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.

2. Теоретичні відомості

2.1. Нормальні базиси скінченних полів характеристики 2

Розглянемо скінченне поле $GF(p^m)$. Якщо x – такий елемент поля $GF(p^m)$, що елементи $\{x, x^p, x^{p^2}, \ldots, x^{p^{m-1}}\}$ лінійно незалежні над $GF(p)$, то ці елементи утворюють базис поля $GF(p^m)$, який називається *нормальним*. Доведено, що нормальний базис існує для довільного скінченного поля.

У полях $GF(2^m)$ для багатьох значень m існує *гаусівський оптимальний нормальний базис* (він є частковим випадком нормального базису). Ми будемо розглядати (згідно ДСТУ 4145-2002) поля, які мають гаусівський оптимальний нормальний базис другого типу, що має місце, якщо число $p = 2m+1$ просте і для найменшого натурального числа k, такого, що $2^k \equiv 1 (\mathrm{mod}\ p)$, виконується одна з наступних умов:

а) $k = 2m$;

б) $p \equiv 3 (\mathrm{mod}\ 4)$ і $k = m$.

Надалі гаусівський оптимальний нормальний базис типу 2 будемо називати просто *оптимальним нормальним базисом (**ОНБ**).*

Наприклад, у $GF(2^3)$ існує ОНБ, бо число 3 задовольняє наведеним вище умовам: по перше, число $p = 2 \cdot 3 + 1 = 7$ – просте, по-друге, оскільки $p \equiv 3 (\mathrm{mod}\ 4)$, то 3 – дійсно найменше натуральне k, для якого $2^k \equiv 1 (\mathrm{mod}\ 7)$ (пункт б)).

Елементи оптимального нормального базису $GF(2^m)$ є коренями деякого незвідного многочлена $p_m(t)$, що називається *нормальним многочленом* даного скінченного поля і будується за рекурсивною формулою:

$$p_0(t) = 1,\ p_1(t) = t + 1,$$
$$p_{i+1}(t) = t \cdot p_i(t) + p_{i-1}(t),\ i = 1, 2, \ldots, m-1.$$

Для $GF(2^3)$ маємо $p_3(t) = t^3 + t^2 + 1$, і ОНБ має вигляд x, x^2, x^4, де x – корінь $p_3(t)$.

Елементи $GF(2^m)$ зображуються двійковими векторами, що відповідають їх розкладу за базисними елементами, причому крайній лівий розряд зображення елемента поля відповідає

елементу базису x, а крайній правий – елементу $x^{2^{m-1}}$ (зверніть увагу, що, на відміну від поліноміального базису, в даному представленні коефіцієнти лічаться від молодших степенів до старших). Одиниці поля у оптимальному нормальному базисі відповідає зображення $(1,1,1,...,1)$.

2.2. Виконання операцій у оптимальному нормальному базисі

2.2.1. Додавання в ОНБ

Додавання в ОНБ виконується так само, як і в поліноміальному базисі – покомпонентно (побітово).

2.2.2. Піднесення до квадрату в ОНБ

Перевага використання оптимального нормального базису особливо відчутна при виконанні операції піднесення до квадрата. Дійсно, для довільного елемента $y=\sum_{i=0}^{m-1} y_i x^{2^i} = (y_0,...,y_{m-1})_{NB} \in GF(2^m)$ з того, що $y_i \in GF(2)$ та лінійності операції піднесення до квадрата у полі характеристики 2 випливає, що

$$y^2 = \left(\sum_{i=0}^{m-1} y_i x^{2^i}\right)^2 = \sum_{i=0}^{m-1}\left(y_i x^{2^i}\right)^2 = \sum_{i=0}^{m-1} y_i x^{2^{i+1}} = (y_{m-1}, y_0, ..., y_{m-2}),$$

$$\text{або } y^2 = (y >>> 1),$$

де $>>>$ – циклічний зсув вправо

Отже, піднесення до квадрата в оптимальному нормальному базисі зводиться до циклічного зсуву вправо компонент векторного зображення елемента.

2.2.3. Обчислення сліду елементу в ОНБ

Іншою операцією, яка ефективно виконується в ОБН, є обчислення сліду елементу. Дійсно, розглянемо елемент $y=(y_0,...,y_{m-1})_{NB} \in GF(2^m)$; тоді $tr(y) = y + y^2 + y^4 + ... + y^{2^{m-1}}$. Однак з п. 2.2 маємо:

$y = (y_0, y_1, y_2, ..., y_{m-1})$,

$y^2 = (y_{m-1}, y_0, y_1, ..., y_{m-2})$,

$y^4 = (y_{m-2}, y_{m-1}, y_0, ..., y_{m-3})$,

…

$y^{2^{m-1}} = (y_1, y_2, y_3, ..., y_{m-1}, y_0)$.

Звідси випливає, що $tr(y) = (c, c, ..., c)_{NB}$, де $c = y_0 + y_1 + ... + y_{m-1}$ (додавання виконується в полі $GF(2)$). Оскільки $(0, 0, 0, ..., 0)$ є зображенням нуля, а $(1,1,1,...,1)$ – зображенням одиниці в нормальному базисі, остаточно маємо:

$$tr(y) = y_0 + y_1 + ... + y_{m-1}.$$

Таким чином, слід елементу дорівнює сумі коефіцієнтів його представлення у нормальному базисі.

