Fields and Coding Theory, Math4109A/6101F, Fall 2021

Instructor: Dr. Steven Wang, 4368HP
Email: wang@math.carleton.ca
http://www.math.carleton.ca/∼wang

Lectures: Tuesday, Thursday : 2:35 pm - 3:55 pm

Office hours: Thursday 1:30pm-2:30pm.

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

Other recommended books:
"*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 40%; midterm 20%; project 40%.

Midterm Exam: The midterm exam (Nov. 4) worths 20 marks.

Assignments: Two assignments (20 marks each). Due dates: Oct. 14 and Nov. 18.

Project: The project worth 40%. A final report is due on Dec. 9. Each student will give a 20-minute presentation. More information will be given separately.

Plagiarism

The following important information concerning plagiarism has been copied from `https://carleton.ca/teaching-regulations/appendices/`.

The University Academic Integrity Policy defines plagiarism as "presenting, whether intentionally or not, the ideas, expression of ideas or work of others as one's own." This includes reproducing or paraphrasing portions of someone else's published or unpublished material, regardless of the source, and presenting these as one's own without proper citation or reference to the original source. Examples of sources from which the ideas, expressions of ideas or works of others may be drawn from include but are not limited to: books, articles, papers, literary compositions and phrases, performance compositions, chemical compounds, art works, laboratory reports, research results, calculations and the results of calculations, diagrams, constructions, computer reports, computer code/software, material on the internet and/or conversations.

Examples of plagiarism include, but are not limited to:

- any submission prepared in whole or in part, by someone else;
- using ideas or direct, verbatim quotations, paraphrased material, algorithms, formulae, scientific or mathematical concepts, or ideas without appropriate acknowledgment in any academic assignment;
- using another's data or research findings without appropriate acknowledgement;
- submitting a computer program developed in whole or in part by someone else, with or without modifications, as one's own; and
- failing to acknowledge sources through the use of proper citations when using another's work and/or failing to use quotations marks.

Plagiarism is a serious offence that cannot be resolved directly by the course's instructor. The Associate Dean of the Faculty conducts a rigorous investigation, including an interview with the student, when an instructor suspects a piece of work has been plagiarized. Penalties are not trivial. They can include a final grade of "F" for the course or even suspension or expulsion from the University.

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 accommodation regarding a formally-scheduled final exam, you must complete the Pregnancy Accommodation Form, found under `https://carleton.ca/equity/contact/form-pregnancy-accommodation/`.

- **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, see here: `https://carleton.ca/equity/focus/discrimination-harassment/religious-spiritual-observances/`.

- **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 `mailto: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).

- **Survivors of Sexual Violence:** As a community, Carleton University is committed to maintaining a positive learning, working and living environment where sexual violence will not be tolerated, and where survivors are supported through academic accommodations as per Carleton Sexual Violence Policy. For more information about the

services available at the university and to obtain information about sexual violence and/or support, visit https://carleton.ca/equity/focus/sexual-violence-prevention-survivor-support/.

- **Accommodation for Student Activities:** Carleton University recognizes the substantial benefits, both to the individual student and for the university, that result from a student participating in activities beyond the classroom experience. Reasonable accommodation will be provided to students who compete or perform at the national or international level. 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. See also https://carleton.ca/senate/wp-content/uploads/Accommodation-for-Student-Activities-1.pdf.

Special Information Regarding Fall 2021 Pandemic Measures

While this course will be fully online, instructors are still supposed to include the following general information in each course outline.

All members of the Carleton community are required to follow COVID-19 prevention measures and all mandatory public health requirements (e.g. wearing a mask, physical distancing, hand hygiene, respiratory and cough etiquette) and mandatory self-screening (see https://carleton.ca/covid19/cuscreen/) prior to coming to campus daily.

If you feel ill or exhibit COVID-19 symptoms while on campus or in class, please leave campus immediately, self-isolate, and complete the mandatory symptom reporting tool (see https://carleton.ca/covid19/cuscreen/symptom-reporting/). For purposes of contact tracing, attendance will be recorded in all classes and labs. Participants can check in using posted QR codes through the cuScreen platform where provided. Students who do not have a smartphone will be required to complete a paper process as indicated on the COVID-19 website (see https://carleton.ca/covid19/).

