applying it to computation very difficult, so much research needs to be conducted in this field before it can be implemented. There are several factors, both theoretically and physically that are holding back the field of quantum computing and preventing the systems from being implemented to their full capability.

Qubit decoherence, or environment-induced decoherence, is where the qubits lose their coherent properties by entanglement with factors from their environment (Camilleri, 2009). The science to isolate quantum systems from their environment is yet to be developed (if possible) and therefore removing decoherence is a large limiting factor for the development of quantum systems (Schlosshauer, 2019). This removes any advantage qubits had to bits as the qubits will decohere to classical bits (Gill et al, 2022).

A factor called quantum noise also limits the capabilities of quantum systems that limits the size of the qubit circuits that can be produced while still producing reliable computations (Preskill, 2018). Examples of factors which cause noise are changes in temperature and stray electric or magnetic fields which can cause degradation of the quantum information (Preskill, 2012). The greater the number of qubits used in the circuits, the greater the noise which makes the system less functional (Xue et al, 2021).

The connectivity between qubits is proving to be problematic. The sparsely connected qubits in current quantum systems require inter-qubit interactions via direct coupling, making the mapping of large depth quantum circuits non-trivial (Gill et al, 2022).

Another hardware issue quantum systems have is the multiple sources of single photons required within the circuits (Tsimvrakidis et al, 2024). In order to achieve quantum supremacy, this being evidence that quantum computing can solve problems faster than any classical computer (Preskill, 2012), circuits will require an incredibly large number of qubits. Producing single photons on a micro level within a quantum system requires precise technology and a large amount of energy which is not yet viable for industrial production (Tsimvrakidis et al, 2024).

Due to the sensitivity of quantum systems, they require error-correction schemes, also known as fault-tolerant quantum computing, to minimize the errors made on calculations. The more error-correction the system needs, the more resources the system requires to meet the demand, such as the size of the system and the electrical power, but more importantly it has been found the more fault-tolerant quantum computing is used, the higher the probability of introducing more errors than it removes (Fellous-Asiani et al, 2021).

**NEW DIRECTIONS FOR RESEARCH**

Quantum physics is a relatively new field with a vast amount still unknown about it. The full extent of quantum computation is still yet to be determined with more applications being theorised and developed as more is discovered about quantum rules (Rieffel & Polak, 2011). Advancements made in any of the quantum fields of research will undoubtedly accelerate the progress in the other quantum fields which is why this field is advancing at a rapid rate.

It is anticipated that quantum computing, when fully developed, will help solve complex problems in a variety of fields including solution to complex algorithms, chemical development and quantum chemistry, secure communications, drug design, data science, clean energy and finance (Gill et al, 2022). As discussed earlier, this has the potential to break encryption as we know it and could be used as a means of obtaining data illegally, therefore methods of quantum encryption must be developed before the development of quantum computers.

As discussed earlier, one of the most anticipated uses of quantum computing is to be able to solve complex algorithms quickly which conventional computers are unable to but is being held back by decoherence and the noise effect from the environment on qubits. Once a method for mitigating noise is developed, it will be possible to implement non-linear optical interactions to use quantum logic gates to help solve these algorithms (Ralph, 2015).

Quantum computing is highly anticipated for its use in quantum simulations, particularly when studying chemical structures. Even though it is not currently possible to use quantum computing in this field, it is anticipated to be able to predict the properties of chemical structures such as folding or chemical interactions (Motta & Rice, 2021), as well as deepen our understanding of molecular biology, such as our understanding of how enzymes work on a chemical level and a means to develop and synthesise new drugs for medicinal use (Stojevic, 2024). These are just a few up-coming fields of interest and the potential for quantum computing in chemistry is limitless.

Due to the nature of a relatively new and undiscovered field such as quantum physics, the applications for this to be used in quantum computing are immensely great as new discoveries are made and their applications to be found, too many to list within this review. The ability for quantum computing to be used across the majority of scientific fields gives it an incredibly large scope of study with endless limitations.

**CONCLUSION**

Quantum computing is an exciting and relatively unknown field with an endless potential of applications. The difficulty this field faces is how little that is currently understood about the laws of the quantum world and how to overcome issues that arise from this micro world such as decoherence and noise. Quantum computing is anticipated to have a major impact on several fields when it is fully understood and developed, in particular in the fields of secure communication, complex algorithm solutions, understanding quantum mechanics, understanding chemical properties and synthesis, and so much more. Much research needs to be done in several quantum fields before applications can be used industrially and commercially, but advancements are being made at a rapid pace as seen by Google’s quantum computer of 2019 and the advancements made towards the quantum internet by Alain Aspect, John Clauser and Anton Zeilinger.

