МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЛОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ И.С. ТУРГЕНЕВА»

Кафедра информационной безопасности

ОТЧЕТ

по лабораторной работе №8

на тему: «**Изучение некоторых свойств линейных последовательных машин»»**

по дисциплине «Информационная безопасность»

Выполнили: Кожухова О.А. Шифр: 170582
Шорин В.Д. Шифр: 171406
Институт приборостроения, автоматизации и информационных технологий
Направление: 09.03.04 «Программная инженерия»
Группа: 71-ПГ
Проверил: Еременко В.Т.
Отметка о зачете:_____

Дата «____» _____ 2021г.

Орел, 2021 г.

Задание

1) Составьте программу генерации выходных последовательностей ЛПМ.
С помощью датчика случайных чисел наработайте входную последовательность u(1), u(2), ... ,u(t) и сохраните ее для дальнейшего использования. Для простоты машинной реализации ограничим размерности векторов u(t), y(t) и s(t) восемью, и будем представлять вектора в байтовом виде.
Постройте таблицы результатов умножения характеристических матриц A=[a1,...,a8], B=[b1,...,bз], c=[c1,...,c8], D=[d1,...,d8] на всевозможные вектора (байты), где ai (bi, ci, di) есть байт, представляющий 1-ю строку матрицы A (B, C. D), 1=1, 2, ... , 8.
Используя заданные матрицы a,b,c,d и входную последовательность из п.2.2, выработайте выходные последовательности для каждого из 255 возможных начальных состояний ЛПМ.
Отсортируйте полученные последовательности и определите число классов эквивалентных состояний ЛПМ.
Повторите задание при другой входной последовательности и сравните полученные результаты.
2) Выработайте выходные последовательности при каждом начальном состоянии ЛПМ и одинаковой входной последовательности.
3) Определите число классов эквивалентных состояний.
4) Повторите пункты 1.2 и 1.3 с другой входной последовательностью, проанализируйте полученные результаты

