Near-Term Quantum Computing for Software Verification and Validation

Dr. Jason Larkin

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Carnegie Mellon University
Software Engineering Institute

Legal

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

2

Dr. Jason Larkin

Research Scientist

CMU SEI,
Emerging Technology Center

Software VV and Advanced Computing

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

3

Why SEI? Software verification and validation (VV)

- Software VV is a core SEI mission (and for any Software Engineer).

- Alignment with ETC technical area: We are applying advanced computing to this core mission.

- Focus on the software engineering challenges

If successful…will have made a significant contribution to…

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

4

Why is Software VV important (and HARD) for DoD?

"…on average, half the **cost** of creating [complex software] is on **VV**."

— C. Elliott, Safe & Secure Systems & Software Symposium 2016.
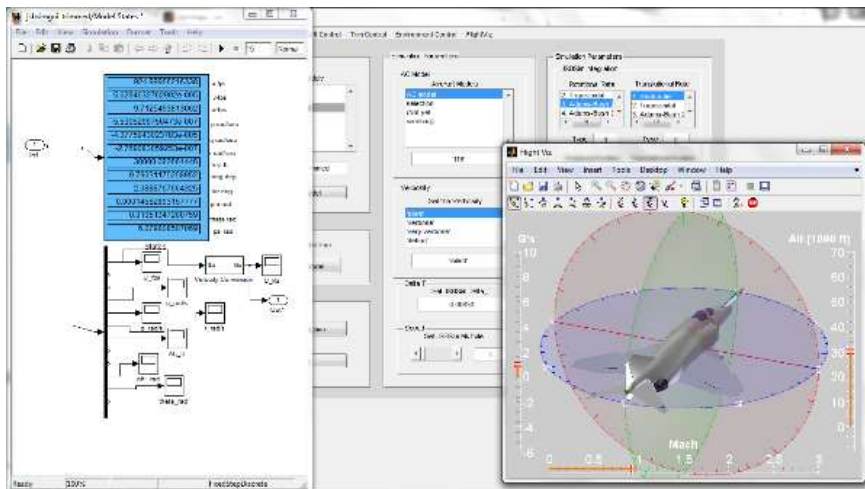
github.com/esp8266/Arduino

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

5

Why is Software VV important (and HARD) for DoD?

"…on average, half the **cost** of creating [complex software] is on **VV**."

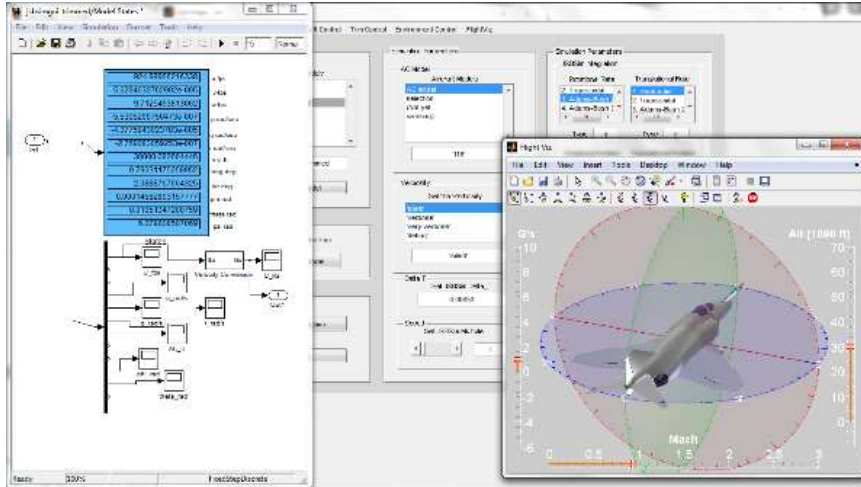— C. Elliott, Safe & Secure Systems & Software Symposium 2016.

