T-79.5501 Cryptology Spring 2009

Homework 4

Tutor : Joo Y. Cho
joo.cho@tkk.fi

19th February 2009

Q1. Consider two LFSRs with polynomials $f(x) = x^5 + x^4 + 1$ and $g(x) = x^4 + x^2 + 1$. Find the shortest LFSR which generates all sequences generated by these LFSRs and its connection polynomial $h(x)$. Determine the exponents of $f(x)$, $g(x)$ and $h(x)$. What kind of periods the sequences in $\Omega(h(x))$ may have?

A1-a) The polynomials $f(x)$ and $g(x)$ factor into:

$$f(x) = x^5 + x^4 + 1 = (x^3 + x + 1)(x^2 + x + 1),$$
$$g(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2.$$

By Theorem 2 in the lecture slides, the LFSR with the connection polynomial

$$h(x) = \mathrm{lcm}(f(x), g(x)) = (x^3 + x + 1)(x^2 + x + 1)^2$$

generates all sequences in $\Omega(f(x))$ and $\Omega(g(x))$.

A1-b). The exponents of factors of $f(x)$ and $g(x)$ are

$$
\begin{aligned}
(x^3+x+1) &: e = 7, \\
(x^2+x+1) &: e = 3, \\
(x^2+x+1)^2 &: e = 6
\end{aligned}
$$

Hence $f(x) \mid (x^{21}+1)$ and $g(x) \mid (x^6+1)$ and $\operatorname{lcm}(21,6) = 42 \mid e_h$. The polynomial $x^{42}+1$ has the factorization

$$
\begin{aligned}
x^{42}+1 = (x^{21}+1)^2 &= (x^6+x^5+x^4+x^2+1)^2(x^6+x^4+x^2+x+1)^2 \\
&\times (x^3+x^2+1)^2(x^3+x+1)^2(x^2+x+1)^2(x+1)^2.
\end{aligned}
$$

Hence, $h(x) \mid (x^{42}+1)$ and $e_h = 42$. Since $42 = 2\cdot 3\cdot 7$, the periods of the sequences in $\Omega(h(x))$ are divisible by 2, 3, or 7.

Theorem

Let $g \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_{2^m}$ with $g(0) \neq 0$ and $ord(g) = e$, and let $f = g^b$ with a positive integer b. Let t be the smallest integer with $2^t \geq b$. Then $ord(f) = e \times 2^t$.

For example, let us find the exponent of f such that

$$g = (x^2 + x + 1), \quad f = g^2.$$

Since the exponent of g is 3 and $2^1 \geq 2$, we get $ord(f) = 3 \times 2^1 = 6$.

Q2. 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.

A2-a) Suppose that the sequence $S \in \Omega(f(x))$ has the period of d with generating function

$$S(x) = \frac{1}{f^*(x)}.$$

We claim that $d = e$.
i) By Theorem 3 (Lecture 4) we know that d divides e.
ii) We show that $d \geq e$.
Since S has period d, $S \in \Omega(1 + x^d)$, and hence there is a polynomial of degree less than d such that $G(x) = \frac{P(x)}{1+x^d}$. Hence,

$$\frac{P(x)}{1 + x^d} = \frac{1}{f^*(x)} \Rightarrow P(x)f^*(x) = 1 + x^d \Rightarrow P^*(x)f^{**}(x) = x^d + 1$$

Hence, $f(x) \mid x^d + 1$ and the exponent $e \leq d$.

Q3. 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, $n > 1$.

A3. We have

$$(x+1)f(x) = xf(x) + f(x) = \sum_{i=1}^{n+1} x^i + \sum_{i=0}^{n} x^i = x^{n+1} + 1.$$

Hence, $f(x) \mid (x^{n+1}+1)$ for all $n > 1$, and the exponent of $f(x)$ is $n+1$.

Q4. Recall that an element of a finite field of size q is primitive if it has multiplicative order $q-1$. The following fact holds: An irreducible polynomial is primitive if and only if $x = 00\ldots010$ is a primitive element in the Galois field $GF(2^n) = \mathbf{Z}_2[x]/(f(x))$ with polynomial $f(x)$.
We know that the polynomial $x^4+x^3+x^2+x+1$ is irreducible but not primitive, since its exponent is 5. Hence x is not a primitive element in the field $\mathbf{Z}_2[x]/(x^4+x^3+x^2+x+1)$. Find some primitive element in this field.

A4. The task is to find a primitive element in the field $F_2[x]/(x^4+x^3+x^2+1)$. We can start searching among small polynomials. Since x is no good, let us try x+1 next. Since the order of the field is 15, the possible orders are 3, 5 and 15. (Use $x^5 \equiv 1$.)

$$(x+1)^3 = x^3+x^2+x+1,$$
$$(x+1)^5 = (x+1)(x^4+1) = x^5+x^4+x+1 = x^4+x,$$
$$(x+1)^{15} = ((x+1)^5)^3 = x^3(x^3+1)^3 = x^3(x^9+x^6+x^3+1) = 1$$

We can find more primitive elements in a similar way.

Q5.
For each of the following 5-bit sequences determine its linear complexity and find one of the shortest LFSR that generates the sequence without using the Berlecamp-Massey algorithm.

a) 0 0 1 1 1
b) 0 0 0 1 1
c) 1 1 1 0 0
d) Determine an LFSR that generates all three sequences.

Q5-a) The sequence contains two consecutive 0's. It follows that LC ≥ 3. Let's try to fit a linear recurrence of length 3 to the sequence. Given five terms of the sequence we get the following two equations:

$$\begin{aligned} c_0 \cdot 0 + c_1 \cdot 0 + c_2 \cdot 1 &= 1 \\ c_0 \cdot 0 + c_1 \cdot 1 + c_2 \cdot 1 &= 1 \end{aligned}$$

from where we get $c_2 = 1$ and $c_1 = 0$. We are looking for a full length three LFSR, hence $c_0 = 1$. Since we found a solution LFSR with polynomial $x^3 + x^2 + 1$ it follows that LC = 3.

Q5-b) Similarly as in a) we see immediately that LC ≥ 4. When fitting a linear recurrence of length 4, only one equation is obtained:

$$c_0 \cdot 0 + c_1 \cdot 0 + c_2 \cdot 0 + c_3 \cdot 1 \quad = \quad 1$$

It follows that $c_3 = 1$. Hence, with $c_0 = 1$, we have four solutions. It follows that LC =4, and that any of the four polynomials works:
$x^4 + x^3 + c_2x^2 + c_1x + 1$.

Q5-c) The non-zero sequence contains two consecutive 0's. It follows that LC ≥ 3. Let's try to fit a linear recurrence of length 3 to the sequence. From the five terms of the sequence we get the following two equations:

$$\begin{aligned} c_0 \cdot 1 + c_1 \cdot 1 + c_2 \cdot 1 &= 0 \\ c_0 \cdot 1 + c_1 \cdot 1 + c_2 \cdot 0 &= 0 \end{aligned}$$

from where we get $c_0 = c_1$ and $c_2 = 0$. We are looking for a full length three LFSR, hence $c_0 = 1$. Since we found a solution LFSR with polynomial $x^3 + x + 1$ it follows that LC = 3.

Q5-d)

Let us try if we could find a degree 4 solution by fitting a linear recurrence of length four to the three sequences. We get three equations:

$$\begin{aligned} c_0 \cdot 0 + c_1 \cdot 0 + c_2 \cdot 1 + c_3 \cdot 1 &= 1 \\ c_0 \cdot 0 + c_1 \cdot 0 + c_2 \cdot 0 + c_3 \cdot 1 &= 1 \\ c_0 \cdot 1 + c_1 \cdot 1 + c_2 \cdot 1 + c_3 \cdot 0 &= 0 \end{aligned}$$

We get $c_0 = c_1$, $c_2 = 0$, and $c_3 = 1$ and hence the common polynomial is $x^4 + x^3 + x + 1$.

Q6.

Let S be a sequence of bits with linear complexity L. Its complemented sequence $\bar{S}$ is the sequence obtained from S by complementing its bits, that is, by adding 1 *modulo* 2 to each bit.

a) Show that $LC(\bar{S}) \leq L + 1$.

b) Show that $LC(\bar{S}) = L - 1,$ or $L,$ or $L + 1$.

A6-a. Let I be a sequence 1111...1... (finite or infinite) that is generated using the feedback polynomial $x + 1$. Then, we have $\bar{S} = S \oplus I$. By Theorem 2 in the lecture slides, we know $\bar{S} \in \Omega(h)$ where $h(x) = \mathrm{lcm}(f(x), (x+1))$. If the original sequence is generated using a polynomial $f(x)$ of degree L then the complemented sequence is generated using a feedback polynomial $\mathrm{lcm}(f(x), (x+1))$, which has degree at most $L + 1$. Hence, $LC(\bar{S}) \leq LC(S) + 1$.

A6-b) Applying the result proved in a) for $\bar{S}$ and observing that $\bar{\bar{S}} = S$ we get $LC(\bar{S}) \geq LC(S) - 1$. Hence $LC(\bar{S} \in \{L-1, L, L+1\}$.
All three cases are possible as shown by the sequences:
111111...(complemented sequence has LC = 0),
01010...(complemented sequence has the same LC),
000000....(complemented sequence has LC = 1)