Эдвардса над конечным полем. *Сучасний захист інформації.* 2011. № 4. С. 33–36.
6. Kovalchuk L., Bessalov A. Exact Number of Elliptic Curves in the Canonical Form, Which are isomorphic to Edwards Curves over Prime field. *Cybernetics and Systems Analysis.* 2015. Vol. 51. I. 2. P. 165–172.
7. Ковальчук Л. В., Бессалов А. В., Беспалов А. Ю. Алгоритм генерации базовой точки кривой Эдвардса с использованием критериев делимости точки. *Кибернетика и системный анализ.* 2016. Т. 52. № 5. С. 14–24.
8. Бессалов А. В., Цыганкова О. В. Новые свойства кривой Эдвардса над простым полем. *Радиотехника*. 2015. № 180. С. 137–143.
9. Державний стандарт України ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. Київ, 2003.

Edwards curves are considered which have no points of the order eight. The description is given for all subgroups and all correspondent adjacement classes.

Key words: *Edwards curve, subgroup, adjacement classes.*

Одержано 28.02.2017

УДК 004.383.3

Р. Б. Трембач*, канд. техн. наук, доцент,
Б. Р. Трембач,** аспірант,
А. І. Сидор*,** аспірант,
Г. В. Возна*,** студентка

* Тернопільський національний технічний університет імені І. Пулюя, м. Тернопіль,
** Національний університет «Львівська політехніка», м. Львів,
*** Тернопільський національний економічний університет, м. Тернопіль

СТРУКТУРА ТА СИСТЕМНІ ХАРАКТЕРИСТИКИ СПЕЦПРОЦЕСОРІВ ВИЗНАЧЕННЯ ХЕММІНГОВОЇ ВІДДАЛІ РЕАЛІЗОВАНИХ В РІЗНИХ ТЕОРЕТИКО-ЧИСЛОВИХ БАЗИСАХ

В роботі розглядається структура та системні характеристики компонентів багаторозрядних спецпроцесорів. Розроблено спецпроцесор сканування та визначення Хеммінгової віддалі між кодами представленими в унітарному теоретико-числовому базисі перетворення у двійковий код Радемахера.

Ключові слова: *спецпроцесор, теоретико-числовий базис, Хеммінгова віддаль.*

Вступ. Теоретичні основи елементної бази структурних та функціональних компонентів універсальних цифрових процесорів та спецпроцесорів закладені в багатьох роботах відомих вчених та спе-

 © Р. Б. Трембач, Б. Р. Трембач, А. І. Сидор, Г. В. Возна, 2017

ціалістів у галузі мікроелектроніки та цифрової техніки. Актуальною науковою задачею є створення високопродуктивних багаторозрядних спецпроцесорів, що визначають Хеммінгову віддаль між двома сигналами $x(t)$ та $y(t)$ або їх цифровими кодами у різних теоретико-числових базисах (ТЧБ) [1, 2]. При побудові компонентів таких процесорів однією з найважливіших задач оптимізації їх системних характеристик є досягнення максимальної швидкодії. Важливим компонентом при цьому є багаторозрядний суматор двійкової системи числення. Він є базовим елементом в акумуляторах, арифметико-логічних пристроях та пристроях модульної арифметики: квадраторах, векторно-матричних перемножувачах та пристроях модульного експоненціювання процесорів шифрування даних. Отже, оптимізація системних характеристик структурної, апаратної та часової складності однорозрядних та багаторозрядних суматорів спецпроцесорів визначення Хеммінгової віддалі є актуальною науково-технічною задачею. При цьому можуть бути успішно вирішені прикладні задачі теорії розпізнавання образів, пеленгації джерел акустичних сигналів.

Визначення оцінки Хеммінгової віддалі між сигналами у цифровій формі виконується згідно виразу:

$$d_{ij} = \sum \left| x_i - y_i \right| .$$

Незалежно від застосованого коду ТЧБ, для реалізації алгоритму обчислення Хеммінгової віддалі, необхідне виконання наступних операцій:

1) аналого-цифрове перетворення сигналів $x(t)$ та $y(t)$;
2) логічне порівняння атрибутів кодових представлень x_i та y_i ;
3) визначення суми, числа співпадань значень атрибутів x_i та y_i;
4) шифрування коду отриманої суми у відповідному ТЧБ.

У загальному випадку логічне порівняння однорозрядних кодів x_i та y_i виконується на основі застосування двовходового логічного елемента «Виключаюче АБО», який є базовим компонентом одно розрядних неповних та повних комбінаційних суматорів базису Радемахера.

