SÉRIE „Informační a počítačové systémy“

[https://doi.org/10.52058/2695-1592-2021-1\(1\)-282-295](https://doi.org/10.52058/2695-1592-2021-1(1)-282-295)

Андрій Роговенко

*старший викладач кафедри Інформаційних та комп'ютерних систем
Національного університету «Чернігівська політехніка»
м. Чернігів, Україна, e-mail: ARogovenko@gmail.com,
<https://orcid.org/0000-0003-4594-5692>*

Ірина Якименко

*аспірант кафедри Інформаційних та комп'ютерних систем Національного
університету «Чернігівська політехніка»
м. Чернігів, Україна, e-mail: iryna.yakymenko93@gmail.com,
<https://orcid.org/0000-0002-7778-8831>*

ПОРІВНЯННЯ ЗАСОБІВ ОБЧИСЛЕННЯ ДАНИХ В СИСТЕМАХ РОЗПОДІЛЕНОЇ ОБРОБКИ ІНФОРМАЦІЇ

Анотація. Запропоновано та проаналізовано результати реалізації засобів обчислення даних для систем розподіленої обробки, які базуються на основі обчислювальних структур для обчислення суми за змінним модулем.

Для побудови зазначених структур використано один з варіантів реалізації оснований на одновимірних каскадах конструктивних модулів, які забезпечують високу продуктивність при помірній обчислювальній складності.

Запропоновано варіанти адаптації засобів обчислення за допомогою методів з використанням прискорення сигналу переносу SUB, ланцюга частково-групового переносу, та гібридної схеми переносу.

Визначені затримки обчислення результату та кількість необхідних ресурсів для реалізацій засобів обчислення, на основі яких було доведено, що запропоновані реалізації надають змогу адаптувати структуру обчислювача на основі суматора за модулем до вимог конкретної задачі.

Відмічено, що в запропонованих структурах засобів обчислення даних можливо досягати зменшення показників затримки сигналів переносу за рахунок

адаптації до вимог задачі, що потенційно дає можливість збільшення швидкості обчислення операцій в декілька разів.

Зазначено, що використання запропонованих засобів обчислення в сучасних мобільних пристроях зв'язку, дає змогу спростити складність реалізації при збільшенні показників продуктивності, що в свою чергу дозволяє задовольнити одну з вимог галузі системах розподіленої обробки інформації, зокрема в телекомунікаційних.

Ключові слова: засоби обчислення даних, розподілені системи, суматор за модулем, схеми переносу, адаптовані структури.

Andrew Rogovenko

*Senior Lecturer, Department of Information and Computer Systems,
Chernihiv Polytechnic National University,
Chernihiv, Ukraine, e-mail: ARogovenko@gmail.com,
<https://orcid.org/0000-0003-4594-5692>*

Iryna Yakymenko

*Phd student, Department of Information and Computer Systems,
Chernihiv Polytechnic National University,
Chernihiv, Ukraine, e-mail: irynayakymenko93@gmail.com,
<https://orcid.org/0000-0002-7778-8831>*

COMPARISON OF DATA CALCULATION MEANS IN DISTRIBUTED INFORMATION PROCESSING SYSTEMS

Abstract. The results of realization of data calculation means for distributed processing systems, which are based on computational structures for calculation of the sum on the variable module, are offered and analyzed.

To build these structures used one of the implementation options based on one-dimensional cascades of structural modules that provide high performance with moderate computational complexity.

Variants of adaptation of computational means by means of methods using SUB transfer signal acceleration, partial-group transfer circuit, and hybrid transfer scheme are offered.

The delays in calculating the result and the number of necessary resources for the implementation of computing tools are determined, on the basis of which it was proved that the proposed implementations allow to adapt the structure of the calculator based on the adder modulo to the requirements of a particular task.

It is noted that in the proposed structures of data computing tools it is possible to reduce the delay of transfer signals by adapting to the requirements of the problem, which potentially allows to increase the speed of computing operations several times.

It is noted that the use of the proposed computing tools in modern mobile communication devices, simplifies the complexity of implementation by increasing performance, which in turn allows to meet one of the requirements of distributed information processing systems industry, in particular in telecommunications.

Keywords: data computing tools, distributed systems, modulator adder, transfer schemes, adapted structures.

