3. Hansen J. P., Stichtenoth H. Group codes on certain algebraic curves with many rational points. AAECC. 1990. N 1. P. 67–77.
4. Халимов Г. З., Котух Е. В. Универсальное хеширование по кривым Сузуки. Журнал *«Прикладная радиоэлектроника»*. Харьков: ХНУРЭ. 2011. Том. 10. № 2. С. 164–170.
5. Pedersen J. P. A function field related to the Ree group. Lecture Notes Mathematics. 1992. Vol. 1518. P. 122–131.

This paper presents the results of universal hashing for curves that are associated with curves Delihne Lustig on extensions of the finite field. An asymptotic comparative estimates of the collision probability of universal hashing are obtained. Evaluation shows that the best result is achieved on the Ri curve over a field of characteristic 3 with parameters $q = 3q_0^2$ and $q_0 = 3^m$.

Key words: *universal hashing, group Suzuki, Suzuki curves, Ri curves, Hermite curves.*

Одержано 15.02.2017

УДК 681.32

Б. Б. Круліковський*, канд. техн. наук, доцент,
Н. Я. Возна,** канд. техн. наук, доцент,
В. М. Грига*,** канд. техн. наук,
А. Я. Давлетова,** аспірантка

*Національний університет водного господарства
та природокористування, м. Рівне,
**Тернопільський національний економічний університет, м. Тернопіль,
***Прикарпатський національний університет
імені Василя Стефаника, м. Івано-Франківськ

ОПТИМІЗАЦІЯ СТРУКТУРНИХ РІШЕНЬ КОМБІНАЦІЙНИХ СУМАТОРІВ ЗГІДНО КРИТЕРІЇВ МІНІМАЛЬНОЇ ЧАСОВОЇ, АПАРАТНОЇ ТА СТРУКТУРНОЇ СКЛАДНОСТІ

Запропонована структура суматора з прискореним переносом для виконання операції додавання двійкових чисел у базисі Радемахера. Виконано мікроелектронну реалізацію запропонованого суматора з прискореним переносом на ПЛІС. В результаті синтезу на ПЛІС відомого та запропонованого суматорів з прискореним переносом отримано характеристики складності, які співпадають з теоретичними розрахунками.

Ключові слова: *суматор з прискореним переносом, базис Радемахера, ПЛІС, САПР, інкрементний суматор.*

Вступ. Традиційно, при розробці компонентів процесорів обчислювальної техніки критерієм оптимальності вважалися мінімальна апаратна та часова складність [1]. Для успішного розвитку цього на-

пряму були розроблені потужні методи мінімізації структур обчислювальних засобів на основі булевої алгебри-логіки.

Сучасні високі досягнення в галузі мікроелектроніки, теорії алгоритмів, програмних засобів САПР, нанотехнологій визначають новий напрям оптимізації характеристик компонентів обчислювальних засобів. При цьому найважливішим критерієм є забезпечення максимальної швидкодії виконання обчислювальних операцій.

Виконання цього критерію особливо важливе при зростанні розрядності процесорів в діапазоні 64, 128, 256, …, 2048 біт, які використовуються в задачах шифрування масивів даних. Таким чином, з'явилася необхідність переглянути класичні структури компонентів процесорів, що реалізуються на логічних елементах з метою синтезу структур, які забезпечують максимально потенційні можливості підвищення швидкодії.

Наприклад, при розрядності процесорів 64 біт та затримці сигналів в однорозрядних повних суматорах на 3–5 мікротактів, число мікроопераций додавання двох двійкових чисел такої розрядності складає $64 \cdot 3 \div 5 = 192 \div 320\upsilon$. У процесорах 1024 — 2048 біт затримка сигналів відповідно складає 2072 — 5120 або 6144 — 10240 мікротактів. При виконанні операції множення, наприклад, двох 64-розрядних двійкових чисел у класичному матричному перемножувачі Брауна, затримка сигналів складає $127 \cdot 3 \div 5 = 381 \div 635\upsilon$.

Викладене обгрунтовує актуальність синтезу мікроелектронних структур компонентів, які працюють у двійковій арифметиці базису Радемахера згідно критерію досягнення їх максимальної швидкодії незалежно від оцінок апаратної складності при заданій розрядності процесорів.

1. Синтез структури швидкодіючого однорозрядного напівсуматора. Вдосконалення однорозрядного напівсуматора шляхом спрощення структури та мікроелектронної реалізації логічного елемента «Виключаюче АБО» на логічному елементі І-НЕ та АБО, виходи яких об'єднані і реалізують логічний елемент «Провідне І», дозволяє зменшити апаратну складність до трьох логічних елементів, тобто у 2–3 рази та підвищити швидкодію переключення за 1 мікротакт, тобто у 3 рази у порівнянні з відомими аналогами [2, 3].

