Міністерство освіти і науки України

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

Навчально-науковий Фізико-технічний інститут

Спеціальні розділи обчислювальної математики

Комп’ютерний практикум №3

Реалізація операцій у скінченних полях характеристики 2
(поліноміальний базис)

Виконав:
студент групи ФІ-12
Юрчук Олексій

Київ 2024

Тема: Реалізація операцій у скінченних полях характеристики 2 в поліноміальному базисі

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

Завдання:
А) Реалізувати поле Галуа характеристики 2 степеня m в поліноміальному 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 $2^m - 1$, де m - степінь розширення);
8) знаходження оберненого елемента за множенням;
9) конвертування (переведення) елемента поля в $m -$ бітний рядок (строкове зображення) і навпаки, де m - степінь розширення;
Б) Проконтролювати коректність реалізації поля для кожної операції; наприклад, для декількох a, b, c, d перевірити тотожності
- $(a + b) \cdot c = b \cdot c + a \cdot c$
- $d^{2^{m-1}} = 1, d \neq 0$
В) Визначити середній час виконання операцій у полі. Підрахувати кількість тактів процесора (або інших одиниць виміру часу) на кожну операцію. Результати подати у вигляді таблиць або діаграм.

Теоретичні відомості:

Полем називається множина елементів з двома заданими на ній бінарними операціями, додаванням та множенням (+ та ·, іноді позначаються $\oplus$ та $\otimes$) для яких виконуються умови:

а) щодо операції додавання елементи поля утворюють абелеву групу з нейтральним елементом 0;

б) щодо операції множення всі елементи, окрім 0, також утворюють абелеву групу з нейтральним елементом 1;

в) додавання та множення пов'язані між собою законом дистрибутивності: для будь-яких елементів поля x, y, z виконується $x(y+z) = xy + xz$.

Число елементів поля називається *порядком* поля. Поле називається *скінченним* (або *полем Галуа*), якщо воно має скінченну кількість елементів. Скінченне поле порядку q позначається $GF(q)$ або F_q. Порядок скінченного поля завжди є степенем деякого простого числа, $q = p^m$, число m називається *степенем* поля, а просте число p – його *характеристикою*.

Многочленом $f(t)$ степеня m над полем $GF(p)$ є вираз вигляду

$$f(t) = a_m t^m + a_{m-1} t^{m-1} + \dots + a_1 t + a_0,$$

де коефіцієнти многочлена $a_i \in GF(p)$, $i = 0, \dots m$, а t – змінна, деякий символ, що не належить полю.

- Операції у поліноміальному базисі для поля характеристики 2

А) Додавання

2.2.1. Додавання у поліноміальному базисі

Додавання у $GF(2^m)$ є звичайним додаванням поліномів над $GF(2)$, що відповідає покомпонентному додаванню за модулем 2 відповідних векторів.

Б) Множення

2.2.2. Множення у поліноміальному базисі

При множенні елементів $GF(2^m)$ відповідні їм многочлени перемножуються, з наступним зведенням результату за модулем незвідного многочлена $f(t)$, який використовується для побудови $GF(2^m)$ як розширення $GF(2)$.

В) Піднесення до квадрату

2.2.3. Піднесення до квадрату в поліноміальному базисі

Піднесення елементу поля $GF(2^m)$ до квадрату можна зробити як звичайне множення цього елементу сам на себе. Втім, із використанням властивості лінійності піднесення до квадрату, можна зробити цю операцію більш ефективно.

Нехай дано елемент $a \in GF(2^m)$:

$$a = (a_m, a_{m-1}, \dots, a_1, a_0) = a_m t^m + a_{m-1} t^{m-1} + \dots + a_1 t + a_0;$$

тоді його квадрат буде виглядати таким чином:

$$a = (a_m t^m + a_{m-1} t^{m-1} + \dots + a_1 t + a_0)^2 \bmod f(t) = a_m t^{2m} + a_{m-1} t^{2m-2} + \dots + a_1 t^2 + a_0 \bmod f(t),$$

або, в бітовому записі,

$$a^2 = (a_m, 0, a_{m-1}, 0, \dots, a_1, 0 a_0) \bmod f(t).$$

Отже, для того, щоб обчислити квадрат елементу a, треба виконати такі дії:

1) «Прорідити» бітовий запис, вставляючи 0 після кожного біту, окрім останнього.

