Theory of Quantum Computation

David Shimkus
SIUE CS 454
April 26, 2023

Outline

1. Introduction
   a. Background
   b. Use Cases (Why Should I Care?)
2. Quantum Basics
   a. Qubits and Linear Algebra
   b. Quantum Entanglement
3. Theory of Quantum Computation
   a. Quantum Turing Machines
   b. Inherent Parallelism
4. Quantum Error Correction
   a. Errors and Noise
   b. Physical and Logical Qubits
   c. Experimental Results
5. Conclusions and Next Steps

https://www.enterpriseappstoday.com/news/quantum-computing-market-size-usd-234-1-billion-by-2032-with-36-89-cagr.html

1. Introduction

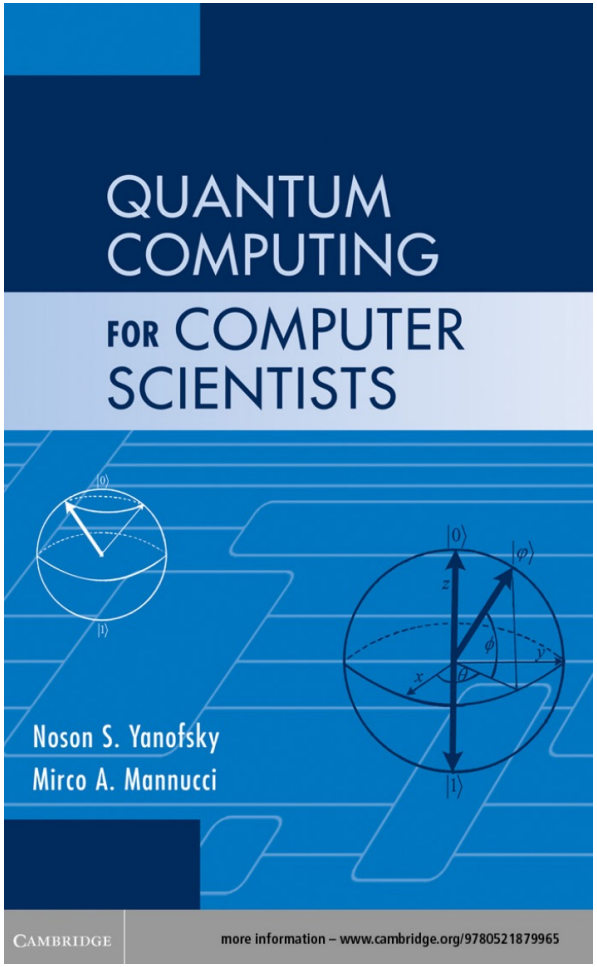
"Computer Science is no more about computers than astronomy is about telescopes."

- E.W. Dijkstra

Recommended Textbook: Quantum Computing for Computer Scientists – Yanofsky and Mannucci

ISBN 978-0-521-87996-5

A little outdated as published in 2008. No practical programming examples, but very good on theory.



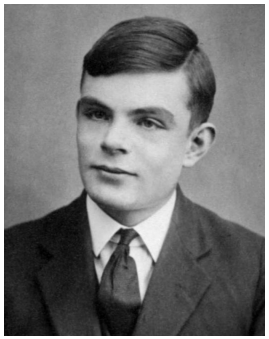
1.a. Introduction - Background

The ancient Greek philosophers Leucippus and Democritus (~400 B.C.) is usually credited as the fathers of atomism – the philosophy of *ἄτομον*, atomon, i.e. "uncuttable, indivisible"

The Church-Turing Thesis laid the groundwork for modern classical computation methods in the 1930's.

The basics of modern quantum computation can be found in any text-book on quantum computing. They were first formulated by David Deutsch in 1989.

Leucippus by Luca Giordano (1652)



Alan Turing in 1928

David Deutsch – physics.ox.ac.uk

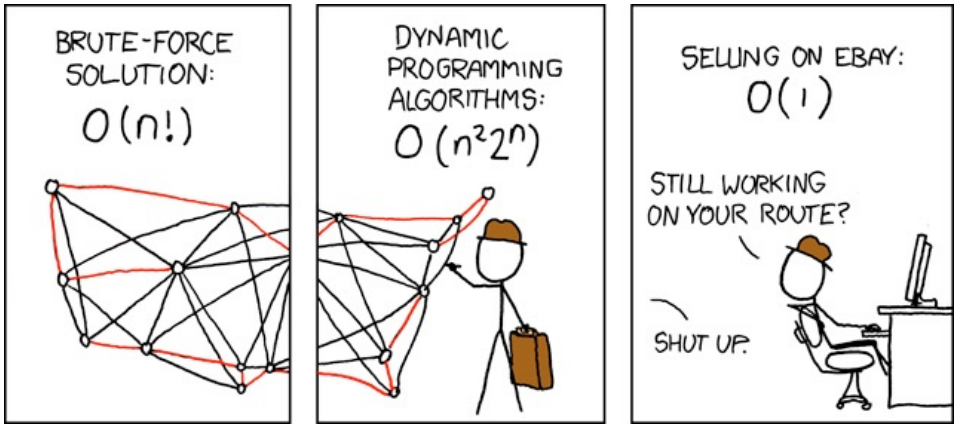
1.b. Introduction – Use Cases

Why Should I Care?

