Prospects and applications of quantum programming

Jarosław Miszczak
IITiS PAN, Gliwice, Poland

25th International Conference on Industrial Engineering and Engineering Management 2019,
August 23-26, 2019, Ma'anshan, China

Outline

Goals of the talk

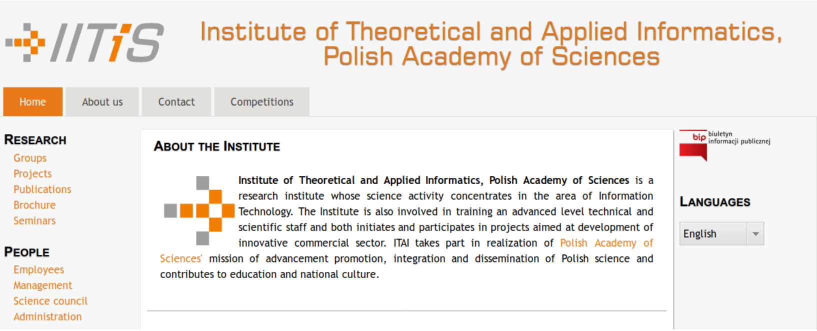
Quantum computing

Quantum platforms and software

Applications of quantum computing

What next?

About IITiS PAN



Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, Gliwice, Poland

https://iitis.pl

About IITiS PAN

Goals of the talk

- Provide basic facts about quantum computing.
- Present available quantum hardware and software platforms.
- Describe possible applications of quantum computing.

Quantum computing

Quantum computing

Quantum computing is a model of computation based on the rules of **quantum mechanics**.

Quantum mechanics can be described on the level of **vectors and unitary matrices** or using **energy levels of Hamiltonian**.

Digital vs. analog

The first appraoch leads to **digital quantum computing**, while the second can be see as **analog quantum computing**.

Quantum computing
Digital quantum computing

Adventage

Parallel execution enabling the speed-up for solving hard problems.

How to use this model?

- Input data have to be encoded into **quantum registers**.
- Sequence of quantum gates (ie. quantum circuit) has to be prepared – **constructed and implemented**.
- **Quantum error correction** is needed to maintain the quantum state during the execution.

Quantum computing

Digital quantum computing – One bit

For one bit we have two possible states.

- We **encode them into vectors** $\vec{0}$ and $\vec{1}$ (or $|0\rangle$ and $|1\rangle$ as it is more commonly used).
- Vectors can be added, so $\vec{0} + \vec{1}$ (or $|0\rangle + |1\rangle$) is also a state.
- We need to fix the length if the length of each component can be **interpreted as a probability**.
- Any operation on these vectors should preserve the length – such operations are represented by **unitary matrices**.

That's it – we have **one qubit** and we can process data in **superposition**.

Quantum computing

Digital quantum computing – Two bits

Two bits can be represented using one qubit twice – or rather wiring two qubits together.

- States are $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle$.
- Tensor product $\otimes$ is needed to **preserve linearity**.
- So $|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle$ is also a state.

And in this way we get **quantum registers** and **entangled states**.

Quantum computing

Analog quantum computing – Evolution of quantum systems

Adventage

Fast solution of optimization problems based on **specialized hardware**

A state of the quantum system tends to the minimum energy.

The state is described by time-independent Schrödinger equation

$$\hat{H}|\psi\rangle = E|\psi\rangle.$$

The logic of our problem has to be encoded into the Hamiltonian operator $\hat{H}$ representing the energy of the system.

Quantum computing

Analog quantum computing – QUBO

Quadratic unconstrained binary optimization (QUBO) problem

Minimize the value of the quadratic form

$$E_{\mathrm{QUBO}} = \sum_i Q_{ii} x_i + \sum Q_{ij} x_i x_j$$

on the space of binary vectors.

