

# Quantum Computing for Programming Language Researchers

or:

I sort of understand quantum computing,  
and so can you!

Jennifer Paykin

PLanQC, January 2020

| galois |

# Quantum Computing: not so scary

quantum battery that ...  
phys.org



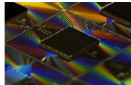
18 Quantum Flagship Project  
nbcnews.com

Quantum Theory Bends The Limits of ...  
sciencemart.com



Why Quantum Computing's Time Is Now  
forbes.com

emerged in record-breaking quantum ...  
sciencemagazine.org



Google confirms 'quantum supremacy' ...  
theverge.com



Quantum Darwinism, an idea to Explain ...  
quantummagazine.org

Quantum physics experiment shows ...  
phys.org



Quantum supremacy from Google? Not so ...  
technologyreview.com

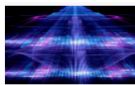
The Introduction to Quantum ...  
coursera.org



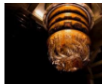
Quantum technology could revolutionise ...  
fortnummagazine.au

Quantum Mechanics Quiz | Britannica  
britannica.com

quantum supremacy not so scary ...  
physicsworld.com



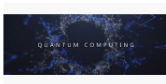
Quantum Computing  
singularityhub.com



Google's Quantum Computer Just ...  
bbcscience.com



Quantum internet just took another step ...  
technologyreview.com



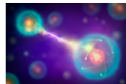
Quantum Computing 101 - Towards Data ...  
towardsdatascience.com



Quantum Computing Holds Promise for the ...  
quantum.com



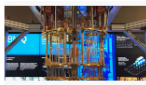
Quantum Biology May Help Solve Some of ...  
the-scientist.com



Quantum Biology ...  
sciencemagazine.com



This quantum physics breakthrough could ...  
theverge.com



Quantum computers | Damien + Magazine ...  
damien.com



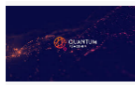
Quantum interference in the service of ...  
phys.org



Quantum Science and ...  
surge.edu



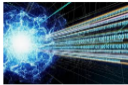
Get Ready for First Quantum Computer to ...  
metatub.com



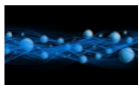
Quantum Technology | The future is Quantum  
ip.ca



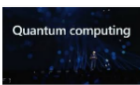
Viral 24.5 Billion Pixel Image ...  
sciencemagazine.com



quantum research ...  
news4journal.com



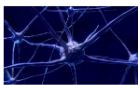
An artificial intelligence algorithm ...  
techglobe.com



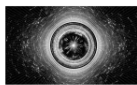
Microsoft unveils Azure Quantum to ...  
getsite.com



Intel and IBM supercomputer group at ...  
siliconpublic.com



AI is terrifying, wait until ...  
themintlab.com



Entirely Different Kind of Quantum Computer  
nbcuipform.com



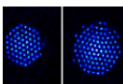
Why are scientists so excited about a ...  
goj.com



Quantum Computing 101  
nrgress.mit.edu



Quantum computing could out ...  
nucleonics.ca



Future of Quantum Information ...  
nrg.com



Negative Energy & Repulsive Gravity  
sciencedaily.com



Quantum Cryptography Demystified: How ...  
extremetech.com



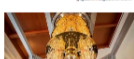
Google Quantum AI Lab's John Martinis ...  
gigamonmagazine.com



Image of quantum entanglement ...  
imgatq.com



This is your pay in quantum computing ...  
news4franciscanians.com



# Quantum Computing: not so scary

- A little linear algebra
- Interest in learning something new

# Quantum Computing: not so scary

- A little linear algebra
- Interest in learning something new

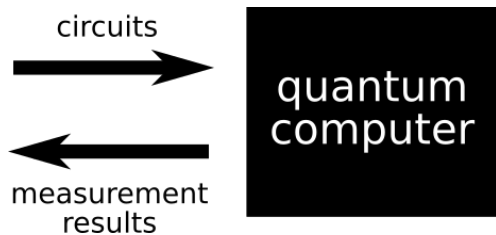
**DISCLAIMER**

I will make some generalizations in this talk... sorry!

