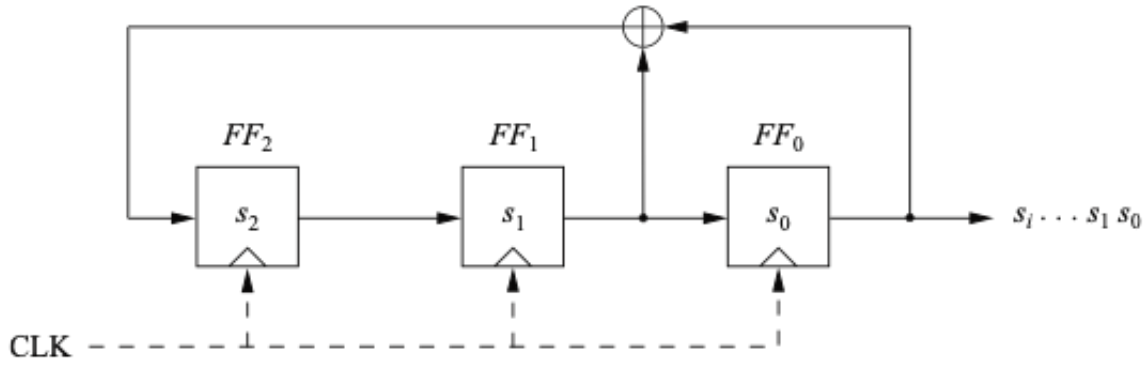
LFSR

LFSR được mô tả như hình sau:



Từ ba giá trị ban đầu s_2, s_1, s_0, các giá trị tiếp theo được tính theo công thức sau:

$$\begin{aligned} s_3 &= s_1 + s_0 \mod 2 \\ s_4 &= s_2 + s_1 \mod 2 \\ s_5 &= s_3 + s_2 \mod 2 \end{aligned}$$

Một cách tổng quát, ta có

$$s_n = s_{n-2} + s_{n-3} \mod 2.$$

Bài 1: Ta sẽ cùng phân tích dãy số giả ngẫu nhiên sinh bởi một LFSR sau.

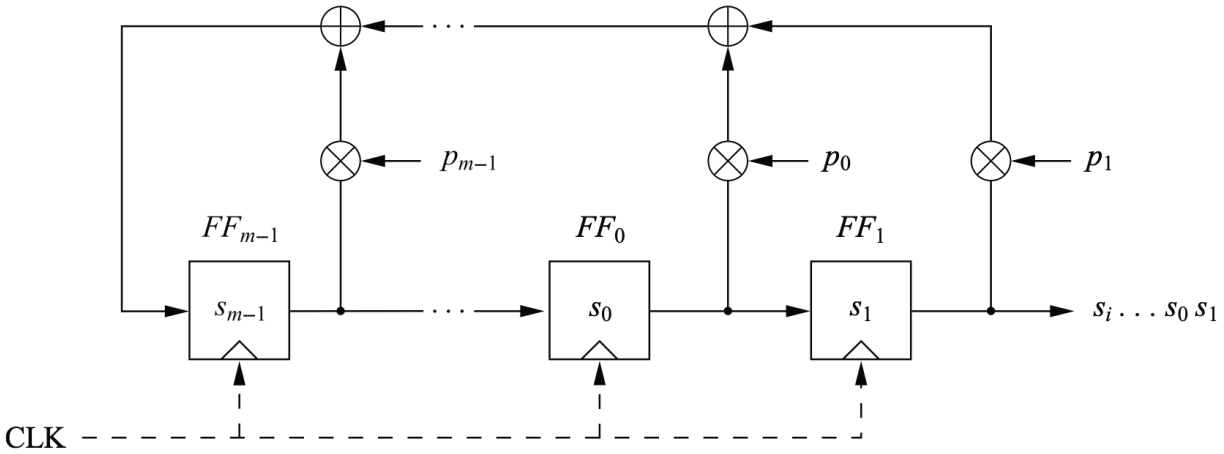
1. Dãy sinh bởi vector khởi tạo $(s_2 = 1,\ s_1 = 0,\ s_0 = 0)$ là gì?
2. Dãy sinh bởi vector khởi tạo $(s_2 = 0,\ s_1 = 1,\ s_0 = 1)$ là gì?
3. Hai dãy này có liên hệ gì với nhau?

Bài 2: Giả sử ta có một hệ mã dòng ở đó chu kỳ khá ngắn. Chuyện gì xảy ra nếu ta biết chu kỳ là $150 - 200$ bit. Ta giả sử ta không biết gì bên trong của hệ mã dòng. Cụ thể, ta không thể giả sử rằng hệ mã dòng là LFSR. Để đơn giản ta giả sử bản rõ là tiếng Anh ở dạng ASCII.

Hãy mô tả cách tấn công hệ mã này.

Dạng tổng quát của LFSR

Dạng tổng quát của LFSR với các hệ số phản hồi p_i và giá trị ban đầu $s_0, s_1, \ldots, s_{m-1}$ được mô tả như hình sau:



Giá trị tiếp theo s_m được tính như sau:

$$s_m = \sum_{j=0}^{m-1} p_j \cdot s_j \mod 2$$

Bài tập: Hãy kiểm tra lại các khẳng định sau bằng tính toán cụ thể:

- Dãy LFSR bậc $m = 4$ và hệ số phản hồi $(p_3 = 0, p_2 = 0, p_1 = 1, p_0 = 1)$, output của dãy này có chu kỳ $2^m - 1 = 15$; và đây là LFSR có độ dài cực đại (maximum - lenght LFSR).
- Dãy LFSR bậc $m = 4$ và hệ số phản hồi $(p_3 = 1, p_2 = 1, p_1 = 1, p_0 = 1)$, output của dãy này có chu kỳ là 5; vậy đây không phải là LFSR có độ dài cực đại.

