Quantum Computing for Programming Language Researchers

or:

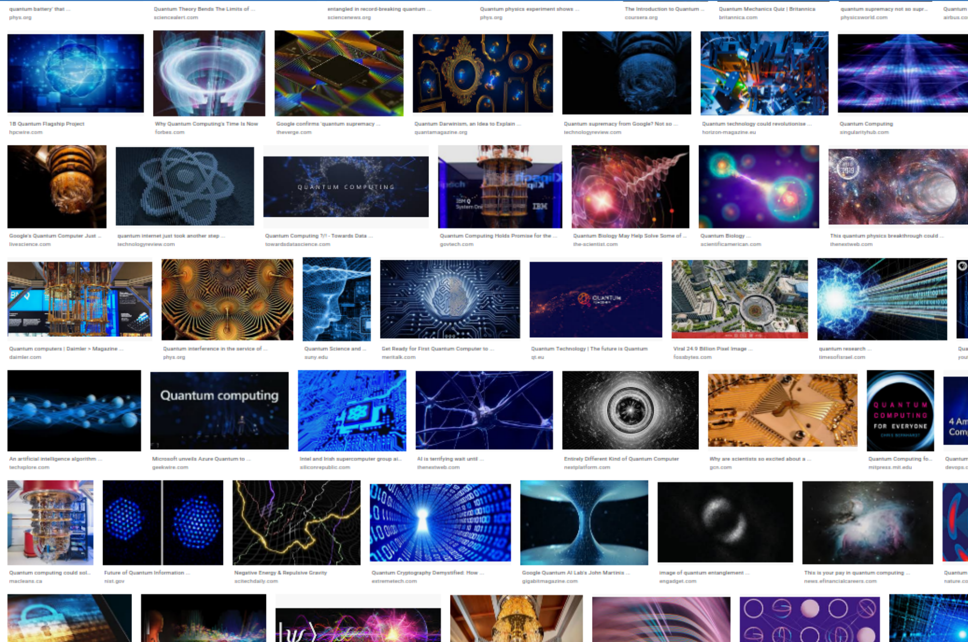
I sort of understand quantum computing, and so can you!

