现代密码学

第十五讲 非线性序列2

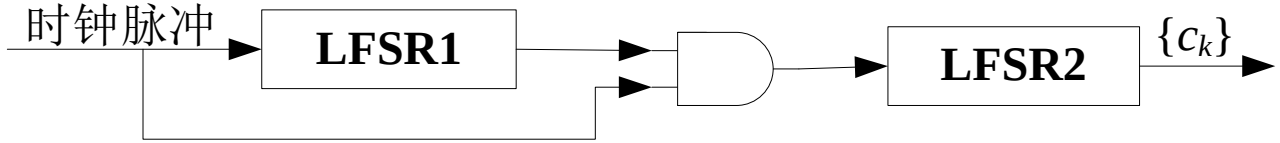
信息与软件工程学院

第十五讲 非线性序列2

钟控序列生成器

钟控序列生成器模型

- 钟控序列最基本的模型是用一个**LFSR**控制另外一个**LFSR**的移位时钟脉冲，如图所示，一个最简单钟控序列生成器



  - 假设**LFSR1**和**LFSR2**分别输出序列$\{a_k\}$和$\{b_k\}$，其周期分别为p_1和p_2。
  - 当**LFSR1**输出**1**时，移位时钟脉冲通过与门使**LFSR2**进行一次移位，从而生成下一位。
  - 当**LFSR1**输出**0**时，移位时钟脉冲无法通过与门影响**LFSR2**。因此**LFSR2**重复输出前一位。

钟控序列的周期

- 假设LFSR1和LFSR2分别输出序列$\{a_k\}$和$\{b_k\}$，其周期分别为p_1和p_2。假设钟控序列$\{c_k\}$的周期为p，可得如下关系：
- $$p=\frac{p_1 p_2}{\gcd(w_1, p_2)}，\quad 其中 w_1=\sum_{i=0}^{p_1-1} a_i$$

- c_k的一个周期至少是LFSR1和LFSR2同时回到初始状态的时刻
  - 显然当运行$p_1\times p_2$个节拍后两个LFSR必然回到初态，因此周期至多是$p_1\times p_2$
  - LFSR1运行一个周期，LFSR2运行$w_1=dt$拍，$d=\gcd(w_1,p_2)$
  - 则LFSR1运行（p_2/d）个周期后，LFSR2刚好运行$dt\times p_2/\mathrm{d}=tp_2$拍，即$t$个周期，于是两个LFSR都回到初态，这时运行了（$p_2/d$）$\times p_1$个节拍

钟控序列的周期（续）

- 若$\{a_k\}$和$\{b_k\}$的极小特征多项式分别为GF(2)上的m和n次本原多项式$f_1(x)$和$f_2(x)$，且$m|n$。
- 则$p_1=2^m-1$, $p_2=2^n-1$。
- 而w_1=为$\{a_k\}$一个周期内1的个数，因此$w_1=2^{m-1}$
- 故$\gcd(w_1, p_2)=1$，所以$p=p_1p_2=(2^m-1)(2^n-1)$。

钟控序列的线性复杂度

- 可推导出$\{c_k\}$的线性复杂度为$n(2^m-1)$，极小特征多项式为 $f_2(x^{2^m-1})$
  - 其对应的LFSR2的抽头每隔周期$p_1=2^m-1$一个，这样，参与运算的每个抽头对应的状态的节奏相同，从而相当于对LFSR2序列进行每2^{m-1}拍的抽样序列(不计由于LFSR1的0游程而产生的重复)，这个序列只是LFSR2的平移和按照LFSR1中的0游程进行迟延，而抽头应该与LFSR2的节奏一致，所以其极小多项式和线性复杂度如上

钟控序列的例子

- 例： 设LFSR1为3级m序列生成器，其特征多项式为$f_1(x)=1+x+x^3$。设初态为$a_0=a_1=a_2=1$，于是输出序列为$\{a_k\}=1,1,1,0,1,0,0,\ldots$
- 又设LFSR2为3级m序列生成器，且记其状态向量为σ_k，则在上图的构造下σ_k的变化情况如下：
  - σ_0，σ_1，σ_2，σ_3，σ_3，σ_4，σ_4，σ_4，
  - σ_5，σ_6，σ_0，σ_0，σ_1，σ_1，σ_1，
  - σ_2，σ_3，σ_4，σ_4，σ_5，σ_5，σ_5，
  - σ_6，σ_0，σ_1，σ_1，σ_2，σ_2，σ_2，
  - σ_0，σ_1，σ_2，σ_2，σ_3，σ_3，σ_3，
  - σ_4，σ_5，σ_6，σ_6，σ_0，σ_0，…
- $\{c_k\}$的周期为$(2^3-1)^2=49$，在它的一个周期内，每个σ_k恰好出现7次

