computing@tanet.edu.te.ua
www.tanet.edu.te.ua/computing

ISSN 1727-6209
International Scientific
Journal of Computing

ОСНОВИ ЕЛЕМЕНТАРНОЇ АРИФМЕТИКИ В ПОЛЯХ ҐАЛУА

Любомир Петришин

Кафедра інформатики Прикарпатського національного університету, petryshynl@poczta.fm

Резюме: *Наведено теоретичні основи і структура засобів перетворення та цифрової обробки повідомлень 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 методи їх елімінування при кодуванні Ґалуа та підвищення швидкодії цифрової обробки.*

ВСТУП

В галузі цифрової обробки повідомлень вирішуються задачі кодування, трансмісії, 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, методами 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 значне зростання обсягів обчислень і вимагає розробки та впровадження швидких високоефективних алгоритмів [4 – 8].

Результати досліджень вказали на ефективність застосування теоретико-числових перетворень в полях Ґалуа [9 – 12], які дозволили реалізувати швидкі прямі алгоритми обчислень, зумовлені простотою апаратної реалізації на базі процедур зсуву. Коди Ґалуа володіють одними із кращих характеристиками кодової дистанції (для розрядності кодового слова $n>6$, де $n=log_2N$, N-модуль системи числення) 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 [3, 7 - 9, 13, 14] означено алгоритми основних арифметичних модульних за деяким простим числом p операцій додавання і множення, на підставі яких базуються похідні операції віднімання та ділення [1, 7, 13, 14]. Існуючі алгоритми логарифмування-антилогарифмування, функцій Якобі-Зеха (звичайних і модифікованих), із підсумовуванням за *mod 2* часткових добутків та кодів поправок, на основі регістрів зсуву зі 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 обмежує швидкодію обчислення кінцевого результату, а за деяких умов унеможливлює використання такого 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 розпаралеленням обчислення результатів цифрової обробки [2, 4, 5, 10]. 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 додавання 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 додавання визначено поліном

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

який можна подати у наступній формі:

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

де d_j^i - значення проміжних коефіцієнтів перемноження коефіцієнтів a_i поліному $A(x)$, отримані після перетворення коефіцієнтів d_i поліному $D(x)$ з метою 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 додавання 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 діагонального запису кодів сум даних 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 операнду $D(x)$. Таким чином, реалізація вказаної операції додавання в полі Ґалуа зводиться до одночасного паралельного взаємно незалежного формування кожного біту результату обчислення як суми за *mod2* без необхідності виконання операцій міжрозрядних переносів, що дозволяє підвищити швидкодію обробки пропорційно розрядності слова даних у порівнянні із двійковою системою числення. Обчислення кожного результату операції здійснюється за один такт обчислення інваріантно розрядності слова даних.

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	$b_1 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2$	$b_2 \oplus b_3$	$b_3 \oplus b_4$
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

Слід звернути увагу на вказану властивість діагональної зверху вниз – справа наліво рекурсії формального подання і, відповідно, виконання операцій додавання. Таке впорядкування дозволяє значно спростити архітектуру обчислювального середовища спецпроцесора та реалізувати його на регулярній розподіленій структурі однотипних обчислювальних елементарних елементів типу комутованих суматорів за *mod2*, підвищити швидкодію та зменшити кошти реалізації біторієнтованих процедур арифметичної обробки.

Для систем кодування вищих порядків n аналогічно визначаються значення n-розрядних сум за *mod2* кожного із елементів послідовності Ґалуа.

Таблиця 1 є прикладом операційної таблиці паралельного додавання кодів в полі $GF(2^4)$, заданому породжуючим вектором *10011*. Для виконання операції над кодом операнду $A(x)$, наприклад, *0101* (4) здійснюються дії, що визначаються логічним вектором $D'(x)$ відповідно значенню операнду $D(x)$, наприклад *0110* (6), тобто, для обчислення 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 кодових матриць визначеного перетворення системи кодів. Для цього за таблицею 1 будується таблиця 2 коефіцієнтів d_j^i, що відображає розряди програмування вмісту масиву елементів 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.

На рисунку 1 зображена структурна схема арифметичного спецпроцесора Ґалуа, на якій БПК - блок перетворення кодів. В узагальненому випадку блок перетворення кодів, що виконує функцію перетворення елементів d_i в $d_j{}^i$, є масивом програмованих логічних елементів матриці з організацією $n \times n^2$.

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

Інша елементарна арифметична операція - віднімання є комплементарною до операції додавання і, як можна підсумувати із вище наведеного, внаслідок властивості рекурсивного впорядкування вектора логічних перетворень кодової послідовності Ґалуа, є тією ж самою операцією додавання із зміною напрямку перетворення вказаної кодової послідовності. Інакше, знак віднімання не потребує зміни логіки обчислень, а тільки формально вказує на зміну складу логічних операцій визначення кожного із одиничних бітів результату. Внаслідок цього вказана операція також не вимагає зміни організації обчислювального середовища і може бути реалізована арифметичним спецпроцесором додавання із функціональним розширенням знаку арифметичної операції.

