How Will Linux Handle Quantum Computing?

An entangled superposition of views
Overview

- Who cares about quantum computing?
- What is so great about quantum computing?
- Quantum computing technical trends
- Trouble with thermodynamics
- What is quantum computing's killer app?
- Quantum computing and Linux?
- Summary

Notes:
- Quantum communication/encryption already relatively advanced
- For programming quantum computers, see IBM-Q or get a D-Wave
Who Cares About Quantum Computing?
Who Cares About Quantum Computing?

- D-Wave Systems: Champion in qubit count
- Google: Champion in QC memory
- Intel: Investing $50M in partnership w/Google, NASA, USRA
- Microsoft: Champion in QC languages
- IBM: Champion in QC to the masses
  - And **real** qubits, not the cheap imitations that you might find elsewhere
  - [https://github.com/qiskit](https://github.com/qiskit)
- However, current QC offerings are a bit primitive
  - Think 1940s computers...
What Did 1940s Computers Look Like?

https://en.wikipedia.org/wiki/CSIRAC

Photo by John O'Neill under GNU FDL v1.2
What Did 1940s Computers Look Like?

- **CSIRAC**: Oldest intact electronic stored-program computer
  - Operational in November 1949 at University of Melbourne

- 2,000 Vacuum tubes: Each an incandescent lightbulb in size
  - And less capable than a transistor: Need more tubes than transistors

- 768 words of memory, 20 bits each, in mercury delay lines
  - Hence “surviving” rather than operational
    - 2017 safety regs unforgiving of metallic mercury and exposed 600V wiring

- CPU core clock frequency of... 1KHz

- Energy-efficient design sips only 30kW
What Did 1940s Computers Look Like?

- **CSIRAC**: Oldest intact electronic stored-program computer
  - Operational in November 1949 at University of Melbourne

- 2,000 Vacuum tubes: Each an incandescent lightbulb in size
  - And less capable than a transistor: Need more tubes than transistors

- 768 words of memory, 20 bits each, in mercury delay lines
  - Hence “surviving” rather than operational
    - 2017 safety regs unforgiving of metallic mercury and exposed 600V wiring

- CPU core clock frequency of... 1KHz

- Energy-efficient design sips only 30kW (about 300 people)

- Present-day QC systems are similarly crude
IBM's Five-Qubit Quantum Computer
IBM's Five-Qubit Quantum Computer (And Now 16!!!)
What is so Great About Quantum Computing???
Superposition in Qubit as Bloch Sphere

Qubit is a pair of FP #s, but measurement projects onto z axis
http://research.ibm.com/ibm-q/
Superposition by Itself is Unexciting

- All it gets you is an extremely inaccurate, slow, and error-prone reinvention of a small subset of the capabilities of this 1960s analog computer
- Which was emphatically obsoleted by classic computing
Entanglement!!! Entangled Qubits as Bloch Spheres

Entanglement can act sort of like constraints between groups of qubits
https://www.smbc-comics.com/comic/the-talk-3
https://xkcd.com/1240/
Quantum Computing Technical Trends
QC Trends: D-Wave Number of “Qubits”

<table>
<thead>
<tr>
<th>System</th>
<th>Availability</th>
<th># Qubits</th>
<th>Years per Doubling</th>
</tr>
</thead>
<tbody>
<tr>
<td>D-Wave One</td>
<td>May 2011</td>
<td>128</td>
<td>1.4</td>
</tr>
<tr>
<td>D-Wave Two</td>
<td>May 2013</td>
<td>512</td>
<td>1.9</td>
</tr>
<tr>
<td>D-Wave 2X</td>
<td>August 2015</td>
<td>1152</td>
<td>1.7</td>
</tr>
<tr>
<td>D-Wave 2000Q</td>
<td>January 2017</td>
<td>2048</td>
<td>–</td>
</tr>
</tbody>
</table>

Moore's-Law-style exponential growth
IBM-Q supports 16 full-function qubits, but 50 expected soon
IBM-Q doubling every 8 months, sustainable?
QC Trends: Coherence Time (DRAM, But No Refresh)

Ten seconds in 2027? 39 minutes but...
QC Trends: Number of Entangled Qubits

- IBM-Q: restricted entanglement among 8 16 qubits
- Claims of up to 8-qubit D-Wave entanglement
- Up to 3,000 rubidium atoms entangled in lab experiment
  - But not clear how to make useful computer of low-temperature gas
  - Reproducing this in QC would greatly build confidence!
Quantum Computing Technical Trends: Summary

- Exponential Moore's-Law-like progress:
  - Number of qubits
  - Coherence times

- Jury still out on entanglement
  - Seems reasonable to expect similar progress

- Connectivity also important: “quantum volume”
Quantum Computing Technical Trends: Summary

- Exponential Moore's-Law-like progress:
  - Number of qubits
  - Coherence times

- Jury still out on entanglement
  - Seems reasonable to expect similar progress

- Connectivity also important: “quantum volume”

- But never forget the three laws of thermodynamics!
  - Because they sure aren't going to forget you!!!
Trouble With Thermodynamics
Trouble With Thermodynamics: The Three Laws

1) Energy is conserved
   - In English: *You cannot win*
Trouble With Thermodynamics: The Three Laws

1) Energy is conserved
   – In English: *You cannot win*

2) Entropy increases in closed systems
   – In English: *You cannot break even*
Trouble With Thermodynamics: The Three Laws

1) Energy is conserved
   – In English: *You cannot win*

2) Entropy increases in closed systems
   – In English: *You cannot break even*

3) Entropy approaches a constant value as temperature approaches absolute zero
   – In English: *You cannot get out of the game*
Trouble With Thermodynamics: The Three Laws

1) Energy is conserved
   – In English: *You cannot win*

2) Entropy increases in closed systems
   – In English: *You cannot break even*

3) Entropy approaches a constant value as temperature approaches absolute zero
   – In English: *You cannot get out of the game*

- Thermodynamics is to physical-world engineering as the halting problem is to computer science:
  – “The answer is NO!!! What was the question?”
Trouble With Thermodynamics: The Three Laws

1) Energy is conserved
   – In English: *You cannot win*

2) Entropy increases in closed systems
   – In English: *You cannot break even*

3) Entropy approaches a constant value as temperature approaches absolute zero
   – In English: *You cannot get out of the game*

- Thermodynamics is to physical-world engineering as the halting problem is to computer science:
  – “The answer is **NO!!!** What was the question?”

- Key point: IBM-Q operates at a temperature of 0.015K
  – In contrast, helium boils at the tropical temperature of 4.2K
  – *Significant energy is therefore required for refrigeration*
### Trouble With Thermodynamics: Keeping it Cool

<table>
<thead>
<tr>
<th></th>
<th>T (K)</th>
<th>$C_p$</th>
<th>Theoretical Minimum Power per Watt Waste Heat (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dry Ice</td>
<td>195</td>
<td>1.990</td>
<td>0.5</td>
</tr>
<tr>
<td>Liquid Nitrogen</td>
<td>77</td>
<td>0.356</td>
<td>2.8</td>
</tr>
<tr>
<td>Liquid Hydrogen</td>
<td>20</td>
<td>0.073</td>
<td>23.7</td>
</tr>
<tr>
<td>Liquid Helium</td>
<td>4</td>
<td>0.0138</td>
<td>72.3</td>
</tr>
<tr>
<td>IBM Q</td>
<td>0.015</td>
<td>0.000051</td>
<td>19,500.0</td>
</tr>
</tbody>
</table>

19.5kW is admittedly less than two-thirds of CSIRAC's consumption!
But Aren't QC Operations Zero Energy Cost???
But Aren't QC Operations Zero Energy Cost???
Yes, In Theory, But...

Heat is conducted along wires, and use of light for data delivers energy
Liquid surroundings transport heat via convection
Vacuum chambers transport heat via radiation
Initialization and readout of quantum state generates waste heat
## Trouble With Thermodynamics: Keeping it Cool

<table>
<thead>
<tr>
<th></th>
<th>$T$ (K)</th>
<th>$C_p$</th>
<th>Theoretical Minimum Power per Watt Waste Heat (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dry Ice</td>
<td>195</td>
<td>1.990</td>
<td>0.5</td>
</tr>
<tr>
<td>Liquid Nitrogen</td>
<td>77</td>
<td>0.356</td>
<td>2.8</td>
</tr>
<tr>
<td>Liquid Hydrogen</td>
<td>20</td>
<td>0.073</td>
<td>23.7</td>
</tr>
<tr>
<td>Liquid Helium</td>
<td>4</td>
<td>0.0138</td>
<td>72.3</td>
</tr>
<tr>
<td>IBM Q</td>
<td>0.015</td>
<td>0.000051</td>
<td>19,500.0</td>
</tr>
</tbody>
</table>

And suppose further progress requires even lower temperatures?
## Trouble With Thermodynamics: Keeping it Cool

<table>
<thead>
<tr>
<th></th>
<th>$T$ (K)</th>
<th>$C_p$</th>
<th>Theoretical Minimum Power per Watt Waste Heat (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dry Ice</td>
<td>195</td>
<td>1.990</td>
<td>0.5</td>
</tr>
<tr>
<td>Liquid Nitrogen</td>
<td>77</td>
<td>0.356</td>
<td>2.8</td>
</tr>
<tr>
<td>Liquid Hydrogen</td>
<td>20</td>
<td>0.073</td>
<td>23.7</td>
</tr>
<tr>
<td>Liquid Helium</td>
<td>4</td>
<td>0.0138</td>
<td>72.3</td>
</tr>
<tr>
<td>IBM Q</td>
<td>0.015</td>
<td>0.000051</td>
<td>19,500.0</td>
</tr>
<tr>
<td>Bose-Einstein Condensate (BEC)</td>
<td>0.000000017</td>
<td>0.000000000062</td>
<td>1,605,882,351.9</td>
</tr>
</tbody>
</table>
Trouble With Thermodynamics: Keeping it Cool

Transporting a watt of waste heat from BEC requires 1.6 gigawatts...
Trouble With Thermodynamics: Keeping it Cool

Transporting a watt of waste heat from BEC requires 1.6 gigawatts...
Even Emmet Brown's flux capacitor only required 1.21 gigawatts!!!
Transporting a watt of waste heat from BEC requires 1.6 gigawatts... Even Emmet Brown's flux capacitor only required 1.21 gigawatts!!! But if the computation is valuable enough, who cares?
What is Quantum Computing's Killer App?
What is Quantum Computing's Killer App?

- Current possibilities:
  - Shor's integer factorization algorithm
  - Grover's search algorithm
  - Optimization problems (e.g., traveling salesman problem for logistics)
  - Quantum mechanical dynamics (e.g., quantum chemistry)
  - Gaming
Killer App: Integer Factorization

- Shor's algorithm promises polynomial-time factorization
  - Extremely valuable, if rather destructive
- Requires general-purpose qubits (IBM-Q, not D-Wave)
  - Thousands of them!
- Assuming 1.4 years per doubling, we have about 15 years until QC cracks 1000-bit RSA
  - Also assumes that Shor's algorithm actually works on real hardware
  - On the other hand, IBM-Q may be adding qubits faster than 1.4 years per doubling, doubling every 8 months from May 2016 to May 2017
  - So it might not be too early to start work on QC-resistant cyphers!!!
Killer App: Integer Factorization: Quantum Error Rate

“A few thousand” stable qubits

Quantum Error Correction

One hundred million real qubits

Killer App: Integer Factorization: Quantum Error Rate

“A few thousand” stable qubits

Quantum Error Correction

One hundred million real qubits

15-30 years, so still not to early for QC-resistant cypher!!! Besides, perhaps error rates will decrease

Killer App: Integer Factorization: Competition

- 2002: Polynomial-time integer primality test
- Perhaps integer factorization will also succumb to pure math
  - Easy to dismiss this until you review the past 50 years of progress:
    - 1970: Proof that Hilbert’s 10th problem is unsolvable
    - 1976: Proof of the four-color problem (stood for centuries)
    - 1984: Polynomial-time algorithm for solving linear programming problems
    - 1994: Proof of Fermat’s Last Theorem (stood for centuries)
    - 1998: Proof of Kepler’s conjecture (sphere packing, stood for centuries)
    - 2002: Proof of Catalan’s conjecture ($2^3$ and $3^2$, stood for centuries)
    - 2003: Proof of the Poincaré conjecture (topology)
    - 2004: Proof of the classification of finite simple groups
    - 2013: Proof that there is no bound on the values of pairs of primes differing by a finite number (first real progress in more than two millennia)
Killer App: Integer Factorization: Competition

- 2002: Polynomial-time integer primality test

- Perhaps integer factorization will also succumb to pure math
  - Easy to dismiss this until you review the past 50 years of progress:
    - 1970: Proof that Hilbert’s 10th problem is unsolvable
    - 1976: Proof of the four-color problem (stood for centuries)
    - 1984: Polynomial-time algorithm for solving linear programming problems
    - 1994: Proof of Fermat’s Last Theorem (stood for centuries)
    - 1998: Proof of Kepler’s conjecture (sphere packing, stood for centuries)
    - 2002: Proof of Catalan’s conjecture (2^3 and 3^2, stood for centuries)
    - 2003: Proof of the Poincaré conjecture (topology)
    - 2004: Proof of the classification of finite simple groups
    - 2013: Proof that there is no bound on the values of pairs of primes differing by a finite number (first real progress in more than two millennia)

- So QC needs to step lively if it wants this one!
Killer App: Grover's Search Algorithm for DBMS: Search Length-N Unordered in $O(\sqrt{N})$ time

When there are sufficient searches, classical computing wins
Killer App: Grover's Algorithm Remaining Hope: Cases Where List is Implicit, Need Not Be Formed

