УДК 681.325

О.І. ВОЛИНСЬКИЙ, П.В. ГУМЕННИЙ
Тернопільський національний економічний університет

ТЕОРЕТИЧНІ ЗАСАДИ ВИЗНАЧЕННЯ ЗАЛИШКІВ НА ОСНОВІ ЛІЧИЛЬНИКІВ У РІЗНИХ ТЕОРЕТИКО-ЧИСЛОВИХ БАЗИСАХ

В статті проведений аналіз теоретичних основ базисів Крестеннсона та Галуа, як одних з найперспективніших шляхів для реалізації швидкодіючих процесорів опрацювання даних, оскільки вони характеризуються найкомпактнішими кодовими матрицями. Досліджено принципи виконання арифметичних операцій та їх характеристик системами числення, що утворюються на основі досліджуваних базисів. Також проведено дослідження системних характеристик синхронних лічильників в різних теоретико-числових базисах та розроблено модульні лічильники. Проведено дослідження апаратних та часових затрат для роботи відповідних лічильників.

Ключові слова: теоретико-числовий базис (ТЧБ), система залишкових класів (СЗК), вертикально-інформаційна технологія (ВІТ).

O.I. VOLYNSKYY, P.V. HUMENNIY
Ternopil National Economic University

THEORETICAL FOUNDATIONS FOR IDENTIFYING RESIDUES BASED IN COUNTERS IN THE VARIOUS BETWEEN-BASES TRANSFORMATIONS

The paper is the research of the process of formation and use for work in Krestenson's theoretical-digital basis. Also, research and development of modular meters as one of the ways to implement components between-bases transformations.

The paper analyzed the theoretical foundations Krestennson`s bases and Galois`s bases as one of the most promising ways to implement high-speed data processing processors, since they possess the most compact code matrix. Research the principles of arithmetic operations and their characteristics notation, formed on the basis of the investigated bases. Also in the article studied the system characteristics of synchronous counters in various theoretical and numerical bases and developed a modular counters. Research hardware costs and time costs for the respective counters.

The obtained results show the possibility of using counters as modular component of Rademacher-Krestenson`s between-bases transformations and demonstrate SRC the ability to integrate other TDB as built counters have provided the main elements of the number system - the remainder.

Keywords: theoretical-digital basis (TDB), the system of residual classes (SRC), vertical information technology (VIT).

Впродовж тривалого часу прогрес в області вдосконалення функціональних можливостей та технічних характеристик мікропроцесорів розвивався пропорційно тенденціям підвищення тактової частоти мікроелектронних компонентів, зменшення габаритів, енергоспоживання та підвищення надійності [1].

При цьому на межі 2000 року рівень мікроелектронної технології досяг границі 0,2-0,01 мкм, а в даний час інтенсивно розвиваються нано- та оптоелектронні технології реалізації компонентів на мікроелектронному рівні [2]. При цьому тактові частоти сучасних процесорів досягли значень 10 ГГц. Збільшення тактової частоти процесорів останнім часом зростає дуже повільно, це залежить від витрат енергії, підвищення максимальної температури, а також інших, заснованих на законах фізики, явищах. В останні десятиліття різко покращуються технології виготовлення малогабаритної постійної та оперативної пам'яті великих об'ємів (10 Гбайт – 10 Терабайт) [3].

Постановка проблеми

Високі вимоги до продуктивності сучасних процесорів забезпечуються використанням матричних і конвеєрних архітектур, які базуються на основі двійкової системи числення теоретико-числового базису Радемахера. Двійкова система числення має функціональні обмеження, зокрема, наявність міжрозрядних зв'язків, велику розрядність шин адрес, управління та даних (n=32, 64, 128…) і необхідність реалізації великого числа інформаційних міжкомпонентних зв'язків. Для усунення даних функціональних обмежень перспективними для побудови високопродуктивних процесорів з обмеженим числом міжкомпонентних зв'язків є теоретико-числові базиси (ТЧБ), відмінні від базису Радемахера, до яких належать ортогональні дискретні базиси: Крестенсона, Хаара, унітарний та Галуа.

Аналіз останніх досліджень і публікацій

Методологічні основи теорії проектування архітектури та функціональних характеристик процесорів розроблені відомими зарубіжними науковцями: Д. фон Нейман, М. Флін, Р. Хокні, Д. Скілкорн Г.І. Новіков, С.А. Майоров; українськими вченими: В.М. Глушков, О.В Палагін, Л.Д. Самофалов, А.О. Мельник, Б.М. Маліновський, М.В. Черкаський, Р.Б. Дунець [2–9]. У той же час, відомі класи процесорів не у повній мірі відповідають сучасним вимогам їх проектування на кристалах та мережевих комунікаційних середовищах. Для їх побудови недостатньо використовуються можливості теорії виконання арифметико-логічних операцій на основі рекурентних властивостей кодової системи базису Галуа. Не розроблені і не освоєні базові компоненти спецпроцесорів та їх компонентів на основі базисів Крестенсона та Галуа, у тому числі: аналого-цифрові перетворювачі (АЦП) та арифметико-логічні пристрої, шифратори, дешифратори, адресні лічильники, асоціативна пам'ять з паралельним доступом та ін. Значний внесок у розвиток теорії побудови високопродуктивних спецпроцесорів на основі ТЧБ Крестенсона та Галуа

здійснили І.Я. Акушський, Я.М. Николайчук, Г.І. Брюхович, М.В. Синьков, В.П. Тарасенко, В.С. Глухов [11–17]. Перспективною є також побудова високопродуктивних мультиядерних та мультибазисних процесорних систем на основі вертикально-інформаційної технології (ВІТ) зі спільним потоком команд та опрацюванням біт-орієнтованих потоків інформації, що дозволяє реалізувати розпаралелення операцій формування, обробки, зберігання та колективного доступу до даних[18].

Отже, розробка компонентів операційних вузлів та структурна організація спецпроцесорів на основі ВІТ при застосуванні різних ТЧБ з покращеними технічними характеристиками, є актуальною науковою задачею.

