

# Quantum Floyd–Hoare Verification and its Implementations

Samantha Norrie

A dark blue diagonal gradient bar that starts from the bottom left and extends towards the top right, covering the lower half of the slide.

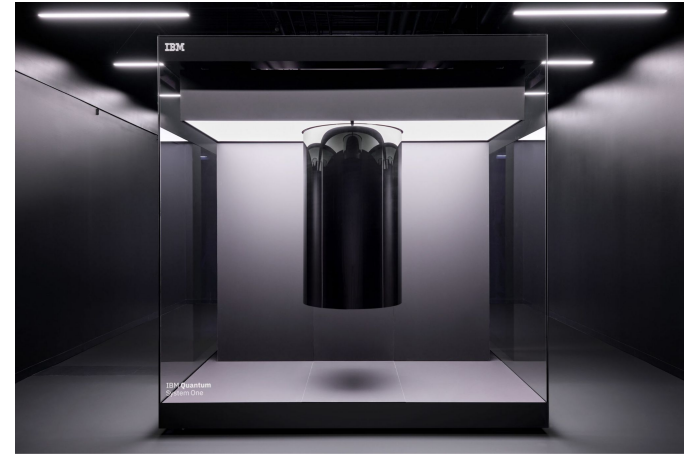
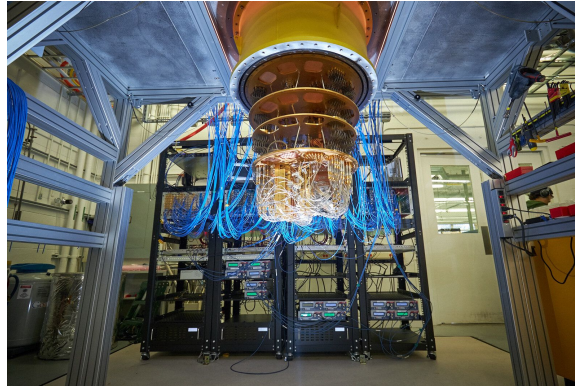
# Quantum Computing Introduction



# What is Quantum Computing?

Quantum Computing is a multidisciplinary field that focuses on harnessing the power of Quantum Mechanics to compute and solve problems that have been thought to be unsolvable [1]. Some of the fields involved in Quantum Computing include Physics, Biology, Chemistry, Computer Science, Software Engineering, Electrical Engineering, and Mechanical Engineering.

The Computer Science and Software Engineering research within Quantum Computing largely revolves around the creation and implementation of Quantum algorithms (which often are inspired by classical algorithms) as well as the creation of fault-tolerant Quantum Software.



## Development Roadmap

IBM Quantum

	2016–2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2033+
	Run quantum circuits on the IBM Quantum Platform	Release multi-dimensional roadmap publicly with initial aim focused on scaling	Enhancing quantum execution speed by 100x with Qiskit Runtime	Bring dynamic circuits to unlock more computations	Enhancing quantum execution speed by 5x with quantum serverless and Execution modes	Improving quantum circuit quality and speed to allow 5K gates with parametric circuits	Enhancing quantum execution speed and parallelization with partitioning and quantum modularity	Improving quantum circuit quality to allow 7.5K gates	Improving quantum circuit quality to allow 10K gates	Improving quantum circuit quality to allow 15K gates	Improving quantum circuit quality to allow 100M gates	Beyond 2033, quantum-centric supercomputers will include 1000's of logical qubits unlocking the full power of quantum computing
Data Scientist						Platform	Code assistant	Functions	Mapping Collection	Specific Libraries		General purpose QC libraries
Researchers						Middleware						
Quantum Physicist						Quantum Serverless	Transpiler Service	Resource Management	Circuit Knitting + P	Intelligent Orchestration		Circuit libraries
			Qiskit Runtime									
	IBM Quantum Experience		QASM3	Dynamic circuits	Execution Modes	Heron (5K) Error Mitigation 5k gates 133 qubits Classical modular 133x3 = 399 qubits	Flamingo (5K) Error Mitigation 5k gates 156 qubits Quantum modular 156x7 = 1092 qubits	Flamingo (7.5K) Error Mitigation 7.5k gates 156 qubits Quantum modular 156x7 = 1092 qubits	Flamingo (10K) Error Mitigation 10k gates 156 qubits Quantum modular 156x7 = 1092 qubits	Flamingo (15K) Error Mitigation 15k gates 156 qubits Quantum modular 156x7 = 1092 qubits	Starling (100M) Error correction 100M gates 200 qubits Error corrected modularity	Blue Jay (1B) Error correction 1B gates 2000 qubits Error corrected modularity
	Early Canary 5 qubits Albatross 16 qubits Penguin 20 qubits Prototype 53 qubits	Falcon Benchmarking 27 qubits		Eagle Benchmarking 127 qubits								

## Innovation Roadmap

Software Innovation	IBM Quantum Experience	Qiskit Circuit and operator API with compilation to multiple targets	Application modules Modules for domain specific application and algorithm workflows	Qiskit Runtime Performance and abstract through Primitives	Serverless Demonstrate concepts of quantum-centric supercomputing	AI enhanced quantum Prototype demonstrations of AI enhanced circuit transpilation	Resource management System partitioning to enable parallel execution	Scalable circuit knitting Circuit partitioning with classical reconstruction at HPC scale	Error correction decoder Demonstration of a quantum system with real-time error correction decoder			
Hardware Innovation	Early Canary 5 qubits Albatross 16 qubits	Falcon Demonstrate scaling with I/O routing with Bump bonds	Hummingbird Demonstrate scaling with multiplexing readout	Eagle Demonstrate scaling with MLW and TSV	Osprey Enabling scaling with high density signal delivery	Condor Single system scaling and fridge capacity	Flamingo Demonstrate scaling with modular connectors	Kookaburra Demonstrate scaling with nonlocal c-coupler	Demonstrate path to improved quality with logical memory	Cockatoo Demonstrate path to improved quality with logical communication	Starling Demonstrate path to improved quality with logical gates	
						Heron Architecture based on tunable-couplers	Crossbill m-coupler					