Software VV Tools
Computational Cost ~ exp(size)
100-1 millions years

And this cost is increasing…
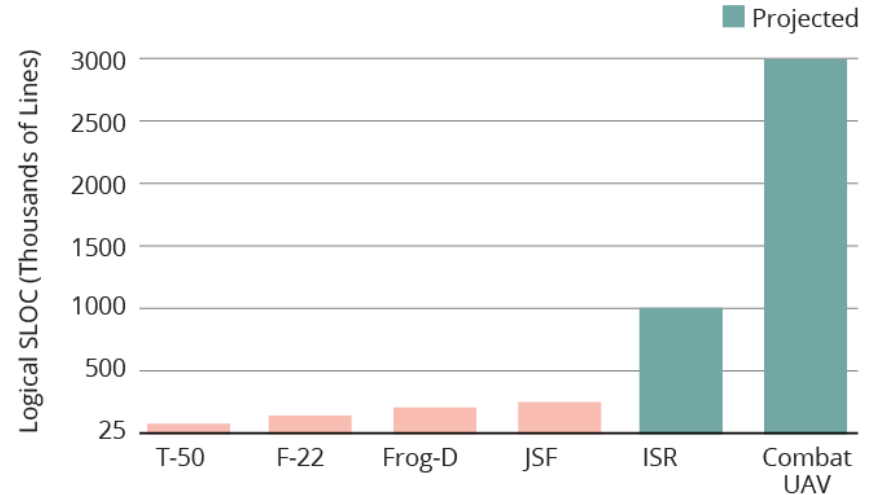
"next generation **Software VV will require new computing paradigm...**"

T. Belote, C. Elliott, Safe & Secure Systems & Software Symposium 2014.

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

6

Software VV Challenges

Historical schedule trends with complexity
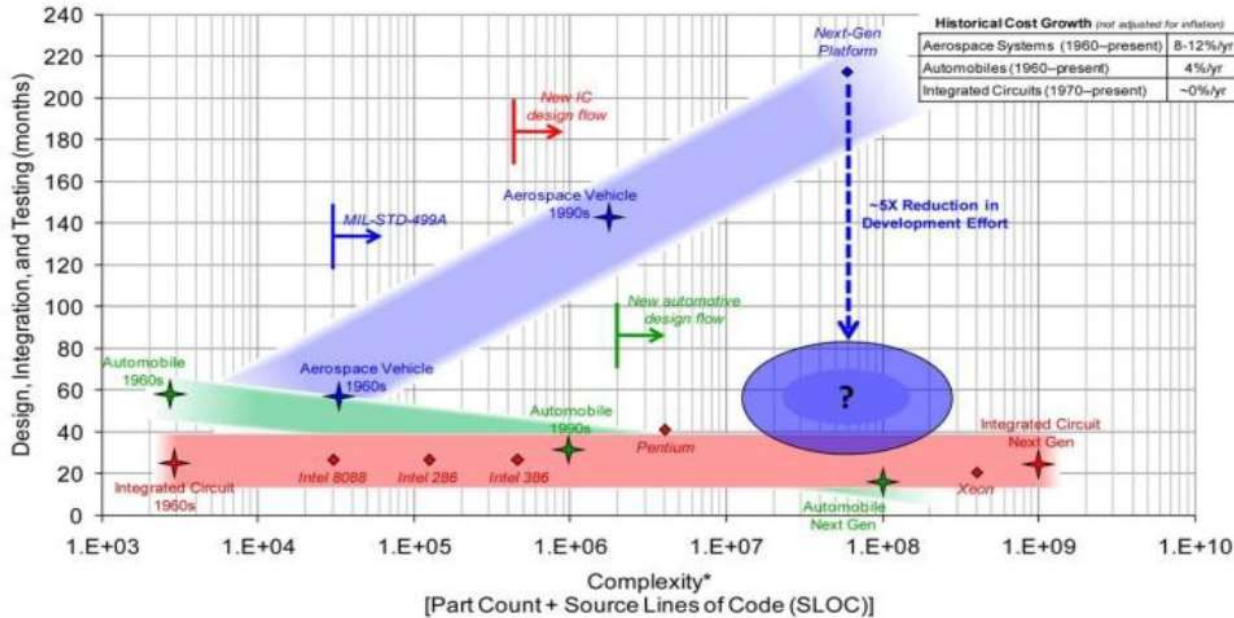
Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