Дослідження літературних джерел, що до застосування перспективних та найпоширеніших ТЧБ для перетворення, передавання та опрацювання інформаційних потоків в сучасних комп'ютерних системах показує, що:

1) в базисі Радемахера [19] реалізована виключна більшість універсальних процесорів комп'ютерної та комунікаційної техніки, а також сигнальних процесорів різних застосувань [20];

2) базис Крестенсона, який породжує систему числення залишкових класів знайшов успішне застосування для побудови спецпроцесорів стиснення інформації [10] та реалізації високопродуктивних процесорів опрацювання інформаційних потоків [14], системах протиповітряної оборони та опрацювання великорозрядних чисел в системах крипто захисту інформації;

3) базис Галуа серед відомих базисів отримав особливо широке застосування, для побудови спецпроцесорів та рішеннях прикладних задач в галузях:

а) аналого-цифрового перетворення та кодування інформації;

б) передавання інформації на основі кодів Баркера та М-послідовностей;

в) стиснення інформації [15].

Значні успіхи досягненні при побудові спецпроцесорів на основі комбінованого використання різних ТЧБ. Наприклад: Хаара-Крестенсона, Крестенсона-Галуа [15], а також, реалізації високопродуктивних мультибазисних RCG-процесорів на основі базисів Радемахера, Крестенсона та Галуа [14]. Оскільки найбільш взаємопов'язаними між собою є названі процесори, тобто, обчислювальні операції арифметики, які виконуються за один такт найбільш швидкодійні у базисі Крестенсона, представляється залишками базису Галуа в кодах базису Крестенсона. Тому, поглиблення теоретичних засад арифметики базису Крестенсона є найбільш важливим фактором вдосконалення та покращення системних характеристик широкого спектру спецпроцесорів опрацювання, багаторозрядних чисел, що визначає високий рівень актуальності дослідження в цьому напрямку.

Постановка завдання

1. Дослідження властивостей та характеристик системи залишкових класів (СЗК).

2. Принципи реалізації та оцінка функціональних можливостей реалізації арифметики та базових функцій над числами в базисах Радемахера, Крестенсона та Галуа.

3. Дослідження лічильників для визначення залишків в різних теоретико-числових базисах.

Теоретичні засади виконання та характеристики арифметико-логічних операцій у базисах Радемахера, Крестенсона та Галуа

Система числення залишкових класів, яка породжується теоретико-числовим базисом Крестенсона, характеризується суттєвими перевагами по відношенню до базису Радемахера при виконанні операцій додавання та множення. Оскільки СЗК непозиційна і в ній відсутні наскрізні переноси при виконанні арифметичних операцій, то процес виконання операцій додавання та множення виконується за один такт на основі матриць [10, 21]. Тому є важливим реалізація та дослідження міжбазисних перетворень Радемахера-Крестенсона для проектування спецпроцесорів опрацювання великорозрядних чисел.

Двійкова система числення належить до позиційних систем числення і є частковим випадком системи числення залишкових класів з набором модулів p^i, де p=2, 3,…, 8, 10, 16…; i=0, 1, 2,… [12, 22].

Арифметичні операції над двома числами у двійковій системі числення базису Радемахера описуються наступними виразами:

$$X = \sum_{i=0}^{n-1} x_i 2^i \ , \ x_i \in \overline{0,1} \, ; Y = \sum_{i=0}^{n-1} y_i 2^i \ , \ y_i \in \overline{0,1} \, .$$

Тобто, двійкові коди чисел X і Y :

$$X = (x_{n-1}, x_{n-2}, ..., x_i, ..., x_0) \, ; Y = (y_{n-1}, y_{n-2}, ..., y_i, ..., y_0) \, .$$

визначаються на основі модульних операцій згідно аналітичних виразів:

$$X \rightarrow \begin{cases} resX(\bmod 2^0) = x_0 \, ; \\ resX(\bmod 2^1) = x_1 \, ; \\ \cdots \quad \cdots \quad \cdots \\ resX(\bmod 2^i) = x_i \, ; \\ \cdots \quad \cdots \quad \cdots \\ resX(\bmod 2^{n-1}) = x_{n-1} \, ; \end{cases} \qquad Y \rightarrow \begin{cases} resY(\bmod 2^0) = y_0 \, ; \\ resY(\bmod 2^1) = y_1 \, ; \\ \cdots \quad \cdots \quad \cdots \\ resY(\bmod 2^i) = y_i \, ; \\ \cdots \quad \cdots \quad \cdots \\ resY(\bmod 2^{n-1}) = y_{n-1} \, , \end{cases}$$

де *res*- операція знаходження найменшого невід'ємного залишка по модулю 2^i.

Невиконання умови взаємної простоти модулів в різних розрядах двійкових кодів відповідно ускладнює алгоритми додавання та множення двійкових чисел, оскільки при виконанні операції додавання між двійковими розрядами виникають наскрізні переноси з молодших в старші розряди.

$$\begin{array}{cccccccc} & x_{n-1} & \dots & x_i & \dots & x_1 & x_0 \\ + & y_{n-1} & \dots & y_i & \dots & y_1 & y_0 \\ \hline P_n & P_{n-1} & \dots & P_i & \dots & P_1 & \\ S_n & S_{n-1} & \dots & S_i & \dots & S_1 & S_0 \end{array}.$$

Наявність наскрізних переносів при виконанні операції додавання в базисі Радемахера в $2n$-разів знижує швидкодію виконання операції сумування чисел по відношенню до тактової частоти роботи процесорів. У зв'язку з цим існують різні способи побудови суматорів базису Радемахера з більш швидкою реалізацією наскрізних переносів, що особливо важливо при виконанні операцій над великорозрядними числами [22].

Відсутність взаємної простоти модулів системи числення базису Радемахера обумовлює значну складність алгоритмів множення двійкових чисел згідно графа (рис. 1) [22], де AND-лінійка операторів, яка формує *n* *n*-розрядних результатів логічного множення множеного X на розряди множника *Y*, які зсуваються праворуч на R_i (i=1, 2,..., n-1).