# Outline

- 1 Quantum computers
- 2 Syntax and semantics

# Circuit model semantics



# The NISQ era

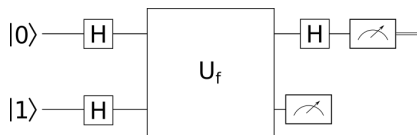
State-of-the-art quantum computers have...

- 50-100 qubits
- a variety of implementation techniques
- quantum supremacy (well, almost)
- a lot of noise introducing errors

NISQ = Noisy Intermediate-Scale Quantum

# Quantum PL

- Language design
  - Functions, data types, modularity
- Quantum circuits



Simple, intuitive,  
compositional

- Operational, denotational, categorical semantics



# Quantum PL

- Compilers, optimizations
- Algorithms
- Application areas
  - Chemistry, cryptography, machine learning...
- Logic, formal methods

# Outline

- 1 Quantum computers
- 2 Syntax and semantics

# Qubits (Quantum bits)

## Syntax

$q ::= |0\rangle \mid |1\rangle$

$\langle \text{bra} \mid \text{ket} \rangle$

# Qubits

## Syntax

$q ::= |0\rangle \mid |1\rangle$

$\mid \alpha |0\rangle + \beta |1\rangle$

$\langle \text{bra} \mid \text{ket} \rangle$

where  $\alpha, \beta \in \mathbb{C}$

and  $\alpha^2 + \beta^2 = 1$

# Qubits

## Syntax

$q ::= |0\rangle \mid |1\rangle$

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

$\langle \text{bra} \mid \text{ket} \rangle$

where  $\alpha, \beta \in \mathbb{C}$

and  $\alpha^2 + \beta^2 = 1$

## Semantics

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

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

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

# A quantum programming language

$c ::= \dots$  (quantum commands)

$c \vdash q \rightarrow^p q'$  (operational semantics)

$q ::= \alpha |0\rangle + \beta |1\rangle \mid \dots$  (quantum state)

$p \in \mathbb{R}$  (probability)

# Measurement: $c ::= \dots \mid \text{meas}(x)$

## Semantics

$$\text{meas}(x) \vdash \alpha |0\rangle + \beta |1\rangle \rightarrow^{\alpha^2} |0\rangle$$

$$\text{meas}(x) \vdash \alpha |0\rangle + \beta |1\rangle \rightarrow^{\beta^2} |1\rangle$$

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



# Measurement: $c ::= \dots \mid \text{meas}(x)$

## Semantics

$$\text{meas}(x) \vdash \alpha |0\rangle + \beta |1\rangle \rightarrow^{\alpha^2} |0\rangle$$



$$\text{meas}(x) \vdash \alpha |0\rangle + \beta |1\rangle \rightarrow^{\beta^2} |1\rangle$$



## Example (Measuring a classical state)

$$\text{meas}(x) \vdash |0\rangle \rightarrow^1 |0\rangle \quad \alpha = 1, \beta = 0$$

$$\text{meas}(x) \vdash |0\rangle \rightarrow^0 |1\rangle$$



# Measurement: $c ::= \dots \mid \text{meas}(x)$

## Semantics

$$\text{meas}(x) \vdash \alpha |0\rangle + \beta |1\rangle \rightarrow^{\alpha^2} |0\rangle$$



$$\text{meas}(x) \vdash \alpha |0\rangle + \beta |1\rangle \rightarrow^{\beta^2} |1\rangle$$



## Example (Measuring superposition)

$$\text{meas}(x) \vdash \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \rightarrow^{\frac{1}{2}} |0\rangle$$

$$\text{meas}(x) \vdash \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \rightarrow^{\frac{1}{2}} |1\rangle$$

