

А-08-19, Балашов

ЛР 6

1. Определить номер варианта $nv = N \bmod 6 + 1$ (N- номер по списку в группе), и выбрать многочлен для построения РСЛОС из таблицы:

1. Определить номер варианта $nv = N_{\bmod 6} + 1$ (N- номер по списку в группе), и выбрать многочлен для построения РСЛОС из таблицы:

nv	Многочлен	nv	Многочлен
1	$1+x^2+x^5$	4	$1+x+x^2+x^4+x^5$
2	$1+x^3+x^5$	5	$1+x+x^3+x^4+x^5$
3	$1+x+x^2+x^3+x^5$	6	$1+x^2+x^3+x^4+x^5$

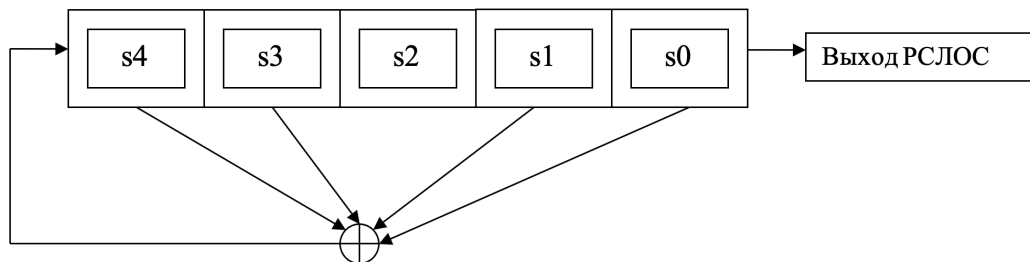
$N=4$; $nv=N \bmod 6 + 1 = 4+1=5$

Многочлен: $1+x+x^3+x^4+x^5$

2. Составить таблицу соответствия степеней многочлена, элементов РСЛОС и коэффициентов обратной связи.

Многочлен	$1*x^5$	$1*x^4$	$1*x^3$	$0*x^2$	$1*x$	1
РСЛОС		s4	s3	s2	s1	s0
Коэффициенты обратной связи		1	1	0	1	1

3. Нарисовать структуру РСЛОС с учетом функции обратной связи.



4. Разработать программный модуль, реализующий работу заданного РСЛОС, провести проверку работоспособности при начальной загрузке 1Fh и получить выходную последовательность длиной $2*(2^5-1)$.

$$2*(2^5-1)=2*(32-1)=2*31=62$$

$$1Fh=1*16+15=31=11111b$$

```

In[143]:= RSLOS[list0_, length0_] := Module[{list = list0, length = length0},
  outlfsr = {};
  Do[outlfsr = Append[outlfsr, list[[5]]];
    list = {Mod[list[[5]] + list[[4]] + list[[2]] + list[[1]], 2},
    list[[1]], list[[2]], list[[3]], list[[4]]}, {i, length}];
  outlfsr
];
list4 = RSLOS[{1, 1, 1, 1, 1}, 2 * (2^5 - 1)]
Length[list4]

```

```

Out[144]= {1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0,
  1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0}

```

```

Out[145]= 62

```

5. Определить “вручную” и программным путем число тактов РСЛОС для достижения состояния 1Eh из начального состояния N.

N=4=0100h=00100h

Определение программным путём:

```

In[146]:= {s4, s3, s2, s1, s0} = {0, 0, 1, 0, 0};
Do[{s4, s3, s2, s1, s0} = {Mod[s0 + s1 + s3 + s4, 2], s4, s3, s2, s1};
  If[{s4, s3, s2, s1, s0} == {1, 1, 1, 1, 0}, {Print["Число тактов: ", i];
    Break[];}], {i, 2^5 - 1}];

```

Число тактов: 7

Определение числа тактов вручную:

6. Сформировать программным путем матрицу m и вектор b, с параметрами n=5 k=N+7 ,для решения системы линейных уравнений $(m \cdot c) \bmod 2 = b$, которая позволяет по 2n элементам последовательности S РСЛОС (см. п.4) определить коэффициенты обратной связи.

```

In[148]:= n = 5;
k = 4 + 7;
list6 = list4[[k ;; k + 2 * n - 1]]

```

```

Out[150]= {1, 1, 1, 0, 0, 0, 0, 1, 1, 0}

```

```

In[151]:= m = Table[0, {n}, {n}];
Do[m[[i]] = list6[[i ;; i + n - 1]], {i, n}];
m // MatrixForm

```

```

Out[153]//MatrixForm=

```

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

```
In[154]:= b = list4[k + n ;; k + 2 * n - 1]
```

```
Out[154]= {0, 0, 1, 1, 0}
```