Постановка проблеми. В розподілених системах, зокрема телекомунікаційних при обчисленні даних, операції в скінчених полях займають суттєву частину обчислювального процесу, в яких базовою є операція додавання за модулем. Таким чином, прискорення виконання операції додавання за модулем приведе до прискорення обчислень загалом. В скінченому полі $GF(P)$ операція додавання визначається як операція додавання за модулем простого числа $Z=(X+Y) \bmod P$, і є базовою для реалізації операцій множення та піднесення до степеня. Вказані операції мають широке практичне застосування, наприклад, в завадостійкому кодуванні та криптографічних перетвореннях, які є невід'ємною частиною розподілених систем. З розвитком технологій все більшу практичну значимість набуває перенесення складних операцій з програмної в апаратну реалізацію, що потребує пошуку ефективних структур по таких загальноприйнятих критеріях як продуктивність та обчислювальні витрати.

Аналіз останніх досліджень та публікацій. Загальноприйнятим методом реалізації додавання за змінним модулем є послідовне виконання наступних операцій над двійковими числами – $S=X+Y$, $S1=S-P$, та вибору в якості результату значення S або $S1$ в залежності від результату віднімання. В [1] запропоновано метод реалізації операції додавання в полі $GF(P)$ на регулярній логічній мережі лінійної складності від кількості розрядів чисел X та Y , де фактично операції додавання, віднімання та вибору виконуються одночасно. Як і у випадку двійкового суматора, суматор за змінним модулем формується як ланцюг однорозрядних суматорів – однонаправлений каскад конструктивних модулів (ОККМ), де на кожний однорозрядний суматор (конструктивний модуль – КМ) поступають значення поточного розряду чисел X, Y та P . (рис.1).

Крім того на кожний однорозрядний суматор поступають сигнали узагальненого переносу з боку молодших та з боку старших розрядів. КМ реалізується трьома комбінаційними схемами (КС), на першій із них формується значення розряду результату як булева функція від значень поточних розрядів аргументів та значень сигналів узагальненого переносу як з боку молодших так і з боку старших розрядів. Очевидно, що суматор за змінним модулем також є комбінаційною схемою.

У роботах [2], [3], [4], [5] були запропоновані методи підвищення швидкодії або зменшення апаратних ресурсів суматора на основі одновимірного каскаду конструктивних модулів.

Мета статті. Порівняти запропоновані засоби обчислень для систем розподіленої обробки, які базуються на основі обчислювальних структур для обчислення суми за змінним модулем. Дослідити варіанти адаптації засобів обчислення та визначити затримки обчислення результату та кількість необхідних ресурсів для реалізацій засобів обчислення.

Виклад основного матеріалу. Базисом проектування комбінаційних схем, наприклад в мікросхемах ПЛІС Spartan-6, Virtex – 6 [4], є сукупність будь яких булевих функцій від 6, 7 та 8 змінних, які реалізуються на LUT (LUT – LookUpTable – таблиця перетворення). При цьому на одному LUT можуть бути реалізовані одна функція від 6 змінних, або дві функції від п'яти змінних. В блоках ПЛІС за допомогою мультіплексорів можна реалізувати булеві функції від семи змінних, з використанням 2-х LUT, або від 8 змінних, з використанням 4-х LUT. Реалізація довільної булевої функції від будь якої кількості змінних в такому базисі ґрунтується на розкладі Шеннона. Основним підходом у реалізації суматорів за модулем на основі ОККМ є використання таблиць перетворення у якості складових блоків конструктивного модуля. Оптимальне використання LUT забезпечується при структурному описі, т.я. при поведінковому синтезатор використовує універсальні алгоритми спрощення схеми. При практичному порівнянні поведінкового, та структурного підходів опису конструктивного модуля суматора, отримані результати наведені у таблиці 1 та 2.

Таблиця 1 – Кількість LUT при поведінковому та структурному описах ОККМ

Розрядність	Структурний опис	Поведінковий опис
32	128	199
64	256	401
96	384	612

Таблиця 1 – Кількість LUT при поведінковому та структурному описах ОККМ

128	512	943
160	640	1311

Таблиця 2 – Час обчислення результату при поведінковому та структурному описах ОККМ

Розрядність	Структурний опис	Поведінковий опис
32	40.605	12.6
64	79.509	30.2
96	118.49	62.0
128	157.474	94,15
160	196.458	171.9

У результаті даного експерименту впливає, що при структурному описі схема КМ використовує меншу кількість елементів LUT ніж при поведінковому.