2) Отриманий бітовий вектор довжини $2m+1$ біт представити як поліном та звести за модулем $f(t)$

Г) Знаходження оберненого в поліноміальному базисі

2.2.4. Знаходження оберненого елемента поліноміальному базисі

Обернений елемент до a ($a \neq 0$) можна знайти як a^{2^m-2}. Обчислення правої частини цієї формули ефективно виконується за схемою Горнера: оскільки $2^m - 2 = 2^{m-1} + 2^{m-2} + \dots + 2$, то $a^{-1} = a^{2^{m-1}} a^{2^{m-2}} \dots a^2 = (a^{2^{m-2}} a^{2^{m-3}} \dots a^{2^0})^2$.

Більш швидкий спосіб: за допомогою розширеного алгоритму Евкліда знайти поліном, обернений до поліному a за модулем $f(x)$.

Хід роботи

Введені числа:

a = 15795109c9b0e4f4f2f6ef8b1cbadc4adadaefcafff

b = 0edf130b2a5bf30a816c4131bcdb4523caef5480134

c = 16cdef39cbdb4523caef5480134edf130b2a5bf30a8

d = fffffffffffffffffffffffffffffffffffffffffff

Перевірка властивостей:

```
Checking the properties:
First property:          (a+b)*c = a*c + b*c
9a2e393489ddad544749908895d531b0200f9aecbab

9a2e393489ddad544749908895d531b0200f9aecbab

Second property:         a^(2^(m-1)) = 1
1
```

Результат НСД, НСК багаторозрядних чисел:

```
GCD is: 3
LCM is: 1b3b7bb3ebd114baf6b59dee004b95098772ee5e8fe9fb4cbb040580118a1d21cb7b88689b52340fa2a05d9784cf8cd382ef3d59e76d7ae2
a2d6590a8cbe54b16ba09e2c6e7f70f641c294a9feec4bc732c1755184ce48107e18a0f803e19da154a380a6b30d63d11f727bb3d77426ec7e555d40
4a2f0265de02040359346072b4a67c3c4da8697cf455ed39c4ba4e6f4da760468cf8e980ee
```

Результат додавання, множення, піднесення до степеню за модулем незвідного полінома, знаходження сліду та оберненого елемента в полі:

```
SUM:    1ba64202e3eb17fe739aaebaa06199691035bb4aecb

Multiply:       16bf4d1480b322c2c0ba0e09893eb2478203f25473c4

Square: 175956754bdd74756db6d283cb386b0578820b84b43c

Degree: 8869a1383b9e2b5a490acf6b6502cfc32b24f5da3db

Trace:  1

Inverse to a:   18ff177548ba2dd77bb8ce7a76208576513607b8b19b
```

Усі операції працюють коректно, перевірено за допомогою TestL2.exe

Також було виміряно середній час виконання кожної зазначеної операції, на 10 запусках, та відповідна кількість тактів процесора, результати були згруповані у таблицю:

Операція	Середній час виконання (секунди)	Кількість тактів процесора
Додавання	4.2e-07	546
Множення	0.00085179	1107327
Піднесення в квадрат	0.00116171	1510223
Піднесення до степеня	0.220815	287059500
Слід	0.153059	198976700
Обернений	0.298032	387441600

Кількість тактів процесора обрахована за формулою:
кількість тактів = час виконання (секунди) * тактова частота (Гц)
Тактова частота комп'ютера: 1,30ГГц, тобто 1300000000Гц

Додатки:

Увесь код можна знайти за посиланням, на GitHub:
https://github.com/MansteinOrGuderian/SpRzOM-3