Теоретичною основою системи числення залишкових класів (СЗК) є Китайська теорема про залишки [21], на основі якої реалізується пряме та зворотне перетворення СЗК:

$$X \rightarrow \begin{cases} resX(\bmod p_0) = b_0; \\ resX(\bmod p_1) = b_1; \\ \dots \\ resX(\bmod p_i) = b_i; \\ \dots \\ resX(\bmod p_k) = b_k; \end{cases} \qquad Y \rightarrow \begin{cases} resY(\bmod p_0) = a_0; \\ resY(\bmod p_1) = a_1; \\ \dots \\ resY(\bmod p_i) = a_i; \\ \dots \\ resY(\bmod p_k) = a_k; \end{cases}$$

$$X = res\sum_{i=0}^{k-1} b_i \cdot B_i(\bmod P); \quad Y = res\sum_{i=0}^{k-1} a_i \cdot B_i(\bmod P),$$

де $P = \prod_{i=0}^{k-1} p_i$; $p_1, p_2, \dots, p_i, \dots, p_k$ – система взаємно простих модулів; $B_i = \frac{P}{p_i} \cdot m_i \equiv 1(\bmod\ p_i)$; $0 \le m_i \le p_i - 1$ нормуючі коефіцієнти базисних чисел B_i.

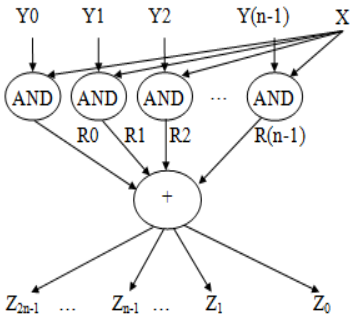


Рис. 1. Граф виконання операції множення в базисі Радемахера

Виконання умови взаємної простоти модулів СЗК базису Крестенсона суттєво спрощує алгоритми виконання операцій додавання та множення над числами, представленими кодами СЗК $X = (b_0, b_1, ..., b_j, ..., b_{k-1})$ та $Y = (a_0, a_1, ..., a_j, ..., a_{k-1})$ згідно з граф-алгоритмами рис. 2, де (+)res відповідає операції $C_j = res(b_j + a_j) \bmod P_j$, а (×)res – операції $\gamma_j = res(b_j \cdot a_j) \bmod P_j$:

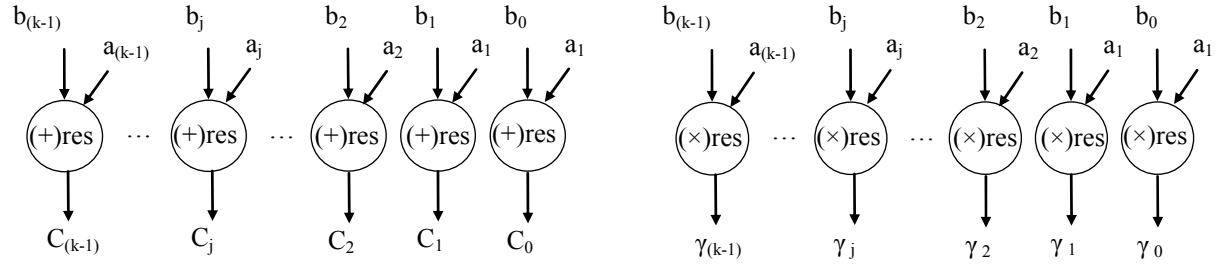


Рис. 2. Графи виконання операцій додавання та множення в базисі Крестенсона.

Головною особливістю представлення даних в базисі Галуа є рекурентність [23]. Суть рекурентності полягає в максимальній упаковці біт-орієнтованої послідовності кодового ключа

$$X_{i+1} = \sum_{i=1}^{n} (X_i \oplus X_{i-j}),$$

де $\oplus$ – символ додавання по *mod*2; n – число пар елементів кодового ключа.

Коди поля Галуа [24] за загальною класифікацією відносяться до підкласу циклічних блокових кодів, які володіють всіма основними властивостями завадозахищених кодів. В блокових кодах послідовність елементарних повідомлень розбивається на блоки символів (*B*1*, B*2*, B*3*, ..., Bn*) фіксованої довжини К, кожному з яких ставиться у відповідності певна комбінація символів кодового слова (*b*1*, b*2*, b*3*, ..., bn*). Циклічні коди Галуа відносяться до класу систематичних кодів. Для останніх можна записати відповідний їм аналітичний вираз у вигляді логічного співвідношення, яке визначається правилами створення цих кодів. Найбільш зручною формою представлення циклічних кодів є використання алгебраїчного виразу [25]

$$G(x) = a_{n-1} \times x^{n-1} + a_{n-2} \times x^{n-2} + a_1 \times x + a_1,$$

де $a_0 - a_{n-1}$ – числа, що дорівнюють «*0*» чи «1», які визначають відповідні значення розрядів кодових комбінацій.

Наприклад, у полі Галуа $GF\begin{pmatrix}5\\2\end{pmatrix}$ з ключем *10010* на основі незвідного полінома $x^5 + x^2 + 1$ формується послідовність елементів a_0, a_1, a_2,..., a_{31}, де a_{31} це – Ø останній многочлен, визначається на основі рекурентного рівняння

$$G_{i+1} = G_i \overline{\oplus} G_{i-n}\ ;\ \text{n=5},$$

та має вигляд послідовності елементів: 11111001101001000001010111011000, які кодують числа у діапазоні 0, 1, 2, …, 31:

$b_5, b_4, b_3, b_2, b_1,\ b_2 \oplus b_5, b_1 \oplus b_4, b_2 \oplus b_3 \oplus b_5, b_1 \oplus b_2 \oplus b_4,\ b_1 \oplus b_2 \oplus b_3 \oplus b_5, b_1 \oplus b_4 \oplus b_5,$

$b_2 \oplus b_3 \oplus b_4 \oplus b_5, b_1 \oplus b_2 \oplus b_3 \oplus b_4, b_1 \oplus b_3 \oplus b_5, b_4 \oplus b_5, b_3 \oplus b_4, b_2 \oplus b_3, b_1 \oplus b_2, Ø,\ b_1 \oplus b_2 \oplus b_5,$

$b_1 \oplus b_2 \oplus b_4 \oplus b_5, b_1 \oplus b_2 \oplus b_3 \oplus b_4 \oplus b_5, b_1 \oplus b_3 \oplus b_4 \oplus b_5, b_3 \oplus b_4 \oplus b_5, b_2 \oplus b_3 \oplus b_4, b_1 \oplus b_2 \oplus b_3,$

$b_1 \oplus b_5, b_2 \oplus b_4 \oplus b_5, b_1 \oplus b_3 \oplus b_4, b_3 \oplus b_5, b_2 \oplus b_4, b_1 \oplus b_3.$

b_{31} = Ø, де Ø – пуста множина.

