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 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

Developments in quantum algorithms for evaluating AND-OR trees: These can be viewed as trees—such as balanced binary trees—whose gates at each level alternate between AND and OR gates, and whose leaves are labelled $x_1, \ldots, x_n$. The goal is to evaluate the root of the tree with as few queries to the input values as possible. Classically, the cost has been long known to be $O(n^{0.753\ldots})$, by an "alpha-beta pruning" technique. It has recently been shown that quantum algorithms can do better than this: $O(n^{0.5})$, for balanced binary trees (and this performance if also known to be optimal). This quantum algorithm has implications for game trees (for example, for more efficient algorithms for Chess and Go).

The development can be traced by the sequence of papers below. The first one is written in a physicist's language, and the subsequent ones are from a more "computer science" perspective. Nevertheless, this may be a challenging topic to digest in the context of a course project—the recommended approach is to focus technically on one aspect of the subject, while giving a non-technical broad overview to put things in context.

E. Farhi, J. Goldstone, S. Gutmann, "A Quantum Algorithm for the Hamiltonian NAND Tree".
http://arxiv.org/abs/quant-ph/0702144

A. Childs, B. Reichardt, R. Spalek, S. Zhang, "Every NAND formula of size N can be evaluated in time N^{1/2+o(1)} on a quantum computer".
http://arxiv.org/abs/quant-ph/0703015

A. Ambainis, “A nearly optimal discrete query quantum algorithm for evaluating NAND formulas”.
http://arxiv.org/abs/0704.3628

B. Reichardt, R. Spalek, “Span-program-based quantum algorithm for evaluating formulas”.
http://arxiv.org/abs/0710.2630

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 Alogrithms 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 Alogrithms 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