SP2023 Week 06 • 2023-03-02

Quantum Computing

George

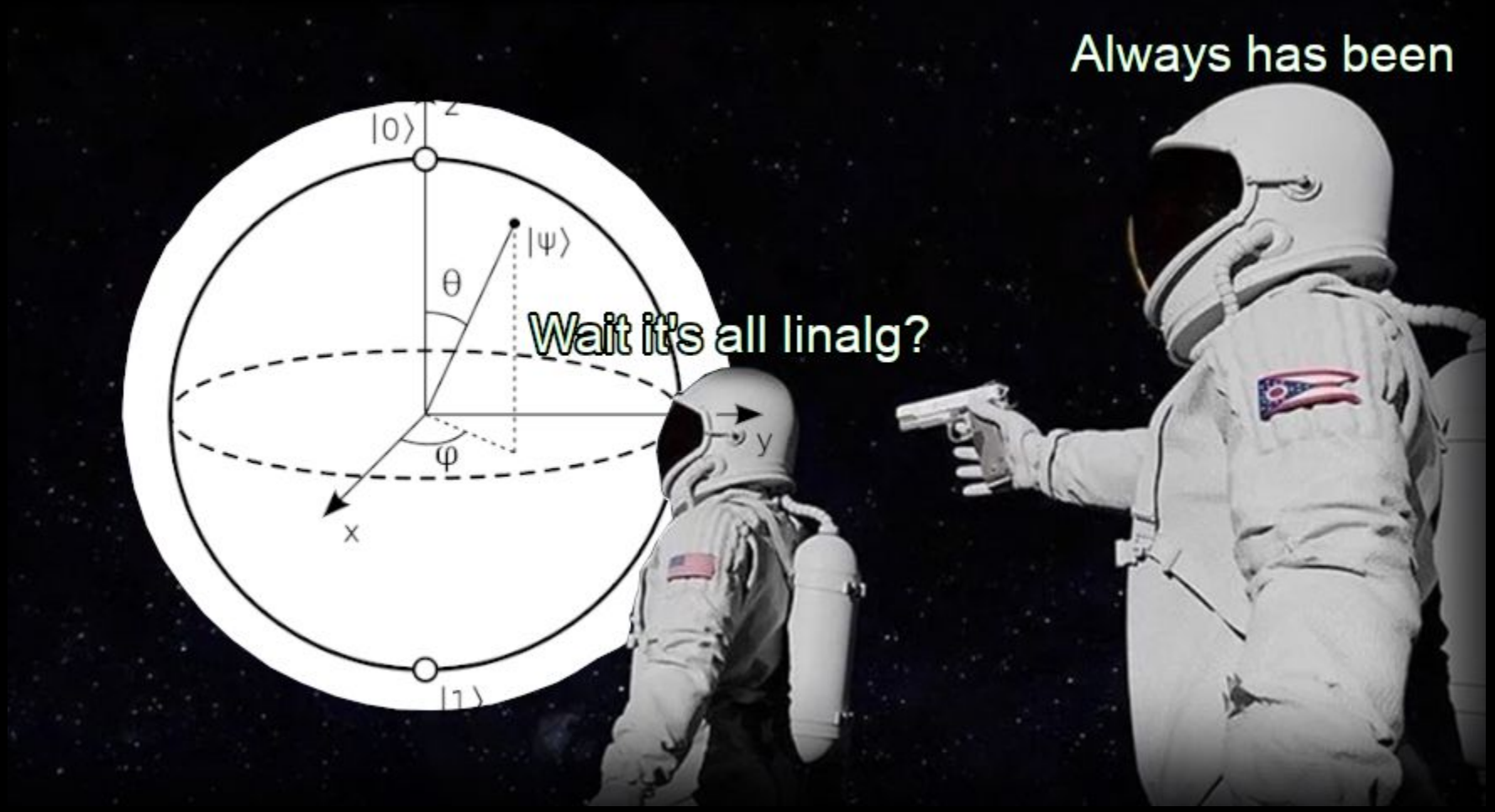
Announcements

- Our scavenger hunt with WiCyS has been moved to April 15!
  - New signup link here: https://forms.gle/GJrSnRzTZxvvLNSz5

- Social next Thursday
  - Take an hour to relax with us!

ctf.sigpwny.com

sigpwny{qu4n7um4n14_15_f4k3}



Disclaimer

- I have no idea what I'm talking about!
- Theorists, don't kill me
  - Take ECE 305, ECE 406, PHYS 214, PHYS 398 to learn more
- Quantum computing is very confusing and a relatively new type of challenge in CTF: ask for help!