На основі даного співвідношення на рис. 3 показаний принцип формування 5-розрядного коду Галуа.

Рис. 3. Формування коду Галуа при *n*=5

Відповідно за даним принципом на основі незвідних поліномів формуються n-розрядні двійкові коди Галуа. Результати досліджень, показані в роботі [3] вказали на ефективність теоретико-числових перетворень із застосуванням теорії полів Галуа, які дозволяють реалізувати швидкі прямі алгоритми обчислень, що зумовлені простотою апаратної реалізації на базі процедур зсуву. Коди поля Галуа володіють одними з кращих характеристик кодової дистанції і кореляційних функцій, а також множинністю алгоритмів декодування, які реалізовуються на основі високорегулярних послідовних структур. Всі 2^n-1 n-розрядні ненульові кодові комбінації послідовності Галуа є результатом циклічного зсуву вихідного ненульового кодового фрагменту і мають однакову вагу, що характеризує їх, як еквідистантні, або симплексні [23].

Складність виконання арифметичних операцій у полях Галуа визначається великою розрядністю операндів та необхідністю порівняння проміжних результатів з модулем n [10]. Відомий метод Монтгомері [11], який полягає у виконанні вказаних операцій за модулем $N>n$, із зведенням всіх проміжних результатів r, більших або рівних N за модулем n. N вибирають зручним для аналізу умови $r<N$. Недоліками методу є

низька швидкодія довгих комбінаційних схем додавання необхідного для зведення за модулем n невизначеність часу обчислення (для різних проміжних результатів модулів) від 0 до 4 зведень за модулем n. Тому актуальним є задача прискорення обчислень за методом Монтгомері, стабілізації часу обчислень та переходу від математичної до логічної реалізації.

У скінченних полях Галуа на основі вищенаведених властивостей визначені алгоритми основних арифметичних модульних, за деяким простим числом p, операцій сумування та множення, на основі яких базуються похідні операції віднімання та ділення. Існуючі алгоритми логарифмування – функцій Якобі-Зеха [23, 24], із додаванням за *mod*2 часткових добутків та кодів поправок, на основі регістрів зсуву із зворотними зв'язками, двійкових векторів та поліномів, розкладу за нормальним базисом в окремих випадках мають досить 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 [15].

Так, процедура виконання арифметичних операцій в полях Галуа визначається правилами додавання, віднімання, множення, ділення над відповідними поліномами по модулю *P*.

При цьому операція множення реалізується у вигляді згортки двох многочленів:

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

Операція згортки послідовно починається зі старших розрядів за k – тактів. Результат згортки отримує вигляд:

$$A(x)\cdot H(x) = a_{k-1}\cdot h_{r-1}x^{r-2} + (a_{k-2}\cdot h_{r-1} + a_{k-1}\cdot h_{r-2})x^{k+r-3} + (a_{k-3}\cdot h_{r-1} + a_{k-2} + a_{k-1}\cdot h_{r-1})\cdot x^{k+r-3} + \ldots$$

$$+ (a_2 h_2 + a_1 h_1 + a_0 h_0)\cdot x^2 + (a_0 h_1 + a_1 h_0)\cdot x + a_0 h_0.$$

Важливою перевагою такої рекурсивної процедури множення є простота реалізації процесора на регістрах зсуву [24].

Здійснення арифметичних операцій в полі Галуа характеризується різною формою подання двох операндів. Перший операнд подається у вигляді коду, а другий – у вигляді логічних рівнянь, які визначають операції над значенням коду першого операнда[23].

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

Незважаючи на те, що код Галуа є непозиційним, в цьому коді існує правило операцій рекурсивного зсуву, які дозволяють виконувати арифметичні дії та обчислення над двійковими числами – полями кодів.

Найбільш компактні кодові матриці формують системи ортогональних функцій базисів Радемахера, Крестенсона та Галуа. При чому кожен з названих базисів породжує окрему систему числення, які використовуються для реалізації арифметики відповідних універсальних та спеціальних процесорів. Висока популярність та широке застосування базису Радемахера ґрунтується на достатньо простій реалізації арифметики позиційної двійкової системи числення, яка включає шість базових операцій [19]:

1) додавання «+»;
2) зсув «⟶ ⟵»;
3) множення «× »;
4) рівності «=»;
5) знакова (старшинства) «< >»;
6) віднімання «-»;
7) ділення «/»;
8) модульна «*mod*».

З метою підвищення ефективності міжбазисних перетворень запропонована бінарно-розмежована система числення залишкових класів (БРСЗК) [26].

Важливе значення, також, має програмно-апаратна, структурна та алгоритмічна складність міжбазисних перетворень в середовищі досліджуваних ТЧБ.

Дослідження та оцінка функціональних можливостей реалізації арифметики та базових функцій над числами в базисах Радемахера, Крестенсона та Галуа.

Порівняльна оцінка функціональних можливостей досліджуваних ТЧБ подана в табл. 1.

Таблиця 1

Функціональні можливості досліджуваних ТЧБ

№	Базові операції	Радемахер	Крестенсон	Галуа	БРСЗК
1	Додавання	2*nv*	*v*	3*v*	*v*
2	Зсув	*v*	-	2*v*	*v*
3	Множення	2*v*(2n+1)	*v*	?	?
4	Рівності	*v*	*v*	*v*	*v*
5	Знакова(старшинства)	*nv*	?	?	*nv*
6	Віднімання	*(3n+5)v*	?	?	2nv
7	Ділення	n^2v	?	-	?
8	Модульна	n^2v	*2nv*	?	2*nv*

В таблиці 2 n – розрядність представлення чисел, а v – тривалість спрацювання мікроелектронного

обладнання. Перспективними для дослідження являються лічильники, що дозволять отримати залишки чисел в різних теоретико-числових базисах.

