Л.Б. Петришин

ОСНОВИ БІНАРНОЇ АРИФМЕТИКИ В КОДАХ ҐАЛУА

Наведено теоретичні основи перетворення форми та цифрової обробки інформації в кодових системах Ґалуа і обґрунтовано ефективність їх застосування у порівнянні із відомими методами двійкового кодування. Проаналізовано вади динаміки виконання арифметичних операцій в двійкових кодах і методів їх уникнення при кодуванні Ґалуа та підвищення швидкодії цифрової обробки.

В галузі цифрової обробки повідомлень вирішуються задачі кодування, цифрового прийому, декодування та обробки інфопотоків на основі арифметико-логічних та дискретних теоретико-числових перетворень [1 - 3]. При цьому техніко-економічна ефективність цифрової обробки інформації визначається формою подання вхідних даних, системою кодування та закладеними алгоритмами. Актуальність завдання розробки сучасних методів ефективних обчислень зумовлена невпинним зростом точності подання даних та результатів, який спричиняє до розширення їх розрядності (в системах радіолокації і обробки зображень) та розмірності вирішуваних задач (в комп'ютерній томографії, сейсмодіагностиці і метеорології), що в процесі обробки зумовлює до значного зростання об'ємів обчислень і вимагає розробки та впровадження швидких високоефективних алгоритмів [4 - 8].

Результати досліджень вказали на ефективність теоретико-числових перетворень із застосуванням теорії полів Ґалуа [9 - 12], які дозволяють реалізувати швидкі прямі алгоритми обчислень, що зумовлені простотою апаратної реалізації на базі процедур зсуву. Коди Ґалуа володіють одними із кращих характеристиками кодової дистанції (для $n>6$) і кореляційних функцій, а також множинністю алгоритмів декодування, які реалізуються на основі високорегулярних послідовних структур [4 - 6, 13]. Всі 2^n-1 n-розрядні ненульові кодові комбінації послідовності Ґалуа є результатом циклічного зсуву вихідного ненульового кодового фрагменту і мають однакову вагу, що характеризує їх як еквідистантні, або симплексні.

В скінчених полях Ґалуа на основі властивостей, наведених в [2, 3, 7 - 9, 13, 14] означені алгоритми основних арифметичних модульних за деяким простим числом p операцій сумування та множення, на підставі яких базуються похідні операції віднімання та ділення [1, 7, 13, 14]. Існуючі алгоритми логарифмування-антилогарифмування, функцій Якобі-Зеха (звичайних та модифікованих), із сумуванням за *mod 2* часткових добутків та кодів

поправок, на основі регістрів зсуву із зворотними зв'язками, двійкових векторів та поліномів, розкладу за нормальним базисом [14, 15] в окремих випадках мають достатньо просту технічну реалізацію, однак передбачають виконання цілого ряду послідовних проміжних операцій, що значно зменшує швидкодію обчислення кінцевого результату, а за деяких умов унеможливлює використання певного алгоритму.

Так, процедура перемноження двох векторів

$$A(x) = a_{k-1} x^{k-1} + a_{k-2} x^{k-2} + \ldots + a_1 x + a_0$$
$$H(x) = h_{r-1} x^{r-1} + h_{r-2} x^{r-2} + \ldots + h_1 x + h_0$$

передбачає виконання послідовної згортки на періоді слідування $k+r$ тактів, починаючи із коефіцієнтів старших порядків із формуванням добутку

$$A(x)\,H(x) = a_{k-1} h_{r-1} x^{k+r-2} + (a_{k-2} h_{r-1} + a_{k-1} h_{r-2}) x^{k+r-3} +$$
$$+ (a_{k-3} h_{r-1} + a_{k-2} h_{r-2} + a_{k-1} h_{r-3}) x^{k+r-4} + \ldots +$$
$$+ (a_0 h_2 + a_1 h_1 + a_2 h_0) x^2 + (a_0 h_1 + a_1 h_0) x + a_0 h_0$$

За умови простої технічної реалізації наведеної процедури на основі регістрів зсуву швидкодія вказаного методу достатньо низька та визначається розрядністю k та r операндів і, відповідно, кількістю тактів перемноження (максимально теоретично можлива - $k+r$).

