UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS
Department of Combinatorics and Optimization

C&O Comprehensive Exam Syllabus for Quantum Computation

The comprehensive exam is intended to assess students' understanding of foundational topics in quantum computation. To prepare for the exam we recommend that students focus on developing a mastery of the formalism, a familiarity with the foundational topics listed below, and an ability to apply this knowledge by solving exercises or practice problems. Questions on the exam may test the material directly, or through its application to a specific instance, another problem or in another context. For example, students may be guided through applications of QECC in other areas, such as in quantum cryptography or quantum communication.

We provide standard, primary references at a level suitable for the exam below. *Note that the references given for each topic include overlapping material.* The reference [NC] covers all the topics except the hybrid method for black-box lower bounds (which is covered in [KLM]) and impossibility results in quantum cryptography (which is covered in [LSP]).

Due to the highly interdisciplinary nature of the subject, there are multiple approaches to each topic. Students may find it helpful to consult more than one treatment of a given topic in order to deepen their understanding, or for an exposition more suitable for themselves.

1. **Quantum information toolbox** (KLM 1-5, NC 2, 4.1-4.6, 8, 9.2, Leu)
   - Quantum mechanics and linear algebra basics
   - Quantum states and quantum operations
   - Fidelity and trace distance
   - Quantum circuits, universal sets of quantum gates
   - Basic protocols
2. **Algorithms and complexity** (KLM 6-9, NC 4.7, 5-6)
   - Algorithms based on the Quantum Fourier Transform
   - Grover search; Hamiltonian simulation
   - Black-box model and lower bounds
3. **Quantum error correction and fault tolerance** (KLM 10, NC 10, Got)
   - Theory of quantum error correction
   - CSS codes and Stabilizer codes
   - Fault tolerant quantum computation
4. **Quantum cryptography** (LSP Chapter "Quantum cryptology", NC 12.6)
   - Quantum key distribution
   - Impossibility results: bit commitment, coin tossing, and oblivious transfer

Suggested References:

[NC] Nielsen, Michael A., and Isaac Chuang. Quantum computation and quantum information. Cambridge University Press, 2002.
[KLM] Kaye, Phillip, Raymond Laflamme, and Michele Mosca. An introduction to quantum computing. Oxford University Press, 2007.
[LSP] Lo, Hoi-Kwong, Tim Spiller, and Sandu Popescu. Introduction to quantum computation and information. World Scientific, 1998. Available online through the UW Library.
[Got] Gottesman, Daniel. Stabilizer codes and quantum error correction. Caltech Ph.D thesis. arXiv preprint quant-ph/9705052 (1997).
[Leu] Leung, Debbie W. Choi's proof as a recipe for quantum process tomography. Journal of Mathematical Physics 44.2 (2003): 528-533.

Additional references:

[KSV] Kitaev, Alexei Yu., Alexander H. Shen, and Mikhail N. Vyalyi. Classical and quantum computation. Graduate Studies in Mathematics No. 47. American Mathematical Society, 2002.
[Wat] Watrous, John. The theory of quantum information. Cambridge University Press, 2018.
[Mer] Mermin, N. David. Quantum computer science: an introduction. Cambridge University Press, 2007.
[LB] Lidar, Daniel A., and Todd A. Brun, eds. Quantum error correction. Cambridge University Press, 2013. (Especially Chapter 2 by D. Bacon)

Detailed list of topics

Quantum information toolbox. Vector spaces, norms, bases, linear independence, tensor products, operators, unitarity, hermiticity, commutators, eigenvalue and singular value decompositions.

Pure and mixed states, measurement, reduced density matrix, Schmidt decomposition, purification.

No cloning theorem, superdense coding and teleportation.

Quantum gates, quantum circuits, reversible computation and garbage cleanup, universal gate sets, statement of the Solovay-Kitaev theorem.

Formalisms for quantum operations including the unitary representation (a.k.a. Stinespring dilation or isometric extension), the operator sum representation (a.k.a. Kraus representation), and the axiomatic approach (a.k.a. the Choi-representation), how these formalisms characterize quantum noise processes, how they are related, how quantum operations represent quantum noisy processes, and how they can be treated in quantum error correction.

Definitions of fidelity and trace distance, relations between them; the different ways to approximate quantum operations, and error analysis using these tools.

Algorithms and complexity. Deutsch-Jozsa algorithm, Quantum Fourier Transform, period finding, order finding, discrete log, factoring, hidden subgroup problem, phase estimation, Grover search, Hamiltonian simulation.

Definition and set-up of quantum black-box complexity (a.k.a. query complexity), the polynomial method and the hybrid method for proving lower bounds.

Quantum error correction and fault-tolerance. Basic notions of quantum error correction (QEC), e.g., block length, rate, distance; necessary and sufficient conditions for QEC; discretization of quantum errors; limitations and the tradeoff between rate and distance.

CSS and stabilizer code formalisms and corresponding specialized QEC conditions.

Methods of performing encoded operations that are fault-tolerant, including transversal operations for Clifford gates and gate teleportation to achieve universality.

Quantum cryptography. Standard quantum key distribution (QKD) protocols such as BB84 and E91, physical principles behind security, techniques used in the security proofs.

Impossibility results for ideal bit commitment, coin tossing, and oblivious transfer. Analysis of some given protocol for these or a similar cryptographic task, or for key distribution; in particular, whether the given protocol satisfies some ideal or approximate security conditions.