# Density matrix semantics

$$\text{meas}(x) \vdash \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \rightarrow^{\frac{1}{2}} |0\rangle$$

$$\text{meas}(x) \vdash \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \rightarrow^{\frac{1}{2}} |1\rangle$$

Density matrix encodes a *probability distribution* over quantum states.

$$\llbracket \text{meas}(x) \rrbracket \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

# Systems of multiple qubits

## Syntax

$q ::= \dots | \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$

where  $\alpha_{00}^2 + \alpha_{01}^2 + \alpha_{10}^2 + \alpha_{11}^2 = 1$

# Systems of multiple qubits

## Syntax

$q ::= \dots | \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$   
where  $\alpha_{00}^2 + \alpha_{01}^2 + \alpha_{10}^2 + \alpha_{11}^2 = 1$

## Semantics

$\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$  where  $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \dots$

# Combining independent qubits

## Syntax

$$q ::= \dots \mid q_1 \otimes q_2$$

## Semantics

$$\begin{aligned} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} &= \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} \\ &= \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle \end{aligned}$$

# Entanglement

Not all 2-qubit states can be factored into two 1-qubit states.

## Example (Bell state)

$$\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

# Multiple qubits

$$c \vdash \gamma \rightarrow^p \gamma$$

$$\gamma ::= \langle [ls]; q \rangle \quad (\text{configuration})$$

$$ls ::= [x_1, \dots, x_n] \quad (\text{qubit ordering})$$

$$q ::= \dots \quad (\text{quantum state})$$

$$p \in \mathbb{R} \quad (\text{probability})$$

# Measurement with multiple qubits

## Semantics (Independent)

$$\begin{aligned} \text{meas}(x) \vdash \langle [x, y]; (\alpha |0\rangle + \beta |1\rangle) \otimes q_y \rangle \\ \rightarrow^{\alpha^2} \langle [x, y]; |0\rangle \otimes q_y \rangle \end{aligned}$$

$$\begin{aligned} \text{meas}(x) \vdash \langle [x, y]; (\alpha |0\rangle + \beta |1\rangle) \otimes q_y \rangle \\ \rightarrow^{\beta^2} \langle [x, y]; |1\rangle \otimes q_y \rangle \end{aligned}$$



# Measurement with multiple qubits

## Semantics (Entangled)

$$\begin{aligned} \text{meas}(x) \vdash \langle [x, y]; \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rangle \\ \rightarrow^{\frac{1}{2}} \langle [x, y]; |00\rangle \rangle \end{aligned}$$

$$\begin{aligned} \text{meas}(x) \vdash \langle [x, y]; \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rangle \\ \rightarrow^{\frac{1}{2}} \langle [x, y]; |11\rangle \rangle \end{aligned}$$

# Initialization

## Syntax

$c ::= \dots \mid x = \text{init}(b)$   
 $b \in \text{Bit}$

$|b\rangle$  —

## Semantics

$x = \text{init}(b) \vdash \langle [ls]; q \rangle \rightarrow \langle [ls, x]; q \otimes |b\rangle \rangle$

# Initialization

## Syntax

$c ::= \dots \mid x = \text{init}(b)$   
 $b \in \text{Bit}$

$|b\rangle$  —

## Semantics

$x = \text{init}(b) \vdash \langle [ls]; q \rangle \rightarrow \langle [ls, x]; q \otimes |b\rangle \rangle$

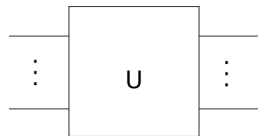
We initialize *classical, independent* qubits.  
How to get *superpositions* and *entanglement*?

