Lecture Three

Stream Cipher and Shift Register

8. Golomb and Massey Definition for Shift Register

8.1 Golomb Definition

Golomb considered that the shift register is a r arrangement of memory, every memory contains the signal "on" (1) or "off" (0). Every cell shift its contain to the next cell in one time, and when there are no entry signals then the shift register will be "off" after r shifting and to prevent that the shift register must be re-fed in the 1st cell by sum xor some/all the contains of the shift register. The values $a_{-1},a_{-2},\ldots,a_{-r}$ are the initial values of the shift register. The output at time n, n=0,1,2,…, is:

$$a_n = c_1a_{n-1}+c_2a_{n-2}+\ldots+c_ra_{n-r} = \sum_{i=1}^{r} c_i a_{n-i} \qquad \ldots(8.1)$$

this relation called the Linear Recurrence Relation and:

$$c(x) = 1+\sum_{i=1}^{r} c_i x^i$$

called characteristic polynomial of the LFSR.

8.2 Massey Definition

Massey's definition does not different than Golomb's definition, the code <C(D),L> denotes the LFSR with length L and has connection polynomial C(D) s.t.:

$$C(D) = 1+c_1D+\ldots+c_LD^L \qquad \ldots(8.2)$$

Where D is the delay operator, if $c_i=1$ then the cell is take a part in connection function, else it is not. The initial value are $s_0,s_1,\ldots,s_{L-1}$ s.t. then the output (the output sequence) are $s_{L-1},\ldots,s_1,s_0$ when $j<L$ but when $j\geq L$ then the output s_j can be obtained by the following recurrence relation:

$$s_j = \sum_{i=1}^{L} c_i s_{j-i} \text{ , } j\geq L \qquad \ldots(8.3)$$

for the recurrence relation (8.3) there is a Monic polynomial c(X) called characteristic polynomial of the LFSR.

$c(X) = X^L+c_1X^{L-1}+\ldots+c_{L-1}X+c_L\in GF(2)[X]$.

$c_i\in GF(2)$, GF(2)[X] is the ring of the all binary polynomials defined on GF(2).

Note that c(X) and C(D) are the reciprocal polynomial s.t.:

$C(D) = D^Lc(D^{-1})$ or $c(X)=X^LC(X^{-1})$.

Theorem (8.1): $c(x)=\sum_{i=0}^{L} c_i x^i$ is primitive (irreducible) polynomial iff $c'(x)=\sum_{i=0}^{L} c_i x^{L-i}$ is primitive (irreducible) polynomial.

Note that c(x) and c′(x) are reciprocal polynomials.