7. Найти коэффициенты обратной связи {c4,c3,c2,c1,c0} решая следующее матричное уравнение:

Reverse[LinearSolve[m,b,Modulus→2]].

```
In[155]:= Reverse[LinearSolve[m, b, Modulus → 2]]
```

```
Out[155]= {1, 1, 0, 1, 1}
```

8. Проверить линейную сложность, применив алгоритм Берлекэмп-Масси к случайному отрезку последовательности длиной 2n.

```
In[156]:= s = list4[1 ;; 2 * 5];
```

```
Lol = 0; fol = 1;
```

```
diff = 0; Clear[x];
```

```
f = 1;
```

```
L = 0;
```

```
g = CoefficientList[f, {x}];
```

```
Do[If[Mod[Sum[g[[i]] s[[j - 1 - L + i]], 2] == s[[j]], diff = diff + 1,
```

```
Lne = Max[j - L, L]; fne = PolynomialMod[xLne-L f + xLne-Lol-diff-1 fol, 2];
```

```
If[Lne ≠ L, fol = f;
```

```
Lol = L;
```

```
L = Lne;
```

```
diff = 0, diff = diff + 1];
```

```
f = fne;
```

```
g = CoefficientList[f, {x}]]];
```

```
Print["j=", j, ", L=", L, ", f=", f], {j, Length[s]}]
```

```
j=1, L=1, f=1 + x
```

```
j=2, L=1, f=1 + x
```

```
j=3, L=1, f=1 + x
```

```
j=4, L=1, f=1 + x
```

```
j=5, L=1, f=1 + x
```

```
j=6, L=5, f=1 + x4 + x5
```

```
j=7, L=5, f=1 + x4 + x5
```

```
j=8, L=5, f=1 + x2 + x3 + x4 + x5
```

```
j=9, L=5, f=1 + x + x3 + x4 + x5
```

```
j=10, L=5, f=1 + x + x3 + x4 + x5
```

9. На базе трех РСЛОС с номерами вариантов nv, (nv+2)mod6, (nv+4)mod6, сформировать программную реализацию генератора Геффе. Использовать поразрядные логические операторы: BitAnd[], BitNot[], BitXor[]. Получить последовательность в 150 бит.

```

In[160]:= nv = Mod[4, 6] + 1
Out[160]= 5

In[161]:= Mod[nv + 2, 6]
Out[161]= 1

In[162]:= Mod[nv + 4, 6]
Out[162]= 3

In[163]:= RSL0S1 = {}; {s4, s3, s2, s1, s0} = {1, 1, 0, 1, 1};
Do[RSL0S1 = Append[RSL0S1, s0];
  {s4, s3, s2, s1, s0} = {Mod[s0 + s1 + s3 + s4, 2], s4, s3, s2, s1}, {i, 150}];
RSL0S1
Out[165]= {1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1,
  1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1,
  1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1,
  1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0,
  1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0}

In[166]:= RSL0S2 = {}; {s4, s3, s2, s1, s0} = {0, 0, 1, 0, 1};
Do[RSL0S2 = Append[RSL0S2, s0];
  {s4, s3, s2, s1, s0} = {Mod[s0 + s2, 2], s4, s3, s2, s1}, {i, 150}];
RSL0S2
Out[168]= {1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0,
  1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1,
  0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1,
  1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1,
  1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1}

In[169]:= RSL0S3 = {}; {s4, s3, s2, s1, s0} = {0, 1, 1, 1, 1};
Do[RSL0S3 = Append[RSL0S3, s0];
  {s4, s3, s2, s1, s0} = {Mod[s0 + s1 + s2 + s3, 2], s4, s3, s2, s1}, {i, 150}];
RSL0S3
Out[171]= {1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1,
  1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0,
  1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1,
  0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1,
  1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0}

In[172]:= GenGeffe = BitXor[BitAnd[RSL0S1, RSL0S2], BitAnd[BitNot[RSL0S1], RSL0S3]]
Out[172]= {1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0,
  1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1,
  0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1,
  1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1,
  1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0}