Структура однорозрядного напівсуматора показана на рис. 1.

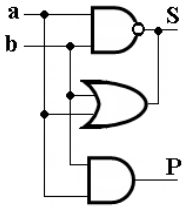
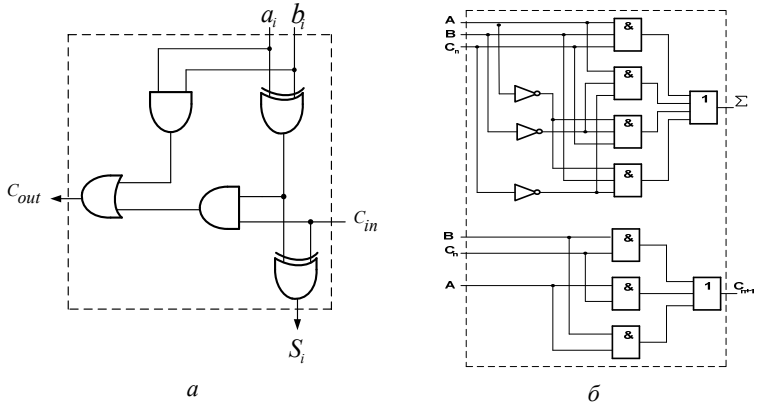


Рис. 1. *Структура однорозрядного напівсуматора*

Використання логічних елементів реалізованих на мікроелектронній технології ЕЗЛ передбачає наявність транзисторів на виходах логічних елементів І-НЕ та АБО, що дозволяє об'єднувати їх виходи без втрати функціональності та реалізувати логічний елемент «Провідне І» [4].

2. Синтез структури багаторозрядного суматора з прискореним переносом (СПП). При класичній реалізації m-розрядних суматорів значним недоліком є велика апаратна складність, яка обумовлена наявністю великого числа компонентів, які реалізують комбінаційну структуру пристрою на логічних елементах, число яких швидко зростає при збільшенні розрядності суматора.

Низька швидкодія відомих структур СПП [5, 6] обумовлена сумарною затримкою сигналів наскрізного переносу між m-розрядними суматорами, починаючи з другого. Наприклад, при розрядності пристрою $n = 32$ біт і $m = 4$ загальна затримка сигналів переносу у такому суматорі з прискореним переносом складає $\tau = 7\tau_{МП} + 4\tau_{СМ}$, де $\tau_{МП}$ — затримка сигналів в однофазному 4-розрядному мультиплексорі ($\tau_{МП} = 3\nu$ мікротакти), який містить три послідовно з'єднаних логічних елементи (НЕ $\rightarrow$ І $\rightarrow$ АБО), $\tau_{СМ}$ — затримка сигналів у першому 4-розрядному двійковому суматорі ($\tau_{СМ} = 8\nu$ мікротактів), при застосуванні однорозрядних суматорів згідно структур показаних на рис. 2, що складає загальну затримку сигналів у пристрої на $\tau = (7 \times 3) + 8 = 29\upsilon$.



а *б*

Рис. 2. *Структура повного однорозрядного суматора на:*
а — елементах «Виключаюче АБО» та б — елементах АБО-І-НЕ

Структура *n*-розрядного суматора з прискореним переносом, на прикладі $m = 4$ -розрядних суматорів показана на рис. 3.

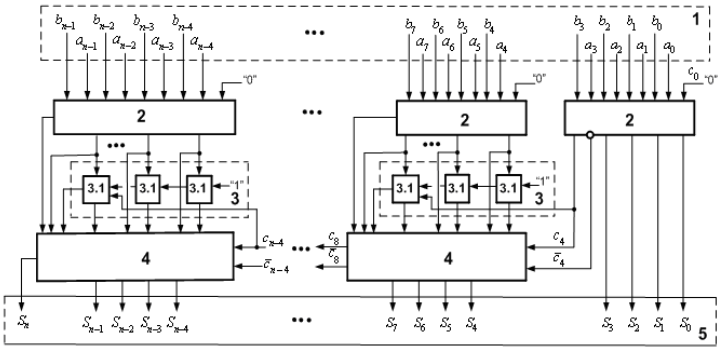


Рис. 3. *Суматор з прискореним переносом*

Суматор з прискореним переносом включає у себе: 1 — вхідну 2^n-розрядну шину; 2 — n/m, m-розрядних суматорів; 3 — m-розрядний інкрементний суматор (рис. 4); 4 — $m + 1$-розрядний мультиплексор з парафазними керуючими входами (рис. 5); 5 — вихідну $n + 1$-розрядну шину.