Chips away at combinatorics problems – but not all of them!

Combinatorics – finding an "arrangement" or "configuration" of items that optimizes some goal. As the number of items increases, the possible "arrangements" increases exponentially.

i.e. NP-Hard Travelling Salesman still has subpar performance



https://doi.org/10.3389/fphy.2021.760783
https://xkcd.com/399/

1.b. Introduction – Use Cases

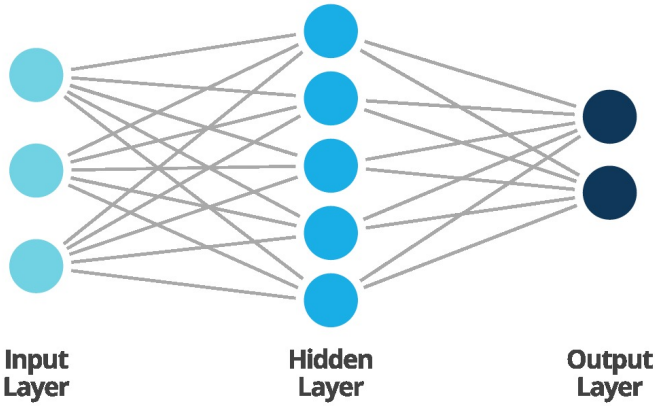
Why Should I Care?

Cybersecurity – Encryption methods such as RSA employs computationally intensive functions to obfuscate some secret.

Pharmaceuticals – Manipulating subatomic particles always involves quantum properties. Chemistry reactions and molecular configurations are obviously complex.

Artificial Intelligence – Choosing "better" predictions/paths can be hard.

And more…

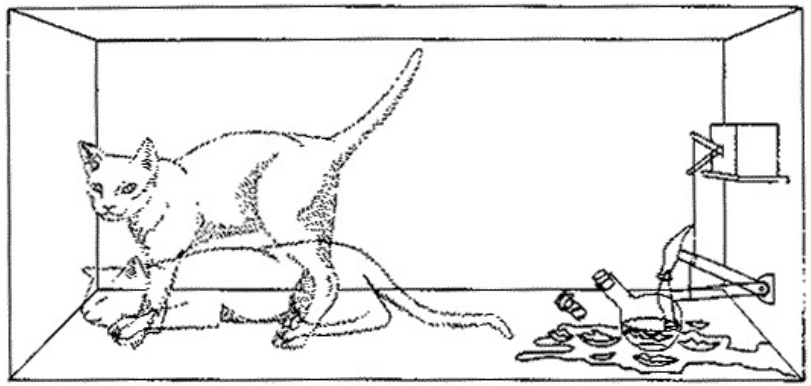


https://hbr.org/2021/07/quantum-computing-is-coming-what-can-it-do
https://www.smartsheet.com/neural-network-applications

2. Quantum Basics

Classical Mechanics – The study of everyday objects and their properties such as kinematics, etc. Objects exist at a specific place at a particular time.

Quantum Mechanics – The study of sub-molecular physics including atoms, electrons, photons, etc. Objects exist in **probabilistic** "superposition" of multiple places at the same time.



https://www.livescience.com/33816-quantum-mechanics-explanation.html
https://erwinschrodingerbiography.weebly.com/schrodingers-cat.html

2.a. Quantum Basics – Qubits

Qubit - The quantum analog for a classical bit

Bloch Sphere – A common representation of a qubit, it shows how values 0 or 1 can be in a superposition.