All members of the Carleton community are required to follow guidelines regarding safe movement and seating on campus (e.g. directional arrows, designated entrances and exits, designated seats that maintain physical distancing). In order to avoid congestion, allow all previous occupants to fully vacate a classroom before entering. No food or drinks are permitted in any classrooms or labs.

For the most recent information about Carleton's COVID-19 response and required measures, please see the University COVID-19 webpage, https://

carleton.ca/covid19/, and review the Frequently Asked Questions (FAQs), https://carleton.ca/covid19/faq/. Should you have additional questions after reviewing, please contact mailto:covidinfo@carleton.ca.

Please note that failure to comply with University policies and mandatory public health requirements, and endangering the safety of others are considered misconduct under the Student Rights and Responsibilities Policy, https://carleton.ca/studentaffairs/student-rights-and-responsibilities/. Failure to comply with Carleton's COVID-19 procedures may lead to supplementary action involving Campus Safety and/or Student Affairs.

Math4109A/Math6101F
Tentative lecture schedule –subject to change

Week	Dates	Sections	Topics
1	Sep. 9	Chapter 3	Introduction; Fields and Characteristic
2	Sep. 13 - 17	Chapter 3, 4	Binomial Theorem, Prime fields. Polynomial rings, Division algorithm
3	Sep. 20- 24	Chapter 5	Euclidean algorithm and unique factorization in $\mathbb{F}[x]$, Residue class rings, Residue class fields, fields extension.
4	Sep. 27 - Oct. 1	notes	Linear codes, Syndrome, Coset leaders, Hamming codes
5	Oct. 4 - 8	Chapter 6	Structures of finite fields Primitive elements, sizes of finite fields
6	Oct. 11- 15	Chapter 6	Irreducible polynomials, existence of finite fields; Subfields; **Assign # 1 due (Oct. 14)**
7	Oct. 18-22	Chapter 7	Automorphisms, characteristic polynomials, minimal polynomials, primitive polynomials
8	Oct. 25-29		Reading break
9	Nov. 1-5	Chapter 8	Trace and norm; Basis Midterm (**Nov. 4**);
10	Nov. 8-12	Chapter 9	Factorization of polynomials, Berlekamp's algorithm
11	Nov. 15-19	Chapter 9	Factorization of $x^n - 1$; cyclic codes **Assign # 2 due (Nov. 18)**
12	Nov. 22-26	notes	Cyclic codes, double error correcting BCH codes,
13	Nov. 29 - Dec. 3	notes	BCH codes with designed distance; Reed-Solomon codes
14	Dec. 6- 10	notes	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 10, 2021**. You must have a meeting with the instructor to discuss your project before **Oct. 1, 2021**. That will ensure that everything is in order with your project. Each student will give a 20-minute presentation.

Structures of finite fields:

- Normal bases, normal elements and generalization.
- Algorithms to find elements of high orders (papers)

Polynomials over finite fields:

- Dickson polynomials
- Construction of irreducible polynomials (Wan 10.5-10.7, LN 3.3, papers)
- Linearized polynomials (papers)
- Permutation polynomials (LN 7, papers)
- Permutation binomials (papers)
- APN functions; Bent functions
- Maximally nonlinear functions
- Factorization of polynomials over finite fields
- Factorization of cyclotomic polynomials
- Explicit factorization of $x^n - 1$.
- Explicit factorization of Dickson polynomials
- Permutation polynomials EA-equivalent to the inverse function over $\mathbb{F}_{2^n}$.
- etc

Coding theory:

- Rank metric codes
- Linear codes and orthogonal arrays,
- Optimal cyclic codes from polynomials.
- Weight enumeration and Gauss sums
- Turbo codes and Permutation polynomial based interleavers (Sun and Takeshita),
- LDPC codes,
- Reed-Solomon codes and Sudan's algorithm.
- Additive quantum codes.