УДК 681.32

***Я.М. Николайчук*[1], *О.Б. Посвятовська*[2], *С.В. Івасьєв*[1]**

[1]*Тернопільський національний економічний університет*

[2]*Галицький коледж ім. В. Чорновола*

ПРИСТРІЙ КОМПАКТНОГО КОДУВАННЯ БАГАТОРОЗРЯДНИХ ПРОСТИХ ЧИСЕЛ

Вступ. При реалізації алгоритмів опрацювання багаторозрядних простих чисел в задачах вибору системи взаємно простих модулів для процесорів теоретико числового базису Крестенсона, пошуку найбільшого спільного дільника, виявлення квадратичного лишку, виконання арифметичних операцій модульної арифметики виникає необхідність зберігання та генерування великих масивів багаторозрядних простих чисел[1]. Генерування та зберігання багаторозрядних простих чисел, представлених повнорозрядними двійковими кодами, є неефективним у зв'язку з тим, що потребує великих об'ємів пам'яті.

Метою роботи є дослідження та розробка пристрою компактного кодування багато розрядних простих чисел.

1. Складові пристрою

На основі запропонованого у [2] методу компактного кодування [3] розроблена структурна схема пристрою зберігання та генерування БПЧ, яка показана на рисунку 1.

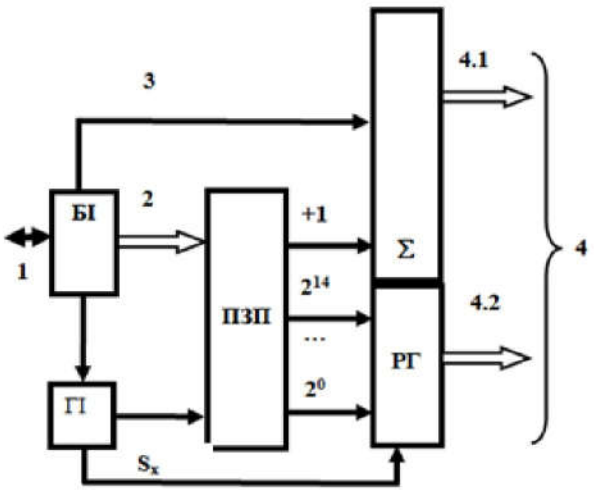

Рисунок 1 – Структурна схема пристрою компактного кодування та генерування багаторозрядного простого числа

Пристрій містить: 1- вхідна інтерфейсна шина; 2 – адресна шина; 3 – шина стартового коду старших розрядів простого числа; 4 – вихідна шина коду БПЧ; +1 – інкрементна одиниця накопичуючого суматора; 2^0-2^{14} – код БПЧ; БІ – блок ініціалізації; ГІ – генератор імпульсів; ПЗП – постійний запам'ятовуючий пристрій; РГ – регістр пам'яті; $\sum$ - багаторозрядний паралельний суматор; 2 – вихідна шина.

В основу пристрою покладено процес зберігання в ПЗП 15 молодших розрядів кодів багаторозрядних простих чисел(БПЧ) та одного розряду – біту синхронізації, на основі якого відбувається інкрементне нарощення старших бітів у суматорі $\sum$, починаючи з 16-го розряду числа у суматорі.

В структурі пристрою функціональні модулі виконують наступні операції: БІ – блок ініціалізації, оснащений інтерфейсною шиною 1, реалізує інформаційний зв'язок з зовнішнім комп'ютерним пристроєм і виконує стартові функції: записує в ПЗП стартовий код 15 біт молодших розрядів БПЧ, а в суматор - багаторозрядний стартовий код старших розрядів БПЧ і запускає генератор імпульсів ГІ.

В процесі генерування імпульсів відбувається інкрементне генерування адресів ПЗП, що забезпечує генерування кодів молодших розрядів БПЧ. У момент появи біта синхронізації на виході ПЗП відбувається інкрементне нарощення кодів суматора.

Перший вихід генератора інкрементує адресацію ПЗП, а другий вихід генератора реалізує запис інформації в регістр та запис стартового коду суматора. На вихідній шині 4 формується послідовність багаторозрядних кодів БПЧ.

