Examples of Possible Project Topics

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

Low-depth quantum circuits can provably outperform low-depth classical circuits: This paper shows that constant-depth quantum circuits can perform feats that require logarithmic-depth for classical probabilistic circuits. This is the reference that introduced the concept:

> S. Bravy, D. Gosset, R. König, "Quantum advantage with shallow circuits". https://arxiv.org/abs/1704.00690

Uncloneable encryption: This is a method of encrypting a classical message such that two collaborating but isolated adversaries are prevented from simultaneously recovering the message, even when the encryption key is revealed.

> A. Broadbent and S. Lord, "Uncloneable Quantum Encryption via Oracles". https://arxiv.org/abs/1903.00130

Position-based quantum cryptography: This is an interesting story about a proposal to use the properties of quantum information to enable a party to "prove" that they are at a specific location in space at a particular time.

The original paper that introduced the topic:

> H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, "Position-based quantum cryptography: impossibility and constructions". https://arxiv.org/abs/1101.1065

A simplification of an attack on the proposed protocol:

> S. Beigi and R. Koenig "Simplified instantaneous non-local quantum computation with applications to position-based cryptography". https://arxiv.org/abs/1101.1065

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://arxiv.org/abs/quant-ph/0303081
>
> A. Ambainis, "Quantum walks and their algorithmic applications". http://arxiv.org/abs/quant-ph/0403120

Also, a paper by:

> F. Magniez, A. Nayak, J. Roland, and M. Santha, "Search via Quantum Walk". http://arxiv.org/abs/quant-ph/0608026

Here are a few more papers in this area. Part of the second reference and the third reference concern a *continuous-time* quantum walk.

H. Krovi, F. Magniez, M. Ozols, and J. Roland, "Finding is as easy as detecting for quantum walks". http://arxiv.org/abs/1002.2419

C. Moore and A. Russell, "Quantum Walks on the Hypercube". http://arxiv.org/abs/quant-ph/0104137

A. M. Childs, "Universal computation by quantum walk". http://arxiv.org/abs/0806.1972

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://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://arxiv.org/abs/quant-ph/9906129

J. Preskill, "Fault-tolerant quantum computation".
http://arxiv.org/abs/quant-ph/9712048

E. Knill, R. Laflamme, W. Zurek, "Threshold Accuracy for Quantum Computation". http://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://arxiv.org/abs/cs.CC/0009002

J. Watrous, "PSPACE has 2-round quantum interactive proof systems".
http://arxiv.org/abs/cs.CC/9901015

There are other related topics in various section of the following survey monograph

J. Watrous, T. Vidick, "Quantum proofs".
https://arxiv.org/abs/1610.01664

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://arxiv.org/abs/quant-ph/9612026

C. Mochon, "Hamiltonian Oracles". http://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://arxiv.org/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://arxiv.org /abs/quant-ph/0406196

The hidden subgroup problem, as well as the *hidden shift 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*. See also survey (1) for a broad overview.

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://arxiv.org /abs/quant-ph/0401083

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://arxiv.org/abs/quant-ph/0302112

Other papers related to the hidden subgroup problem:

> O. Regev, "A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space". http://arxiv.org/abs/quant-ph/0406151
>
> G. Ivanyos, L. Sanselme, M. Santha, "An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups". http://arxiv.org/abs/0707.1260
>
> G. Ivanyos, L. Sanselme, M. Santha, "An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups". http://arxiv.org/abs/quant-ph/0701235
>
> Van Dam, S. Hallgren, and L. Ip, "Quantum Algorithms for some Hidden Shift Problems". http://arxiv.org/abs/quant-ph/0211140
>
> A. Childs and W. van Dam, "Quantum algorithm for a generalized hidden shift problem". http://arxiv.org/abs/quant-ph/0507190

Quantum Shannon theory: A generalization of classical Shannon theory, concerned with the capacities of noisy channels (quantum and classical). See also surveys (2) and (3) at the end of this document for a broad overview. The third reference makes an interesting connection with the so-called "black hole information" paradox.

G. Smith, "Quantum Channel Capacities". http://arxiv.org/abs/1007.2855

P. Hayden, M. Horodecki, A. Winter & J. Yard, "A decoupling approach to the quantum capacity," https://arxiv.org/abs/quant-ph/0702005

Ryszard Horodecki, Pawel Horodecki, Michal Horodecki, Karol Horodecki, "Quantum entanglement," (long fantastic review article) https://arxiv.org/abs/quant-ph/0702225

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

C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, A. Winter, "Quantum Reverse Shannon Theorem". http://arxiv.org/abs/0912.5537

T. S. Cubitt, D. Leung, W. Matthews, A. Winter, "Improving zero-error classical communication with entanglement". http://arxiv.org/abs/0911.5300