Quantum Primer

- Qubits
  - Bloch Sphere
- Circuits
  - Other models exist: Quantum Turing Machines, ZX-Calculus
  - algassert.com/quirk
- Hardware
  - Superconducting, Ion-trap
  - Simulators

What Makes Qubits Special

- Superposition
  - Having a certain amount of 0-ness and 1-ness simultaneously
  - This alone can encode arbitrary amounts of information
- Entanglement
  - Make qubits best friends 4 ever
  - Schrödinger’s cat
- Interference
  - All sorts of tricks to make the math “work out” to pick out your desired state(s)

Brief Math Interlude

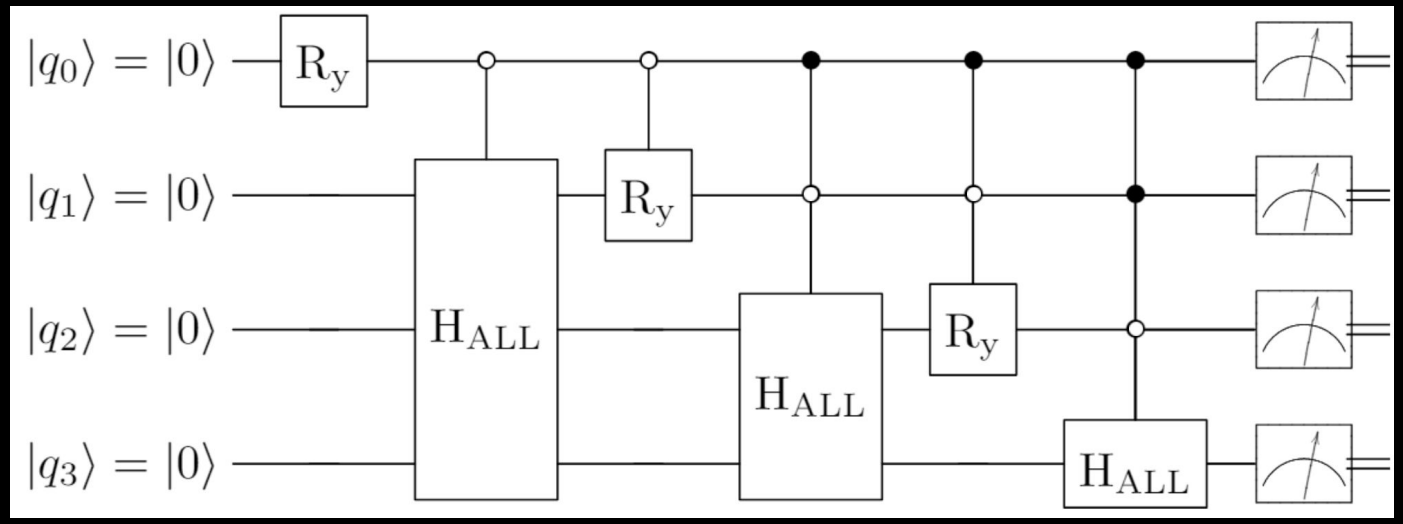
Circuits/gates are just unitary matrices

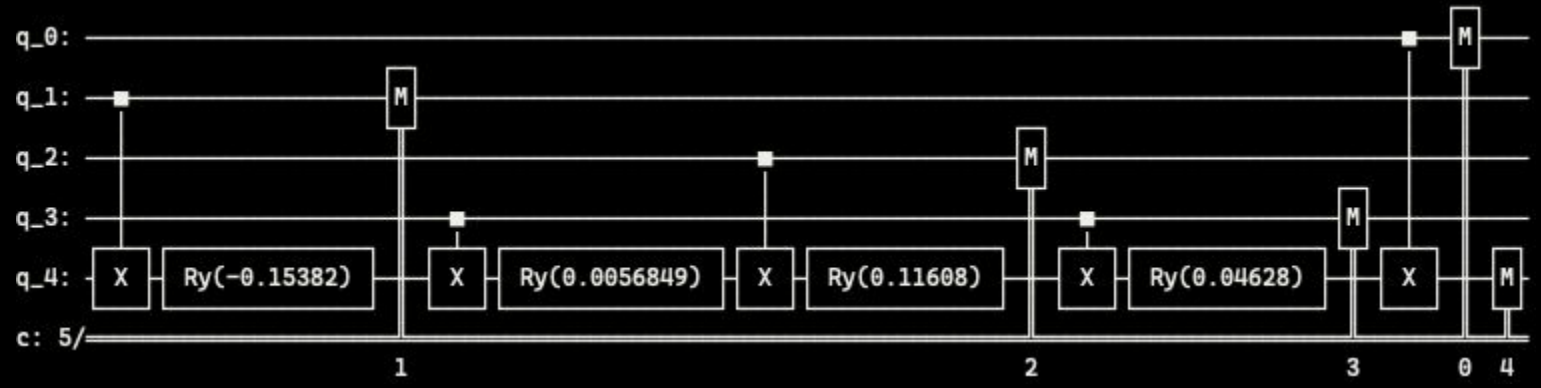
Notation:

- $|0\rangle, |1\rangle$ are classical 0 and 1
- You can “concatenate” (read: tensor product) kets together to form a register like so: $|0\rangle \otimes |1\rangle = |01\rangle$, $|0\rangle^{\otimes n} = |\underbrace{0 \ldots 0}_{n}\rangle$

Don’t calculate anything by hand: use `numpy`!

Circuit Diagrams





Quantum Gates

Useful gates:

- Hadamard, R_X, R_Y, R_Z, SWAP

Controlled gates: if statement's buff cousin

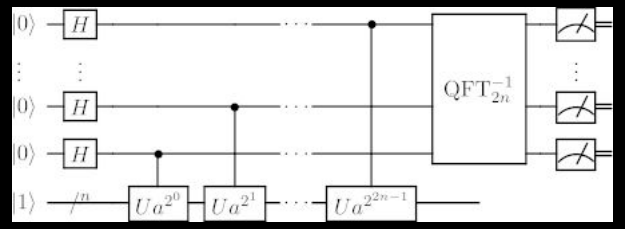
- How you get entanglement!
- You can control any gate

The Quantum Speedup

Fourier Transform

⚡Blazingly fast⚡

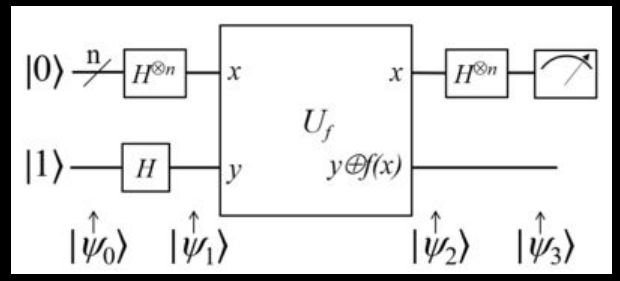
Used as a component of many, many quantum algorithms



$$O(2^n) \rightarrow O(n^2)$$

Search

Given a black box function, find the unique input that produces a given output.



$$O(n) \rightarrow O(\sqrt{n})$$

Simulation

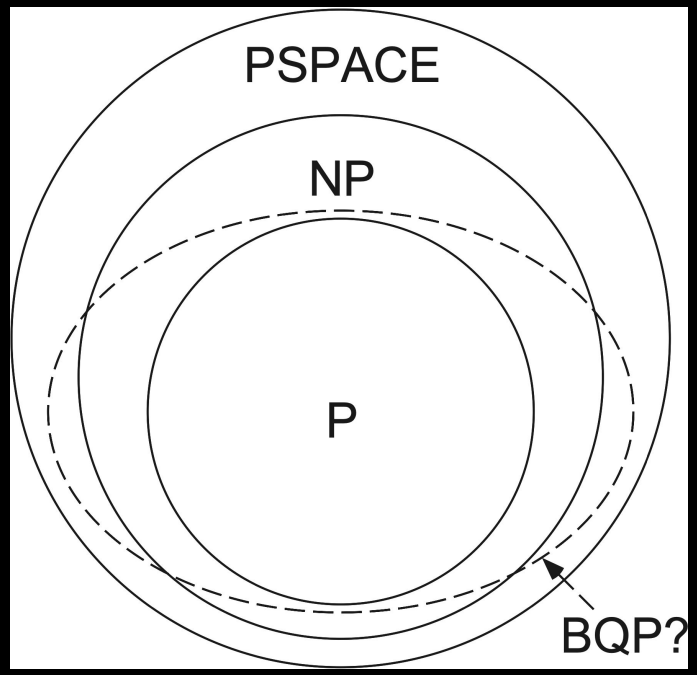
Creating new proteins, materials, medicines

Quantum corollary to Moore's Law

$$O(c^n) \rightarrow O(n)$$

A New Hope

- Not all problems in NP are in **B**ounded-error **Q**uantum **P**olynomial complexity class (probably…)
- Elliptic curve cryptography, lattices (CRYSTALS-Kyber)



Caveats

- No-cloning theorem
- No-teleportation theorem
- Ancilla qubits
- Hardware is fickle
  - Largest quantum computer at time of writing is IBM Osprey (433 qubits)
- Qubits decohere quickly, gates are imperfect, and there's noise everywhere — what to do?
  - Error correction!