Các LFSR thường được xác định bởi đa thức như sau. Một LFSR với hệ số phản hồi $(p_{m-1}, \ldots, p_0)$ được biểu diễn bởi đa thức

$$P(x) = x^m + p_{m-1}x^{m-1} + \cdots + p_1 x + p_0$$

Ví dụ, LFSR (đầu tiên) trong bài tập trước với hệ số $(p_3 = 0, p_2 = 0, p_1 = 1, p_0 = 1)$ được xác định bởi đa thức $x^4 + x + 1$. Việc xác định đa thức này cho phép xác định LFSRs có độ dài cực đại. Cụ thể, LFSR có độ dài cực đại có biểu diễn đa thức nguyên thuỷ. Dưới đây liệt kê một số đa thức nguyên thuỷ.

Ký hiệu $(0, 2, 5)$ chỉ ra đa thức $1 + x^2 + x^5$.

(0,1,2)	(0,1,3,4,24)	(0,1,46)	(0,1,5,7,68)	(0,2,3,5,90)	(0,3,4,5,112)
(0,1,3)	(0,3,25)	(0,5,47)	(0,2,5,6,69)	(0,1,5,8,91)	(0,2,3,5,113)
(0,1,4)	(0,1,3,4,26)	(0,2,3,5,48)	(0,1,3,5,70)	(0,2,5,6,92)	(0,2,3,5,114)
(0,2,5)	(0,1,2,5,27)	(0,4,5,6,49)	(0,1,3,5,71)	(0,2,93)	(0,5,7,8,115)
(0,1,6)	(0,1,28)	(0,2,3,4,50)	(0,3,9,10,72)	(0,1,5,6,94)	(0,1,2,4,116)
(0,1,7)	(0,2,29)	(0,1,3,6,51)	(0,2,3,4,73)	(0,11,95)	(0,1,2,5,117)
(0,1,3,4,8)	(0,1,30)	(0,3,52)	(0,1,2,6,74)	(0,6,9,10,96)	(0,2,5,6,118)
(0,1,9)	(0,3,31)	(0,1,2,6,53)	(0,1,3,6,75)	(0,6,97)	(0,8,119)
(0,3,10)	(0,2,3,7,32)	(0,3,6,8,54)	(0,2,4,5,76)	(0,3,4,7,98)	(0,1,3,4,120)
(0,2,11)	(0,1,3,6,33)	(0,1,2,6,55)	(0,2,5,6,77)	(0,1,3,6,99)	(0,1,5,8,121)
(0,3,12)	(0,1,3,4,34)	(0,2,4,7,56)	(0,1,2,7,78)	(0,2,5,6,100)	(0,1,2,6,122)
(0,1,3,4,13)	(0,2,35)	(0,4,57)	(0,2,3,4,79)	(0,1,6,7,101)	(0,2,123)
(0,5,14)	(0,2,4,5,36)	(0,1,5,6,58)	(0,2,4,9,80)	(0,3,5,6,102)	(0,37,124)
(0,1,15)	(0,1,4,6,37)	(0,2,4,7,59)	(0,4,81)	(0,9,103)	(0,5,6,7,125)
(0,1,3,5,16)	(0,1,5,6,38)	(0,1,60)	(0,4,6,9,82)	(0,1,3,4,104)	(0,2,4,7,126)
(0,3,17)	(0,4,39)	(0,1,2,5,61)	(0,2,4,7,83)	(0,4,105)	(0,1,127)
(0,3,18)	(0,3,4,5,40)	(0,3,5,6,62)	(0,5,84)	(0,1,5,6,106)	(0,1,2,7,128)
(0,1,2,5,19)	(0,3,41)	(0,1,63)	(0,1,2,8,85)	(0,4,7,9,107)	
(0,3,20)	(0,1,2,5,42)	(0,1,3,4,64)	(0,2,5,6,86)	(0,1,4,6,108)	
(0,2,21)	(0,3,4,6,43)	(0,1,3,4,65)	(0,1,5,7,87)	(0,2,4,5,109)	
(0,1,22)	(0,5,44)	(0,3,66)	(0,8,9,11,88)	(0,1,4,6,110)	
(0,5,23)	(0,1,3,4,45)	(0,1,2,5,67)	(0,3,5,6,89)	(0,2,4,7,111)	

Bài tập Hãy xác định các dãy sinh bởi

1. $x^4 + x + 1$
2. $x^4 + x^2 + 1$
3. $x^4 + x^3 + x^2 + x + 1$

Vẽ các LFSR cho mỗi đa thức trên. Đa thức nào là nguyên thuỷ, đa thức nào là bất khả quy?

Bài tập Chúng ta cùng thực hiện bằng cách tấn công khi biết bản rõ vào một hệ mã dòng sinh bởi LFSR. Ta biết bản rõ đã gửi là:

```
1001 0010 0110 1101 1001 0010 0110
```

Ta cũng quan sát trên kênh truyền và thấy bản mã là

```
1011 1100 0011 0001 0010 1011 0001
```

1. Bậc m của bộ sinh khoá mã dòng là gì?
2. Vector khởi tạo là gì?

3. Hãy xác định các hệ số phản hồi của LFSR.
4. Hãy vẽ sơ đồ mạch và kiểm tra dãy output của LFSR.