СПЕЦІАЛЬНІ РОЗДІЛИ ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Реалізація операцій у скінченних полях характеристики 2 (поліноміальний базис)

1. Мета роботи

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.

2. Теоретичні відомості

2.1. Деякі відомості про скінченні поля

Полем називається множина елементів з двома заданими на ній бінарними операціями, додаванням та множенням (+ та ·, інколи 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*.

Абелева група ненульових елементів поля з операцією множення називається *мультиплікативною групою поля* (позначається $GF^*(q)$ або F_q^*) Мультиплікативна група скінченного поля є циклічною групою порядку p^m-1, її твірний елемент (або генератор) називається *примітивним* елементом поля.

Скінченне поле степеня 1 називається *простим*. Просте скінченне поле можна ототожнити з множиною класів лишків за модулем числа p з операціями додавання та множення за модулем p. Наприклад, скінченне поле $GF(2)$ складається з двох елементів 0 і 1. У цьому полі операції додавання й множення виконуються наступним чином: 0+0=0, 0+1=1+0=1, 1+1=0, 0·0=1·0=0·1=0, 1·1=1, тобто за модулем 2.

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

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

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

Операції над такими многочленами виконуються як операції над звичайними многочленами, тільки операції над коефіцієнтами здійснюються в полі $GF(p)$. Зокрема, многочлен $g(t)$ ділиться з залишком $r(t)$ на многочлен $f(t)$, $f(t) \neq 0$, якщо $g(t) = h(t)f(t) + r(t)$, де степінь многочлена $r(t)$ менша за степінь многочлена $f(t)$. Операція обчислення залишку від ділення многочлена $g(t)$ на многочлен $f(t)$ називається *зведенням* (або *редукцією*) многочлена $g(t)$ за модулем $f(t)$, а залишок $r(t)$ позначається $g(t) \bmod f(t)$. Якщо $r(t) \equiv 0$, то многочлен $g(t)$ ділиться на многочлен $f(t)$ без залишку.

Многочлен $f(t)$ ненульового степеня називається *незвідним* над полем $GF(p)$, якщо він ділиться без залишку над цим полем тільки на самого себе і на многочлени нульового степеня. Елемент x скінченного поля $GF(p^m)$ називається коренем многочлена $f(t)$, якщо $f(x) = 0$. Незвідний многочлен $f(t)$ називається *примітивним*, якщо його корені є примітивними елементами поля.

Будь-яке скінченне поле $GF(p^m)$ є m-вимірним векторним простором над полем $GF(p)$.

Якщо x – корінь незвідного многочлена $f(t)$ степеня m над $GF(p)$, то елементи $\{x^{m-1}, \ldots, x, 1\}$ утворюють *базис* скінченного поля $GF(p^m)$ як векторного простору над полем $GF(p)$. Цей базис називається *поліноміальним*. Будь-який елемент основного поля однозначно виражається через елементи поліноміального базису. Найзручніше поліноміальний базис задавати примітивним многочленом $f(t)$ степеня m. Тоді елементи поля задаються многочленами степеня не вище $m-1$, їх сума задається сумою цих многочленів, а добуток – добутком цих многочленів по модулю $f(t)$.

Для будь-яких елементів x, y скінченного поля $GF(p^m)$ мають місце рівності:

$$x^{p^m} = x, \ \ (x+y)^p = x^p + y^p.$$

Таким чином, операція піднесення до степеня p у полі $GF(p^m)$ лінійна над $GF(p)$:

$$(ax+by)^p = ax^p + by^p,$$

для довільних $a, b \in GF(p)$, $x, y \in GF(p^m)$.

2.2. Виконання операцій у поліноміальному базисі полів характеристики 2

У поліноміальному зображенні елементи поля $GF(2^m)$ являють собою многочлени степеня, що не перевищує $m-1$, над $GF(2)$. Елементи $GF(2^m)$ зображуються двійковими векторами, що відповідають їх розкладу за базисними елементами (тобто, коефіцієнтам відповідного полінома), причому крайній лівий розряд зображення елемента поля відповідає степеню x^{2^m-1}, а крайній правий – степеню x^0; таким чином, елемент 1 має зображення $(0,0,0,...,0,1)$ або просто 0000…01, а елемент x – зображення $(0,0,0,...,1,0)$ або 0000…010.

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.

2.2.2. Множення у поліноміальному базисі

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

2.2.3. Піднесення до квадрату в поліноміальному базисі

Піднесення елементу поля $GF\left(2^m\right)$ 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 $a \in GF\left(2^m\right)$:

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

тоді його квадрат буде виглядати таким чином:

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

або, в бітовому записі,

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

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 $f(t)$

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 $2^m - 2 = 2^{m-1} + 2^{m-2} + ... + 2$, то $a^{-1} = a^{2^{m-1}} a^{2^{m-2}} ... a^2 = (a^{2^{m-2}} a^{2^{m-3}} ... a^{2^0})^2$.

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

2.2.5. Приклади

Розглянемо поле $GF\left(2^3\right)$, для побудови якого використаємо примітивний многочлен 3-го степеня $f(x) = x^3 + x + 1$.

Елементами $GF\left(2^3\right)$ є поліноми 0, 1, *x*, $x+1$, x^2, x^2+1, x^2+x, x^2+x+1 або, інакше, відповідні їм вектори (000), (001), (010), (011), (100), (101), (110), (111).

