Lecture Three

Stream Cipher and Shift Register

7. Algebraic Concept of Linear Shift Register

7.1 Linear Shift Register Components

Linear Shift Register (LSR) is Linear Machine (LM) on finite filed F, combined from three kinds of devices:

1. **Adder**: this device has $s \in Z^+$, inputs s.t. $x_1, x_2, \ldots, x_s \in F$, and has one output represent the (+) operation defined of F as in figure (4-a).

2. **Multiplier**: multiply by constant $\alpha \in F$ s.t. has one input $x \in F$ and one output $\alpha x \in F$ as in figure (4-b).

3. **Delay**: this device has memory, the time on it divided into equal and short intervals as in figure (4-c).

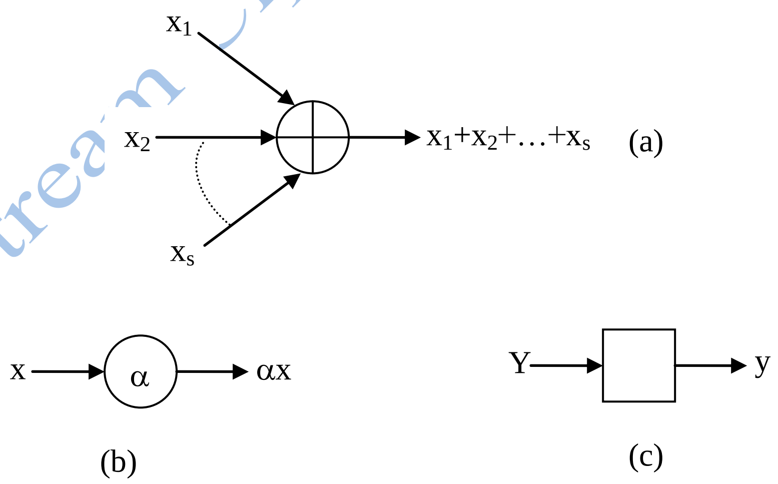


Figure (4) (a). Adder, (b). Multiplier (c). Delay

The response of adder and multiplier are in time.

The output of delay in time t is the input to it in time t-1, if we denote the input in time t by Y(t) and the output by y(t) then:

$$y(t) = Y(t-1) \qquad \ldots(6.1)$$

The LM contains k of delays which can denote the states of the machine in time t by:

$$\begin{bmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_k(t) \end{bmatrix} \in F_k$$

As a special case, the initial state is:

$$\begin{bmatrix} y_1(0) \\ y_2(0) \\ \vdots \\ y_k(0) \end{bmatrix} \in F_k$$

7.2 Linear Feedback SR

The linear feedback SR is the most important of one output terminal LM. Figure (5) shows the diagram of this device.

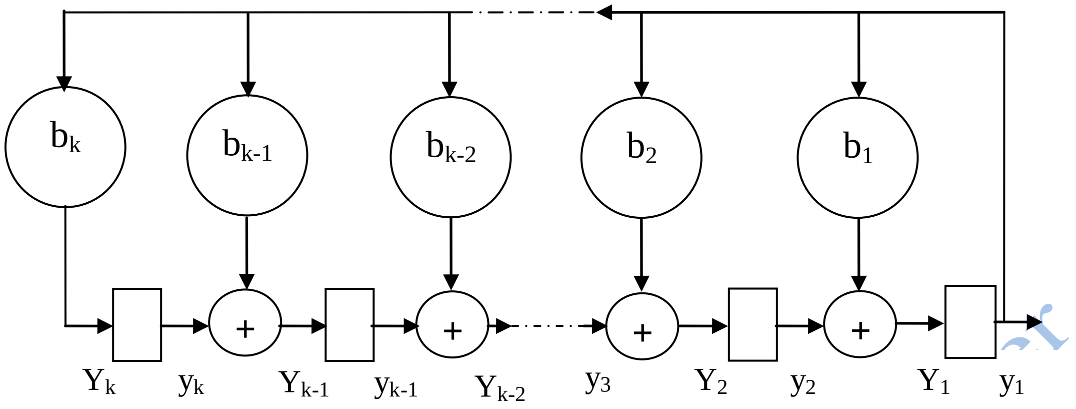


Figure (5) Linear Feedback SR

Notice that the Linear Feedback SR exploits the output as a feed back, therefore, $F_\ell=F_0$.