Відомо, що найвищою швидкодією володіють методи із розпаралелюванням обчислень результатів цифрової обробки. Той факт, що на сьогоднішній день не відомі методи паралельного виконання арифметичних операцій безпосередньо в кодах Ґалуа, зумовив актуальність проведення досліджень щодо можливості реалізації та розробки основ бінарної арифметики реального часу в полях Ґалуа .

Розроблений метод виконання основних арифметичних операцій в кодах Ґалуа ґрунтується на безпосередній паралельній обробці операндів на підставі синтезованих логічних функцій порозрядного сумування за *mod p* [3].

Нехай для двох заданих операндів

$$A(x) = \sum_{i=0}^{n-1} a_i x^i \bmod p$$

та

$$D(x) = \sum_{i=0}^{n-1} d_i x^i \bmod p$$

результатом сумування визначений поліном

$$C(x) = \sum_{i=0}^{n-1} c_i x^i \bmod p,$$

який можна подати у наступній формі:

$$\begin{aligned} C(x) &= (a_{n-1}d_{n-1}^{\,n-1} + a_{n-2}d_{n-2}^{\,n-1} + \ldots + a_1 d_1^{\,n-1} + a_0 d_0^{\,n-1})\, x^{n-1} \bmod p + \\ &+ (a_{n-1}d_{n-1}^{\,n-2} + a_{n-2}d_{n-2}^{\,n-2} + \ldots + a_1 d_1^{\,n-2} + a_0 d_0^{\,n-2})\, x^{n-2} \bmod p + \\ &+ \quad \cdots \quad + \\ &+ (a_{n-1}d_{n-1}^{\,1} + a_{n-2}d_{n-2}^{\,1} + \ldots + a_1 d_1^{\,1} + a_0 d_0^{\,1})\, x^{1} \bmod p + \\ &+ (a_{n-1}d_{n-1}^{\,0} + a_{n-2}d_{n-2}^{\,0} + \ldots + a_1 d_1^{\,0} + a_0 d_0^{\,0}) \bmod p = \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i\, d_j^{\,i}\, x^i \bmod p = \sum_{i=0}^{n-1} c_i x^i \bmod p, \end{aligned} \qquad (1)$$

де $d_j^{\,i}$ – значення проміжних коефіцієнтів перемноження коефіцієнтів a_i поліному $A(x)$, отримані після перетворення коефіцієнтів d_i поліному $D(x)$ для синтезу коефіцієнта $c(x)$ j-го степеню при x результату $C(x)$, причому в наведеному розкладі $a_j = a_i$.

З метою отримання аналітичних закономірностей для обчислення $d_j^{\,i}$ необхідно здійснити кілька теоретико-числових перетворень формального переходу із послідовного рекурсивного виконання операції сумування в паралельне векторне.

Для прикладу поля Ґалуа $GF(2^4)$ із породжуючим вектором 10011 рекурсивна послідовність кодових елементів 111101011001000 подається формалізовано у наступному вигляді:

$b_1,\ b_2,\ b_3,\ b_4,\ b_1 \oplus b_4,\ b_1 \oplus b_2 \oplus b_4,\ b_1 \oplus b_2 \oplus b_3 \oplus b_4,\ b_1 \oplus b_2 \oplus b_3,\ b_2 \oplus b_3 \oplus b_4,\ b_1 \oplus b_3,\ b_2 \oplus b_4,\ b_1 \oplus b_3 \oplus b_4,\ b_1 \oplus b_2,\ b_2 \oplus b_3,\ b_3 \oplus b_4,\ b_1,\ b_2,\ b_3$.