Executed by IBM

On target

Noisy Intermediate Scale  
Quantum Era = NISQ Era



# Qiskit

Elements for building a quantum future

# Qubits

The bit equivalent for Quantum Computers

A qubit can exist as 0, 1, or as a state in between 0 and 1

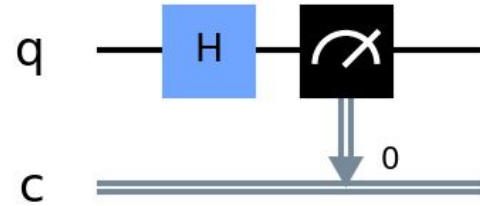
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1.$$

# Superposition

A qubit is in superposition when it is neither completely  $|0\rangle$  or  $|1\rangle$

Measuring a qubit takes it out of superposition and forces it to return a classical value (0 or q)



*The application of the Hadamard gate to a single qubit, which is then measured to a classical bit*



# The Hadamard Gate: One of the stars of Quantum Computing

Puts a qubit into equal superposition

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

$$|0\rangle \longrightarrow \boxed{H} \longrightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|1\rangle \longrightarrow \boxed{H} \longrightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

remember  $|\alpha|^2 + |\beta|^2 = 1.$

# Why the negative?

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & \ominus 1 \end{pmatrix}$$



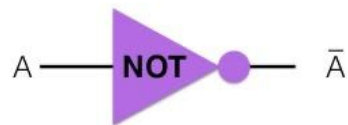
Denotes a negative **relative phase** (out of scope for today's presentation)!

It is important to note that the negative relative phase does not impact measurement probabilities due to

$$|\alpha|^2 + |\beta|^2 = 1.$$

# The NOT (Pauli X) gate

Just like a classical NOT gate



$A$	$\bar{A}$
0	1
1	0

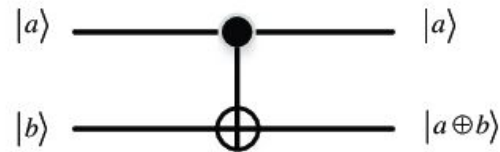
PAULI X GATE



$ A\rangle$	$ \bar{A}\rangle$
0	1
1	0

# The CNOT (Controlled Not) Gate

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



# Entanglement and Bell States

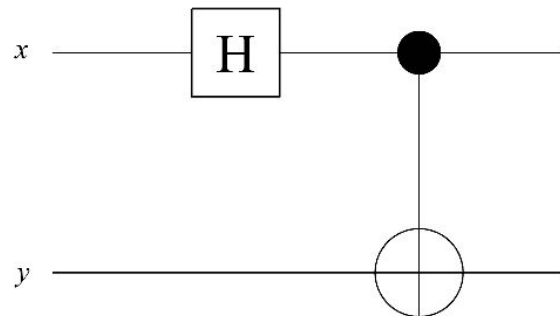
When qubits are entangled, the measurement of one instantly reveals the state of another

Bell States are simple two-qubit examples of entangled states

They only have two possible states

There are **four** two-qubit Bell states

Jupyter Notebook Exercise 1



$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

One of the Bell States

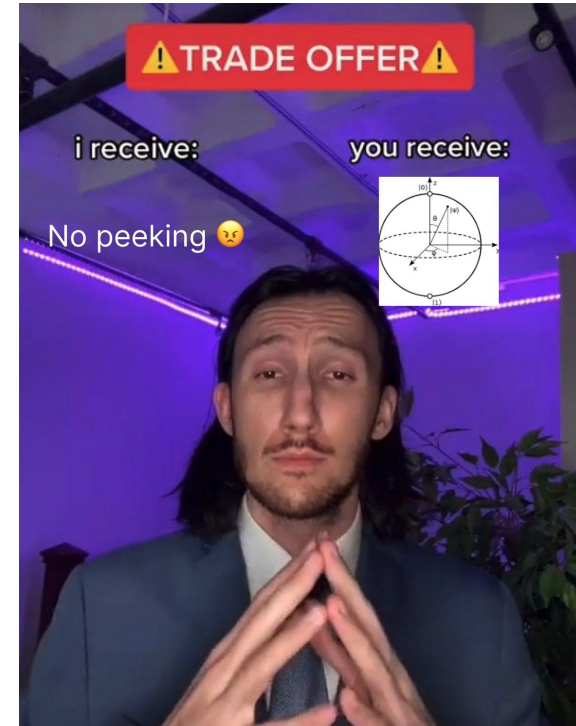
# Entanglement

When qubits are entangled, the measurement of one instantly reveals the state of another

# Quantum Computing Con: No Peeking

Measuring a qubit immediately returns a binary value, taking the qubit and any qubits entangled to it out of superposition