Роздільна здатність такого лічильника, тобто мінімальний інтервал між вхідними імпульсами, дорівнює одному періоду тактових імпульсів. Зверху ніяких обмежень на проміжок часу між сусідніми вхідними імпульсами немає. Час встановлення нового коду на всіх розрядах регістра, що входить у лічильник (на виходах *Вих. тр.),* дорівнює одному періоду тактових імпульсів $i_{вст}=T$. Час видачі сигналу 2^n-1, про заповнення лічильника з моменту надходження останнього, вихідного імпульсу дорівнює $0,5T$ [25].Важливою перевагою лічильника на основі регістра зі зворотними зв'язками є також те, що тут практично відсутні обмеження на кількість розрядів, поєднуваних однією загальною структурою (однією групою лічильника). Час видачі сигналу про заповнення лічильника при використанні двоступінчастої схеми І збільшиться лише на $0,5T$, тобто стане рівним T.

За економічністю структури лічильник на основі регістра з функціональними зворотними зв'язками значно кращий, ніж лічильники, побудовані по «класичній» схемі з застосуванням T-тригерів [25]. Викладене дозволяє зробити висновок, що розглянутий лічильник є у синхронній системі найбільш зручною і доцільною для застосування структурою, особливо корисною в тих випадках, коли потрібна висока швидкодія.

Вихідна послідовність даного типу лічильників є псевдовипадковою величиною, оскільки структура лічильника Галуа є аналогічною до структур генераторів M-послідовностей, що будуються на базі регістрів зсуву зі зворотними зв'язками. Системні характеристики синхронних лічильників в різних теоретико-числових базисах представлено в табл. 2.

Таблиця 2

Системні характеристики синхронних лічильників в різних теоретико-числових базисах.

Базис	**Час видачі сигналу**	**Кількість кодових комбінацій**	**Кількість елементів І-НЕ**	**Регулярність структури**	**Вихідний код**
1	2	*3*	4	5	6
Унітарний	$t=T$	$N=n$	$K=8n+2$	так	Паралельний /послідовний
Хаара	$t=T$	$N=n$	$K=4n$	так	паралельний
Крейга	$t=T$	$N=2\cdot n$	$K=4n$	так	Паралельний /послідовний
Радемахера	$t=2T$	$N=2^n$	$K=8n+2$ *(n-2)*	ні	паралельний
Крестенсона	$t=2T$	$N=\prod_{i=1}^{m} P_i$	$K=\left[\sum_{i=1}^{n}\left(\hat{E}(\log_2 P_i)\right)\cdot 8+2\cdot\hat{E}(\log_2 P_i)-2\right]$	ні	паралельний
Галуа	$t=0.5T$	$N=2^n$-1	$K=4n+4$	так	Паралельний /послідовний

На рис. 4 представлено порівняльну гістограму ефективності синхронних лічильників в різних кодових базисах, побудовану за табл. 2. Як видно рис. 5, найбільш ефективні системні характеристики лічильника базису Галуа, що зумовлює доцільність подальших досліджень і пошуку використання цифрових пристроїв даного типу. Незважаючи на те, що код Галуа є непозиційним, в цьому коді існує правило операцій рекурсивного зсуву, які дозволяють виконувати арифметичні дії та обчислення над двійковими числами – полями кодів.

Дослідження лічильників для визначення залишків в різних теоретико-числових базисах

Створення спецпроцесорів опрацювання багаторозрядних чисел у базисі Крестенсона потребує схемотехнічної реалізації спеціалізованих компонентів: лічильників по модулю P; аналого-цифрових перетворень базису Крестенсона [16, 17]; шифраторів Радемахера-Крестенсона [19]; рандомізаторів по модулю p_i.

Вказані модульні компоненти спецпроцесорів досліджуваного класу можуть бути з різною ефективністю реалізовані на основі алгоритмічного та схемо-технічного виконання у різних теоретико-числових базисах (ТЧБ) згідно заданих критеріїв мінімальної апаратної та часової складності в залежності від типу обчислювальних задач.

Тому створення цих компонентів спецпроцесорів у базисі Крестенсона потребує теоретико-математичної формалізації алгоритмів виконання операцій такими цифровими пристроями та оптимізації їх програмно-апаратних, функціонально-структурних та схемо технічних рішень.

