# Trabalho Pratico 2 - Cifra A5/1

## Grupo 27

### LCC 2024/2025

Rafaela Antunes Pereira A102527

Gonçalo Gonçalves Barroso A102931

Ricardo Eusebio Cerqueira A102878

## Explicação do problema a)

Considerando a descrição da cifra A5/1, pretende-se definir e codificar, em Z3 e usando o tipo BitVec para modelar a informação, uma FSM que descreva o gerador de chaves.

```
from z3 import *
import random

def declare(i):
    return {
        'LFSR1': BitVec(f'LFSR1{i}', 19),
        'LFSR2': BitVec(f'LFSR2{i}', 22),
        'LFSR3': BitVec(f'LFSR3{i}', 23),
        'keys': BitVec(f'keys_{i}', 64),  # Vetor de 64 bits
        'kepos': BitVec(f'kepos_{i}', 7)


    }

def init(state):
    z0 = random.getrandbits(19)
    z1 = random.getrandbits(22)
    z2 = random.getrandbits(23)

    return And(
        state['LFSR1'] == BitVecVal(z0, 19),
        state['LFSR2'] == BitVecVal(z1, 22),
        state['LFSR3'] == BitVecVal(z2, 23),
        state['keys'] == BitVecVal(0, 64),  # Inicializado com zero
        state['kepos'] == BitVecVal(0, 7)
    )

def avanca(curr, bits_tapped):
    feed_bits = [Extract(i, i, curr) for i in bits_tapped]
    feedback = BitVecVal(0, 1)
```

```
    for bit in feed_bits:
        feedback ^= bit
    LFSR_deslocado = curr >> 1
    feed_deslocado = ZeroExt(curr.size() - 1, feedback) <<
(curr.size() - 1)
    return LFSR_deslocado | feed_deslocado

def maioria_bit(control_1, control_2, control_3):
    return (control_1 & control_2) | (control_1 & control_3) |
(control_2 & control_3)

def trans(curr, prox):
    control_1 = Extract(8, 8, curr['LFSR1'])
    control_2 = Extract(10, 10, curr['LFSR2'])
    control_3 = Extract(10, 10, curr['LFSR3'])
    maioria = maioria_bit(control_1, control_2, control_3)
    bits_tapped1 = [13, 16, 17, 18]
    bits_tapped2 = [20, 21]
    bits_tapped3 = [7, 20, 21, 22]

    next_LFSR1 = If(maioria == control_1, avanca(curr['LFSR1'],
bits_tapped1), curr['LFSR1'])
    next_LFSR2 = If(maioria == control_2, avanca(curr['LFSR2'],
bits_tapped2), curr['LFSR2'])
    next_LFSR3 = If(maioria == control_3, avanca(curr['LFSR3'],
bits_tapped3), curr['LFSR3'])

    new_bit = Extract(0, 0, next_LFSR1) ^ Extract(0, 0, next_LFSR2) ^
Extract(0, 0, next_LFSR3)
    updated_keys = (curr['keys'] << 1) | ZeroExt(63, new_bit)
    updated_pos = curr['kepos'] + 1

    return And(
        prox['LFSR1'] == next_LFSR1,
        prox['LFSR2'] == next_LFSR2,
        prox['LFSR3'] == next_LFSR3,
        prox['keys'] == updated_keys,
        prox['kepos'] == updated_pos,

    )



# (posições que estão a uma distância de no máximo 2 ** (t // 2) de i)

def print_state(i, model, state):
    LFSR1val = model[state['LFSR1']].as_long()
    LFSR2val = model[state['LFSR2']].as_long()
    LFSR3val = model[state['LFSR3']].as_long()
```

```
    keysval = model[state['keys']].as_long()
    posval = model[state['kepos']].as_long()

    print(f"\nEstado {i}:")
    print(f"LFSR 0 - {bin(LFSR1val)[2:].zfill(19)}")
    print(f"LFSR 1 - {bin(LFSR2val)[2:].zfill(22)}")
    print(f"LFSR 2 - {bin(LFSR3val)[2:].zfill(23)}")
    print(f"Output -  {bin(keysval)[2:].zfill(64)}")



def main(declare, init, trans, k, t):
    states = [declare(i) for i in range(k + 1)]
    solver = Solver()
    solver.add(init(states[0]))

    for i in range(k):
        solver.add(trans(states[i], states[i + 1]))
        if solver.check() == sat:
            model = solver.model()
            print_state(i, model, states[i])


# Execução com os parâmetros k e t especificados
print("\nExemplo com k = 64 e t = 4")
k = 64
t = 3
main(declare, init, trans, k, t)

print("\nExemplo com k = 10 e t = 3")
k = 10
t = 3
main(declare, init, trans, k, t)
```

```
Exemplo com k = 64 e t = 4

Estado 0:
LFSR 0 - 0010001011011110101
LFSR 1 - 1001101000110001010100
LFSR 2 - 10110110010110010011100
Output -
0000000000000000000000000000000000000000000000000000000000000000

Estado 1:
LFSR 0 - 0010001011011110101
LFSR 1 - 1100110100011000101010
LFSR 2 - 11011011001011001001110
Output -
```

```
00000000000000000000000000000000000000000000000000000000000000001

Estado 2:
LFSR 0 - 0010001011011110101
LFSR 1 - 11100110100011000010101
LFSR 2 - 11101101100101100100111
Output -
00000000000000000000000000000000000000000000000000000000000000011

Estado 3:
LFSR 0 - 1001000101101111010
LFSR 1 - 11110011010001100010010
LFSR 2 - 11110110110010110010011
Output -
00000000000000000000000000000000000000000000000000000000000000111

Estado 4:
LFSR 0 - 1100100010110111101
LFSR 1 - 11110011010001100010010
LFSR 2 - 11111011011001011001001
Output -
00000000000000000000000000000000000000000000000000000000000001110

Estado 5:
LFSR 0 - 1100100010110111101
LFSR 1 - 11111001101000110001010
LFSR 2 - 11111101101100101100100
Output -
00000000000000000000000000000000000000000000000000000000000011100

Estado 6:
LFSR 0 - 1100100010110111101
LFSR 1 - 11111100110100011000010
LFSR 2 - 11111110110110010110010
Output -
00000000000000000000000000000000000000000000000000000000000111001

Estado 7:
LFSR 0 - 1110010001011011110
LFSR 1 - 11111110011010001100010
