Fields and Coding Theory, Math4109A/6011F, Fall 2012

Instructor: Dr. Steven Wang, 4368HP
Tel: (613) 520 2600 (Ext. 2139)
Email: wang@math.carleton.ca
http://www.math.carleton.ca/∼wang

Lectures: Tuesday, Thursday : 11:35 am - 12:55 pm, Canal Building 2400

Office hours: Monday 2:30pm-3:30pm; Thursday 2:00pm-3:00pm.
Other time is available by appointment.

Textbook: "*Lectures on Finite Fields and Galois Rings*",
by Zhe-Xian Wan (World Scientific Publishing Co. Pte. Ltd.).

Other recommended books:(Reserved in library)
"*Introduction to Finite fields and applications*" by Rudolf Lidl and Harald Niederreiter;
"*Coding Theory: A First Course*" by San Ling and Chaoping Xing

Prerequisites: Math2100, or Math3101 or Math 2108 or equivalent; or permission of the School.

Course Objective: The purpose of this course is to introduce students the mathematics of finite fields and applications to coding theory. We will emphasize the structure of finite fields, polynomials over finite fields, and applications to some cyclic codes like BCH codes etc.

Evaluation: assignments 20%; midterm 15%; final exam 50%; project 15%.

Midterm Exam: The midterm exam (Nov. 1) worths 15 marks.

Assignments: Two assignments (10 marks each). Due dates: Oct. 11 and Nov. 15.

Final Examination: This is a three hour closed-book exam scheduled by the University and will take place sometime during the examination period

(Dec. 6- Dec. 19).

Project: The project worth 15%. Due on Dec. 1. More information will be given separately.

Academic Accommodation
You may need special arrangements to meet your academic obligations during the term. For an accommodation request the processes are as follows:
Pregnancy obligation: write to me with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details visit the Equity Services website: http://carleton.ca/equity/accommodation/student_guide.htm
Religious obligation: write to me with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details visit the Equity Services website: http://carleton.ca/equity/accommodation/student_guide.htm
Academic Accommodations for Students with Disabilities: The Paul Menton Centre for Students with Disabilities (PMC) provides services to students with Learning Disabilities (LD), psychiatric/mental health disabilities, Attention Deficit Hyperactivity Disorder (ADHD), Autism Spectrum Disorders (ASD), chronic medical conditions, and impairments in mobility, hearing, and vision. If you have a disability requiring academic accommodations in this course, please contact PMC at 613-520-6608 or pmc@carleton.ca for a formal evaluation. If you are already registered with the PMC, contact your PMC coordinator to send me your Letter of Accommodation at the beginning of the term, and no later than two weeks before the first in-class scheduled test or exam requiring accommodation (if applicable). After requesting accommodation from PMC, meet with me to ensure accommodation arrangements are made. Please consult the PMC website for the deadline to request accommodations for the formally-scheduled exam (if applicable).
Note: There are TA opportunities within the School for future terms. Information on how to apply can be found on our School web page. In hiring undergraduate TAs, the priority shall first be given to students who have passed some of the following Honours courses: MATH 1002, 1102, 2000, 2100, STAT 2655, 2559 with grades A- or better.

Math4109/Math6101
Tentative lecture schedule –subject to change

Week	Dates	Sections	Topics
1	Sep. 6	Chapter 3	Introduction; Fields and Characteristic
2	Sep. 10 - 14	Chapter 3, 4	Binomial Theorem, Prime fields. Polynomial rings, Division algorithm
3	Sep. 17-21	Chapter 5	Euclidean algorithm and unique factorization in $\mathbb{F}[x]$, Residue class rings, Residue class fields, fields extension.
4	Sep. 24 - 28	notes	Linear codes, Syndrome, Coset leaders, Hamming codes
5	Oct. 1 - 5	Chapter 6	Structures of finite fields Primitive elements, sizes of finite fields
6	Oct. 8- 11	Chapter 6	Irreducible polynomials, existence of finite fields; Subfields; **Assign # 1 due (Oct. 11)**
7	Oct. 15-19	Chapter 7	Automorphisms, characteristic polynomials, minimal polynomials, primitive polynomials
8	Oct. 22-26	Chapter 8	Trace and norm; Basis
9	Oct. 29 - Nov. 2	Chapter 9	Factorization of polynomials, Berlekamp's algorithm Midterm (**Nov. 1**);
10	Nov. 5 -9	notes	Factorization of $x^n - 1$; cyclic codes
11	Nov. 12-16	notes	Cyclic codes, double error correcting BCH codes, **Assign # 2 due (Nov. 15)**
12	Nov. 19-23	notes	BCH codes with designed distance; Reed-Solomon codes
13	Nov. 26 - 30		Reed-Solomon codes; Course review.