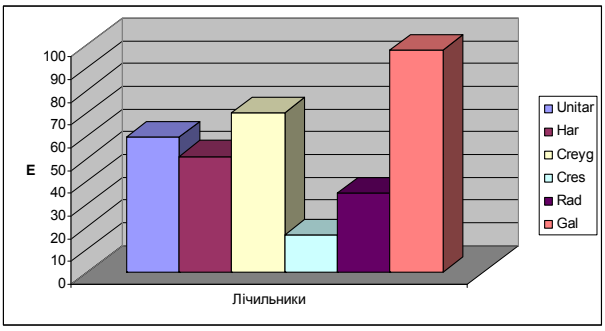


Рис. 4. Ефективність синхронних лічильників в різних кодових базисах

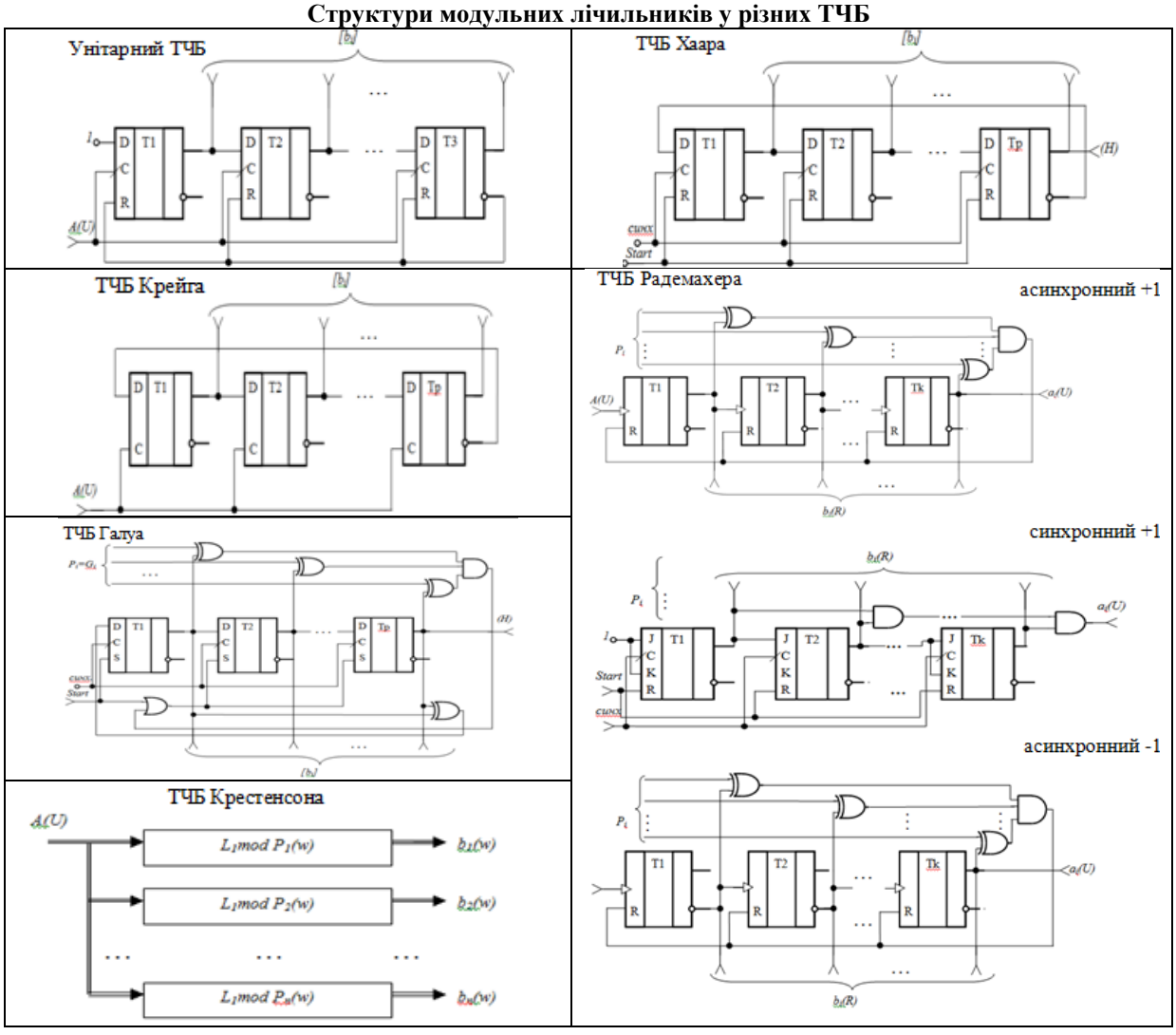
Таблиця 3

Модульні лічильники у різних ТЧБ

ТЧБ	Асинхронні	Синхронні
Унітарний	-	+1
Хаара	-	+1
Крейга	-	+1
Радемахера	+1, -1	+1
Галуа	-	+1, -1
Крестенсона	+1, -1	+1

Таблиця 4

Структури модульних лічильників у різних ТЧБ



Алгоритм даного класу пристроїв отримання залишків по модулю реалізується для ТЧБ унітарного, Хаара, Крейга та Радемахера згідно виразів:

$$b_i(U) = resA(U)(\mathrm{mod}\, P_i(U)),$$

де b_i – код залишку у відповідному ТЧБ; $A(U)$ – унітарний код числа з якого отримується залишок по модулю P_i; P_i =(2, 3,..., U-1) – ціле число; $b_i(H) = resA(U)(\mathrm{mod}\, P_i(H))$ – Хаара; $b_i(K) = resA(U)(\mathrm{mod}\, P_i(R))$ – Крейга; $b_i(R) = resA(U)(\mathrm{mod}\, P_i(R))$ – Радемахера.

У загальному випадку обчислення залишку та рангу числа A на основі модульного лічильника у ТЧБ (w) описується виразами:

$$A = a_i \cdot P_i + b_i;\ \ b_i(w) = resA(U)(\mathrm{mod}\, P_i(w));\ \ a_i(U) = \left(\frac{A - b_i}{P_i}\right)(U),$$

де $b_i(w)$ – паралельний код залишку числа A по модулю P_i у ТЧБ (w); $a_i(U)$ – унітарний код рангу числа

A по модулю P_i у ТЧБ (*w*). Алгоритм обчислення залишку у ТЧБ Галуа виконується згідно виразу :

$$G_{i+1} = res(x_i \cdot G_i \oplus x_{i-1} \cdot G_{i-1} \oplus ... \oplus x_{i-n} \cdot G_{i-n}) \bmod 2,$$

де $x_i\ x_{i-1}\ x_{i-n}$ – незвідний поліном (ключ) поля Галуа $G\begin{pmatrix} n \\ 2 \end{pmatrix}$.

При цьому, особливістю ТЧБ Галуа є те, що, на відміну від інших базисів, на паралельному виході лічильника Галуа формується паралельний бінарний код залишку, а на послідовному виході формується послідовний біт-орієнтовний код Галуа залишку. Реалізація відповідного модульного лічильника виконується на базі синхронних *D*-тригерів згідно значенню модуля P_i заданого у коді Галуа, що забезпечує високу швидкодію даного класу процесорних модулів і меншу апаратну складність по відношенню до синхронних пристроїв визначення залишку у базисі Радемахера.