Quantum

O(√N) Search

Length-N Unordered Implicit List

Classical

O(????) Search

Searching for factors of a large composite number is one example
Killer App: Traveling Salesman Problem (TSP)

Polynomial-time algorithm guaranteed within 40% of optimal solution
2006 solvers finding optimal solutions to 85,900-city problems
Seven years for D-Wave to catch up, assuming one qubit per city and no classical-computing progress
Killer App: Boolean Satisfiability (SAT) Problem

SAT is NP-complete, but heuristics' capabilities doubling about every 1.3 years. Early experiments incorporating machine learning showing some promise. Classical computing is putting up an impressive fight!!!
Killer App: Solving Other Optimization Problems

- To be fair, TSP and SAT have received huge investments
  - Classical computing thus has a huge head start
  - Machine learning also likely to help in near term

- Perhaps less well-known problem become important
  - And provide QC with a level playing field
  - One possible current example: SAT involving pigeonhole principle

- To probe deeper:
Killer App: Quantum Mechanical Dynamics (QMD)

Consumes entire clusters inverting billion-row/column sparse matrices
IBM, Microsoft, Harvard interested, IBM looking to 50-qubit PoC
H₂, LiH, BeH₂ thus far (https://arxiv.org/abs/1704.05018)
Chinese researchers looking to QC for quantum photon modeling
Competition: fold.it, machine learning, advances in physical chemistry
IBM used up to six qubits of its superconducting quantum processor to address electronic structure problems for the molecules $\text{H}_2$, $\text{LiH}$ and $\text{BeH}_2$.

50-qubit system performance/scalability PoC planned

Killer App: Gaming???

We start with Player 1.
Look away Player 2!

The lines in the bowtie shape below are the places you can place your ship.

```
|\ |  /
|d b |
| \ / |
|f X a
| / \ |
| e c |
|/   \|
```

Choose a line for your ship. (a, b, c, d, e or f)

Player 2: You're up!

Quantum Computing and Linux?
Quantum Computing and Linux?

But this is quantum computing!!!
Quantum Computing: Why not Superposed OSes?

Windows Kernel

Quantum Computer Hardware
Quantum Computing: Why not Superposed OSes?

Not without a **lot** more qubits!!!
Quantum Computing and Linux?

Accelerator, similar to GPGPU or FPGA
But no context switching, at least not until quantum memory
Quantum Computing and Linux?

Maybe qubit-division multiplexing? Isolation? Security?
Quantum Computing and Linux?

Maybe qubit-division multiplexing? Isolation? Security?
Need quite a few more qubits before this is a real problem!!!
Quantum Computing and Open Source???
Quantum Computing and Open Source???

Open-Source Application

Proprietary Application

Open-Source Libraries

Linux Kernel

Drivers

Firmware?

Quantum Computer Hardware

Classical Computer Hardware

We should expect the collaboration to continue!!!
Quantum Computing and Open Source??

Open-Source Application

Proprietary Application

Open-Source Libraries

Linux Kernel

Drivers

Firmware?

Classical Computer Hardware

Quantum Computer Hardware

We should expect the collaboration to continue!!!
Quantum Computing Hardware and Open Source???
Quantum Computing Hardware and Open Source???
Summary
Summary

- Within past decade, QC moved from theory to real hardware
- QC will be accelerator, shared by partitioning
  - We won't be running Linux on QC itself, not anytime soon, anyway
  - But a great deal of open-source software will surround QC
- QC needs killer app: Some possibilities, but jury still out
  - Optimization and quantum mechanical dynamics current best bets
  - Note: Quantum cryptography already seeing some use
- Classical computing is putting up quite a fight!!!
  - Competition should be good for end users no matter who wins
- Free advice:
  - If you can afford it, do both classical and quantum computing
  - If you can only afford one, stick with classical computing
Summary

- Within past decade, QC moved from theory to real hardware
- QC will be accelerator, shared by partitioning
  - We won't be running Linux on QC itself, not anytime soon, anyway
  - But a great deal of open-source software will surround QC
- QC needs killer app: Some possibilities, but jury still out
  - Optimization and quantum mechanical dynamics current best bets
  - Note: Quantum cryptography already seeing some use
- Classical computing is putting up quite a fight!!!
  - Competition should be good for end users no matter who wins
- Free advice:
  - If you can afford it, do both classical and quantum computing
  - If you can only afford one, stick with classical computing
  - Disclaimer: This advice is subject to change without notice
Legal Statement

- This work represents the view of the author and does not necessarily represent the view of IBM.

- IBM and IBM (logo) are trademarks or registered trademarks of International Business Machines Corporation in the United States and/or other countries.

- Linux is a registered trademark of Linus Torvalds.

- Other company, product, and service names may be trademarks or service marks of others.
Questions?