УДК 681.04 DOI: 10.26565/2519-2310-2021-1-05

АЛГОРИТМ ПОБУДОВИ СТРУКТУРИ СУММАТОРУ ДВОХ ЗАЛИШКІВ ЧИСЕЛ ПО МОДУЛЮ

Михайло Багмут, Катерина Кузнєцова, Людмила Горбачова

Харківський національний університет імені В.Н. Каразіна, пл. Свободи, 4, Харків, 61022, Україна
Mikhail56@ukr.net, kate7smith12@gmail.com, lusyag23@gmail.com

Рецензент: В'ячеслав Калашников, д.ф.-м.н., проф., Технологічний університет Монтеррея, 64849 Монтеррей, Нуево-Леон, Мексика
kalash@itesm.mx

Надійшла: Лютий 2021.

***Анотація**: Відомо, що завдання побудови структури суматора, який працює по довільному модулю m_i і виконаний на логічних елементах з двома стійкими станами, є актуальною науково-прикладною задачею. Даний тип суматора використовується, як в позиційній двійковій системі числення (ПСЧ), так і в непозиційній системі числення в залишкових класах (СЗК). Якщо залишки a_i і b_i чисел $A = (a_1 || a_2 || ... || a_i || ... || a_k)$ і $B = (b_1 || b_2 || ... || b_i || ... || b_k)$, представлених в СЗК, дані в двійковій ПСС, тоді суматор двох залишків ai і bi по модулю ті являє собою сукупність з $n = [\log2 (m_i - 1) +1]$ двійкових однорозрядних суматорів (ДОС). При цьому всі ДОС об'єднані між собою зв'язками, подібно зв'язків позиційних двійкових суматорів. Метою статті є розробка алгоритму побудови структури суматору двох залишків a_i і b_i чисел A та B для довільного значення m_i модуля СЗК. Це процес реалізований, шляхом організації нових міжрозрядних зв'язків ДОС, з використанням позиційного суматора по модулю $M = 2^n - 1$. Відзначено, що існують спеціальні набори модулів, які застосовуються при обробці даних в СЗК. Так, при виконанні операції модульного складання залишків чисел, може використовуватися один з 3-х взаємно попарно простих чисел (виду $M = 2^n - 1$, $M = 2^n$ або $M = 2^n + 1$). Показано, що для синтезу суматора по модулю m_i СЗК, в структурі суматора по модулю М, необхідно відповідним чином сформувати додаткові зв'язки.*

***Ключові слова:** непозиційна система числення; однобітовий суматор; система залишкових класів; суматор залишків; цілочисельні арифметичні операції.*

1 Вступ

Виконання цілочисельних арифметичних операцій додавання, віднімання і множення двох чисел $A=(a_1||a_2||...||a_i||...||a_k)$ і $B=(b_1||b_2||...||b_i||...||b_k)$ в непозиційній системі числення в залишкових класах (СЗК) здійснюється шляхом реалізації відповідних залишків a_i і b_i чисел A і B за відповідними модулями (основами) m_i $(i=\overline{1,k})$ незалежно один від одного і паралельно в часі по кожному з k основ СЗК [1-3]. Відомо, що основною операцією, яка реалізується комп'ютерною системою (КС), як в позиційній двійковій системі числення (ПСЧ), так і в СЗК, є операція додавання двох чисел. В цьому аспекті одним з головних компонент КС є суматор двох чисел. Зокрема, компонентами КС в СОК, поряд з позиційними суматорами, є також суматори двох чисел по модулю m_i. В СОК модульна операція складання $(a_i+b_i)\bmod m_i$ реалізується на основі використання малорозрядних суматорів за модулем m_i. Один з методів реалізації модульної операції складання $(a_i+b_i)\bmod m_i$ ґрунтується на використанні структур малорозрядних двійкових суматорів [4]. Даний підхід надає широкий вибір варіантів реалізації структури таких суматорів. Це дозволяє в повній мірі використовувати наявний практичний досвід проектування і вибору структур довічних суматорів.

Таким чином, важливою і актуальною науково-прикладною задачею є задача по-будови структур суматорів, що працюють за довільним модулем m_i, виконаних на логічних елементах з двома стійкими станами. Якщо залишки a_i і b_i чисел $A=(a_1||a_2||...||a_i||...||a_k)$ та $B=(b_1||b_2||...||b_i||...||b_k)$ по модулю m_i СЗК представлені в двійковій ПСС, тоді суматор двох залишків a_i і b_i по модулю m_i представляє собою послідовну сукупність з $n=[\log_2(m_i-1)+1]$

двійкових однорозрядних суматорів (ДОС), які об'єднані між собою зв'язками, подібно зв'язків позиційних двійкових суматорів.

Мета статті – представити алгоритм побудови структури суматора двох залишків a_i і b_i чисел *A* та *B*, для довільного значення модулю m_i СЗК, шляхом нової організації міжрозрядних зв'язків ДОС, з використанням позиційного суматора по модулю $M = 2^n - 1$.

