CS 2429 – Winter 2017
Location: UC 273
Time: 3-5

Instructor: Toniann Pitassi
Office: 2305A Sandford Fleming Building
email: toni@cs.toronto.edu
Office hours: by appointment

Course Web Site: http://www.cs.toronto.edu/ toni/Courses/ProofComp2017/CS2429.html
Refer to this site periodically for important announcements and other information. All handouts will be available on the site in postscript form.

Course Materials: There is no book for this course. Each lecture will have supplemental reading material such as a paper or lecture notes, available on the website.

Course Description

This is a topics course in propositional proof complexity. The only prerequisite for this course is the equivalent of CS364 (undergraduate complexity theory).

Proof complexity, the study of the lengths of proofs in propositional logic, is an area of study that is fundamentally connected both to major open questions of computational complexity theory and to practical properties of automated theorem provers and reasoning systems. In the last decade, there have been a number of significant advances in proof complexity. Moreover, new connections between proof complexity and circuit complexity have been uncovered, and the interplay between these two areas has become quite rich. In addition, concepts and techniques in proof complexity have borrowed from and contributed to several other areas of computer science, including: crytography, automated reasoning and AI, complexity of search classes within NP, the analysis of heuristics and algorithms for NP-hard problems, and bounded arithmetic. In this course, we will cover the fundamentals of propositional proof complexity in the first half of the course.

In the second half we will cover recent connections between proof complexity lower bounds and other areas. Topics here include: connections to SAT solving, extended formulations, and semidefinite hierarchies (SOS).

Here is an outline of topics that I hope to cover in this course. Please let me know if there is a specific topic (listed or otherwise) that you are particularly interested in, as we are likely to not get through all of the material.

(1.) Introduction to proof complexity, propositional proof complexity, basic concepts and definitions, motivation, connections to complexity theory and logic.

(2.) Define standard proof systems: Resolution, Frege systems, bounded-depth Frege systems, Extended Frege, Substitution Frege, Cutting Planes, algebraic proof systems. Complexity measures: size, width, number of lines, tree versus dag form, space measures. Polynomial-simulations and relative complexity of these proof systems. Connection between lower bounds for proof system and lower bounds for SAT. Connection between propositional proof systems and bounded arithmetic.

(3.) Important upper bounds. The pigeonhole principle and the weak pigeonhole principle, matrix identities, graph expansion properties, existence of infinitely many primes.

(4.) Lower Bounds via Width. The pigeonhole principle, Tseitin formula, random formulas. Lower bounds via the width method, and random restrictions.

(5.) Lower Bounds via Interpolation. Craig's interpolation, feasible interpolation, and connection to complexity theory. Prove that Resolution and Cutting Planes have feasible interpolation, and how this implies superpolynomial lower bounds. Limitations of the method–negative results for Frege systems under cryptographic assumptions.

(6.) Proof search and automatizability. NP-hardness of finding optimal sized proofs. Connection between automatizability and feasible interpolation. Nonautomatizability of Resolution and connection to learning. Nonautomatizability of Frege. Canonical disjoint NP pairs.

(7.) Lower Bounds via Communication Complexity. Lower bounds for Cutting Planes, polynomial proof systems, and time-space tradeoffs.

(8.) Lower bounds via Switching Lemmas. Lower bounds for bounded-depth Frege systems.

(9.) Frege systems. The sequent calculus. Equivalence between tree and dag form. Hard examples for Frege including consistency statements, Avigad's formulas, the P versus NP statement, statements from linear algebra. Subsystems of Frege including: bounded arithmetic, LA, LAP. Connections with bounded arithmetic. The best known lower bounds for unrestricted Frege.

(10.) Extended Frege. Equivalence of Extended Frege (EF), substitution Frege, Hajos Calculus. Hard examples. Best known lower bounds. Beyond EF: is there a strongest (super) proof system?

(11.) Algebraic proof systems. Algebraic proofs, nullstellensatz proofs, polynomial calculus. Simulations and connections to standard proof systems. The IPS proof system and connection to the permanent versus determinant question in algebraic complexity. Lower Bounds.

(12.) Proof complexity, Linear Programming and Extended Formulations

(13.) Proof complexity and Semidefinite Hierarchies

(14.) Proof Complexity and SAT Solving.

(15.) Proof Complexity and Total Search Problems (For example, PPA, PPAD, stochastic search problems)

Grading and Assignments

Grading will be based on a couple of assignments which will be handed out during the semester – probably 2. You will have at least one week to turn in each assignment. Extra challenging questions will be marked with a (*). The work you submit must be your own. You may discuss problems with each other; however you should prepare written solutions alone. Class attendence is manditory and you are encouraged to ask many questions in class. I will also ask you to either prepare scribe notes for a lecture, or to read a paper and present it. For the latter, you are welcome to work in pairs.