Таким чином, не дивлячись на такі недоліки структурного опису як складність й непереносимість коду між сімействами ПЛІС, структурний опис дає більш оптимальний результат. Виходячи з цього, усі структури для дослідження, надалі будуть реалізовані за допомогою структурного підходу.

Всі експерименти по визначенню кількості ресурсів та часових затримок проводилися на САПР ISE DesignSuite -14.7 від Xilinx, а визначення граничної тактової частоти на XILINX SPARTAN-6 XC6SLX9 FPGA Board від CantonElectronics, за схемою що описана у [3].

Дослідимо суматори на основі базової структури ОККМ, що описані в [1]. Зазначимо що такий суматор складається з однакових конструктивних модулів типу A1, в свою чергу, кожен з яких складається з трьох комбінаційних схем, див рисунок 1. Схеми СС2, та СС3 формують перенос у старші та молодші розряди, а СС1 виконує обчислення цільової функції. Таким чином суматор має регулярну структуру. Умовно віднесемо цю структуру до типу А. Максимальна швидкодія схеми визначається критичним шляхом, тобто шляхом проходження сигналу від входу схеми до її виходу, з найбільшою затримкою.

Рисунок 1 – Критичні шляхи реалізації суматора за змінним модулем на основі одновимірного каскаду конструктивних модулів (тип А)

Максимальна затримка розповсюдження по обом шляхам t_1 та t_2 пропорційна кількості комбінаційних схем, з яких вона утворена. Тобто швидкодія має бути у лінійній залежності від розрядності операндів.

При реалізації суматора типу А у базисі ПЛІС використовується структурний підхід, згідно якому на реалізацію схем CC2 та CC3 витрачається по одному LUT. На обчислення цільової функції 2 LUT.

Досліди проводилися за схемою та алгоритмом описаним у [3].

Таблиця 3 – Характеристики суматора на основі модулів типу А в залежності від розрядності операндів

Розрядність	Кількість LUT	Кількість LUT на bit	Затримка, нс	Частота, МГц
256	1022	3.99	313.409	3,1
512	2046	3.99	625.279	1,5
1024	4094	3.99	1249.029	0,8
2048	8190	3.99	2496.529	0,4

Вочевидь кількість LUT менша ніж розрахунково, це є наслідком оптимізації імплементації найстаршого та наймолодшого модуля, т.я. результати роботи LUT формування переносу не використовуються й тому виключаються зі складу схеми. Характеристики реалізації для розрядностей 256, 512, 1204, 2048 наведені у таблиці 3.

Розглянемо суматор за модулем на основі одновимірного каскаду конструктивних модулів з ланцюгом прискорення переносу сигналу SUB детально описаний у [2], [3]. Умовно віднесемо його структуру до типу В. Такий суматор складається з комірок двох типів В1 та В2 (рисунок 2). Комірка В2 складається з схеми CC1 яка обчислює цільову функцію, та схеми CC3 яка

генерує сигнал SUB. Конструктивний модуль типу B1 складається з схеми CC1, яка аналогічним чином обчислює цільову функцію, та схеми CC2 яка подібно як і у модулі типу A1 формує перенос у старші розряди.

Рисунок 2 – Критичні шляхи реалізації суматора за змінним модулем на основі одновимірного каскаду конструктивних модулів з сигналом SUB (тип B)

Особливості суматора за такою схемою полягають в тому, що втрачається регулярність структури, але зменшується кількість використаних ресурсів. Самий довгий шлях затримки розповсюдження сигналу по каскаду відмічений на рисунку 2. Характеристики реалізації для розрядностей 256, 512, 1204, 2048 наведені у таблиці 4.