2 Основна частина

Відомо, що двійкові суматори в ПСЧ мають фіксовану величину модуля, рівну значенню числа $M = 2^n - 1$. Дана обставина виключає можливість їх безпосереднього використання для довільного модуля m_i СЗК. Якщо модуль *M* суматора, відрізняється від модулю m_i СЗК на одиницю, то існує два варіанти практичної реалізації операції додавання $(a_i + b_i) \bmod m_i$ двох залишків a_i і b_i по модулю СЗК. Розглянемо більш детально ці варіанти [1].

Перший варіант. Має місце наступне співвідношення модулів: $M = m_i + 1$. В цьому випадку розглянемо можливі умови виконання процедур реалізації модульного складання двох залишків чисел.

Перша умова. Якщо залишки чисел відповідають вимозі $a_i + b_i < m_i$, то корекція результату операції модульного складання не потрібна.

Друга умова. Якщо виконується співвідношення $a_i + b_i = m_i$, то вміст суматора по модулю обнуляється (*скидається*).

Третя умова. Якщо виконується співвідношення $a_i + b_i = M$, то при наявності нуля суматора, в молодшому розряді суматора встановлюється одиниця з одночасним обнулінням (*скиданням*) інших двійкових розрядів суматора.

Четверта умова. Якщо $a_i + b_i > M$, то результат операції буде дорівнювати значенню $a_i + b_i - M = (a_i + b_i - m_i - 1) \bmod m_i = a_i + b_i - 1$. В цьому випадку, в суматорі, ланцюг перенесення з виходу старшого розряду переходить на вхід молодшого розряду.

Другий варіант. Має місце наступне співвідношення модулів $M = m_i - 1$. У цьому разі є необхідність в коректуванні результату операції модульного складання залишків.

Перша умова. Якщо виконується співвідношення $a_i + b_i < m_i$, то корекція результату операції не вимагається.

Друга умова. Якщо виконується співвідношення $a_i + b_i = m_i$, то результат операції дорівнює одиниці. Здійснюється попередня видача сигналу, щодо перенесення вмісту зі старшого розряду. Вміст суматора скидається.

Третя умова. Якщо $a_i + b_i = M$, то обнуляється вміст суматора з паралельним занесенням в суматор одиниці.

Четверта умова. Якщо $a_i + b_i > M$, то отримуємо результат операції модульного додавання в наступному вигляді: $a_i + b_i - M = (a_i + b_i + 1) \bmod m_i$.

Вочевидь, що при розглянутих варіантах співвідношень між модулями m_i та *M*, реалізація операції додавання залишків $(a_i + b_i) \bmod m_i$, здійснюється відносно просто. Але відзначимо, що в разі наявності різниці значень величин модулів m_i і *M*, операція модульного складання $(a_i + b_i) \bmod m_i$ двох залишків чисел, є досить складним завданням. Це призводить до необхідності постановки і вирішення окремого завдання побудови структури суматора за довільним модулем m_i.

3 Структура суматора за довільним модулем

Розглянемо метод побудови суматорів за довільним модулем m_i СЗК, що заснований на структурі суматора по модулю $M = 2^n - 1$, шляхом організації і використання додаткових між-

розрядних зв'язків $X_{\downarrow i\uparrow j}$, в загальному випадку, між j-м та i-м ДОС суматора, по модулю *M*. Сформулюємо задачу побудови суматора 2-х залишків чисел по модулю, наступним чином.

Нехай задана довільна вихідна структура *n* - розрядним двійкового суматора по модулю $M = 2^n - 1$ (рис. 1). Необхідно створити структуру суматора для реалізації операції складання двох залишків чисел за довільним модулем m_i СЗК. Іншими словами, необхідно забезпечити, умову, щоб суматор за модулем $M = 2^n - 1$, виконував операцію додавання двох залишків, a_i і b_i чисел, $A = (a_1 \| a_2 \| ... \| a_i \| ... \| a_k)$ та $B = (b_1 \| b_2 \| ... \| b_i \| ... \| b_k)$, по модулю m_i. Це досягається шляхом введення додаткових зв'язків $X_{\downarrow i\uparrow j}$, в суматорі за модулем *M (де знак* $X_{\downarrow i\uparrow j}$ *позначає зв'язок між виходом* j*-го та входом* i*-го ДОС)*.