Using matrix notation this is equivalent to

$$\min_{\vec{x} \in \{0,1\}^n} \vec{x}^T Q \vec{x}.$$

Quantum computing

Analog quantum computing – Ising model

Simple and powerful model for describing quantum systems, successfully used in statistical mechanics.

The energy of the system is described by the function

$$H = \sum_{i=1} h_i s_i + \sum_{i \sim j} J_{ij} s_i s_j,$$

with $s_i \in \{-1, +1\}$.

Quantum computing

Analog quantum computing – Ising model

In the quantum realm this function is represented by an operator $\hat{H}$, where values s_i are replaced by operators with two eigenvalues.

Calculating ground state of the Ising Hamiltonian is equivalent to solving QUBO with mapping

$$s \mapsto 2q - 1.$$

Quantum computing

Analog quantum computing – QUBO and Ising model

QUBO to Ising mapping provides logic for embedding optimization problems in quantum systems.

Problem formulation	Term			
	linear	quadratic	variable	states
QUBO	Q_{ii}	Q_{ij}	x_i	$\{0, 1\}$
Ising model	h_i	J_{ij}	s_i	$\{-1, +1\}$
QPU (physical device)	qubit bias	coupling strength	qubit state	$\{\uparrow, \downarrow\}$

Quantum system undergoes the evolution leading to the optimal solution of the problem given in the form of the total energy of the system.

Quantum computing

Analog quantum computing – XNOR gate

Simple example – find a configuration of x_1 and x_2, fulfilling the condition of XNOR gate – output 1 if inputs are identical.

The energy function is given by

$$f(\vec{x}) = a_1 x_1 + a_2 x_2 + b_{12} x_1 x_2.$$

Using biases $a_1 = \alpha$, $a_2 = \alpha$ we introduce penalty for states $(x_1, x_2) = (0, 1)$ and $(x_1, x_2) = (1, 0)$. To promote state $(1, 1)$ we introduce coupling $b_{12} = -\frac{1}{2}\alpha$.

Quantum computing

Advantages of quantum computers

- **Parallel execution** enabling the speed-up for solving hard problems.
- Fast solution of optimization problems based on **specialized hardware**.

Quantum platforms and software

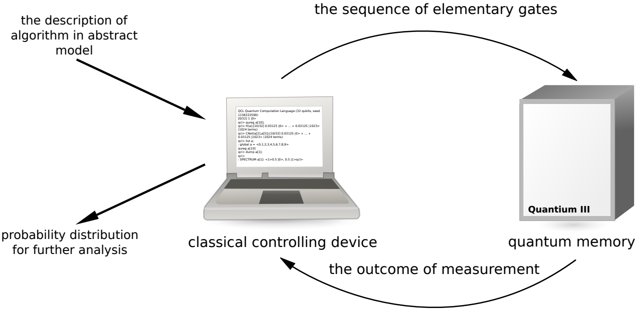
Quantum platforms and software

Quantum programming is a process that leads from an **original formulation** of a computing problem to **executable** quantum computer programs.

Quantum platforms and software

Quantum co-processor

QRAM $\equiv$ Quantum Random Access Machine



(E. Knill. Conventions for quantum pseudocode. Technical report, LANL, 1996.)

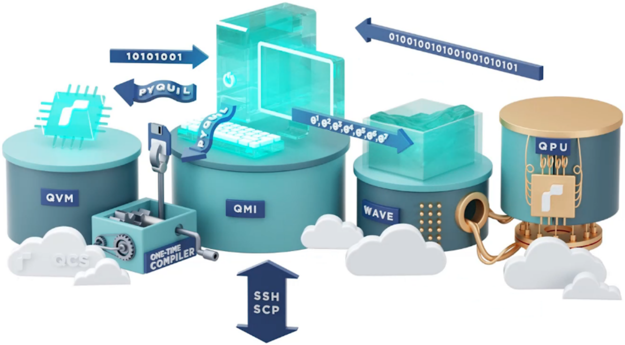
Quantum platforms and software

Quantum co-processor

- Developed for describing gate model of quantum computing – digital quantum computing with classical controlling device.
- Crucial assumption: **quantum and classical parts are suitable for different types of computation**.
- Nowadays quantum computing is delivered as service, not as machine available for the user – quantum computing as a service (QCaaS) appraoch.