7
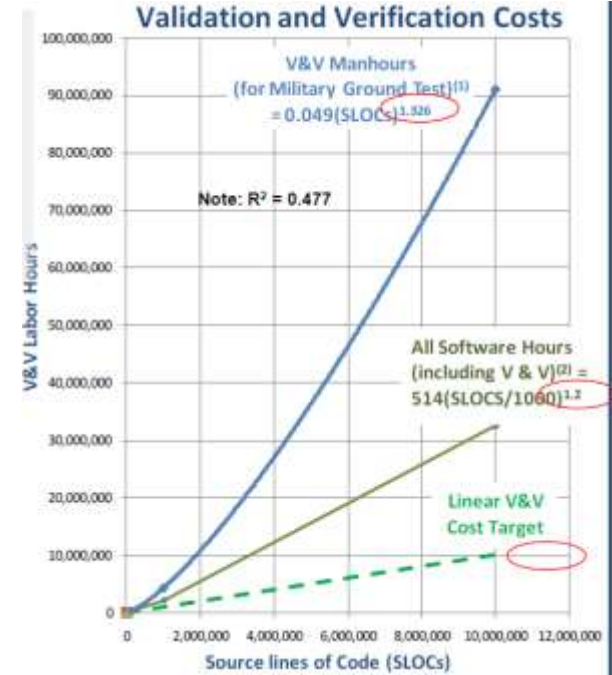
Is Quantum Computing the next major Paradigm?
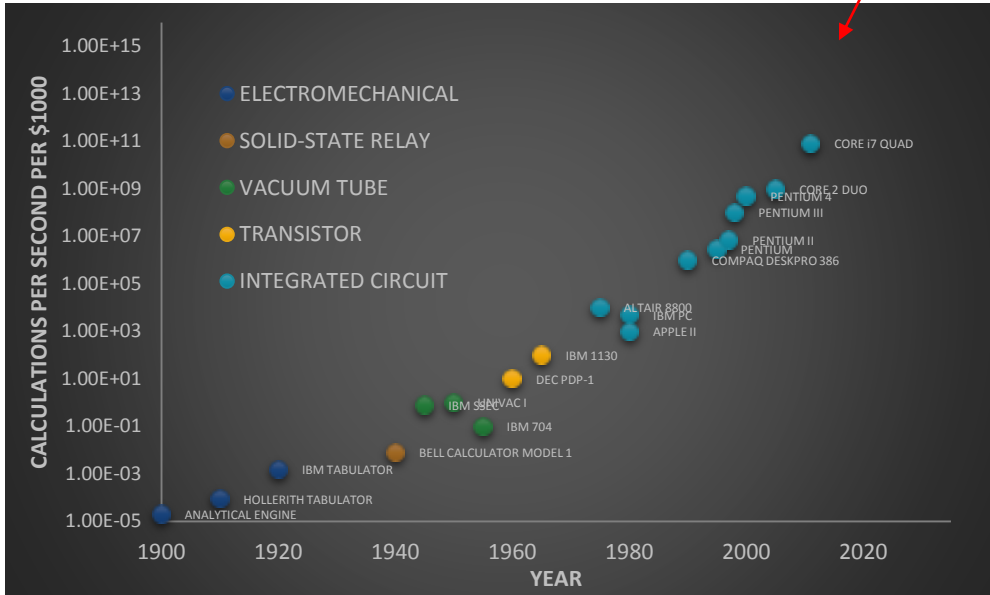
H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019

115th Congress (2017-2018) | Get alerts

SEC. 234. DEFENSE QUANTUM INFORMATION SCIENCE AND TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM.

IN THE SENATE OF THE UNITED STATES

A BILL

To require the Secretary of Defense to establish the Defense Quantum Information Consortium, and for other purposes.

Quantum Computing Applications with State of the Art Capabilities Request for Information (RFI)

Solicitation Number: DARPA-SN-18-68
Agency: Other Defense Agencies
Office: Defense Advanced Research Projects Agency

https://www.congress.gov/bill/115th-congress/senate-bill/2987/
https://www.harris.senate.gov/news/press-releases/harris-introduces-bill-to-increase-resources-for-quantum-computing-and-research-to-benefit-national-security
https://www.fbo.gov/spg/ODA/DARPA/CMO/DARPA-SN-18-68/listing.html

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

8

What is Quantum Computing?