Ход работы

Вариант № 4

A=[1. 255, 32, 2, 15, 3, 32, 100] B=[12. 45, 56, 13, 127, 214, 1, 11]
C=[14, 230, 200. 6, 9, 3, 101, 201] D=[14, 254, 16, 18, 20, 154, 3, 7]

```
Входная последовательность: 181 230
Выходная последовательность при s0 = 0: 77 124
Выходная последовательность при s0 = 1: 66 226
Выходная последовательность при s0 = 2: 153 135
Выходная последовательность при s0 = 3: 150 25
Выходная последовательность при s0 = 4: 249 41
Выходная последовательность при s0 = 5: 246 183
Выходная последовательность при s0 = 6: 45 210
Выходная последовательность при s0 = 7: 34 76
Выходная последовательность при s0 = 8: 39 80
Выходная последовательность при s0 = 9: 40 206
Выходная последовательность при s0 = 10: 243 171
Выходная последовательность при s0 = 11: 252 53
Выходная последовательность при s0 = 12: 147 5
Выходная последовательность при s0 = 13: 156 155
Выходная последовательность при s0 = 14: 71 254
Выходная последовательность при s0 = 15: 72 96
Выходная последовательность при s0 = 16: 178 175
Выходная последовательность при s0 = 17: 189 49
Выходная последовательность при s0 = 18: 102 84
Выходная последовательность при s0 = 19: 105 202
Выходная последовательность при s0 = 20: 6 250
Выходная последовательность при s0 = 21: 9 100
Выходная последовательность при s0 = 22: 210 1
Выходная последовательность при s0 = 23: 221 159
Выходная последовательность при s0 = 24: 216 131
Выходная последовательность при s0 = 25: 215 29
Выходная последовательность при s0 = 26: 12 120
Выходная последовательность при s0 = 27: 3 230
Выходная последовательность при s0 = 28: 108 214
```

```
Выходная последовательность при s0 = 230: 208 140
Выходная последовательность при s0 = 231: 223 18
Выходная последовательность при s0 = 232: 218 14
Выходная последовательность при s0 = 233: 213 144
Выходная последовательность при s0 = 234: 14 245
Выходная последовательность при s0 = 235: 1 107
Выходная последовательность при s0 = 236: 110 91
Выходная последовательность при s0 = 237: 97 197
Выходная последовательность при s0 = 238: 186 160
Выходная последовательность при s0 = 239: 181 62
Выходная последовательность при s0 = 240: 79 241
Выходная последовательность при s0 = 241: 64 111
Выходная последовательность при s0 = 242: 155 10
Выходная последовательность при s0 = 243: 148 148
Выходная последовательность при s0 = 244: 251 164
Выходная последовательность при s0 = 245: 244 58
Выходная последовательность при s0 = 246: 47 95
Выходная последовательность при s0 = 247: 32 193
Выходная последовательность при s0 = 248: 37 221
Выходная последовательность при s0 = 249: 42 67
Выходная последовательность при s0 = 250: 241 38
Выходная последовательность при s0 = 251: 254 184
Выходная последовательность при s0 = 252: 145 136
Выходная последовательность при s0 = 253: 158 22
Выходная последовательность при s0 = 254: 69 115
Выходная последовательность при s0 = 255: 74 237
Количество классов эквивалентности: 256
```

```
Входная последовательность: 237 22
Выходная последовательность при s0 = 0: 173 80
Выходная последовательность при s0 = 1: 162 206
Выходная последовательность при s0 = 2: 121 171
Выходная последовательность при s0 = 3: 118 53
Выходная последовательность при s0 = 4: 25 5
Выходная последовательность при s0 = 5: 22 155
Выходная последовательность при s0 = 6: 205 254
Выходная последовательность при s0 = 7: 194 96
Выходная последовательность при s0 = 8: 199 124
Выходная последовательность при s0 = 9: 200 226
Выходная последовательность при s0 = 10: 19 135
Выходная последовательность при s0 = 11: 28 25
Выходная последовательность при s0 = 12: 115 41
Выходная последовательность при s0 = 13: 124 183
Выходная последовательность при s0 = 14: 167 210
Выходная последовательность при s0 = 15: 168 76
Выходная последовательность при s0 = 16: 82 131
Выходная последовательность при s0 = 17: 93 29
Выходная последовательность при s0 = 18: 134 120
Выходная последовательность при s0 = 19: 137 230
Выходная последовательность при s0 = 20: 230 214
Выходная последовательность при s0 = 21: 233 72
Выходная последовательность при s0 = 22: 50 45
Выходная последовательность при s0 = 23: 61 179
Выходная последовательность при s0 = 24: 56 175
Выходная последовательность при s0 = 25: 55 49
Выходная последовательность при s0 = 26: 236 84
Выходная последовательность при s0 = 27: 227 202
Выходная последовательность при s0 = 28: 140 250
```

```
Выходная последовательность при s0 = 230: 48 160
Выходная последовательность при s0 = 231: 63 62
Выходная последовательность при s0 = 232: 58 34
Выходная последовательность при s0 = 233: 53 188
Выходная последовательность при s0 = 234: 238 217
Выходная последовательность при s0 = 235: 225 71
Выходная последовательность при s0 = 236: 142 119
Выходная последовательность при s0 = 237: 129 233
Выходная последовательность при s0 = 238: 90 140
Выходная последовательность при s0 = 239: 85 18
Выходная последовательность при s0 = 240: 175 221
Выходная последовательность при s0 = 241: 160 67
Выходная последовательность при s0 = 242: 123 38
Выходная последовательность при s0 = 243: 116 184
Выходная последовательность при s0 = 244: 27 136
Выходная последовательность при s0 = 245: 20 22
Выходная последовательность при s0 = 246: 207 115
Выходная последовательность при s0 = 247: 192 237
Выходная последовательность при s0 = 248: 197 241
Выходная последовательность при s0 = 249: 202 111
Выходная последовательность при s0 = 250: 17 10
Выходная последовательность при s0 = 251: 30 148
Выходная последовательность при s0 = 252: 113 164
Выходная последовательность при s0 = 253: 126 58
Выходная последовательность при s0 = 254: 165 95
Выходная последовательность при s0 = 255: 170 193
Количество классов эквивалентности: 256
```