В табл. 1 наведено порядкові номери дискретних повідомлень в десятковій системі числення, відповідні їм кодові слова Ґалуа та формалізоване подання всіх 4-розрядних кодів Ґалуа, виражених через $n = 4$ перші члени $b_1,\ b_2,\ b_3,\ b_4$ згідно рекурсивного закону. Із формалізованого рекурсивного запису кодів сум повідомлень операція додавання двох кодів $A(x)$ та $D(x)$ визначається як процедура рекурсивного зсуву, починаючи з вихідної позиції заданого коду $A(x)$ на кількість дискретних позицій, визначену десятковим еквівалентом іншого заданого коду доданку $D(x)$. Для систем кодування порядку n аналогічно визначаються значення n-розрядних сум за *mod2* кожного із елементів послідовності Ґалуа.

Табл. 1 є операційною таблицею паралельного сумування кодів в полі $GF(2^4)$, заданому породжуючим вектором 10011. Для виконання операції над кодом операнду $A(x)$, наприклад, 0101 (4) проводяться дії, що визначаються логічним вектором $D'(x)$

Таблиця 1

Формалізоване подання кодів Ґалуа $GF(2^4)$

№	Код Ґалуа	Розряди кодів Ґалуа, виражені через b_1, b_2, b_3, b_4			
0.	1 1 1 1	b_1	b_2	b_3	b_4
1.	1 1 1 0	b_2	b_3	b_4	$b_1 \oplus b_4$
2.	1 1 0 1	b_3	b_4	$b_1 \oplus b_4$	$b_1 \oplus b_2 \oplus b_4$
3.	1 0 1 0	b_4	$b_1 \oplus b_4$	$b_1 \oplus b_2 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3 \oplus b_4$
4.	0 1 0 1	$b_1 \oplus b_4$	$b_1 \oplus b_2 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3$
5.	1 0 1 1	$b_1 \oplus b_2 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3$	$b_2 \oplus b_3 \oplus b_4$
6.	0 1 1 0	$b_1 \oplus b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3$	$b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_3$
7.	1 1 0 0	$b_1 \oplus b_2 \oplus b_3$	$b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_3$	$b_2 \oplus b_4$
8.	1 0 0 1	$b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_3$	$b_2 \oplus b_4$	$b_1 \oplus b_3 \oplus b_4$
9.	0 0 1 0	$b_1 \oplus b_3$	$b_2 \oplus b_4$	$b_1 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2$
10.	0 1 0 0	$b_2 \oplus b_4$	$b_1 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2$	$b_2 \oplus b_3$
11.	1 0 0 0	$b_1 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2$	$b_2 \oplus b_3$	$b_1 \oplus b_4$
12.	0 0 0 1	$b_1 \oplus b_2$	$b_2 \oplus b_3$	$b_3 \oplus b_4$	b_1
13.	0 0 1 1	$b_2 \oplus b_3$	$b_3 \oplus b_4$	b_1	b_2
14.	0 1 1 1	$b_3 \oplus b_4$	b_1	b_2	b_3

відповідно значенню $D(x)$, наприклад 0110 (6), тобто, для обрахунку кожного розряду $C(x)$ одночасно виконуються наступні операції:

	b_1	b_2	b_3	b_4	
$A(x) =$	0	1	0	1	$= 4_{(10)}$
$D(x) =$	0	1	1	0	$= 6_{(10)}$
$D'(x) =>$	$b_1 \oplus b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3$	$b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_3$	
	$0 \oplus 1 \oplus 0 \oplus 1$	$0 \oplus 1 \oplus 0$	$1 \oplus 0 \oplus 1$	$0 \oplus 0$	
$C(x) =$	0	1	0	0	$= 10_{(10)}$.

Код Ґалуа результату $C(x) = 0100$ відповідає десятковому числу $10_{(10)}$, яке і є результатом суми чисел $4_{(10)}$ та $6_{(10)}$ - десяткових еквівалентів операндів Ґалуа $A(x)$ та $D(x)$.

