Exercise sheet 2, 21 November 2019

Some convenient computer algebra systems are sage `http://sagemath.org/`and for small computations Pari-GP `http://pari.math.u-bordeaux.fr/`. I made a sage "cheat sheet" `http://hyperelliptic.org/tanja/teaching/alg14/sage-ref.pdf` for the algebra class.
If you know how to use Mathematica chances are that there are also some functions provided.
To settle notation:
We study *order-k* LFSRs, that means that the state has k entries. The matrix C defined in class is called the *state matrix*. The characteristic polynomial $P(x)$ of a matrix C is defined as $P(x) = \det(xI - C)$. Over $\mathbb{F}_2$ we have $P(x) = x^k + \sum_{i=0}^{k-1} c_i x^i$.
Over arbitrary fields we need to pay attention to signs and have that $P(x) = x^k - \sum_{i=0}^{k-1} c_i x^i$.

1. For the following LFSR descriptions find the characteristic polynomial, the order of the associated matrix and for all starting vectors the period length (only need this for one representative for each sequence); one sequence should be started at $S_0 = (s_0, s_1, s_2, \ldots, s_{k-1}) = (0, 0, \ldots, 0, 1)$.

   For each of the LFSRs try to factor the characteristic polynomial over $\mathbb{F}_2$. Can you find any relation between the degrees of the factors and the largest of the periods? Compute the *order* of each factor. The order of a polynomial $f(x) \in \mathbb{F}_2[x]$ is the smallest $\ell \in \mathbb{Z}_{>0}$ with $x^\ell \equiv 1 \bmod f(x)$.

   (a) $s_{n+2} = s_n + s_{n+1}$;
   (b) $s_{n+3} = s_n + s_{n+2}$;
   (c) $s_{n+3} = s_n + s_{n+1} + s_{n+2}$;
   (d) $s_{n+7} = s_{n+6} + s_{n+5} + s_{n+1} + s_n$;
   (e) $s_{n+10} = s_{n+7} + s_{n+2} + s_{n+1} + s_n$.

2. The sequence $s_{n+2} = s_n + s_{n+1}$ over the integers with starting values $s_0 = 0, s_1 = 1$ is called the Fibonacci sequence. Compute the first 10 elements. Factor the characteristic polynomial of this sequence and call the roots α and $\bar{\alpha}$. Compute $(\alpha^j - \bar{\alpha}^j)/\sqrt{5}$ for $1 \leq j \leq 10$. What do you notice?

3. Can you find a similar result for the sequences over $\mathbb{F}_2$?

4. Prove that the characteristic polynomial of the LFSR $s_{n+k} = \sum_{i=0}^{k-1} c_i s_{n+i}$ is $P(x) = x^k + \sum_{i=0}^{k-1} c_i x^i$ over $\mathbb{F}_2$.

5. Show that $P(x) = x^k - \sum_{i=0}^{k-1} c_i x^i$ over arbitrary fields.
   Hint: remember the checkerboard rule for determinants.