

CAS705: Computability and Complexity
Fall 2008

- Instructor:** Michael Soltys
Office: ITB-214, Ext: 27769, Email: my last name at mcmaster dot ca
- Lectures:** Tentative Tu & Th 17:30-19:00, in ITB-222
- Web Page:** <http://www.cas.mcmaster.ca/~soltys/cas705-f08>
- Textbook:** “An Introduction to Computational Complexity”, by Michael Soltys
(Coming out next year, so preprints will be given in class.)
- Course Outline:** The relationship between problems, algorithms, and languages.
Computability: finite automata, rewriting systems, Turing machines (linear speedup, robustness, and the Universal Turing machine). Recursive functions and Cobham’s Theorem. Determinism and non-determinism. Recursive and recursively enumerable languages. The Halting problem and the diagonalization technique. Church-Turing thesis, and Rice’s theorem.
Complexity: classes defined in terms of time, space, and circuits. Uniformity. The reachability method (Savitch’s theorem, and the Immerman-Szelepcsenyi theorem). The P versus NP problem (and Cook’s Theorem), reductions and completeness. The Time and Space Hierarchy Theorems. Randomized and parallel computations. NP and co-NP, propositional proof systems, and Horn clauses. Kolmogorov complexity, and the Shannon principle.
Cryptography: RSA, Elliptic-curve based, and lattice-based crypto.
Proof Complexity: Logic and the complexity of formal reasoning.
- Marking Scheme:** There will be a test every-other week, written in class, without aids, and it will take 60 minutes. The tests will be worth 50% of the course grade; a final exam, worth 30%; and 20% for attendance & participation. No aids will be allowed for the tests and the final exam.
- Academic Integrity:** Academic dishonesty consists of misrepresentation by deception or by other fraudulent means and can result in serious consequences, e.g. the grade of zero on an assignment, loss of credit with a notation on the transcript (notation reads: ”Grade of F assigned for academic dishonesty”), and/or suspension or expulsion from the university. It is your responsibility to understand what constitutes academic dishonesty. For information on the various kinds of academic dishonesty please refer to the Academic Integrity Policy, specifically Appendix 3, located at <http://www.mcmaster.ca/senate/academic/ac.integrity.htm>
The following illustrates only three forms of academic dishonesty: 1. Plagiarism, e.g. the submission of work that is not one’s own or for which other credit has been obtained. 2. Improper collaboration in group work. 3. Copying or using unauthorized aids in tests and examinations.