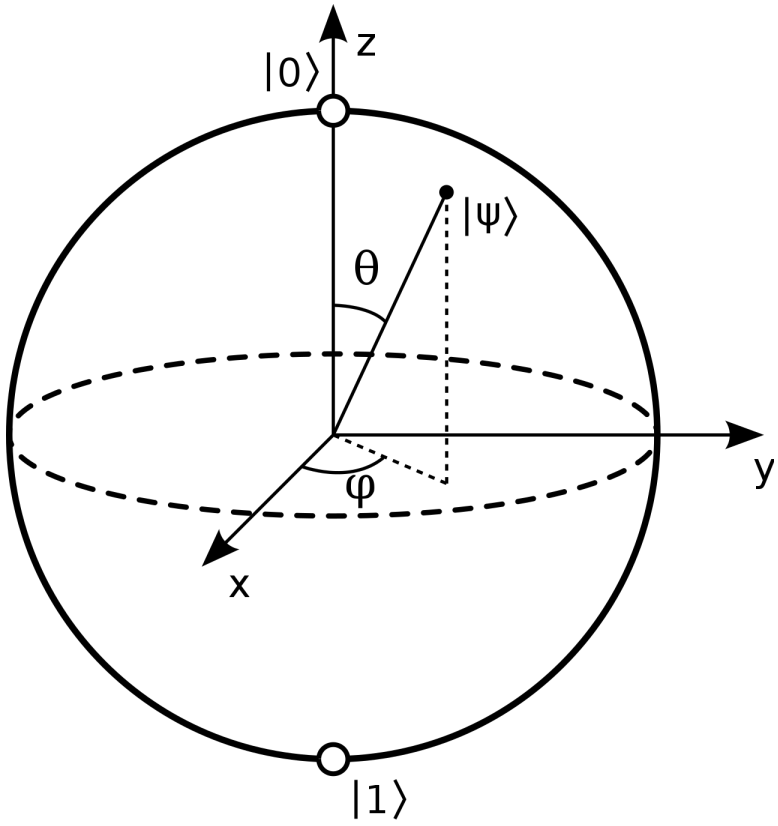
Bra-Ket notation

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle$$

where $0 \le \theta \le \pi$ and $0 \le \varphi < 2\pi$

and i is imaginary where $i^2 = -1$ or $i = \sqrt{(-1)}$

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



https://en.wikipedia.org/wiki/Bloch_sphere

2.a. Quantum Basics – Linear Algebra

Qubit: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Probability of "collapsing" to $|0\rangle$ or $|1\rangle$ state: $|\alpha|^2 + |\beta|^2 = 1$

Imagine this qubit has 100% probability of being $|0\rangle$, then it can just be represented as $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Without loss of generality $|1\rangle$ is $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

A qubit with a value of $\begin{bmatrix} 1/\sqrt{(2)} \\ 1/\sqrt{(2)} \end{bmatrix}$ is a 50% chance of being a $|0\rangle$ or a $|1\rangle$

2.a. Quantum Basics – Linear Algebra

Quantum logic gates can operate similarly to classical logic gates.

i.e. Bit Flip Gate X = $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Example 0: apply the bit flip gate against a qubit initialized to $|0\rangle$

Recall: $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Therefore: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} (0 * 1) + (1 * 0) \\ (1 * 1) + (0 * 0) \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$

2.b. Quantum Basics – Entanglement

Multiple qubits can become entangled influencing each others' "spin"
This can be represented by a tensor product

Example 1: $|00\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$

This shows two entangled $|0\rangle$ qubits. Note the resulting 4 state vertex

2.b. Quantum Basics – Entanglement

Example 2: now with three entangled qubits, $|1\rangle$, $|1\rangle$, and $|0\rangle$

$$|110\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\begin{bmatrix}0\\1\end{bmatrix}\\1\begin{bmatrix}0\\1\end{bmatrix}\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\begin{bmatrix}1\\0\end{bmatrix}\\0\begin{bmatrix}1\\0\end{bmatrix}\\0\begin{bmatrix}1\\0\end{bmatrix}\\1\begin{bmatrix}1\\0\end{bmatrix}\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\\0\\1\\0\end{bmatrix}$$

With two entangled qubits we had a resulting $2^2 = 4$ result state

With three entangled qubits we have $2^3 = 8$ result state

With n entangled qubits we have 2^n result state! Exponential increase

3. Theory of Quantum Computation

How does this apply to what we have learned in CS 454? Complexity, number theory, and generalizations of existing material

Certain types of problems can be solved more efficiently, but the scope of problems able to be solved is not changed.

Incorrect assumption: hypercomputing or super-Turing

Quantum computers do NOT solve the halting problem!

3.a. Theory of Quantum Computation - Quantum Turing Machines

Unitary operations – operations are reversible. All operations on a quantum system such as entanglement and the application of quantum logic gates are unitary

Unitary matrices – a matrix multiplied by its own conjugate transpose results in the identity matrix .

i.e. $UU^{\dagger} = U^{\dagger}U = I$

The state of the quantum system evolves via unitary operations

3.a. Theory of Quantum Computation - Quantum Turing Machines

Hilbert Space – a real or complex inner product space $\mathcal{H}$

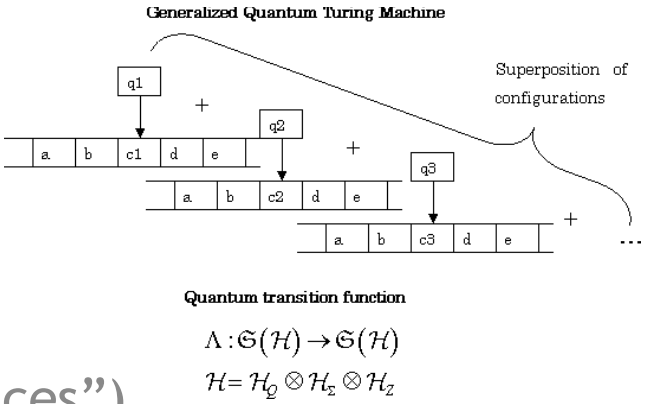
The state of a quantum system is a vector ψ belonging to $\mathcal{H}$

The evolution of the state can be thought of as $|\psi^1\rangle = U|\psi\rangle$

3.a. Theory of Quantum Computation - Quantum Turing Machines

Quantum Turing Machines can be defined similarly to classical Turing Machines, with some differences and generalizations

$M = (Q, \Sigma, \Gamma, \delta, Q_0, \square, F)$



Q = the overall "Hilbert Space" of the system

Σ = input alphabet - can be classical!