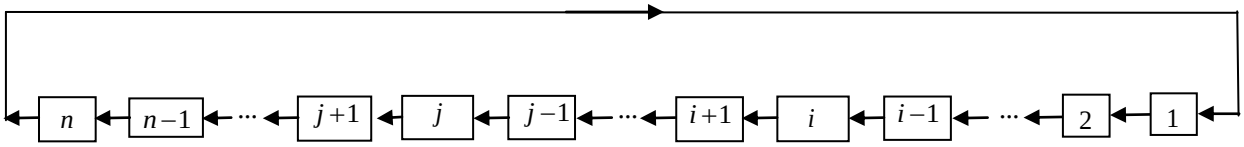

Рис. 1 – Структура двійкового суматора по модулю $M = 2^n - 1$

Задача побудови суматора за модулем m_i СЗК, буде здійснена шляхом вирішення задачі встановлення в суматорі за модулем, додаткових міжрозрядних зв'язків між певними ДОС виду $X_{\downarrow i\uparrow j}$. Для побудови суматора за модулем m_i СЗК, в структурі суматора необхідно, між певною парою ДОС (*вихідного суматора по модулю M*), сформувати додаткові зв'язки $X_{\downarrow i\uparrow j}$ таким чином, щоб за допомогою суматора по модулю *M*, здійснювалася операція додавання двох залишків чисел по модулю m_i. Схема організації додаткової зв'язку $X_{\downarrow i\uparrow j}$ між виходом j-го та входом i-го ДОС, представлена нижче, на рис. 2 ($j > i$).

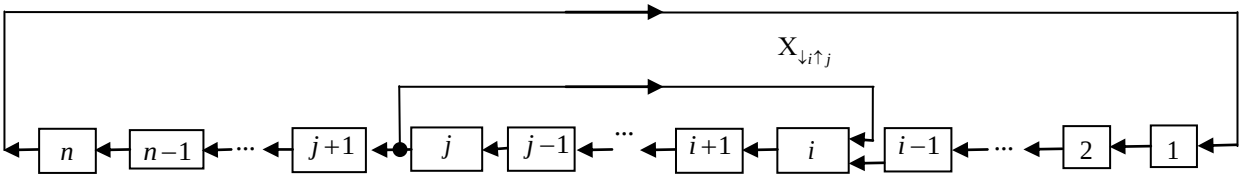

Рис. 2 – Схема двійкового суматора по модулю $M = 2^n - 1$ з одним зворотнім зв'язком

Розглянемо вплив наявності одного додаткового зв'язку/зв'язків $X_{\downarrow i\uparrow j}$ на величину вмісту суматора за модулем *M*.

4 Структура суматора по модулю *M* з додатковими зв'язками $X_{\downarrow i\uparrow j}$

Розглянемо вплив одного додаткового зв'язку $X_{\downarrow i\uparrow j}$, який встановлюється між виходом j-го та входом i-го ДОС в суматорі за модулем $M = 2^n - 1$ (рис. 2), на величину G_L вихідного вмісту суматору. Покажемо, що число $L = \{l_i\}$, $i = \overline{1, n}$, що є вмістом G_L суматора, при введенні одного додаткового зв'язку $X_{\downarrow i\uparrow j}$, зменшується на величину $\Delta G_L = 2^{i-j-2} \cdot \sum_{m=j+1}^{n} 2^m \cdot l_m$ [1]. При цьому, слід зазначити, що введення додаткового зв'язку $X_{\downarrow i\uparrow j}$, переводить обчислення значень з двійкової системи числення (СЧ), в якій працює суматора по модулю *M*, в поліадичну СЧ з основами $\tau_1, \tau_2, ..., \tau_k$ та модулем $M = \tau_1 \cdot \tau_2 \cdot ... \cdot \tau_k - 1$. В цьому випадку, одиниця m-го розряду числа $L = \{l_i\}$, $i = \overline{1, k}$, визначається наступним чином:

$$G_L = \sum_{m=1}^{k} l_m \cdot \prod_{i=1}^{m-1} \tau_i = l_1 \cdot \tau_2 \cdot \tau_3 \cdot ... \cdot \tau_k + l_2 \cdot \tau_3 \cdot \tau_4 \cdot ... \cdot \tau_k + ... + l_{k-2} \cdot \tau_{k-1} \cdot \tau_k + l_{k-1} \cdot \tau_k + l_k . \quad (1)$$

Співвідношення (1) можна представити в наступному вигляді:

$$G_L = l_1 \cdot \prod_{i=2}^{k} \tau_i + l_2 \cdot \prod_{i=3}^{k} \tau_i + ... + l_{k-2} \cdot \prod_{i=k-1}^{k} \tau_i + l_{k-1} \cdot \prod_{i=k}^{k} \tau_i + l_k . \quad (2)$$

У двійковій СЧ ($\tau_1 = \tau_2 = ... = \tau_k = 2$) вираз (2) прийме наступний вигляд:

$$G_L = \sum_{m=1}^{k} l_m \cdot 2^{k-m} = l_1 \cdot 2^{k-1} + l_2 \cdot 2^{k-2} + ... + l_{k-1} \cdot 2 + l_k . \quad (3)$$

В разі відсутності в суматорі додаткових зв'язків $X_{\downarrow i \uparrow j}$, величина G_L, вмісту суматора, дорівнює (*вираз 4*):

$$G_L = \sum_{m=1}^{n} l_m \cdot q_m , \quad (4)$$

де значення l_m є число одиниць, що містяться в m -ому розряді двійкового суматора, а значення q_m є вага m-го розряду двійкового суматора, який визначається положенням двійкового розряду суматора (рис. 1).

