T-79.503 Foundations of Cryptology
Homework 3
October 7, 2004

1. 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 $L + 1$.

2. a) Prove: If $\Omega(f) \subset \Omega(g)$, then $f(x)$ divides $g(x)$. *Hint: Handout 1, Theorem 1*

   b) Prove: For all $S(x) \in \Omega(f)$ also $\bar{S}(x) \in \Omega(f)$, if and only if $x + 1$ divides $f(x)$. (Here $\bar{S}(x)$ denotes the complemented sequence of $S(x)$.)

3. Find the LFSR asked in HW02 Problem 4 using Berlekamp-Massey algorithm.

4. For each of the following 5-bit sequences determine its linear complexity and find one of the shortest LFSR that generates the sequence.

   a) 0 0 1 1 1

   b) 0 0 0 1 1

   c) 1 1 1 0 0

   Find also an LFSR which generates all these sequences.

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. Consider a cryptosystem where $\mathcal{P} = \{A, B\}$ and $\mathcal{C} = \{a, b, c\}$, $\mathcal{K} = \{1, 2, 3, 4\}$, and the encryption mappings e_K are defined as follows:

K	$e_K(A)$	$e_K(B)$
1	a	b
2	b	c
3	b	a
4	c	a

   The keys are chosen with equal probability.

   a) Show that

   $$\mathbf{Pr}[\mathbf{x} = A | \mathbf{y} = b] = \frac{2\mathbf{Pr}[\mathbf{x} = A]}{1 + \mathbf{Pr}[\mathbf{x} = A]}.$$

   b) Does this cryptosystem have perfect secrecy?