Qiskit

pwntools, But Quantum!

Almost all challenges are either running a quantum circuit locally (OpenQASM) or applying gates to a server

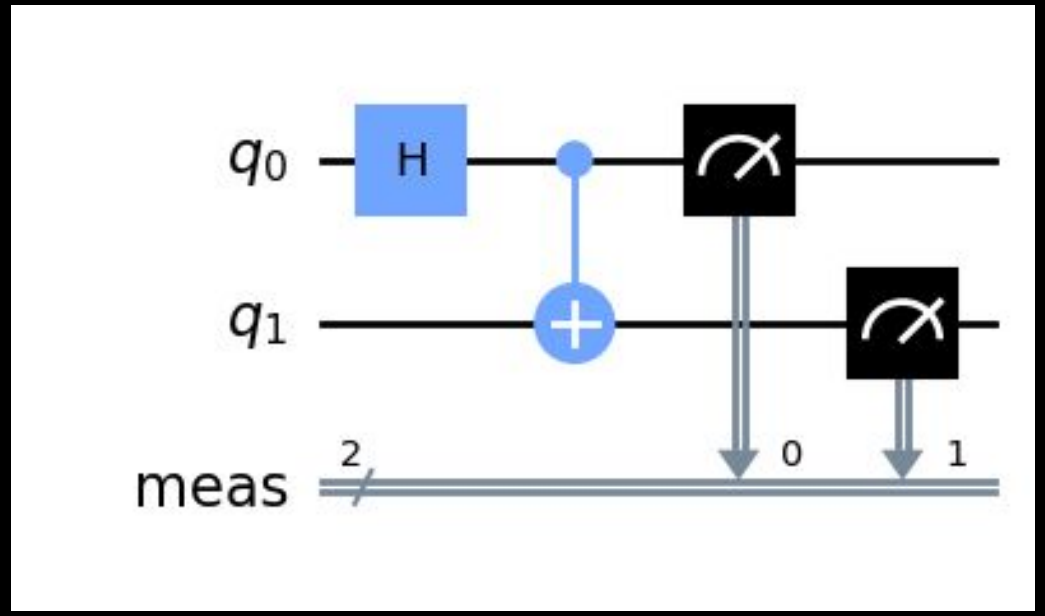
Create circuit ⟹ Apply gates ⟹ Simulate ⟹ Post-processing

```
pip install qiskit[visualizations]
```

Example: Entanglement

```
from qiskit import *

circ = QuantumCircuit(2)
circ.h(0)
circ.cx(0, 1)
circ.measure_all()
```



DiceCTF 2023: super-qomputer

“Just run the program and it prints the flag: assuming you have a quantum computer available”

Given `challenge.7z`, which decompresses to `challenge.qasm`

Intuition: How can this be efficiently simulated?

DiceCTF 2023: super-qomputer

```
circ = QuantumCircuit.from_qasm_file("challenge.qasm")
sim = Aer.get_backend("aer_stabilizer_simulator")
res = execute(circ, sim, shots=1).result()
bin_num = list(res.get_counts(0).keys())[0]
print(int(bin_num[:len(bin_num)//2], 2).to_bytes(41, "big"))
```

CSAW 22 CTF Qual: quantum-leap

“My friend took the quantum leap and purchased a quantum computer with two qubits. They mentioned using a quantum logic gate to input the flag and they gave me the computers output. I have been stuck and Can NOT figure out the flag.”

Output: `wxqvn$Zae${deyZv$d"i`

Intuition: Something with CNOTs; check the output format

CSAW 22 CTF Qual: quantum-leap

```
output = "wxqvn$Zae${deyZv$d\\\"i"
wow = ''.join([format(ord(x), '08b') for x in output])
for i in range(0, len(wow), 2):
    qc, output = XOR(wow[i], wow[i+1])
    tmp += output
print(binary2string(tmp))
```

Resources

Qiskit Textbook

Xanadu Quantum Codebook *(uses Pennylane!)*

MITRE Intro to Quantum Software Development

quantumcomputing.stackexchange

Resources (For Nerds)

Quantum Information and Quantum Computation, *Michael Nielsen and Isaac Chuang*

From Classical to Quantum Shannon Theory, *Mark Wilde*

arXiv > quant-ph

Next Meetings

2023-03-05 - This Sunday

- Fuzzing with Richard and Juniper
- Learn what fuzzing is and how to use a fuzzer to find vulnerabilities!

2023-03-09 - Next Thursday

- Social!
- Chill with us as spring break nears

sigpwny{qu4n7um4n14_15_f4k3}