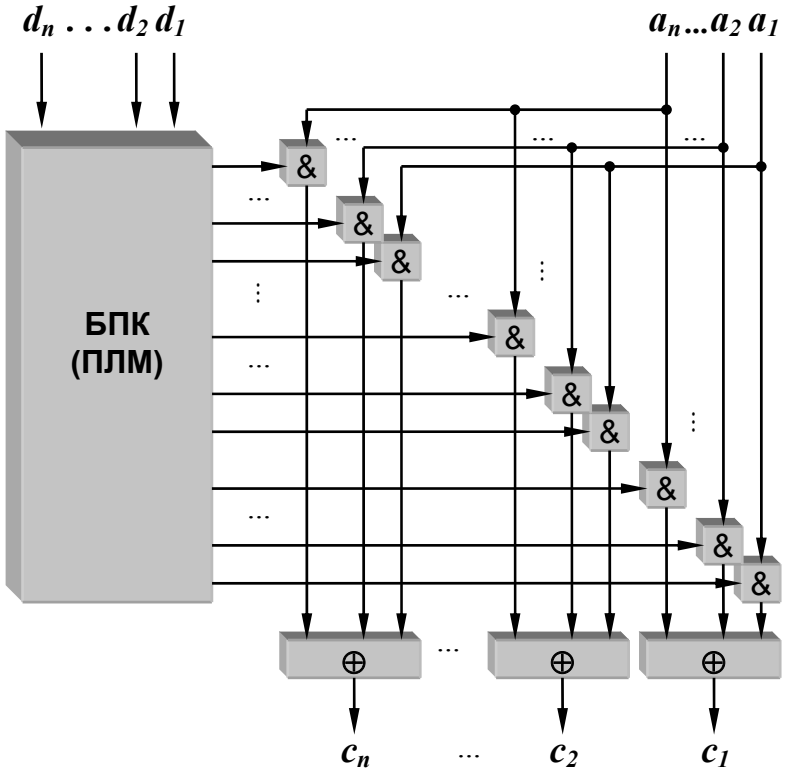

Рисунок 1 – Структура арифметичного спецпроцесора Ґалуа.

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

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

Швидкодія відомих двійкових суматорів паралельної дії із накопиченням визначається розрядністю n кодів додавання 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 та обробки бітів переносу.

Максимальний час додавання двох чисел в паралельному суматорі з накопиченням і 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.

Аналіз вказує на вищу швидкодію процесорів Ґалуа у порівнянні з двійковими процесорами, оскільки значення величин t_b , t_k , t_c для процесорів Ґалуа значно менші відповідних значень величин t_0 , $t_{затр.}$, $t_{см.}$ із врахуванням n міжрозрядних послідовних переносів та процедур формування сум двійковими процесорами.

Виграш в швидкодії досягається за рахунок нарощування потужності апаратних засобів, оскільки потребує використання матриці програмованих логічних елементів розмірності n x n^2, операційного поля із n^2 ключів комутації і n-входових пристроїв суми за *mod 2*. Наприклад, для 32-розрядних спецпроцесорів Галуа розмірність БПК складає 32 вхідні x 1024 вихідні розряди, операційне поле складається відповідно із 1024 двійкових модульних суматорів, а також із 32 32-входових суматорів за модулем 2. Для сучасного рівня технологічного розвитку мікроелектроніки розробка вказаного спецпроцесора не становить складності, потребує незначних коштів і визначає реальним його виготовлення.

Перевагою структур арифметичних процесорів Ґалуа є високий ступінь однорідності обчислювального середовища [3], що спрощує їхню реалізацію в мікроелектронному виконанні.

ЛІТЕРАТУРА

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

[2]. Микропроцессорные системы / Е.К.Александров, Р.И.Грушвицкий и др. - СПб.: Политехника, 2002. - 935 с.

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

[4]. Калабеков Б.А. Цифровые устройства и многопроцессорные системы. - М.: Горячая линия-Телеком, 2003. - 336 с.

[5]. Кравец О.Я., Подвальный Е.С., Хисамутдинов Р.А. Вычислительные комплексы и системы: архитектура, конвейеризация. параллелизм. - Уфа: УГАТУ, 2004. - 190 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]. Даджион Д., Мерсеро Р. Цифровая обработка многомерных сигналов: Пер. с англ. - М.: Мир, 1988. - 488 с.

