Problem Solving

Unit 6: Pseudo Random Number Generator

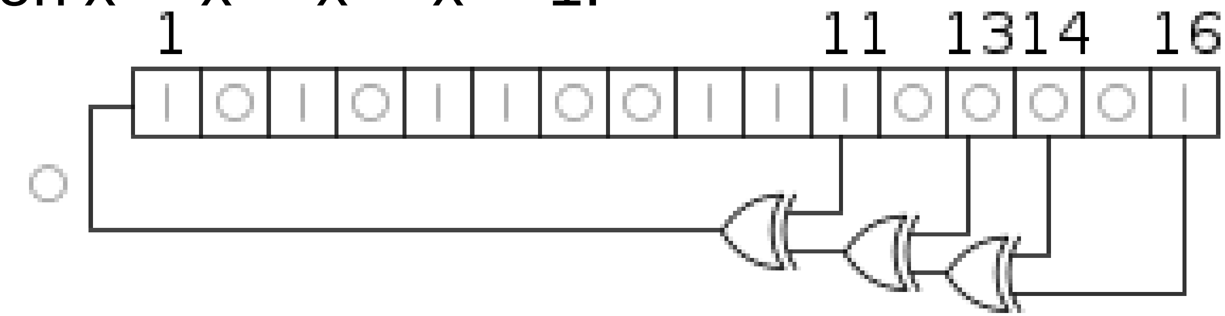
Rung-Bin Lin
International Bachelor Program in Informatics
Yuan Ze University

Nov. 2, 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 $x^{16}+x^{14}+x^{13}+x^{11}+1$.

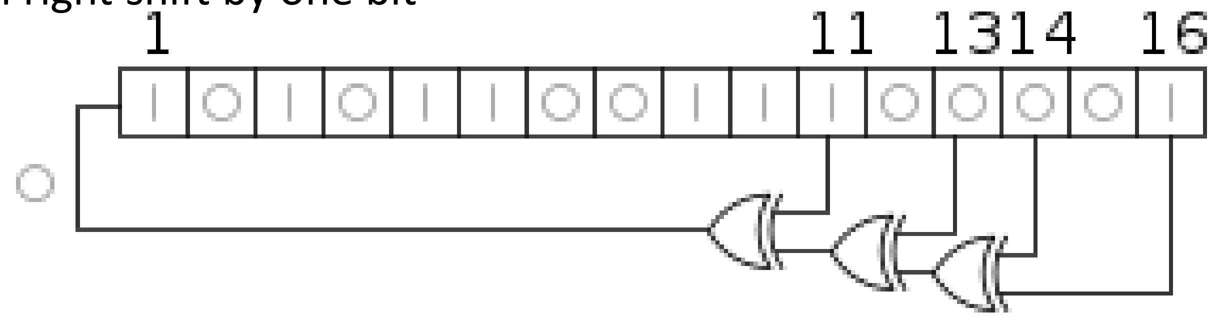


- The bit positions that affect the next state are called the taps. Bits 11, 13, 14, and 16 are taps.
- The bit pattern corresponds to an integer $(ACE1)_{16}$.
- The next state (bit pattern) is formed by doing logical right shift by one bit and setting bit_1= bit_11 XOR bit_13 XOR bit_14 XOR bit_16.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

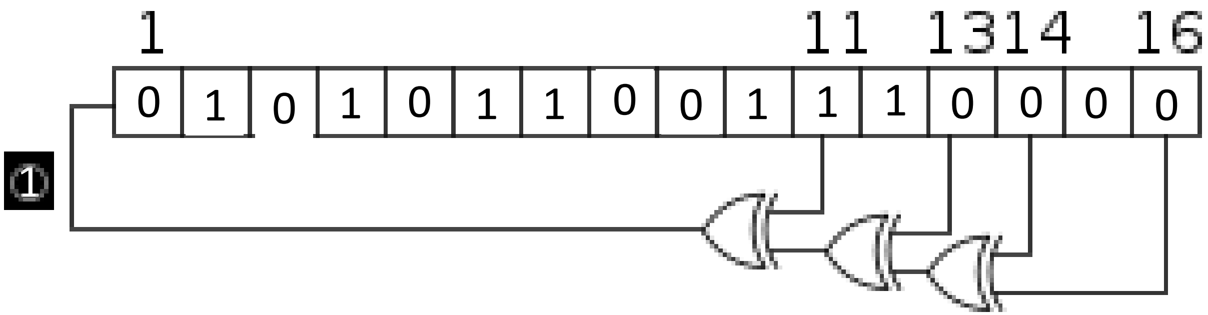
Random Number Generators (2)