Information for the course project:

The following is a list of some possible topics for the course project. You can choose topics outside this list; in this case, you must talk with me and we should agree on the project. I strongly suggest you start your search for a topic that fits your interests as soon as possible. The kind of topics in the list are mainly theoretical but you may consider experimentations too. Indeed, a project involving both components (some implementations together with some theoretical explanations) could be very interesting. However, if a topic is essentially an implementation of some algorithm, then it must include a report explaining how and why the program works, and must contain well-justified data testing. A portion of the marks go to how your project is written and organized. I suggest you consider the following scheme: include a title with an abstract. In a first section, explain the problem you are addressing, the background (if needed), and clearly state your results and conclusions. No proof of theorems or programming code must appear in the first section. Then, describe the problem, the method you used (if applicable), how and why it works, and tables summarizing your experiments (if applicable) with clear explanations of the results. Finally, a list of references should appear. Programs (if applicable) should appear in an appendix. Of course, there is no need of new results, but if you do have something that is new explicitly point this out. We include a list of possible references for most of the topics. In general, this is intended as a starting point for the search but in some cases is self-contained. When a reference contains only a section or a chapter, the relevant information is in that book. In case there is no reference included you must consult me. In any case, you should consult the instructor to clear out doubts, suggest lines of action, help you on decisions about the topic, etc. Just come to office hours, or send me mail, or drop by my office and we talk. The project must be your own work. In particular, you must cite everything you are taking from the literature. You can take proofs, explanations, etc, from papers and books but the final writing must be only yours. One possible way to enhance (and show) your understanding of some work is giving new proofs of results, filling some missing steps in theorems, adding examples, and so on. The due date is **December 1, 2012**. You must have a meeting with the instructor to discuss your project before **Oct 25, 2012**. That will ensure that everything is in order with your project. Each graduate student will give a 20-minute presentation.

Structures of finite fields:

- Normal bases (Wan 8 & papers)
- Quadratic forms over finite fields (Wan 11)
- Primitive elements and Costas arrays (papers)
- Generating Costas arrays by using C++ and NTL library.
- Galois Rings (Wan 14)
- Algorithms to find elements of high orders (papers)

Polynomials over finite fields:

- Construction of irreducible polynomials(Wan 10.5-10.7, LN 3.3)
- Permutation polynomials (LN 7, papers)
- Permutation binomials (papers)
- Generating permutation polynomials by using C++ and NTL library.
- Generating inverse polynomials by using C++ and NTL library.
- APN functions; Bent functions
- Maximally nonlinear functions
- Generating APN functions by using C++ and NTL library.
- Orthomorphisms
- Factorization of polynomials over finite fields
- Factorization of cyclotomic polynomials
- Permutation polynomials EA-equivalent to the inverse function over $GF(2^n)$.
- etc

Coding theory:

- Reed Muller codes,
- Linear codes and orthogonal arrays,
- Permutation codes (see me for papers of Chu, Colbourn, Dukes), implementation,
- Turbo codes and Permutation polynomial based interleavers (Sun and Takeshita),
- LDPC codes,
- Reed-Solomon codes and Sudan'a algorithm.
- Array Codes for Multiple Phased Burst Correction
- Additive quantum codes.

- etc

Other applications:

- Linear Recurring sequences (LN 8),
- XTR cryptosystem,
- GH cryptosystem,
- etc

and many more....