University of Minho
School of Engineering

Quantum Algorithms and Applications

Leander Reascos

Quantum Computing School @ Yachay

November 14, 2023

Contents

1. Shor's Algorithm
2. Grover's Algorithm
3. Complexity Theory
4. Cryptography

Factoring

What are the prime factors of

$$p \cdot q = 21606371083676 3057$$

Factoring

$$p = 225865261$$

$$q = 956604437$$

Shor's Algorithm

Shor's Algorithm

- Shor's algorithm is a quantum algorithm for integer factorization.
- It was invented in 1994 by Peter Shor.
- It solves the following problem in polynomial time:

$$a^r \equiv 1 \pmod{N} \tag{1}$$

- Where N is a composite number and $2 \leq a < N$ is a random integer.

Shor's Algorithm

Find r such that $a^r \equiv 1 \pmod{N}$

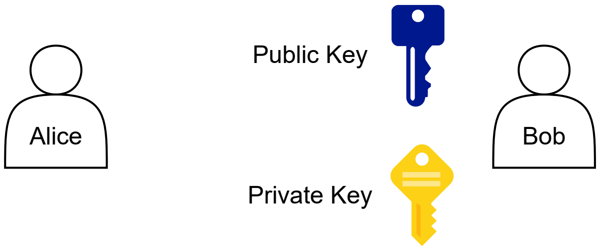
$$\frac{N}{a^r - 1} = \frac{N}{\left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right)} \tag{2}$$

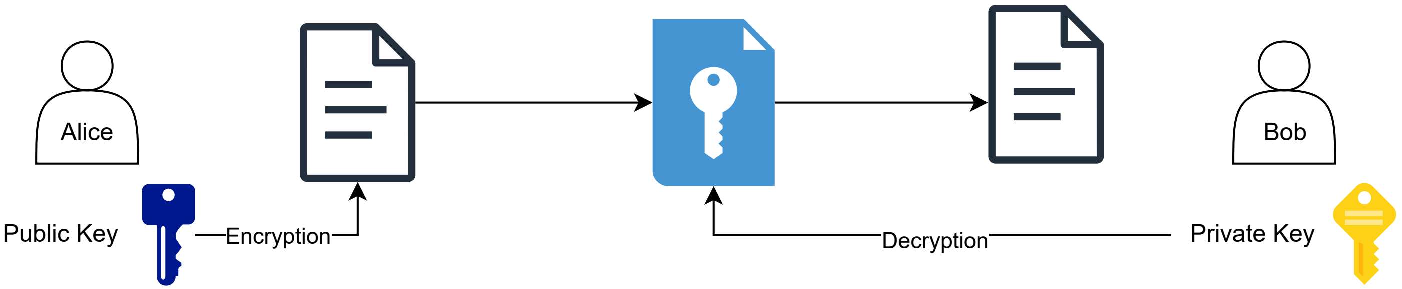
Implications

- Shor's algorithm can be used to break RSA encryption.
- It can also be used to solve the discrete logarithm problem.
- It can be used to solve the hidden subgroup problem.

RSA Protocol

RSA encryption is based on the difficulty of factoring large integers (2048 bits - 600 decimal digits).





NISQ Era

John Preskill coined the term Noisy Intermediate-Scale Quantum (NISQ) in 2017.

- NISQ computers are quantum computers with 50-100 qubits.
- They are noisy and have a short coherence time.
- They are not powerful enough to run Shor's algorithm.
- They can be used to run variational quantum algorithms.

Grover's Algorithm

Grover's Algorithm

- Grovers algorithm is a quantum search algorithm.
- It was invented in 1996 by Lov Grover.
- It solves the following problem in polynomial time:

$$f(x) = 1 \tag{3}$$

- Where f is a function that takes n-bit strings as input and returns a single bit.

Grover Operator

Let's define the Grover operator G as follows:

$$G \equiv U_d U_f \tag{4}$$

where,

$$U_f \left|x\right\rangle = (-1)^{f(x)} \left|x\right\rangle \quad \text{Oracle} \tag{5}$$

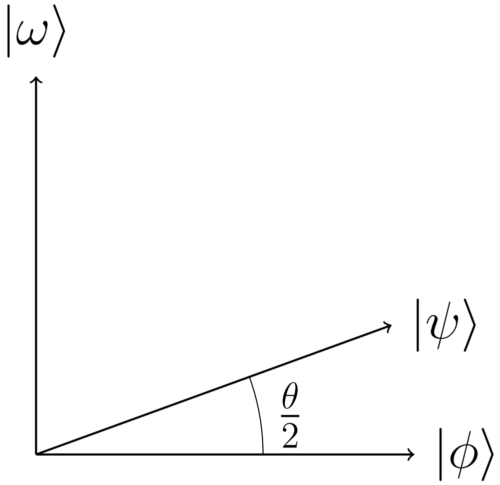
U_d Diffusion Operator

$$U_d = 2 \left|\psi\right\rangle \left\langle\psi\right| - I \tag{6}$$

where,

$$\left|\psi\right\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \left|x\right\rangle \tag{7}$$