Bill Phillips
NIST/JQI
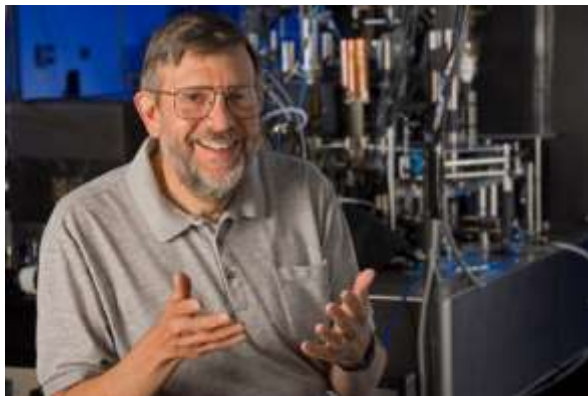
"A Quantum Computer differs more from a classical computer…than a classical computer differs from an ABACUS"
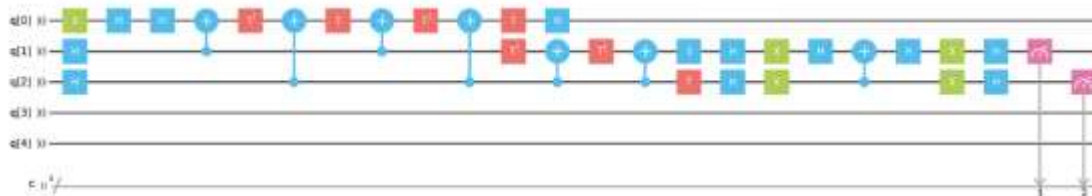
FIG. 2: The circuit that was executed on IBM's 5-qubit quantum computer (ibmqx4 was used). The first two time slots correspond to the state preparatio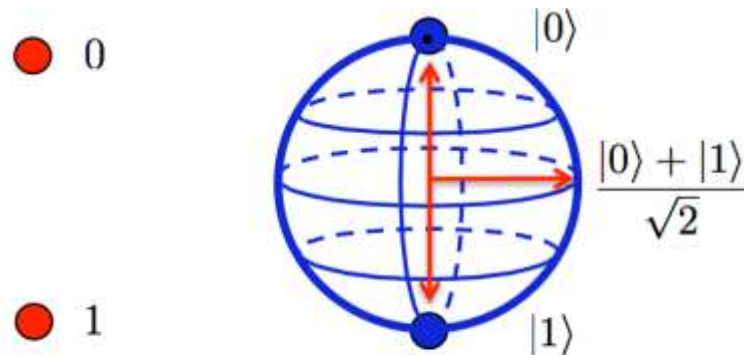n. The next 13 time slots implement a Toffoli gate. The next 7 time slots implement the $2 |\psi\rangle \langle\psi| - I$ operator, and the final two time slots are used for observing x_1 and x_2.

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

9

Why is it important to DoD?

Science Home News Journals Topics Careers

Update: Quantum physics gets attention—
and brighter funding prospects—in Congress

By Gabriel Popkin | Jan. 22, 2018, 12:30 PM

Many members of Congress admit they find quantum physics mind-boggling, with its counterintuitive account of the subatomic world. But that isn't stopping U.S. lawmakers, as well as policymakers in President Donald Trump's administration, from backing an emerging effort to better organize and boost fund...

INTELLIGENCE COMMUNITY NEWS

Your source for breaking news from across the intelligence community contracting landscape, delivered daily.

DARPA posts quantum computing RFI

DARPA

On July 10, the Defense Advanced Research Projects Agency (DARPA) posted a request for information for Quantum Computing Applications with State of the Art Capabilities (Solicitation Number: DARPA-SN-18-68). Responses are due by 4:00 p.m. Eastern on August 10.

* The Defense Advanced Research Projects Agency (DARPA) Defense Sciences Office (DSO) is seeking information on new capabilities that could be enabled by current...