LFSR 2 - 11111111011011001011001
Output -
00000000000000000000000000000000000000000000000000000000001110010

Estado 8:
LFSR 0 - 1111001000101101111
LFSR 1 - 11111111001101000110000
LFSR 2 - 11111111011011001011001
Output -
00000000000000000000000000000000000000000000000000000000011100100
```

```
Estado 9:
LFSR 0 - 1111100100010110111
LFSR 1 - 11111111100110100011100
LFSR 2 - 111111111011011001011100
Output -
00000000000000000000000000000000000000000000000000000000111001001

Estado 10:
LFSR 0 - 1111110010001011011
LFSR 1 - 11111111100110100011100
LFSR 2 - 111111111101101100101110
Output -
00000000000000000000000000000000000000000000000000000001110010011

Estado 11:
LFSR 0 - 1111110010001011011
LFSR 1 - 11111111110011010001110
LFSR 2 - 111111111110110110010111
Output -
00000000000000000000000000000000000000000000000000000011100100110

Estado 12:
LFSR 0 - 1111111001000101101
LFSR 1 - 11111111111001101000111
LFSR 2 - 111111111110110110010111
Output -
00000000000000000000000000000000000000000000000000000111001001101

Estado 13:
LFSR 0 - 1111111100100010110
LFSR 1 - 11111111111110011010001
LFSR 2 - 111111111110110110010111
Output -
00000000000000000000000000000000000000000000000000000111001001101

Estado 14:
LFSR 0 - 1111111110010001011
LFSR 1 - 11111111111111001101000
LFSR 2 - 111111111111011011001011
Output -
00000000000000000000000000000000000000000000000000000111001001101

Estado 15:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111001101000
LFSR 2 - 111111111111110110110010
Output -
00000000000000000000000000000000000000000000000000000111001001101
```

```
Estado 16:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111100110100
LFSR 2 - 11111111111111011011001
Output -
00000000000000000000000000000000000000000000000011100100110100010

Estado 17:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111110011010
LFSR 2 - 11111111111111101101100
Output -
00000000000000000000000000000000000000000000000011100100110100101

Estado 18:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111111001101
LFSR 2 - 11111111111111110110110
Output -
00000000000000000000000000000000000000000000000011100100110100101010

Estado 19:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111111100110
LFSR 2 - 11111111111111111011011
Output -
00000000000000000000000000000000000000000000000011100100110100101010100

Estado 20:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111111110011
LFSR 2 - 11111111111111111101101
Output -
00000000000000000000000000000000000000000000000011100100110100101001001

Estado 21:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111111111001
LFSR 2 - 11111111111111111110110
Output -
00000000000000000000000000000000000000000000000011100100110100101001010

Estado 22:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111111111100
LFSR 2 - 11111111111111111111011
Output -
00000000000000000000000000000000000000000000000011100100110100101001001100

Estado 23:
```

```
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111110
LFSR 2 - 11111111111111111111101
Output -
00000000000000000000000000000000000000000011100100110100101001000

Estado 24:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111110
Output -
00000000000000000000000000000000000000000011100100110100101001000010000

Estado 25:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000000000000000000000000011100100110100101001000100001

Estado 26:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000000000000000000000000011100100110100101001000011

Estado 27:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000000000000000000000000011100100110100101001000010000111

Estado 28:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000000000000000000000000011100100110100101001000010000111

Estado 29:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000000000000000000000000011100100110100101001000011111

Estado 30:
LFSR 0 - 1111111111001000101
```

```
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000000000000000000000000000000011100100110100101001000011111

Estado 31:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000000000000000000000000000000011100100110100101001000011111

Estado 32:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000000000000000000000000000000011100100110100101001000011111

Estado 33:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000000000000000000000000000000011100100110100101001000011111

Estado 34:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000000000000000000000000000000011100100110100101001000011111

Estado 35:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000000000000000000000000000000011100100110100101001000011111

Estado 36:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000000000000000000000000000000011100100110100101001000011111

Estado 37:
LFSR 0 - 11111111111001000101
LFSR 1 - 11111111111111111111
```

```
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000000000011100100110100101001000011111111111111

Estado 38:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000000000011100100110100101001000011111111111111