P. Hayden and J. Preskill "Black holes as mirrors: quantum information in random subsystems". http://arxiv.org/abs/0708.4025

M. Horodecki, J. Oppenheim, A. Winter "Quantum information can be negative". http://arxiv.org/abs/quant-ph/0505062

G. Smith, J. Yard, "Quantum Communication With Zero-Capacity Channels". http://arxiv.org/abs/0807.4935

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://arxiv.org/abs/quant-ph/0508205

C. Durr, M. Heiligman, P. Høyer, M. Mhalla "Quantum query complexity of some graph problems". http://arxiv.org/abs/quant-ph/0401091

B. Furrow, "A panoply of quantum algorithms". http://arxiv.org/abs/quant-ph/0606127

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

> W. van Dam, "Quantum oracle interrogation: getting all information for almost half the price". http://arxiv.org/abs/quant-ph/9805006

Linear optics: Proposes problems that are "hard" in a complexity theoretic sense but nevertheless solvable by easily implementable quantum computers. (Warning: the definitions of the problems and their hardness are somewhat subtle.)

> S. Aaronson, A. Arkhipov, "The Computational Complexity of Linear Optics". http://arxiv.org/abs/1011.3245

Approximating any unitary gate from a simple set of generating operations:

> P. Selinger, "Efficient Clifford+T approximation of single-qubit operators", https://arxiv.org/abs/1212.6253
>
> J. Ross & P. Selinger, "Optimal ancilla-free Clifford+T approximations of z-rotations", https://arxiv.org/abs/1403.2975
>
> Ori Parzanchevski & Peter Sarnak, "Super golden gates for PU(2)", https://arxiv.org/abs/1704.02106

Quantum computation using only measurement gates:

> R. Jozsa, "An introduction to measurement based quantum computation". http://arxiv.org/abs/quant-ph/0508124
>
> R. Raussendorf, D. Browne & H. Briegel, "Measurement-based quantum computation with cluster states", https://arxiv.org/abs/quant-ph/0301052

Using the mathematics of quantum information to prove theorems: There are a few mathematical theorems whose statements seem to have nothing to do with quantum information, but which have been reduced to questions about quantum information and then proved by techniques of quantum information. These are applications of quantum computing that stand whether or not one ever builds a quantum computer! (Note: this is quite different from the topic "Quantum 'proof systems'," which is also interesting but for different reasons.)

A good survey:

A. Drucker, R. de Wolf, "Quantum Proofs for Classical Theorems". http://arxiv.org/abs/0910.3376

A recent breakthrough, where quantum computing ideas were used to resolve a 20-year-old problem, by proving that linear programs (used in a certain way) cannit be used to solve NP-complete problems:

S. Fiorini, S. Massar, S. Pokutta, H. R. Tiwary, R. de Wolf, Linear vs. "Semidefinite Extended Formulations: Exponential Separation and Strong Lower Bounds" http://arxiv.org/abs/1111.0837

A nice quantum proof of a classical result in computational complexity about the hardness of computing the permanent:

S. Aaronson, "A Linear-Optical Proof that the Permanent is #P-Hard" http://arxiv.org/abs/1109.1674

Complexity of finding the minimum eigenvalue of certain Hamiltonians: Related to the "minimum energy levels" of a certain quantum mechanical systems

J. Kempe, A. Kitaev, O. Regev, "The Complexity of the Local Hamiltonian Problem". http://arxiv.org/abs/quant-ph/0406180

Quantum money: The idea is for people to circulate quantum states around that have properties that cash has (or should have): it cannot be counterfeited, it's validity can be checked without having to interact with bank (unlike debit cards), it is anonymous (it cannot be traced back to a spender. With classical information, this is information theoretically impossible, even under cryptographic assumptions about (say) trapdoor or one-way functions. With quantum information and computational assumptions, it is conceivable that this can be done. The following paper is a recent one that is advanced but very well written. A component of this paper could be the basis of a project topic. For example, "mini-schemes".

Scott Aaronson, Paul Christiano, "Quantum Money from Hidden Subspaces" http://arxiv.org/abs/1203.4740

Using "nonlocal" behaviour to accomplish various things securely: What can you do securely even if you are using devices supplied by your adversary? Although this may look like a hopeless situation, one can actually use properties of quantum information (in nonlocal settings) to "guarantee" certain things, such as: bit strings actually being certifiable random, cryptographic keys being secure, and more.