Doing logical right shift by one bit

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.

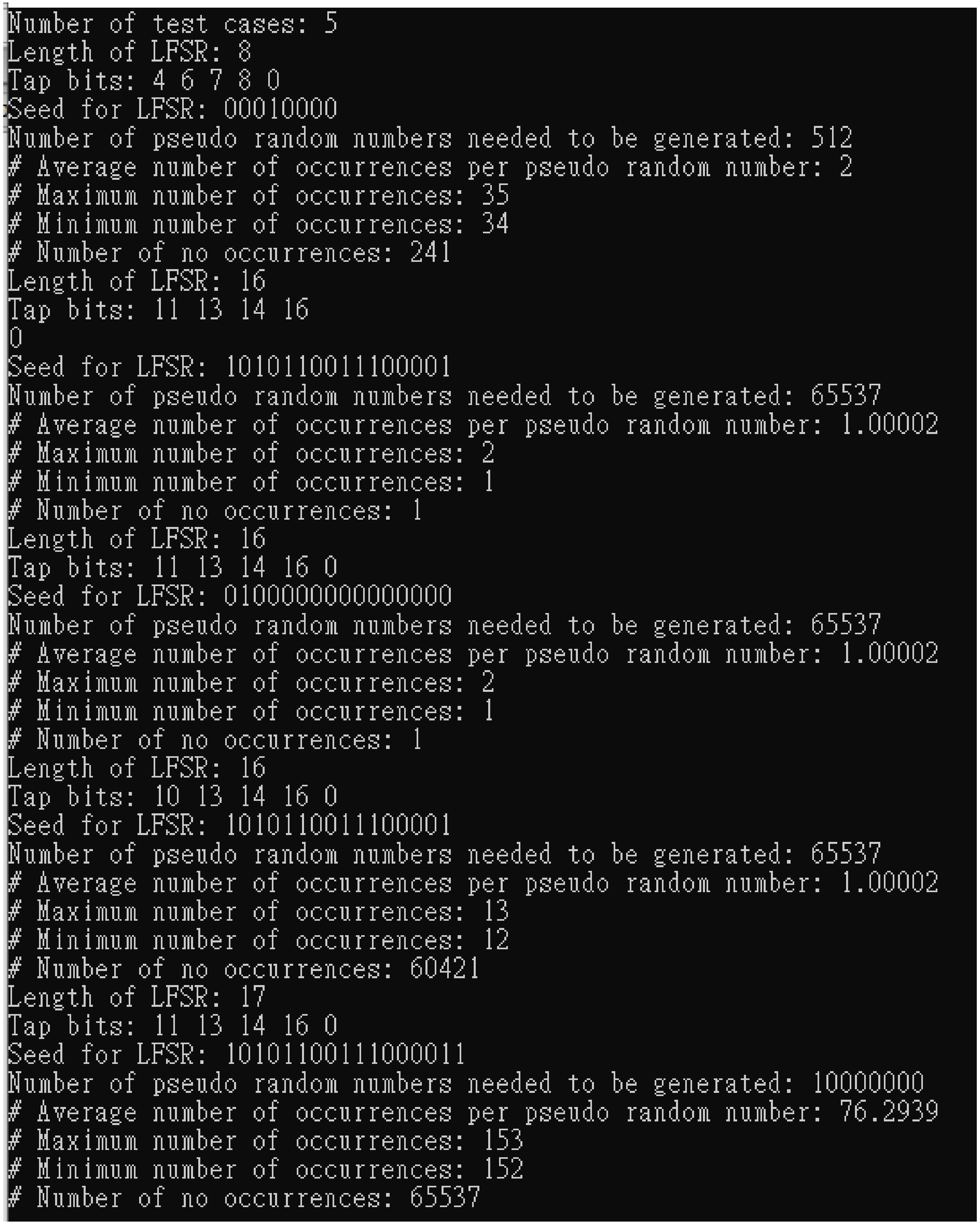
Input

- The first line gives the number of test cases. It then followed by the input of each test case. The input of each test case has four lines. The first line gives the number of bits of an LFSR. The second line gives the tap bits where the last bit in the line is 0 used to terminate the line. The tap bits are presented in order of increasing values. There should be at least two taps. The third line is the seed for the LFSR. The fourth line is the number of pseudo random numbers must be generated for a test case. Assume that the length of LFSR is not larger than 17 and the number of pseudo random numbers that need be generated is less than 2^{31}-1.

Output

- The output of each test case has four numbers. The first number is the average number of occurrences for each pseudo random number. The second is the maximum number of occurrences of pseudo random numbers. The third is the minimum number of occurrences of pseudo random numbers. The fourth number of the number of pseudo random numbers which do not occur at all for a test case.

Example



```
Number of test cases: 5
Length of LFSR: 8
Tap bits: 4 6 7 8 0
Seed for LFSR: 00010000
Number of pseudo random numbers needed to be generated: 512
# Average number of occurrences per pseudo random number: 2
# Maximum number of occurrences: 35
# Minimum number of occurrences: 34
# Number of no occurrences: 241
Length of LFSR: 16
Tap bits: 11 13 14 16
0
Seed for LFSR: 1010110011100001
Number of pseudo random numbers needed to be generated: 65537
# Average number of occurrences per pseudo random number: 1.00002
# Maximum number of occurrences: 2
# Minimum number of occurrences: 1
# Number of no occurrences: 1
Length of LFSR: 16
Tap bits: 11 13 14 16 0
Seed for LFSR: 0100000000000000
Number of pseudo random numbers needed to be generated: 65537
