A Novel Environment for Simulation of Quantum Computing

Joanna Patrzyk (1), Bartłomiej Patrzyk (1), Katarzyna Rycerz (1,2), Marian Bubak (1,2,3)

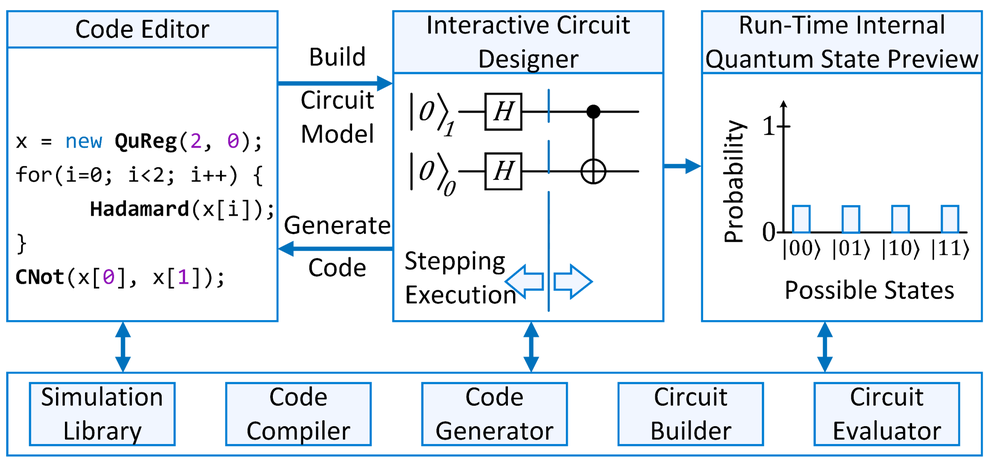
(1) AGH University of Science and Technology, Institute of Computer Science AGH, Department of Computer Science, al. Mickiewicza 30, 30-059 Kraków, Poland

(2) ACC Cyfronet AGH, Nawojki 11, 30-950,Kraków, Poland

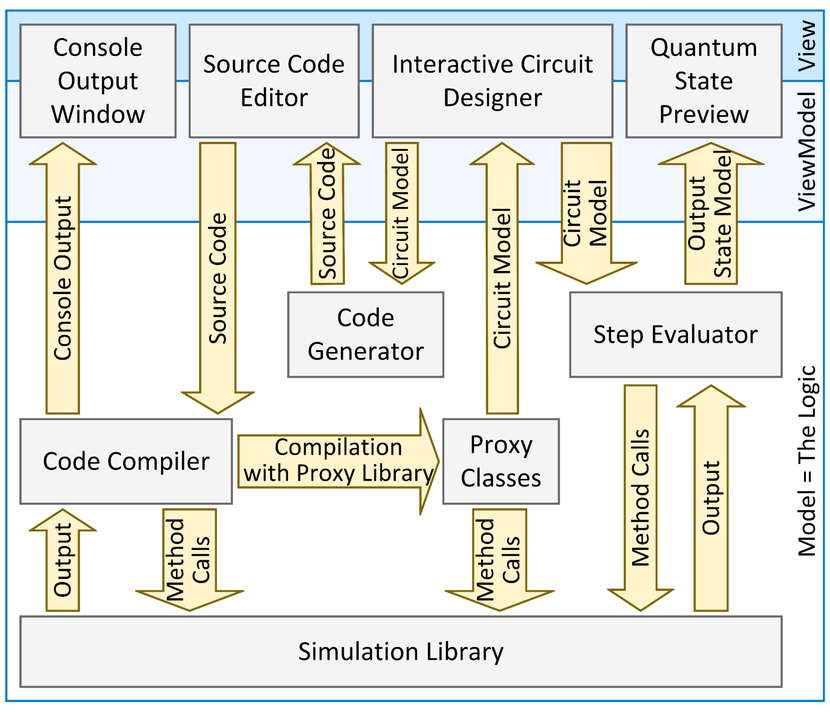
(3) University of Amsterdam, Institute for Informatics, Faculty of Science, Science Park 904, 1098XH Amsterdam, The Netherlands

