LFSR（一）：基本结构与概念

LFSR是线性反馈移位寄存器（Linear Feedback Shift Register）的简称。LFSR应用在编码，随机数生成，校验，BIST等多种场景。

 一个n阶的LFSR由n个触发器和若干个异或门组成。在实际应用当中，主要用到两种类型的LFSR，即异或门外接线性反馈移位寄存器（IE型LFSR）和异或门内接线性反馈移位寄存器（EE型LFSR）。



IE型LFSR



EE型LFSR

这两种LFSR是等价的。

若认为{Qn，Qn-1，… Q2，Q1，Q0}为一个状态，可见，每一个时钟周期下，LFSR都会完成一次状态跳转。基于此，LFSR可以进行状态机，随机数生成等工作。

在继续介绍LFSR之前，我们先了解数字序列的另一种表示方法，多项式表示。

对于一个二进制序列（左侧为先输入的高位），比如10011，我们可以将其表示为多项式形式：

$$x^{4}+x+1$$

一般的，对于一个二进制序列{Gn,Gn-1，… G2,G1,G0}，我们用多项式：

$$M\left(x\right)=\sum\_{i=0}^{n}G\_{i}x^{i}$$

来表示。

这里不加证明的给出几个结论，

1. LFSR结构也可以使用多项式的形式表示，我们称其为生成多项式：

$$G\left(x\right)=\sum\_{i=0}^{n}G\_{i}x^{i}$$

1. 对于LFSR，其输入序列：$M\left(x\right)=\sum\_{i=0}^{n}G\_{i}x^{i}$ ，生成多项式$G\left(x\right)=\sum\_{i=0}^{n}G\_{i}x^{i}$，则有

$$R\left(x\right)=\frac{M（X）}{G（X）}$$

R（X）为LFSR中剩余的数据。这里的除法是亦或运算完成的，没有进位和借位运算。

正是由于LFSR在有限域上这个特性，它可以通过初始化种子产生伪随机序列（n个寄存器可以产生2^n-1个状态），也可用于CRC校验等。此外，LFSR还有其他更为广泛的应用，比如分析状态机，构造加、解扰算法等模型（可参考FPGA硬件算法——加扰并行化）。