Quantum platforms and software

QRAM/QPU in the cloud

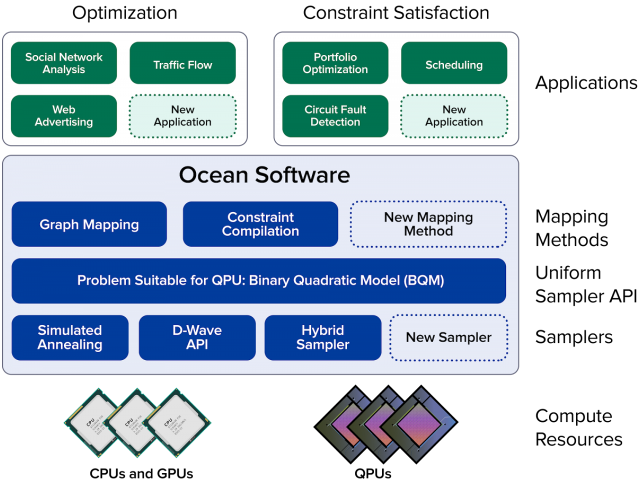


Quantum Cloud Services

Source: http://rigetti.com/qcs

Quantum platforms and software

QRAM/QPU in the cloud (mixed model)



D-Wave software environment

Source: https://www.dwavesys.com/software

Quantum platforms and software

Quantum middleware

Quantum computers are expensive $\rightarrow$ utilize a layer of intermediary software to provide access to your machine.

Usually this is

- embedded domain specific language $\rightarrow$ Python with library of functions
- data abstraction $\rightarrow$ allocation of classical and quantum registers based on qu(b$|$d)its
- classical control of quantum memory $\rightarrow$ by using host language
- quantum functions $\rightarrow$ custom gates defined by matrices or compound statements

Quantum platforms and software

Software for quantum hardware

In terms of software $\rightarrow$ hardware (or planned hardware)

- QISKit $\rightarrow$ IBM
- pyQuil $\rightarrow$ Rigetti
- ProjectQ $\rightarrow$ IBM (and other backends)
- Leap (cloud service) $\rightarrow$ D-Wave Systems
- Quantum Development Kit/Q# $\rightarrow$ Microsoft (???)
- Cirq $\rightarrow$ Google (???)
- QX Simulator $\rightarrow$ Intel/QuTech (???)

Quantum platforms and software

Software for quantum hardware

- *[]designing a language that enables a programmer to exploit quantum interference in a quantum algorithm is a unique and nontrivial challenge.*[1]

[1] Quantum Computing. Progress and Prospects, The National Academies Press, 2019

Applications of quantum computing

Applications of quantum computing

Digitial vs. analog

- Digital – we are interested in the exact solutions.
- Analog – the approximate solutions are also interesting.

Note!

In both regimes we have to deal with probabilistic answers!

Applications of quantum computing
Fast factorization

- Invented in 1994 by the American mathematician Peter Shor.
- Task: Given an integer n, find its prime factors, p_1 and p_2, such that $p_1 p_2 = n$.
- Running time: $\mathcal{O}(\mathrm{poly}(\log n))$.
- Can be used to **attack cryptosystems based on RSA**.

Applications of quantum computing

Fast factorization

- Resulted in significant efforts for delivering cryptographic solutions immune to quantum computers.
- The 7th ETSI/IQC Quantum Safe Cryptography Workshop organized by ETSI in partnership with Amazon Web Services (AWS)

Applications of quantum computing

Unconditionally secure cryptography and quantum internet

- Invented in 70s (Wiesner), 80s (Bennett and Brassard), and 80s (Ekert).
- Task: Send a bit without giving opportunity to read it while not being detected.
- Based on the **no-cloning theorem** – quantum state cannot be copied, you destroy it in the process of measuring.
- Provides unconditional security.