Γ = tape alphabet (these are also "Hilbert Spaces")

δ = (Q – F) x Γ ("Hilbert Space" transitions – think tensor products)

Q_0 = start state (the initial "Hilbert Space")

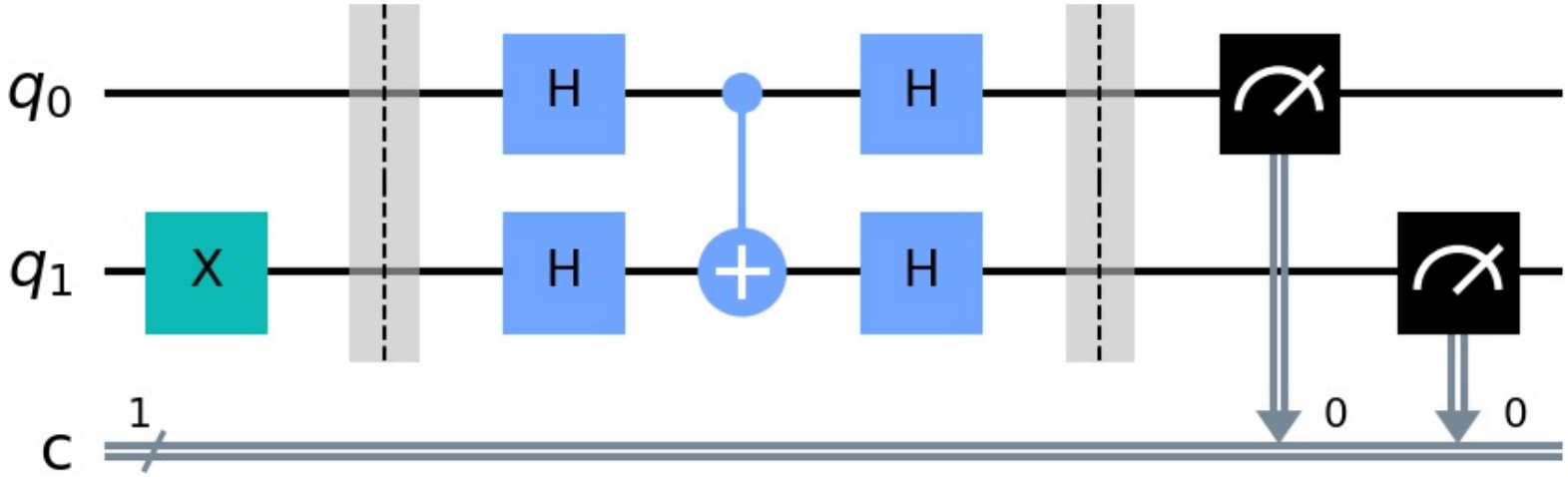
F = set of final states (the possible final "Hilbert Spaces")

https://regilanj.wordpress.com/2018/01/07/quantum-computing/

3.b. Theory of Quantum Computation – Quantum Turing Machines

Instead of Quantum Turing Machines, Quantum Computations are usually represented with Quantum Circuits

Example generated using IBM's Python Qiskit library:



3.b. Theory of Quantum Computation – Inherent Parallelism

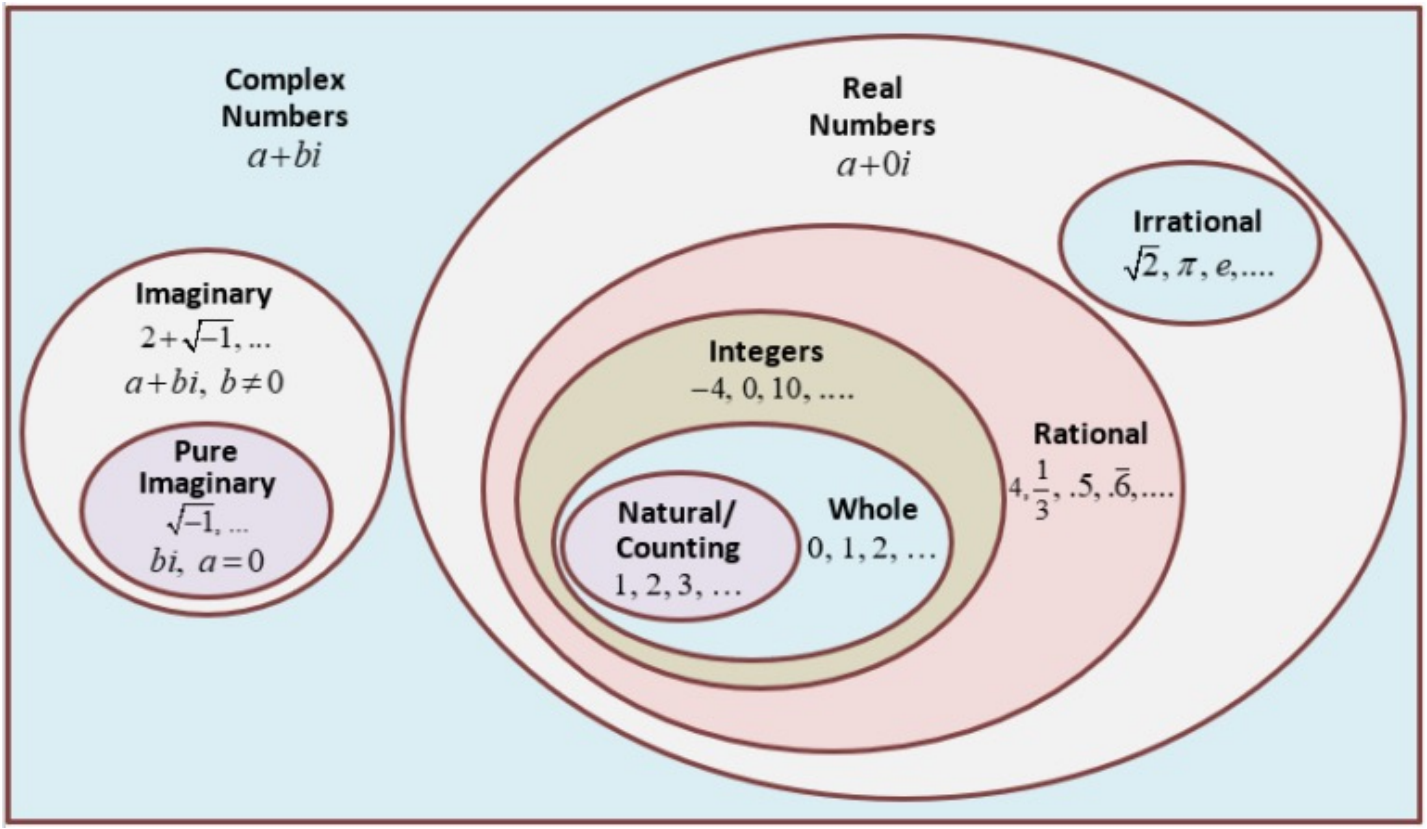
With n entangled qubits we have 2^n result state! Exponential increase!
Compare against a theoretical 3 GHz CPU with one operation per cycle.

# of qubits	# bits or # loops	RAM	Time
13	8192	1 kB	2.73×10^{-6} s
20	1048576	128 kB	3.5×10^{-4}s
23	8388608	1 MB	2.8×10^{-3}s
33	8589934592	1 GB	2.9 s
43	8.8×10^{12}	1 TB	49 mins
53	9.0×10^{15}	1 PB	35 hours
63	9.2×10^{18}	1 EB	97.5 years
1000	1.1×10^{301}	1.3×10^{282} EB	1.1×10^{284} years

https://vincentlauzon.com/2018/03/21/quantum-computing-how-does-it-scale/

3.b. Theory of Quantum Computation – Inherent Parallelism

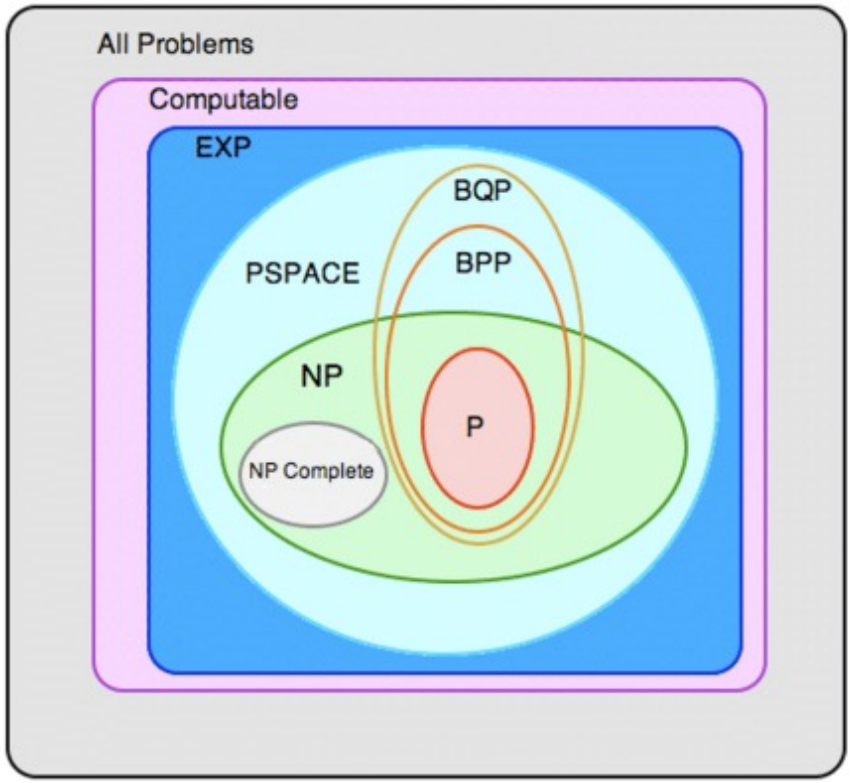
Qubits are computationally "complex" numbers



https://mathhints.com/complex-numbers/

3.b. Theory of Quantum Computation – Inherent Parallelism

Quantum computers operate in a bounded-error quantum polynomial time (BQP) class of decision problems