Якщо є додаткова зв'язок ($X_{\downarrow i \uparrow j}$), який об'єднує виконавчі розряди суматора з номерами від i до j, в єдиний (*узагальнений*) розряд суматора за модулем

$$\tau_{ij} = 2^{j-(i-1)} - 1 = 2^{j-i+1} - 1, \quad (5)$$

то, тоді, вага q_m кожного розряду суматора з номерами від $(i-1)$-го до першого (*молодшого розряду суматора*), буде дорівнює значенню $q_m = 2^{m-1}$ $(m = \overline{1, i-1})$ (*див. рис. 3*).

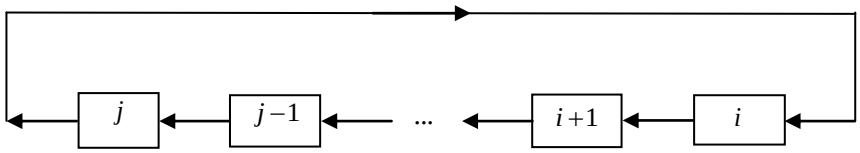

Рис. 3 – Схема узагальненого $(j-i+1)$-го розряду суматора по модулю τ_{ij}

Виходячи зі структури суматора по модулю (рис. 4), вага розрядів суматора з номерами від $(j+1)$-го до n (*старшого розряду суматора*) буде визначатися виразом (6):

$$q_m = 2^{i-1} \cdot \tau_{ij} \cdot 2^{m-j-1} . \quad (6)$$

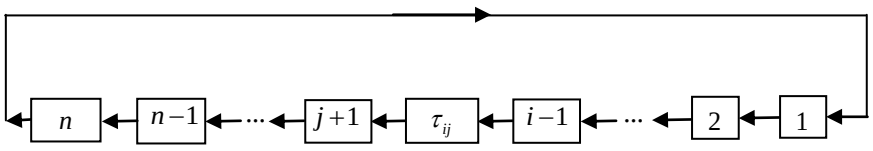

Рис. 4. Еквівалентна схема суматора по модулю з додатковим зв'язком $X_{\downarrow i \uparrow j}$

Враховуючи на співвідношення (5), вираз (6) можна представити в наступному вигляді

$$q_m = 2^{m+i-j-2} \cdot \tau_{ij} = 2^{m+i-j-2} \cdot (2^{j-i+1} - 1) = 2^{m-1} - 2^{m+i-j-2} . \quad (7)$$

Величина G_L числа L дорівнює різниці (8)

$$G_L = \sum_{m=1}^{n} l_m \cdot 2^{m-1} - \sum_{m=j+1}^{n} l_m \cdot 2^{m+i-j-2}. \quad (8)$$

Зі співвідношення (8) видно, що введення в суматор одного додаткового зв'язку. виду $X_{\downarrow i \uparrow j}$, зменшує його вміст G_L на величину, що дорівнює значенню

$$\Delta G_L = \sum_{m=j+1}^{n} l_m \cdot 2^{m+i-j-2} = 2^{i-j-2} \cdot \sum_{m=j+1}^{n} l_m \cdot 2^m.$$

Таким чином, при введенні одного додаткового зв'язку $X_{\downarrow i \uparrow j}$ початковий вміст суматора по модулю M , зменшується на величину ΔG_L, де

$$\Delta G_L = 2^{i-j-2} \cdot \sum_{m=j+1}^{n} l_m \cdot 2^m. \quad (9)$$

Одним з важливих ефектів виконаних досліджень є те, що при введенні додаткового зв'язку виду $X_{\downarrow i \uparrow j}$, значення величини модуля $M = 2^n - 1$, вихідного суматора, зменшується на величину

$$\Delta M = 2^{i-j-2} \cdot \sum_{m=j+1}^{n} S_m \cdot 2^m, \quad (10)$$

де S_m – значення *m*-го розряду числа, що міститься в суматорі [1]. При цьому, вочевидь, що діапазон чисел за модулем *M*, які представляються, зменшується на величину $\triangle M$. Ця обставина надає можливість, за рахунок введення в суматор за модулем *M* певних зв'язків (*або одного додаткового зв'язку*), зменшити величину *M* модуля до необхідного значення модуля m_i СЗК. В цьому випадку має виконуватися наступна умова

$$m_i = M - \Delta M \text{ или } m_i = 2^n - 1 - 2^{i-j-2} \cdot \sum_{m=j+1}^{n} l_m \cdot 2^m. \quad (11)$$

Виходячи з виразу (11), чисельне значення заданого модуля СЗК буде визначено набором значень n, j та i. Таким чином, необхідно визначити значення n, j та i, як такі, що задовольняють виконання рівності (11).