Оптимізація системних характеристик компонентів процесорів визначення Хеммінгової віддалі виконується згідно наступних критеріїв:

$$A = \sum_{j=1}^{m} V_j \ ; \ \tau = \sum_{j=1}^{m} V_j \ ; \ k_c = \sum_{i=1}^{n} \alpha_i P_i \ ,$$

де A — апаратна складність визначається числом логічних елементів або вентилів мікроелектронної реалізації; τ — часова складність визначається сумарною затримкою сигналів у максимальному числі послідовно з'єднаних вентилів, k_c — структурна складність визначається коефі-

цієнтом структурної складності згідно виразу включає α_i — вагові коефіцієнти експертних оцінок інформативності компонентів атрибутів поліфункціональних даних (ПФД), P_i — параметри атрибутів ПФД.

Визначення Хеммінгової віддалі можна виконувати безпосередньо над двійковими кодами базису Радемахера. У цьому випадку розрядність кодів для обчислення Хеммінгової віддалі зменшується до величини $\log_2 n$ у порівняні з унітарним ТЧБ.

Спецпроцесор, який виконує операцію визначення Хеммінгової віддалі реалізується на основі багаторозрядного суматора.

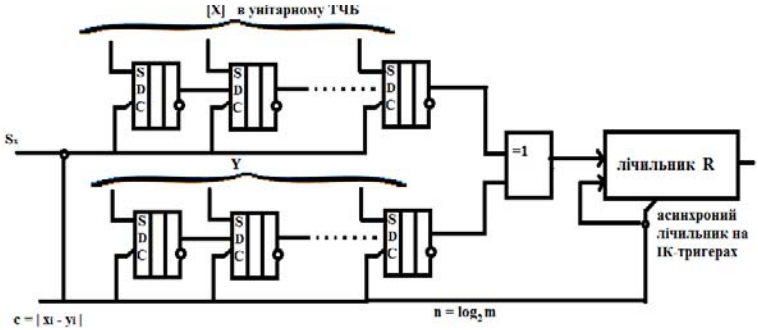

Рис. 1. *Спецпроцесор сканування та визначення Хеммінгової віддалі між кодами представленими в унітарному ТЧБ перетворення у двійковий код Радемахера*

Функціональними обмеженнями такої структури спец процесора є низька швидкодія, оскільки для визначення Хеммінгової віддалі у двійковому коді базиса Радемахера потрібно виконати *n* зсувів інформаційних кодів у регістрах, реалізованих на *D*-тригерах. При цьому часова складність, обумовлена затримкою сигналів у *D*-тригерах, логічному елементі «Виключаюче АБО» та двійковому лічильнику складає: $\tau = 2 \cdot 2^n + 4 + 2$. При $n = 8$ отримаємо $\tau = 2 \cdot 2^8 + 4 + 2 = 518\nu$ (мікротактів).

Перспективним рішенням створення спецпроцесора визначення Хеммінгової віддалі є його схемо технічна реалізація у кодах базиса Радемахера.

Відомий пристрій визначення Хеммінгової віддалі шляхом додавання багаторозрядних двійкових чисел, визначення залишку по модулю багаторозрядного числа, який містить вхідну і вихідну шини, які є відповідно *m*-розрядними входами і *n*-розрядними виходами пристрою, в кожному розряді пристрою міститься однорозрядний суматор та *D*-тригер, вхід якого з'єднаний з відповідним розрядом вхідної шини, входи синхронізації об'єднані між собою і є другим

входом пристрою, вихід суми найстаршого розряду суматора з'єднаний з третім входом мультиплексора [3].

Недоліком такого пристрою є обмежені функціональні можливості обумовлені тим, що він здійснює визначення модульної різниці між двома двійковими числами тільки у випадку коли перше більше число представлене прямим двійковим кодом, а друге менше число, яке представлене доповнюючим кодом і не дозволяє накопичувати усереднене значення суми вибірки двох потоків двійкових чисел.

Інший відомий пристрій, який може виконувати функції визначення Хеммінгової віддалі, містить n-розрядну вхідну шину, $k+m$-розрядну вихідну шину, $k+m$-розрядний накопичуючий суматор, виходи якого з'єднані з першими входами $k+m$-розрядного паралельного регістра, другий вхід якого з'єднаний з входом синхронізації запису, а виходи з'єднанні з входами накопичуючого суматора і з виходами пристрою [4].

Недоліком такого пристрою є обмежені функціональні можливості обумовлені тим, що даний пристрій не дозволяє накопичувати усереднене значення модульних різниць вибірки двох потоків двійкових чисел.

Суть запропонованого схемо технічного рішення спец процесора визначення Хеммінгової віддалі полягає у тому, що для накопичення усередненої суми модульних різниць двох потоків двійкових чисел здійснюється одночасне додавання їх прямих та доповнюючи кодів у двох додатково введених суматорах, логікою переносу старшого розряду одного з суматорів та мультиплексором визначаються прямі коди модульних різниць між двома двійковими числами, які додаються n разів у накопичувальному суматорі та шляхом віднімання n — числа молодших розрядів формується вихідний m-розрядний двійковий код оцінки Хеммінгової віддалі між двома дискретизованими випадковими процесами ($m = \log_2 n$).