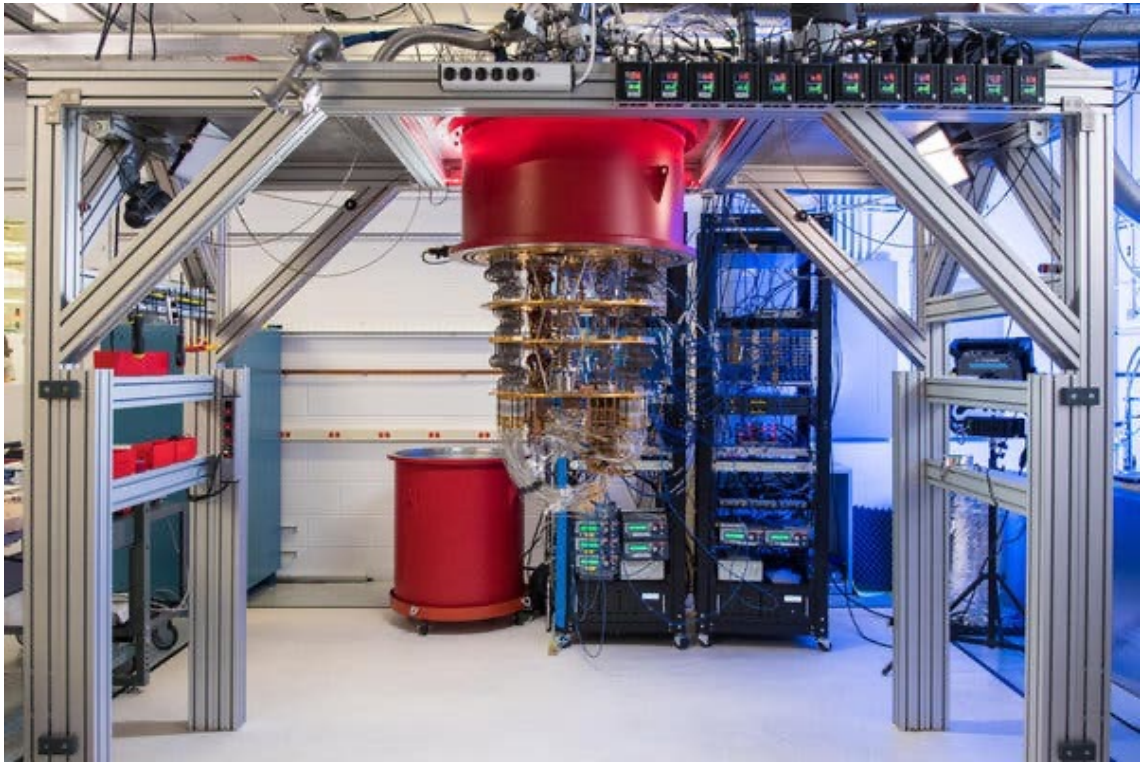
P	solution can be found in time polynomial in the size (number of bits)
NP	solution can be checked in polynomial time
NP COMPLETE	any NP problem can be reduced to one of these
BPP	solution in polynomial time at probability $p>1/2$
BQP	solution in polynomial time at probability $p>1/2$ on quantum computer
PSPACE	solution requires a polynomial amount of memory
EXP	solution can be found in exponential time
COMPUTABLE	solution can be found eventually

Source: Adiabatic Quantum Computing - Masters Thesis of Sebastian D. Pinski supervised by Dr. John Samson - Department of Physics Loughborough University (England)

Note: there are other representations of this diagram, and all are not universally agreed upon.

4. Quantum Error Correction

Too good to be true? "sort of"



A Quantum Computer from Google
https://www.nytimes.com/2019/10/23/technology/quantum-computing-google.html

https://kayfrancisfilms.com/trouble-in-paradise-1932/

4.a. Quantum Error Correction – Errors and Noise

Types of Errors:

- Bit Flip
  $|0\rangle \rightarrow |1\rangle$
- Sign Flip
  $|1\rangle \rightarrow -|1\rangle$
- Bit AND Sign Flip
  $|0\rangle \rightarrow -|1\rangle$