5 Алгоритм побудови суматорів за довільним модулем m_i

У загальному вигляді, в представленні модулю m_i, вміст двійкових розрядів має наступний вигляд:

$$m_i = S_n \cdot 2^{n-1} + S_{n-1} \cdot 2^{n-2} + ... + S_2 \cdot 2 + S_1, \quad (12)$$

та нехай початковий вміст G_L суматора по модулю $M = 2^n - 1$ має вид:

$$G_L = l_n \cdot 2^{n-1} + l_{n-1} \cdot 2^{n-2} + ... + l_2 \cdot 2 + l_1. \quad (13)$$

В цьому випадку, для виконання умови (11) в суматор за модулем $M = 2^n - 1$ вводять додаткові зв'язку $X_{\downarrow i \uparrow j}$. При цьому *(див. вирази (12) і (13))*, i-й ДОС прийме значення $l_i + c_{i-1} + x_{ij}$, де l_i – це вміст l_i -го ДОС вихідного стану суматора по модулю *M*; c_i – значення сигналу перенесення вмісту $(i-1)$-го ДОС в i-й ДОС; x_{ij} – це значення l_j вмісту j-го ДОС суматора; S_i – значення вмісту i-го двійкового розряду модуля m_i СЗК. У цьому випадку маємо (14):

$$l_i + c_{i-1} + x_{ij} + S_i = l_i. \quad (14)$$

Враховуючи одно з властивостей модуля суматора (*модуль суматора є його другим нулем*) вираз (14) набуває вигляду (15)

$$c_{i-1} + x_{ij} + S_i = 0, \quad (15)$$

що для двійкового представлення чисел, рівнозначно співвідношенню (16)

$$S_i = c_{i-1} + x_{ij}. \quad (16)$$

Беручи до уваги все вищезазначене, та виходячи з результатів аналізу виразів (15) і (16), можна зробити наступні висновки, стосовно впливу додаткових встановлених зв'язків $X_{\downarrow i \uparrow j}$, на вміст позиційного суматора по модулю $M = 2^n - 1$.

Вплив встановлених зв'язків $X_{\downarrow i \uparrow j}$, на вміст позиційного суматора по модулю $M = 2^n - 1$, обумовлює правила синтезу структури суматора по модулю m_i СОК.

Сформулюємо ***правила*** побудови структури суматора двох залишків чисел по модулю m_i.

1. Наявність додаткових зв'язків $X_{\downarrow i \uparrow j}$ і їх вплив на зменшення величини $\Delta M = 2^{i-j-2} \cdot \sum_{m=j+1}^{n} S_m \cdot 2^m$ вмісту G_L суматора по модулю $M = 2^n - 1$ не залежить від вихідного стану цього позиційного суматора.

2. У позиційному суматорі по модулю $M = 2^n - 1$ додатковий зв'язок $X_{\downarrow i \uparrow j}$ має місце (*вихід доп. зв'язку* $X_{\downarrow i \uparrow j}$) лише для i-х S_i ДОС (S_i; $i = \overline{2, n}$), відповідних нульових значень двійкової кодової комбінації модулю m_i, за яким працює суматор.

3. У двійкових розрядах S_i кодової комбінації, модулю m_i суматора, які відповідають одиничним значенням, додаткові зв'язки $X_{\downarrow i \uparrow j}$ повинні бути відсутніми. Тобто необхідно, щоб виконувалася умова $x_{ij} = 0$.

4. Вміст G_L суматора не зміниться, якщо додатковий зв'язок $X_{\downarrow i \uparrow n}$ буде «взят» з виходу старшого ДОС (старшого розряду суматора).

5. При введенні одного додаткового зв'язку $X_{\downarrow i \uparrow j}$, модуль $M = 2^n - 1$ позиційного суматора зменшується на величину $\Delta M = 2^{i-j-2} \cdot \sum_{m=j+1}^{n} S_m \cdot 2^m$.

6. Число, яке описує вміст G_L суматора по модулю $M = 2^n - 1$ з одним додатковим зв'язком $X_{\downarrow i \uparrow j}$, може приймати не більше $(n + i - j)$ різних числових значень, що відповідають $(n + i - j)$ можливим конструкціям суматору по модулю m_i. Фактично, майже для кожної основи m_i СЗК, можна побудувати кілька варіантів структур суматорів. В цьому випадку, може виникнути необхідність вибору «найкращої» структури суматору за модулем m_i, із всіх можливих варіантів. Однак, в рамках даної роботи, оптимізація та вибір суматора по модулю m_i, з усіх можливих варіантів, не розглядаються.

Таким чином, суть алгоритму побудови суматорів за модулем m_i СЗК полягає в наступному: - в вихідному суматорі за модулем $M = 2^n - 1$, на підставі вищенаведених правил, формуються додаткові зв'язки суматора, а використання додаткових зв'язків дозволяє реалізувати вихідний суматор для виконання операції додавання вирахувань чисел за модулем m_i СЗК. При цьому слід мати на увазі, що введення додаткових зв'язків $X_{\downarrow i \uparrow j}$ змінює категорію ваги окремих розрядів суматора та зменшує величину модуля від M до m_i.

