Cryptography Project 2

João Pedro Lourenço (jo1360lo-s)
Group 12

November 2020

Exercise 1

Home

1. $p(x) = x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 + x + 1)$ over F_2, which means that the polynomial is not irreducible, and therefore can't be primitive.

2. $p(x) = x^3 + x + 1 = (x + 2)(x^2 + x + 2)$ over F_3, which means that the polynomial is not irreducible, and therefore can't be primitive.

3. $p(x) = x^2 + \alpha^5 x + 1$ where $\alpha^4 + \alpha + 1 = 0$

   As suggested by the hint, if we can find an i such that $p(\alpha^i) = 0$, then that means that p(x) has a root, and will not be primitive. If we take $i = 6$,

$$\begin{aligned} p(\alpha^6) &= (\alpha^6)^2 + \alpha^5(\alpha^6) + 1 \\ &= \alpha^{12} + \alpha^{11} + 1 \\ &= (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^3 + \alpha^2 + \alpha) + 1 \qquad \text{(according to the table)} \\ &= 2\alpha^3 + 2\alpha^2 + 2\alpha + 2 \\ &= 0 \end{aligned}$$

   Therefore, the polynomial is not primitive, and is reducible.

Laboratory

1. The polynomial is primitive.

```
> Primitive(x^23 + x^5 + 1) mod 2
true
```

2. The polynomial is reducible.

```
> Primitive(x^23 + x^6 + 1) mod 2
false
> Irreduc(x^23 + x^6 + 1) mod 2
false
```

3. The polynomial is irreducible, but not primitive.

```
> Primitive(x^18 + x^3 + 1) mod 2
false

> Irreduc(x^18 + x^3 + 1) mod 2
true
```

4. The polynomial is reducible.

```
> Primitive(x^8 + x^6 + 1) mod 7
false

> Irreduc(x^8 + x^6 + 1) mod 7
false
```

Exercise 2

Home

Since $|F_{2^4}| = 16$, we have to calculate the remainder of each element to the powers of all divisors of $16-1 = 15$ (which are 1, 3, 5 and 15) by $\alpha^4+\alpha+1$. When we find that the remainder is 1, then that power if the order of that element.

1. The order of α is 15.

$$\begin{aligned}\alpha &\equiv \alpha \\ \alpha^3 &\equiv \alpha^3 \\ \alpha^5 &\equiv \alpha(\alpha+1) \\ \alpha^{15} &\equiv 1\end{aligned}$$

2. The order of α^2 is 15.

$$\begin{aligned}\alpha^2 &\equiv \alpha^2 \\ (\alpha^2)^3 &\equiv \alpha^3+\alpha^2 \\ (\alpha^2)^5 &\equiv \alpha^2+\alpha+1 \\ (\alpha^2)^{15} &\equiv 1\end{aligned}$$

3. The order of α^3 is 5.

$$\begin{aligned}\alpha^3 &\equiv \alpha^3 \\ (\alpha^3)^3 &\equiv \alpha^3+\alpha \\ (\alpha^3)^5 &\equiv 1\end{aligned}$$

4. The order of α^5 is 3.

$$(\alpha^5)^3 \equiv \alpha^{15} \equiv 1$$

Laboratory

First, we create a GF with the given parameters and name it G18:

```
> G18 := GF(2, 18, α^18 + α^3 + 1)
G18 := 𝔽_(2^18)
```

Then, we can find the order of the requested elements by converting them into the field, and asking for their order:

1. The order of α is 189.
   ```
   > G18:-order(G18:-ConvertIn(α))
   189
   ```
2. The order of α^2 is 189.
   ```
   > G18:-order(G18:-ConvertIn(α^2))
   189
   ```
3. The order of α^3 is 63.
   ```
   > G18:-order(G18:-ConvertIn(α^3))
   63
   ```
4. The order of $\alpha + \alpha^3$ is 262143.
   ```
   > G18:-order(G18:-ConvertIn(α + α^3))
   262143
   ```

Exercise 3

Home

Cycle set for $p(x) = x^4 + x^2 + 1$

We know that $x^4 + x^2 + 1 = (x^2 + x + 1)^2$. This means that we have $C(D) = C_1(D)^n$, where $C(D) = C_1(D)^2$ and $C_1(D) = 1 + D + D^2$.