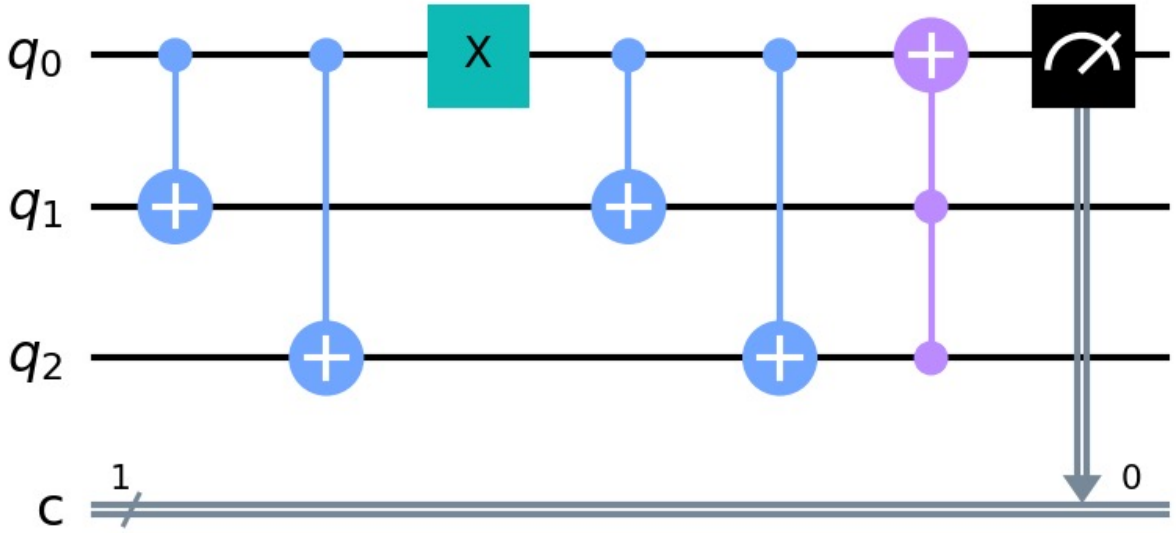
These errors can be thought of as the “spin” getting corrupted

Sources of Error in Physical Systems:

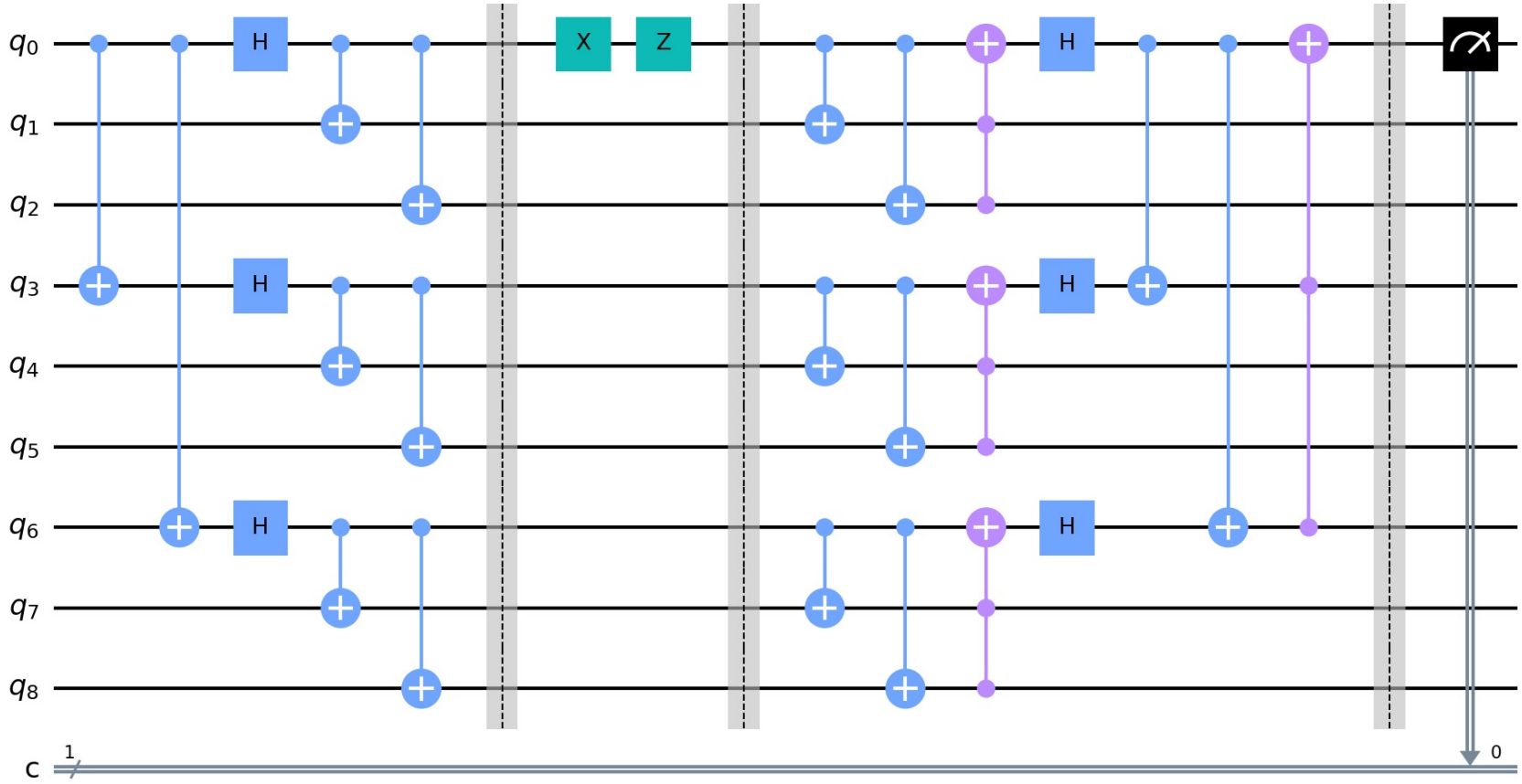
- Vibrations
- Temperature Fluctuations
- Electromagnetic Interference
- Other interactions outside the environment
- Decoherence