例（续）

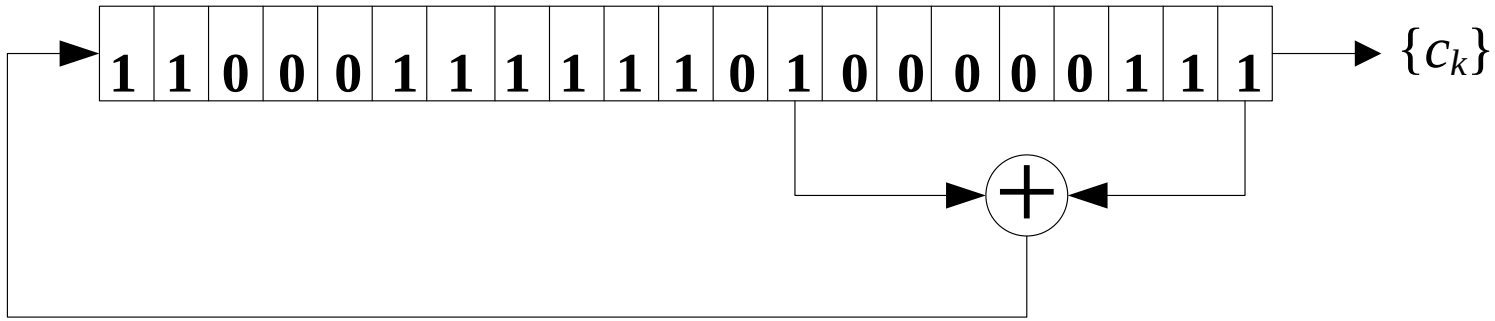
- 设$f_2(x)=1+x^2+x^3$为LFSR2的特征多项式，且初态为$b_0=b_1=b_2=1$，则$\{b_k\}=1,1,1,0,0,1,0,1,1,1\ldots$
  - 由σ_k的变化情况得 $\{c_k\}=1,1,1,0,0,0,0,0,\ 1,0,1,1,1,1,1,1,\ 1,0,0,0,1,1,1,$ $0,1,1,1,1,1,1,\ 0,0,1,1,0,0,0,\ 1,1,1,1,0,0,0,\ 0,1,0,0,1,1,\ldots$

$\sigma_0,\ \sigma_1,\ \sigma_2,\ \sigma_3,\ \sigma_3,\ \sigma_4,\ \sigma_4,\ \sigma_4,$

- $\sigma_5,\ \sigma_6,\ \sigma_0,\ \sigma_0,\ \sigma_1,\ \sigma_1,\ \sigma_1,$
- $\sigma_2,\ \sigma_3,\ \sigma_4,\ \sigma_4,\ \sigma_5,\ \sigma_5,\ \sigma_5,$
- $\sigma_6,\ \sigma_0,\ \sigma_1,\ \sigma_1,\ \sigma_2,\ \sigma_2,\ \sigma_2,$
- $\sigma_0,\ \sigma_1,\ \sigma_2,\ \sigma_2,\ \sigma_3,\ \sigma_3,\ \sigma_3,$
- $\sigma_4,\ \sigma_5,\ \sigma_6,\ \sigma_6,\ \sigma_0,\ \sigma_0,\ \ldots$

状态 (b_3,b_2,b_1)	输出
σ_0 1 1 1	1
σ_1 0 1 1	1
σ_2 0 0 1	1
σ_3 1 0 0	0
σ_4 0 1 0	0
σ_5 1 0 1	1
σ_6 1 1 0	0

- $\{c_k\}$的极小特征多项式为$1+x^{14}+x^{21}$，其线性复杂度为$3(2^3-1)=21$，下图是其线性等价生成器。



感 谢 聆 听!

xynie@uestc.edu.cn