We also have:

- $L_1 = \deg C_1(D) = 2$
- $T_1 = 3$ (because $\alpha^0 = 1,\ \alpha^1 = \alpha,\ \alpha^2 = \alpha + 1$ and then $\alpha^3 = 1$ again)
- $T_2 = 2^2 T_1$ (because $C_1(D)$ is irreducible, $p = 2$ is the characteristic of the field, and $m = 2$ satisfies $2^{2-1} < 2 \leq 2^2$)

Finally, using the formula for the cycle set we have:

$$1(1) \oplus \frac{(2^2 - 1)}{3}(3) \oplus \frac{2^2(2^2 - 1)}{6}(6) = 1(1) \oplus 1(3) \oplus 2(6)$$

Cycle set for $p(x) = x^3 + x + 1$

We know that $x^3 + x + 1 = (x + 2)(x^2 + x + 2)$, so we can write:

$$C_1(D) = 2 + D \quad C_2(D) = 2 + D + D^2$$

$$C(D) = C_1(D) \times C_2(D)$$

- The order of $C_1(D)$ is 2, because $1 = (2 + D)(2 + 2D) + D^2$
  - Then, the cycle set for $C_1(D)$ is $1(1) \oplus \frac{2^1-1}{2}(2) = 1(1) \oplus \frac{1}{2}(2)$
- The order of $C_2(D) = 8$ because $1 = (2 + D + D^2)(2 + 2D + D^2 + D^4 + D^5 + 2D^6) + D^8$
  - Then, the cycle set for $C_2(D)$ is $1(1) \oplus \frac{2^2-1}{8}(8) = 1(1) \oplus \frac{3}{8}(8)$

The cycle set for $C(D)$ can be calculated as:

$$[1(1) \oplus \frac{1}{2}(2)] \times [1(1) \oplus \frac{3}{8}(8)] = 1(1) + \frac{3}{8}(8) + \frac{1}{2}(2) + \frac{3}{16}(16)$$

Laboratory

Cycle set for $p(x) = x^{23} + x^5 + 1$

The order of the polynomial can be calculated with the following sequence of commands:

```
> G23 := GF(2, 23, α^23 + α^5 + 1)
G23 := 𝔽_(2^23)

> a := G23:-ConvertIn(α)
a := α mod 2

> G23:-order(a)
8388607
```

We can observe that $2^{23} - 1 = 8388607$, which means that the cycle contains all elements except 0, and can be represented by:

$$1(1) \oplus \frac{2^{23} - 1}{8388607}(8388607) = 1(1) \oplus 1(8388607)$$

Cycle set for $p(x) = x^{23} + x^6 + 1$

This polynomial is not irreducible modulo 2 - therefore, we must find its factors, and then calculate the cycle set for each one and multiply them together.

To find the factors, Maple provides us with the Berlekamp function:

```
> Berlekamp(x^23 + x^6 + 1, x) mod 2
{x^3 + x + 1, x^4 + x^3 + 1, x^16 + x^15 + x^13 + x^12 + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1}
```

To get the cycle set for each factor, we first use the same Maple commands to get the order as for an irreducible polynomial (like done before this subsubsection). The results are below:

- The order of $x^4 + x^3 + 1$ is 15
- The order of $x^3 + x + 1$ is 7
- The order of $x^{16} + x^{15} + x^{13} + x^{12} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$ is 21845

By having the order, calculating the cycle set for each one is a matter of applying the formula:

- The cycle set of $x^4 + x^3 + 1$ is

$$1(1) \oplus \frac{2^4 - 1}{15}(15) = 1(1) \oplus 1(15)$$

- The cycle set of $x^3 + x + 1$ is

$$1(1) \oplus \frac{2^3 - 1}{7}(7) = 1(1) \oplus 1(7)$$

- The cycle set of $x^{16} + x^{15} + x^{13} + x^{12} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$ is

$$1(1) \oplus \frac{2^{16} - 1}{21845}(21845) = 1(1) \oplus 3(21845)$$

Finally, the cycle set for $p(x) = x^{23} + x^6 + 1$ is:

$$\begin{aligned}
&[1(1) \oplus 1(15)] \otimes [1(1) \oplus 1(7)] \otimes [1(1) \oplus 3(21845)] \\
=&[1(1) \oplus 1(7) \oplus 1(15) \oplus 1(105)] \otimes [1(1) \oplus 3(21845)] \\
=&1(1) \oplus 3(21845) \oplus 1(7) \oplus 3(152915) \oplus 1(15) \oplus 3(327675) \oplus 1(105) \oplus 3(2293725)
\end{aligned}$$

Exercise 4

Home

We must choose a polynomial that satisfies p(0) = p(1) = 1, and does not have linear or quadratic factors. For example, $p(x) = x^4 + x + 1$.