4.b. Quantum Error Correction – Physical and Logical Qubits

Quantum Error Correction (QEC) – variety of methods employed to detect and correct for errors at the tradeoff of additional "ancilla" qubit or temporal overhead



4.b. Quantum Error Correction – Physical and Logical Qubits

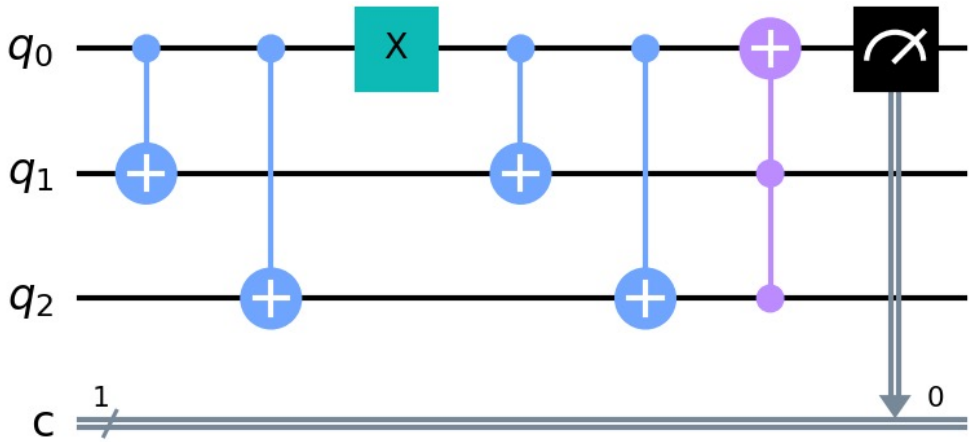


The first "logical" qubit – the 9 qubit Shor Code – Note the two simulated errors in green.
There are other kinds of logical qubits of varying complexities and tradeoffs.

4.c. Quantum Error Correction – Experimental Results

```
print('\nBit Flip Code')
print('----------------')

q = QuantumRegister(3,'q')
c = ClassicalRegister(1,'c')

circuit = QuantumCircuit(q,c)

circuit.cx(q[0],q[1])
circuit.cx(q[0],q[2])
circuit.x(q[0]) #Add this to simulate a bit flip error
circuit.cx(q[0],q[1])
circuit.cx(q[0],q[2])
circuit.ccx(q[2],q[1],q[0])
circuit.measure(q[0],c[0])

circuit.draw(output='mpl',filename='bit-flip.png') #Draws

job = execute(circuit, backend, shots=1000)

job_monitor(job)

counts = job.result().get_counts()

print("\nBit flip code with error")
print("-----------------------")
print(counts)
input()
```

```
Bit Flip Code
----------------
Job Status: job has successfully run

Bit flip code with error
-----------------------
{'0': 1000}
```



5. Limitations and Next Steps

IBM Qiskit used for all experiments

- Up to 100 simulated “general purpose” qubits
  - https://quantum-computing.ibm.com/lab/docs/iql/manage/simulator
- OR up to 127 physical qubits – sporadic results and occasionally queue times for hours

Name	Qubits ↓	QV	CLOPS	Status	Total pending jobs
ibm_washington	127	64	850	Online - Queue paused	26
ibm_sherbrooke	127	32	904	Online	298
ibm_kyiv Exploratory	127	-	-	Online - Queue paused	0
ibm_brisbane	127	-	-	Online	4
ibm_ithaca Exploratory	65	-	-	Online - Queue paused	46
ibm_prague Exploratory	33	-	-	Online	0
ibmq_kolkata	27	128	2K	Online	238
ibmq_mumbai	27	128	1.8K	Online - Queue paused	87
ibm_cairo	27	64	2.4K	Online	164
ibm_auckland Exploratory	27	64	2.4K	Online	1158

5. Limitations and Next Steps

Comparing against our theoretical 3GHz processor earlier:

# of qubits	# bits or # loops	RAM	Time	ibm_cairo qubits	Ibm_cairo CLOPS
23	8388608	1 MB	2.8×10^{-3}s	27	2.4K
33	8589934592	1 GB	2.9 s	27	2.4K

CLOPS = circuit layout operations per second

https://quantum-computing.ibm.com/services/

https://www.tomshardware.com/news/ibm-introduces-clops-performance-standard-for-quantum-computing

5. Limitations and Next Steps

Entangled Logical Qubits (ELQ) - Department of Defense research grant opportunity

Missed deadline: 21 March 2023 (only discovered in April 2023)

Other opportunities?

https://www.arl.army.mil/collaborate-with-us/opportunity/elq/

5. Limitations and Next Steps

Fall 2023 – M.Sc. thesis defense

Research Grants for Graduate Students (RGGS) awarded - $479 for two NVIDIA T600 GPU's

THANK YOU!