QuIDE – Quantum IDE

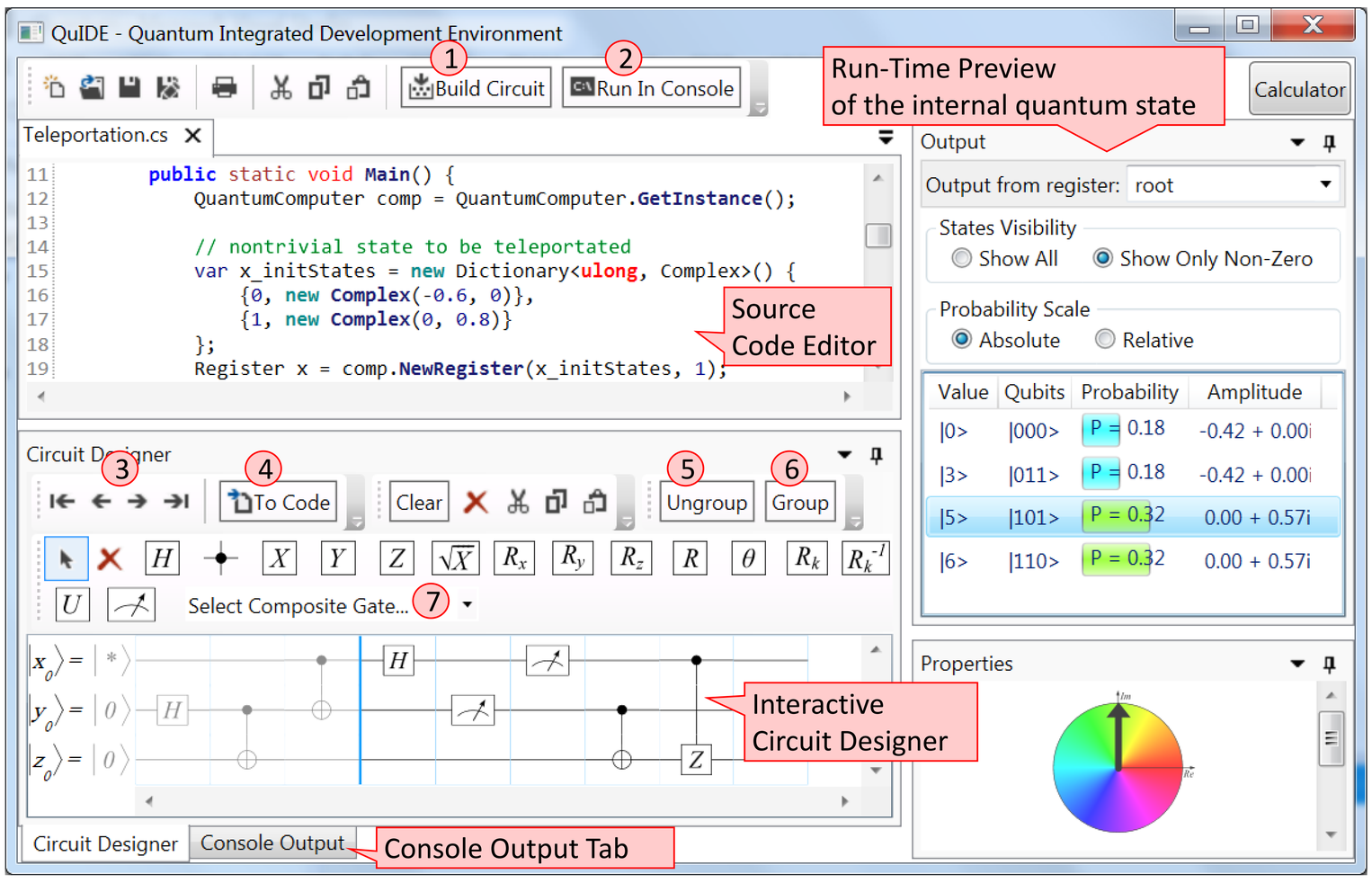
- Building and analysing quantum circuits and algorithms via source code and graphically
- step-by-step execution with the step back option
- preview of the actual internal quantum state