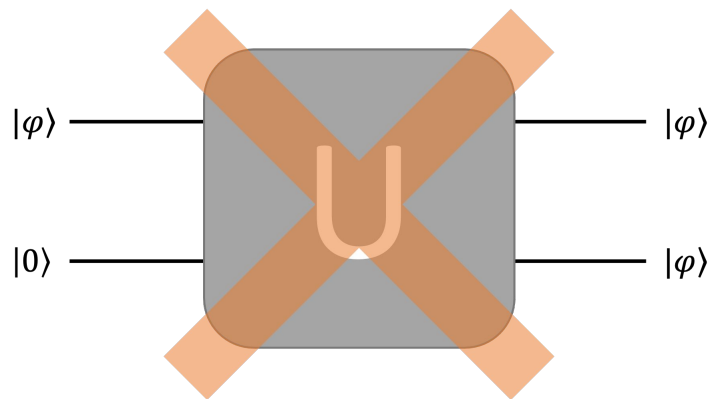
This can be referred to as the quantum measurement problem or the collapse of the wave function (useful when talking about quantum from a Quantum Mechanics perspective)



# Quantum Computing Con: No-Cloning Theorem

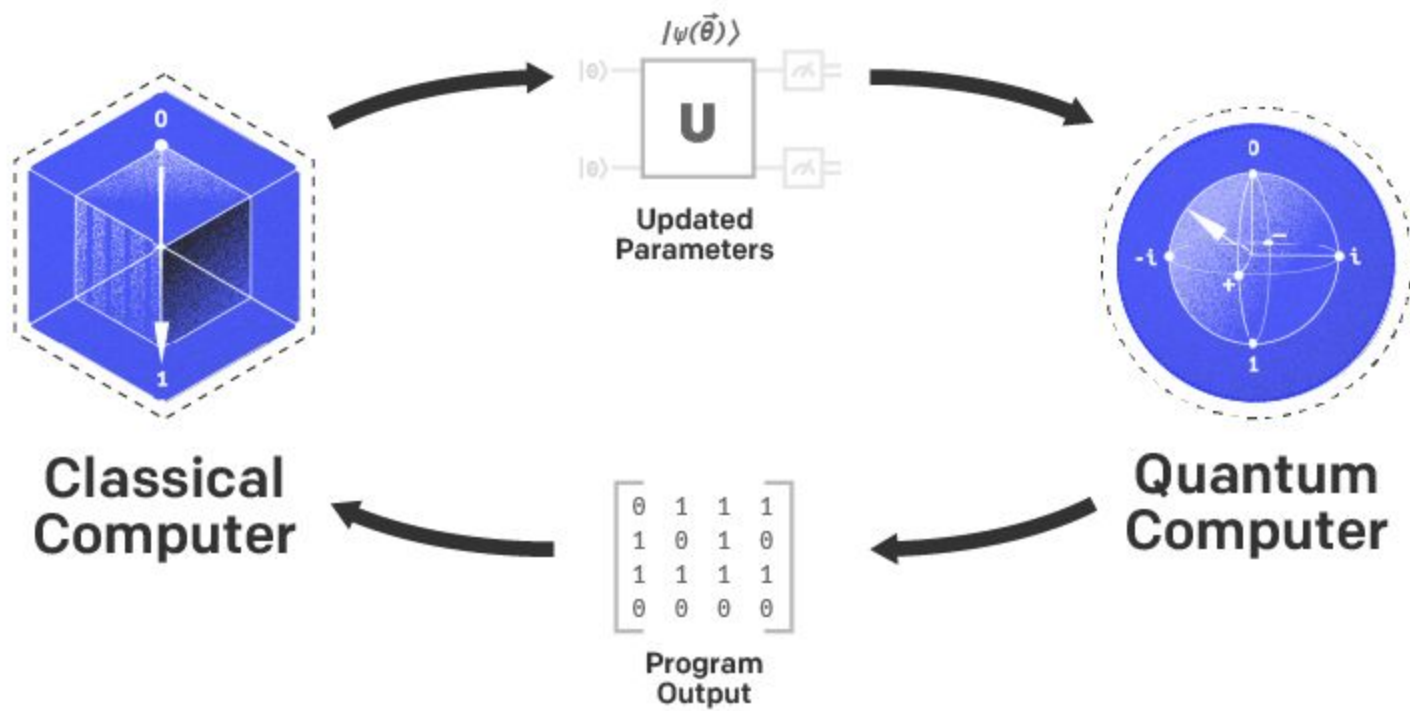
Unlike in classical computing, a value cannot be copied from one qubit to another. This is referred to as the *No-Cloning Theorem*

It is important to note that a qubit's value can be teleported, that is the value can be moved to another qubit, but the value at the original qubit will be destroyed.

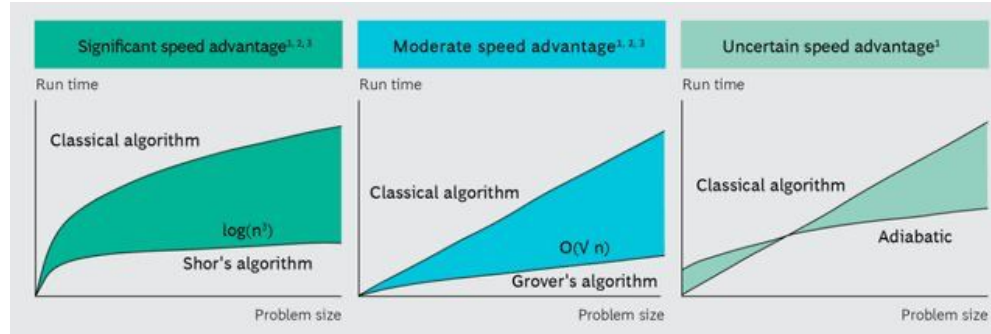


No-Cloning Theorem





# Quantum Computing Pros



Significant algorithmic speedup, leading to advancements in cryptography, machine learning, and chemistry.

