

**CS 2429F – Winter 2014**  
**Approaches to the P versus NP Problem and Related Questions**  
**Location: BA B026**  
**Time: Wed 12-2**

**Instructor: Toniann Pitassi**

Office: 2305A Sandford Fleming Building

email: [toni@cs.toronto.edu](mailto:toni@cs.toronto.edu)

Office hours: by appointment

**Course Web Site:**

<http://www.cs.toronto.edu/toni/Courses/PvsNP/CS2429.html>

Refer to this site periodically for important announcements and other information. All handouts will be available on the site in postscript or pdf form.

**Course Materials:**

Each lecture will have supplemental reading material such as papers or lecture notes, available on the website. A recommended supplementary textbook for this course is *Computational Complexity: A Modern Approach* by Arora and Barak. Another excellent text that covers many of the topics that we will cover in this course is *Boolean Function Complexity: Advances and Frontiers* by Stasys Jukna.

**Course Description**

The P versus NP problem is one of the most famous and most important problems in computer science and mathematics. In this course, we will first discuss the history of this problem, and then spend the bulk of the course on recent approaches to separating P from NP, and other major complexity separations. Topics to be covered include: (i) The P versus NP question and (ii) Separating NP from coNP (iii) Separating P/Poly from NEXP and the (nearly) equivalent problem of proving that  $P=BPP$  (iv) Separating P from any of L, NL, NC. (v) Barriers to resolving these questions

This course will be run as a reading course. I will give some of the lectures, and we will also have some guest lectures. Participants will be asked to present and lead discussion on a paper or a series of papers.

The only prerequisite for this course is the equivalent of CS364 (undergraduate complexity theory). However a graduate course in computational complexity (CS2401) will be very helpful.

### **Grading and Assignments**

Grading will be based on a presentation (50 percent), in class attendance and participation (20 percent) and lecture notes (30 percent). Your presentation will be based on one paper, and you will be given classtime to present the result. You should prepare slides (powerpoint or something similar) to accompany your presentation, and may want to additionally use the board for derivations or proofs. You should also be prepared to lead a general discussion on the approaches and methodologies presented in the paper, and how they might be used to make further progress. You will also be asked to prepare lecture notes for your presentation, and one additional lecture. Class attendance is mandatory and you are encouraged to ask many questions in class. I will present many open problems during the course and hope that some of you will solve some of these problems!

### **Course Outline**

The topics that we will cover in the course will include most of the following although not necessarily in this particular order. methodologies will include: random restrictions, the polynomial method and Fourier analysis, information theory and communication complexity. Some themes are: normal form theorems, the close connection between upper bounds and lower bounds, information bottlenecks, and a blending of techniques (for example, diagonalization together with combinatorial methods).

- (1.) Overview: Best lower bound known for an NP problem is  $4.5n - o(n)$ .  
Overview of circuit classes, and known separations. Overview of proof systems and known separations.
- (2.) Random Restrictions
  - Warmup: Lower bound for Resolution using random restrictions.
  - Hastad's Switching Lemma, and Parity not in  $AC^0$ .
  - Other applications of switching lemma: lower bounds for bounded-depth Frege proofs of PHP, upper bounds for  $AC^0$ -Sat, LMN.

- (3.) More Random Restrictions–Formula size lower bounds.
- (4.) Polynomial method and Parity not in  $AC0[p]$ ,  $p \neq 2$  [Razborov, Smolensky]
- (5.) Clique not in monotone  $P/poly$  [Razborov]
- (6.) On Separating  $P$  from  $NC$  or  $L$ 
  - Circuit Depth Lower Bounds [Karchmer-Wigderson]; Monotone depth lower bounds
  - On proving  $NC1 \neq P$  via direct sum approach.
  - Cook’s approach to separating  $P$  from  $L$ .
- (7.) On proving  $P \neq ACC$  via Yao/Beigel-Tarui and NOF communication complexity.
- (8.) On separating  $NEXP$  from  $P/Poly$  and the nearly equivalent problem of proving  $P = BPP$ .  $NEXP \neq ACC$  [Williams].
- (9.) Time/space tradeoffs: branching program lower bounds (uniform and nonuniform)
- (10.) Algebraic lower bounds
  - Connected components
  - Mulmuley’s lower bound
  - Lower bounds for linear size, log depth circuits [Valiant]
  - Lower bounds for log-depth circuits for matrix multiplication and matrix rigidity;
  - The GCT program for proving proving algebraic  $P \neq NP$ ;
- (11.) Barriers to Proving  $P$  versus  $NP$  and related separations: natural proofs, algebrization.