Приклад додавання:

$(011) + (101) = (110)$.

Приклад множення:

$(011) \cdot (101) = (x+1)(x^2+1) \bmod f(x) = (x^3 + x^2 + x + 1) \bmod (x^3 + x + 1) = x^2 = (100)$.

Приклад піднесення до квадрату:

$(101)^2 = (10001) \bmod f(x) = (x^4 + 1) \bmod f(x) = x^2 + x + 1 = (111)$.

3. Завдання до комп'ютерного практикуму

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 – 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).

Варіанти завдань

Номер варіанта	***m* (розмірність поля)**	$p(x)$ **(генератор поля)**
1	163	$p(x) = x^{163} + x^7 + x^6 + x^3 + 1$
2	173	$p(x) = x^{173} + x^{10} + x^2 + x + 1$
3	179	$p(x) = x^{179} + x^4 + x^2 + x + 1$
4	191	$p(x) = x^{191} + x^9 + 1$
5	233	$p(x) = x^{233} + x^9 + x^4 + x + 1$
6	239	$p(x) = x^{239} + x^{15} + x^2 + x + 1$
7	251	$p(x) = x^{251} + x^{14} + x^4 + x + 1$
8	281	$p(x) = x^{281} + x^9 + x^4 + x + 1$
9	283	$p(x) = x^{283} + x^{26} + x^9 + x + 1$
10	293	$p(x) = x^{293} + x^{11} + x^6 + x + 1$
11	359	$p(x) = x^{359} + x^{18} + x^4 + x^2 + 1$
12	409	$p(x) = x^{409} + x^{15} + x^6 + x + 1$
13	419	$p(x) = x^{419} + x^{21} + x^{14} + x + 1$
14	431	$p(x) = x^{431} + x^5 + x^3 + x + 1$
15	443	$p(x) = x^{443} + x^{28} + x^3 + x + 1$
16	491	$p(x) = x^{491} + x^{17} + x^6 + x^2 + 1$
17	509	$p(x) = x^{509} + x^{23} + x^3 + x^2 + 1$
18	571	$p(x) = x^{571} + x^{10} + x^5 + x^2 + 1$

Б) Проконтролювати коректність реалізації поля для кожної операції; наприклад, для декількох a, b, c, d перевірити тотожності $(a+b)\cdot c = b\cdot c + c\cdot a$, $d^{2^m - 1} = 1$ ($d \neq 0$) та ін.

Додатково можна запропонувати свої тести на коректність.

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.

Примітка: роботи приймаються до здачі незалежно від швидкодії програми (адже правильна повільна програма є незрівнянно кращою, ніж неправильна, але швидка!)

Продемонструвати працюючу програму викладачеві (бажано компілювати на місці, щоб була можливість змінювати програму)

4. Оформлення звіту

Звіт оформлюється відповідно до стандартних правил оформлення наукових робіт. Звіт має містити:

1) мету, теоретичну частину та завдання, наведені вище;
2) бітові зображення тестових елементів та результатів операцій над ними;
3) бітові зображення результатів контролю за пунктом Б);
4) аналітичні відомості за пунктом В)
5) текст програми (у додатку)

Також текст програми передається викладачеві в електронному вигляді.

5. Оцінювання лабораторної роботи

За виконання лабораторної роботи студент може одержати до 15 рейтингових балів; зокрема, оцінюються такі позиції:

– реалізація основного завдання – до 8-ти балів;
– виконання аналітичного завдання (за пунктом В) – до 4-х балів;
– оформлення звіту – 2 бали;
– своєчасне виконання завдання – 1 бал;
– несвоєчасне виконання роботи – (-1) бал за кожні два тижні пропуску.

6. Контрольні питання

1. Які представлення елементів скінченного поля використовуються для визначення операцій над ними? Опишіть представлення у вигляді лінійного векторного простору, поліномів, степенів генератору поля.
2. Що таке поліноміальний базис скінченного поля?
3. Як виконуються додавання, множення, піднесення до степеню, пошук оберненого елементу у поліноміальному базисі?
4. Які переваги та недоліки реалізації поля в поліноміальному базисі?
5. Опишіть алгоритм пошуку оберненого елементу за допомогою алгоритму Евкліда. Яка його складність?
6. Опишіть метод Карацуби для множення двох елементів поля. В чому його відмінності від алгоритму для множення двох великих чисел?

7. Література

1. *Лидл Р., Нидеррайтер Г.,* Конечные поля, т. 1, 2 – М.: Мир, 1998
2. *Бессалов А. В., Телиженко А.Б.* Криптосистемы на эллиптических кривых: учеб. пособие. – Київ, «Політехніка», 2004. - 224 с.
3. *Болотов А.А, Гашков С.Б., Фролов А.Б., Часовских А.А.* Алгоритмические основы современной криптографии. – М.: МЭИ, 2000 – 112 с.
4. *Державний стандарт України.* Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. ДСТУ 4145. Київ, Держстандарт України, 2003.
5. Standards for Efficient Cryptography (SEC) 1: Elliptic Curve Cryptography, version 2.0 (May 21, 2009).
6. Standards for Efficient Cryptography (SEC) 2: Recommended Elliptic Curve Domain Parameters, version 2.0 (January 27, 2010).