В якості ПЗП використовуються кристали флеш-пам'яті з відповідною адресною розрядністю. При цьому, враховуючи, що для запису 15 молодших розрядів БПЧ і біта синхронізації необхідно 2 байти, незалежно від розрядності БПЧ, що забезпечує необхідну компактність зберігання великого об'єму кодів.

Наприклад, при об'ємі флеш-пам'яті 32 ГБ число компактно закодованих та генерованих 32-бітних простих чисел відповідно складатиме $64 \cdot 10^9$ розрядів кодів чисел.

В залежності від розрядності стартового коду розрядність генерованих БПЧ може довільно зростати.

У результаті досягається зменшення об'єму кодів для зберігання БПЧ відповідно в межах 32 розрядів у два рази, для 256 розрядів в 16 разів,

а при 1024 розряди - в 64 рази[3].

У таблиці 1 приведено характеристики та об'єми рекомендованої флеш-пам'яті.

Таблиця 1 – Рекомендовані характеристики флеш-пам'яті, необхідної при реалізації пристрою кодування

Модель пристрою	Характеристики (об'єм / швидкість)
Silicon Power Marvel M01	32 Гб; 5 Гбіт/с.
Transcend JetFlash 350	32 Гб; 5 Гбіт/с.
Kingston DataTraveler SE9 G2	64 Гб; 15 МБ/с.
Kingston DataTraveler 101 G2	128 Гб; 5 МБ/с.

На рисунках 2, 3, показані структури мікроелектронних компонентів пристрою компактного кодування та генерування БПЧ.

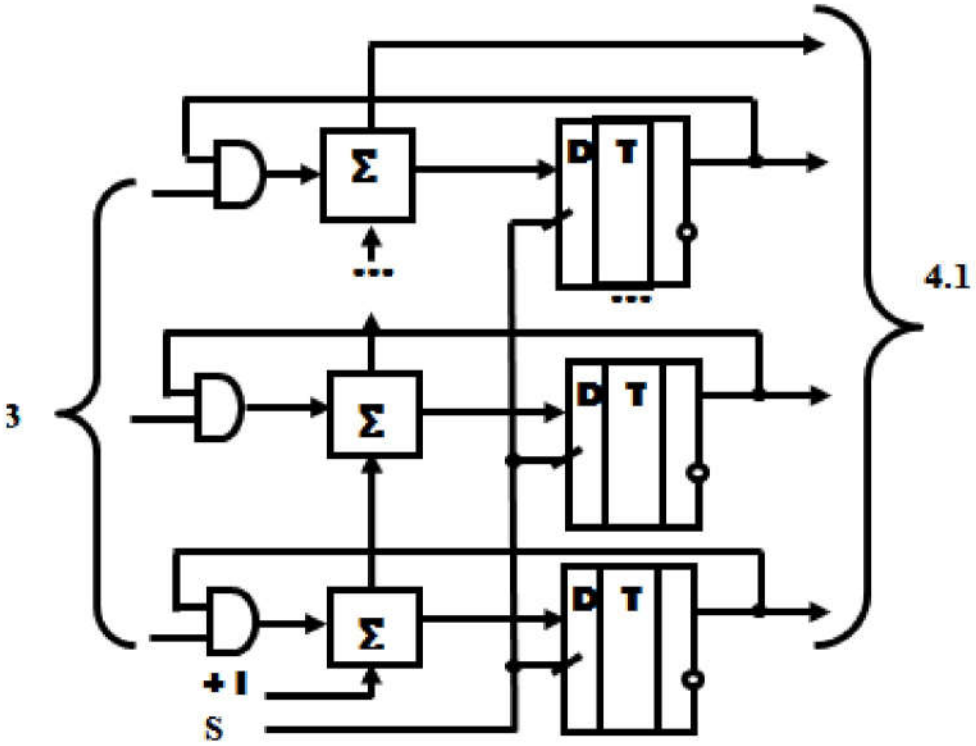

Рисунок 2 - Структурна схема накопичуючого суматора з паралельним 3 та інкрементним +1 входами - формувача старших розрядів БПЧ

Швидкодія структури неповного суматора, представленого на рисунку 4, визначається часом переключення одного логічного елемента, тобто складає 1υ.