Алгоритм побудови суматора по модулю m_i СЗК складається з наступних операцій:

1. Представлення структури суматору по модулю $M = 2^n - 1$, де $n = [\log_2(m_i - 1)] + 1$. В цьому випадку визначається розрядність n (*кількість ДОС*) суматора по модулю m_i;

2. Визначення двійкових розрядів S_i суматора для яких виконується умова $S_i = 0$. Процес визначення умови $S_i = 0$, проводиться виходячи з подання модуля числа m_i, в двійковому коді;

3. Як правило, додатковий зв'язок починається з виходу n-го (старшого) двійкового розряду ($j = n$);

4. Додатковий зв'язок $X_{\downarrow i \uparrow j}$ надходить на вхід ДОС, для якого $S_i = 0$ *(див. п. 2 методу)*.

6 Приклади виконання операції додавання залишків чисел за модулем

Відповідно до представленого вище алгоритму, розглянемо приклади синтезу суматорів для різних модулів m_i СЗК.

Приклад 1. Нехай $m_i = 11$. Розглянемо етапи синтезу суматора за модулем $m_i = 11$ СЗК.

1. Відповідно до величини $m_i = 11$ модуля СЗК, визначимо кількість n ДОС. Для модуля $m_i = 11$ маємо, що $n = [\log_2(11-1)]+1 = 4$. При цьому, структура суматора по модулю буде $n = [\log_2(11-1)]+1 = 4$ мати вигляд, який наведено на рис. 5.

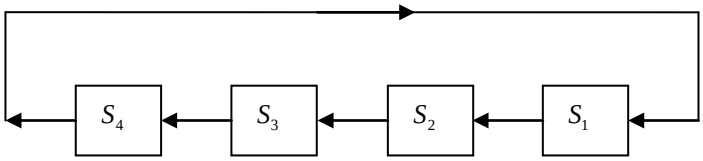

Рис. 5 – Вихідна структура суматора за модулем $M = 2^n - 1$

2. Для синтезу суматора по модулю $m_i = 11$ СЗК, попередньо, визначимо значення двійкових розрядів S_i суматора, в запису модуля $m_i = 11$ яких, містяться нулі, тобто для випадку, коли $S_i = 0$. Таким розрядом буде третій розряд, тобто $S_3 = 0$, так як в двійковому коді модуль $m_i = 11$ має наступний вигляд 1011.

3. Виходячи з того, що $S_3 = 0$, додатковий зв'язок в суматорі матиме вигляд $X_{\downarrow 3 \uparrow 4}$.

Структура суматора за модулем $m_i = 11$ представлена нижче, на рис. 6.

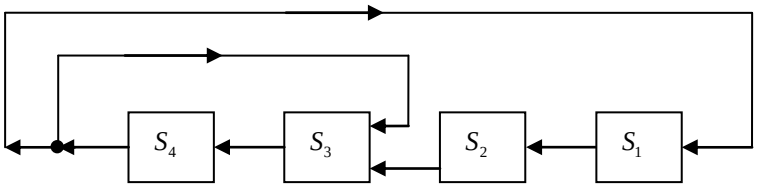

Рис. 6 – Структура суматора за модулем $m_i = 11$

Для структури суматора, що представлена на рис. 6, визначимо значення модуля $M = m_i$ СЗК. Попередньо розглянемо частину структури (*див. рис. 7*) цього суматора.

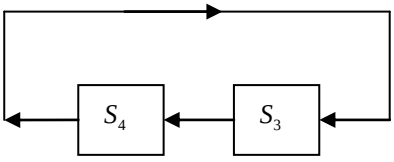

Рис. 7 – Частина структури суматора за модулем m_i

Для цієї частини структури суматора значення модуля M_1 визначиться, як $M_1 = \tau_4 \cdot \tau_3 - 1$. Значення модуля $M = m_i$ СЗК суматора (*рис. 6*) визначиться наступним чином (*див. рис. 8*)

$$m_i = M_1 \cdot \tau_2 \cdot \tau_1 - 1 = (\tau_4 \cdot \tau_3 - 1) \cdot \tau_2 \cdot \tau_1 - 1 = (2 \cdot 2 - 1) \cdot 2 \cdot 2 - 1 = 11.$$

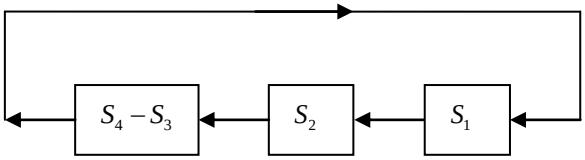

Рис. 8 – Частина структури суматора за модулем m_i

Таким чином, синтез суматора за модулем $m_i = 11$ проведений вірно.

Приклад 2. Нехай m_i =37. Етапи синтезу суматора по модулю СЗК.

1. Відповідно до величини модуля $m_i = 37$, визначимо кількість n двійкових розрядів (*кількість ДОС*) суматора по модулю. Для модуля $m_i = 37$ маємо, що $n = [\log_2(37-1)]+1 = 6$.

2. Для синтезу структури суматора по модулю $M = 63$ введемо додаткові зв'язки $X_{\downarrow i \uparrow j}$. Попередньо визначимо двійкові розряди S_i суматора, в яких в запису модуля m_i, в двійковому коді, містяться нулі, тобто $S_i = 0$. Так як модуль в двійковому коді має вигляд 100101, то нульовими двійковими розрядами суматора будуть наступні: $S_2 = 0$, $S_4 = 0$ та $S_5 = 0$.

