

CS667/CO681/PH767 Potential Project Topics

Note: You should feel free to pursue a project not on this list

Quantum walks: These can be used as quantum analogues of random walks, and have been shown to be useful for algorithmic purposes.

Two survey papers:

J. Kempe, “Quantum random walks – an introductory overview”.

<http://lanl.arxiv.org/abs/quant-ph/0303081>

A. Ambainis, “Quantum walks and their algorithmic applications”.

<http://lanl.arxiv.org/abs/quant-ph/0403120>

Also, a recent paper by:

F. Magniez, A. Nayak, J. Roland, and M. Santha, “Search via Quantum Walk”.

<http://xxx.lanl.gov/abs/quant-ph/0608026>

Quantum algorithms for solvable groups: Interesting algorithm for computing the size of solvable groups, and testing membership in such a group.

J. Watrous, “Quantum algorithms for solvable groups”.

<http://lanl.arxiv.org/abs/quant-ph/0011023>

The theory of fault-tolerant computing: These (lengthy) papers show that arbitrarily large quantum computers can be built from finite components whose accuracy and resilience to noise is bounded below some fixed constant. An overview and detailed explanation of some key component of one of these papers would be suitable for a course project.

D. Aharonov and M. Ben-Or, “Fault-Tolerant Quantum Computation with Constant Error Rate”. <http://lanl.arxiv.org/abs/quant-ph/9906129>

J. Preskill, “Fault-tolerant quantum computation”.

<http://lanl.arxiv.org/abs/quant-ph/9712048>

E. Knill, R. Laflamme, W. Zurek, “Threshold Accuracy for Quantum Computation”. <http://lanl.arxiv.org/abs/quant-ph/9610011>

Quantum “proof systems”: A number of results have emerged showing that the expressive power of proof systems increases when quantum information is available.

J. Watrous, “Succinct quantum proofs for properties of finite groups”.

<http://lanl.arxiv.org/abs/cs.CC/0009002>

J. Watrous, “PSPACE has 2-round quantum interactive proof systems”.

<http://lanl.arxiv.org/abs/cs.CC/9901015>

Continuous-time quantum algorithms: This is a variant of the query (black-box) model where queries can occur continuously in time.

E. Farhi and S. Gutman, “An Analog Analogue of a Digital Quantum Computation”. <http://lanl.arxiv.org/abs/quant-ph/9612026>

C. Mochon, “Hamiltonian Oracles”. <http://lanl.arxiv.org/abs/quant-ph/0602032>

Quantum self-testing: This is about verifying quantum devices that may be provided by adversarial parties.

F. Magniez, D. Mayers, M. Mosca, H. Ollivier, “Self-Testing of Quantum Circuits”. <http://xxx.lanl.gov/abs/quant-ph/0512111>

Classical simulations of stabilizer circuits: This is about an interesting restricted class of quantum circuits that is useful for quantum error-correction, but nevertheless can be efficiently simulated classically.

S. Aaronson and D. Gottesman, “Improved Simulation of Stabilizer Circuits”. <http://xxx.lanl.gov/abs/quant-ph/0406196>

Dihedral hidden subgroup problem: Simon’s Algorithm, as well as Shor’s Algorithms for factoring and discrete log can be seen as solving a more abstract problem: the *hidden subgroup problem*. This paper considers the hidden subgroup problem for a particular non-abelian group.

G. Kuperberg, “A subexponential-time quantum algorithm for the dihedral hidden subgroup problem”. <http://xxx.lanl.gov/abs/quant-ph/0302112>

Hidden subgroups for arbitrary groups: Simon’s Algorithm, as well as Shor’s Algorithms for factoring and discrete log can be seen as solving a more abstract problem: the *hidden subgroup problem*. This paper shows that the general case can be solved very efficiently in terms of black-box queries, but it uses exponentially many auxiliary operations.

M. Ettinger, P. Høyer, E. Knill, “The quantum query complexity of the hidden subgroup problem is polynomial”. <http://xxx.lanl.gov/abs/quant-ph/0401083>

Quantum Shannon theory: A generalization of classical Shannon theory, concerned with the capacities of noisy channels (quantum and classical).

P. Shor, “Capacities of quantum channels: how to find them”. <http://xxx.lanl.gov/abs/quant-ph/0304102>

Quantum algorithms for miscellaneous “traditional” problems: Employs quantum algorithms to obtain speed-ups for various traditional problems in computer science.

A. Ambainis and R. Spalek, “Quantum algorithms for matching and network flows”. <http://xxx.lanl.gov/abs/quant-ph/0508205>

C. Durr, M. Heiligman, P. Høyer, M. Mhalla “Quantum query complexity of some graph problems”. <http://xxx.lanl.gov/abs/quant-ph/0401091>

B. Furrow, “A panoply of quantum algorithms”.
<http://xxx.lanl.gov/abs/quant-ph/0606127>

Oracle interrogation: Addresses the problem of *completely* determining a function $f: \{0,1\}^n \rightarrow \{0,1\}$.

W. van Dam, “Quantum oracle interrogation: getting all information for almost half the price”. <http://xxx.lanl.gov/abs/quant-ph/9805006>