# Average number of occurrences per pseudo random number: 1.00002
# Maximum number of occurrences: 2
# Minimum number of occurrences: 1
# Number of no occurrences: 1
Length of LFSR: 16
Tap bits: 10 13 14 16 0
Seed for LFSR: 1010110011100001
Number of pseudo random numbers needed to be generated: 65537
# Average number of occurrences per pseudo random number: 1.00002
# Maximum number of occurrences: 13
# Minimum number of occurrences: 12
# Number of no occurrences: 60421
Length of LFSR: 17
Tap bits: 11 13 14 16 0
Seed for LFSR: 10101100111000011
Number of pseudo random numbers needed to be generated: 10000000
# Average number of occurrences per pseudo random number: 76.2939
# Maximum number of occurrences: 153
# Minimum number of occurrences: 152
# Number of no occurrences: 65537
```

Follow All Requirements

- Input formats
- Output formats
- All constraints on input data
- Coding styles
    - Avoiding using variables which do not have expressive power. That is, a variable name should carry the meaning of the matter in which the variable intends to represent.

If you don’t follow the requirements, up to 30% of the points for your lab will be deduced.

Rules for Program Submission

- Put all the relevant files in the same folder.
- Name your folder SID_LabX, where ID is your student ID number and X is the number assigned to the lab. If a lab has N parts, N>1, then create N sub-folders with their names SID_LabX_N in the the folder SID_LabX.
  - ➢ For example, for Lab 2 with only one part and with student ID number 1041544, the name of the folder must be S1041544_Lab2. N is omitted if there is only one part.
  - ➢ Another example, similar to the above but Lab 2 has two parts. Then, you have to create a folder S1041544_Lab2 and two sub-folders S1041544_Lab2_1 and S1041544_Lab2_2
- Compress the folder into a file named SID_LabX.zip, for example, S1041533_Lab2.zip. Then, submit the compressed file
- If you violate this rule, your lab will not be graded. If graded other penalty will be applied.