Problem Solving

Unit 6: Pseudo Random Number Generator

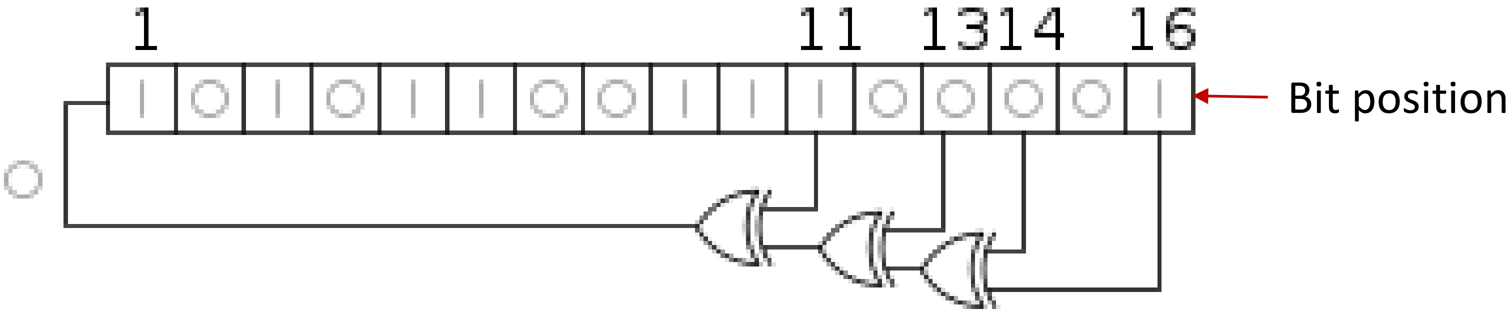
Rung-Bin Lin
International Bachelor Program in Informatics
Yuan Ze University

Oct 18, 2022

Lab 6: Random Number Generators

https://en.wikipedia.org/wiki/Linear-feedback_shift_register

- Write a program to implement a pseudo random number generator using Linear Feedback Shift Register (LFSR).
- Below is a Fibonacci LFSR associated with a characteristic function $x^{16}+x^{14}+x^{13}+x^{11}+1$. There will be a xi term for each tap position for i>0.

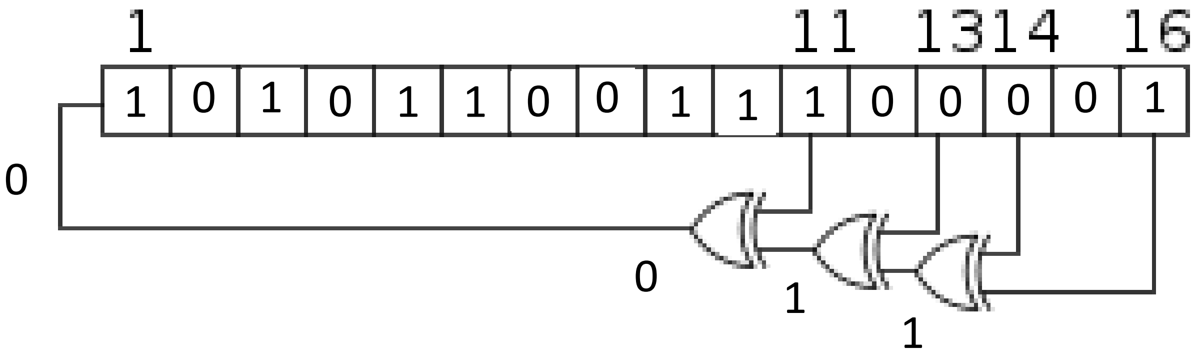


- The bit positions that affect the next state are called the taps. For example, bits 11, 13, 14, and 16 are taps.
- The bit pattern corresponds to an integer $(ACE1)_{16}$.
- The next state (bit pattern) is formed by doing logical right shift by one bit and setting bit_1= bit_11 XOR bit_13 XOR bit_14 XOR bit_16. This counts the total number of 1's. If it is odd, bit_1 =1.