Architecture of QuIDE

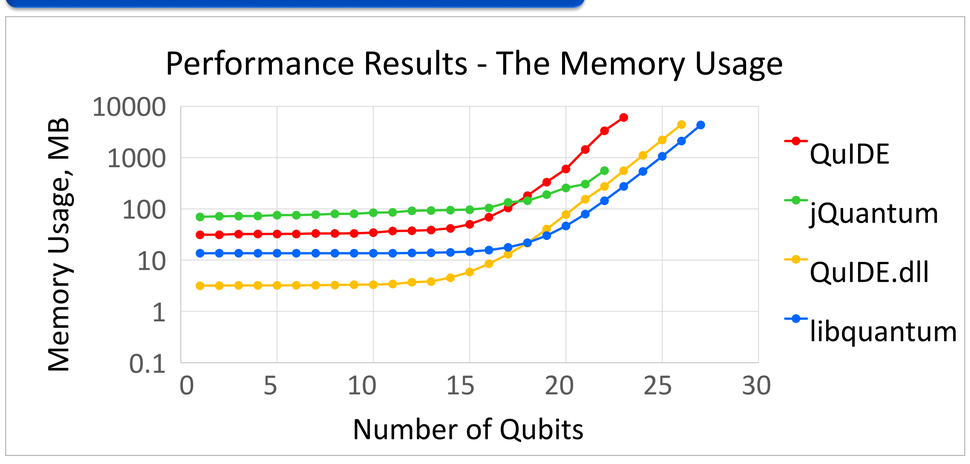


QuIDE User Interface



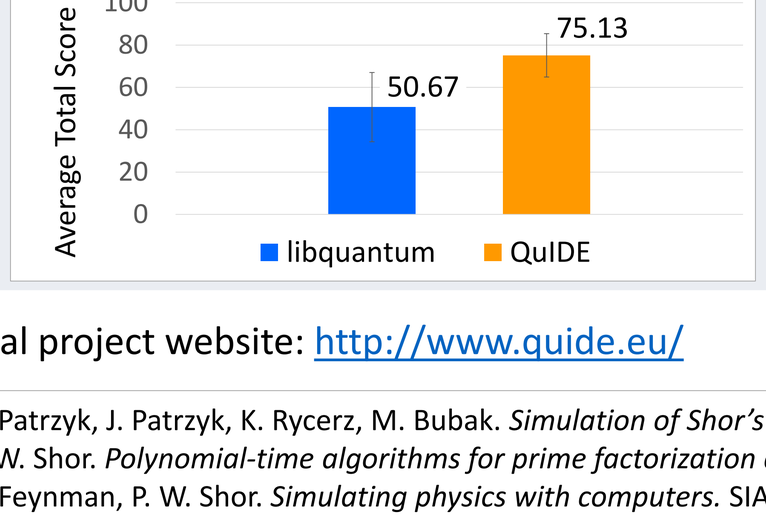
- users can generate the quantum circuit from the source code (1) as well as the source code from the circuit (4)
- the quantum circuit can be executed in the console (2) or evaluated step-by-step in the Run-Time Preview (3)
- the quantum gates in the circuit can be grouped into composite gates (6), which can be then ungrouped (5)
- a big set of predefined composite gates is available (7)

QuIDE Performance



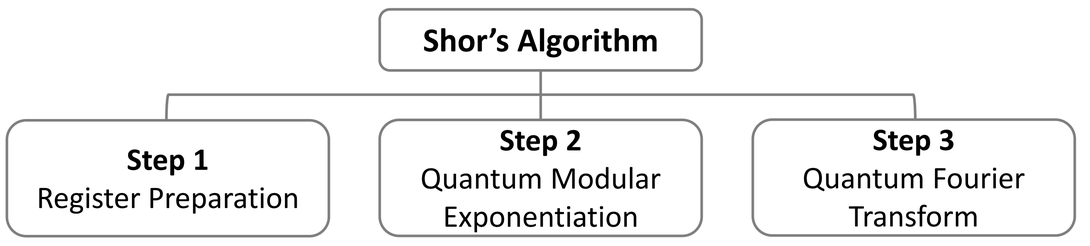
QuIDE Usability Evaluation

- QuIDE was used during the Quantum Computation classes at DCS AGH
- The students assessed the usability with the System Usability Scale
- QuIDE was compared to libquantum



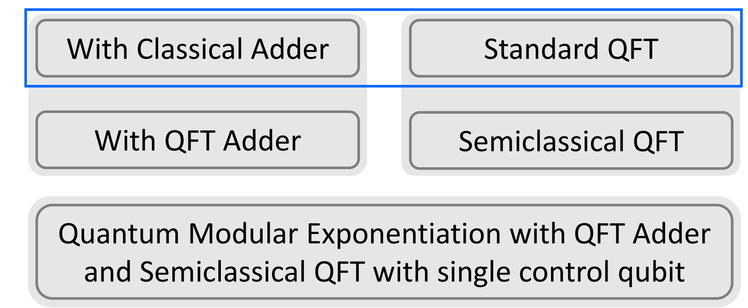
Simulation of Shor's Algorithm

Shor's Algorithm enables to factor numbers on quantum computer in polynomial time – it could thus compromise the RSA cryptosystem. Two optimization variants of the algorithm were implemented and compared.

