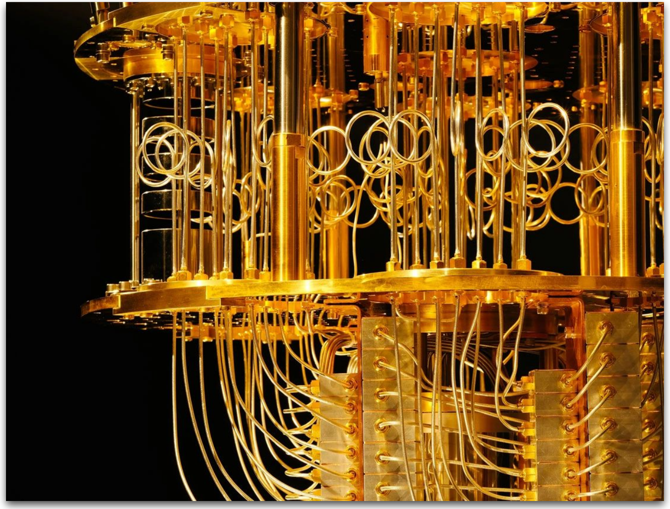
An Introduction to

Quantum Computing



Source: https://thequantuminsider.com/2022/11/09/ibm-quantum-computing/

Ali Almasi
Institut Polytechnique de Paris
May 2024

Disclaimer

“Those who are not shocked when they first come across quantum theory cannot possibly have understood it.” [*]

–Niels Bohr

Source: https://en.wikipedia.org/wiki/Niels_Bohr

* Heisenberg, Werner (1971). Physics and beyond: encounters and conversations. London: G. Allen & Unwin.

Prologue:

A Brief History

The First Ideas

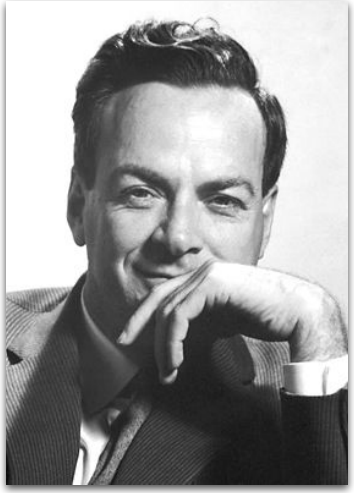
Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

- How hard is it “to simulate the quantum mechanical effect” with a computer?
  The number of variables grows exponentially!
- Feynman suggested:
  “Can you do it with a ***new kind of computer*** *— a* ***quantum computer****? Now it turns out, as far as I can tell, that you can simulate this with* ***a quantum system, with quantum computer elements.*** *It’s not a Turing machine, but a machine of a different kind.”**
- Around the same time as Feynman, Y. Manin and P. Benioff also brought up the idea.**



Source: https://en.wikipedia.org/wiki/Richard_Feynman

* Feynman, R.P. Simulating physics with computers. Int J Theor Phys 21, 467-488 (1982). https://doi.org/10.1007/BF02650179
**Preskill, John. "Quantum computing 40 years later." Feynman Lectures on Computation. CRC Press, 2023. 193-244.

A Timeline (From Feynman to Shor)

- (1985-1988) David Deutsch formalized the notion of a quantum computer.
- (1993) Umesh Vazirani and Ethan Bernstein formulated a problem that a quantum computer could solve with a **superpolynomial** speedup.
- (1996) Lov Grover introduced an algorithm with **quadratic** speedup for the **unstructured search** problem.
- (1997) Daniel Simon showed that a quantum computer could achieve an **exponential** speedup.
- (1999) Peter Shor introduced **efficient** quantum algorithms for solving the discrete logarithm and integer factorization problems.
- And then, it officially started . . .

Preskill, John. "Quantum computing 40 years later." Feynman Lectures on Computation. CRC Press, 2023. 193-244.

Is this just a new paradigm in algorithm design?

Quantum
Information Theory

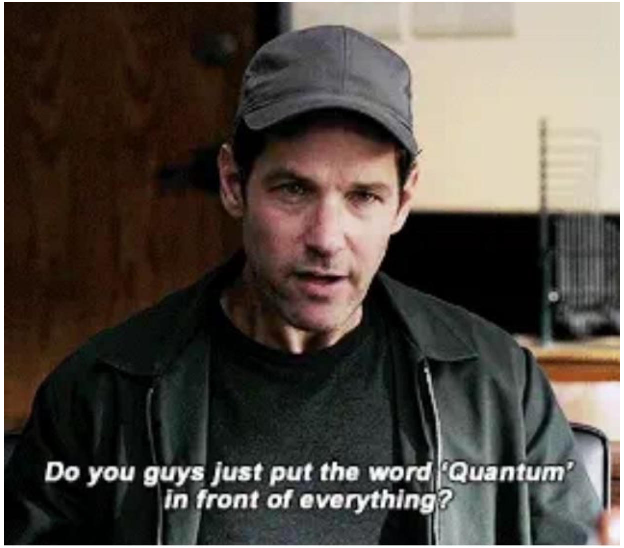
Quantum
Cryptography

Quantum Software
Verification

Quantum
Complexity Theory

Quantum Machine
Learning

...



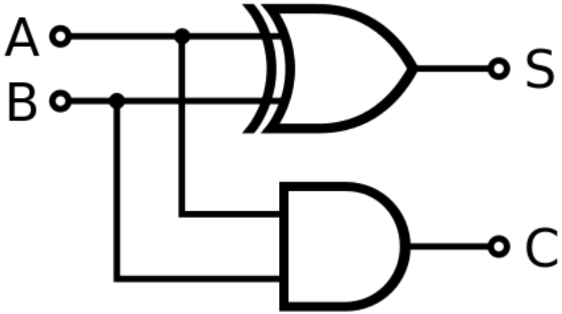
Hands-on Experience:

What is
A Quantum Algorithm?

And How Does it Work?

Towards a Mathematical Model of *Quantum* Computation (I)

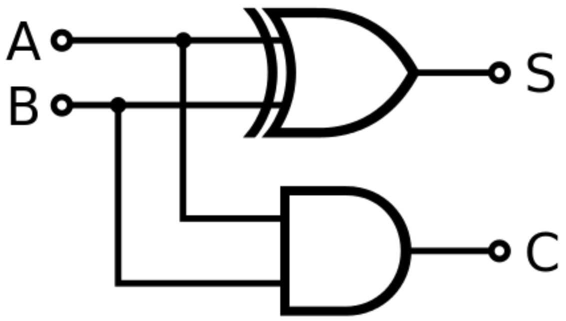
- We wish to find an abstract model for the types of computations that can be performed using a quantum hardware.
- Different abstractions have been developed for the classical setting: Turing Machines (Alan Turing, 1936), Lambda Calculus (Alonzo Church, 1936), **Circuit Model (Claude Shannon, 1937)**, . . .



Source: https://en.wikipedia.org/wiki/Adder_(electronics)

Towards a Mathematical Model of *Quantum* Computation (I)

- A circuit consists of three components:
  - Wires
  - Gates
  - (Measurements)

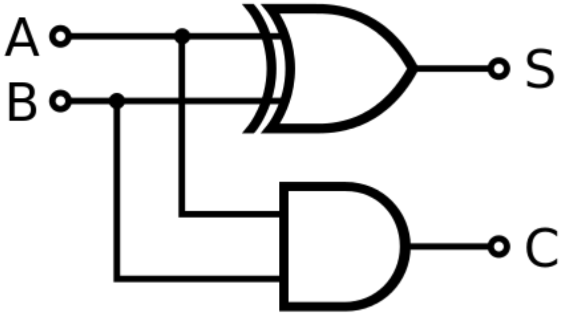


Source: https://en.wikipedia.org/wiki/Adder_(electronics)

Towards a Mathematical Model of *Quantum* Computation (II)

- A circuit consists of three components:
  - Wires
  - Gates
  - (Measurements)

What is the quantum analogue of each of these components?



Source: https://en.wikipedia.org/wiki/Adder_(electronics)

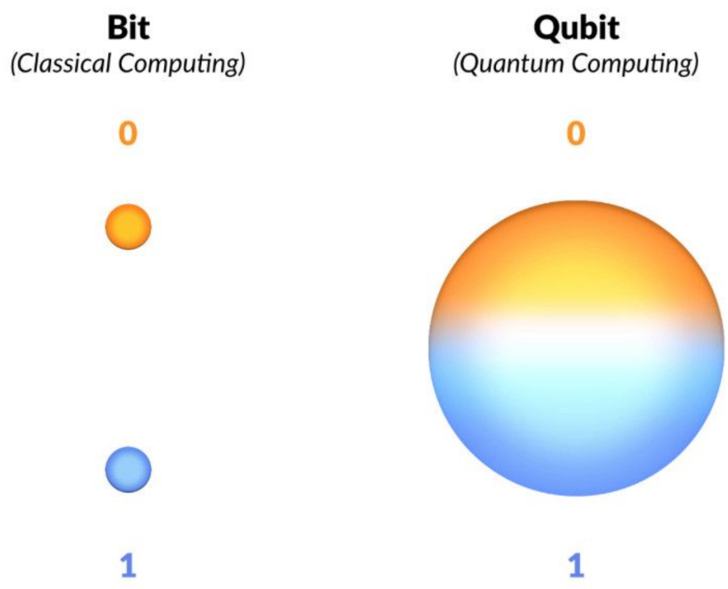
Quantum Mechanics

State Space

- Wires represent *bits*: b ∈ {0,1}.
  In hardware, they are systems that can be in two distinct states.
- There are also quantum systems having two different states, e.g. the spin of an electron.
- However, quantum 2-level systems (or qubits) have a strange behavior.
- They can be in 0 and 1 simultaneously!
  It is called Quantum Superposition!

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

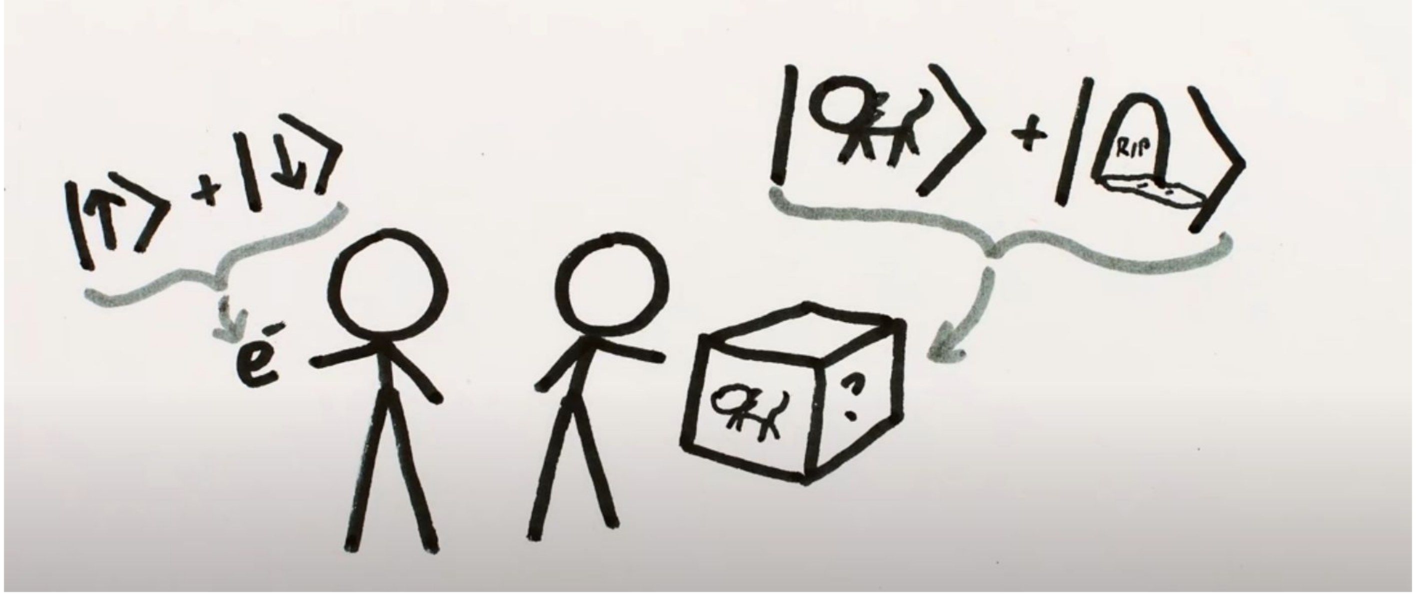
$$\alpha, \beta \in \mathbb{C}, \; |\alpha|^2 + |\beta|^2 = 1,$$