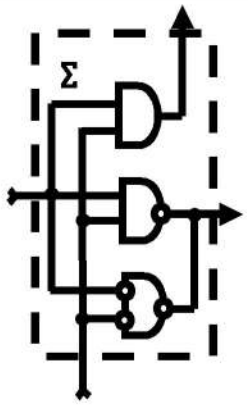

Рисунок 3 - Структура неповного суматора на логічних елементах І, І-НЕ та І-НЕ з інверсними входами

Така реалізація компонента багаторозрядного суматора забезпечує підвищення швидкодії наскрізних переносів у 3 – 5 разів у порівнянні з відомими схемами, які побудовані на логічних елементах І, АБО, НЕ, а також на елементах типу XOR, які в своїй структурі містять п'ять логічних елементів, з яких три з'єднані послідовно.

Розрахунок апаратної складності запропонованих компонентів пристрою компактного кодування та генерування БПЧ у залежності від розрядності розраховується згідно виразу:

$$A = A_{PГ} + A_{\sum}$$

$$A_{PГ} = 15 \cdot A_{\text{DT}} = 15 \cdot 2 = 30\upsilon,$$

де υ - вентилі, які реалізуються на ПЛІС.

$$A_{\sum} = ЛЕ + \text{A}_S + A_{DT},$$

де $\text{A}_S = 3ЛЕ$ - число логічних елементів однорозрядного неповного суматора, звідки

$$A_{\sum} = \text{n}(ЛЕ + 3ЛЕ + 2ЛЕ) = 6\text{n}\upsilon.$$

На рисунку показано характеристики апаратної складності базових компонентів пристрою та зменшення об'єму використовуваної пам'яті при зростанні розрядності БПЧ.

З рисунку видно, що зменшення апаратної складності порівняно з відомими структурами складає півтора-два рази, а об'єм пам'яті при зростанні розрядності БПЧ в межах 32-1024 відповідно зменшується в 2 – 64 рази.

На рисунку 4 показано характеристики часової складності пристрою, які розраховуються на основі параметрів накопичуючого суматора, який

має більше число послідовно з'єднаних елементів $\tau_{PГ} = 2\upsilon$, а $\tau_{\Sigma} = 3n$ нс.

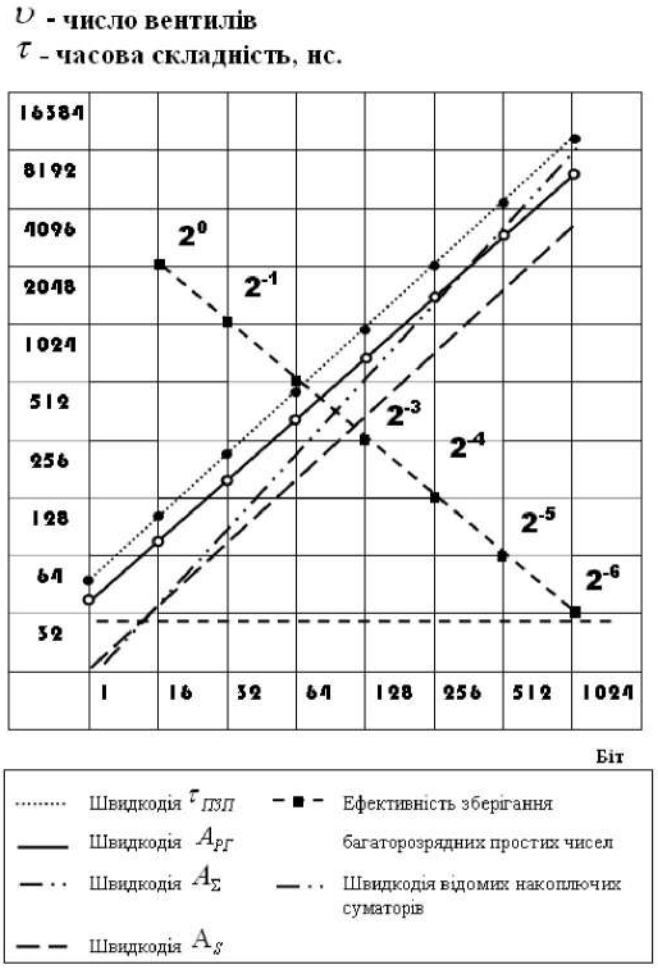

Рисунок 4 - Характеристики часової складності пристрою кодування багаторозрядних чисел та його структурних елементів

Це призводить до зменшення часової складності в більш, ніж два рази в порівнянні з відомими реалізаціями накопичуючих суматорів, часова складність яких складає $\tau_{\Sigma} = 7n$,. Тобто швидкодія розробленого схемотехнічного рішення перевищую аналоги в два рази.