Алгоритм обчислення залишку на основі модульних лічильників базису Крестенсона реалізується згідно виразів:

$$b_i(C) = res(U)(\bmod P_i(C)), \text{ якщо } P_i = P_i^2(R);$$

$$C_k = \begin{cases} 1, & (b_i + b_j) = P_1 + 1, \\ 2, & (b_i + b_j) = P_2 + 2, \\ ... & \\ k, & (b_i + b_j) = P_1 + k, \\ ... & \\ P-1, & (b_i + b_j) = P + (P-1), \end{cases}$$

тобто $C(b_1(w), b_2(w), ..., b_j(w), ..., b_k(w)) = resA(U) \bmod(P_1(w), P_2(w), ..., P_j(w), ..., P_k(w))$, якщо $P_i = \prod_{j=1}^{k} P_j$.

В табл. 5 представленні формули обчислення відповідних характеристик синхронних лічильників де n – розрядність лічильника; A – апаратні затрати; T – часові затрати; *DR* – *D*-тригер з додатковим входом *R*; *D* – *D*-тригер; *DS* – D-тригер з додатковим входом S; *вик.АБО* – виключаюче *АБО*; *ЛЕ* – логічний елемент; *JKR* – *JK*-тригер з додатковим входом *R*. Також для обчислення характеристик лічильника в базисі Крестенсона було встановлено умову, що кодування в діапазоні *n*, будуть використовуватися 4 модуля однакової розрядності (розрядність модуля *n*/2).

Таблиця 5

Дослідження апаратних та часових затрат при проектуванні синхронних лічильників в різних ТЧБ

ТЧБ	**Формула обчислення апаратних затрат синхронних лічильників в різних ТЧБ**	**Формула обчислення часових затрат синхронних лічильників в різних ТЧБ**
Унітарний	$A_{Uni} = A_{DR} \cdot n$	$T_{Uni} = T_{DR} \cdot n$
Хаара	$A_{Har} = A_{DR} \cdot n$	$T_{Har} = T_{DR} \cdot n$
Крейга	$A_{Kre} = A_D \cdot n$	$T_{Kre} = T_D \cdot n$
Галуа	$A_{Gal} = (A_{DS} + A_{вик.АБО}) \cdot n + (A_{вик.АБО} + 2 \cdot A_{ЛЕ})$	$T_{Gal} = T_{DS} \cdot n + T_{вик.АБО} + T_{ЛЕ}$
Радемахера	$A_{Rad} = A_{JKR} \cdot n + A_{ЛЕ} \cdot (n-1)$	$T_{Rad} = T_{JKR} \cdot n + T_{ЛЕ}$
Крестенсона	$A_{Krs} = 4 \cdot (A_{JKR} \cdot n + A_{ЛЕ} \cdot (n-1))$	$T_{Krs} = T_{JKR} \cdot n + T_{ЛЕ}$

Відповідно до таблиці в якій представлені формула обчислення апаратних та часових затрат синхронних лічильників в різних ТЧБ побудовані графіки представлені на рис. 5 та рис. 6.

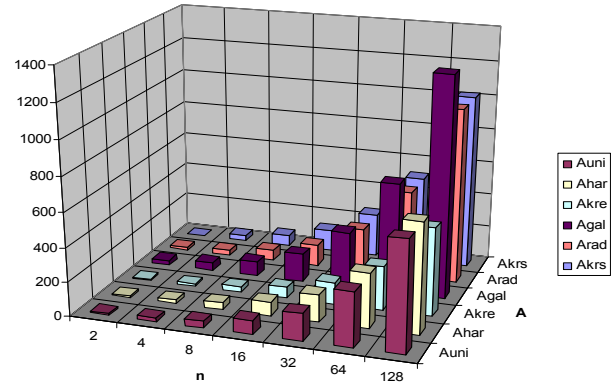


Рис. 5. Апаратні затрати синхронних модульних лічильників в різних ТЧБ

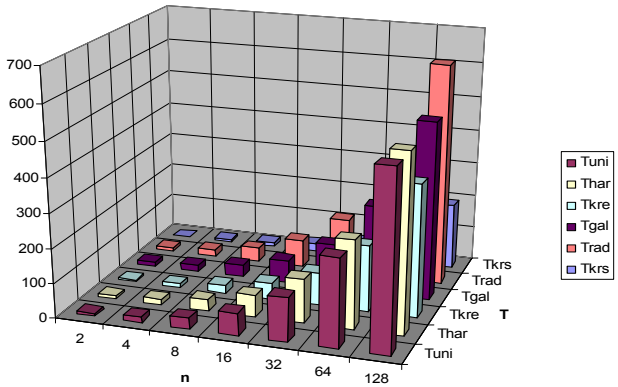


Рис. 6. Часові затрати синхронних модульних лічильників в різних ТЧБ

Досліджені апаратні та часові затрати модульних лічильників демонструють перевагу в часових затрат та деякий ріст апаратних для лічильника базису Крестенсона в порівнянні з лічильниками в інших ТЧБ і хоча він є не ефективними для реалізації міжбазисного перетворення Радемахера-Крестенсона, але його реалізація та аналогічних лічильників в інших ТЧБ дають наглядний приклад можливості застосування лічильників в якості компонента міжбазисного перетворювача для відповідних ТЧБ.

Висновки

В статті проведений аналіз теоретичних основ базисів Крестеннсона та Галуа, як одних з найперспективніших шляхів для реалізації швидкодіючих процесорів опрацювання даних, оскільки вони характеризуються найкомпактнішими кодовими матрицями. Досліджено принципи виконання арифметичних операцій та їх характеристик системами числення, що утворюються на основі досліджуваних базисів. Також в статті проведено дослідження системні характеристики синхронних лічильників в різних теоретико-числових базисах та розроблено модульні лічильники. Проведено дослідження апаратних та часових затрат для роботи відповідних лічильників.

Отримані результати досліджень доводять можливість використання модульних лічильників як компонента міжбазисного перетворення Радемахера-Крестенсона та демонструють можливість інтеграції СЗК в інші ТЧБ, оскільки побудовані лічильники дозволяють отримати основний елемент відповідної системи числення – залишок.

Література

1. Flynn M. Some Computer Organizations and Their Effectiveness / M. Flynn // IEEE Trans. Computers. – 1972. –Vol. 21. No. 9. – pp. 948–960.

2. Хокни Р. Параллельные ЭВМ. Архитектура, программирование и алгоритмы / Р. Хокни, К. Джессхоуп. – М. : Радио и свіязь, 1986. – 392 с.