Код

```
using System;
using System.Collections.Generic;

namespace IS_L_8
{
    class Program
    {
        private static int t = 2;
        private static int n = 8;


        static void Main(string[] args)
        {
            int[] a = new int[] { 1, 255, 32, 2, 15, 3, 32, 100 };
            int[] b = new int[] { 12, 45, 56, 13, 127, 214, 1, 11 };
            int[] c = new int[] { 14, 230, 200, 6, 9, 3, 101, 201 };
            int[] d = new int[] { 14, 254, 16, 18, 20, 154, 3, 7 };


            int[] u = GenerateU(n, t);
            Console.Write("Входная последовательность: ");
            foreach (var item in u)
            {
                Console.Write(item + " ");
            }
            Console.WriteLine();

            Dictionary<int[], int> m0 = new Dictionary<int[], int>();
            for (int i = 0; i < 256; i++)
            {
                int[] answer = Solve(t, i, u, a, b, c, d);

                if (m0.ContainsKey(answer))
                {
                    Console.WriteLine("Contains");
                    m0[answer]++;
                }
                else
                {
                    m0.Add(answer, 0);
                }

                Console.Write($"Выходная последовательность при s0 = {i}: ");
                foreach (var item in answer)
                    Console.Write(item + " ");
                Console.WriteLine();
            }

            Console.WriteLine("Количество классов эквивалентности: " + m0.Count);

        }

        private static int[] Solve(int t, int s0, int[] u, int[] a, int[] b, int[] c,
int[] d)
        {
            int[] s = new int[t + 1];
            s[0] = s0;
            int[] answer = new int[t];

            for (int i = 0; i < t; i++)
            {

                s[i + 1] = T(Foo(
```

```
                            Dot(a, T(new int[] { s[i] }, n), 1),
                            Dot(b, T(new int[] { u[i] }, n), 1),
                            1), 1
                        )[0];

                answer[i] = T(Foo(
                            Dot(c, T(new int[] { s[i] }, n), 1),
                            Dot(d, T(new int[] { u[i] }, n), 1),
                            1), 1
                        )[0];
            }

            return answer;
        }

        private static int[] T(int[] a, int n)
        {
            int[] result = new int[n];
            for (int i = 0; i < a.Length; i++)
                for (int j = 0; j < n; j++)
                    result[j] |= (Get(a[i], j) << i);

            return result;
        }

        private static int[] Foo(int[] a, int[] b, int n)
        {
            int[] result = new int[a.Length];
            for (int i = 0; i < result.Length; i++)
                for (int j = 0; j < n; j++)
                    result[i] |= ((Get(a[i], j) ^ Get(b[i], j)) << j);

            return result;
        }

        private static int[] Dot(int[] a, int[] b, int n)
        {
            int[] result = new int[a.Length];
            for (int i = 0; i < a.Length; i++)
                for (int j = 0; j < n; j++)
                    for (int k = 0; k < b.Length; k++)
                        result[i] ^= ((Get(a[i], k) * Get(b[k], j)) << j);
            return result;
        }

        private static int Get(int a, int i) => ((a & (1 << i)) != 0) ? 0 : 1;

        private static int[] GenerateU(int n, int t)
        {
            int[] result = new int[t];
            Random random = new Random();
            for (int i = 0; i < t; i++)
                result[i] = random.Next(0, 1 << n);
            return result;
        }

    }
}
```