# Classical Floyd-Hoare Verification: A Review



# Floyd–Hoare Verification aims to prove correctness by using different rules

1. The assignment axiom  $\{P[x/e]\} x = e \{P\}$
2. The sequential composition rule  $\{P\} C1 \{Q\}, \{Q\} C2 \{R\} \Rightarrow \{P\} C1; C2 \{R\}$
3. The conditional rule  $\{P \wedge B\} C1 \{Q\}, \{P \wedge \neg B\} C2 \{Q\} \Rightarrow \{P\} \text{ if } B \text{ then } C1 \text{ else } C2 \{Q\}$
4. The while loop rule  $\{P \wedge B\} C \{P\} \Rightarrow \{P\} \text{ while } B \text{ do } C \{P \wedge \neg B\}$
5. The consequence rule  $P' \Rightarrow P, \{P\} C \{Q\}, Q \Rightarrow Q' \Rightarrow \{P'\} C \{Q'\}$

$$\{P\} \ c \ \{Q\}$$

*If the precondition (P) is true before the execution of program @, then postcondition (Q) will be met []*

So, how does Quantum Floyd–Hoare Verification differ from Classical Floyd–Hoare Verification?

# *Quantum Floyd–Hoare* is new and evolving!

Many new definitions have  
been being created as Quantum  
Computing has started  
becoming more and more  
popular

# Quantum Floyd–Hoare Verification Version 1

Proposed by Mingsheng Ying



# Notation

$$\{P\}S\{Q\}$$



# Notation

New letter!  $S$  is used to denote  
quantum program


$$\{P\}S\{Q\}$$

# Notation

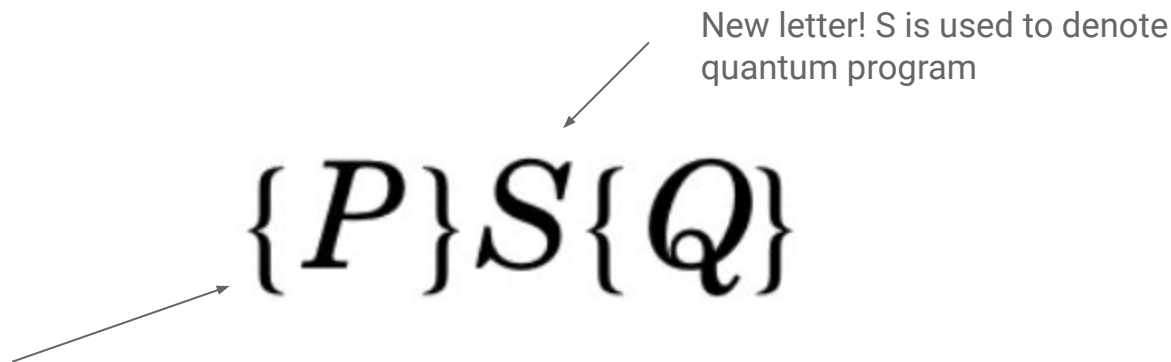
New letter!  $S$  is used to denote quantum program



$\{P\}S\{Q\}$

In order for classical Floyd-Hoare to work for quantum programs, the notions of weakest precondition and weakest liberal precondition must be used in order to ensure relative completeness.

# Notation



New letter! S is used to denote quantum program

$$\{P\}S\{Q\}$$

In order for classical Floyd-Hoare to work for quantum programs, the notions of weakest precondition and weakest liberal precondition must be used in order to ensure relative completeness.

**Weakest precondition:** defines what must be true in order for postcondition to be satisfied using a *minimal* number of requirements

**Weakest liberal precondition:** similar to the weakest precondition, only it accounts for non-deterministic behaviour

# Rules

$$(Skip) \quad \overline{\langle \mathbf{skip}, \rho \rangle \rightarrow \langle E, \rho \rangle}$$

$$(Initialization) \quad \overline{\langle q := 0, \rho \rangle \rightarrow \langle E, \rho_0^q \rangle}$$

$$(Sequential Composition) \quad \frac{\langle S_1, \rho \rangle \rightarrow \langle S'_1, \rho' \rangle}{\langle S_1; S_2, \rho \rangle \rightarrow \langle S'_1; S_2, \rho \rangle}$$

$$(Measurement) \quad \overline{\langle \mathbf{measure} \ M[\bar{q}] : \bar{S}, \rho \rangle \rightarrow \langle S_m, M_m \rho M_m^\dagger \rangle}$$

$$(Loop\ 0) \quad \overline{\langle \mathbf{while} \ M[\bar{q}] = 1 \ \mathbf{do} \ S, \rho \rangle \rightarrow \langle E, M_0 \rho M_0^\dagger \rangle}$$

$$(Loop\ 1) \quad \overline{\langle \mathbf{while} \ M[\bar{q}] = 1 \ \mathbf{do} \ S, \rho \rangle \rightarrow \langle S; \mathbf{while} \ M[\bar{q}] = 1 \ \mathbf{do} \ S, M_1 \rho M_1^\dagger \rangle}$$