3. Спираючись на отримані в п. 2 результати (*опис метода синтезу суматора по модулю* m_i), введемо в суматор за модулем $M = 2^n - 1$ три додаткові зв'язку: $X_{\downarrow 5 \uparrow 6}$, $X_{\downarrow 4 \uparrow 6}$ та $X_{\downarrow 2 \uparrow 6}$. У цьому випадку структура суматора за модулем $m_i = 37$ має вид, що представлений на рис. 9.

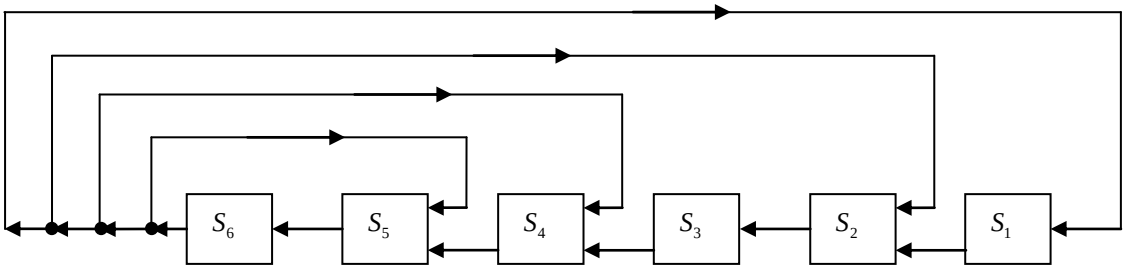

Рис. 9 – Структура суматора за модулем $m_i = 37$

Визначимо для даної структури (рис. 9) значення модуля $M = m_i$ СЗК. Для цього, попередньо, складемо ряд структур окремих частин суматора, що представлений на рис. 9.

Перша частина структури суматора представлена на рис. 10.

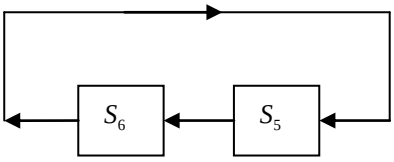

Рис. 10 – Перша частина структури суматора за модулем m_i

Для 1-ої частини структури суматора, модуль M_1 визначиться наст. чином $M_1 = \tau_6 \cdot \tau_5 - 1$.

Друга частина структури суматора представлена на рис. 11. Для цієї структури суматора, модуль M_2 визначається наступним чином: $M_2 = M_1 \cdot \tau_4 - 1 = (\tau_6 \cdot \tau_5 - 1) \cdot \tau_4 - 1$.

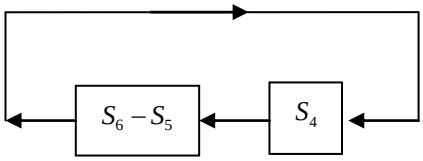

Рис. 11 – Друга частина структури суматора за модулем m_i

Третя частина структури суматора представлена на рис. 12.

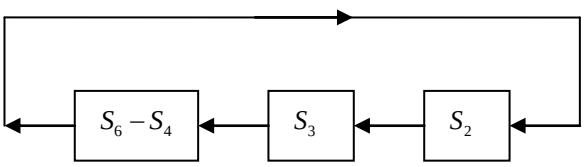

Рис. 12 – Третя частина структури суматора за модулем m_i

Для третьої частини структури суматора, модуль M_3 визначиться наступним чином $M_3 = M_2 \cdot \tau_3 \cdot \tau_2 - 1 = \left[(\tau_6 \cdot \tau_5 - 1) \cdot \tau_4 - 1\right] \cdot \tau_3 \cdot \tau_2 - 1$.

Четверта частина структури суматора представлена на рис. 13

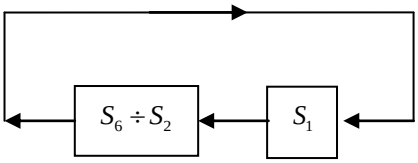

Рис. 13 – Четверта частина структури суматора за модулем m_i

Значення модуля $M = m_i$ СЗК визначається наступним чином $m_i = M_3 \cdot \tau_1 - 1 = \left\{\left[(\tau_6 \cdot \tau_5 - 1) \cdot \tau_4 - 1\right] \cdot \tau_3 \cdot \tau_2 - 1\right\} \cdot \tau_1 - 1 = \left\{\left[(2 \cdot 2 - 1) \cdot 2 - 1\right] \cdot 2 \cdot 2 - 1\right\} \cdot 2 - 1 = 37$. Т.ч., синтез суматора по модулю m_i =37 проведений вірно.

Приклад 3. Нехай $m_i = 53$. Розглянемо етапи синтезу суматора по модулю СЗК.