Source: https://www.linkedin.com/pulse/brief-introduction-quantum-computing-tanisha-bassan/

Quantum Mechanics

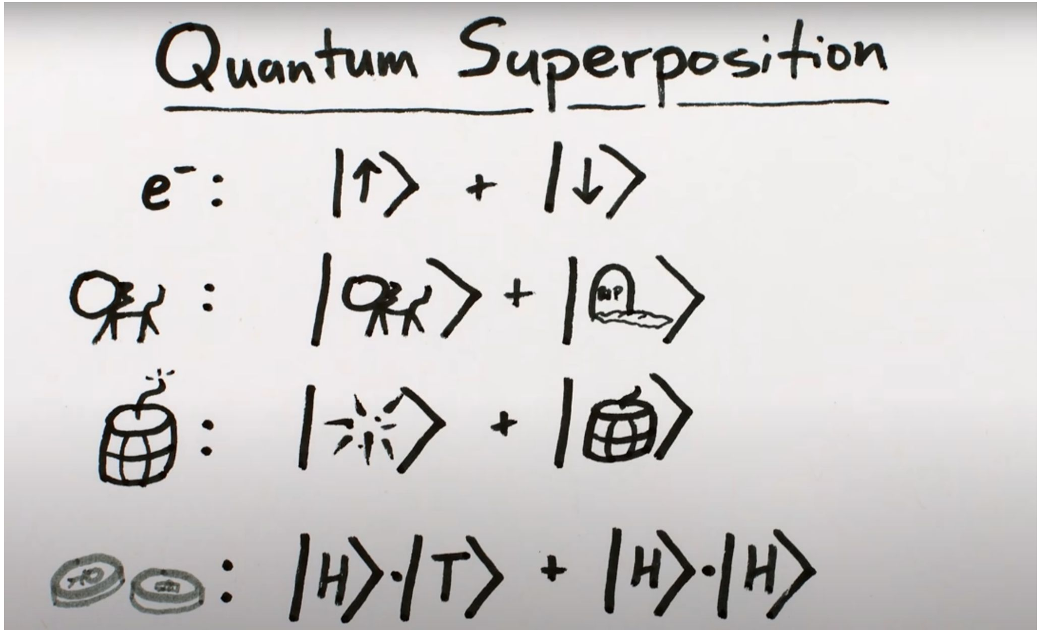
State Space



Source: A very nice video by Henry Reich (https://www.youtube.com/watch?v=DxQK1WDYI_k)

Quantum Mechanics

State Space



Source: A very nice video by Henry Reich (https://www.youtube.com/watch?v=DxQK1WDYI_k)

Quantum Mechanics

State Space

Postulate 1.2.10 State Space *Every isolated physical system is associated with a Hilbert space known as the system's **state space**. The **state vector** (or more succinctly, **state**) of the system is a unit vector in the corresponding state space [4].*

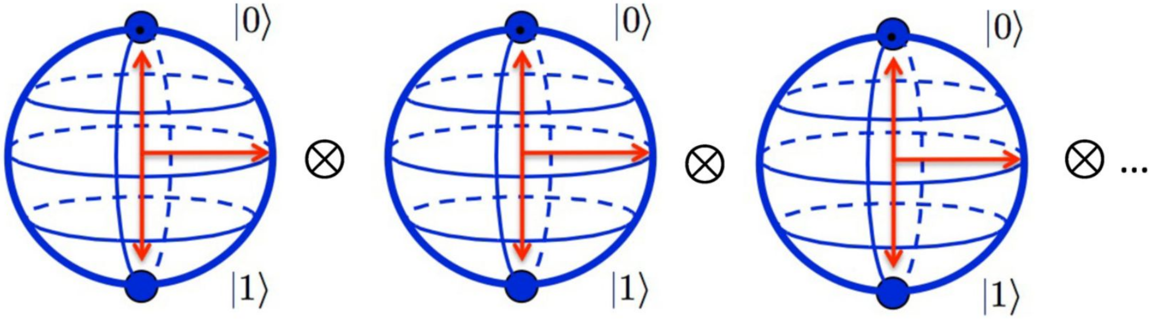
Definition 1.2.11 A **qubit** is a quantum system whose state space is the two-dimensional Hilbert space $\mathbb{C}^2$. ▶

Quantum Mechanics

Composite Systems

- How about n bits?
- Classically, we have **b** $\in \{0, 1\}^n$
- Quantumly, the state of an n-qubit system is a unit vector in $\mathbb{C}^{2^n}$

Now you understand why we said the number of variables in quantum system simulations increases exponentially.