Universal Gate Quantum Computing

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

10
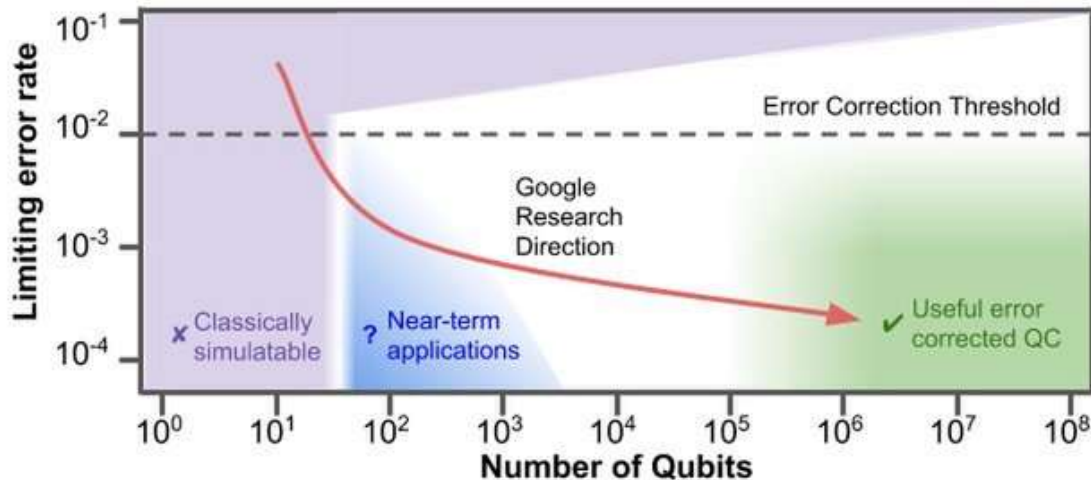
Is Quantum Computing the next major Paradigm?
What is the path to mission-capable…

Quantum Software Engineering

0		

$|0\rangle$

$\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$

$|1\rangle$

Classical Bit   **Qubit**

What are we doing?
So

Sat

- S
  (

- S

Combinatorial?

X = 1

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

12
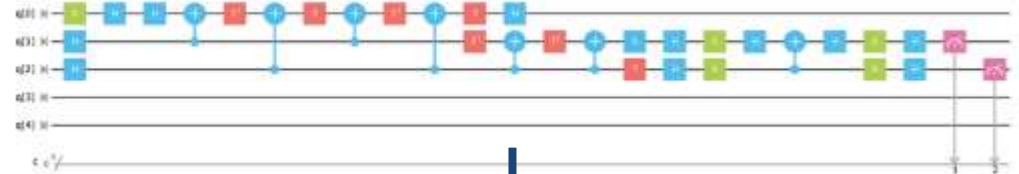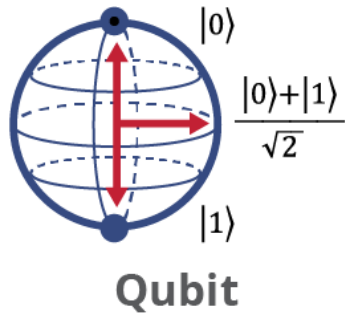
Why is it significant?
Quantum Speedup and Software VV

Grover's Algorithm (SAT):

$$(v_1 \lor v_2 \lor v_3) \land \neg(\neg v_1 \lor \neg v_2 \lor v_3) \land \dots$$

Grover's algorithm: quantum search algorithm that finds with high probability the unique input to a black box function that produces a particular output value, using just **O(sqrt(N))** evaluations of the function, where **N** is the size of the function's domain.

classical $O(2^n)$ -> quantum $O(2^{n/2})$

```
int get_sign(int x) {
  if (x == 0)
    return 0;

  if (x < 0)
    return -1;
  else
    return 1;
}
```

SMT

X = 0
X = -1
X = 1

http://satcompetition.org/

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

13

What are we going to do?

Lockheed Martin Challenge Problem
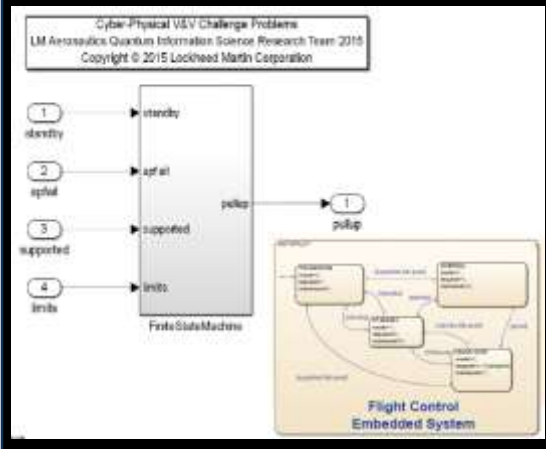
Satisfiability (SAT) Solver

```c
int get_sign(int x) {
  if (x == 0)
    return 0;

  if (x < 0)
    return -1;
  else
    return 1;
}
```