Таблиця 4 – Характеристики суматора на основі модулів типу B в залежності від розрядності операндів

Розрядність	Кількість LUT	Кількість LUT на bit	Затримка, нс	Частота, МГц
256	512	2	309,229	3,2
512	1024	2	612,504	1,6
1024	2048	2	1217,836	0,8
2048	4096	2	2431,146	0,4

Розглянемо суматори на основі каскаду конструктивних модулів типу A з ланцюгом групового переносу які описані у [4], [5], [6]. Основу суматора складають модулі типу A1 об'єднані разом з схемою прискореного формування переносу G у групи AG див рисунок 3. У відповідності до [5] перша й остання група не має схеми прискореного переносу G. Загальна структура такого суматора зображена на рисунку 4.

Нижня оцінка затримки на такому суматорі визначається як:

$$T = (2\sqrt{2n})T_{LUT} \quad (1)$$

Верхня оцінка кількості LUT на такому суматорі визначається як:

$$C = 12n - 16(\sqrt{n/2} - 1) - 8\sqrt{2n} \quad (2)$$

Рисунок 3 – Блок групи суматора за модулем з груповим переносом на основі структури типу А

Рисунок 4 – Суматор за модулем з груповим переносом на основі структури типу А

Характеристики реалізації для розрядностей 256, 512, 1204, 2048 наведені у таблиці 5.

Таблиця 5 – Характеристики суматора з груповим переносом на основі структури типу А в залежності від розрядності операндів

Розрядність	Кількість LUT	Кількість LUT на bit	Затримка, нс	Частота, МГц
256	1762	7 - 11	64.667 – 22.174	15,4
512	3584	7	104.793	9,5
1024	7168	7	183.825	5,4
2048	14336	7	346.540	2,8

Для вибору необхідної розрядності слід керуватися рекомендаціями наданими у [3]. А також при виборі балансу продуктивності з витратами ресурсів.

Суматори на основі каскаду конструктивних модулів типу В з ланцюгом групового переносу будуються на основі блоків BG, кожен з яких містить групу суматорів В та модифіковану схему прискореного переносу G. Особливістю цієї схеми є відсутність сигналів переносу у молодші розряди G4. Перенос у молодші розряди виконується сигналом SUB згідно рисунку 2. Таким чином нижня оцінка затримки на такому суматорі буде визначатися як:

$$T = \left(m + \left(\frac{n-1}{m} \right) \right) T_{LUT} \quad (3)$$

Виходячи з формули оптимальне значення кількості модулів A1 об'єднаних у групу буде визначається як:

$$m = \sqrt{n-1} \quad (4)$$

Верхня оцінка кількості LUT на такому суматорі визначається як:

$$C = 12n - 16 \left(\sqrt{n/2} - 1 \right) - 8\sqrt{2n} \quad (5)$$

Функція залежності затримки від розрядності групи має один екстремум, на якому приймає мінімальне значення. Для пошуку точки екстремума знайдемо похідну по m:

$$\frac{dt}{dm} = 2 - \frac{1}{m^2}n \quad (6)$$

Мінімумом буде точка, в якій похідна буде дорівнювати 0:

$$2 - \frac{1}{m^2}n = 0 \quad (7)$$

З виразу 2 аргумент при якому функція мінімальна:

$$m_{min} = \sqrt{\frac{n}{2}} \quad (8)$$

Але слід брати до уваги, що екстремум може знаходитись не в точках розрядності, а між ними, тобто число $m_{\min}$ буде дробовим, а не цілим, а на оптимальне значення розрядності групи буде претендувати два найближчі цілі. Тоді оптимальну розрядність групи можна знайти таким чином:

$$m_{imin} = \operatorname{argmin} t(m_{min}, m_{min}) \quad (9)$$

де m_{imin} – ціле число розрядів групи при якому досягається мінімальна затримка.

Дослідимо схему одновимірного каскаду конструктивних модулів з груповим переносом та сигналом sub складається з k груп неоднорідної структури. Старша група виконує генерацію sub , причому фактично її виконує тільки старший конструктивний модуль у групі, у той час як молодші модулі його тільки використовують. Решта $k-1$ груп використовують сигнал sub для обчислення результату. Розрядність усіх груп прийнята фіксованою й позначається як m .

