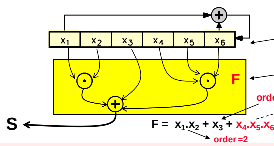
Introduction to Cryptology

Tutorial-06
Secret-Key Ciphers
Stream Ciphers: Design Principles

03.05.2023, v43

A Template for Designing a Running Key Generators
Non-linear Combination of LFSR Sequences



LFSR with primitive connection polynomial Of length L.
PN sequence: period $2^L-1 = 2^6-1=63$

Non-linear function F with non-linear order NLO=m

$F = x_1.x_2 + x_3 + x_4.x_5.x_6$

order =1
order =2
NLO= m= 3=L/2
Largest product of adjacent cells

$\binom{L}{m} = \frac{L!}{m!(L-m)!}$

If C (D) is primitive then the resulting linear complexity is: $L(\underline{S}) \geq \binom{L}{m} - (L-m)$

For m = L/2
Linear Complexity $L(\underline{S}) \approx 2^{L-\log_2 L}$

Design steps:

1. Select a primitive polynomial of degree L
2. Select a function F with a nonlinear order m=L/2
3. Select some low order terms in F (for good 1/0 distribution)
4. Compute effective linear complexity L(S)

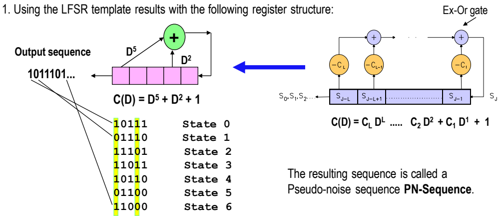
Problem 6-1:

Construct a linear feedback shift register using the connection Polynomial $C(D) = D^5 + D^2 + 1$. The polynomial C(D) is irreducible.

1. Start the constructed register with the initial state 10111 and generate the first 5 bits of its output sequence.
2. Which possible length can the sequence period take?
3. Find the period of the resulting sequence.
4. If C(D) is not known to an external attacker. How many consecutive sequence bits are required to generate the rest of this sequence?
5. How much is the linear complexity of that sequence?

Solution 6-1:

1. Using the LFSR template results with the following register structure:



The resulting sequence is called a Pseudo-noise sequence **PN-Sequence**.

2. C(D) is irreducible with period p, where p should divide $2^5-1 = 31$. The divisors of 31 are 1 or 31. Thus the period can be 1 or 31.
3. As the period is not 1 (see the sequence in 1), it should be 31 => p = 31 q.e.d
4. If we apply Massey-Berlekamp algorithm using only 2L = 10 consecutive bits are required to find C(D).
5. Linear complexity is the length of the shortest linear feedback shift register LFSR which generates the sequence. Thus the linear complexity of our sequence is L = 5.

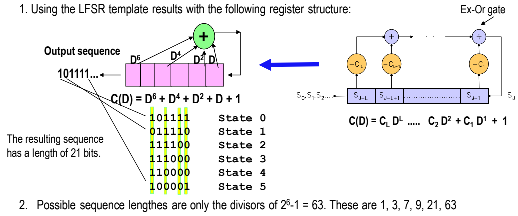
Problem 6-2:

Construct a linear feedback shift register using the connection Polynomial $C(D) = D^6 + D^4 + D^2 + D + 1$. The polynomial C(D) is irreducible.

1. Start the constructed register with the initial state 101111 and generate the first 5 bits of its output sequence.
2. Which possible length can the sequence period take?
3. Find the period of the resulting sequence.
4. If C(D) is not known to an external attacker. How many consecutive sequence bits are required to generate the rest of this sequence?
5. How much is the linear complexity of that sequence?

Solution 6-2:

1. Using the LFSR template results with the following register structure:



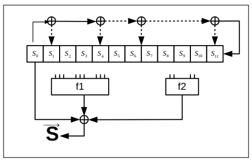
The resulting sequence has a length of 21 bits.

2. Possible sequence lengthes are only the divisors of $2^6-1 = 63$. These are 1, 3, 7, 9, 21, 63
3. Looking in the table of irreducible polynomials, the period of the selected polynomial is e = 21. (can also be found by computing the order of x modulo $C(x) = x^6 + x^4 + x^2 + x + 1$)
4. Applying Massey-Berlekamp algorithm requires only 2L = 12 consecutive bits to find C(D).
5. Linear complexity is the length of the shortest linear feedback shift register LFSR which generates the sequence. Thus the linear complexity of our sequence is L = 6.

Problem 6-3: Stream Cipher Design

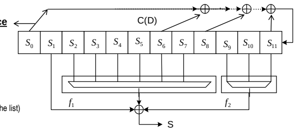
1. Define the connection polynomial for the running key generator shown such that it produces a maximum length output sequence. Compute the length of the output sequence.
2. Compute the number of possible polynomials which can produce such sequences.
3. Define possible functions for f1 and f2 using logical gates such that the output sequence S shows a maximum linear complexity. Write the function of the output sequence in terms of the register states.
4. Compute the linear complexity of the output sequence S.

