Problem Solving

Unit 6: Pseudo Random Number Generator

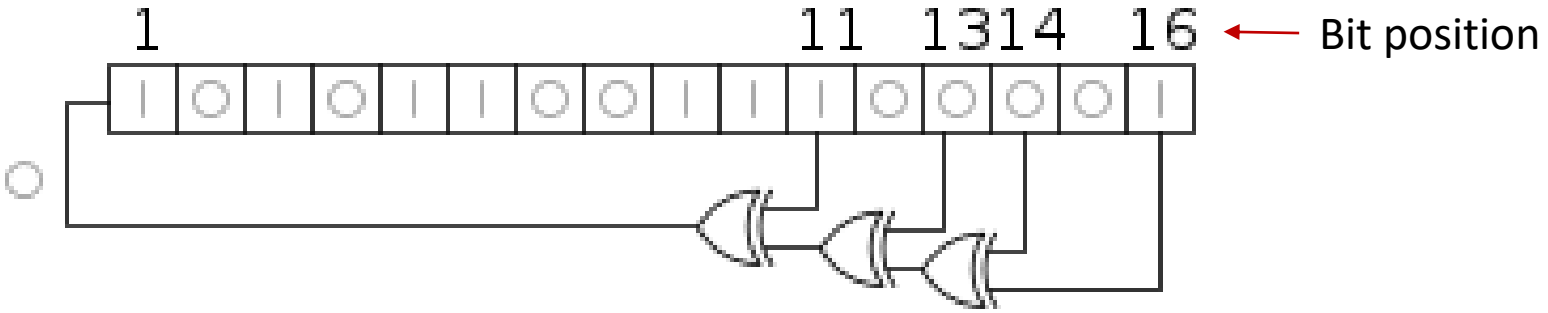
Rung-Bin Lin
International Bachelor Program in Informatics
Yuan Ze University

Oct 24, 2023

Lab 6: Random Number Generator

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 an x^i term for each tap position for i>0.

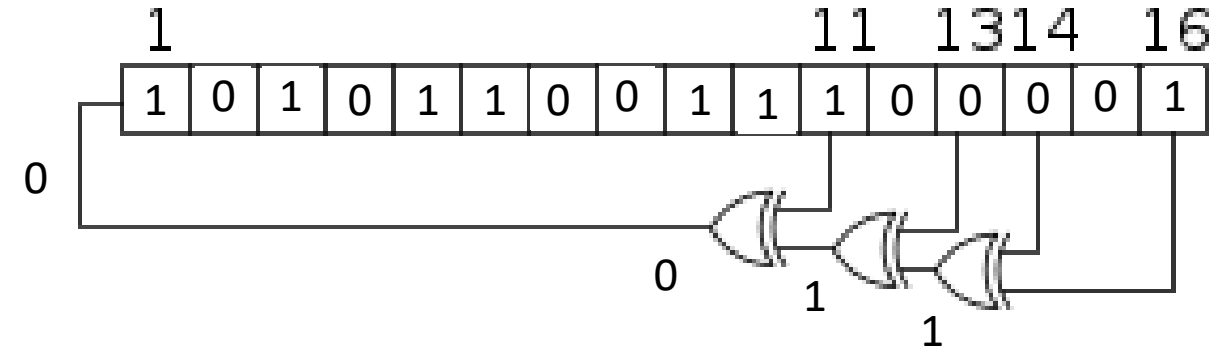


- The bit positions that affect the next state are called the taps. For example, bits 11, 13, 14, and 16 are taps.
- The bit pattern corresponds to an integer $(ACE1)_{16}$.
- The next state (bit pattern) is formed by doing logical right shift by one bit and setting bit_1= bit_11 XOR bit_13 XOR bit_14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

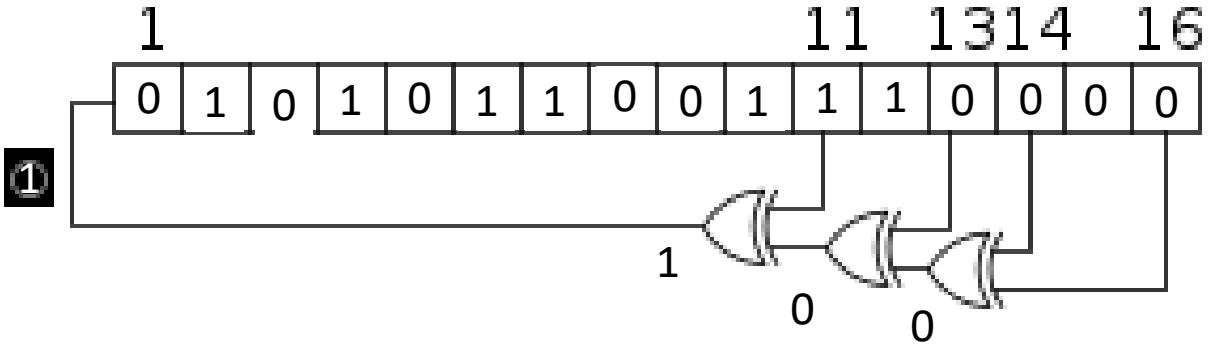
Random Number Generator (2)

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 patterns, 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 first time a number s_n equal to s_j. 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 only one line which contains two positive integers. The first integer k gives the number of bits of an LFSR, which is less than 32. The second integer N < 2^{32}-1 provides the locations of tap bits and forms the seed of the LFSR in the following way:**
  1. **Convert N into an unsigned binary number.**
  2. **The seed of the LFSR is formed by taking the first k least significant bits of N. The least significant bit of the first k bits corresponds the bit at position 1 of the LFSR. The rest of the bits corresponds in the same way.**
  3. **The positions of tap bits are determined by the values of the bits in the seed. If a position has a non-zero bit value, it is the position of a tab in the LFSR. If the number of tap bits is less than two, ask for re-entering the integer N.**

Output

- The output of each test case has three lines. The first line should give the bit positions of tab bits in the order of increasing bit positions. The second line should give the bit values of seed in order of increasing bit positions. No blank space is needed between two bit values. The third line has three 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 and third number give the minimum and maximum Hamming distances of two consecutive pseudo numbers in the whole sequence, respectively.

Input Example

6
5 84
10 2188
10 2706
10 767
32 4294967295
29 1507

The first test case specifies that there are five bits in the LFSR. Since the bit pattern of the second integer 84 is 1010100. Since the five least significant bit is 10100. So the seed will be 00101 in order of increasing bit positions. The positions of tap bits are 3 and 5.

Output

```
Number of test cases: 6
Length of LFSR: 5
Integer determines tap bits and seed: 84
3 5
00101
31 1 5
Length of LFSR: 10
Integer determines tap bits and seed: 2188
3 4 8
0011000100
0 2 9
Length of LFSR: 10
Integer determines tap bits and seed: 2706
2 5 8 10
0100100101
51 1 8
Length of LFSR: 10
Integer determines tap bits and seed: 767
1 2 3 4 5 6 7 8 10
1111111101
434 1 9
Length of LFSR: 32
Integer determines tap bits and seed: 4294967295
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
11111111111111111111111111111111
33 1 2
Length of LFSR: 29
Integer determines tap bits and seed: 1057
1 6 11
10000100001000000000000000000
0 5 22

Process returned 0 (0x0)   execution time : 234.605 s
Press any key to continue.
```

Note that the last test case might take several minutes.