Прикладне застосування пропонованого методу виконання арифметичних операцій полягає у розробці реальних кодових матриць програмованого перетворення системи кодів. Для цього згідно табл. 1 будується табл. 2 коефіцієнтів d_j^i, що відображає розряди програмування вмісту масиву елементів пам'яті як постійної пам'яті, або програмованої логічної матриці, де кодовий рядок Ґалуа визначає коди $d_3\ d_2\ d_1\ d_0$ адресної вибірки масиву пам'яті, а рядки d_j^i – вихідні коди його адресованого вмісту.

Таблиця 2

Значення проміжних коефіцієнтів d_j^i операції додавання кодів в полі Ґалуа $GF(2^4)$

№	адреса	$d_4^4 d_3^4 d_2^4 d_1^4$	$d_4^3 d_3^3 d_2^3 d_1^3$	$d_4^2 d_3^2 d_2^2 d_1^2$	$d_4^1 d_3^1 d_2^1 d_1^1$
0.	1 1 1 1	1 0 0 0	0 1 0 0	0 0 1 0	0 0 0 1
1.	1 1 1 0	0 1 0 0	0 0 1 0	0 0 0 1	1 0 0 1
2.	1 1 0 1	0 0 1 0	0 0 0 1	1 0 0 1	1 1 0 1
3.	1 0 1 0	0 0 0 1	1 0 0 1	1 1 0 1	1 1 1 1
4.	0 1 0 1	1 0 0 1	1 1 0 1	1 1 1 1	1 1 1 0
5.	1 0 1 1	1 1 0 1	1 1 1 1	1 1 1 0	0 1 1 1
6.	0 1 1 0	1 1 1 1	1 1 1 0	0 1 1 1	1 0 1 0
7.	1 1 0 0	1 1 1 0	0 1 1 1	1 0 1 0	0 1 0 1
8.	1 0 0 1	0 1 1 1	1 0 1 0	0 1 0 1	1 0 1 1
9.	0 0 1 0	1 0 1 0	0 1 0 1	1 0 1 1	1 1 0 0
10.	0 1 0 0	0 1 0 1	1 0 1 1	1 1 0 0	0 1 1 0
11	1 0 0 0	1 0 1 1	1 1 0 0	0 1 1 0	0 0 1 1
12.	0 0 0 1	1 1 0 0	0 1 1 0	0 0 1 1	1 0 0 0
13.	0 0 1 1	0 1 1 0	0 0 1 1	1 0 0 0	0 1 0 0
14.	0 1 1 1	0 0 1 1	1 0 0 0	0 1 0 0	0 0 1 0

В узагальненому випадку блок перетворення кодів, що виконує функцію перетворення елементів d_i в $d_j{}'$, представляє собою масив елементів пам'яті з організацією n x n^2.

Операція перемноження операндів в полі Ґалуа зводиться до сумування значення одного із операндів $A(x)$ кількість разів, визначену значенням іншого операнду $D(x)$ із приведенням кінцевого результату за $mod\ 2^n-1$.

Для зменшення громіздкості викладок в якості прикладу приймається поле $GF(2^3)$, синтезоване за вектором 1011. Отримана кодова послідовність 1110100 подається у наступному вигляді:

b_1 , b_2 , b_3 , $b_1 \oplus b_3$, $b_1 \oplus b_2 \oplus b_3$, $b_1 \oplus b_2$, $b_2 \oplus b_3$, b_1 , b_2 , b_3 .