Applications of quantum computing

Unconditionally secure cryptography and quantum internet

- Available commercial solutions.
- Proposed standards and protocols.

A Link Layer Protocol for Quantum Networks

Axel Dahlberg[1,2], Matthew Skrzypczyk[1,2], Tim Coopmans[1,2], Leon Wubben[1,2], Filip Rozpędek[1,2], Matteo Pompili[1,2], Arian Stolk[1,2], Przemysław Pawełczak[1], Robert Knegjens[1], Julio de Oliveira Filho[1], Ronald Hanson[1,2], Stephanie Wehner[1,2]

[1]QuTech, Delft University of Technology and TNO
[2]Kavli Institute of Nanoscience, Delft University of Technology
s.d.c.wehner@tudelft.nl

Applications of quantum computing

Optimization

- Task: Find the best of many possible combinations.
- Rule: Every system tends to evolve towards a minimum energy state.

Applications of quantum computing

Optimization

- Energy of quantum systems can be described using Ising model.
- Quantum processing unit (QPU) is used to provide solutions described by the configuration with minimum energy.
- D-Wave represents problems as a binary quadratic model (BQM).

Note

QUBO can be used to run optimization on many types of devices, not necessarily quantum.

Applications of quantum computing

Optimization

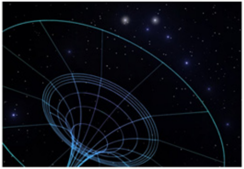
Labeling images

Extracting meaning from news stories

Detecting and tracking objects in images

Finding correlations in bioinformatic data

Improving natural language in machines



Creating and testing scientific hypotheses

Source: https://www.dwavesys.com/

Applications of quantum computing

Machine learning

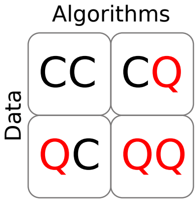
Quantum systems produce atypical patterns that classical systems are thought not to produce efficiently, so it is reasonable to postulate that quantum computers may outperform classical computers on machine learning tasks

(J. Biamonte *et al.*, *Quantum machine learning*, Nature, Vol. 549 (2017))

Applications of quantum computing

Machine learning

Quantum machine learning aims at utilizing the advantages of quantum computing in the context of data processing. This can be achieved in many scenarios...



Applications of quantum computing

Machine learning

Where can quantum computers help in machine learning?

- Many methods in machine learning require iterative optimization – quantum version of procedures such as PCA can be used to improve their performance.
- Analysis of quantum data using quantum computers can be achievable on small devices.

What are the limitations of quantum computers?

- Loading data in QRAM-based machines is costly (and currently impossible).
- Without good optimization, the circuit size and circuit depth overhead can outweigh the advantages.

Applications of quantum computing

Startups in quantum computing

1QBit
Cambridge Quantum Computing
ENTROPICA LABS
GTN LTD
HQS QUANTUM SIMULATIONS
OTI
ProteinQure
QC WARE
Qu & Co
QULAB
QunaSys
Q^xBranch
rahko
RIVERLANE
SolidStateAI
STRANGE WORKS
ZAPATA

(Source: https://www.microsoft.com/en-us/quantum/quantum-network)

Applications of quantum computing

Volkswagen/D-Wave collaboration

Quantum Computing at Volkswagen:

Traffic Flow Optimization using the D-Wave Quantum Annealer

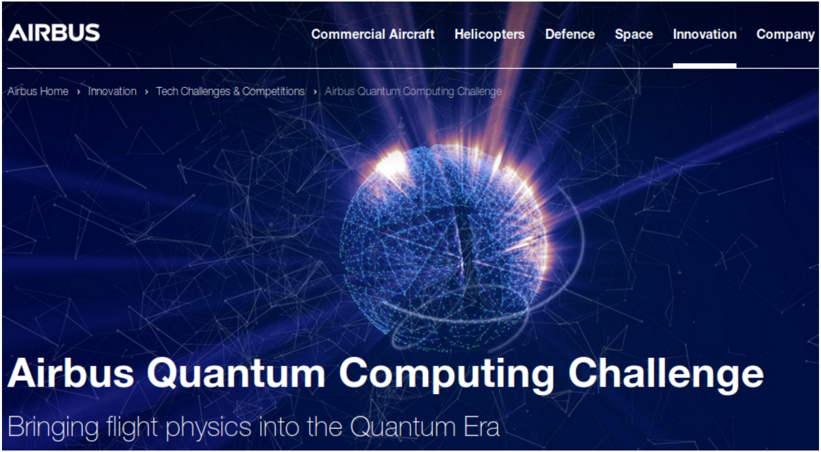
D-Wave Users Group Meeting - National Harbour, MD

27.09.2017 – Dr. Gabriele Compostella

Report: https://www.dwavesys.com/sites/default/files/VW.pdf

Applications of quantum computing

Airbus Quantum Computing Challenge



Launch: January 2019.

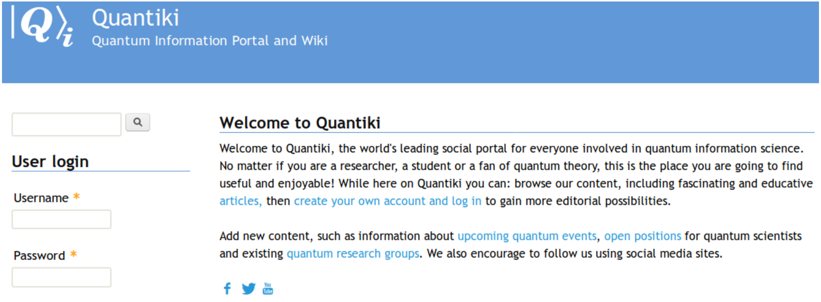
Applications of quantum computing

Challenges

- Development of new algorithms **harnessing quantum parallelism** for real-world problems.
- Utilization of existing hardware to benefit from **small quantum computers** – noisy intermediate-scale quantum (NISQ) technology.
- Construct **optimized programs** for specific quantum hardware.

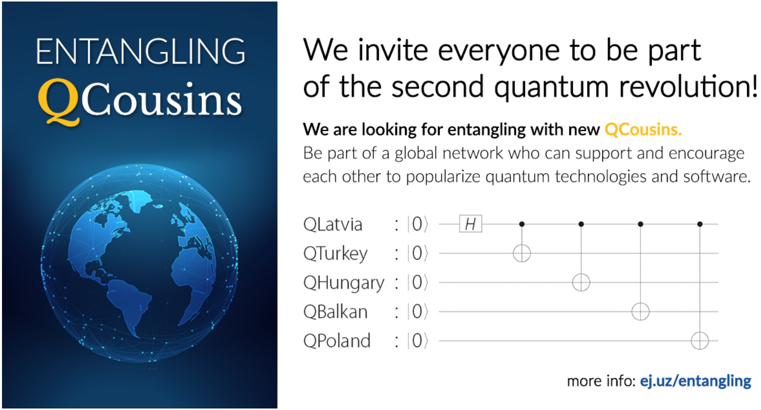
What next?

- Quantum Computing. Progress and Prospects, The National Academies Press, 2019 (https://www.nap.edu/read/25196/)
- J. Miszczak, *Quantum programming tutorial: slides and code examples* (https://github.com/jmiszczak/qprog-tutorial)
- Quantiki – Quantum Information Portal and Wiki (https://quantiki.org/)



What next?

QWorld – initiative by Center for Quantum Computer Science, University of Latvia, groups from Poland, Hungary, Turkey...



Thank you.

https://iitis.pl/∼miszczak