Homework 1

1 - Pinwheel Machine Periods

A pinwheel machine is a machine in which the known-period element is a set of wheels of various sizes, each of which presents a bit on its edge in each position it assumes. At each clock tick, each wheel steps **1** place. On the first wheel, note pins sticking left next to E, F, and G, right next to H and I, then left again next to J.

Suppose a pinwheel machine has n wheels of sizes (number of pins, i.e., bits) l_1 through l_n. Show that the machine has maximal period only if $l_1 ... l_n$ are relatively prime.

More generally, show that the period of the machine is lcm ($l_1 ... l_n$)

Proof:

First we want to prove that the period of the machine is lcm ($l_1 ... l_n$).

Assume that $l_1 \leq l_2 \leq ... \leq l_n$. We know $\sum_{i=1}^{n} \frac{1}{l_i} = 1$ because at each clock tick, each wheel steps 1 place.

Let S be the period of the machine of length m. Then each i must occur exactly $\frac{m}{l_i}$ times in S. Furthermore, successive occurrences of i in S must be exactly l_i slots apart. Lastly, m must be a multiple of lcm ($l_1 ... l_n$). Because each i must occur at least $\lceil \frac{m}{l_i} \rceil$ times in S, we get $m \geq \sum_{i=1}^{n} \lceil \frac{m}{l_i} \rceil$. But $m = m \sum_{i=1}^{n} \frac{1}{l_i} = \sum_{i=1}^{n} \frac{m}{l_i}$. Hence, we get a contradiction if for any i, $\lceil \frac{m}{l_i} \rceil > \frac{m}{l_i}$. Thus each i must occur exactly l_i times in S. As a result, we see that $\frac{m}{l_i}$ must be integral for every i and hence lcm ($l_1 ... l_n$) must divide m.

It follows that m = r lcm ($l_1 ... l_n$). Now divide S into r identical segments, each of size lcm ($l_1 ... l_n$). Consider an arbitrary slot k in the first segment. Suppose this slot contains i. Since the kth slot of the jth segment is the $k + l_i (j \operatorname{lcm}(l_1, ..., l_n)/l_i)^{\text{th}}$ slot of S, which also contains i. Hence, S consists of r identical segments. Therefore, the period of the pinwheel machine is lcm ($l_1 ... l_n$).

Then we prove the machine has maximal period only if $l_1 ... l_n$ are relatively prime, that is, lcm ($l_1 ... l_n$) is maximal only if gcd ($l_1 ... l_n$)=1.

By contrapositive, assume gcd($l_1 ... l_n$)=d>1. Then $l_1 = dr_1$ $l_2 = dr_2$... and $l_n = dr_n$. So $\operatorname{lcm}(l_1 ... l_n) \leq dr_1 r_2 ... r_n < (dr_1)(dr_2)...(dr_n) = l_1 l_2 ... l_n$

Now assume gcd($l_1 ... l_n$)=1. Let

$l_1 = p_1 p_2 ... p_n$

...

$l_n = q_1 q_2 ... q_m$

where p, ..., q are prime and $\forall i, j$ $p_i \neq q_j$, or else $l_1 ... l_n$ would have a common divisor greater than 1. Then, any number divisible by $l_1 ... l_n$ must be of the form: $k(p_1 p_2 ... p_n)...(q_1 q_2 ... q_m)$ for some natural number k. Then, the smallest such number that is still divisble by $l_1 ... l_n$ is when $k = 1$. So, lcm($l_1 ... l_n$)=$l_1 ... l_n$ is maximal only if gcd ($l_1 ... l_n$)=1.

2 - M-109

Consider a pinwheel machine with smaller and fewer wheels than the M-209, say of sizes 18, 17, 15, 13, and 11 for which the pin positions on each wheel are numbered 0 through n-1.

Suppose that the pins on the wheels are set as follows:

- 18: 1, 3, 5, 7, 9, 11, 13, 15, 17
- 17: 0, 1, 2, 3, 4, 5, 6, 7, 8
- 15: 7, 8, 9, 10, 11, 12, 13, 14
- 13: 2, 3, 4, 5, 6, 7, 8
- 11: 0, 2, 3, 5, 10

and that the machines starts (message indicator) in position: 6, 4, 13, 1, 9. That is to say that the first wheel has been rotated six from straight up, etc.

Solution:

According to Problem 1, the period of this machine is lcm(18, 17, 15, 13, 11)=18×17×5×13×11=218790.

$x_0 : 6 mod\ 18 = 6(0)$

$x_1 : 4 mod\ 17 = 4(1)$

$x_2 : 13 mod\ 15 = 13(1)$

$x_3 : 1 mod\ 13 = 1(0)$

$x_4 : 9 mod\ 11 = 9(0)$

The 5-bit number that presents straight up is 01100.