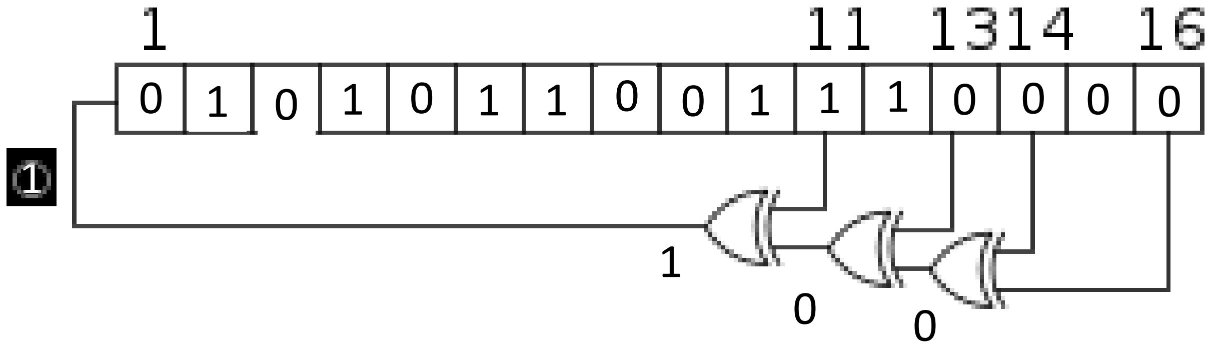
Random Number Generators (2)

Doing logical right shift by one bit, i.e., shifting all the bits to the right by one place at the same time.

Current state $(ACE1)_{16}$



Next state $(5670)_{16}$



- The first bit pattern is called the seed of the random number generator. It can be set to any value. Starting from a seed s_0, if we repeatedly shift the bits at the same time to the right, we will obtain a sequence of bit pattern, s_0, s_1, s_2, ..., s_n, s_{n+1}, s_{n+2}, ...each of which represents an integer number. Any two consecutive numbers in the sequence are normally different.

Hamming Distance

- The Hamming distance of two consecutive pseudo random numbers (i.e., two bit patterns) is the number of same-bit positions which have different bit values in these two random numbers. For example, the Hamming distance of the two bit patterns 00110 and 10101 is 3. The Hamming distance of the two pseudo random numbers in the previous slide is 9.

Length of a Cycle

- Given a sequence of pseudo random numbers s_0, s_1, s_2, ..., s_n, s_{n+1}, s_{n+2}, ..., there exists a number s_n which is equal to s_j such that *n-j* is minimum for all n's and j's, $s_n \neq s_i$, i=j+1,..., n-1. Then, the subsequence s_j, s_{j+1}, s_{j+2}, ..., s_{n-1} is called a cycle and *n-j* is called the length of the cycle. Note that a cycle may not include the seed, i.e., a seed is not repeated.
- Given a k-bit pseudo random number generator, the cycle length is at most 2^k-1. It is not easy to find the cycle length. So in this lab you are asked to generate a sequence of numbers s_0, s_1, s_2, ..., s_m until s_0 is repeated. Otherwise, continue generating random numbers until m=2^k-2.

Input

- The first line gives the number of test cases. It is then followed by the input of each test case. The input of each test case has three lines. The first line gives the number of bits of an LFSR, which is less than 35. The second line gives the tap bits where the last bit in the line is 0 which is used to terminate the line. The tap bits are presented in order of increasing position values. There should be at least two taps. The third line is the seed for the LFSR. The left most bit is at position one. Any two adjacent bits are separated by space characters.

