CSC 2429
TOPICS IN THEORY OF COMPUTATION

Time:	Thursday 10-12
Instructor:	Toniann Pitassi
Class location:	SF 3202
Office:	2305A Sandford Fleming Building
Email:	toni@cs.toronto.edu
Office hours:	by appointment

Course Web Site: `http://www.cs.toronto.edu/~toni/Gradcourse/2429.html`
Refer to this site periodically for important announcements and other information.

Course Notes: Posted on course web site.

Course Materials: There is no required text for this course. Background material can be found in the book, "Introduction to the Theory of Computation" by Michael Sipser, PWS Publishing Company. The readings for the course are available on the course website, in postscript format.

Course Description

This is a topics course in the theory of computation, The course will cover two topics that have received considerable attention over the past 10 years, and where exciting progress is being made. The first is derandomization in complexity theory, and the second is the complexity of propositional proofs.

Randomized algorithms are very commonplace, but the meaning and use of randomness is very unclear. In particular, is randomness essential in these algorithms, or is it just an illusion caused by our inability to understand what is going on? We will study various randomized complexity classes, BPP, RP and ZPP. We state known relationships between these classes, and how they fit into other well-studied complexity classes. The focus on this half of the course will be movitated by the open problem of whether or not $P = BPP$. We will study several arguments showing that BPP can be derandomized under believable complexity assumptions assumptions. These arguments introduce and use some beautiful ideas that are connected other areas such as cryptography, coding theory, and boosting.

In the second part of the course we will discuss the complexity of propositional proofs. The big open problem here is to prove that a strong propositional system, such as the Frege proof system, cannot provide polynomial-size proofs of all propositional tautologies. Such a result would have remarkable consequences for complexity theory, ruling out a huge class of candidate algorithms for solving SAT in polynomial-time. We will discuss this open problem and them focus on what is known about lower bounds for the very popular Resolution proof system. A major focus of this half of the course will be to prove that the weak pigeonhole principle does not have polynomial-size Resolution proofs.

Below we give a more detailed list of the topics that will be covered.

(1) **Derandomization, Nonuniform and Uniform Hardness**

(a) The complexity classes P, NP, RP, BPP, $coNP$, E, EXP, P $poly$, and known relationships between these classes. BPP is in P $poly$. BPP in the second level of the polynomial hierarchy. Valentine's Lemma showing that if every function in E has subexponential-size circuits then $P \neq NP$.

(b) Pseudorandomness. Definitions of statistical indistinguishability, computational indistinguishability, pseudorandom number generator. We will demonstrate the robustness of the notion of pseudorandom number generator by stating/proving several theorems showing the equivalence between the existence of a PRNG and the existence of other related combinatorial objects. (For example, equivalent to (i) pseudo-random generator against multiple sampling, (ii) stretching by one bit versus polynomially-many bits, (iii) unpreditability, (iv) pseudo-random function generator, (v) one-way function. We will not prove all of these results.

(c) The seminal hardness versus randomness tradeoff of Nisan and Wigderson, showing that BPP=P under average case hardness assumptions. Time permitting, the basics behind Luca Trevisan's application of their generator to extractors.

(d) Impagliazzo-Wigderson Theorem showing that $BPP = P$ under worst-case hardness assumptions. We will study the original Impagliazzo-Wigderson proof as well as an alternative proof of Sudan,Trevisan,Vadhan.

(e) Andreev-Clementi-Rolins results showing BPP=P assuming the existence of hitting set generators.

(f) (Time-permitting) Partial results on derandomization under uniform hardness assumptions, derandomization of space complexity classes.

(2) **Complexity of Propositional Proofs and Connections to Complexity**

(a) Resolution proofs, and lower bounds on lengths of Resolution proofs. The wide-clause method, and the method of restrictions. Open problems in this area.

(b) The resolution complexity of the WPHP and the connection to the P versus NP question. State-of-the-art upper bounds for the WPHP. Resolution lower bounds for the WPHP.

(c) Frege proofs. Current approaches toward proving lower bounds for Frege proofs, and potential barriers.

Marking Scheme:

Class attendance and participation will be worth 20 percent. There will also be 4 assignments, worth 20 percent each. There will be no exams.