COMPENG 4DM4 Lab 1 Report

Aaron Pinto
pintoa9

Raeed Hassan
hassam41

October 1, 2022

Exercise Part (A) - Generate Random Numbers

(A1) The LSFR is implemented in '`exerciseA.m`', submitted in the pdf '`exerciseA.pdf`'. As we expect the period of the output data stream to be $2^n - 1$, we initialized an output vector `DATA_OUT` with size $2^{22} - 1$ for our 22-bit LSFR. The LSFR is stored in a vector `S`. In each clock tick we store the least significant bit or output in variable `LSB`, shift bits 2–21 into 1–20, use the MATLAB built-in `xor` function to XOR bit 22 and `LSB` and shift the result into bit 21, and shift `LSB` into bit 22. The output or `LSB` at each clock tick is stored into `DATA_OUT`.

(A2) For each clock-tick of the LSFR, we check if the current state of the LSFR is equal to the initial state. If these states are equal, then the LSFR will begin to repeat. The 22-bit LSFR reaches a steady-state after 4194303 clock-ticks, with the initial state of the LSFR appearing again after the 4194303 clock-ticks. This means the period of the LSFR is 4194303, and it can generate a pseudo-random output bit-stream that is 4194303 bits long.

(A3) The code to generate '`my_random_numbers.m`' is implemented in '`exerciseA.m`', submitted in the pdf '`exerciseA.pdf`'. The code stores the output bit-stream for one period from `DATA_OUT` and stores it into `BITS`, which we modify and then convert each byte from the bit-stream into a decimal number using MATLAB's built-in `num2str` and `bin2dec` functions. These decimal numbers are then written to the file '`my_random_numbers.m`'.

(A4)

(A5) The number of conditional probability for 0-runs was determined by dividing the number of 0-runs of length k by the total number of 0-runs. The conditional probabilities are shown in Listing 1.

Listing 1: Conditional probability of 0-runs

```
>> zeroruns_table(3,:)

ans =

    0.5000    0.2500    0.1250    0.0625    0.0313    0.0156    0.0078
         0.0039    0.0020    0.0010    0.0005    0.0002    0.0001
      0.0001    0.0000    0.0000    0.0000    0.0000    0.0000
      0.0000         0    0.0000         0         0
```

There are no discrepancies between the theoretical and experimental conditional probabilities, the conditional probabilities match what we expect from the theoretical values.

(A6) We see the same results for 1-runs as we do for 0-runs, as explained in A5. The conditional probabilities are shown in Listing 2.

Listing 2: Conditional probability of 1-runs

```
>> oneruns_table(3,:)

ans =
```

```
0.5000    0.2500    0.1250    0.0625    0.0312    0.0156    0.0078
    0.0039    0.0020    0.0010    0.0005    0.0002    0.0001
  0.0001    0.0000    0.0000    0.0000    0.0000    0.0000
  0.0000         0    0.0000         0         0
```

There are no discrepancies between the theoretical and experimental conditional probabilities, the conditional probabilities match what we expect from the theoretical values.

Exercise Part (B) - A Simple Stream Cipher

(B1)

(B2)

(B3)

(B4)

(B5)

(B6)