# Unitary transformations

## Syntax

$c ::= \dots \mid U(x_1, \dots, x_n)$

$U ::= \dots$  (Unitary operations)

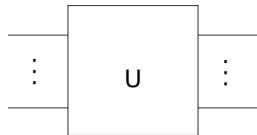


# Unitary transformations

## Syntax

$c ::= \dots \mid U(x_1, \dots, x_n)$

$U ::= \dots$  (Unitary operations)



## Semantics

$$U(\vec{x}\vec{s}) \vdash \langle [\vec{x}\vec{s}]; q \rangle \rightarrow \langle [\vec{x}\vec{s}]; \llbracket U \rrbracket(q) \rangle$$

$\llbracket U \rrbracket \in \mathcal{U}$ : a square, complex matrix satisfying

$$\llbracket U \rrbracket^\dagger \llbracket U \rrbracket = \llbracket U \rrbracket \llbracket U \rrbracket^\dagger = I.$$

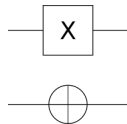
# Unitary transformations (X/NOT)

## Syntax

$U ::= \dots \mid X$

## Semantics

$$\llbracket X \rrbracket = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



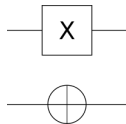
# Unitary transformations (X/NOT)

## Syntax

$U ::= \dots | X$

## Semantics

$$\llbracket X \rrbracket = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



## Example

$$\begin{aligned} \llbracket X \rrbracket (\alpha |0\rangle + \beta |1\rangle) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta |0\rangle + \alpha |1\rangle \end{aligned}$$

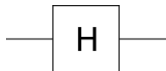
# Unitary transformations (Hadamard)

## Syntax

$U ::= \dots \mid H$

## Semantics

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





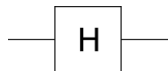
# Unitary transformations (Hadamard)

## Syntax

$U ::= \dots \mid H$

## Semantics

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



## Example

$$\begin{aligned} \llbracket H \rrbracket(|0\rangle) &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \\ \llbracket H \rrbracket(|1\rangle) &= \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \end{aligned}$$

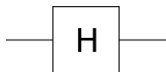
# Unitary transformations (Hadamard)

## Syntax

$U ::= \dots \mid H$

## Semantics

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



## Example

$$\llbracket H \rrbracket(|0\rangle) = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle = |+\rangle$$

$$\llbracket H \rrbracket(|1\rangle) = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle = |-\rangle$$

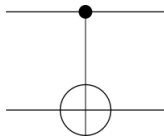
# Unitary transformations (CX/Controlled NOT)

## Syntax

$U ::= \dots \mid \text{CX}$

## Semantics

$$\llbracket \text{CX} \rrbracket = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



# Unitary transformations (CX/Controlled NOT)

## Syntax

$U ::= \dots \mid \text{CX}$

## Semantics

$$\llbracket \text{CX} \rrbracket = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

