Implementando LFSRs- configuração Galois

Um linear feedback shift-register, LFSR, é um registrador de deslocamento que possui realimentação entre as saídas de um conjunto de elementos de armazenamento e as suas entradas, a partir de realização de operações lógicas. LFSRs são usados de forma generalizada para geração aleatória de vetores. Existem dois tipos de LFSRs, de acordo com a configuração da realimentação utilizada, conhecidos na literatura por configurações Fibonacci e Galois. Neste texto trataremos apenas da configuração Galois, ficando por conta do aluno interessado uma pesquisa mais detalhada sobre o assunto, para o qual existe farta documentação na Internet e literatura técnica especializada.

1. Configuração de LFSR e Polinômio Primitivo

Na configuração Galois, o LFSR é um registrador de deslocamento onde o próximo estado de todos os elementos de armazenamento, excetuando-se o primeiro (da esquerda para a direita como mostrado na Figura 1), é igual a uma combinação entre o estado atual do elemento de armazenamento na posição anterior da cadeia e do estado atual do último elemento da cadeia ($D_{i-1}=Q_i \oplus a_i Q_0$, para i = 1..n-1). Caso a ligação a_i estiver inativa, ou seja, $a_i=0$, o estado futuro será o valor do estado atual do elemento de armazenamento na posição anterior da cadeia, ou seja, $D_{i-1}=Q_i$, para i = 1..n-1. Se a ligação existir, com $a_i=1$, $D_{i-1}=Q_i \oplus Q_0$, para i = 1..n-1.

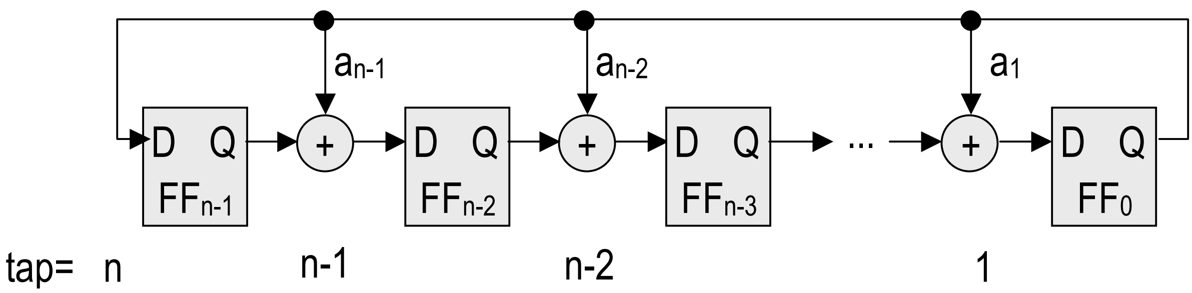


Figura 1. LFSR- configuração Galois

Como podemos observar na figura, cada uma das ligações existentes é conhecida por *tap* que recebe a enumeração de acordo com a sua posição. Um LFSR pode ser identificado pelos seus *taps*, apesar de que não há um padrão exato de como se expressar isto. Um padrão usado (compatível com o software que apresentaremos mais adiante), define LFRS com os taps (n, a_in-i). O exemplo da Figura 2 ilustra o caso de LFSR (4, 3, 1).

A equação de estados do LFSR pode ser expressa por um polinômio característico na forma

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + ... + a_1 x + a_0$$

onde $a_0=1$ e $a_n=1$ para um polinômio de grau *n* (ou LFSR de grau *n*). Então,

$$p(x) = x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + ... + a_1 x + 1$$

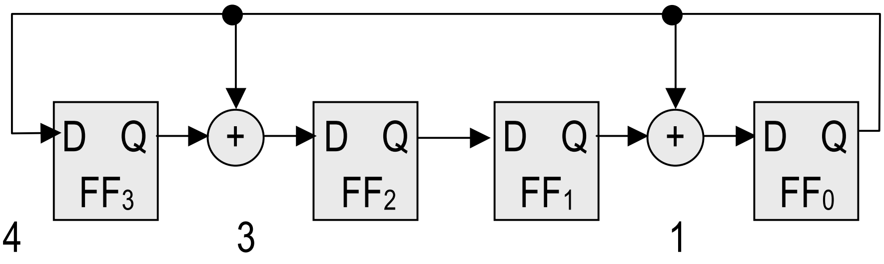


Figura 2. LFSR (4, 3, 1)

Por simplicidade, usamos como coeficientes os mesmos parâmetros indicativos de ligação da figura 1. Desta forma, o polinômio característico do LFSR da figura 2 é

$$p(x) = x^4 + x^3 + x^1 + 1$$

A máquina de estados gera uma sequência pseudo-aleatória de vetores representados pelos bits das saídas dos registradores. Há duas questões bastante relevantes no uso dos LFSRs.

1) o tamanho da sequência: a teoria diz que a sequência aleatória é máxima somente quando o polinômio é primitivo, ou seja, ele não é divisível por outro polinômio qualquer. Por exemplo, o polinômio do LFSR (4, 3, 1) é primitivo, com uma sequência de tamanho n^4-1=15. Quando o polinômio não é primitivo, pode-se ter várias sequências independentes de tamanhos menores.

