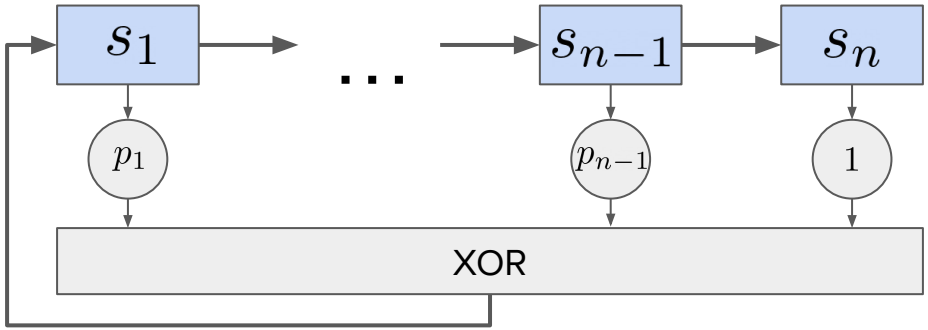
Генерация псевдослучайных чисел

Генератор псевдослучайных чисел

Генератор псевдослучайных чисел (ГПСЧ, PRNG) — алгоритм, порождающий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению

LFSR

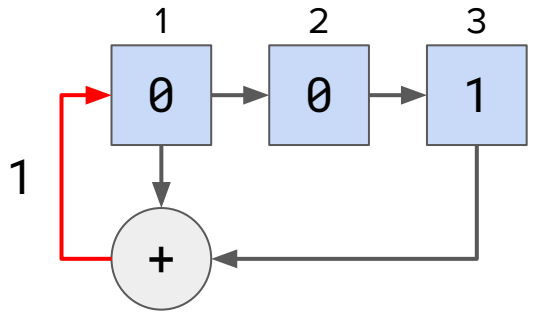
Регистр сдвига с линейной обратной связью (РСЛОС, linear feedback shift register, LFSR)



- Генерирует (2^n-1)-периодическую последовательность, если характеристический многочлен p(x) — примитивный над полем GF(2)
- Можно использовать как генератор псевдослучайных чисел

$$p(x) = x^n + p_{n-1}x^{n-1} + ... + p_1x + 1$$

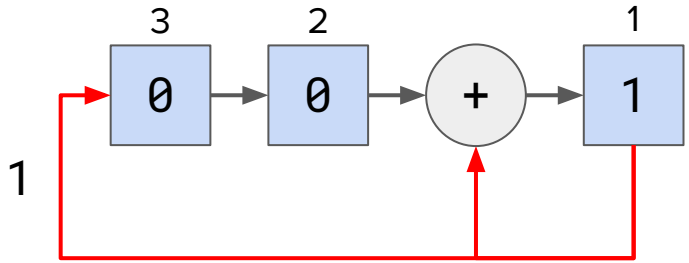
Конфигурация Фибоначчи



$$p(x) = x^3 + x + 1$$

#	1	2	3	OC
0	0	0	1	1
1	1	0	0	1
2	1	1	0	1
3	1	1	1	0
4	0	1	1	1
5	1	0	1	0
6	0	1	0	0
7	0	0	1	1

Конфигурация Галуа

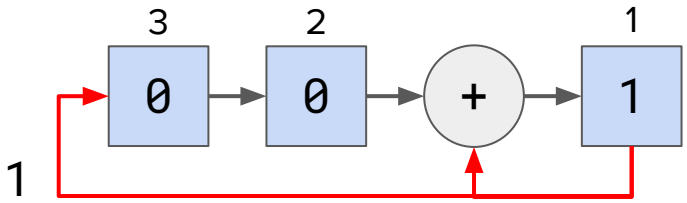


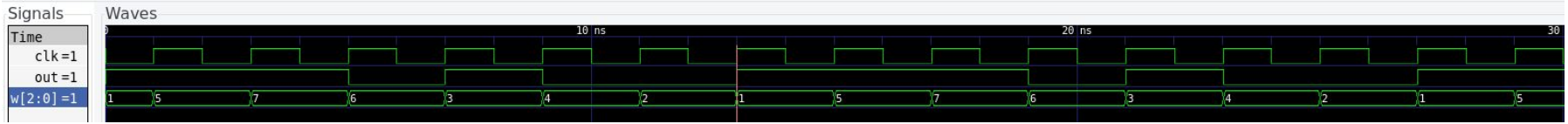
$$p(x) = x^3 + x + 1$$

#	3	2	1	OC
0	0	0	1	1
1	1	0	1	1
2	1	1	1	1
3	1	1	0	0
4	0	1	1	1
5	1	0	0	0
6	0	1	0	0
7	0	0	1	1

lfsr3.v — аппаратная реализация

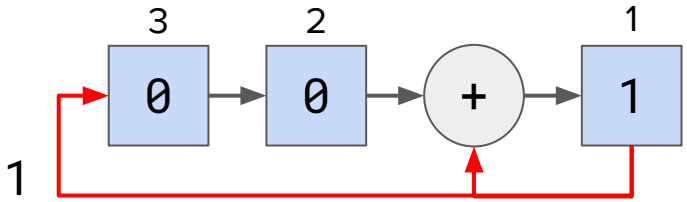
```
module lfsr(
    input clk,

    output reg [2:0]w;
);

initial w = 3'b001;
wire feedback = w[0];

always @(posedge clk) begin
    w[2] <= feedback;
    w[1] <= w[2];
    w[0] <= w[1] ^ feedback;
end

endmodule
```

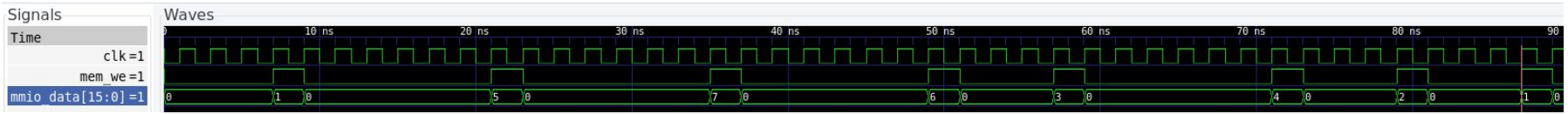




lfsr3.s — программная реализация

```
.text
.globl _start

_start:
    li      t0,   1           ; init LFSR state
    li      a0,   1           ; shifted taps mask
    li      t2,   4           ; w[2] mask

_next:
    sw      t0,   0x20(zero)
    andi    t1,   t0,   1     ; get w[0]
    srli    t0,   t0,   1
    beq     t1,   zero, _next
    xor     t0,   t0,   a0
    or      t0,   t0,   t2    ; w[2] <= 1
    beq     zero, zero, _next
```





Сравнение

	Hard	Soft
Logic Elements	3	1791
Регистры	3	729
Количество тактов	1.00	6.13

GitHub

github.com/viktor-prutyanov/drec-fpga-intro