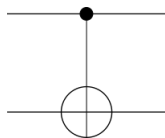
## Example

$$\llbracket \text{CX} \rrbracket(|00\rangle) = |00\rangle$$

$$\llbracket \text{CX} \rrbracket(|01\rangle) = |01\rangle$$

$$\llbracket \text{CX} \rrbracket(|10\rangle) = |11\rangle$$

$$\llbracket \text{CX} \rrbracket(|11\rangle) = |10\rangle$$

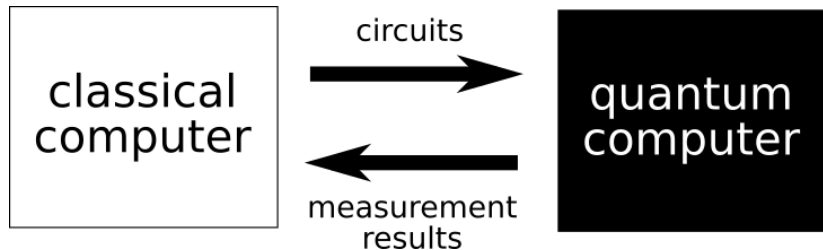


# Classical control flow?

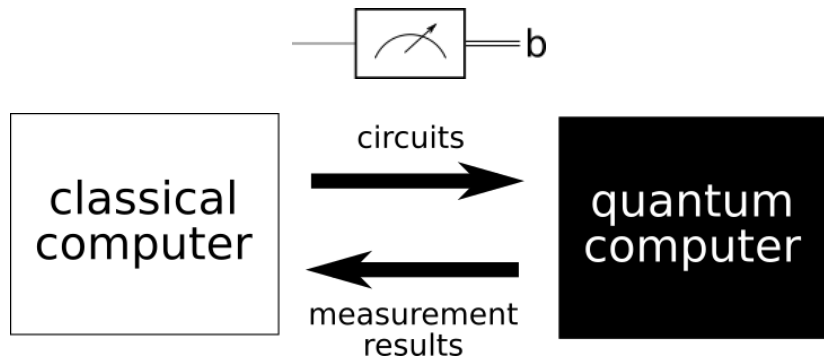


if b then c1 else c2

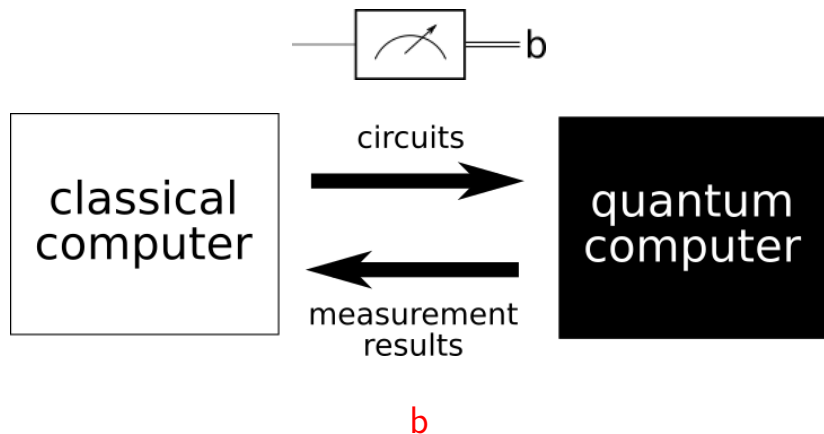
# QRAM model semantics



# QRAM model semantics

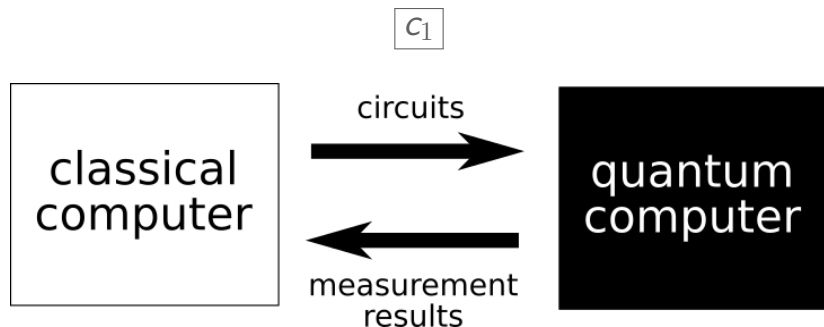


# QRAM model semantics





# QRAM model semantics



b

# Quantum while language

## Syntax

$$c ::= \dots \mid \text{while meas}(q) \text{ do } c$$
$$\mid \text{if meas}(q) \text{ then } c_1 \text{ else } c_0$$

“Quantum data, classical control”

# A small quantum language

## Syntax

$c ::= x = \text{init}(b) \mid \text{meas}(x) \mid U(\vec{x}_i)$   
SKIP  $\mid c; c \mid \text{if meas}(q) \text{ then } c_1 \text{ else } c_0$   
 $\mid \text{while meas}(q) \text{ do } c$

$$c \vdash \langle [l_s]; q \rangle \rightarrow^P \langle [l_s']; q' \rangle$$

# Other language designs

- Functional languages with linear types
- Embedded language
- Quantum-specific abstractions and applications
- Categorical semantics
- Graphical calculi e.g. ZX-calculus
- A lot of creativity!

# Quantum Computing for Programming Language Researchers

or:

I sort of understand quantum computing,  
and so can you!

Jennifer Paykin

PLanQC, January 2020

| galois |