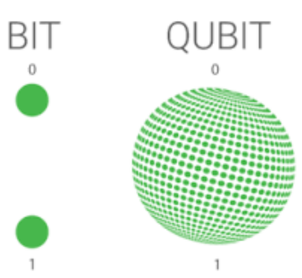
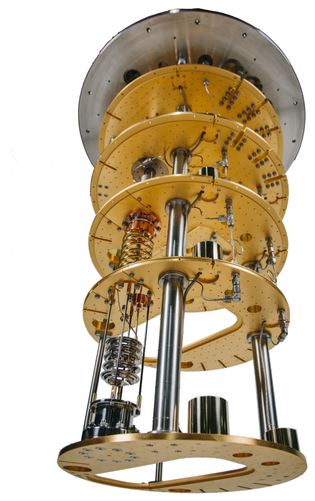


Quantum Computing and Looking into the Future with Shor's Algorithm

Researcher: Yashasvi Asuru, Mentor: Mohsen Heidari Khoozani
Indiana University Bloomington UROC Fall '22 Research



Abstract

Quantum Computing is is a topic that has seen a lot of development primarily because it has interesting applications for the future. It is the area of Computer Science that utilizes Quantum Theory and unlike classical computers that use bits of 0s and 1s that only have two states, Quantum Computing uses "qubits" which allow particles to exist in more than one states at the same time. This introduces many possibilities of what Quantum Computers can achieve and gives us access to exponential computing power compared to current classical computers. One application that gives us a glimpse of what the future of Quantum Computing looks like is cracking RSA encryption which is the most common form of secure encryption today used for messaging. Shor's Algorithm is a Quantum algorithm that cracks this encryption in polynomial time and is currently the only way to crack this form of encryption. This algorithm is one of the few simple algorithms that illustrate the applications of Quantum Computing since it can be simulated using classical computers, which is what was done in this research using Python and the Qiskit Library.

Results

	Register Output	Phase
0	11000000(bin) = 192(dec)	192/256 = 0.75
1	10000000(bin) = 128(dec)	128/256 = 0.50
2	01000000(bin) = 64(dec)	64/256 = 0.25
3	00000000(bin) = 0(dec)	0/256 = 0.00

	Phase	Fraction	Guess for r	P	Q
0	0.75	3/4	4	3	5
1	0.50	1/2	2	3	1
2	0.25	1/4	4	3	5
3	0.00	0/1	1	15	1

The above images are the results after taking the phase states and converting them into decimal numbers that we can use to find the period value (r value) and subsequently, the two factors (P and Q).

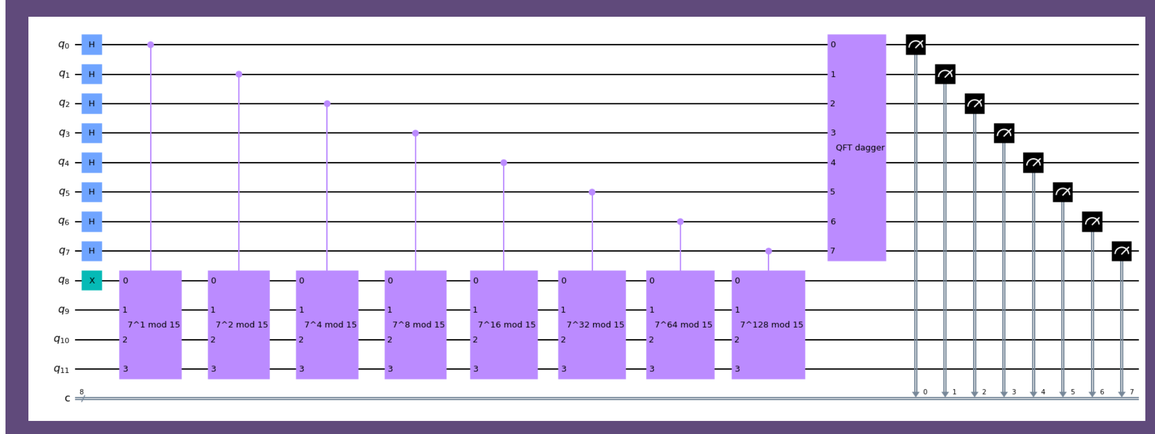
Since our input number was 15, our factors should be 3 and 5 to be correct and phases 0.75 and 0.25 give us factors of 3 and 5 with the period value being 4.

One important factor to note about using Shor's Algorithm is that because Quantum is probabilistic, its success rate is not 100%. This means that we could have period values that may give us the wrong factors which is why the algorithm must be run many times for it to be accurate.

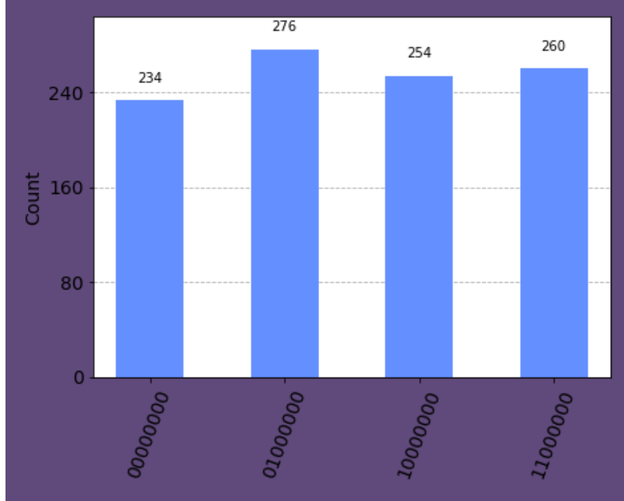
Methodology

The general outline of this project was to create a Quantum Circuit that can run Shor's Algorithm given an input. Shor's Algorithm is an algorithm that finds the factors of an integer in polynomial time and is broken into three main parts:

1) Converting the factoring problem into a period finding problem with Modular Exponentiation Function
2) Find period of Modular Exponentiation Function using a Quantum Fourier Transform
3) Use resulting period value to compute the original factors of the given input number.



The above image shows what the Quantum circuit looks like when ran and this specific circuit was designed with the input value of 15.



The Histogram to the left represents the 4 phase states that are tested, and the bars represents the number of counts for each state signifying the probabilities for each state likely being the correct period value we are looking for.

Conclusion

Shor's Algorithm provides a look into what Quantum Computing is capable in the future. While the simulation of Shor's Algorithm with smaller numbers is not practical since we can easily figure out factors of small integers, think about real Quantum computers using this algorithm to figure out the factors of numbers that are larger than classical computers can compute. Being able to harness computational power to that degree can change what the standard of modern computers look like in the future. It can help increase security of our online infrastructures, perform resource simulations, and even make the transferring of data exponentially faster.

The future iterations of this simulation would be to look into how the degree of qubits used in the circuit change the efficiency as well as looking into the current limit of digits that can be used for testing.

Acknowledgements

1."Shor's Algorithm." *IBM Quantum*, https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm.
2. Shor, P. W. (1995). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *arXiv*. https://doi.org/10.1137/S0097539795293172