Sequences in Finite Fields

Winter 2021, MATH 5900
School of Mathematics and Statistics, Carleton University

Instructor: Daniel Panario
Office: #4372 HP, **Tel:** (613) 520 2600 (Ext. 2159)
Email: daniel@math.carleton.ca
Lectures: Thursdays 13:35-16:25. **Room:** online, synchronous, in Zoom.
Office hours: Tuesdays 11:35-12:25, or by appointment (send me mail or talk with me).

General Information

- **Course objectives:** to study sequences and feedback shift registers over finite fields, as well as, their properties and applications in cryptography and communications.
- **Textbook:**
  - Signal Design for Good Correlation, Solomon W. Golomb and Guang Gong, Cambridge University Press, 2005.

  Other textbooks that will be used:
  - Algebraic Shift Register Sequences, Mark Goresky and Andrew Klapper, Cambridge University Press, 2012.
  - Shift Register Sequences, Solomon Golomb, Aegean Park Press, 1982.
  - Finite Fields, Rudi Lidl and Harald Niederreiter, Cambridge University Press, 1997.
  - Introduction to Finite Fields and their Applications, Rudi Lidl and Harald Niederreiter, Cambridge University Press, 1994.
  - Handbook of Finite Fields. Gary Mullen and Daniel Panario, Chapman Hall/CRC, 2013.

  All the above books are available at Carleton's library.
- **Prerequisites:** a course in finite fields like MATH 4109 or equivalent; or permission of the School.
- **Classes begin:** Tuesday January 12, 2021.
  Classes end: Tuesday April 13, 2021.
- **Evaluation:** There will be two sequences assignments (worth 20% each):

Assignment	Hand-out Date	Due Date	Worth
1	Jan. 28	Feb. 25	20%
2	Mar. 4	Apr. 1	20%

Moreover, there will be a project (60%) formed by three oral presentations (5%, 10% and 15%, respectively) and a written project (30%). The list of possible topics for the project will be distributed in late January. Students must pick a topic by Thursday February 4. The project marks are formed by: (1) a 10-15 minutes introductory to the project talk on Thursday March 11; (2) a 15-20 minutes middle advances on the project second talk on Thursday March 25; (3) a third final 25-30 minutes presentation on the project on Thursday April 8; and (4) a written 15-20 pages project due on **Tuesday April 13**.

- **Withdrawal:** The last day for withdrawal from the course without academic penalties is the last day of classes.

- **Tentative lecture schedule** as of December 2020 (before classes start and subject to change):

WEEK	DATES	LECTURES	REMARKS
1	Jan. 12-14	Introduction to the course. Sequences over finite fields and applications. Feedback shift registers and linear feedback shift registers. Examples.	Finite fields material distributed.
2	Jan. 19-21	LFSR: periodic properties; polynomial view; minimal polynomials and periods.	List of projects distributed.
3	Jan. 26-28	LFSR: irreducible and reducible decomposition; matrix representation.	Assignment 1 handed out.
4	Feb. 2-4	LFSR: traces representation; decimation; generating function. Revision of LFSR theory.	Projects decided this week.
5	Feb. 9-11	Randomness criteria. Golomb's postulates for binary and q-ary sequences. Short introduction to characters.	
-	Feb. 16-18	Reading week	
6	Feb. 23-25	Randomness of m-sequences. Applications to random generators and stream ciphers.	Assignment 1 due.
7	Mar. 2-4	Discrete Fourier transform of periodic sequences. Trace representation.	Assignment 2 handed out.
8	Mar. 9-11	Student presentations #1.	
9	Mar. 16-18	Trace representation (cont). DFT and linear span of a sequence.	
10	Mar. 23-25	Student presentations #2.	
11	Mar. 30 - Apr. 1	Berlekamp-Massey algorithm.	Assignment 2 due.
12	Apr. 6-8	Final project presentations #3.	Final project due Tuesday April 13.

- **Academic Integrity:**
  The University states unequivocally that it demands academic integrity from all its members. Academic dishonesty, in whatever form is ultimately destructive to the values of the University. Students who violate the principles of academic integrity through dishonest practices undermine the value of the Carleton degree. Dishonesty in scholarly activity cannot be tolerated. Any student who violates the standards of academic integrity will be subject to appropriate sanctions. If you are unsure whether something you are doing is actually cheating just ask the instructor.

- **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 and Student Parental Leave:** 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 the Parental Leave Guide.
  - **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).
  - **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 the Religious Observation Guide.

Contact Information:

Office Hours are Tuesdays 11:35-12:25.
e-mail: daniel@math.carleton.ca