School of Mathematics and Statistics - Carleton University
Finite Fields and Coding Theory, MATH 4109/6101, Fall 2024

Instructor: Daniel Panario
Tel: (613) 520 2600 (Ext. 2159)
Email: daniel@math.carleton.ca
http://www.math.carleton.ca/∼daniel

Day and time of course: Tue and Thu 11:35 - 12:55, HP 4369.

Office hours and location: Tuesdays 13:35 - 14:25 in HP 4372, or at a time arranged with the professor.

Textbook: There is no official textbook for this course. However, for most of the lectures, we will have notes available. They were prepared by students of a previous version of the course and checked by the professor. We will use material from the following books:

1. *Introduction to Finite Fields and Their Applications* by R. Lidl and H. Niederreiter, 1994;
2. *Lectures on Finite Fields and Galois Rings* by Zhe-Xian Wan, 2003;
3. *Algebraic Coding Theory* by E. Berlekamp, 1984;
4. *Modern Computer Algebra* by J. von zur Gathen and J. Gerhard, 3rd edition, 2013;
5. *Coding Theory and Cryptography: the Essentials* by D.R. Hankerson, D.G Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger and J.R. Wall, 2000;
6. *Finite Fields* by R. Lidl and H. Niederreiter, 1997;
7. *Handbook of Finite Fields* by G. Mullen and D. Panario, 2013;
8. *The Theory of Error-Correcting Codes* by F.J. MacWilliams and N.J.A. Sloane, 1977;
9. *Finite Fields for Computer Scientists and Engineers* by R. McEliece, 1987.

Course Objective: This course is an introduction to finite fields, emphasizing their structure and applications to coding theory. The influence of computational problems will be considered. Therefore, this course centers around three main issues: the mathematics of finite fields, the applications to coding theory, and the associated computational problems.

Prerequisites: MATH 2108 or MATH 3101 or MATH 2100; knowledge of a computer language.

Evaluation: Midterm tests (30%), Assignments (30%), and a written project and oral presentation (40%).

Midterm Exams: There will be two midterm exams in class for 15% of the final mark each on Tuesdays October 8 and November 19.

Assignments: There will be two assignments for 15% of the final mark each. The assignments will be given in class. Deadlines: Assignment 1 out on September 19, and in on October 17; Assignment 2 out on October 31, and in on November 28.

Final project: The project is worth 40%. This involves writing a report (12-15 pages) plus an oral presentation (25-30 minutes) on a topic related to the material in the course. More information about the project, including list of potential topics and date for the presentations, will be given later.

Chat GPT/Generative AI usage: In no component of this course, the use of Chat GPT or Generative AI is allowed.

Academic Accommodation

Carleton is committed to providing academic accessibility for all individuals. You may need special arrangements to meet your academic obligations during the term. The accommodation request processes, including information about the Academic Consideration Policy for Students in Medical and Other Extenuating Circumstances, are outlined on the Academic Accommodations website: http://students.carleton.ca/course-outline

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.

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.

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).

Tentative lecture schedule

Week	Dates	Topics
1	Sep. 5	Introduction to the course: finite fields and coding theory.
2	Sep. 10-12	Basics of finite fields.
3	Sep. 17-19	Linear codes. Decoding linear codes. Bounds. **Sep. 19: A1 out.**
4	Sep. 24-26	Structure of finite fields. Extension fields. Splitting fields. Subfield criterion.
5	Oct. 1-3	Primitive elements. Gauss algorithm.
6	Oct. 8-10	Irreducible polynomials, number and properties. **Midterm #1 on Tuesday Oct. 8.**
7	Oct. 15-17	Normal bases. Traces. **Oct. 17: A1 in.**
8	Oct. 21-25	**Fall break, no classes.**
9	Oct. 29-31	Finding irreducible polynomials. Factoring polynomials. **Oct. 31: A2 out.**
10	Nov. 5-7	Squarefree, distinct-degree and equal-degree factorization. Permutation polynomials.
11	Nov. 12-14	Cyclic codes. Minimal polynomials.
12	Nov. 19-21	Computing minimal polynomials. BCH codes revisited; t-error correcting BCH codes. **Midterm #2 on Tuesday Nov. 19.**
13	Nov. 26-28	Reed-Solomon, Reed-Muller and MDS codes. LDPC codes. **Nov. 28: A2 in.**
14	Dec. 3-5	Course review. Project presentations.