Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №4

з дисципліни

«Криптографія»

на тему: «Побудова регістрів зсуву з лінійним зворотним зв'язком та дослідження їх властивостей»

Виконали:

студенти 3 курсу ФТІ

групи ФБ-72

Топорова Варвара та Лобанова Уляна

Перевірив: _____

Мета роботи :

Ознайомлення з принципами побудови регістрів зсуву з лінійним зворотним зв’язком; практичне освоєння їх програмної реалізації; дослідження властивостей лінійних рекурентних послідовностей та їх залежності від властивостей характеристичного полінома регістра.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

1. Вибрати свій варіант завдання згідно зі списком. Варіанти завдань містяться у файлі Crypto_CP4 LFSR_Var.

2. За даними характеристичними многочленами p1(x), p2(x) скласти лінійні рекурентні співвідношення для ЛРЗ, що задаються цими характеристичними многочленами.

3. Написати програми роботи кожного з ЛРЗ L1 , L2 .

4. За допомогою цих програм згенерувати імпульсні функції для кожного з ЛРЗ і підрахувати їх періоди.

5. За отриманими результатами зробити висновки щодо влавстивостей кожного з характеристичних многочленів p1(x), p2(x): многочлен примітивний над F2 ; не примітивний, але може бути незвідним; звідний.

6. Для кожної з двох імпульсних функцій обчислити розподіл k-грам на періоді, $k \leq ni$, де ni - степінь полінома fi(x), i=1,2 а також значення функції автокореляції A(d) для $0 \leq d \leq 10$. За результатами зробити висновки..

Результати роботи:

P1(X)= X25 + X20 + X19 + X17 + X15 + X14 + X13 + X10 + X8 + X7 + X6 + X3 + 1

Період: 33554431 - примітивний

Автокореляція:

0: 0

1: 16777216

2: 16777216

3: 16777216

4: 16777216

5: 16777216

6: 16777216

7: 16777216

8: 16777216

9: 16777216

10: 16777216

Монограми	Біграми	3-грами	4-грами	5-грами
"0": 16777215 "1": 16777216	"00": 4195309 "01": 4195128 "10": 4191469 "11": 4195309	"000": 1396895 "001": 1397531 "010": 1398583 "011": 1397829 "100": 1400251 "101": 1397542 "110": 1398429 "111": 1397750	"0000": 524164 "0001": 525176 "0010": 524408 "0011": 525027 "0100": 524746 "0101": 524940 "0110": 524247 "0111": 523513 "1000": 522718 "1001": 523589 "1010": 524236 "1011": 523536 "1100": 524905 "1101": 523977 "1110": 524499 "1111": 524926	"00000": 209971 "00001": 209559 "00010": 209307 "00011": 209867 "00100": 209143 "00101": 209360 "00110": 210490 "00111": 209643 "01000": 209611 "01001": 209680 "01010": 209972 "01011": 210064 "01100": 209978 "01101": 209459 "01110": 210690 "01111": 209883 "10000": 209475 "10001": 210034 "10010": 209630 "10011": 210156 "10100": 209585 "10101": 209612 "10110": 210239 "10111": 209582 "11000": 209573 "11001": 209501 "11010": 209480 "11011": 209204 "11100": 209698 "11101": 209357 "11110": 209363 "11111": 209720

P2(X)= X20 + X17 + X15 + X13 + X11 + X10 + X9 + X6 + X4 + X2 + 1

Період: 11275 – незвідний

Автокореляція:

0: 0

1: 5608

2: 5648

3: 5616

4: 5608

5: 5648

6: 5624

7: 5680

8: 5760

9: 5624

10: 5624

Монограми	Біграми	3-грами	4-грами	5-грами
"0": 5595 "1": 5680	"00": 1394 "01": 1369 "10": 1438 "11": 1436	"000": 459 "001": 468 "010": 453 "011": 534 "100": 462 "101": 446 "110": 472 "111": 464	"0000": 171 "0001": 170 "0010": 200 "0011": 168 "0100": 151 "0101": 172 "0110": 183 "0111": 200 "1000": 184 "1001": 156 "1010": 176 "1011": 190 "1100": 179 "1101": 165 "1110": 172 "1111": 181	"00000": 74 "00001": 70 "00010": 67 "00011": 64 "00100": 68 "00101": 63 "00110": 70 "00111": 71 "01000": 79 "01001": 54 "01010": 75 "01011": 60 "01100": 74 "01101": 61 "01110": 80 "01111": 73 "10000": 70 "10001": 57 "10010": 80 "10011": 65 "10100": 69 "10101": 72 "10110": 77 "10111": 66 "11000": 68 "11001": 75 "11010": 70 "11011": 75 "11100": 85 "11101": 64 "11110": 77 "11111": 82

Код програми

```
const fs = require('fs');

const firstPol = [1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0];

const secondPol = [1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0];

const getAutocorr = (result, period, file) => {
    for (let d = 0; d < 11; d ++) {
        let amount = 0;
        for (let i = 0; i < period; i++) {
```

```
            amount += (Number(result[i]) + Number(result[(i + d) % period])) % 2;
        }
        fs.appendFileSync(file, `${d}: ${amount}\n`);
    }
}
const generateNGrams = (n, i = 1, res = [], str = '') => {
    [0, 1].forEach(val => {
        if (i === n) res.push(str + val);
        else generateNGrams(n, i + 1, res, str + val);
    });
    return res;
}
const getNGramsAmount = (result, n, file) => {
    const nGrams = generateNGrams(n);
    nGrams.forEach(ngram => {
        let amount = 0;
        for (let i = 0; i <= result.length - n; i += n) {
            if (result.slice(i, i + n) === ngram) amount ++;
        }
        fs.appendFileSync(file, `"${ngram}": ${amount}\n`);
    });
}
const main = (arr, file) => {
    const start = Array(arr.length);
    start.fill(0, 0, arr.length - 1);
    start[arr.length - 1] = 1;
    startStr = '';
    let endStr = '';
    let period = 0;
    while (startStr !== start.join('')) {
        if (period === 0) startStr = start.join('');
        let sum = 0;
        let odd = 0;
        start.forEach((el, i) => {
            sum += el * arr[i];
```

```
        if (i === 0) odd = el;
        else if (i > 0) start[i - 1] = el;
        if (i === arr.length - 1) start[i] = sum % 2;
      });
      endStr += odd;
      ++ period;
    }
fs.appendFileSync(file, `${endStr}\n\nPeriod: ${period}\n Autocorrelation: \n`);
getAutocorr(endStr, period, file);
fs.appendFileSync(file, 'NGrams: \n');
    for (let i = 1; i < 6; i++) {
      getNGramsAmount(endStr, i, file)
    }
}
fs.appendFileSync('pol1_results.txt', 'FIRST POLYNOM\n\n');
main(firstPol, 'pol1_results.txt');
fs.appendFileSync('pol2_results.txt', 'SECOND POLYNOM\n\n');
main(secondPol, 'pol2_results.txt');
```

Висновок: В даному комп'ютерному практикумі було набуто навичок роботи з лінійними регістрами зсуву, а саме: їх програмна реалізація, дослідження властивостей характеристичного полінома регістра. Окрім цього було досліджено властивості лінійних рекурентних послідовностей.