Estado 39:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000000000011100100110100101001000011111111111111

Estado 40:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000000000011100100110100101001000011111111111111

Estado 41:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000000000011100100110100101001000011111111111111

Estado 42:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000000000011100100110100101001000011111111111111

Estado 43:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000000000011100100110100101001000011111111111111

Estado 44:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111111
LFSR 2 - 11111111111111111111111
```

```
Output -
00000000000000000000111001001101001010010000111111111111111111111

Estado 45:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000111001001101001010010000111111111111111111111

Estado 46:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000111001001101001010010000111111111111111111111

Estado 47:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000111001001101001010010000111111111111111111111

Estado 48:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000111001001101001010010000111111111111111111111

Estado 49:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000111001001101001010010000111111111111111111111

Estado 50:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111111
Output -
00000000000000000000111001001101001010010000111111111111111111111

Estado 51:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111111
Output -
```

```
00000000000001110010011010010100100001111111111111111111111111111

Estado 52:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000000000011100100110100101001000011111111111111111111111111111

Estado 53:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000000000111001001101001010010000111111111111111111111111111111

Estado 54:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000000001110010011010010100100001111111111111111111111111111111

Estado 55:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000000011100100110100101001000011111111111111111111111111111111

Estado 56:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000000111001001101001010010000111111111111111111111111111111111

Estado 57:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000001110010011010010100100001111111111111111111111111111111111

Estado 58:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000011100100110100101001000011111111111111111111111111111111111
```

```
Estado 59:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00000111001001101001010010000111111111111111111111111111111111111

Estado 60:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00001110010011010010100100001111111111111111111111111111111111111

Estado 61:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00011100100110100101001000011111111111111111111111111111111111111

Estado 62:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
00111001001101001010010000111111111111111111111111111111111111111

Estado 63:
LFSR 0 - 1111111111001000101
LFSR 1 - 11111111111111111111
LFSR 2 - 11111111111111111111
Output -
01110010011010010100100001111111111111111111111111111111111111111

Exemplo com k = 10 e t = 3

Estado 0:
LFSR 0 - 1001000110101000100
LFSR 1 - 0100101100100111111000
LFSR 2 - 1010100011110100010000
Output -
00000000000000000000000000000000000000000000000000000000000000000

Estado 1:
LFSR 0 - 1001000110101000100
LFSR 1 - 1010010110010011111100
LFSR 2 - 1101010001111010001000
Output -
```

```
00000000000000000000000000000000000000000000000000000000000000000

Estado 2:
LFSR 0 - 1100100011010100010
LFSR 1 - 1101001011001001111110
LFSR 2 - 1110101000111101000 1000
Output -
00000000000000000000000000000000000000000000000000000000000000000

Estado 3:
LFSR 0 - 1110010001101010001
LFSR 1 - 1110100101100100111111
LFSR 2 - 1110101000111101000 1000
Output -
00000000000000000000000000000000000000000000000000000000000000000

Estado 4:
LFSR 0 - 1111001000110101000
LFSR 1 - 1110100101100100111111
LFSR 2 - 1111010100011110100 0100
Output -
00000000000000000000000000000000000000000000000000000000000000001

Estado 5:
LFSR 0 - 1111100100011010100
LFSR 1 - 1110100101100100111111
LFSR 2 - 1111101010001111010 0010
Output -
00000000000000000000000000000000000000000000000000000000000000011

Estado 6:
LFSR 0 - 1111110010001101010
LFSR 1 - 1111010010110010011111
LFSR 2 - 1111101010001111010 0010
Output -
00000000000000000000000000000000000000000000000000000000000000111

Estado 7:
LFSR 0 - 1111110010001101010
LFSR 1 - 1111101001011001001111
LFSR 2 - 1111110101000111101 0001
Output -
00000000000000000000000000000000000000000000000000000000000001110

Estado 8:
LFSR 0 - 1111111001000110101
LFSR 1 - 1111101001011001001111
LFSR 2 - 1111111010100011110 1000
Output -
00000000000000000000000000000000000000000000000000000000000011100
```

```
Estado 9:
LFSR 0 - 1111111100100011010
LFSR 1 - 11111010010110010011111
LFSR 2 - 111111110101000111101000
Output -
00000000000000000000000000000000000000000000000000000000000111001
```