Quantum Universal Gate

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

14
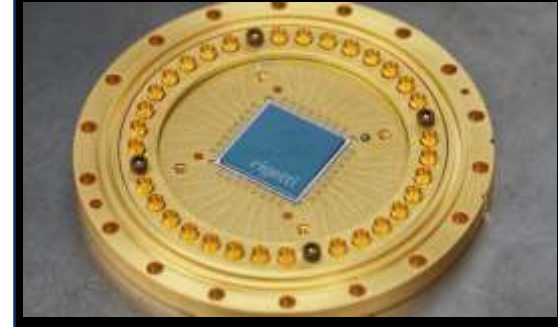
Benchmarking

SAT Solver (Grover's Algorithm):

FIG. 2: The circuit that was executed on IBM's 5-qubit quantum computer (ibmqx4 was used). The first two time slots correspond to the state preparation.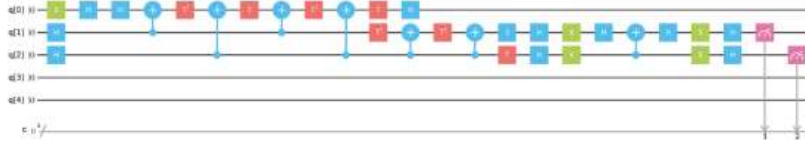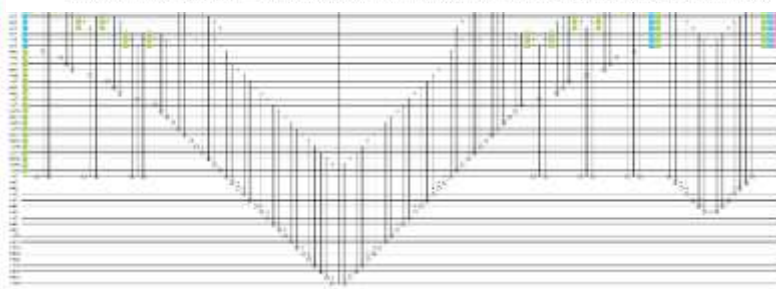 The next 13 time slots implement a Toffoli gate. The next 7 time slots implement the $2 |\psi\rangle \langle\psi| - I$ operator, and the final two time slots are used for observing x_1 and x_2.

$(v_1 \lor v_2) \land (v_1 \lor v_3) \land (v_2 \lor v_3)$ (50 qubits)

LM Challenge Problem…   (? qubits)

Automatically Solving NP-Complete Problems on a Quantum Computer
ICSE '18 Companion, May 27-June 3, 2018, Gothenburg, Sweden

Full-Stack Software Universal Gate

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public
release and unlimited distribution.

15
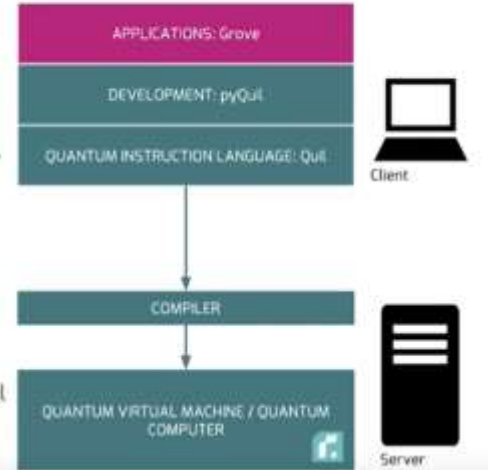
Deliverable: Projection for LM Challenge Problem

Unsupervised ML
on Rigetti 19Q
with Forest 1.2

QVM
(AWS)

QVM
(SC)

Google

LM Challenge Problem?