# Rules

$$(Skip) \quad \overline{\langle \mathbf{skip}, \rho \rangle \rightarrow \langle E, \rho \rangle}$$

Qubits are always initialized to zero

$$(Initialization) \quad \overline{\langle q := 0, \rho \rangle \rightarrow \langle E, \rho_0^q \rangle}$$

$$(Sequential\ Composition) \quad \frac{\langle S_1, \rho \rangle \rightarrow \langle S'_1, \rho' \rangle}{\langle S_1; S_2, \rho \rangle \rightarrow \langle S'_1; S_2, \rho \rangle}$$

Classical measurement

$$(Measurement) \quad \overline{\langle \mathbf{measure} \ M[\bar{q}] : \bar{S}, \rho \rangle \rightarrow \langle S_m, M_m \rho M_m^\dagger \rangle}$$

Classical measurement

$$(Loop\ 0) \quad \overline{\langle \mathbf{while} \ M[\bar{q}] = 1 \ \mathbf{do} \ S, \rho \rangle \rightarrow \langle E, M_0 \rho M_0^\dagger \rangle}$$

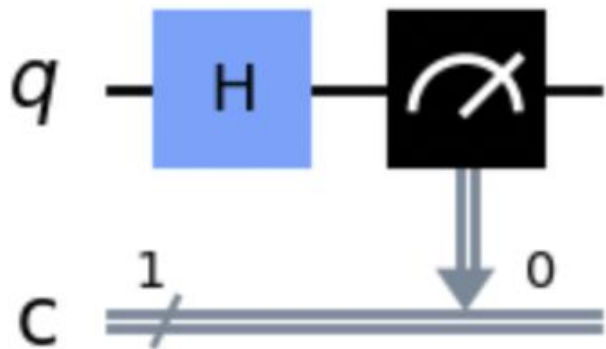
$$(Loop\ 1) \quad \overline{\langle \mathbf{while} \ M[\bar{q}] = 1 \ \mathbf{do} \ S, \rho \rangle \rightarrow \langle S; \mathbf{while} \ M[\bar{q}] = 1 \ \mathbf{do} \ S, M_1 \rho M_1^\dagger \rangle}$$

# A Quick note on types

In Ying's Quantum-Floyd Hoare Verification, variables can be of type Boolean or Integer

I won't be using integers in today's examples, but they will be briefly mentioned later

# An example using a Hadamard gate



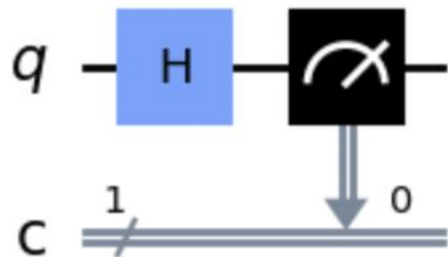
Good precondition and postcondition?

Assert that the quantum state is valid *before* and *after* the quantum program (S) has executed.

$$|\alpha|^2 + |\beta|^2 = 1.$$

$$S \equiv q := 0; q := Hq; \mathbf{measure} \ M[q] : \overline{S},$$

# An example using a Hadamard gate



$$S \equiv q := 0; q := Hq; \mathbf{measure} \ M[q] : \bar{S},$$

$S$  = our quantum state (our quantum program)

$p$  = the current state(s) of our quantum state

$$\langle S, \rho \rangle \rightarrow \langle q := Hq; \mathbf{measure}, \rho \rangle$$

$$\rightarrow \langle \mathbf{measure}, |+\rangle_q \left\langle +| \otimes \bigotimes_{q' \neq q} |0\rangle_{q'} \right\rangle_{q'} \langle 0| \rangle$$

$$\rightarrow \begin{cases} \langle S_0, \frac{1}{2}|0\rangle_q \langle 0| \otimes \bigotimes_{q' \neq q} |0\rangle_{q'} \langle 0| \rangle \rightarrow \langle E, \frac{1}{2}\rho \rangle, \\ \langle S_1, \frac{1}{2}|1\rangle_q \langle 1| \otimes \bigotimes_{q' \neq q} |0\rangle_{q'} \langle 0| \rangle \rightarrow \langle E, \frac{1}{2}\rho \rangle, \end{cases}$$



# An example using a Hadamard gate

$$\langle S, \rho \rangle \rightarrow \langle q := Hq; \mathbf{measure}, \rho \rangle$$

$$\rightarrow \langle \mathbf{measure}, |+\rangle_q \left\langle +| \otimes \bigotimes_{q' \neq q} |0\rangle_{q'} \right\rangle_{q'} \langle 0| \rangle$$

$$\rightarrow \begin{cases} \langle S_0, \frac{1}{2} |0\rangle_q \langle 0| \otimes \bigotimes_{q' \neq q} |0\rangle_{q'} \langle 0| \rangle \rightarrow \langle E, \frac{1}{2} \rho \rangle, \\ \langle S_1, \frac{1}{2} |1\rangle_q \langle 1| \otimes \bigotimes_{q' \neq q} |0\rangle_{q'} \langle 0| \rangle \rightarrow \langle E, \frac{1}{2} \rho \rangle, \end{cases}$$

S = our quantum state (our quantum program)

p = the current state(s) of our quantum state

# An example using a Hadamard gate

$$\langle S, \rho \rangle \rightarrow \langle q := Hq; \mathbf{measure}, \rho \rangle$$

$$\rightarrow \langle \mathbf{measure}, |+\rangle_q \rangle$$

$|0\rangle H$

$$\rightarrow \begin{cases} \langle S_0, \frac{1}{2}|0\rangle_q \\ \langle S_1, \frac{1}{2}|1\rangle_q \end{cases}$$

