T-79.5501 Cryptology
Homework 4
February 13, 2007

1. Consider the LFSRs with polynomials $f(x) = x^3 + x^2 + 1$ and $g(x) = x^4 + x^2 + 1$. Initialize the first LFSR with 100, and the second one with 1011 (the LFSRs are shifted from right to left). Generate the two output sequences and take their xor-sum. The task is to determine the shortest LFSR which generates the sum-sequence.

2. Show that the exponent of the polynomial $f(x) = x^n + x^{n-1} + ... + x^2 + x + 1 = \sum_{i=0}^{n} x^i$ is equal to $n + 1$ for all integers n, $n > 1$.

3. Prove Corollary 2. Prove also that the converse of Corollary 2 holds: If $\Omega(f) \subset \Omega(h)$, then $f(x)$ divides $h(x)$.

4. Let e be the exponent of $f(x)$. Show that then there is a sequence $S \in \Omega(f)$ such that the period of S is equal to e.

5. Linear recurrence sequences can be considered also over other rings than just $\mathbb{Z}_2$. Consider $\mathbb{Z}_3 = \{0, 1, 2\}$ and a sequence $z_0, z_1, z_2, ...$ generated recursively using the equation $z_{k+3} = 2z_{k+2} + z_{k+1} + z_k$ where all calculations are done mod 3. This corresponds to polynomial equation $x^3 = 2x^2 + x + 1$ what is equivalent to $x^3 + x^2 + 2x + 2 = 0$. The generating polynomial is now $f(x) = x^3 + x^2 + 2x + 2$, where the coefficients are in $\mathbb{Z}_3 = \{0, 1, 2\}$.

   a) $x + 2$ divides $f(x)$. Find the second factor of $f(x)$.

   b) Find the periods of the generated sequences.

6. Let us play with the set of integers $\{0, 1, 2, ..., 9\}$. Given two integers from this set, generate a new number by computing the sum of the two previous numbers. If the sum is a one-digit number then the new term is equal to the sum. If the sum is a two digit number then the new term is equal to the sum of the two digits. For example, if the previous numbers are 2 and 5, then the new number is 7. And if the previous numbers are 7 and 9, the new term is $1 + 6 = 7$. Describe this procedure in terms of a linear recursion over a finite ring. Show that the period of any sequence of integers generated in this manner is a divisor of 24.