Laboratory

We know that any polynomial of degree 4 over F_5 (with constant +1) contains the following properties:

- Evaluates to True in the expression `Primitive(p(x)) mod 5`
- Is of the form $ax^4 + bx^3 + cx^2 + dx + 1$, where the coefficients can range from 0 to 4 (as those are the possible values mod 5)

It's possible to do these checks by hand: however, since there aren't that many possible values, we can also brute-force them in a short time with the following program:

```
for a from 0 to 4 do
 for b from 0 to 4 do
  for c from 0 to 4 do
   for d from 0 to 4 do
    if `mod`(Primitive(a*x^4+b*x^3+c*x^2+d*x+1), 5)
     then print(a, b, c, d, 1)
    end if
   end do
  end do
 end do
end do
```

It's now just a matter of picking one of the given solutions. One of the possible polynomials is $2x^4 + 2x^2 + x + 1$.

Exercise 5

Home

A drawing of the device is found on figure 1. On green (upper most line), you can find the linear part: only the 1st and last entry of the register are considered and XORed together. Below that line, in blue, the circuit is responsible for outputting 1 whenever the register is `[1, 0, 0, 0]`. In this situation, the green circuit also outputs 1, so 1 XOR 1 equals 0, which is the new digit. Finally, whenever all entries are 0, the bottom (orange) circuit outputs 1.

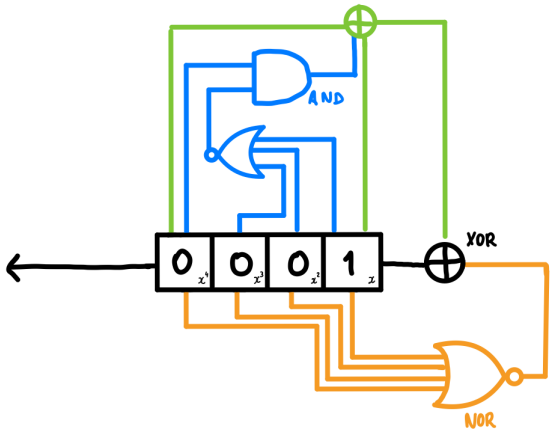

Figure 1: Device that generates a de Bruijn sequence of length 16, with the polynomial x^4+x+1

Laboratory

The generator was implemented in Python. It's quite compact, but it's built to work only for the given sequences (of Z_2 and Z_5).

There are only really 2 parts of interest: the non-linear part, and the mapping function.

Non-linearity

This is achieved by the first 2 checks on the `lfsr` method. The first one is to move out of the all zero state. The second one checks for a specific state to move to the all zero state - on Z_2

it's the state `[1, 0, 0, 0]` and on Z_5 it's the state `[2, 0, 0, 0]`. These states were tested manually until a combination was found that generated a proper de Bruijn sequence.

Mapping function

On Z_2, the sequence generates either 0 or 1. On Z_5, the sequence generates 0, 1, 2, 3 or 4. However, we need a sequence from 0 - 9. This can be achieved one of the ways: either by multiplying the digits from Z_2 by 5 and adding digits from Z_5 (resulting in at most $5 \times 1 + 4 = 9$, and at minimum 0, as we wanted) or by multiplying the digits from Z_5 by 2 and adding digits from Z_2 (resulting in at most $2 \times 4 + 1 = 9$ and at minimum 0, as we wanted). I chose the first approach just because it was first - there was no further consideration.

The program

```
def lfsr(polynomial, register, base):
    if register == [0, 0, 0, 0]:
        register.append(1) # returns to main cycle

    elif ((base == 2 and register == [1, 0, 0, 0]) or
          (base == 5 and register == [2, 0, 0, 0])):
        register.append(0) # goes to all zero register

    else: # linear behaviour
        new_register_value = 0
        for coefficient, content in zip(polynomial, register):
            new_register_value += -coefficient * content

        register.append(new_register_value % base)

    return register.pop(0)

def main():
    register2 = [0, 0, 0, 1]
    register5 = [0, 0, 0, 1]

    z2_polynomial = [1, 0, 0, 1]
    z5_polynomial = [2, 0, 2, 1]

    with open("sequence.txt", "w") as output:
        for _ in range(10003):
            out_z2 = lfsr(z2_polynomial, register2, 2)
            out_z5 = lfsr(z5_polynomial, register5, 5)
            output.write(str((5*out_z2 + out_z5)))

main()
```