2.2.4. Множення в ОНБ

Добуток $z = u \cdot v$ елементів $u = (u_0, u_1, ..., u_{m-1})$ та $v = (v_0, v_1, ..., v_{m-1})$ в ОНБ обчислюється за формулою

$$z_i = (u <<< i) \cdot \Lambda \cdot (v <<< i)^{\mathrm{T}} =$$
$$= (u_i, u_{i+1}, ..., u_{m-1}, u_{0,}, u_1, ..., u_{i-1}) \cdot \Lambda \cdot (v_i, v_{i+1}, ..., v_{m-1}, v_{0,}, v_1, ..., v_{i-1})^{\mathrm{T}},$$

де $<<< i$ позначає циклічний зсув вліво на i компонент,

$^{\mathrm{T}}$ – знак транспонування,

Λ – мультиплікативна матриця розмірності m на m,

$z = (z_0, z_1, ..., z_{m-1})$.

Складність множення визначається числом ненульових елементів у матриці Λ (як її обчислювати, написано в п. 2.5). В загальному випадку в цій матриці не менше $2m-1$ ненульових елементів. Якщо нормальний базис є оптимальним, то ненульових елементів рівно $2m-1$ (власне, з цієї причини такий базис і називається оптимальним). Повільні програмні реалізації (як ця лабораторна робота ☺) можуть оптимальність базису і не використовувати, а рахувати $u\Lambda v^T$ «в лоб».

2.2.5. Знаходження мультиплікативної матриці в ОНБ

Мультиплікативна матриця Λ складається з рядків, які є розкладом в ОНБ m добутків елементів базису вигляду $x \cdot x^{2^j}$, $j = 0, \ldots, m-1$, тобто

$$\Lambda = \begin{bmatrix} x \cdot x \\ \cdots \\ x \cdot x^{2^j} \\ \cdots \\ x \cdot x^{2^{m-1}} \end{bmatrix}$$

Доведено, що матриця Λ не залежить від вибору ОНБ (бо він єдиний з точністю до циклічного зсуву).

Виявилося, що можна зовсім позбавитися від мови теорії скінченних полів і обчислювати мультиплікативну матрицю в ОНБ за такою простою формулою:

$\lambda_{i,j} = 1$, якщо виконується одна з таких умов: $\begin{bmatrix} 2^i + 2^j \equiv 1 \bmod p \\ 2^i - 2^j \equiv 1 \bmod p \\ -2^i + 2^j \equiv 1 \bmod p \\ -2^i - 2^j \equiv 1 \bmod p \end{bmatrix}$,

$\lambda_{i,j} = 0$ в усіх інших випадках,

де $p = 2m+1$, $0 \le i, j \le m-1$. Тепер все, що потрібно – це знати $2^i \bmod p$ для $0 \le i \le m-1$.

Приклад

В полі $GF(2^3)$ маємо $\Lambda = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$.

Якщо $u=(011)$, $v=(101)$ – розклад елементів u, v поля $GF\left(2^3\right)$ за оптимальним нормальним базисом, то компоненти розкладу добутку $z=u\cdot v$ обчислюються як

$$z_0=(011)\cdot\Lambda\cdot(101)^T=1,$$
$$z_1=(110)\cdot\Lambda\cdot(011)^T=0,$$
$$z_2=(101)\cdot\Lambda\cdot(110)^T=0.$$

Отже, $u\cdot v=(011)\cdot(101)=(100)$.

2.2.6. Знаходження оберненого елемента в ОНБ

Обернений елемент в оптимальному нормальному базисі також можна знайти за формулою $y^{-1}=y^{2^m-2}$, $y\neq 0$, або за допомогою алгоритму Евкліда. Втім, для ОНБ був розроблений спеціальний алгоритм пошуку оберненого елементу, що використовує багато возведень до квадрату та порівняно малу кількість множень – це так званий алгоритм Ітo-Цудзії.

3. 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 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)**	**Номер варіанта**	***m* (розмірність поля)**
1	113	10	293
2	173	11	359
3	179	12	593
4	191	13	419
5	233	14	431
6	239	15	443
7	251	16	491
8	281	17	509
9	131	18	641

(А ще тут будуть додаткові завдання, але пізніше!..)

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) перевірку існування ОНБ (пункт А завдання);
3) бітові зображення тестових елементів та результатів операцій над ними;
4) бітові зображення результатів контролю за пунктом Б);
5) аналітичні відомості за пунктом В)
6) текст програми (у додатку)

Також текст програми передається викладачеві в електронному вигляді.

5. Оцінювання лабораторної роботи

За виконання лабораторної роботи студент може одержати до 12 рейтингових балів; зокрема, оцінюються такі позиції:

– реалізація основного завдання – до 6-ти балів;
– реалізація додаткового завдання – до 4-х балів;
– оформлення звіту – 1 бал;
– своєчасне виконання основного 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 оптимальний нормальний базис скінченного поля? Що таке ОНБ типу 2?
3. Як виконуються додавання, множення, піднесення до степеню, пошук оберненого елементу у оптимальному нормальному базисі?
4. Що таке мультиплікативна матриця?
5. Які переваги та недоліки реалізації поля в оптимальному нормальному базисі?
6. Опишіть алгоритм Ітo-Цудзії для пошуку оберненого елементу в ОНБ. Яка його складність?

7. Чи можна використати алгоритм Карацуби для множення елементів поля в ОНБ?

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).