Introduction to Algebraic Information Theory for Quantitative Finance
Homework 6

August 30, 2025

Timothy Tarter
James Madison University
Department of Mathematics

1. Using $\mathbb{Z}_2[x]/\langle x^8 + x^4 + x^3 + x + 1\rangle$, convert the polynomial the following polynomials to binary, then multiply them by x.
   - $x^7 + x^3 - x$
   - $x^7 + x^6 + x + 1$
   - $x^4 + x + 1$
   - $x^8 + x^7 + x$
2. Backsolve the following binary sequences using the first 11 digits (from the right), but start with $x_{n+2} = c_0 x_n + c_1 x_n + 1$ and go until the determinant is non-zero with at least 3 zeroes following it.
   - 10010101100101011001010110010101100101
   - 11011101110111011101110111011101110111011101
   - 10101110101110101110101110101110101110111010111
3. Now that you know the order of the keys for each of the previous 3 sequences, take a key of starting length 3, and use $Gal(GF(2^{o(key)}) : GF(2^3))$ to find the possible polynomials that you could try for recursion. Show that your previous answer is in that Galois group.
4. Find the points of the following groups of rational points on elliptic curves. What $\mathbb{Z}_p$ groups are these groups isomorphic to? What are the orders of the elements?
   - $E : y^2 \equiv x^3 + 4x + 4 \bmod 5$ (rework this, even though we did it in class - trust me, it helps to have a reference initially).
   - $E : y^2 \equiv x^3 + 2x + 3 \bmod 7$
   - $E : y^2 \equiv x^3 - 6x \bmod 5$
5. Using $E : y^2 \equiv x^3 + 2x + 7 \bmod 179$, encode the word "galois" as $7, 1, 12, 15, 9, 19$, with K=9. Decode it with $m = \lfloor \frac{x}{K} \rfloor$ to check your work.