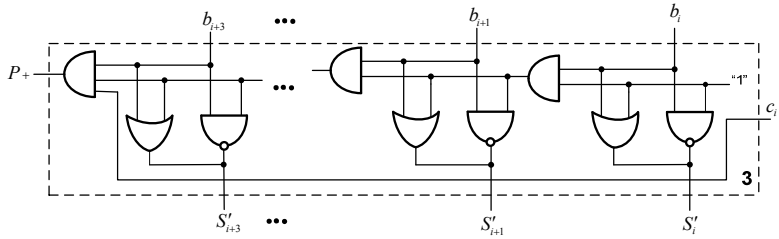


Рис. 4. *Інкрементний суматор*

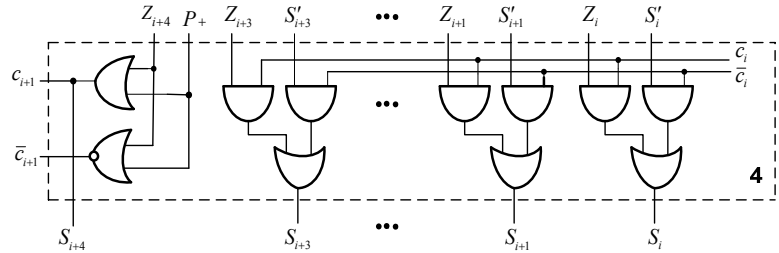


Рис. 5. *Мультиплексор*

Апаратна складність такого суматора з прискореним переносом розраховується згідно виразу: $A = A_{C0} + A_{C1} + A_{MП}$, де A_{C0} — апаратна складність всіх m-розрядних пірамідальних суматорів 2 (рис. 6) з входами логічного нуля; A_{C1} — апаратна складність всіх m-розрядних інкрементних суматорів 3 з входами логічної одиниці

(рис. 4); $A_{МП}$ — апаратна складність мультиплексора 4 з парафазними керуючими входами та виходами (рис. 5).

При $n = 32$ і $m = 4$, отримаємо $A = 8A_{C0} + 7A_{C1} + 7A_{МП}$.

Апаратна складність інкрементного суматора (рис. 4): $A_{C1} = 1 + (3 \times 3) = 10$.

Апаратна складність мультиплексора (рис. 5): $A_{МП} = (3 \times 4) + 2 = 14$.

Апаратна складність пірамідального суматора (рис. 6): $A_{C0} = 10 \times 3 + 1 = 31$.

Таким чином оцінка загальної апаратної складності суматора з прискореним переносом складає:

$A = (8 \times 31) + (7 \times 10) + (7 \times 14) = 416$ логічних елементи.

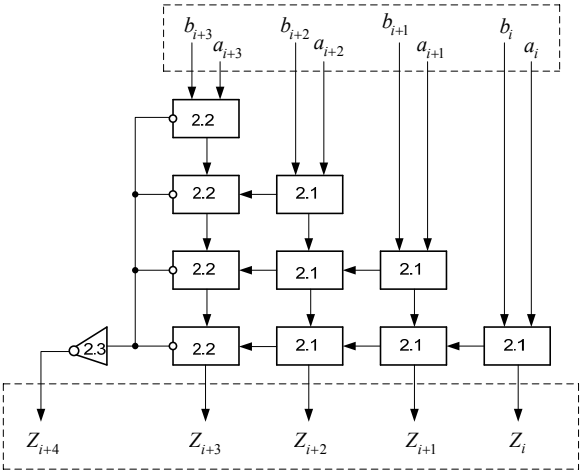
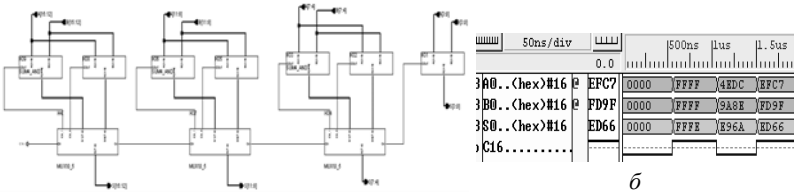


Рис. 6. *Пірамідальна структура суматора*

Часова складність суматора з прискореним переносом, в якому затримка сигналів у першому 4-розрядному суматорі 2 з пірамідальною структурою (рис. 5), в якому застосовані неповні однорозрядні суматори з затримкою сигналів переносу на 1 мікротакт (рис. 1), а також затримкою сигналів у вихідному інверторі 2.3 (рис. 5) складає 5 мікротактів та затримкою сигналів у мультиплексорах з парафазними входами на 2 мікротакти, загальна затримка сигналів у запропонованому суматорі при $n = 32$ біти і $m = 4$ буде рівна $\tau = (n/m - 1) \times \tau_{МП} + \tau_{СМ}$. Тобто, $\tau = (7 \times 2) + 5 = 19\nu$.

Отже, зменшення апаратної складності запропонованого суматора з прискореним переносом по відношенню до прототипа складає 842/416=2 рази, а збільшення швидкодії складає 29/19=1.5 рази.