3. Майоров С.А. Принципы организации цифровых машин / С.А. Майоров, Г.И. Новиков. – Л. : Машиностроение, 1974. – 432 с.

4. Глушков В.М. Основы безбумажной информатики / В.М. Глушков. – М. : Наука, 1987. – 552 с.

5. Палагин А.В. Опыт разработки микропроцессорных распределенных систем реального времени / А.В. Палагин, Я.Н. Николайчук. – К. : Знание, 1988. – 19 с.

6. Справочник по цифровой вычислительной технике: Процессоры и пам'ять / [Б.Н. Малиновский, Е.И. Брюхович, Е.Л. Денисенко и др.] ; под ред. Б.Н. Малиновского. – К. : Техника, 1979. – 366 с.

7. Самофалов К.Г. Цифровые ЭВМ / К.Г. Самофалов, В.И. Корнейчук, В.П. Тарасенко. – К. : Выща школа, 1989. – 424 с.

8. Дунець Р.Б. Арифметичні основи комп'ютерної техніки : [навч. посіб.] / Р.Б. Дунець, О.Т. Кудрявцев.
– Львів : Ліга-Прес, 2006. – 142 с.

9. Черкаський М.В. Складність пристрою керування / М.В. Черкаський, Мурад Хуссей Халіл // Вісник Національного університету "Львівська політехніка". – Львів, 2004. – № 521. – С. 3–7.

10. Николайчук Я.М. Теорія джерел інформації / Я.М. Николайчук. – Тернопіль : ТзОВ "Терно-граф", 2010. – 536 с. – (Видання друге, виправлене).

11. Глухов В.С. Спеціалізований однорозрядний процесор для захисту інформації в гарантоздатних системах / В.С. Глухов, М.В. Ногаль // Радіолектроніка і комп'ютерні системи. – 2008. – № 5(32). – С. 103–109.

12. Акушский И.Я. Машинная арифметика в остаточных класах / И.Я. Акушский, Д.И. Юдицкий. – М. : Сов.радио, 1968. – 440 с.

13. Computer technologies in information security : monograph / [Petro Humenniy and others] ; edited by Valeriy Zadiraka, Yaroslav Nykolaichuk. – Ternopil : Kart-blansh, 2015. – P. 387.

14. Заставний О.М. Теорія та принципи побудови спецпропесора на основі базисів Радемахера, Крестенсона, Галуа / О.М. Заставний, Я.М. Николайчук, Н.Д. Круцкевич, Р.І. Король // Тези доповідей сьомої міжнародної науково-технічної конф. – Вінниця : УНІВЕРСУМ – Вінниця, 2003 – С. 114.

15. Яцків Н.Г. Спецпроцесори обробки даних на основі перетворення Крестенсона-Галуа / Н.Г. Яцків, Р.І. Король, В.В. Яцків, Т.Г. Федчишин // Вісник Технологічного університету Поділля. – 2003. – № 3. – С. 105–108.

16. Николайчук Я.М. Теоретичні основи побудови спецпроцесорів у базисі Крестенсона / Я.М. Николайчук, О.І. Волинський, С.В. Кулина // Вісник Хмельницького національного університету – 2007. – Т. 1, № 3 (93). – С. 85–90.

17. Николайчук Я.М. Проектування спеціалізованих ком'ютерних систем : [навч. посіб. для втузів] / Я.М. Николайчук, Н.Я. Возна, І.Р. Пітух. – Т. : Тено-граф, 2010. – 392 с.

18. Патент на корисну модель № 83756 Україна, МПК G06F 1/00. Спосіб паралельного доступу до пам'яті колективного користування / Я.М. Николайчук, П.В. Гуменний. – опуб. 25.09.2013, бюл. № 18.

19. Николайчук Я.М. Швидкодіючий алгоритм та процесор порівняння чисел у системі залишкових класів / Я.М. Николайчук, О.І Волинський, С.В. Кулина // Искусственный интеллект : науково-теоретичний журнал. ІПШІ МОН і НАН України "Наука і освіта". – 2008. – № 3. – С. 348–352.

20. Advanced Micro Devices, AMD – Processor Homepage [Електронний ресурс]. – Режим доступу : http://amd.com.

21. Николайчук Я.М. Теоретичні основи побудови та структура спецпроцесорів в базисі Крестенсона / Я.М. Николайчук, О.І Волинський, С.В. Кулина // Вісник Хмельницького національного університету.
– 2007. – № 3. Т. 1. – С. 85–90.

22. Мельник А.О. Архітектура комп'ютера : наукове видання / А.О. Мельник. – Луцьк : Волинська обласна друкарня, 2008. – 470 с.

23. Николайчук Я.М. Теоретичні засади та принципи побудови арифметико-логічного пристрою на основі вертикально-інформаційної технології / Я.М. Николайчук, О.М. Заставний, П.В. Гуменний // Вісник Хмельницького національного технічного університету. – 2012. – № 2. – С. 190–197.

24. Гуменний П.В. Функціональна структура спецпроцесора вертикально-інформаційної технології та його компоненти / П.В. Гуменний, Я.М. Николайчук // Вісник національного університету "Львівська політехніка". – 2012. – № 745. – С. 69–77.

25. Гуменний П.В. Аналіз архітектури лічильників, вертикально-інформаційна технологія у різних теоретико-числових базисах / П.В. Гуменний // Інформаційні проблеми комп'ютерних систем юриспруденції, енергетики, економіки, моделювання, та управління (ПНМК) : матеріали міжнародної проблемної наукової міжгалузевої конференції. – 2011. – № 7. – С. 62–67.

26. Волинський О.І. Розмежована система числення залишкових класів та спецпроцеси на її основі / О.І. Волинський, І.З. Якименко // Збірник праць Бучацького інституту менеджменту і аудиту. – Бучач, 2010. – Т. 1, № 6. – С. 80–83.

Рецензія/Peer review : 25.7.2016 р. Надрукована/Printed : 26.8.2016 р.
Рецензент: д.т.н., професор Я.М. Николайчук