[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]. Евстигнеев В.Г. Недвоичные компьютерные арифметики. – Зеленоград: МИЭТ, февраль 2005, http://www.computer-museum.ru/books/archiv/sokcon06.pdf.

[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]. Щукина О.Н. Архитектура компьютера. Часть 1. Информационно-логическая и функционально-структурная организация персонального компьютера. - М.: МГОУ, Елец: ЕГУ им. И.А.Бунина, 2003. - 234 с.

[17]. Фрике К. Вводный курс цифровой электроники. - М.: Техносфера, 2003. - 432 с.

***Петришин Любомир Богданович**, професор, доктор технічних наук, завідувач кафедри інформатики Прикарпатського національного університету. Область наукових досліджень – теоретичні основи, методи і засоби перетворення форми та цифрової обробки інформації.*

BASES OF ELEMENTARY ARITHMETICS IN GALOIS'S FIELDS

Lubomyr Petryshyn

Department of informatics of the Prycarpathian national university, petryshynl@poczta.fm

Theoretical bases and structure of means of transformation of the form and digital processing of the information in code systems Galois are resulted and is determined efficiency of their application in comparison with known methods of binary coding. Lacks of dynamics of performance of arithmetic operations of binary codes and methods of their elimination are analysed at coding Galois and increase of operating speed of digital processing. In digital processing of communications are solved the problems of coding, transmission, decoding and treating information streams on the arithmetic-logical basis and discrete theoretical-numerical transformations. Thus technical and economic efficiency of digital processing of information is defined by the form of representation of the entrance data, methods of coding and the incorporated algorithms.

The results of researches have specified efficiency of application of theoretical-numerical transformations in Galois's fields which made it possible to realize the fast direct algorithms of calculations caused by simplicity of hardware realization on the basis of procedures of shift. Galois's Codes own one of the best characteristics of a code distance and correlation functions, and also plurality of algorithms of decoding which are realized on the basis of regular consecutive structures.

It is known, that the highest fast-acting is owned by methods from the execution in parallel of the calculations of results of digital processing.

That fact, that for today methods of parallel performance of arithmetic operations directly in Galois's codes are not known, has caused a urgency of carrying out of researches concerning to an opportunity of realization and developing the bases of the binary arithmetic of real time in Galois's fields.

The developed method of performance of the basic arithmetic operations in Galois's codes is based on direct parallel processing of operands on the basis of the synthesized logic functions of digit-by-digit summation on mod p. With the purpose of obtaining of analytical law it is necessary to carry out some theoretical-numerical transformations on formal transition from sequential recursive performance of operation of summation in parallel vector.

From the formal recursive diagonal record of the codes of the sums of data the operation of the adding up of two codes A(x) and D(x) is defined as the procedure of recursive shift, beginning from initial position of the set code A(x) to the quantity of discrete positions, determined by the decimal equivalent of other set code of operand D(x). Thus, realization of the operation of addition in the Galois field is reduced to the simultaneous parallel mutually independent forming of everyone bit of result of calculation as sums on mod2 without the necessity of implementation of operations of digit carries, that lets to promote the fast-acting of processing proportional to the word length of the word of data by comparison with the binary number system.

The calculation of the result of fulfilment by each of the operations is carried for one step of the calculation invariantly of the word length of the word of data. Should be focused attention on the indicated property of diagonal from top to bottom - from right to left the recursion of formal presentation and, accordingly, implementation of operations of addition. This order they will make it possible to considerably simplify the architecture of the computational medium of special-processor and to realize it on the regular distributed structure of the same types computational elementary elements of the type of the commutated adders on mod2, to increase fast-acting and to reduce the means of the realization of the bits-oriented procedures of arithmetical processing.

Another elementary arithmetical operation - subtraction is complementary to operation of addition and as it is possible to sum up from than higher given, as a result of property of recursive ordering a vector of logic transformations of sequence of Galois code, is the same operation of addition with change of a direction of transformation of the indicated code sequence.

Operating speed of the offered arithmetical units is determined by times to access to the content of memory cells, switch time of keys and by times of addition-subtraction in the modular adders. Analysis specifies on a higher speed of Galois's processors in comparing to the binary processors, as a value of the quantities for Galois's processors is considerably less than the appropriate values taking into п-account of discharge sequential transfers and procedures of the

formation of sums by binary processors.

Winning in a fast-acting is reached due to increase in the capacity of hardware as it is necessary to use a matrix of programmed logic elements of dimension п x п2, an operational field from п2 keys of switching and n-bit input devices of the sum on mod 2. For a modern level of technological development of microelectronics development the special-processor does not make complexity, requires insignificant means and its production is determined by real.

By the advantage of the structures of the arithmetical Galois's processors there is the high degree of homogeneity of computational medium, which simplifies their realization in the microelectronic performance.