Вираз, що описує процедуру перемноження в полі Ґалуа, аналогічний виразу (1) процедури додавання, з тією різницею, що коефіцієнти d_j^i при перемноженні будуть функціоналом не тільки значень d_i, але й a_i :

$$d_j^i = f(d_i, a_i). \qquad (2)$$

Значення функціоналу (2) для прикладу поля $GF(2^3)$ наведені в табл. 3, в якій з метою спрощення табличного відображення прийнято умовне позначення $b_i \equiv i$. На підставі табл. 3 синтезовані значення коефіцієнтів d_j^i (табл. 4) програмування масиву елементів пам'яті розмірності $2n$ x n^2 (6 x 9). В таблиці коди Ґалуа операндів $A(x)$ та $D(x)$

є $2n$-розрядними кодами адресної вибірки пристрою перетворення кодів, на n^*-розрядній шині даних якого формуються значення d_j^i, згідно яких здійснюється оперування над значеннями розрядів коду $A(x)$.

Таким чином, із наведеного можна підсумувати, що реалізація арифметичних операцій над кодами в полі Галуа дозволяє вилучити істотні недоліки двійкової арифметики, один із яких – наявність міжрозрядних переносів, що знижують швидкість виконання арифметичних операцій, в результаті чого підвищити швидкодію процесора. Інший – позиційність кодів, яка призводить до нерівноймовірного значення помилки в довільному із розрядів коду числа, що дозволяє зрівноважити значення помилки спотворення розрядів коду. В той же час запропоновані паралельні методи порівняно із існуючими методами оперування в полі Галуа дозволяють виконувати одночасну обробку всіх розрядів та формування коду результату в реальному часі, в наслідок чого скоротити час обчислення результату від n для відомих методів до одного такту для запропонованого.

Швидкодія запропонованих арифметичних пристроїв визначається часом доступу до вмісту масиву елементів пам'яті - t_b, часом перемикання ключів – t_k і часом сумування – t_c в модульних суматорах:

$$T_G = t_b + t_k + t_c.$$

Швидкодія відомих двійкових накопичуючих суматорів паралельної дії визначається розрядністю n кодів сумування і становить [16, 17]

$$T'_{д.с.} = n\, t_0 + (n\text{-}1)\, t_{затр.},$$

де t_0 – час спрацювання одного суматора, $t_{затр.}$ – час запізнення в лінії затримки.

Основний недолік останніх – низька швидкодія, зумовлена значним часом передавання бітів переносу. Максимальний час сумування двох чисел в паралельному накопичуючому суматорі з наскрізним переносом визначається як

$$T''_{д.с.} = 2\, t_0 + t_{затр} + (n\text{-}1)\,(t_i + t_{або}),$$

де t_i, $t_{або}$ - час запізнення сигналу в логічних схемах комутації.

Для алгоритму перемноження, що володіє максимальною швидкодією [18] і описується визначенням суми часткових добутків на i - му кроці:

$$S_i = S_{i-1} + A\, b_i\, 2^{-n+i-1},$$

Таблиця 4

Значення коефіцієнтів операції перемноження кодів в $GF(2^3)$

	111	**110**	**101**	**010**	**100**	**001**	**011**
1	100	100	100	010	100	001	001
1	100	100	100	010	100	001	001
1	100	100	100	010	100	001	001
1	100	100	100	100	100	100	100
1	100	010	010	010	010	010	010
0	100	001	001	001	001	001	001
1	100	010	001	101	111	110	011
0	100	001	101	111	110	011	100
1	100	101	111	110	011	100	010
0	100	001	111	011	010	101	110
1	100	101	110	100	001	111	011
0	100	111	011	010	101	110	100
1	100	101	011	001	110	010	111
0	100	111	100	101	011	001	110
0	100	110	010	111	100	101	011
0	100	111	010	110	001	011	101
0	100	110	001	011	101	100	111
1	100	011	101	100	111	010	110
0	100	110	101	010	011	111	001
1	100	011	111	001	100	110	101
1	100	100	110	101	010	011	111

де A – множене, $B = b_{n-1},...,b_i,...,b_0$ – множник, $A\ 2^{n+1}$ – відповідає пересиланню множеного на першому кроці в суматор, а швидкодія визначається виразом

$$T_{д\ м} = t_{см.}\ n,$$

де $t_{см}$ – час сумування двох чисел.