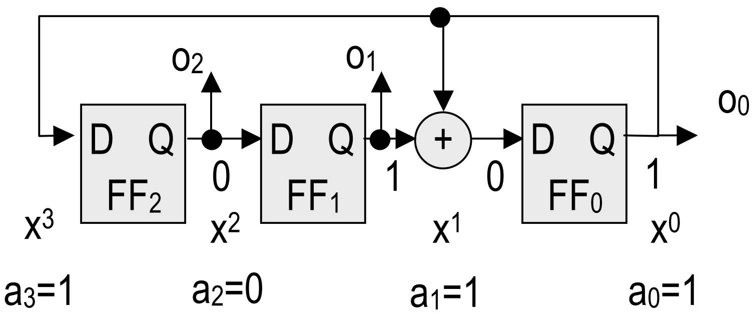
2) a semente: os LFSRs devem ter uma condição ou estado inicial para os registradores. No exemplo do polinômio acima, se a semente for (0,0,0,0), não ocorrerá nenhuma sequência (esta é a razão da sequência máxima ser de apenas 15 vetores); qualquer outro estado inicial (1,1,1,1, por exemplo) faz com que a sequência máxima ocorra. Quando as sequências não são máximas, dependendo da escolha da semente, uma sequência diferente poderá ocorrer.

2. Exemplo

Polinômio

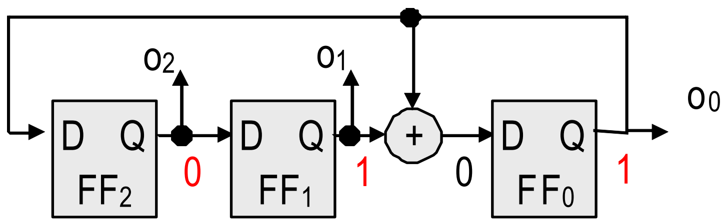
$x^3 + x + 1$

($a_3.x^3 + a_2.x^2 + a_1.x^1 + a_0.x^0$, onde $a_3=a_1=a_0=1$ e $a_2=0$).

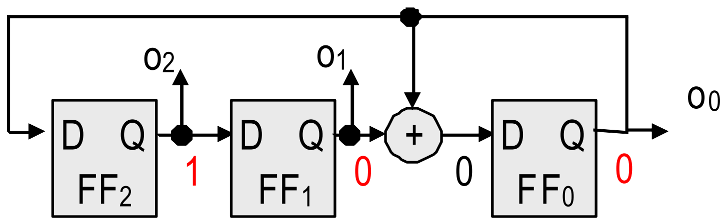


Funcionamento

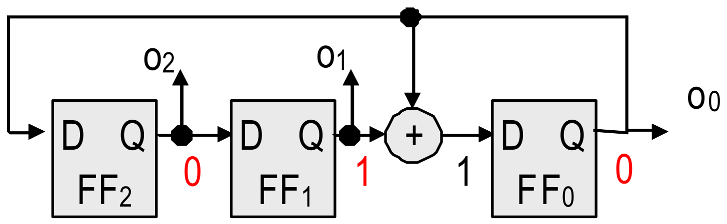
Passo 1:



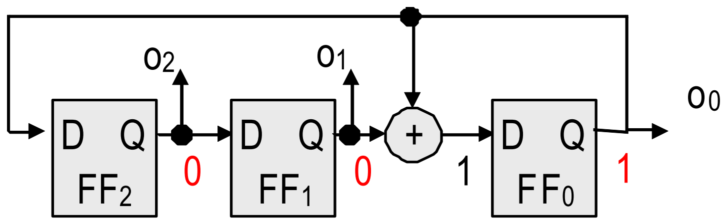
Passo 2:



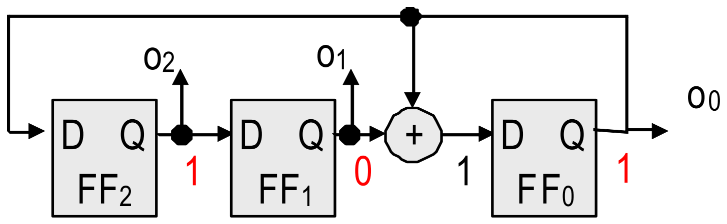
Passo 3:



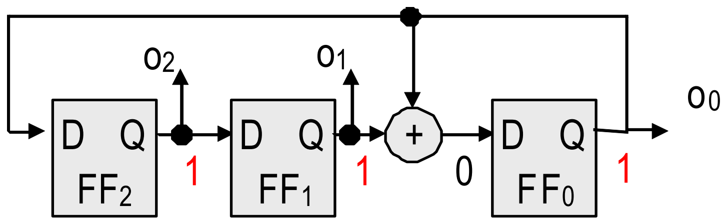
Passo 4:



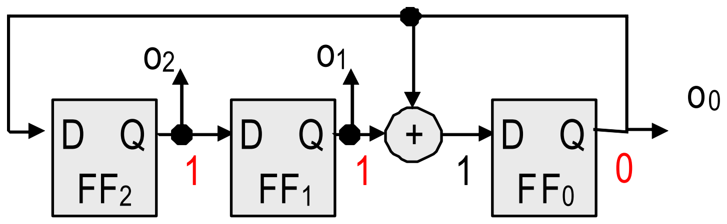
Passo 5:



Passo 6:



Passo 7:



Passo 8: Idêntico ao Passo 1