Jennifer Paykin

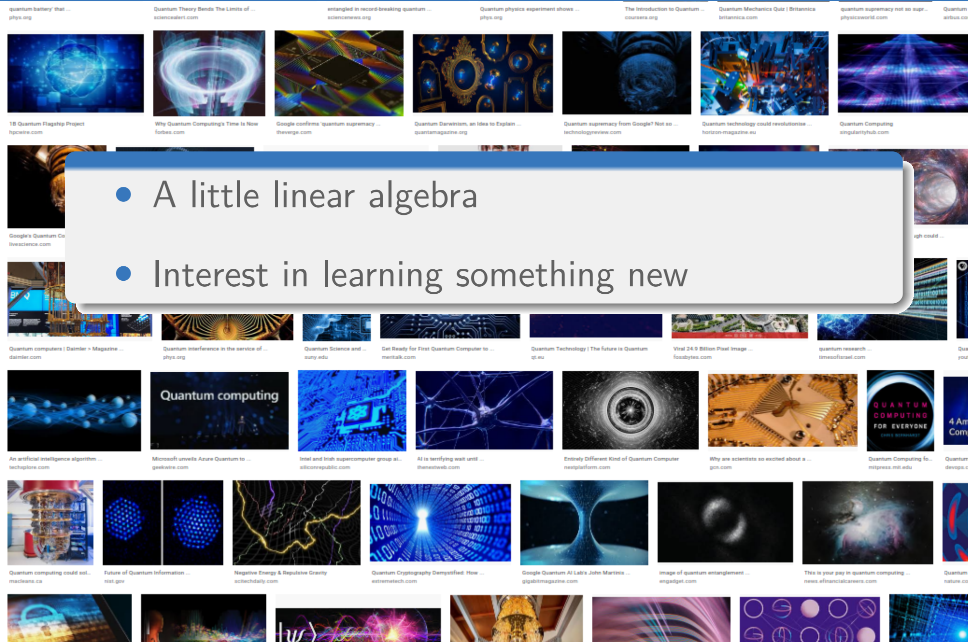
PLanQC, January 2020

|galois|

Quantum Computing: not so scary

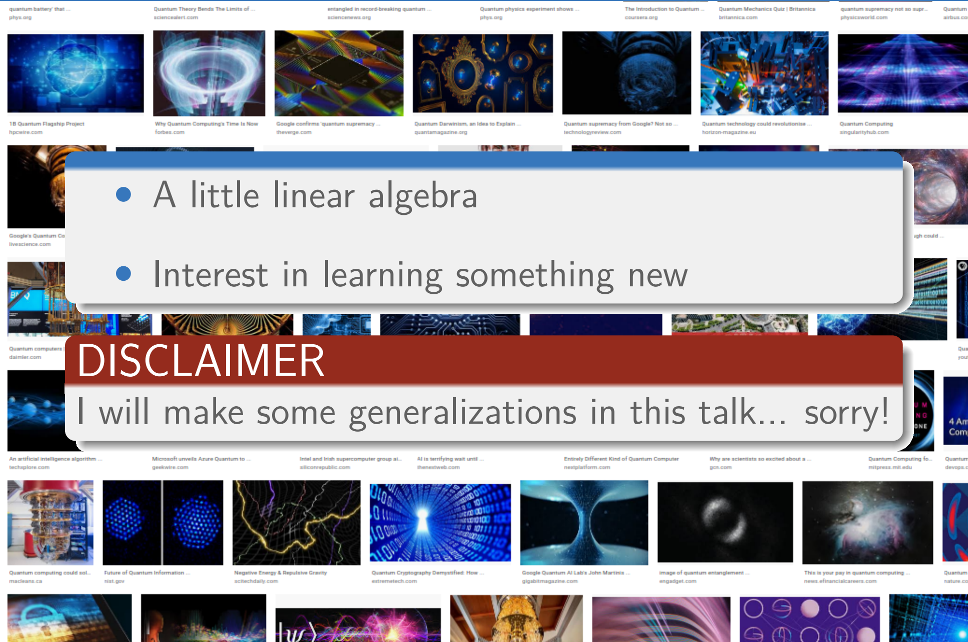


Quantum Computing: not so scary



- A little linear algebra
- Interest in learning something new

Quantum Computing: not so scary



- A little linear algebra
- Interest in learning something new

DISCLAIMER

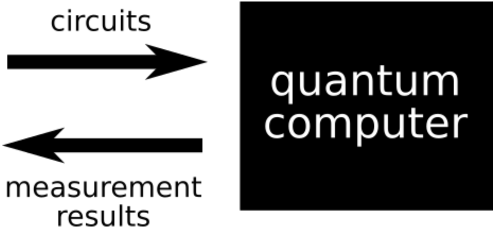
I will make some generalizations in this talk... sorry!

Outline

1. Quantum computers

2. Syntax and semantics

Circuit model semantics



The NISQ era

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

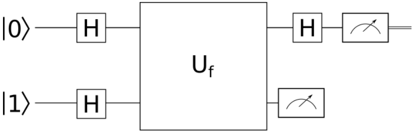
- 50-100 qubits
- a variety of implementation techniques
- quantum supremacy (well, almost)
- a lot of noise introducing errors

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 (**Qu**antum **bits**)

Syntax

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

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

Qubits

Syntax

$$q ::= |0\rangle \mid |1\rangle \qquad \langle \text{bra} \mid \text{ket} \rangle$$

$$\mid \alpha|0\rangle + \beta|1\rangle \qquad \text{where } \alpha, \beta \in \mathbb{C}$$

$$\text{and } \alpha^2 + \beta^2 = 1$$

Qubits

Syntax

$$q ::= |0\rangle \mid |1\rangle$$
$$\mid \alpha\,|0\rangle + \beta\,|1\rangle$$

$\langle$bra | ket$\rangle$

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

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

Semantics

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

where $|0\rangle = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$

and $|1\rangle = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$

A quantum programming language

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

$c \vdash q \to^{p} q'$ (operational semantics)

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

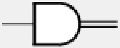
$p \in \mathbb{R}$ (probability)

Measurement: $c ::= \cdots \mid \mathsf{meas}(x)$

Semantics

$\mathsf{meas}(x) \vdash \alpha\,|0\rangle + \beta\,|1\rangle \to^{\alpha^2} |0\rangle$

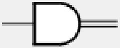
$\mathsf{meas}(x) \vdash \alpha\,|0\rangle + \beta\,|1\rangle \to^{\beta^2} |1\rangle$



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

Measurement: $c ::= \cdots \mid \mathsf{meas}(x)$

Semantics



$\mathsf{meas}(x) \vdash \alpha\,|0\rangle + \beta\,|1\rangle \to^{\alpha^2} |0\rangle$

$\mathsf{meas}(x) \vdash \alpha\,|0\rangle + \beta\,|1\rangle \to^{\beta^2} |1\rangle$

Example (Measuring a classical state)

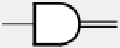
$\mathsf{meas}(x) \vdash |0\rangle \to^{1} |0\rangle \qquad \alpha = 1, \beta = 0$

$\mathsf{meas}(x) \vdash |0\rangle \to^{0} |1\rangle$

Measurement: $c ::= \cdots \mid \mathsf{meas}(x)$

Semantics

$$\mathsf{meas}(x) \vdash \alpha\,|0\rangle + \beta\,|1\rangle \to^{\alpha^2} |0\rangle$$



$$\mathsf{meas}(x) \vdash \alpha\,|0\rangle + \beta\,|1\rangle \to^{\beta^2} |1\rangle$$