Рисунок 5 – Блок групи суматора за модулем з груповим переносом на основі структури типу В

Рисунок 6 – Суматор за модулем з груповим переносом на основі структури типу В

Групи молодших розрядів мають відмінності від групи старших розрядів у тому що відсутній конструктивний модуль в якому формується сигнал sub, тобто усі модулі крім старшого у групі старших розрядів, використовують сигнал sub для обчислення результату.

Характеристики реалізації зі завантаження для розрядностей 256, 512, 1204, 2048 наведені в таблиці 5.

Таблиця 5 – Характеристики суматора з груповим переносом на основі структури типу В в залежності від розрядності операндів

Розрядність	Кількість LUT	Кількість LUT на bit	Затримка, нс	Частота, МГц
256	1280	5	64.667	15,4
512	2560	5	104.793	9,5
1024	5120	5	183.825	5,4
2048	10240	5	346.540	2,8

На рисунку 7 приведений порівняльний графік залежностей кількості LUT від розрядності, для наступних реалізацій: 1- суматор на основі базової структури одновимірного каскаду конструктивних модулів, 2 -суматор адаптований за методом введення ланцюгів прискорення переносу сигналу SUB, 3 - суматор адаптований за методом введення групового переносу, 4 - суматор з адаптований за гібридним методом.

Рисунок 7 – Порівняльний графік залежностей кількості LUT від розрядності 1-4 реалізацій.

На рисунку 8 приведений порівняльний графік залежності затримки від

розрядності, для наступних реалізацій: 1- суматор на основі базової структури одновимірного каскаду конструктивних модулів, 2 -суматор адаптований за методом введення ланцюгів прискорення переносу сигналу SUB, 3 - суматор адаптований за методом введення групового переносу, 4 - суматор з адаптований за гібридним методом.

Рисунок 8 – Порівняльний графік залежностей затримки від розрядності 1-4 реалізацій

В результаті дослідження було запропоновано та проаналізовано чотири варіанти суматорів за модулем. Це суматор на основі базової структури ККМ, суматор адаптований за методом введення ланцюгів прискорення переносу сигналу SUB, суматор адаптований за методом введення групового переносу, та суматор з адаптований за гібридним методом. Перший варіант дозволяє створити суматор з питомим використанням 4 LUT на розряд, та затримкою 1.22 нс на розряд. ККМ с сигналом SUB дозволяє заощадити 2 LUT на кожному розряді та має приблизно таку саму величину затримки (1.2 нс на розряд). Крім того, цей варіант виключає один симетричний ланцюг переносу, й таким чином дозволяє прискорити процес обчислення суми шляхом вибору правильної послідовності завантаження частин слів, але при побудові на основі таких суматорів блоків множення та підведення до степеню за модулем т.я. у цьому випадку слова завантажуються у схему обчислення повністю за один такт синхросигналу.

Прискорити отримання результату дозволяє реалізація ККМ адаптована за методом використання групового переносу, при чому збільшується кількість ресурсів (в експериментах отримано прискорення в 5 разів, при збільшенні використаних ресурсів у 2.5). Ці коефіцієнти можна покращити, якщо дослідним шляхом підібрати найближче значення розрядності групи до екстремуму.

Остання реалізація за швидкодією не поступається попередній, але дозволяє зекономити деяку кількість LUT, що в окремих випадках може бути критичним.

Висновки. Сукупність отриманих результатів дає можливість підбирати метод реалізації за потребами користувача, балансуючи ресурсами ПЛІС та швидкодією за вимогами кінцевої реалізації. Таким чином, виникає змога адаптувати структуру обчислювача на основі суматора за модулем до вимог кожної конкретної реалізації.

В структурах суматорів в скінченному полі $GF(P)$ на основі ОККМ, шляхом подальшого розвитку методів швидкого переносу, які використовуються в традиційних реалізаціях, можливо досягати аналогічних показників затримки сигналів переносу, що потенційно дає принаймні п'ятикратний виграш в швидкості операції додавання.

З огляду на те, що галуззю використання суматорів за змінним модулем є мобільні пристрої зв'язку в сучасних телекомунікаційних системах, таким чином одна з вимог, що полягає в спрощенні складності реалізації при збільшенні показників продуктивності може бути задоволена за допомогою використання запропонованих схем обчислення суми.

Подальші дослідження полягають в розробці блоків обчислення операції множення та підведення до степеню за модулем, які є більш вживані у сучасних телекомунікаційних системах.