Source: Joseph, Ilon & Shi, Yuan & Porter, M. & Castelli, A. & Geyko, V. & Graziani, Frank & Libby, Stephen & DuBois, J.. (2023). Quantum computing for fusion energy science applications. Physics of Plasmas. 30. 010501. 10.1063/5.0123765.

Quantum Mechanics

Composite Systems

Postulate 1.2.14 Compound Systems *The state space of a compound quantum system composed of* n *individual systems with state spaces* $V_1, \ldots, V_n$ *is the tensor product of the individual state spaces,* $V_1 \otimes \cdots \otimes V_n$*. If each component system is in state* $|v_i\rangle$*, then the joint state of the compound system is* $|v_1\rangle \otimes \cdots \otimes |v_n\rangle$ *[4].*

Quantum Mechanics

Time Evolution

- In classical circuits, we have logic gates that perform computation.
- Each gate is a boolean function: $f : \{0,1\}^n \to \{0,1\}^m$
- Quantum gates should be of the form $U : \mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$ and they should be linear.
- Thus, a gate is basically a matrix.
- Moreover, this matrix should be **unitary**, i.e. its columns form an orthonormal basis (or equivalently, it preserves the inner product (or norm), or equivalently, $U = (U^T)^*$).
- The application of more than one gates can be specified using tensor product..

Source: https://quantum.microsoft.com/en-us/explore/concepts/single-qubit-gates

Quantum Mechanics

Time Evolution

Some examples of quantum gates:

Gate Name	Matrix	Diagram [2]
Pauli-I	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$-\boxed{I}-$
Pauli-X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$-\boxed{X}-$
Pauli-Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$-\boxed{Y}-$

Gate Name	Matrix	Diagram
Pauli-Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$-\boxed{Z}-$
Hadamard	$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$	$-\boxed{H}-$
T-gate	$\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$	$-\boxed{T}-$
Phase (S-gate)	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	$-\boxed{S}-$
Relative Phase Rotation	$\begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i\theta} \end{pmatrix}$	$-\boxed{R_\theta}-$

Quantum Mechanics

Time Evolution

Postulate 1.2.13 Time Evolution *This postulate may be presented in two ways, which can be proven to be equivalent [4]:*

- *The state of a closed quantum system evolves according to Schrödinger's equation, i.e.*

  $$i\hbar \frac{d\left|\psi(t)\right\rangle}{dt} = H\left|\psi(t)\right\rangle,$$

  where $\psi(t)$ is the state of system at time t, H is a Hermitian operator known as the system's Hamiltonian, and $\hbar$ is Planck's constant.

- *If the state of a closed quantum system at time t_1 is $\left|\psi(t_1)\right\rangle$, the state at time $t_2 > t_1$ is determined by*

  $$\left|\psi(t_2)\right\rangle = U\left|\psi(t_1)\right\rangle$$

  where U is a unitary operator that only depends on $t_2 - t_1$.

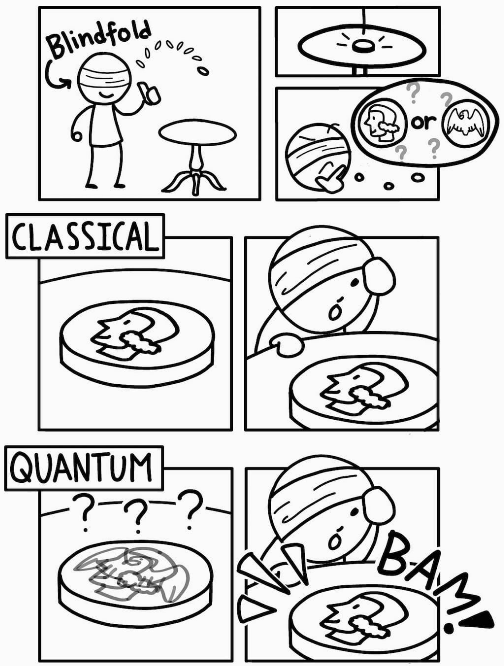
Quantum Mechanics

Measurement

- When we measure a quantum state, the outcome is determined probabilistically!

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \xrightarrow{measure} \begin{cases} |0\rangle & \textit{with probability } |\alpha|^2 \\ |1\rangle & \textit{with probability } |\beta|^2 \end{cases}$$

- Moreover, the state of the system will change (or **collapse**).
- Note that measuring in the basis {0,1} is not our only option!



Source: https://quantumatlas.umd.edu/entry/measurement/

Quantum Mechanics

Measurement

Postulate 1.2.16 Measurement *A measurement on a quantum system is a collection of operators* $M = \{M_1, \ldots, M_m\}$ *that satisfy* $\sum_{i=1}^{m} M_i^\dagger M_i = I$. *When a quantum system in the state* $|\psi\rangle$ *is measured using a collection of measurement operators* M, *the probability of the measurement outcome being* i *is derived by*

$$p(i) = \left\langle \psi \middle| M_i^\dagger M_i \middle| \psi \right\rangle,$$

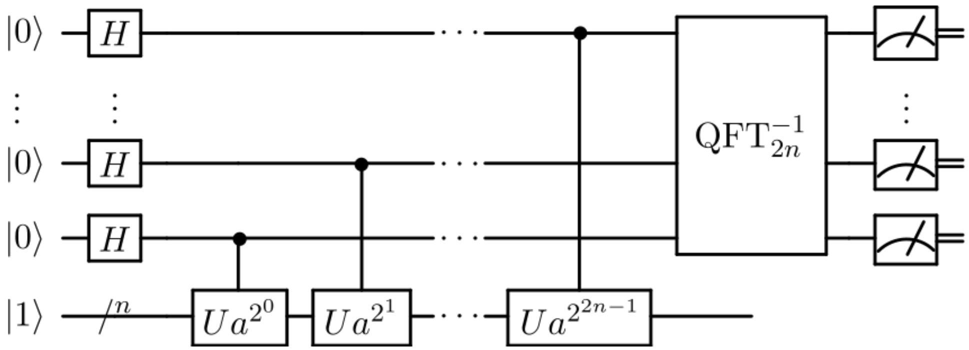
and the system collapses to the state

$$\frac{M_i|\psi\rangle}{\sqrt{\left\langle \psi \middle| M_i^\dagger M_i \middle| \psi \right\rangle}}$$

following the measurement [4].

Quantum Circuits

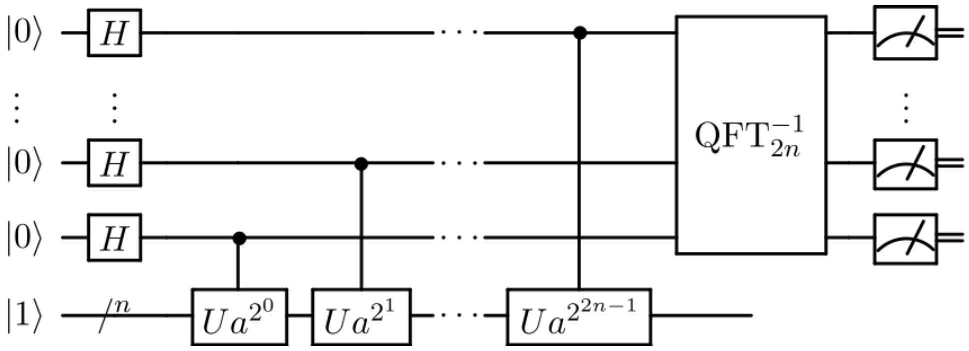
- They're nothing but applying a bunch of unitaries on some qubits, and then measuring the qubits to extract the result.



Source: https://en.wikipedia.org/wiki/Shor%27s_algorithm

Quantum Circuits

- They're nothing but applying a bunch of unitaries on some qubits, and then measuring the qubits to extract the result.



Source: https://en.wikipedia.org/wiki/Shor%27s_algorithm

Let's think about it for a moment:

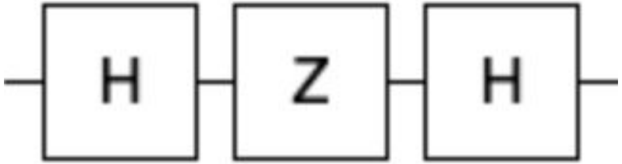
In the quantum setting, we have things that we didn't have in the classical setting:

- Superposition
- Entanglement (we haven't discussed yet!)

And there are things that we could do classically but we can not do it in the quantum world:

- Copying an arbitrary qubit
- Irreversible computation (?)
- Measurement without destroying the state

Our First Quantum Circuit



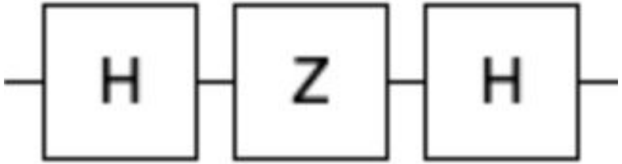
Remember

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad -\boxed{Z}-$$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \qquad -\boxed{H}-$$

Our First Quantum Circuit



On

On

Remember

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad -\boxed{Z}-$$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \qquad -\boxed{H}-$$

A Quantum Algorithm for the Search Problem

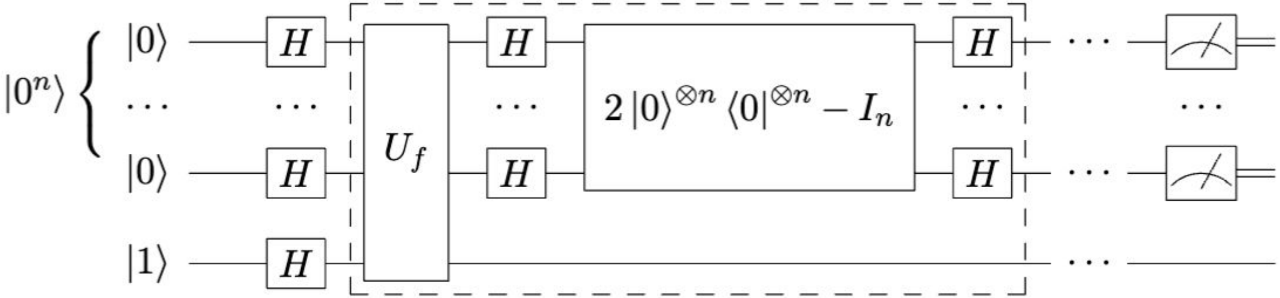
Problem.

Input: Black box access to a function $f : \{0,1\}^n \to \{0,1\}$ together with a promise that $card(\{x \in \{0,1\}^n \ : \ f(x) = 1\}) = t$.
Output: An $x \in \{0,1\}^n$ such that $f(x) = 1$.

Grover's Solution

First, apply Hadamard gates to obtain a uniform superposition of all binary strings:

$$|\psi\rangle = |+\rangle^{\otimes n} |-\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |-\rangle$$



Grover's Solution

Now, consider only the first n qubits:

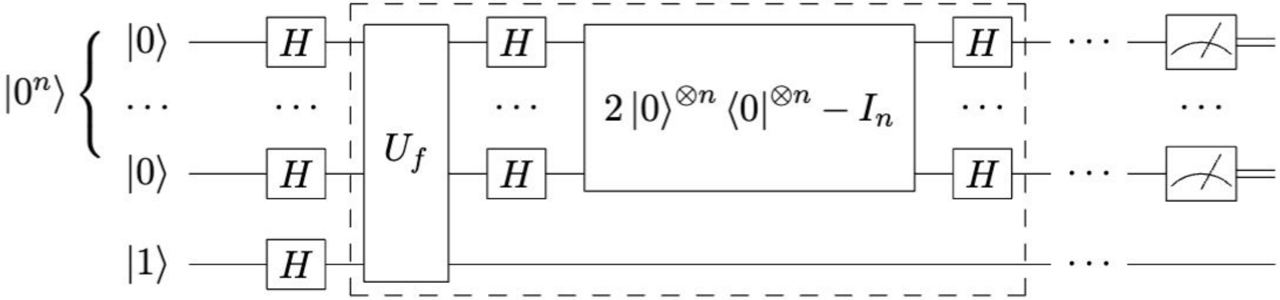
$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Define:

$$|G\rangle = \frac{1}{\sqrt{t}} \sum_{x:f(x)=1} |x\rangle\,, \qquad |B\rangle = \frac{1}{\sqrt{2^n - t}} \sum_{x:f(x)=0} |x\rangle\,, \qquad \sin\theta = \sqrt{\frac{t}{2^n}}$$

We can write:

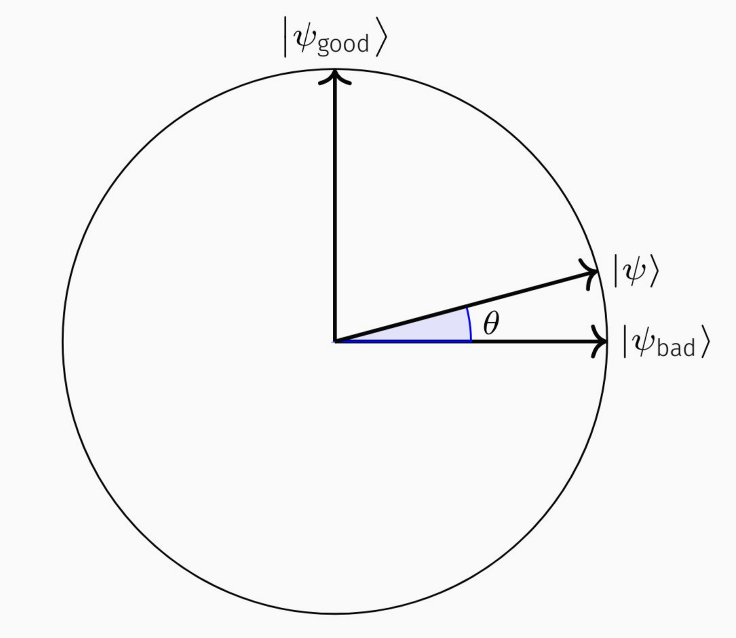
$$|\psi_0\rangle = \sin\theta\,|G\rangle + \cos\theta\,|B\rangle$$

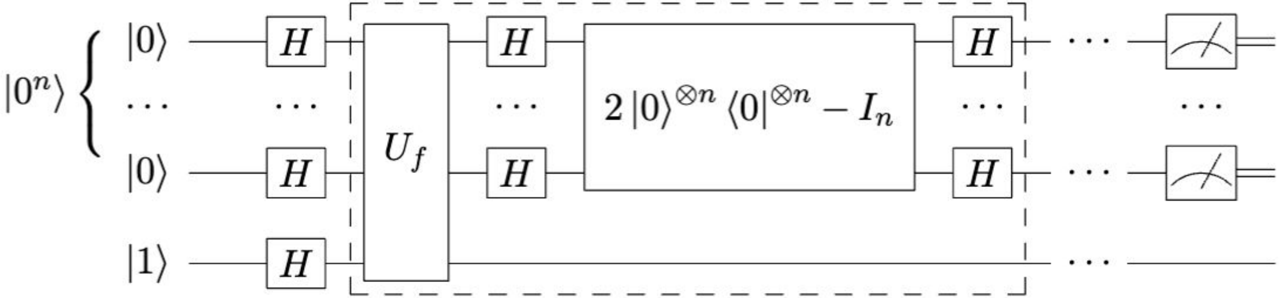


Grover's Solution

We can write:

$$|\psi_0\rangle = \sin\theta\,|G\rangle + \cos\theta\,|B\rangle$$



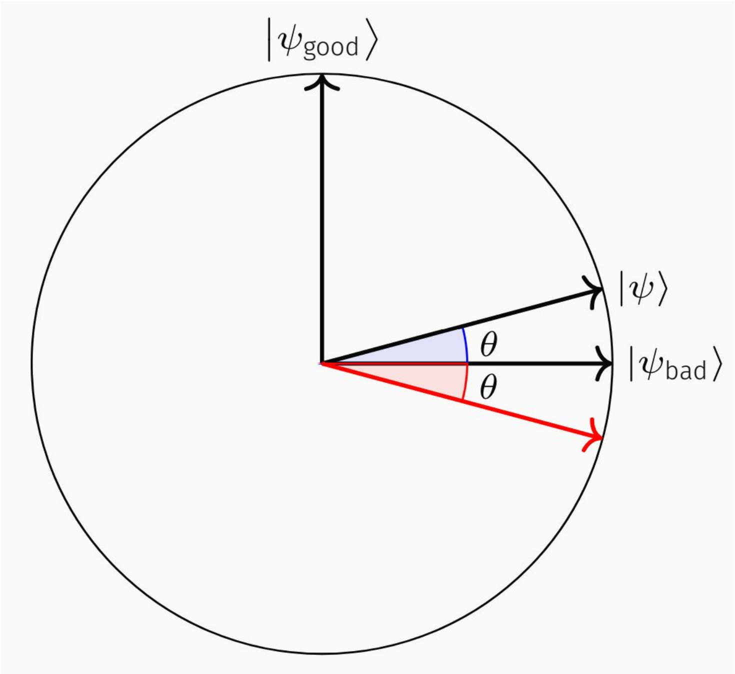


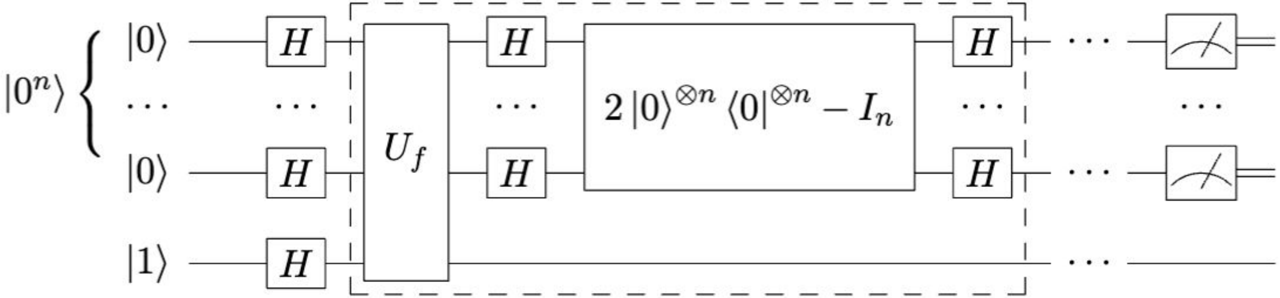
Grover's Solution

We can write:

$$|\psi_0\rangle = \sin\theta\,|G\rangle + \cos\theta\,|B\rangle$$

By applying U_f we perform a reflection over



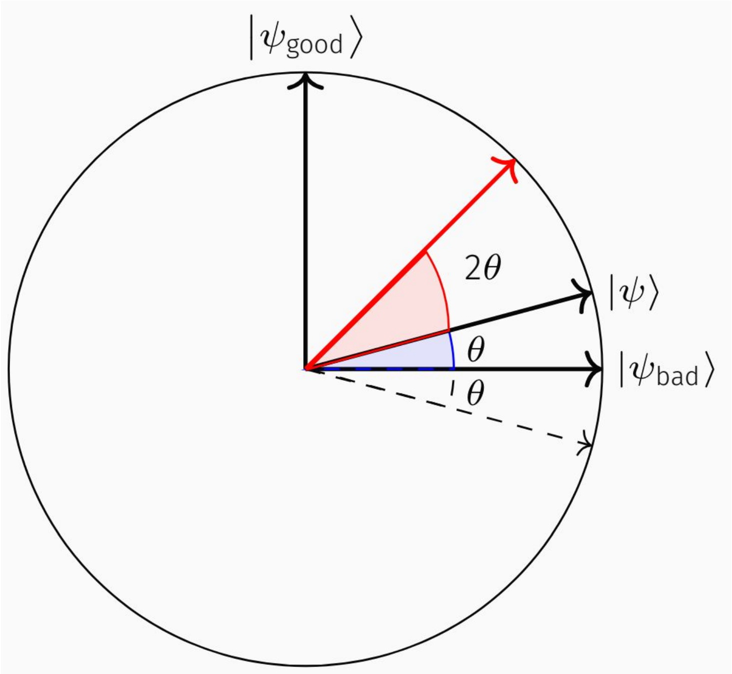


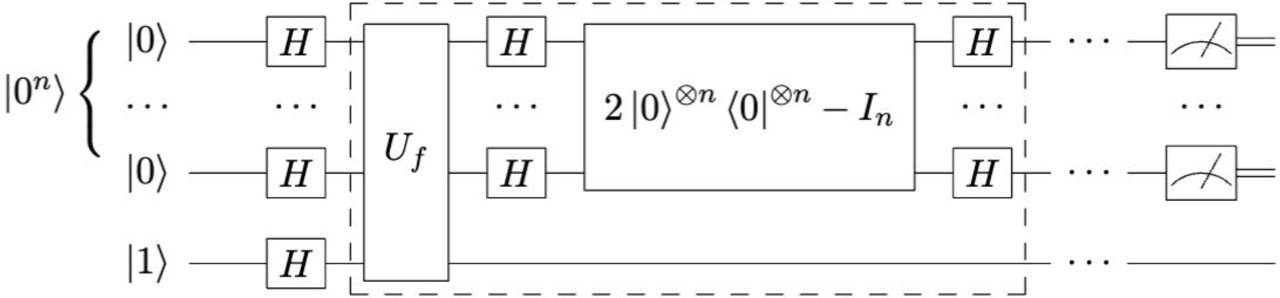
Grover’s Solution

We can write:

$$|\psi_0\rangle = \sin\theta\,|G\rangle + \cos\theta\,|B\rangle$$

- By applying U_f we perform a reflection over
- By applying the rest of the iteration we perform a reflection over





Grover's Solution

We can write:

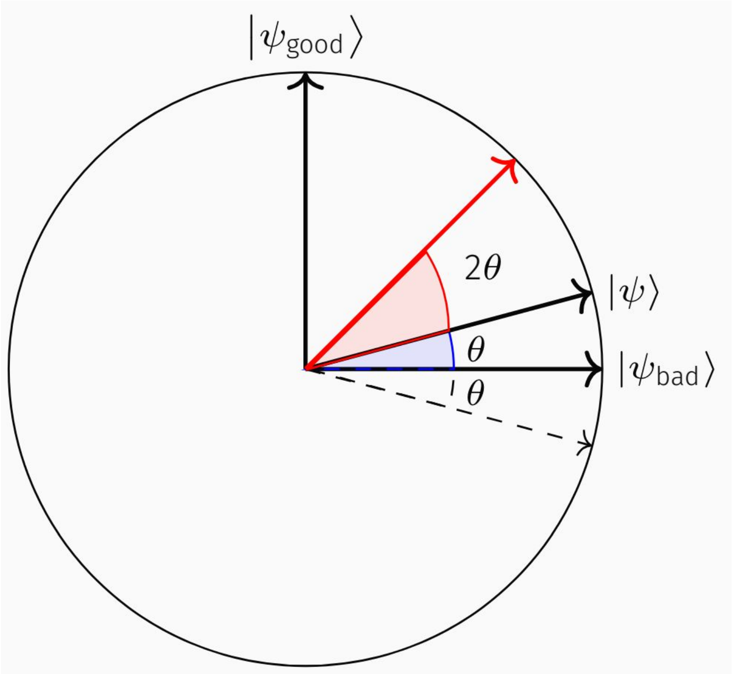
$$|\psi_0\rangle = \sin\theta\,|G\rangle + \cos\theta\,|B\rangle$$