На рис. 2 показана схема пристрою, де: 1 — вхідна $2k$-розрядна шина ($a_0, a_1, ..., a_{n-1}$ та $b_0, b_1, ..., b_{n-1}$ — відповідні входи x_i та y_i багаторозрядних двійкових чисел); 2 — вихідна $k+m$-розрядна шина; 3 — $k+m$-розрядний накопичуючий суматор; 4 — $k+m$-розрядний паралельний регістр; 5 — перший вхід синхронізації запису; 6 — другий вхід синхронізації скиду у нуль; 7 — третій вхід синхронізації запису; 8 — D-тригери $2k$-розрядного паралельного регістра; 9.1 та 9.2 — однорозрядні повні суматори відповідно першого та другого k-розрядних суматорів; 10 — вхід логічної одиниці; 11 — розрядні компоненти мультиплексора; 12 — вхід логічного нуля.

Пристрій працює наступним чином. На початку роботи пристрою після подачі сигналу синхронізації у вигляді фронту наростання на вхід синхронізації 6 скиду у нуль $k+m$-розрядного паралельного регістра 4 на вихідній $k+m$-розрядній шині 2 формується двійкове

число нуль, яке також поступає на перші входи $k+m$-розрядного накопичуючого суматора 3.

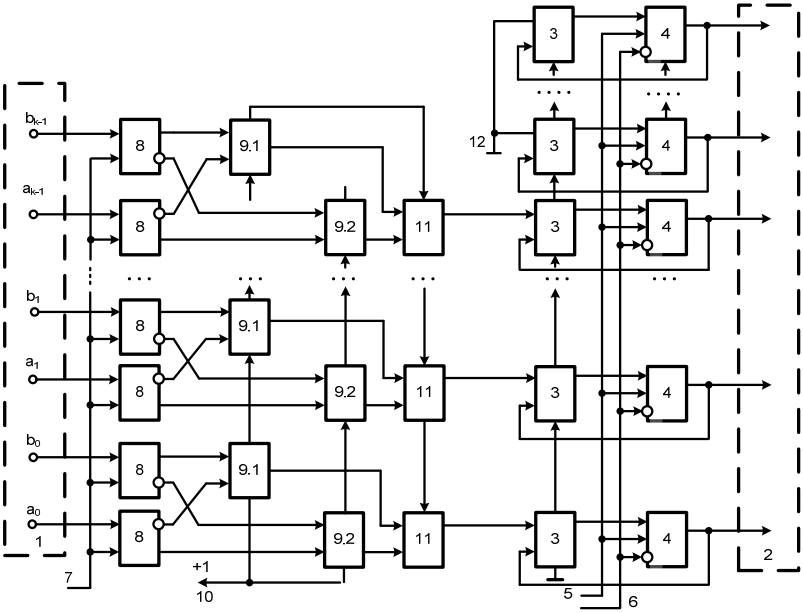

Рис. 2. *Структурна схема спец процесора визначення Хеммінгової віддалі у ТЧБ Радемахера*

Після подачі аналогічного сигналу на вхід синхронізації 7 вхідні двійкові числа x_i та y_i записуються у *D*-тригери *2k*-розрядного паралельного регістра. Вихідні прямі та інверсні коди тригерів подаються на відповідні перші та другі входи першого 9.1 та другого 9.2 *k*-розрядних суматорів. У результаті логічними сигналами переносу у старшому розряді суматора 9.1, який поступає на керуючий вхід мультиплексора на його виходах формуються прямі коди модульних різниць між двома двійковими числами $|x_i - y_i|$, які подаються на входи $k+m$-розрядного накопичуючого суматора 3, де додаються до коду, який сформований на виходах $k+m$-розрядного паралельного регістра 4, а отримана на виходах суматора 3 сума записується і запам'ятовується у регістрі 4. Після *n*-циклів роботи пристрою, отриманий у регістрі 4 код суми модульних різниць двійкових чисел надходить на вихідну $k+m$-розрядну шину у вигляді $k + m - n$-розрядного двійкового коду, починаючи зі старших розрядів паралельного регістра 4.

Наявність додаткового входу логічної одиниці на входах переносу нульових розрядів суматорів 9.1 та 9.2 дозволяє одночасно з формуван-

ням зворотніх кодів двійкових чисел $\overline{x}_i$ та $\overline{y}_i$ на інверсних виходах *D*-тригерів 2*k*-розрядного паралельного регістра 8 формувати їх доповнюючі коди на входах суматорів 9 без додаткових операцій.

