CS 2429F – Fall 2012
Location: BA 2135
Time: Wed 1-3

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/CommComplexity2/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:

The recommended book for this course is *Communication Complexity* by Kushilevitz and Nisan. Each lecture will additionally have supplemental reading material such as a paper or lecture notes, available on the website.

Course Description

This is a topics course in communication complexity, information complexity and applications. This is a vibrant and currently very active area of complexity theory. The setup consists of two players, Alice and Bob, who hold n-bit strings x and y respectively. The basic question in communication complexity is: how many bits must be communicated in order for them to compute a joint function, $f(x, y)$ of their inputs? The basic and interrelated question in information complexity is: how much information must be revealed (about x to Bob, and about y to Alice, or about x and y to an eavesdropper) in order to compute $f(x, y)$? The basic problem in privacy is to compute f with minimal loss to each individual's privacy. In this course we will study these three concepts and their interrelations. We will see some surprising protocols, and explore techniques for proving inherent limitations with respect to these measures, with the goal of developing a unifying theory of interactive information theory, and its applications. 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.

(1.) Introduction to two-player communication complexity. Basic concepts and definitions, motivation, connections to complexity theory and logic. Definition of NOF communication complexity model.

(2.) Deterministic, randomized, and nondeterministic complexity. Connections between the models.

(3.) Lower bound methods. Fooling sets, rank, discrepancy method, the pattern matrix method and lower bounds via polynomial degree.

(4.) Survey of applications of communication complexity lower bounds: (1) Proof complexity lower bounds via NOF communication complexity, (2) ACC circuit lower bounds via NOF communication complexity, (3) branching program lower bounds, (4) data structure lower bounds, (5) streaming lower bounds.

(5.) Information complexity. Basic definitions. Some background in info theory.

(6.) Sampling methods, and message compression. (Best known results on how to take a low information cost protocol and convert it into a fairly low communication cost protocol.)

(7.) FOCS 2012 paper showing that all standard lower bound methods for 2-party randomized communication complexity already imply lower bounds for information complexity

(8.) Unlimited round tight upper bound for set disjointness. (How a lot of communication really is necessary at least for some choices of parameters.)

(9.) Applications to Privacy I: Approximate privacy.

(10.) Applications to Privacy II: Differential privacy.

(11.) Wrapup and open problems.

Grading and Assignments

Grading will be based on 3 assignments (20 percent each) which will be handed out during the semester, plus presentation of one paper to the

class, by yourself or with a partner (40 percent). You will have at least one week to turn in each assignment. One of the three assignments will be the preparation of class notes. 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 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! It is a great area with lots of connections to other problems, and a wealth of interesting open problems.