$|\alpha|^2$

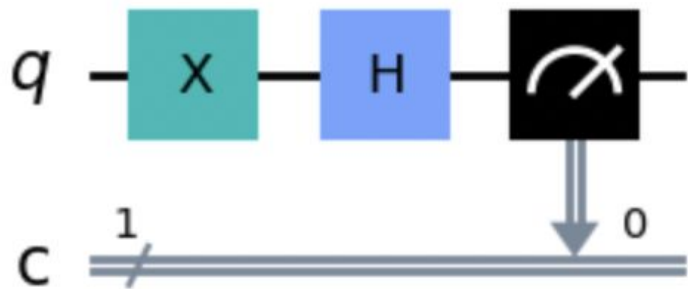
$$\rightarrow \begin{cases} \langle E, \frac{1}{2}\rho \rangle, \\ \langle E, \frac{1}{2}\rho \rangle, \end{cases}$$

$|\beta|^2$

$S$  = our quantum state (our quantum program)  
 $p$  = the current state(s) of our quantum state

$$|\alpha|^2 + |\beta|^2 = 1.$$

# Exercise Two



Hint:  $|-\rangle = |1\rangle H$

# My solution

$\langle S$

Pre-Condition: Does  $107$  satisfy  $p=1$

Yes! Because  $1 + 0 = 1$

$\langle S, p \rangle \rightarrow \langle q : s \text{ Hxq; measure, } p \rangle$

$\rightarrow \text{measure, } 1 + \frac{1}{2}, \text{ } \infty \rightarrow -$

$\rightarrow \begin{cases} \langle S_0, \frac{1}{2}, 107q \rangle \rightarrow \langle E, \frac{1}{2}, p \rangle, \\ \langle S_1, \frac{1}{2}, 107q \rangle \rightarrow \langle E, \frac{1}{2}, p \rangle \end{cases}$

Post-Condition

$$1 = \frac{1}{2} + \frac{1}{2}$$

//

$$\left| \frac{1}{\sqrt{2}} \right|^2$$

$$\left| \frac{1}{\sqrt{2}} \right|^2$$

# Is Ying's Quantum Floyd-Hoare Verification correct?

It can be both partially correct and totally correct.

Any quantum program using Ying's Quantum Floyd-Hoare Verification will be partially correct (complete and sound).

What distinguishes whether it is partially correct or totally correct is the while loop rule used.

In order for the formal method to be totally correct, the while loop rule must be bounded by the number of iterations used.

# Mini example

Using the Born rule!

# Quantum Floyd–Hoare Verification with Ghost variables

Proposed by Dominique Unruh



$\mathbf{c}, \mathbf{d} ::= \underline{\text{apply}}\ U\ \underline{\text{to}}\ \mathbf{X} \mid \underline{\text{init}}\ \mathbf{x} \mid \underline{\text{if}}\ \mathbf{y}\ \underline{\text{then}}\ \mathbf{c}\ \underline{\text{else}}\ \mathbf{d} \mid \underline{\text{while}}\ \mathbf{y}\ \underline{\text{do}}\ \mathbf{c} \mid \mathbf{c}; \mathbf{d} \mid \underline{\text{skip}}$



But first, the syntax being used



# What are ghost variables

Ghost variables are variables that are only visible in the precondition and the postcondition. They are often referred to as 'ghosts'.

Program variables are variables that are visible in the precondition, program, and postcondition

$$X = y^3$$

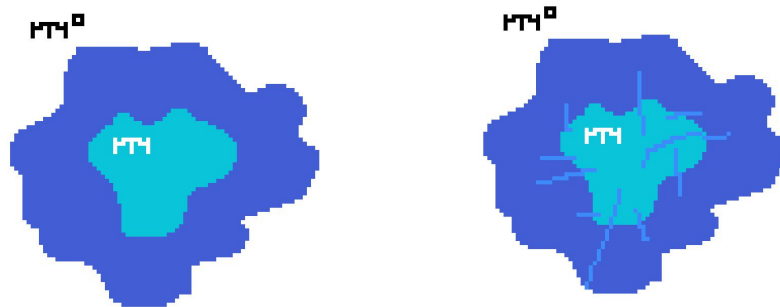
With classical Floyd-Hoare verification, we say that the postcondition above is only true if  $x$  and  $y$  satisfy it *and* that they are both **program variables**

With ghost variables, the postcondition is satisfied if it is possible to assign any value (ex. Of natural numbers, integers, .etc).

# Isn't this too vague?

In the classical case, yes...

# But ghosts can be used to help describe quantum system



$M$  = programming variable set

$M'$  = programming and ghost variable set (called 'mixed memory')

Programming and ghost variables can be entangled, but the decision to allow them to be entangled or not changes the evaluation process.

# Quantum Floyd-Hoare with Hoare Type Theory

Proposed by Kartik Singhal

# What is Hoare Type Theory?

Even the Hoare Triple has a type. It is referred to as a *constructor*.  $x$  is returned from the system.  $A$  is  $x$ 's type.