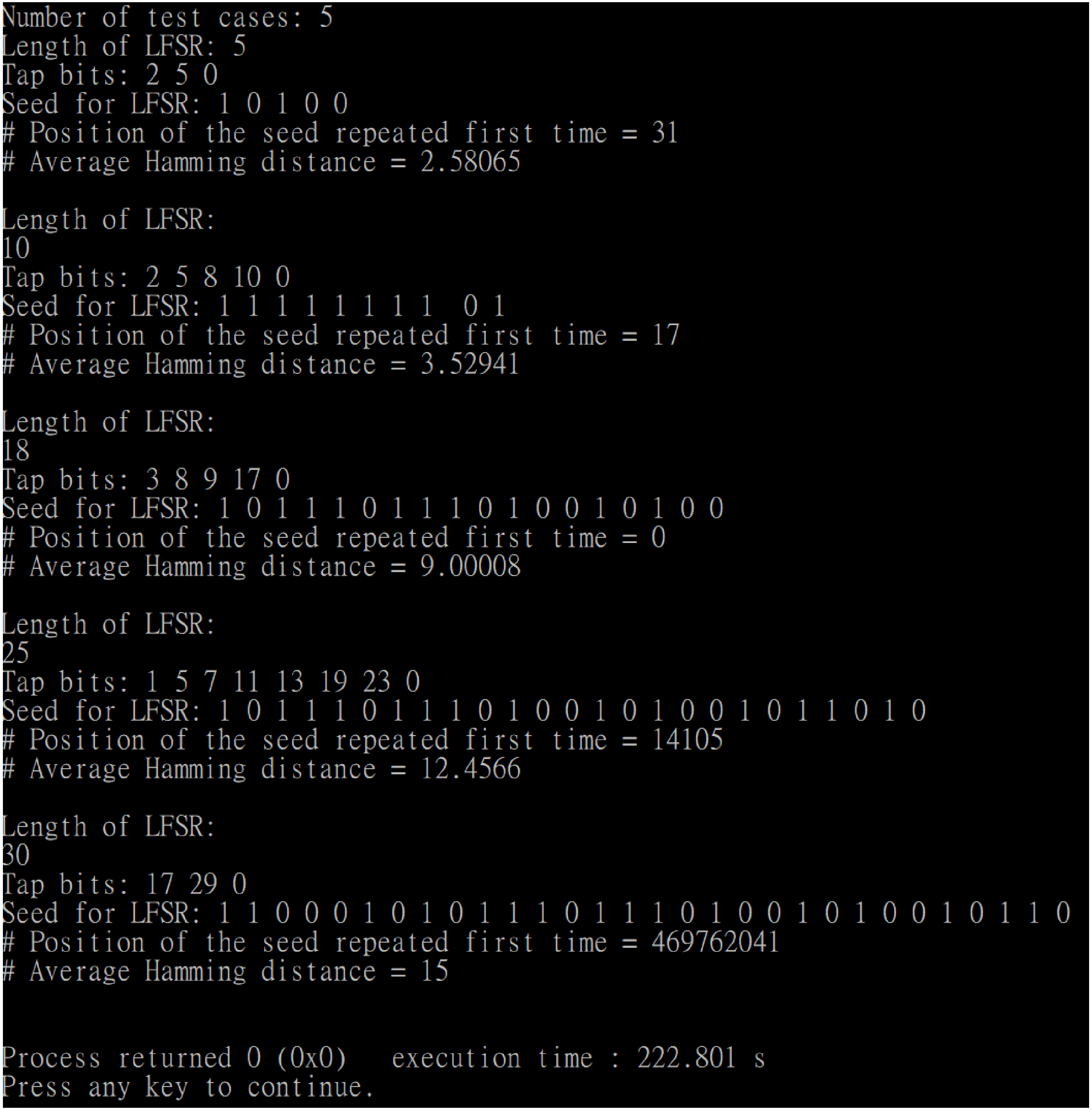
Output

- The output of each test case has two numbers. The first number is the position where the seed re-appears first time. Output 0 if the seed does not re-appear. The second number should give the average Hamming distance of two consecutive pseudo numbers in the whole sequence.

Input Example

```
5
5
2 5 0
1 0 1 0 0
10
2 5 8 10 0
1 1 1 1 1 1 1 1  0 1
18
3 8 9 17 0
1 0 1 1 1 0 1 1 1 0 1 0 0 1 0 1 0 0
25
1 5 7 11 13 19 23 0
1 0 1 1 1 0 1 1 1 0 1 0 0 1 0 1 0 0 1 0 1 1 0 1 0
30
17 29 0
1 1 0 0 0 1 0 1 0 1 1 1 0 1 1 1 0 1 0 0 1 0 1 0 0 1 0 1 1 0
```

Output



```
Number of test cases: 5
Length of LFSR: 5
Tap bits: 2 5 0
Seed for LFSR: 1 0 1 0 0
# Position of the seed repeated first time = 31
# Average Hamming distance = 2.58065

Length of LFSR:
10
Tap bits: 2 5 8 10 0
Seed for LFSR: 1 1 1 1 1 1 1 1  0 1
# Position of the seed repeated first time = 17
# Average Hamming distance = 3.52941

Length of LFSR:
18
Tap bits: 3 8 9 17 0
Seed for LFSR: 1 0 1 1 1 0 1 1 1 0 1 0 0 1 0 1 0 0
# Position of the seed repeated first time = 0
# Average Hamming distance = 9.00008

Length of LFSR:
25
Tap bits: 1 5 7 11 13 19 23 0
Seed for LFSR: 1 0 1 1 1 0 1 1 1 0 1 0 0 1 0 1 0 0 1 0 1 1 0 1 0
# Position of the seed repeated first time = 14105
# Average Hamming distance = 12.4566

Length of LFSR:
30
Tap bits: 17 29 0
Seed for LFSR: 1 1 0 0 0 1 0 1 0 1 1 1 0 1 1 1 0 1 0 0 1 0 1 0 0 1 0 1 1 0
# Position of the seed repeated first time = 469762041
# Average Hamming distance = 15


Process returned 0 (0x0)   execution time : 222.801 s
Press any key to continue.
```