The status of quantum computing versus semi-quantum computing

Round-Table ICQNM 2015

Tal Mor
Technion, Haifa, Israel
D-Wave collaborations

In 2011, Lockheed Martin signed a contract with D-Wave Systems to realize the benefits based upon a quantum annealing processor applied to some of Lockheed's most challenging computation problems. The contract includes the purchase of a "128 qubit Quantum Computing System".

In 2013, a "512 qubit system" was sold to Google and NASA.

Researchers believe that D-Wave model is probably not a quantum computing model. But is it stronger than "classical"?
A “good” quantum computing device – ion trap

- Reached 14 qubits
- Nobel Prize and Wolf Prize

sciencedaily.com
• **Josephson Junctions (the technology Dwave is based upon):** 3-5 qubits, maybe 8 (Dwave?)

• **Q. Optics (7-8 qubits)**

The Australian Centre of Excellence for Quantum Computation and Communication Technology
Current status of fully-quantum computing

• Despite the Nobel prize – we have no clue when ion traps will reach 25 qubits

• Despite of 20M $ D\text{WAVE} \text{ computers already sold} – \text{we have no clue if JJ qubits are of any good}; \text{ We do know (Shin, Smith Smolin, Vazirani; 2014) that there is probably no reason to believe that the D\text{WAVE} \text{ model is quantum}
Limited QC Models:
Semi-quantum computing

- D-Wave’s [???] (closely related to JJ-QC)
- One Clean Qubit (closely related to NMR-QC)
- Linear Optics (closely related to Optics-QC)

Three Extremely Important Questions:
- What algorithms can the limited models run? [OCQ – Trace estimation; LO – boson sampling]
- What kind of Quantumness/Entanglement is there?
- Do they scale much easier/better than full QC?
Quantum Key Distribution and its Applications
Round Table Discussion
ICQNM 2015, 23. – 27. August, Venice

Stefan Schauer
QKD and its Applications

- QKD provides highly (unconditional) secure communication
- Important in several fields where sensitive data is transmitted (government, research, finance, medical, military, etc.)
- Competition with classical solutions is high
  - Devices for classical cryptography are well established
  - Provide high transmission rates and “good” security
- Some applications for QKD have already been developed
  - Well-defined protocols for the communication (Q3P)
  - Integration into standard networks (quantum and classical links)
  - Integration into IPSec (keys coming from QKD)
  - Integration into applications (telephone conferences secure by QKD)
- QKD still faces several challenges before entering day-to-day life
Challenges in QKD

- **Challenge 1: Distance**
  - First implementations over a few centimeters in the lab
  - Today distance of several hundred kilometers possible
  - Losses are rather high – key rate is rather low
  - Quantum networks might be a solution

- **Challenge 2: Bandwidth**
  - Large distances don’t allow a high transmission rate (e.g. ~3bps @ 300km, ~10bps @ 200km)
  - Photon sources and detectors are not perfect and introduce errors
  - Channels are lossy and quantum states are influenced
  - Nevertheless efficient rates are possible at a short distance (e.g. 450 kbps over 25km)
Challenges in QKD

- **Challenge 3: Handling**
  - QKD Systems are rather complex
  - High-end physics and sophisticated hardware involved
  - Hard to maintain in practice (configuration of the system)
  - Trend goes towards “Out-of-the-Box” systems (e.g. ID Quantique) and “QKD-on-a-Chip”

- **Challenge 4: Implementation**
  - QKD is secure in theory
  - In practice there are several physical limitations (e.g. single photon detectors, finite key length, …)
  - Several loopholes and backdoors have been identified in the last years
QKD Networks

- Several installations of QKD networks

- Nodes in the network are connected using quantum links
  - QKD is performed over these links
  - Integration of several different physical implementations

- Usually restricted to a metropolitan area

- Network serves as a backbone for “classical” users and can be accessed over specific nodes and interfaces

- Hierarchical (layered) approach to provide an abstraction for the protocols and applications on higher levels
QKD Networks

- Vienna (2008):  
  - First installment of a network secured by QKD  
  - Six locations across Vienna  
  - Largest Distance over 80km  
  - Application of text, audio and video encryption
QKD Networks

- Tokyo (2010):
  - Network with distances up to 45km
  - Integration of different technologies
  - Application of a secure text, audio and video transmission
QKD Networks

- China (2016):
  - Largest QKD network so far
  - 2000km link between Beijing and Shanghai
  - Large number of nodes to connect them

- Satellite communication secured by QKD as a next step
A Quantum Computer: Dream or Reality

Thierry Ferrus
Hitachi Cambridge Laboratory

Round table on ‘Quantum : getting the momentum’
Outline

Could we (really) realise a quantum computer?

Copenhagen interpretation and no-cloning theorem

Large scale networks
Could we realise the computation part?

- Coherence time, scalability, high-fidelity readout

Could we realise a quantum memory?

- No-cloning theorem

Could we displace qubits over μm distances?

- Surface acoustic waves, photonic crystals…
Do we need a classical circuit to operate a quantum one?

- Pulsing and general operations

The Copenhague interpretation: what about measurement?

- Weak measurement is a measurement...

What about large networks

- Repeaters, fibres, local/flying qubits
A Quantum Computer : Dream or Reality

Thierry Ferrus
Hitachi Cambridge Laboratory
HITACHI
Inspire the Next