Hoare Type Theory asserts that each term in a system has a type

$$\{P\} \ c \ \{Q\}$$



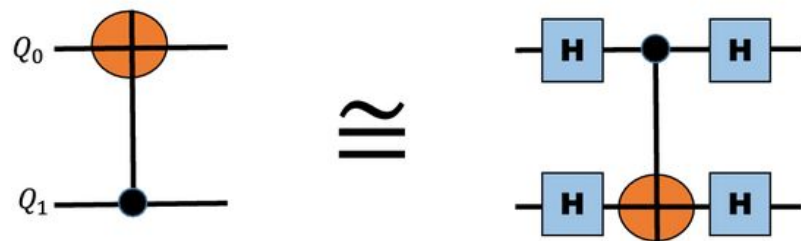
$$\Delta. \{P\} \ x : A \ \{Q\}$$

# A few rules before we go any further

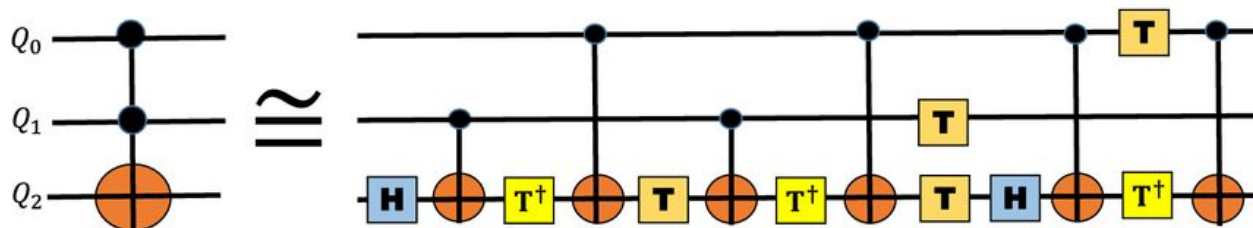
- We must assume that we are working in a universe with countably infinite qubits
- We must assume that only one-qubit and two-qubit gates exist in our world

Is the latter a major issue? Not particularly! The current quantum space is very much like this.

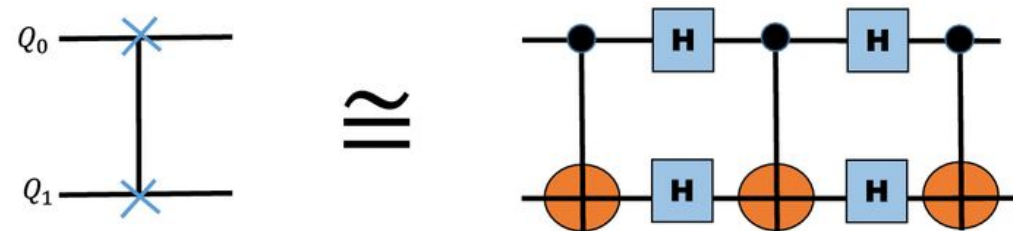
(a)



(b)



(c)



# Notation for Floyd–Hoare Verification with Hoare Type Theory

(Inspired by Unruh and  $F^*$ )



# Some functions and symbols

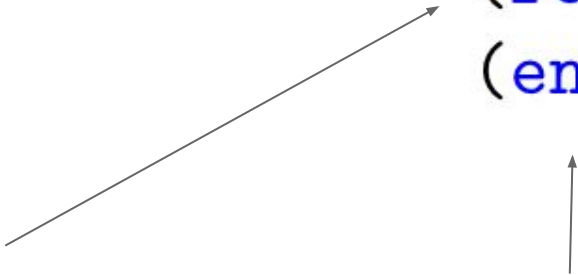
- `class(X)` returns true if X holds a classical state
- `separable(X)` returns true if X is separable (i.e. that it is not entangled with another system)
- T corresponds to the complete state space (when used as a boolean, it always evaluates to true)

# Initialization Notation

```
init : (b: bit) → QST (q: qbit)  
      (requires {⊤})  
      (ensures  {q =q |b⟩}))
```

# Initialization Notation

`init` : (b: bit)  $\rightarrow$  QST (q: qbit)  
(requires { $\top$ })  
(ensures {q =<sub>q</sub> |b⟩})



Evaluates to true. We can always initialize a qubit in our universe of countably infinite qubits

A qubit with the classical value of b will always be created

# Measurement Notation

```
meas : (q: qbit) → QST (x: bit)
```

$$\{\psi: \text{vector}, e_x \leftarrow \text{qbit}\}$$

Asserts that  $q$  exists in our quantum space

$$(\text{requires } \{(q \otimes_{\mathcal{H}} [V \setminus q]) =_q \psi\})$$
$$(\text{ensures } \{\text{class}(q) \wedge (e_x \otimes \mathcal{H}[V \setminus q]) =_q \psi\})$$

a ghost variable

q is measured to a classic value

Ghost variable is used to check that

# Measurement Notation

```
meas : (q: qbit) → QST (x: bit)
      {ψ: vector, ex: qbit}
      (requires {(q ⊗ ℋ[V\q]) =q ψ})
      (ensures {class(q) ∧ (ex ⊗ ℋ[V\q]) =q ψ})
```

# Unitary Gate Application Notation

```
apply _ to _ : (g: unitary) →  
               qs: (qbit  $\otimes$  qbit) →  
               QST (_: unit)  
               {P: prop}  
               (requires {P})  
               (ensures  {(g on qs) · P})
```

# Unitary Gate Application Notation

`apply _ to _ : (g: unitary) →`  
`qs: (qbit  $\otimes$  qbit) →`  
`QST (_: unit)`  
`{P: prop}`  
`(requires {P})`  
`(ensures {(g on qs) · P})`

Gates are always unitary matrices

The qubit(s) the gate will be applied to

# A Great Example From the Paper

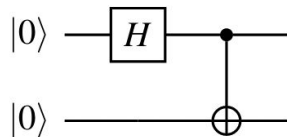


Figure 1: Circuit to prepare the first Bell state

```
1  bell100 : unit → QST (a, b): (qbit⊗qbit)
2          (requires {⊤})
3          (ensures {(a,b) =q |β00⟩})
4  bell100 = λx.do
5      a ← init 0
6      apply H to a
7      b ← init 0
8      apply CX to (a, b)
9      return (a, b)
```



# Exercise Three: Try making the Bell State you found earlier using this notation

Want to try something a bit more difficult? Try making a circuit with three qubits.

