数字电路与数字系统

实验报告

实　　验: 移位寄存器及桶形移位器

姓　　名: 周心同

学　　号: 201220069

目录

1.实验目的

复习寄存器的原理

学习常用的移位寄存器的设计

实现在移位指令中需要用到的桶形移位器

2.实验原理

2.1 随机数发生器

经典的 LFSR（线性反馈移位寄存器，Linear-feedbackshift register）可以使用 n 位移位寄存器生成长度为 2n − 1 的二进制循环序列。这类序列的片段在表观上是随机的，所以被广泛用于通信中的随机序列生成。例如，在 CDMA 通信中的长码的长度就是 2^42 − 1 的伪随机序列。

具体实现时，可以用一个 8 位右移移位寄存器，从左到右的比特以 $x_7x_6x_5x_4x_3x_2x_1x_0$ 表示。每个时钟周期右移一位，x_0 被移出，最左边移入的位按照上一周期的值计算[①]：

$$x_8 = x_4 \oplus x_3 \oplus x_2 \oplus x_0 \tag{6-1}$$

例如，初始二进制值为 00000001 时，移位寄存器的状态将按 00000001 → 10000000 → 01000000 → 001000000 → 00010000 → 10001000 … 变化。该序列的周期为 255。当然，当初始值为全零时，系统将一直停留在全零状态，所以需要对全零状态进行特殊处理。

3.实验环境

- 软件环境

Quartus 17.1 Lite

- 硬件环境

开发板：DE10 Standard

FPGA：Intel Cyclone V SE 5CSXFC6D6F31C6N

4.实验步骤和结果

4.1 随机数发生器

4.1.1 代码

```
module lfsr(input  [7:0]  seed,
    input  clk,
    output reg [7:0] dout,
    input in//置位端
    );
 //add your code here

 always @(posedge clk)
begin
 if(in==1)
 dout<=seed;
 else
    dout<={dout[4]^dout[3]^dout[2]^dout[0],dout[7:1]};
 end

 endmodule
```

4.1.2 接口

```
//====================
wire [7:0] a;
lfsr l(SW[7:0],
    KEY[0],
    a ,
    SW[9]
    );

bcd7seg b(
     a[3:0],
     HEX0
     );

bcd7seg b2(
     a[7:4],
     HEX1
     );

//====================
```

4.1.3 仿真

由于是七段数码管显示数字，见于上板实验。

5. 实验中遇到的问题及解决办法

问题：初始化究竟是否要自己输入还是内置？

解决办法：加了一个置位端来决定自己输入。

6.实验启示和建议

关于思考题，生成的伪随机数序列仍然有一定的规律，如何能够生成更加复杂的伪随机数序列？
我首先的疑问是 为什么

具体实现时，可以用一个 8 位右移移位寄存器，从左到右的比特以 $x_7x_6x_5x_4x_3x_2x_1x_0$ 表示。每个时钟周期右移一位，x_0 被移出，最左边移入的位按照上一周期的值计算[①]：

$$x_8 = x_4 \oplus x_3 \oplus x_2 \oplus x_0 \tag{6-1}$$

这样的算法周期为 255，即能全排列 8 位数字?

由网上得答案知（截取一部分）：

同大多数密钥流产生器一样，LFSR也具有周期。由于一个n级LFSR最多只能遍历 2^n-1 种状态，因此，当LFSR移位到一定程度时，一定会出现重复的状态。而相同状态生成的反馈函数结果总是相同的，因此，LFSR会陷入一种循环，即LFSR存在周期。

可以明显看出，LFSR的周期与其反馈函数有很密切的关系，反馈函数决定了LFSR的循环序列。

我们先引入阶的概念：假设 $f(x)$ 是 $GF(2)$ 上的多项式，使 $f(x)|(x^n-1)$ 成立的**最小的n即为这个多项式的阶。**（这里的n与上文提到的级数n不是一回事）阶往往也被称为**周期。**如下图所示，有 $(x^4+x^3+x^2+x+1)|(x^5-1)$，故 $f(x)$ 的周期为5.

例：$f(x)=x^4+x^3+x^2+x+1$ 为 $GF(2)$ 上多项式，以它为特征多项式的LFSR 的输出序列周期

$$(x^5-1)=(x^4+x^3+x^2+x+1)(x-1)=f(x)(x-1)$$

$$f(x)|x^n-1, \quad n=5$$

图9-5 特征多项式的阶

反馈函数特征多项式的阶，就是LFSR产生序列的周期（证明略）。例如：对于图9-5中的特征多项式，其对应的LFSR和反馈函数如图9-6所示。图9-5说明了该特征多项式的阶为5，则可以验证发现，图9-6中LFSR的周期也为5（假设初始状态为0001）。（可以看出，图中状态的周期为5，输出的周期也为5）

知道这个 我们可以生成周期同样为 255 的算法，当然要变得更复杂，可能需要掺和一些其他的密码学算法进去。（文章见 https://zhuanlan.zhihu.com/p/366067972）