Geometry of Grover's Algorithm

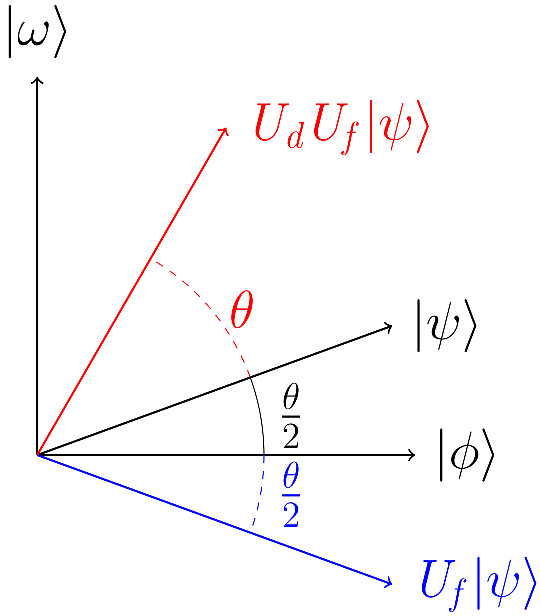


$$|\psi\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}|\phi\rangle + \frac{1}{\sqrt{N}}|\omega\rangle \tag{8}$$

$$|\phi\rangle = \frac{1}{\sqrt{N-1}}\sum_{x\neq\omega}|x\rangle \tag{9}$$

$$|\psi\rangle = \cos\frac{\theta}{2}|\phi\rangle + \sin\frac{\theta}{2}|\omega\rangle \tag{10}$$

Geometry of Grover's Algorithm



$$U_f |\psi\rangle = \cos\frac{\theta}{2}|\phi\rangle - \sin\frac{\theta}{2}|\omega\rangle$$

$$U_d U_f |\psi\rangle = \cos\left(\frac{\theta}{2}+\theta\right)|\phi\rangle + \sin\left(\frac{\theta}{2}+\theta\right)|\omega\rangle$$

Grover Iterator

The Grover iterator G is defined as follows:

$$G = U_d U_f \tag{11}$$

Each iteration of G increases the angle $\frac{\theta}{2}$ by θ.

$$G^k |\psi\rangle = \cos\left(\frac{\theta}{2} + k\theta\right)|\phi\rangle + \sin\left(\frac{\theta}{2} + k\theta\right)|\omega\rangle \tag{12}$$

The number of iterations required to find the solution is $k \leq \frac{\pi}{4}\sqrt{N}$.

Implications

- Cryptography
- Golberg's Conjecture
- Amplitude Amplification

Complexity Theory

Complexity Theory

- **P**: Problems that can be solved in polynomial time.
- **NP**: Problems that can be verified in polynomial time.
- **BQP**: Problems that can be solved in polynomial time by a quantum computer.

Note: The Godel's incompleteness theorem states that there are problems that cannot be solved by any computer.

Cryptography

Cryptography

- **Cryptography** is the study of techniques for secure communication in the presence of third parties.
- **Classical Cryptography** is based on the difficulty of solving mathematical problems.
- **Quantum Cryptography** is based on the laws of quantum mechanics.

Quantum Cryptography

- Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks.
- The best known example of quantum cryptography is **quantum key distribution** which offers an information-theoretically secure solution to the key exchange problem.

Post-Quantum Cryptography

- **Post-quantum cryptography** refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against an attack by a quantum computer. (Dilithium)
- **Quantum-resistant** algorithms are designed to be secure against both quantum and classical computers.

Quantum Internet

- The **quantum internet** is a network that will let quantum devices exchange some information within an environment that harnesses quantum mechanics' weird properties.
- The quantum internet will be used to distribute quantum keys.

Discussion

References I

[1] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

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

[3] A. Aikata, A. C. Mert, M. Imran, S. Pagliarini, and S. S. Roy, "Kali: A crystal for post-quantum security using kyber and dilithium," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 70, no. 2, pp. 747–758, 2022.

[4] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.

References II

[5] S. Lloyd, "Universal quantum simulators," *Science*, vol. 273, no. 5278, pp. 1073–1078, Aug. 23, 1996, ISSN: 0036-8075, 1095-9203. DOI: 10.1126/science.273.5278.1073. [Online]. Available: https://www.science.org/doi/10.1126/science.273.5278.1073 (visited on 12/09/2022).

[6] A. J. Daley, I. Bloch, C. Kokail, *et al.*, "Practical quantum advantage in quantum simulation," *Nature*, vol. 607, no. 7920, pp. 667–676, Jul. 2022, Number: 7920 Publisher: Nature Publishing Group, ISSN: 1476-4687. DOI: 10.1038/s41586-022-04940-6. [Online]. Available: https://www.nature.com/articles/s41586-022-04940-6 (visited on 12/14/2022).

References III

[7] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[8] L. K. Grover, *A fast quantum mechanical algorithm for database search*, 1996. DOI: 10.48550/ARXIV.QUANT-PH/9605043. [Online]. Available: https://arxiv.org/abs/quant-ph/9605043.

References IV

[9] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug. 6, 2018, ISSN: 2521-327X. DOI: 10.22331/q-2018-08-06-79. arXiv: 1801.00862[cond-mat,physics:quant-ph]. [Online]. Available: http://arxiv.org/abs/1801.00862 (visited on 12/09/2022).