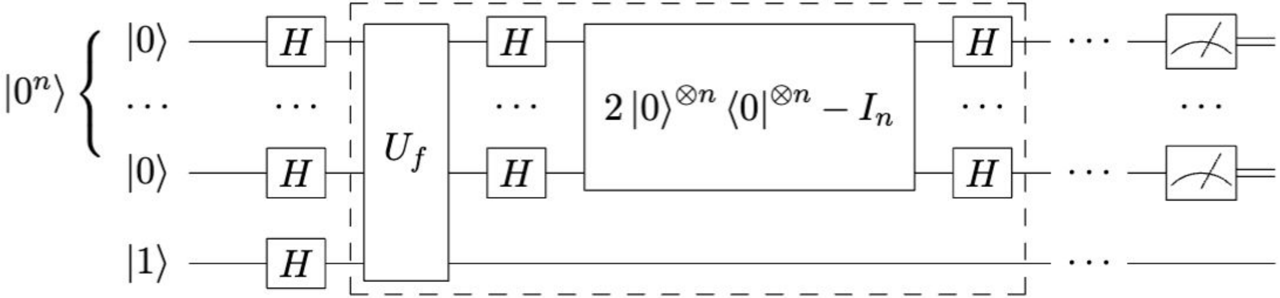
Therefore, after the first iteration, the state is

$$|\psi_1\rangle = \sin 3\theta\,|G\rangle + \cos 3\theta\,|B\rangle$$

And after the k'th iteration is

$$|\psi_k\rangle = \sin(2k+1)\theta\,|G\rangle + \cos(2k+1)\theta\,|B\rangle$$





Grover's Solution

We can write:

$$|\psi_0\rangle = \sin\theta\,|G\rangle + \cos\theta\,|B\rangle$$

Therefore, after the first iteration, the state is

$$|\psi_1\rangle = \sin 3\theta\,|G\rangle + \cos 3\theta\,|B\rangle$$

And after the k'th iteration is

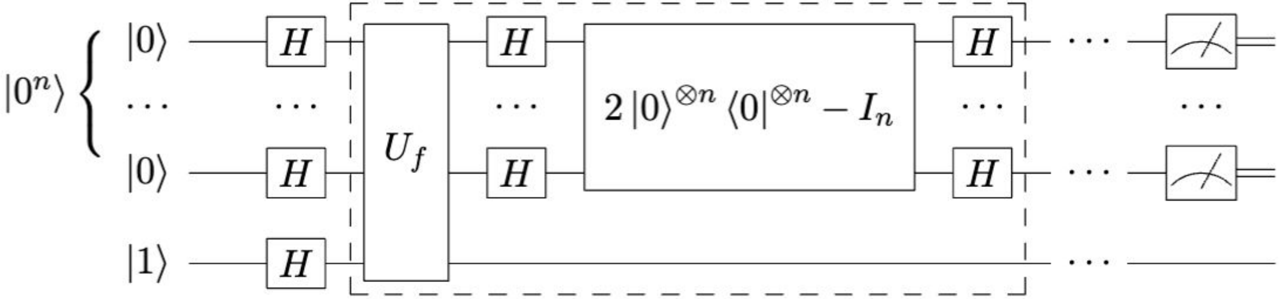
$$|\psi_k\rangle = \sin(2k+1)\theta\,|G\rangle + \cos(2k+1)\theta\,|B\rangle$$

If we measure, we obtain a good state with prob.

$$\sin^2(2k+1)\theta.$$

Choose k such that the above probability is close to 1.

$$k = O\left(\sqrt{\frac{2^n}{t}}\right)$$



Final Words

How can I start to learn more?

Resources in English

Books

1. Nielsen MA, Chuang IL. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press; 2010.

Lecture Notes

1. De Wolf, R. (2019). Quantum computing: Lecture notes. *arXiv preprint arXiv:1907.09415*.
2. Gharibian, S. (2021). Introduction to quantum computation. *Paderborn University*.

Review/Expository Articles

1. Preskill, J. (2023). Quantum computing 40 years later. In *Feynman Lectures on Computation* (pp. 193-244). CRC Press.
2. Montanaro, A. (2016). Quantum algorithms: an overview. *npj Quantum Information*, *2*(1), 1-8.

Resources in Persian

کتاب‌ها

(؟)

درس‌گفتارها

1. بیگی، س. (۱۳۹۱). محاسبات کوانتومی. https://salmanbeigi.github.io/lecturenotes.html
2. کریمی‌پور، و. (۱۴۰۲) محاسبات و اطلاعات کوانتومی. https://physics.sharif.edu/~vahid/teachingQC.html

مقالات توصیفی/مروری

1. محرابیان، ع. (۱۳۹۲). الگوریتم جست‌وجوی گراور. در مجله‌ی ریاضی شریف (دوره‌ی دوم، شماره‌ی هفتم) https://sharif-math-journal.github.io/posts/Series2Issue
2. شور، پیتر. آشنایی با الگوریتم‌های کوانتومی، ترجمه‌ی الهام کاشفی. در نشر ریاضی، ۱۴(۲)، ۳۳-۴۴
3. ا. (۱۴۰۳). نسخه‌ی کوانتومی NP. در مجله‌ی ریاضی شریف (دوره‌ی سوم، شماره‌ی دوم) https://sharif-math-journal.github.io/posts/Series3Issue2