```

10. Определить линейную сложность генератора Геффе.

```

In[173]:= s = GenGeffe;
Lol = 0; fol = 1;
diff = 0; Clear[x];
f = 1;
L = 0;
g = CoefficientList[f, {x}];

Do[If[Mod[ $\sum_{i=1}^L g[[i]] s[[j - 1 - L + i]]$ , 2] == s[[j]], diff = diff + 1,

    Lne = Max[j - L, L];          fne = PolynomialMod[xLne-L f + xLne-Lol-diff-1 fol, 2];
    If[Lne ≠ L, fol = f;
        Lol = L;
        L = Lne;
        diff = 0, diff = diff + 1];
    f = fne;
    g = CoefficientList[f, {x}]];

Print["j=", j, ", ", L="L", " ", f="f", f], {j, Length[s]}]

j=1, L=1, f=1 + x
j=2, L=1, f=x
j=3, L=2, f=1 + x2
j=4, L=2, f=1 + x2
j=5, L=3, f=x3
j=6, L=3, f=x3
j=7, L=4, f=1 + x2 + x4
j=8, L=4, f=1 + x2 + x3 + x4
j=9, L=4, f=1 + x2 + x3 + x4
j=10, L=6, f=x2 + x3 + x4 + x5 + x6
j=11, L=6, f=x + x2 + x6
j=12, L=6, f=x + x2 + x6
j=13, L=7, f=1 + x4 + x7
j=14, L=7, f=1 + x4 + x7
j=15, L=8, f=x2 + x5 + x6 + x8
j=16, L=8, f=x2 + x5 + x6 + x8
j=17, L=9, f=1 + x3 + x4 + x6 + x9
j=18, L=9, f=1 + x2 + x3 + x4 + x5 + x8 + x9
j=19, L=9, f=1 + x2 + x3 + x4 + x5 + x8 + x9
j=20, L=11, f=x4 + x7 + x8 + x10 + x11
j=21, L=11, f=x + x3 + x5 + x6 + x7 + x8 + x9 + x11
j=22, L=11, f=1 + x + x2 + x4 + x6 + x7 + x11
j=23, L=11, f=1 + x + x2 + x4 + x6 + x7 + x11
j=24, L=11, f=1 + x + x2 + x4 + x6 + x7 + x11