Then the LM=$[F_k,F_m,\alpha,\beta]$ and α: $F_k \rightarrow F_k$, s.t. $\alpha(x_i)=x_j$, i,j=1,…,k and β: $F_k \rightarrow F_m$ s.t. $\beta(x_i)=z_j$, i=1,…,k and j=1,…,m.

Example (7.1):

Let F=GF(2), k=2, m=1, $F_1=\{0,1\}$, $F_2=\{\sigma_1,\sigma_2,\sigma_3\}$, and let σ_1 represents the initial state s.t.

$\alpha(\sigma_1)=\sigma_2$, $\alpha(\sigma_2)=\sigma_3$, $\alpha(\sigma_3)=\sigma_1$.

$\beta(\sigma_1)=1$, $\beta(\sigma_2)=1$, $\beta(\sigma_3)=0$.

The next state and outputs can be explained in table (1).

table (1) the next state and outputs.

Next state	σ_1	σ_2	σ_3	σ_4

output	-	1	1	0

If we defined the delay operator (D), which is represents the difference in time, depending on equation (7.1) by:

$y_i(t)=DY_i(t)$, for $t\geq 1$ …(7.2)

if the difference is k then the operator will be D^k.

From figure (5) we notice that:

$Y_k=b_kz$, $Y_i=y_{i+1}+b_iz$, $i=1,\ldots,k-1$, $z=y_1$ …(7.3)

by using equation (6.2) in (6.3) we obtain:

$z=(b_1D+b_2D^2+\ldots+b_kD^k)z$ …(7.4)

this equation can be rewritten as follows:

$(1+b_1D+b_2D^2+\ldots+b_kD^k)z = R(D)z = 0$

R(D) is the Recursive polynomial (or Connection polynomial).

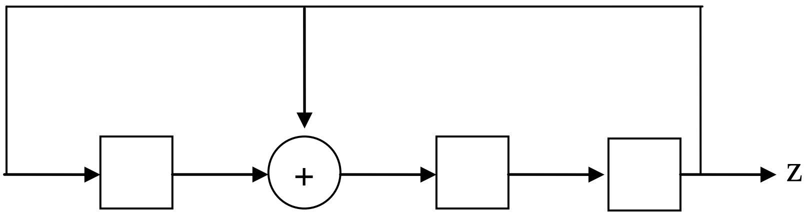
From equation (7.4):

$$\left.\begin{array}{ll} Z(t) = b_1z(t-1)+b_2z(t-2)+\ldots+b_kz(t-k) & \text{(a), when } k<t \\ Z(t) = b_1z(t-1)+b_2z(t-2)+\ldots+b_tz(0)+y_{t+1}(0) & \text{(b), when } k\geq t \end{array}\right\} \ldots(7.5)$$

Form equation (7.5) we can find the current output depending on previous output.

Example (7.2):

In GF(2^3), when F=GF(2) and let $\alpha^3=\alpha+1$, we have linear feedback SR consists from three delays as in figure (6).



t=0	c_0	c_1	c_2
t=1	c_2	$c_0 \oplus c_2$	c_1
t=2	c_1	$c_1 \oplus c_2$	$c_0 \oplus c_2$
.			
.			

Figure (6) Linear Feedback SR with 3 delays.

When t=1 then $\alpha(c_0 \oplus c_1\alpha \oplus c_2\alpha^2)=c_2 \oplus (c_0 \oplus c_2)\alpha \oplus c_1\alpha^2$

And t=2 then $\alpha(c_2 \oplus (c_0 \oplus c_2)\alpha \oplus c_1\alpha^2)=c_1 \oplus (c_1 \oplus c_2)\alpha \oplus (c_0 \oplus c_2)\alpha^2$

By applying relation (7.5-b) to specify the output when t<3:

$z(0)=c_2$, $z(1)=c_1$, $z(2)= c_0 \oplus c_2$

and so on by applying relation (6.5-a) to specify the output when $t \geq 3$:

$z(3)=c_1 \oplus c_2$, $z(4)=c_0 \oplus c_1 \oplus c_2$, …

The binary sequences S =z(0), z(1), z(2),… (or $S=s_0,s_1,s_2,\ldots$, where $s_i=z(i)$, i=0,1,2,…). If the initial state of linear Feedback SR all zero's then $s_i=0$, $\forall i$.