Example (Measuring superposition)

$$\mathsf{meas}(x) \vdash \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \to^{\frac{1}{2}} |0\rangle$$

$$\mathsf{meas}(x) \vdash \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \to^{\frac{1}{2}} |1\rangle$$

Density matrix semantics

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

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

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

$$[\![\mathsf{meas}(x)]\!] \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

Systems of multiple qubits

Syntax

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

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

Systems of multiple qubits

Syntax

$$q ::= \cdots \mid \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$$

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

Semantics

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

Combining independent qubits

Syntax

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

Semantics

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$$

$$= \alpha_0\beta_0 \left|00\right\rangle + \alpha_0\beta_1 \left|01\right\rangle + \alpha_1\beta_0 \left|10\right\rangle + \alpha_1\beta_1 \left|11\right\rangle$$

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

$$c \vdash \gamma \to^{p} \gamma$$

$\gamma ::= \langle [ls]; q \rangle$ (configuration)

$ls ::= [x_1, \ldots, x_n]$ (qubit ordering)

$q ::= \cdots$ (quantum state)

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

Measurement with multiple qubits

Semantics (Independent)

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

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

Measurement with multiple qubits

Semantics (Entangled)

$$\mathsf{meas}(x) \vdash \langle [x, y]; \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\rangle \\ \to^{\frac{1}{2}} \langle [x, y]; |00\rangle\rangle$$

$$\mathsf{meas}(x) \vdash \langle [x, y]; \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\rangle \\ \to^{\frac{1}{2}} \langle [x, y]; |11\rangle\rangle$$

Initialization

Syntax

$$c ::= \cdots \mid x = \mathrm{init}(b)$$
$$b \in \mathrm{Bit}$$

Semantics

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

Initialization

Syntax

$$c ::= \cdots \mid x = \mathrm{init}(b)$$
$$b \in \mathrm{Bit}$$

Semantics

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

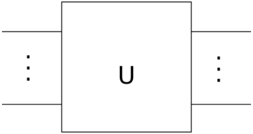
We initialize *classical*, *independent* qubits.
How to get *superpositions* and *entanglement*?

Unitary transformations

Syntax

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

$$U ::= \cdots \text{(Unitary operations)}$$

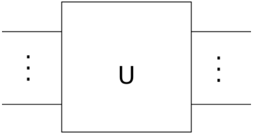


Unitary transformations

Syntax

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

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



Semantics

$$U(\overrightarrow{xs}) \vdash \langle [\overrightarrow{xs}]; q \rangle \to \langle [\overrightarrow{xs}]; [\![U]\!](q) \rangle$$

$[\![U]\!] \in \mathcal{U}$: a square, complex matrix satisfying

$$[\![U]\!]^\dagger [\![U]\!] = [\![U]\!] [\![U]\!]^\dagger = I.$$

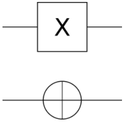
Unitary transformations (X/NOT)

Syntax

$$U ::= \cdots \mid X$$

Semantics

$$[\![X]\!] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



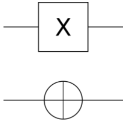
Unitary transformations (X/NOT)

Syntax

$$U ::= \cdots \mid X$$

Semantics

$$[\![X]\!] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



Example

$$\begin{aligned} [\![X]\!](\alpha\,|0\rangle + \beta\,|1\rangle) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta\,|0\rangle + \alpha\,|1\rangle \end{aligned}$$

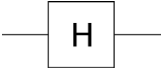
Unitary transformations (Hadamard)

Syntax

$$U ::= \cdots \mid \mathsf{H}$$

Semantics

$$[\![\mathsf{H}]\!] = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$



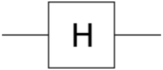
Unitary transformations (Hadamard)

Syntax

$$U ::= \cdots \mid \mathsf{H}$$

Semantics

$$[\![\mathsf{H}]\!] = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



Example

$$\begin{aligned} [\![\mathsf{H}]\!](|0\rangle) &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \tfrac{1}{\sqrt{2}} |0\rangle + \tfrac{1}{\sqrt{2}} |1\rangle \\ [\![\mathsf{H}]\!](|1\rangle) &= \tfrac{1}{\sqrt{2}} |0\rangle - \tfrac{1}{\sqrt{2}} |1\rangle \end{aligned}$$

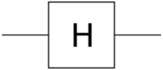
Unitary transformations (Hadamard)