$x_0 : 2^{16} mod\ 18 = 16, (6+16) mod\ 18 = 4(0)$

$x_1 : 2^{16} mod\ 17 = 1, (4+10) mod\ 17 = 5(1)$

$x_2 : 2^{16} mod\ 17 = 1, (13+1) mod\ 15 = 14(1)$

$x_3 : 2^{16} mod\ 13 = 3, (1+3) mod\ 13 = 4(1)$

$x_4 : 2^{16} mod\ 11 = 9, (9+9) mod\ 11 = 7(0)$

The 5-bit number will present after the machine has stepped 2^{16} steps is 01110.

3 - Sigbubba

Consider a Sigaba-like machine, Sigbubba, with has two banks 16-character rotors. The lower bank are the control rotors and the upper bank are the cipher rotors. The lower bank has fifive rotors. These move in an odometer pattern except that wheel 1 (far right) is followed by wheel 3 (center) followed by wheel 5 (far left) followed by wheel 2 (between 1 and 3) and finally wheel 4 (between 3 and 5). (This motion pattern may or may not come up in some future problem.) The upper bank has only four rotors.

Three signals enter at the left end of the control rotors; their positions are selectable. Four groups emerge on the right, each one being the “wire-or” of four emerging wires. Each of these groups will drive one of the cipher rotors.

- What is the expected fraction of the time that each wheel moves?
- What is the expected number of wheels that move at each clock tick?

Solution:

The expected fraction of the time that each wheel moves is:

wheel 1: 1

wheel 3: $1/16$

wheel 5: $1/16^2 = 1/256$

wheel 2: $1/16^3 = 1/4096$

wheel 4: $1/16^4 = 1/65536$

each cipher rotor: $1 - C_{12}^3/C_{16}^3 = 17/28$

The expected number of wheels that move at each clock tick is

$15/16 \times 1 + 1/16 \times 15/16 \times 2 + 1/256 \times 15/16 \times 3 + 1/4096 \times 15/16 \times 4 + 1/65536 \times 5 = 1.067$ when the wheels includes only the control rotors

$1.067 + C_4^1 C_4^1/C_{16}^3 \times 1 + C_4^2 C_2^1 C_4^1 C_4^1/C_{16}^3 \times 2 + C_4^3 C_4^1 C_4^1 C_4^1/C_{16}^3 \times 3 = 3.152$ when the wheels includes the control and cipher rotors

4 - Sigbubba - bis

Since Sigbugga has four cipher rotors, there could be as many as 2^4 possible patters of motion that could occur.

- How many of these patters of motion actually occur?
- For all possible patterns of output from the control rotors, how often does each pattern occur?

Solution:

$C_4^1 + C_4^2 + C_4^3 = 14$ patters of motion actually occur.

1 wheel: $C_4^1/C_{16}^3 = 1/140$

There are A, B, C, D, so the frequency of 1 wheel rotating is $4 \times 1/140 = 1/35$.

2 wheel: $C_2^1 C_4^2 C_4^1/C_{16}^3 = 3/35$

There are AB, AC, AD, BC, BD, CD, so the frequency of 2 wheel rotating is $6 \times 3/35 = 18/35$.

3 wheel: $C_4^1 C_4^1 C_4^1/C_{16}^3 = 4/35$

There are ABC, ACD, BCD, ABD, so the frequency of 3 wheel rotating is $4 \times 4/35 = 16/35$.

5 - Nonlinear FSR

What must the structure of the function *f* be for the shift register to be invertible?

Solution:

An n-bit NLFSR is invertible if and only if its feedback function is of type: $f(x_0, x_1, \ldots, x_{n-1}) = x_0 \oplus g(x_0, x_1, \ldots, x_{n-1})$, where g is a Boolean function of n-1 variables.

Every two consecutive states of an NLFSR overlap in n-1 positions, which implies that each state can have only two possible predecessors and two possible successors. If *f* is in the form $f(x_0, x_1, \ldots, x_{n-1}) = x_0 \oplus g(x_0, x_1, \ldots, x_{n-1})$, then the NLFSR states which correspond to the binary n-tuples $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (\overline{x}_0, x_1, \ldots, x_{n-1})$ always have different successors. The values of $f(x)$ and $f(y)$ depend on the value of $g(x_0, x_1, \ldots, x_{n-1})$ and on the value of x_0. The value of $g(x_0, x_1, \ldots, x_{n-1})$ is the same for x and y. The value of x_0 is different for x and y. Thus, $f(x) \neq f(y)$.