```

$$\begin{aligned}
j=25, L=14, f &= 1 + x^2 + x^7 + x^8 + x^{10} + x^{14} \\
j=26, L=14, f &= 1 + x^2 + x^7 + x^8 + x^{10} + x^{14} \\
j=27, L=14, f &= 1 + x^2 + x^7 + x^8 + x^{10} + x^{14} \\
j=28, L=14, f &= 1 + x^2 + x^7 + x^8 + x^{10} + x^{14} \\
j=29, L=15, f &= 1 + x^2 + x^3 + x^4 + x^6 + x^7 + x^8 + x^9 + x^{15} \\
j=30, L=15, f &= 1 + x^2 + x^3 + x^4 + x^6 + x^7 + x^8 + x^9 + x^{15} \\
j=31, L=16, f &= 1 + x + x^2 + x^3 + x^4 + x^5 + x^9 + x^{14} + x^{16} \\
j=32, L=16, f &= 1 + x + x^2 + x^3 + x^4 + x^5 + x^9 + x^{14} + x^{16} \\
j=33, L=16, f &= 1 + x + x^2 + x^3 + x^4 + x^5 + x^9 + x^{14} + x^{16} \\
j=34, L=16, f &= 1 + x + x^2 + x^3 + x^4 + x^5 + x^9 + x^{14} + x^{16} \\
j=35, L=16, f &= 1 + x + x^2 + x^3 + x^4 + x^5 + x^9 + x^{14} + x^{16} \\
j=36, L=16, f &= 1 + x + x^2 + x^3 + x^4 + x^5 + x^9 + x^{14} + x^{16} \\
j=37, L=16, f &= 1 + x + x^2 + x^3 + x^4 + x^5 + x^9 + x^{14} + x^{16} \\
j=38, L=22, f &= 1 + x^2 + x^3 + x^4 + x^{10} + x^{11} + x^{20} + x^{22} \\
j=39, L=22, f &= 1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{14} + x^{19} + x^{20} + x^{21} + x^{22} \\
j=40, L=22, f &= 1 + x^2 + x^3 + x^{11} + x^{13} + x^{14} + x^{18} + x^{19} + x^{21} + x^{22} \\
j=41, L=22, f &= 1 + x^2 + x^4 + x^5 + x^6 + x^7 + x^8 + x^{11} + x^{12} + x^{13} + x^{14} + x^{17} + x^{18} + x^{21} + x^{22} \\
j=42, L=22, f &= 1 + x^2 + x^4 + x^5 + x^6 + x^7 + x^8 + x^{11} + x^{12} + x^{13} + x^{14} + x^{17} + x^{18} + x^{21} + x^{22} \\
j=43, L=22, f &= 1 + x^2 + x^4 + x^5 + x^6 + x^7 + x^8 + x^{11} + x^{12} + x^{13} + x^{14} + x^{17} + x^{18} + x^{21} + x^{22} \\
j=44, L=22, f &= x + x^3 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{12} + x^{13} + x^{16} + x^{17} + x^{18} + x^{21} + x^{22} \\
j=45, L=23, f &= 1 + x + x^3 + x^5 + x^7 + x^8 + x^{10} + x^{12} + x^{13} + x^{16} + x^{17} + x^{18} + x^{19} + x^{22} + x^{23} \\
j=46, L=23, f &= 1 + x + x^3 + x^5 + x^7 + x^8 + x^{10} + x^{12} + x^{13} + x^{16} + x^{17} + x^{18} + x^{19} + x^{22} + x^{23} \\
j=47, L=23, f &= 1 + x + x^3 + x^5 + x^7 + x^8 + x^{10} + x^{12} + x^{13} + x^{16} + x^{17} + x^{18} + x^{19} + x^{22} + x^{23} \\
j=48, L=25, f &= x + x^2 + x^5 + x^6 + x^8 + x^{10} + x^{11} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} + x^{19} + x^{20} + x^{22} + x^{24} + x^{25} \\
j=49, L=25, f &= x^4 + x^5 + x^9 + x^{10} + x^{15} + x^{16} + x^{18} + x^{22} + x^{23} + x^{25} \\
j=50, L=25, f &= x^4 + x^5 + x^9 + x^{10} + x^{15} + x^{16} + x^{18} + x^{22} + x^{23} + x^{25} \\
j=51, L=25, f &= x^4 + x^5 + x^9 + x^{10} + x^{15} + x^{16} + x^{18} + x^{22} + x^{23} + x^{25} \\
j=52, L=27, f &= 1 + x + x^3 + x^5 + x^6 + x^8 + x^{10} + x^{11} + x^{13} + x^{16} + x^{19} + x^{20} + x^{22} + x^{23} + x^{24} + x^{25} + x^{27} \\
j=53, L=27, f &= 1 + x + x^3 + x^5 + x^6 + x^8 + x^{10} + x^{11} + x^{13} + x^{16} + x^{19} + x^{20} + x^{22} + x^{23} + x^{24} + x^{25} + x^{27} \\
j=54, L=27, f &= 1 + x + x^3 + x^5 + x^6 + x^8 + x^{10} + x^{11} + x^{13} + x^{16} + x^{19} + x^{20} + x^{22} + x^{23} + x^{24} + x^{25} + x^{27} \\
j=55, L=27, f &= 1 + x + x^3 + x^5 + x^6 + x^8 + x^{10} + x^{11} + x^{13} + x^{16} + x^{19} + x^{20} + x^{22} + x^{23} + x^{24} + x^{25} + x^{27} \\
j=56, L=29, f &= x^2 + x^3 + x^4 + x^7 + x^8 + x^9 + x^{12} + x^{13} + x^{16} + x^{21} + x^{23} + x^{24} + x^{26} + x^{27} + x^{29} \\
j=57, L=29, f &= x + x^3 + x^6 + x^8 + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20} + x^{25} + x^{27} + x^{28} + x^{29} \\
j=58, L=29, f &= x + x^3 + x^6 + x^8 + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20} + x^{25} + x^{27} + x^{28} + x^{29} \\
j=59, L=30, f &= 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + \\
& \quad x^{14} + x^{15} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20} + x^{21} + x^{22} + x^{23} + x^{24} + x^{25} + x^{26} + x^{27} + x^{28} + x^{29} + x^{30} \\
j=60, L=30, f &= 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + \\
& \quad x^{14} + x^{15} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20} + x^{21} + x^{22} + x^{23} + x^{24} + x^{25} + x^{26} + x^{27} + x^{28} + x^{29} + x^{30} \\
j=61, L=30, f &= 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + \\
& \quad x^{14} + x^{15} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20} + x^{21} + x^{22} + x^{23} + x^{24} + x^{25} + x^{26} + x^{27} + x^{28} + x^{29} + x^{30}
\end{aligned}$$

$$j=83, L=30, f=1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}+x^{17}+x^{18}+x^{19}+x^{20}+x^{21}+x^{22}+x^{23}+x^{24}+x^{25}+x^{26}+x^{27}+x^{28}+x^{29}+x^{30}$$

$$j=149, L=30, f=1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20} + x^{21} + x^{22} + x^{23} + x^{24} + x^{25} + x^{26} + x^{27} + x^{28} + x^{29} + x^{30}$$

$$j=150, \quad L=30, \quad f=1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{13}+ \\ x^{14}+x^{15}+x^{16}+x^{17}+x^{18}+x^{19}+x^{20}+x^{21}+x^{22}+x^{23}+x^{24}+x^{25}+x^{26}+x^{27}+x^{28}+x^{29}+x^{30}$$