Якщо на виході переносу старшого розряду суматора 9.1 формується логічна «1» , це означає, що число $x_i > y_i$ і на виході першого суматора 9.1 формується код модульної різниці $|x_i - y_i|$, який з виходу мультиплексора поступає на другі входи накопичуючого суматора 3. Якщо на такому виході формується логічний «0», це означає що число $x_i < y_i$, то на виході суматора 9.1 формується результат у вигляді доповнюючого коду, який не поступає на вихід мультиплексора 11. При цьому на вихід мультиплексора 11 поступає прямий код модульної різниці $|x_i - y_i|$ сформований на виході суматора 9.2.

Наприклад: $x_i = 11_{(10)} = 1011_{(2)}$; $y_i = 17_{(10)} = 10001_{(2)}$.

Нехай $x_i - y_i$, тоді число x_i представляється у прямому нормалізованому коді з фіксованою комою, а y_i у доповнюючому коді

$$x_i = 0,01011\,;\ [y_i]_{доп} = 1,01111\,.$$

Додаємо $x_i + [y_i]_{доп} = 0,01011 + 1,01111 = 1,11010$.

Тобто результат від'ємний у доповнюючому коді, оскільки у знаковому розряді одиниця і такий код не поступає на вихід мультиплексора 11.

Нехай $y_i - x_i$, тоді число y_i представляється у прямому нормалізованому коді з фіксованою комою, а x_i у доповнюючому коді

$$y_i = 0,10001\,;\ [x_i]_{доп} = 1,10101\,.$$

Додаємо $y_i + [x_i]_{доп} = 0,10001 + 1,10101 = 0,00110$.

Тобто результат додатний у прямому коді оскільки у знаковому розряді нуль і цей код відповідає модульній різниці $|x_i - y_i|$ і поступає на вихід мультиплексора 11.

Таким чином, запропонований пристрій характеризується розширеними функціональними можливостями, оскільки забезпечується визначення усередненого значення суми модульних різниць вибірки двох потоків двійкових чисел незалежно від того, яке з чисел більше або менше.

Розрахунок часової складності для запропонованого спецпроцесора складає: $\tau = \tau_{P1} + n \cdot \tau_C + \tau_{MП} + 2n \cdot \tau_{HC} + \tau_{P2}$. При $n = 8$, отримаємо: $\tau = 2 + 8 + 3 + 16 + 2 = 31\nu$.

Висновки. Наведені критерії оптимізації системних характеристик схемотехнічних рішень мікроелектронних компонентів спецпроцесорів. Досліджені структурні рішення існуючих обчислювальних засобів обчи-

слення Хеммінгової віддалі в унітарному базисі та базисі Радемахера. Запропонована структура високопродуктивного спецпроцесора визначення Хеммінгової віддалі у ТЧБ Радемахера та оцінена його часова складність, яка зменшена у 16 разів у порівнянні з відомими пристроями.

Список використаних джерел:

1. Николайчук Я. М. Коди поля Галуа. Тернопіль: ТзОВ «Терно граф». 2012. 576 с.
2. Николайчук Я. М., Заведюк Т. О. Структура та функції рекурентного біонейрона для розпізнання образів у Хеммінговому просторі. *Збірник наукових праць Бучацького інституту менеджменту і аудиту*. Бучач. 2010. № 6. С. 37–40.
3. Николайчук Я. М., Кімак В. Л., Волинський О. І., Круліковський Б. Б. Пристрій визначення залишку по модулю багаторозрядного числа. Патент України на корисну модель № 90144, Бюл. № 9, 2014.
4. Устройство для суммирования. [Електронний ресурс]. Режим доступу: http//www.findpatent.ru/patent/254/2546569.html.).

In this paper the structure and components of multi-system characteristics special processors. Developed special processor scans and definition Hemmingi distance between codes presented in unitary theoretical and numerical basis conversion to binary code Rademacher.

Key words: *special processor, theoretical and numerical basis, Hemming distance.*

Одержано 16.02.2017

УДК 681.3.06

Г. З. Халімов, д-р техн. наук

Харківський національний університет радіоелектроніки, м. Харків

АНАЛІЗ СКЛАДНОСТІ РЕАЛІЗАЦІЙ КРИПТОСИСТЕМ НА ГРУПАХ

Представлений порівняльний аналіз реалізацій криптосистем на групах. Показано, що побудова криптосистем на групах вимагає ефективного алгоритму для відображень числа на групу і зворотного відображення з обчислювально простою груповою операцією. До теперішнього часу відома тільки одна реалізація криптосистеми MST_3, побудованої за Абелевим центром групи Судзукі.

Ключові слова: *логарифмічний підпис, криптосистеми PGM, MST_1, MST_2, MST_3.*

Вступ. Криптографія з відкритим ключем будується на складності розв'язання математичних проблем, які дуже часто, але не виключно, виникають з теорії чисел. На початку 80-х років, було запропоновано

 © Г. З. Халімов, 2017