CS 286A-2 Mathematical Methods in Theoretical Computer Science **Fall 2008**

Course Summary and Syllabus

Lecturer: Chris Umans *Date: September 30*

Course summary:

We'll study an assortment of recent papers (and a few older ones) that make critical use of mathematical tools, often in clever ways, to achieve striking results. The intent is to highlight mathematical methods that are likely to be more broadly applicable in theoretical computer science, and beyond.

Two themes will be (1) applications of the Discrete Fourier Transform in algorithms and as a proof technique, and (2) the use of finite fields and polynomials in algorithms, and in explicit constructions of error-correcting codes and pseudo-random objects. We will also cover a few miscellaneous "gems" outside of these themes.

Topic selection is flexible based on the interests of the class.

Course Information:

- Instructor: Chris Umans (`umans@cs.caltech.edu`)
- Lectures: Tuesdays and Thursdays 1:00 – 2:25 in Jorgensen 262
- Office hours: TBD
- Text: none. The webpage will be updated regularly with links to relevant papers, and I may also hand out a few packets copied from textbooks.
- Webpage: `http://www.cs.caltech.edu/~umans/cs286a/`

Prerequisite: This is a graduate-level course but it is open to both undergrads and grad students. Prerequisites are mathematical maturity and curiosity. The course is intended to be largely self-contained, but exposure to elementary abstract algebra and material covered in CS21, CS38 and CS151 is helpful.

Course requirements: Read the papers we are studying and attend/participate in lectures. To receive credit for the course, you must present a paper, or produce scribed lecture notes for 1-2 lectures.

(Very) tentative lecture schedule:

Lecture	Date	Topic
1	Sept 30	Introduction and algebra review efficient algorithms for polynomials over finite fields
2	Oct 2	efficient algorithms for polynomials over finite fields (multiplication, division, multipoint evaluation and interpolation, GCD)
3	Oct 7	Integer multiplication via the DFT (Fürer 2007; De/Kurur/Saha/Saptharishi 2008)
4	Oct 9	Matrix multiplication via the DFT (Cohn/Umans 2003; Cohn/Kleinberg/Szegedy/Umans 2005)
5	Oct 14	quantum computation; integer factorization via the DFT
6	Oct 16	quantum computation; integer factorization via the DFT (Shor 1994)
7	Oct 21	Fourier analysis applications (learning AC_0, fooling DNFs, subspace sampling)
8	Oct 23	Fourier analysis applications (learning AC_0, fooling DNFs, subspace sampling) (Linial/Mansour/Nisan 1993; Bazzi 2007 + Razborov 2008; Moshkovitz/Raz 2006)
9	Oct 28	FOCS 2008: Class cancelled?
10	Oct 30	Fourier analysis applications (long code testing and Håstad's PCP verifier) (Håstad 1997)
11	Nov 4	ϵ-biased sample spaces and pseudorandom generators for polynomials (Viola 2008)
12	Nov 6	fast polynomial factorization via fast modular composition (Kaltofen/Shoup 1995, Umans 2007, Kedlaya/Umans 2008)
13	Nov 11	error-corrcting codes: PV codes, GR codes, and list-decoding algorithms for them (Parvaresh/Vardy 2005, Guruswami/Rudra 2006)
14	Nov 13	unbalanced expanders/condensers from codes (Guruswami/Umans/Vadhan 2007)
15	Nov 18	optimal pseudorandom generators from codes (Shaltiel/Umans 2001, Umans 2002)
16	Nov 20	list-decoding lower bound via subspace polynomials (Ben-Sasson/Kopparty/Radhakrishnan 2006)
17	Nov 25	randomness-efficient curve samplers (Ta-Shma/Umans 2006)
18	Nov 27	NO CLASS: THANKSGIVING (Institute Holiday)
19	Dec 2	paper presentations
20	Dec 4	paper presentations

Possible topics/papers for presentation will be listed on the webpage.