Research Institute
Cyber Defence
Bundeswehr University Munich

Report – Workshop 3 “Bid Data”

The focus of the workshop "Quantum Computers and Applications" at CODE 2019 was on software and application examples.
Moderation and Organization:
Klaus Buchenrieder, Ph.D, Research Institute CODE
Dr. Wolfgang Gehrke, Research Institute CODE, moderator

Sebastian Zielinski from the Ludwig-Maximilians University in Munich held the talk "Software for adiabatic QC".
The major topic was solving problems on a quantum annealing platform.
By example of NP-hard combinatorial optimization problems like 'traveling salesman' and 'graph coloring', the speaker showed a quantum annealing approach to solving these types of problems using the the D-Wave Ocean SDK and discussed the need to make quantum computing more accessible to programmers that are not necessarily experts in quantum computing. The talk concluded with a discussion on noise in quantum computing as well as interconnectivity, number, and entanglement duration of qubits.

Damian Steiger from Microsoft presented the talk 'Q# and and quantum inspired optimization' and showed the potential of quantum computing as an accelerator for specific compute intensive problems from the field of biology, chemistry, medical imaging, or traffic optimization. He further presented the programming language Q# as a means to implement and debug quantum algorithms with Visual Studio and VSCode, integrating CPUs, FPGAs and quantum hardware for quantum inspired optimization. The talk concluded with a discussion on quantum error correction and the experimental implementation of a quantum computer using topological qubits.

François Varchon from IBM presented the open source software development kit 'Qiskit', which programmers can use to create quantum programs and run them over the internet on quantum computer prototypes of the IBM Q initiative.
After demonstrating this workflow by example of the 'Hello World' of quantum computing, the Bell State, the speaker went into depth on technical challenges and techiques in quantum computing. The topics included connectivity limitations, error mitigation, and quantum circuit optimization with transpilers.

Leonie Bruckert from Secunet Security Networks AG talked about 'Post Quantum Cryptography' as an answer to the challenges that quantum computers present for conventional cryptography.
The speaker first discussed the effects of quantum algorithms ,e.g., Grover and Shor, on the security of symmetric and asymmetric cryptography and hash algorithms, followed by a presentation of different mathematical approaches in post quantum algorithms (lattice-based, isogeny-based, etc.) and their challenges with regard to large keys and large signatures.The talk concluded with a discussion of the applicability of post quantum algorithms in resource constrained devices like smart cards.

Challenges for future research in quantum computing presented themselves during the workshop

Error Correction
The need for efficient quantum error correction derives directly from decoherence and noise in quantum computing leading to data errors. Improved error correction can enable more reliable and more complex computations.

Quantum Circuit Combination
Another identified challenge is the efficient combination of simple quantum circuits into a more complex circuit.

Post Quantum Cryptography
Given that the typical time for introducing IT technologies at a large scale is 10 to 20 years, the development, standardization and technical availability of post quantum cryprography is of great importance.