3. Результати мікроелектронної реалізації та синтезу СПП на ПЛІС. На рис. 7 показано схемотехнічну реалізацію відомого 16-ти розрядного СПП [6] та функціональну діаграму його роботи.

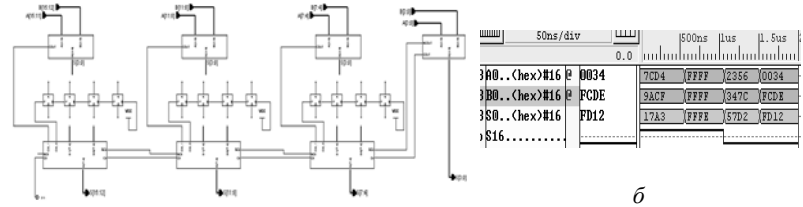


а *б*

Рис. 7. *а — схемотехнічна реалізація відомого СПП та б — його функціональна діаграма роботи*

Дана структура відомого 16-ти розрядного СПП складається з 5-ти 4-розрядних класичних суматорів та 3-ох мультиплексорів, які мають 10 однорозрядних інформаційних входів та 5 однорозрядних інформаційних виходів. Керування даними мультиплексорами здійснюється сигналами вихідних переносів перших 5-ти 4-розрядних суматорів c4, c8 та c12 відповідно. На функціональній діаграмі показано результати додавання 16-ти розрядних чисел поданих на вхідні шини A і B, результат суми формується на шині S. C16 — вихідний перенос СПП.

На рис. 8 показано схемотехнічну реалізацію запропонованого СПП та функціональну діаграму його роботи.



а *б*

Рис. 8. *а — схемотехнічна реалізація запропонованого СПП та б — його функціональна діаграма роботи*

Дана структура запропонованого 16-ти розрядного СПП складається з 4-х 4-розрядних пірамідальних суматорів, 3-х інкрементних суматорів та 3-х мультиплексорів, які мають 10 однорозрядних інформаційних входів та 5 однорозрядних інформаційних виходів. Керування даними мультиплексорами здійснюється прямими та інверсними сигналами вихідних переносів перших 3-х 4-розрядних суматорів. На функціональній діаграмі показано результати додавання 16-ти розрядних чисел поданих на вхідні шини A і B, результат суми формується на шині S. S16 — вихідний перенос СПП.

В таблиці 1 наведено результати синтезу відомого та запропонованого СПП на ПЛІС фірми Xilinx.

Таблиця

Результати синтезу СПП на ПЛІС фірми Xilinx

Назва кристалу ПЛІС	Відомий СПП		Власний СПП	
	Кількість блоків ПЛІС (LUTs)	Тактова частота, МГц	Кількість блоків ПЛІС (LUTs)	Тактова частота, МГц
Spartan 3E (XC35500)	643 (6%)	161,4	338 (3%)	227,8

Отримані значення затрат обладнання і тактової частоти реалізованих СПП є наближеними до значень апаратної і часової складності даних СПП розрахованих аналітичним способом.

Висновки. Виконаний синтез та аналіз системних характеристик часової та апаратної складності однорозрядних та багаторозрядних комбінаційних суматорів теоретико-числового базису Радемахера. Запропоновані нові схемо технічні рішення системно-оптимізованих одно розрядних та багато розрядних суматорів з прискореним переносом, які характеризуються підвищеною у 1,5 рази швидкодією та зменшеною у 2 рази апаратною складністю у порівнянні з відомими схемо технічними рішеннями у ТЧБ Радемахера.

Список використаних джерел:

1. Николайчук Я. М., Возна Н. Я., Пітух Р. І. Проектування спеціалізованих комп'ютерних систем: навч. посіб. Тернопіль: Терно-граф, 2010. 392 с.
2. Шило В. Л. Популярные цифрове микросхемы: Справочник. М: Радио и связь, 1988. 352 с.
3. Карцев М. А. Арифметика цифровых машин. М.: Наука, 1969.
4. Круліковський Б. Б., Давлетова А. Я., Николайчук Я. М., Грига В. М. Архітектура та системні характеристики однорозрядних суматорів на логічних елементах І-НЕ. Матеріали конференції *«Інформаційно-обчислювальні технології, автоматика та електротехніка»*. Рівне, 2016. С. 137–1139.
5. Патент на корисну модель UA № 97162 Бюл. № 5, 2015.
6. Режим доступу: http://phg.su/basis2/x133.HTM.

The proposed structure of the adder accelerated transition for adding operation binary numbers in the base Rademacher. Done Microelectronic implementation the proposed adder accelerated transition on the FPGA. Been received characteristics of complexity of the known and proposed adders with an accelerated transition by synthesis on FPGA.

Key words: *adder with an accelerated transition, Rademacher's basis, FPGA, CAD, incremental adder.*

Одержано 16.02.2017