Література:

1. Тарасенко В.П. Реалізація операцій в скінчених полях на одновимірному каскаді конструктивних модулів. / В.П. Тарасенко, О.К. Тесленко // Системні дослідження та інформаційні технології. - 2006. - №2 - с.7-17.
2. Тарасенко В. П. Оптимізація апаратних витрат на реалізацію параметричних ядер (soft-cores) для виконання операцій в скінчених полях. / В. П. Тарасенко, О. К. Тесленко, А. І. Роговенко // Радіоелектронні і комп'ютерні системи. - 2009. - № 5. - С. 184–188.
3. Tarasenko V.P., Teslenko O.K., Rogovenko A.I. The performance defining foradders with variable module based on onedimensional cascade of constructional modules. / V.P. Tarasenko, O.K. Teslenko, A.I. Rogovenko // Матеріали міжнародної конференції “Сучасні комп'ютерні системи та мережі: розробка та використання” (ACSN'2009), Львів. - с.11-13.
4. Virtex 7 series FPGA ConfigurableLogicBlock. UserGuide. Xilinx UG474, 2013.
5. Тарасенко В. П. Частково-груповий перенос суматорів у скінченному полі $GF(P)$ / В. П. Тарасенко, О. К. Тесленко, А. І. Роговенко // Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі. - 2013. - № 773. - С. 118-125.
6. Тарасенко В.П., Тесленко О.К., Роговенко А.І. Патент України на корисну модель «КОНСТРУКТИВНИЙ МОДУЛЬ ДОДАВАЧА В ЗАЛИШКАХ З ГРУПОВИМ ПЕРЕНОСОМ» №62946 кл.G06F 7/00 Бюл. №18 від 26.09.11, Власник НТУУ «КПІ»
7. Spartan-6 FPGA Data Sheet: DC and Switching Characteristics, DS162 (v3.1.1) January 30, 2015 Product Specification

References:

1. Tarasenko V.P. & Teslenko O.K. (2006). Realizatsiia operatsii v skinchenykh poliakh na odnovymirnomu kaskadi konstruktyvnykh moduliv. [Implementation of operations in finite fields on a one-dimensional cascade of structural modules]. *Systemni doslidzhennia ta informatsiini tekhnologii*, 2, 7-17 [in Ukrainian].
2. Tarasenko V. P. & Teslenko O. K. & Rogovenko A. I. (2009). Optymizatsiia aparatnykh vytrat na realizatsiiu parametrychnykh yader (soft-cores) dlia vykonannia operatsii v skinchenykh poliakh. [Optimization of hardware costs for the implementation of parametric cores (soft-cores) to perform operations in finite fields]. *Radioelektronni i kompiuterni systemy*, 5, 184–188 [in Ukrainian].
3. Tarasenko V.P. & Teslenko O.K. & Rogovenko A.I. (2009). The performance defining foradders with variable module based on onedimensional cascade of constructional modules. *Materialy mizhnarodnoi konferentsii "Suchasni kompiuterni systemy ta merezhi: rozrobka ta vykorystannia"*. (pp.11-13). Lviv.
4. Virtex 7 series FPGA ConfigurableLogicBlock. UserGuide. Xilinx UG474, 2013.
5. Tarasenko V. P. & Teslenko O. K. & Rogovenko A. I. (2013). Chastkovo-hrupovyi perenos sumatoriv u skinchenomu poli GF(P) [Partial group transfer of adders in a finite field GF (P)]. *Visnyk Natsionalnoho universytetu "Lvivska politekhnika"*. *Kompiuterni systemy ta merezhi*, 773, 118-125 [in Ukrainian].
6. Tarasenko V. P. & Teslenko O. K. & Rogovenko A. I. (2011). Patent Ukrainy na korysnu model «KONSTRUKTYVNYI MODUL DODAVACHA V ZALYShKAKh Z HRUPOVYM PERENOSOM» [Patent of Ukraine for the utility model "CONSTRUCTIVE MODULE OF SUPPLIER IN BALANCES WITH GROUP TRANSFER"].
7. Spartan-6 FPGA Data Sheet: DC and Switching Characteristics, DS162 (v3.1.1) January 30, 2015 Product Specification