Суттєве підвищення швидкодії пристрою компактного кодування та генерування БПЧ може бути досягнуте застосуванням в якості компонента накопичуючого суматора запропонованого в роботі [3] швидкодіючого багаторозрядного суматора, структура якого показана на рисунку 5.

При цьому часова складність складає $log_2 n$. В той же час, як видно з рисунку 4, його апаратна складність, практично, на порядок вища в порівнянні з розробленим, що може обмежувати доцільність практичного застосування подібного елемента в розробленому пристрої.

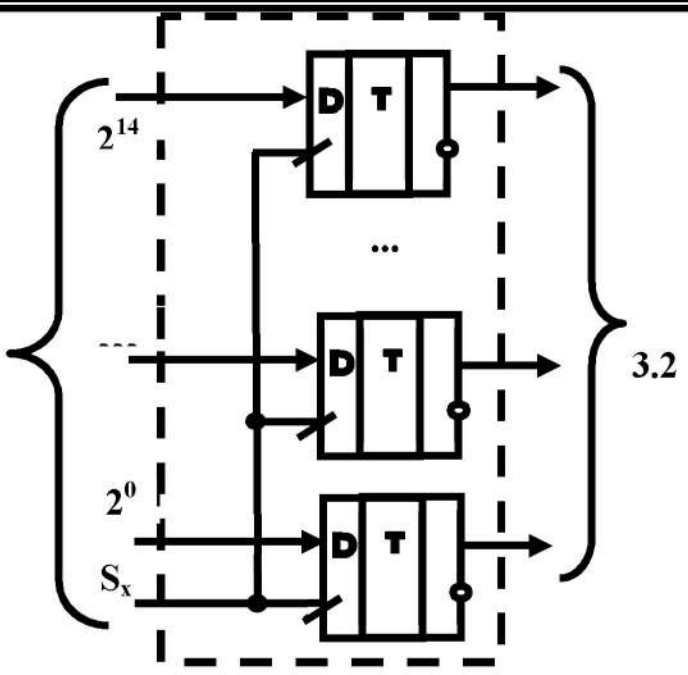

Рисунок 5 – Структура регістра пам'яті молодших розрядів БПЧ на D-тригерах

Висновки.

Обчислимо ефективність пристрою згідно суми ефективності обчислювальних елементів: $\tau = \tau_{ГІ} + \tau_{ПЗП} + \tau_{\sum}$. Кількість логічних елементів генератора імпульсів $\tau_{ГІ} = 2\upsilon$; регістр пам'яті містить $\tau_{РП} < \tau_{\sum}$; постійно запам'ятовуючий пристрій $\tau_{ПЗП} = 10\upsilon$; суматор - $\tau_{\sum} = 4\upsilon$. Таким чином, швидкодія пристрою генерування та кодування БПЧ складає $\tau = 16\upsilon$, що свідчить про високу ефективність розробленого пристрою опрацювання БПЧ.

Перелік джерел.

1. Івасьєв С.В. Метод зберігання простих великорозрядних чисел у базисі Радемахера / С.В. Івасьєв, М.М. Касянчук, І.З. Якименко // Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)" Київ: Інститут кібернетики імені В.М. Глушкова НАН України, 2013. – С. 142-144.

2. Івасьєв С.В. Метод зберігання простих великорозрядних чисел у базисі Радемахера / С.В. Івасьєв, М.М. Касянчук, І.З. Якименко // Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)" Київ: Інститут кібернетики імені В.М. Глушкова НАН України, 2013. – С. 142-144.

3. Івасьєв С.В. Метод організації компактної бібліотеки простих чисел великої розрядності / С.В. Івасьєв //Збірник матеріалів міжнародної наукової координаційної наради «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління» (ICSM) – Тернопіль, 2014. – С. 86-89.