As it currently stands, quantum computing does not give any significant advantage over conventional computing due to its limitations and potential undiscovered limitations (Rieffel & Polak, 2011), but does have the potential to become a world-changing technological advancement with its anticipated applications in so many different fields of study.

**REFERENCES**

Adeh, F. F. A. (2018). Natural Limitations of Quantum  
 Computing. *International Journal of Swarm  
 Intelligence and Evolutionary Computation,* 6(1)

Bernstein, D. J., & Lange, T. (2017). Post-quantum  
 cryptography. *Springer Nature,* 549(7651), 188  
 194

Brassard, G. (2023). Profile of John Clauser, Alain Aspect  
 and Anton Zeilinger: 2022 Nobel laureates in  
 Physics. *National Library of Medicine,* 120(23)

Broadbent, A. (2016). Quantum cryptography beyond  
 quantum key distribution. *Designs, codes, and  
 cryptography,* 78(1), 351-382

Camilleri, K. (2009). A history of entanglement:  
 Decoherence and the interpretation problem.  
 *Science Direct,* 40(4), 290-302

Faisal, S. K., & Phoenix, S. J., D. (2012). *Gaming the  
 Quantum.* Cornell University Library

Fellous-Asiani, M., Chai, J. H., Whitney, R., Auffeves, A.,  
 & Ng, H. K. (2021). Limitations in Quantum  
 Computing from Resource Constraints. *PRX  
 Quantum,* 2(4), 040335

Feynmann, R. (1982). Simulating physics with computers.  
 *International Journal of Theoretical Physics,* 21(67), 467-488

Fingerhuth, M., Babej, T., & Wittek, P. (2018). Open source  
 software in quantum computing. *PLOS ONE,* 13(12), e0208561

Gill, F., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman,  
 M., & Buyya, R. (2022). Quantum computing: A  
 Taxonomy, Systematic Review and Future  
 Directions. *Software, practice & experience*, 52(1)

Gururaj, T. (2023). *The 5 most significant breakthroughs in  
 quantum computing...................................................* www.interestingengineering.com/science/5  
 breakthroughs-in-quantum-computing

Hidary, J. (2021). *Quantum Computing: An Applied  
 Approach.* Springer

Horowitz, M., & Grumbling, E. (2019). *Quantum  
 Computing: Progress and Prospects.* National  
 Academies Pres

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga,  
 F. D., Lacombe, O., Leichenauer, S., Hidary, J.,  
 Venables, P., & Hansen, R. (2022). Transitioning  
 organizations to post-quantum cryptography.  
 *Springer Nature,* 605(7909), 237-243

Mishra, V. K. (2016). *An Introduction to Quantum  
 Communication.* Momentum Press

Motta, M., & Rice, J. E. (2021). Emerging quantum  
 computing algorithms for quantum chemistry.  
 *WIRES Computational Molecular Science*, 12(3),  
 1580

Preskill, J. (2012). Quantum computing and the  
 entanglement frontier. *arXiv: 1203.5813*

Preskill, J. (2018). Quantum Computing in the NISQ era  
 and beyond. *arXiv,* 2(2), 79

Ralph, T. C. (2015). New directions in optical quantum  
 computing. *IEEE Xplore.*

Rieffel, E., & Polak, W. (2011). *Quantum Computing: A  
 Gentle Introduction.* MIT Press

Rohde, P. (2021). *The Quantum Internet: The Second  
 Quantum Revolution.* Cambridge University Press

Sakho, I. (2019). *Introduction to Quantum Mechanics 1:  
 Thermal Radiation and Experimental Facts  
 Regarding the Quantization of Matter.* John Wiley  
 & Sons, Incorporated

Schlosshauer, M. (2019). Quantum decoherence. *Science  
 Direct,* 831, 1-57

Singh, A., Dev, K., Siljak, H., Joshi, H. D., & Magarini, M.  
 (2020). Quantum Internet – Applications,  
 Functionalities, Enabling Technologies,  
 Challenges, and Research Directions. *IEEE  
 Journals & Magazine*, 23(4), 2218-2247

Stojevic, V. (2024). HOW QUANTUM COMPUTING  
 UNLOCKS THE SECRETS OF ENZYME  
 INHIBITION. *Europa Science, LTD.,* 16+

Tsimvrakidis, K., Tsintzos, S., Gates, J., Smith, P., Elshaari,  
 A., Zwiller, V., & Riziotis, C. (2024). Nanowire  
 integrated optical circuits: Limitations and  
 challenges towards quantum computing. *Optics &  
 Laser Technology,* 170, 110276

Xue, C., Chen, Z., Wu, Y., Guo, G. (2021). Effects of  
 Quantum Noise on Quantum Approximate  
 Optimization Algorithm. *Chinese Physics Letters,* 38(3), 030302