Аналіз вказує на вищу швидкодію процесорів Ґалуа, оскільки значення величин t_b, t_k, t_c значно менші значень величин t_0, $t_{затр.}$, $t_{см}$ із врахуванням n міжрозрядних послідовних переносів та процедур формування сум. Виграш в швидкодії досягається за рахунок нарощення потужності апаратних засобів, оскільки потребує використання масиву елементів пам'яті ємністю n x n^2 для суматорів та $2n$ x n^2 для перемножувачів, поля n^2 ключів комутації і n-входових пристроїв сумування за *mod 2*.

Позитивною властивістю структур арифметичних процесорів Ґалуа є високий ступінь однорідності обчислювального середовища [3], що визначає перспективу їхньої реалізації в мікроелектронному виконанні.

Theoretical bases of form transformation and digital processing of information in the code systems Galois's are led and an efficiency of their application by comparison to the known methods of the binary encoding is grounded. Lacks of dynamics of implementation of arithmetic operations in the binary codas and methods of their avoidance in case of the Galois's encoding and rise of fast acting of digital processing are analyzed.

[1]. Яблонский В.С. Введение в дискретную математику. – М.: Наука, 1986. – 384 с.

[2]. Гольденберг Л.М. и др. Цифровая обработка сигналов: Справочник. – М.: Радио и связь, 1985. – 312 с.

[3]. Петришин Л.Б. Теоретичні основи перетворення форми та цифрової обробки інформації в базисі Галуа. – Київ: ІЗіМН МОУ, 1997. – 237 с.

[4]. Голд Б., Рэйдер Ч. Цифровая обработка сигналов: Пер. с англ. – М.: Сов. радио, 1973. – 368 с.

[5]. Даджион Д., Мерсеро Р. Цифровая обработка многомерных сигналов: Пер. с англ. – М.: Мир, 1988. – 488 с.

[6]. Макклеллан Дж.Х., Рэйдер Ч.М. Применение теории чисел в цифровой обработке сигналов. – М.: Радио и связь, 1983. – 264 с.

[7]. Рабинер Л., Голд Б. Теория и применение цифровой обработки сигналов: Пер. с англ. – М.: Мир, 1978. – 848 с.

[8]. Белоглазова О.В., Лабунец В.Г. Теория и применение преобразований Гаусса-Рэйдера // Изд-во АН СССР. Техн. Киберенетика. – 1981. – №2. – С. 193-200.

[9]. Лабунец В.Г. Теоретико-числовые преобразования над полями алгебраических чисел. – В кн.: Применение ортогональных методов при обработке сигналов и анализе систем. – Свердловск: УПИ. – 1981. – С. 44-54.

[10]. Агарвал Р., Баррас С. Теоретико-числовые преобразования для быстрого вычисления цифровой свертки // ТИИЭР. – 1975. – Вып. 4. – С. 4-20.

[11]. Лидл Р., Нидеррайтер Г. Конечные поля: В 2-х т. Пер. с англ. – М.: Мир, 1988. – 822 с.

[12]. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел / Пер. с англ. – М.: Мир, 1987. – 416 с.

[13]. Кларк Дж., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. – М.: Радио и связь, 1987. – 392 с.

[14]. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: Пер. с англ. – М.: Мир, 1976. – 594 с.

[15]. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки /Пер. с англ. – М.: Связь, 1979. – 744 с.

[16]. Соучек Б. Мини-ЭВМ в системах обработки информации. – М.: Мир, 1976. – 520 с.

[17]. Акушский И.А., Амербаев В.М., Пак И.Т. Основы машинной арифметики комплексных чисел. – Алма-Ата: Наука, 1970. – 248 с.

[18]. Микро-ЭВМ / Под ред. А. Диркенса. -М.: Энергоиздат, 1982. – 328 с.