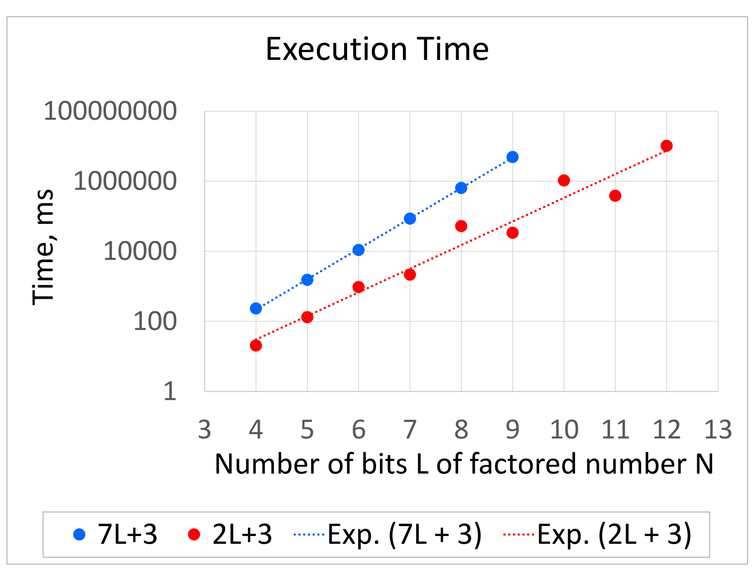


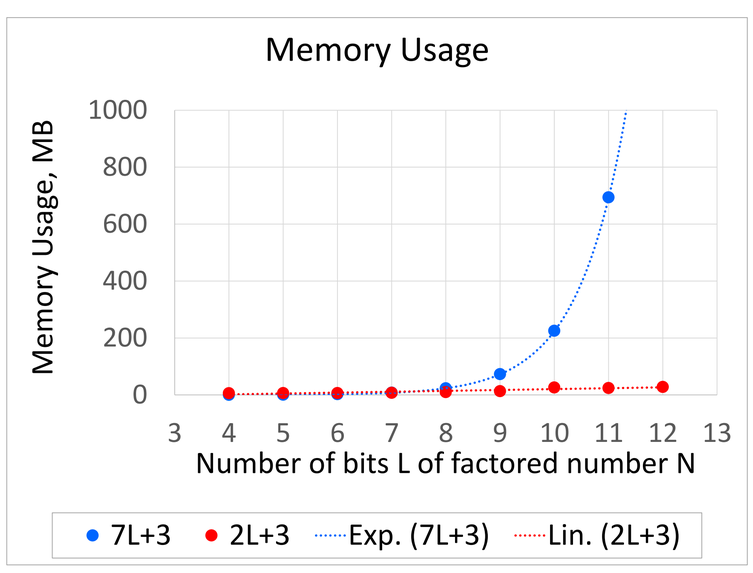
Implemented optimization variants:

- 1st Variant (7L + 3 qubits)*
- 2nd Variant (2L + 3 qubits)*



*L – number of bits of factored number





Official project website: http://www.quide.eu/

1. B. Patrzyk, J. Patrzyk, K. Rycerz, M. Bubak. *Simulation of Shor's algorithm optimization variants* (in preparation)
2. P. W. Shor. *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* SIAM J. Comput., 26(5):1484–1509, October 1997. ISSN 0097-5397.
3. R. Feynman, P. W. Shor. *Simulating physics with computers.* SIAM Journal on Computing, 26:1484–1509, 1982.

This study was partly supported by the AGH grant no 11.11.230.124 and also by Domain-oriented services and resources of Polish Infrastructure for Supporting Computational Science in the European Research Space – PLGrid Plus project no POIG.02.03.00-00-096/10

INNOVATIVE ECONOMY
NATIONAL COHESION STRATEGY

The work was co-funded by the European Regional Development Fund as part of the Innovative Economy program.

http://dice.cyfronet.pl

EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND