



Quantum computing: software perspective

ANDRIS AMBAINIS

CENTRE FOR QUANTUM COMPUTER SCIENCE

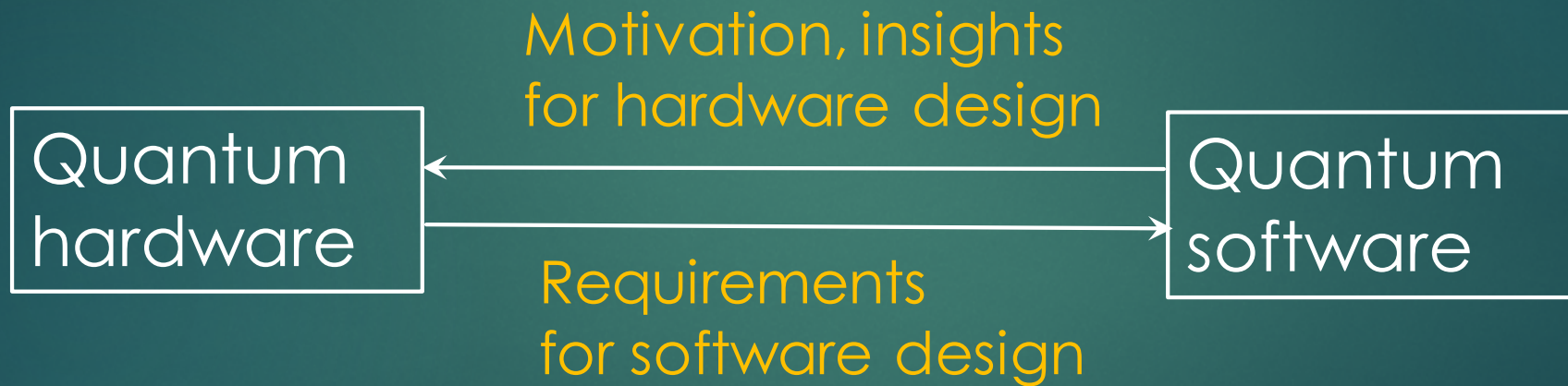
UNIVERSITY OF LATVIA

Motivation for quantum computing

- ▶ Computing model based on different physical laws.
- ▶ Exponentially larger internal memory.
- ▶ Useful for simulating physics and chemistry.
- ▶ Also useful for data processing.
- ▶ Envisaged since 1980s, becoming reality now.

Software/hardware co-design

- Research on quantum hardware and quantum software should proceed together.



Quantum simulation

- ▶ Equations of quantum physics (e.g. Schrodinger equation).
- ▶ Hard for classical computers (10% of supercomputer time).
- ▶ Applications: chemical processes, better materials, drug design.
- ▶ Current research: optimal algorithms for quantum simulation.

Quantum codebreaking

- ▶ Quantum computers can break widely used encryption systems (RSA, El-Gamal, Diffie-Hellman, etc.).
- ▶ Quantum computers can take advantage of mathematical structure of popular cryptosystems.
- ▶ Current research: what data encryption is quantum-safe?

Search, scheduling, AI, etc.

- ▶ Quantum speedups for several basic search methods (e.g. backtracking).
- ▶ Variety of applications, from scheduling to natural language processing.
- ▶ Current research: quantum advantage for machine learning and AI?

Causes of quantum speedups

- ▶ Quantum parallelism: quantum computers can perform many computations in parallel.
- ▶ Quantum interference: results of these computations can be combined into one.
- ▶ Challenge: set up interference so that useful result is obtained.
- ▶ Big speedups for problems with appropriate mathematical structure.

Near term opportunities

- ▶ Quantum advantage: current quantum devices can no longer be simulated on a classical supercomputer.
- ▶ Computations of depth 20-50.
- ▶ Many applications: computations of depth 10,000 and more.
- ▶ Both hardware and software effort needed to close the gap.

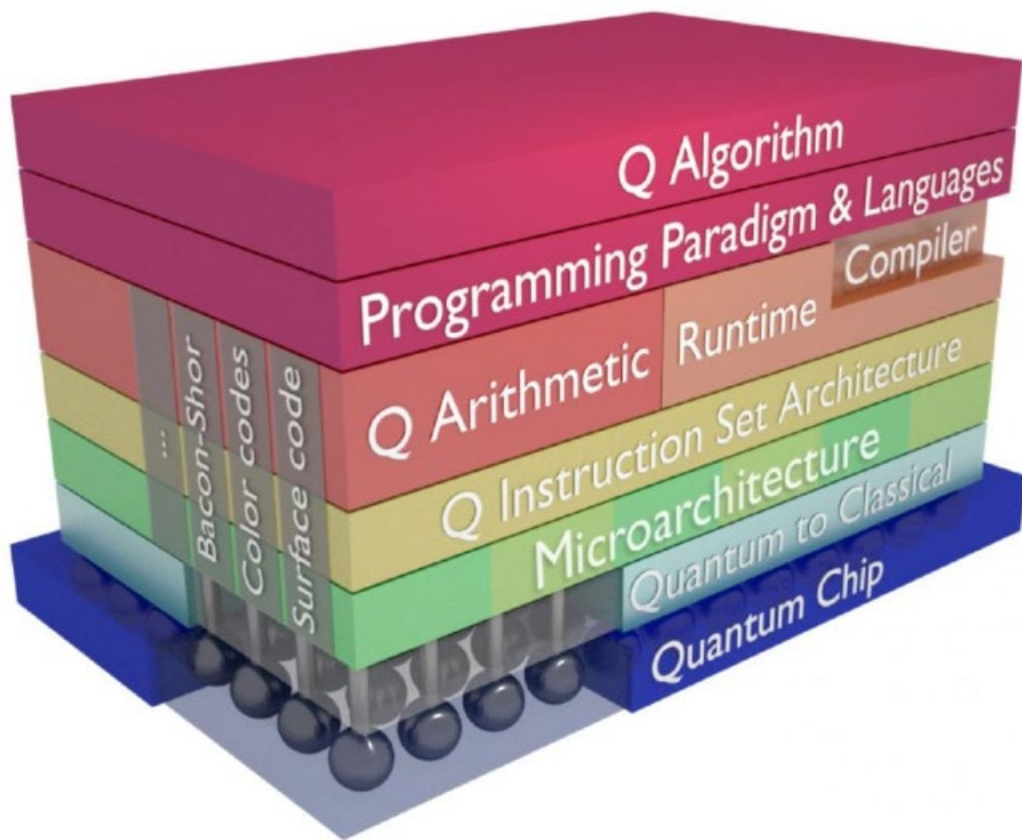
Quantum error correction

- ▶ Detecting and correcting errors on the software level.
- ▶ Error correction threshold: between 10^{-3} to 10^{-2} .
- ▶ Increase in circuit size required.
- ▶ Challenge: develop more efficient protocols for error correction.

Quantum internet

- ▶ Quantum Communication Infrastructure (QCI) – part of Digital Europe.
- ▶ Challenge: what protocols can we run on quantum internet?

Quantum software stack



Most difficult:

- Quantum chips
- Quantum algorithms

Call to action



- ▶ Quantum software is essential for the quantum computing endeavour.
- ▶ Specific support programmes are needed.
- ▶ Grand challenges (fundamental methods of computation, error correction, cryptography) need to be supported.

European Quantum Software Institute



- ▶ QuSoft, Amsterdam.
- ▶ QMATH, Copenhagen
- ▶ Portuguese Quantum Institute, Lisbon.
- ▶ Technical University of Munich.
- ▶ Paris Centre for Quantum Computing.
- ▶ University of Latvia, Riga.

To be launched in November 2022.

Quantum software ecosystem