Automatically Solving
NP-Complete
Problems on a
Quantum Computer
ICSE '18 Companion

Classical Cost = $A*2^n$

Quantum Cost = $B*2^{n/2}$

B = f(
qubits, error,
connectivity, …)

Computational
Cost

Number of Qubits
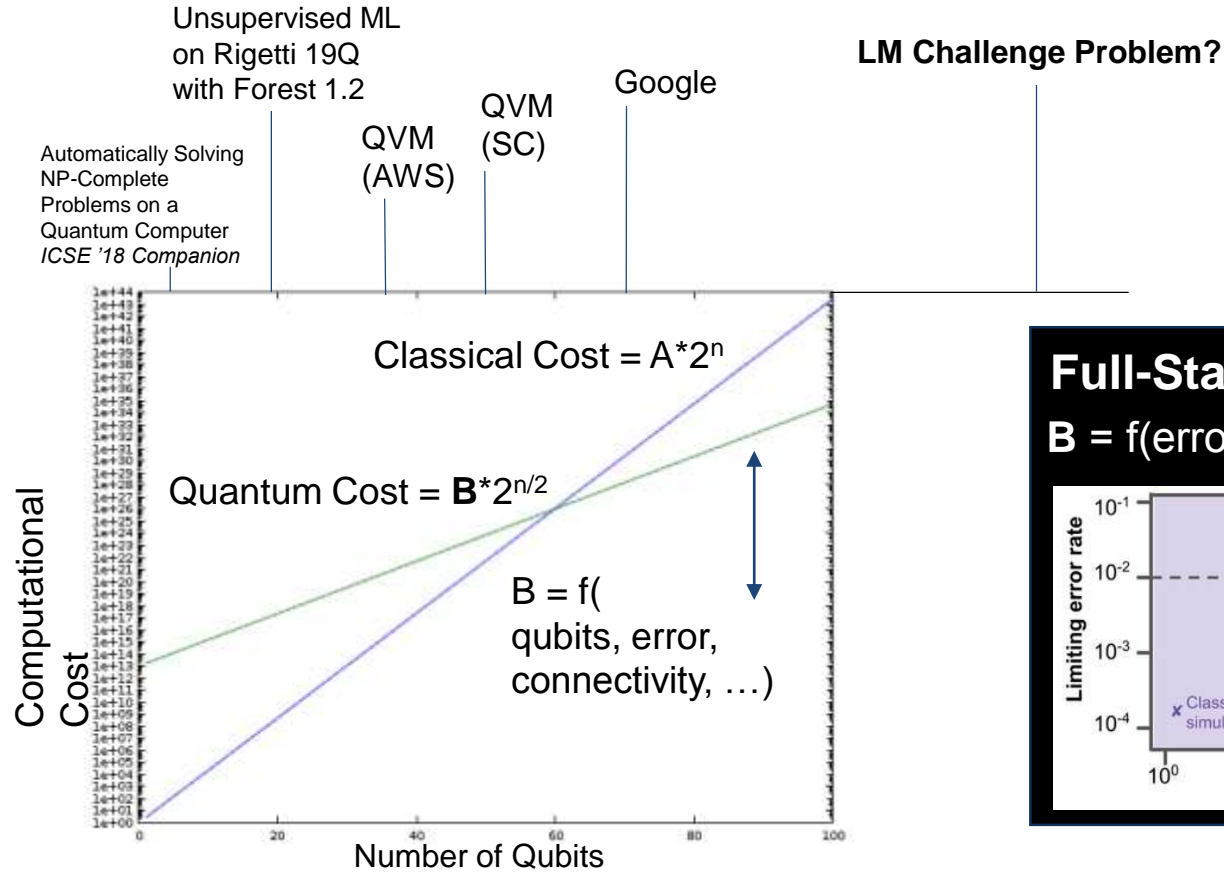
Full-Stack Engineering

B = f(error, connectivity, …)

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public
release and unlimited distribution.

16

Questions?

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public
release and unlimited distribution.

17

Dr. Jason Larkin
Research Scientist **Quantum**
Physics, HPC, Software **VV**

Quantum Physics and Computing

PhD Thesis "Thermal Transport Properties of Disordered Materials from High Performance Atomistic Simulations"
Quantum Chemsitry (DFT), Quantum Computing for Quantum Chemistry
HPC
AFRL, DoD HPCMP

Software VV

SpiralGen: DARPA High-Assurance Cyber Military Systems (HACMS)
"High-Assurance SPIRAL: End-to-End Guarantees for Robot and Car Control", IEEE Control Systems Magazine, 2017.
"High Assurance Spiral: Scalable and Performance Portable Domain-Specific Control System Synthesis".

SEI: GraphBLAS
A Test Framework for GraphBLAS (ICSE 2019, in progress)

Carnegie Mellon University
Software Engineering Institute

Near-Term Quantum Computing for Software Verification and Validation
© 2018 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

18