СПЕЦІАЛЬНІ РОЗДІЛИ

ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №4

Реалізація операцій у скінченних полях характеристики 2

(нормальний базис)

1. Мета роботи

Одержання практичних навичок програмної реалізації обчислень у полі Галуа характеристики 2 в нормальному базисі; ознайомлення з прийомами ефективної реалізації критичних по часу ділянок програмного коду та методами оцінки їх ефективності.

Завдання до комп’ютерного практикуму

А) Перевірити умови існування оптимального нормального базису для розширення (степеня) поля m згідно варіанту. Реалізувати поле Галуа характеристики 2 степеня m в нормальному базисі з операціями:

1) знаходження константи 0 – нейтрального елемента по операції «+»;

2) знаходження константи 1 – нейтрального елемента по операції «□»;

3) додавання елементів;

4) множення елементів;

5) обчислення сліду елементу;

6) піднесення елемента поля до квадрату;

7) піднесення елемента поля до довільного степеня (не вище 2m □ 1 , де m – розмірність розширення);

8) знаходження оберненого елемента за множенням;

9) конвертування (переведення) елемента поля в m -бітний рядок (строкове зображення) і навпаки, де m – розмірність розширення; Мова програмування, семантика функцій, спосіб реалізації можуть обиратись довільно. Під час конвертування елементів поля у бітові рядки потрібно враховувати конвенції щодо зображень елементів поля (зокрема, порядок бітів).

Хід роботи

Написавши бібліотеку для роботи з елементами в поліноміальному базисі, визначеному моїм варіантом проведемо тести для визначення коректності роботи нашої бібліотеки.

Демонстрація роботи.

```python
#!/usr/bin/python3
from compmath.gf import *
from random import getrandbits

def main() -> None:
    fld = GF()
    BITS = fld.m
    print(len(bin(fld.matrix.getBase())[2:]))
    # A,B = getrandbits(BITS),getrandbits(BITS)
    A = 0x2a2d878f41e5c99f64fb7d2497aee5e0d2bc49e98d9abcb08c9599879c12a7e1f330a43b4594f270ef21b4f966c09e5acd06ee8a3
    B = 0x6df2d5505147c6aa31013f32bab48a91f8203f87c0d29f0fda3951f0bc26c73c7b8b81f8e54426219a31d098b7b85447c56afd486
    a,b = fld(A),fld(B)
    print(a,b)
    c = a+ b
    print("a+b",c)
    c = a**2
    print("a**2",c)
    print("trace",a.trace())
    c = a*b
    print("a*b =",bin(c.getBase())[2:].zfill(fld.m))



if __name__ == "__main__":
    main()
```


```
ValueError: 1
gratigo@dedsec
175561
0x2a2d878f41e
a31d098b7b854
a+b 0x47df52d
a**2 0x5516c3
trace 0
a*b = 0100001
0001100000101
0010111011101
gratigo@dedsec
175561
0x2a2d878f41e5c99f64fb7d2497aee5e0d2bc49e98d9abcb08c9599879c12a7e1f330a43b4594f270ef21b4f966c09e5acd06ee8a3 0x6df2d5505147c6aa31013f32bab4
a31d098b7b85447c56afd486
a+b 0x47df52df10a20f3555fa42162d1a6f712a9c766e4d4823bf56acc877203460dd88bb25c3a0d0d45175106461d178ca1d086c13c25
a**2 0x5516c3c7a0f2e4cfb27dbe924bd772f8695e24f4c6cd5e58464accc3ce0953f0f998521da2ca79387790da7cb3604f2d668377451
trace 0
a*b = 0x21216a71f68045fe74ac144d7225ed60e2f0ebdb421fee060abc4d842fee07370cb426cb82779c38aa4fe58a2988c217751813a5f
gratigo@dedsec:~/Documents/term8/SROM/lab4/source$
```