U.V. Vazirani and T. Vidick, "Certifiable Quantum Dice - Or, testable exponential randomness expansion" http://arxiv.org/abs/1111.6054

U.V. Vazirani and T. Vidick, "Fully device independent quantum key distribution" http://arxiv.org/abs/1210.1810

B.W. Reichardt, F. Unger, U. Vazirani, "Classical command of quantum systems via rigidity of CHSH games" http://arxiv.org/abs/1209.0449

Quantum Algorithms for Quantum Field Theories: Using a quantum computer to simulate problems in quantum field theory (where quantum mechanical as well relativistic effects occur). It's probably good to be already familiar with quantum field theory to tackle this one:

S. P. Jordan, K. S. M. Lee, J. Preskill, "Quantum Algorithms for Quantum Field Theories", http://arxiv.org/abs/1111.3633

Blind quantum computing: Suppose that you want to compute something on someone else's quantum computer without revealing any information about what you are computing. This paper addresses this issue:

A. Broadbent, J. Fitzsimons, E. Kashefi, "Universal blind quantum computation" http://arxiv.org/abs/0807.4154

Merkle puzzles: A nice toy problem related to cryptography in a quantum world:

G. Brassard, P. Hoyer, K. Kalach, M. Kaplan, S. Laplante, L. Salvail, "Merkle Puzzles in a Quantum World" http://arxiv.org/abs/1108.2316

Surveys:

These are included for you to peruse for a broad perspective about an "area of research". You might select a topic based on a specific part of one of these surveys (the entire survey would be long). In some cases, this list (above) or the originally posted list already has an item pertaining to a section of the survey.

(1) A. Childs and W. van Dam, "Quantum algorithms for algebraic problems". http://arxiv.org/abs/0812.0380

(2) I. Devetak, A.W. Harrow, and A. Winter, "A resource framework for quantum algorithms".http://arxiv.org/abs/quant-ph/0512015

(3) G. Smith, "Quantum Channel Capacities". http://arxiv.org/abs/1007.2855

(4) J. Watrous, "Quantum Computational Complexity". http://arxiv.org/abs/0804.3401

Boson Sampling is computationally hard for classical computers but accomplished by quantum computers:

S. Aaronson, A. Arkhipov, "The Computational Complexity of Linear Optics" http://arxiv.org/abs/1011.3245

An interesting connection between state transformation problems and the exponent for matrix multiplication:

P. Vrana, M. Christandl, "Asymptotic entanglement transformation between W and GHZ states" http://arxiv.org/abs/1310.3244

Quantum information results pertaining to the issue of information escaping from black holes:

P. Hayden, J. Preskill, "Black holes as mirrors: quantum information in random subsystems" http://arxiv.org/abs/0708.4025

D. Harlow and P. Hayden, "Quantum Computation vs. Firewalls" http://arxiv.org/abs/1301.4504

New developments in query complexity separations:

We have seen the exponential quantum improvement in query-complexity over classical methods for Simon's problem. Note that Simon's problem is based on a function with a promise (that most functions from $\{0,1\}^n$ to $\{0,1\}$ do not satisfy). On the other hand, Grover's algorithm, that will be covered later in class, solves a problem that makes sense for *any* function from $\{0,1\}^n$ to $\{0,1\}$. (And the aforementioned AND-OR tree algorithms also address a problem without a promise.) For problems without a promise, until recently, the best quantum improvement has been quadratic (where the quantum algorithm makes a number of queries that is the square root of the number that the best classical algorithm does), and this had been conjectured to be the best possible. Recently, this square root barrier was broken, and the two relevant papers are:

(1) A. Ambainis, K. Balodis, A. Belovs, T. Lee, M. Santha, J. Smotrovs, "Separations in Query Complexity Based on Pointer Functions" https://arxiv.org/abs/1605.01142

(2) S. Aaronson, S. Ben-David, R. Kothari, "Separations in query complexity using cheat sheets" https://arxiv.org/abs/1511.01937

They are technical (especially the second one), so please look one of the papers over before selecting it.

Quantum machine learning: This is somewhat of a controversial topic. There is extreme interest in using quantum computers for machine learning applications, especially from industry. Very recently, some preprints appeared showing that the performance of some proposed quantum algorithms for machine learning is essentially matched by classical algorithms.

(1) Scott Aaronson, "Read the fine print," https://www.scottaaronson.com/papers/qml.pdf

(2) Harrow, Aram W., Avinatan Hassidim, and Seth Lloyd. "Quantum algorithm for linear systems of equations." https://arxiv.org/abs/0811.3171

(3) Seth Lloyd, Silvano Garnerone, Paolo Zanardi, "Quantum algorithms for topological and geometric analysis of big data", https://arxiv.org/abs/1408.3106

(4) Ewin Tang, "A quantum-inspired classical algorithm for recommendation systems," https://arxiv.org/abs/1807.04271

(5) Ewin Tang, "Quantum-inspired classical algorithms for principal component analysis and supervised clustering" https://arxiv.org/abs/1811.00414

(6) András Gilyén, Seth Lloyd, Ewin Tang, "Quantum-inspired low-rank stochastic regression with logarithmic dependence on the dimension," https://arxiv.org/abs/1811.04909