Use the factorization table below:



$2^3 - 1 = 7$	$2^{19} - 1 = 524287$
$2^4 - 1 = 3 \times 5$	$2^{20} - 1 = 3 \times 5 \times 5 \times 11 \times 31 \times 41$
$2^5 - 1 = 31$	$2^{21} - 1 = 7 \times 7 \times 127 \times 337$
$2^6 - 1 = 3 \times 3 \times 7$	$2^{22} - 1 = 3 \times 23 \times 89 \times 683$
$2^7 - 1 = 127$	$2^{23} - 1 = 47 \times 178481$
$2^8 - 1 = 3 \times 5 \times 17$	$2^{24} - 1 = 3 \times 3 \times 5 \times 7 \times 13 \times 17 \times 241$
$2^9 - 1 = 7 \times 73$	$2^{25} - 1 = 31 \times 601 \times 1801$
$2^{10} - 1 = 3 \times 11 \times 31$	$2^{26} - 1 = 3 \times 2731 \times 8191$
$2^{11} - 1 = 23 \times 89$	$2^{27} - 1 = 7 \times 73 \times 262657$
$2^{12} - 1 = 3 \times 3 \times 5 \times 7 \times 13$	$2^{28} - 1 = 3 \times 5 \times 29 \times 43 \times 113 \times 127$
$2^{13} - 1 = 8191$	$2^{29} - 1 = 233 \times 1103 \times 2089$
$2^{14} - 1 = 3 \times 43 \times 127$	$2^{30} - 1 = 3 \times 3 \times 7 \times 11 \times 31 \times 151 \times 331$
$2^{15} - 1 = 7 \times 31 \times 151$	$2^{31} - 1 = 2147483647$
$2^{16} - 1 = 3 \times 5 \times 17 \times 257$	$2^{32} - 1 = 3 \times 5 \times 17 \times 257 \times 65537$
$2^{17} - 1 = 131071$	$2^{33} - 1 = 7 \times 23 \times 89 \times 599479$
$2^{18} - 1 = 3 \times 3 \times 3 \times 7 \times 19 \times 73$	$2^{34} - 1 = 3 \times 43691 \times 131071$

Solution 6-3:



1. A possible connection polynomial is the following primitive polynomial from the irreducible polynomial table
   C(D) = 1000001010011
   $= D^{12} + D^6 + D^4 + D + 1$ (8th polynomial in the list)
   Periode $2^L - 1 = 2^{12} - 1 = 4095$

2. Number of existing primitive polynomials of degree L is : $\frac{\varphi(2^L - 1)}{L}$

   for L = 12, number of primitive polynomials is:
   $\varphi(2^{12} - 1) / 12 = \varphi(4095) / 12 = \varphi(5 * 3^2 * 7 * 13) / 12$
   $= 4095(1-1/5)(1-1/3)(1-1/7)(1-1/13) / 12$
   = 1728 / 12 = 144 possible polynomials (or possible PN-Sequences)

3. Selecting m = 12/2 for highest linear complexity $\vec{S} = S_9 S_{10} S_{11} + S_7 S_6 S_5 S_4 S_3 S_2 + S_1$

4. The linear complexity is $L(\vec{S}) \geq \binom{12}{6} - (12-6) = \frac{12!}{6! \cdot (12-6)!} - 6 = 924 - 6 = 918$ bits

Annex Irreducilbe polynomials of degree 12:

m=12	e
1000000001001	45
1000000010111	315
1000000100001	819
1000000110011	819
1000000110101	195
1000000111111	1365
1000001001101	819
1000001010011	4095
1000001101001	4095
1000001110111	195
1000001111011	4095
1000001111101	4095
1000010001011	455
1000010011001	4095
1000010100011	819
1000010100101	585
1000011001111	273
1000011010001	4095
1000011101011	4095
1000011101101	1365
1000011111111	117
1000100000111	4095
1000100011111	4095
1000100100011	4095
1000100110001	273
1000100110111	819
1000100111011	4095
1000101001111	4095
1000101010111	4095
1000101101011	4095
1000101101101	105
1000101111001	91
1000110000011	455
1000110000101	4095
1000110101011	819
1000110110011	4095
1000111011001	4095
1000111011111	4095
1000111100011	273
1000111101111	1365
1000111110001	65
1001000001101	4095
1001000010011	455
1001000011001	819
1001000100101	1365
1001000110111	4095
1001000111011	105
1001000111101	4095
1001001001001	315
1001001100111	4095
1001001101101	1365
1001001110011	4095
1001001111111	4095
1001010110101	819
1001010111001	4095
1001011001011	4095
1001100001111	4095
1001100011011	585
1001100011101	4095
1001100110011	819
1001100111001	4095
1001100111111	4095
1001101001101	4095
1001101100101	1365
1001110011111	585
1001110100011	4095
1001110101111	1365
1001110111011	819
1001111000011	455
1001111010111	1365
1001111011101	1365
1001111110011	1365