Syntax

$$U ::= \cdots \mid \mathsf{H}$$

Semantics

$$[\![\mathsf{H}]\!] = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



Example

$$[\![\mathsf{H}]\!](|0\rangle) = \tfrac{1}{\sqrt{2}} |0\rangle + \tfrac{1}{\sqrt{2}} |1\rangle = |+\rangle$$
$$[\![\mathsf{H}]\!](|1\rangle) = \tfrac{1}{\sqrt{2}} |0\rangle - \tfrac{1}{\sqrt{2}} |1\rangle = |-\rangle$$

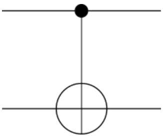
Unitary transformations (CX/Controlled NOT)

Syntax

$$U ::= \cdots \mid \mathsf{CX}$$

Semantics

$$[\![\mathsf{CX}]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



Unitary transformations (CX/Controlled NOT)

Syntax

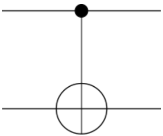
$$U ::= \cdots \mid \mathsf{CX}$$

Semantics

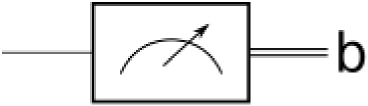
$$[\![\mathsf{CX}]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Example

$$[\![\mathsf{CX}]\!](|00\rangle) = |00\rangle$$
$$[\![\mathsf{CX}]\!](|01\rangle) = |01\rangle$$
$$[\![\mathsf{CX}]\!](|10\rangle) = |11\rangle$$
$$[\![\mathsf{CX}]\!](|11\rangle) = |10\rangle$$

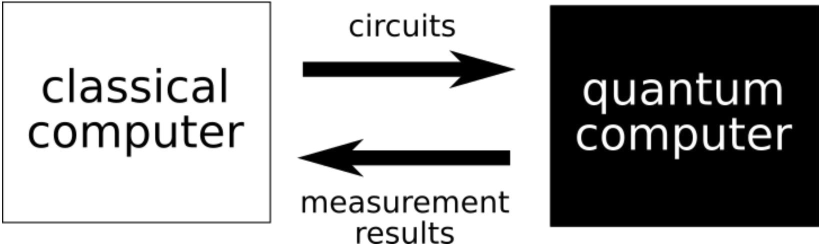


Classical control flow?

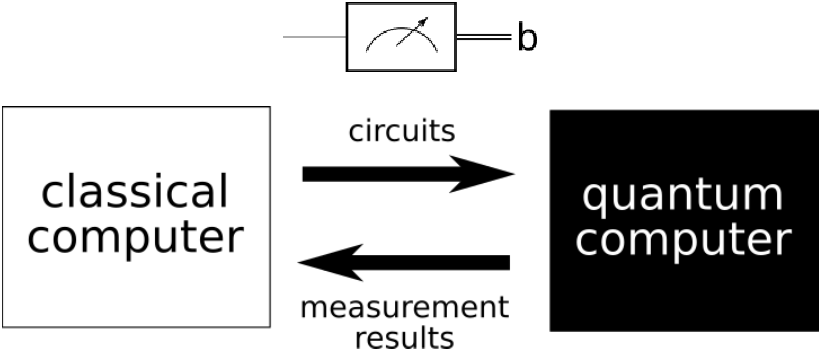


if b then c1 else c2

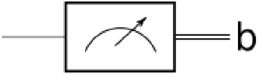
QRAM model semantics

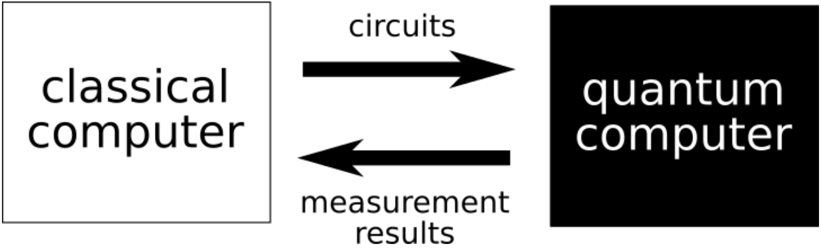


QRAM model semantics



QRAM model semantics

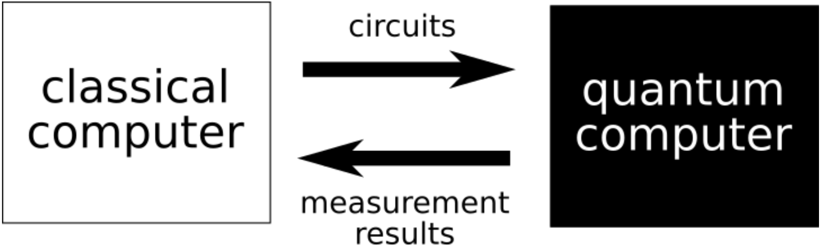




b

QRAM model semantics

c_1



b

Quantum while language

Syntax

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

"Quantum data, classical control"

A small quantum language

Syntax

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

$$c \vdash \langle [ls]; q \rangle \to^p \langle [ls']; q' \rangle$$

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|