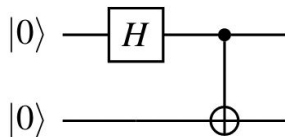


Figure 1: Circuit to prepare the first Bell state

```
1  bell100 : unit → QST (a, b): (qbit⊗qbit)
2          (requires {⊤})
3          (ensures {(a,b) =q |β00⟩})
4  bell100 = λx.do
5      a ← init 0
6      apply H to a
7      b ← init 0
8      apply CX to (a, b)
9      return (a, b)
```

# Formal Methods in Quantum Software Engineering

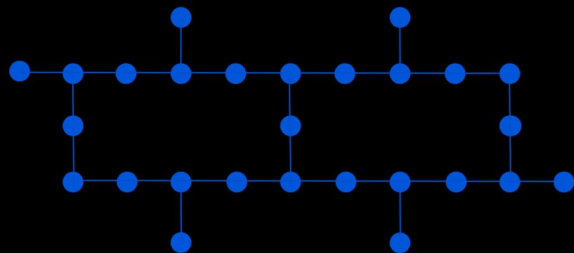
- Multiple formal methods (and multiple versions of Quantum Floyd-Hoare) have been used to describe quantum programs on paper, but not many have been used within Quantum Software Engineering
- My first hypothesis: many formal methods may not be suitable for NISQ era quantum computers (even if mathematically they are suitable)
  - Likely a scalability issue
- My second hypothesis: the application of formal methods in Quantum Computing is done within *Quantum Error Correction*

# Quantum Error Correction

An algorithmic approach to analysing and preventing unexpected behaviour that may occur while a quantum program is running.

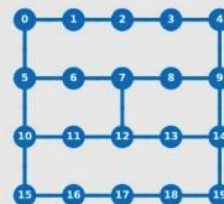
# Predictive Quantum Error Correction

IBM Quantum

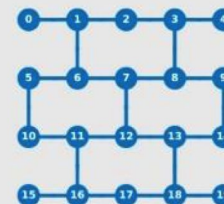


Montreal, 27 Qubits, QV64, Falcon r4

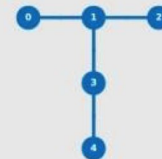
## IBM's 10 Quantum Device Lineup



Johannesburg  
Poughkeepsie



Almaden  
Boeblingen  
Singapore



Ourense  
Valencia  
Vigo

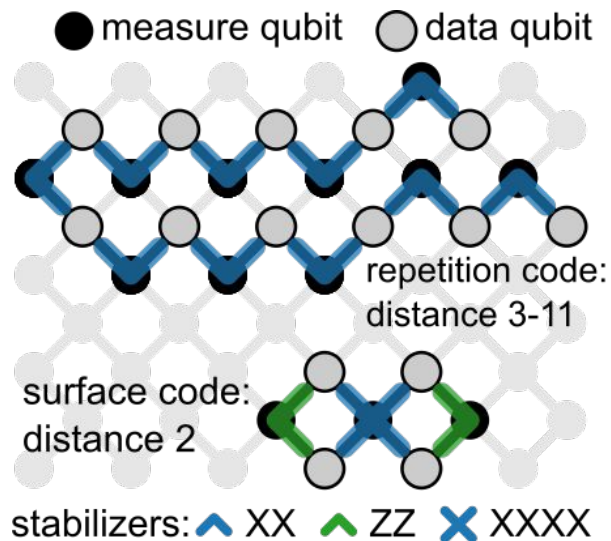
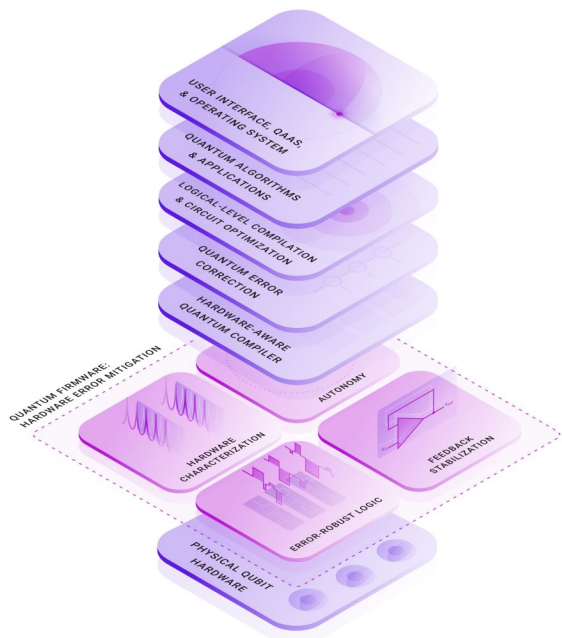


Melbourne



Yorktown

# Quantum Error Correction Within the Program



# Thank you for listening!

All references have been included in the Jupyter Notebook!