1. Відповідно до величини модуля $m_i = 53$, визначимо кількість n ДОС суматора по модулю $M = 2^n - 1$. Для модуля $m_i = 53$ маємо, що $n = [\log_2(m_i - 1)] + 1 = [\log_2(53 - 1)] + 1 = 6$. Структура суматора по модулю $M = 2^n - 1 = 63$ представлена на рис. 14. Вихідна структура суматора по модулю $m_i = 53$ без додаткових зв'язків $X_{\downarrow i \uparrow j}$ матиме той же вигляд.

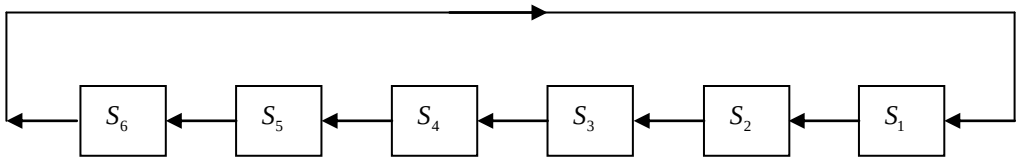

Рис. 14 – Вихідна структура суматора за модулем $M = 2^6 - 1$.

2. Модуль $m_i = 53$, в двійковому коді $S_6\, S_5\, S_4\, S_3\, S_2\, S_1$, представляється у вигляді 110101, тобто $S_6 = 1$, $S_5 = 1$, $S_4 = 0$, $S_3 = 1$, $S_2 = 0$ та $S_1 = 1$. З вигляду, який представлений в двійковому коді модулю $m_i = 53$ визначимо, що $S_2 = S_4 = 0$.

3. На основі отриманих результатів, структура суматора за модулем $m_i = 53$ має вигляд, який представлений нижче,е на рис. 15.

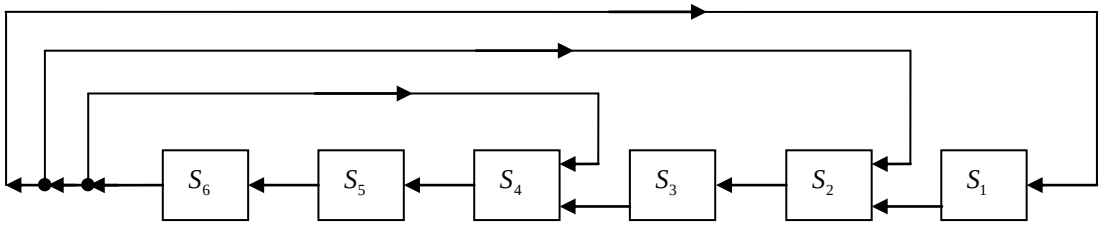

Рис. 15 – Структура суматора за модулем $m_i = 53$

Відповідно до методу синтезу, в суматор за модулем $M = 2^6 - 1$ введені два додаткові зв'язку $X_{\downarrow 4 \uparrow 6}$ та $X_{\downarrow 2 \uparrow 6}$. З метою перевірки правильності синтезу суматора по модулю $m_i = 53$, визначимо для даної структури суматора, значення модулю $M = m_i$ СЗК.

Враховуючи схему на рис. 15 складемо ряд окремих частин суматора по модулю $m_i = 53$.

Перша частина структури такого суматору, представлена на рис. 16.

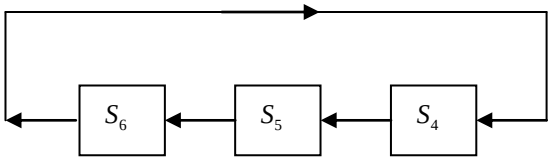

Рис. 16 – Перша частина структури суматора за модулем m_i

Для першої частини структури суматора, модуль M_1 визначиться наступним чином $M_1 = \tau_3 \cdot \tau_5 \cdot \tau_4 - 1$. Друга частина структури суматора представлена на рис. 17.

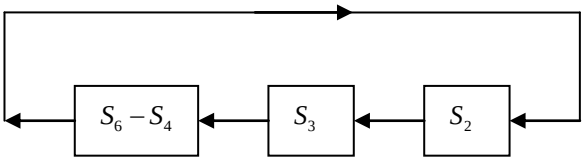

Рис. 17 – Друга частина структури суматора за модулем m_i

Для цієї частини структури, модуль M_2 визначиться виразом $M_2 = M_1 \cdot \tau_3 \cdot \tau_2 - 1 = (\tau_6 \cdot \tau_5 \cdot \tau_4 - 1) \cdot \tau_3 \cdot \tau_2 - 1$.

Для суматора по модулю, значення модуля $M = m_i$ СЗК визначається наступним чином (*див. рис. 15-17*) $m_i = M_2 \cdot \tau_1 - 1 = \left[(\tau_6 \cdot \tau_5 \cdot \tau_4 - 1) \cdot \tau_3 \cdot \tau_2 - 1\right] \cdot \tau_1 - 1 = \left[(2^3 - 1) \cdot 2^2 - 1\right] \cdot 2 - 1 = 53$. - Т.ч. на основі проведених розрахунків, можна зробити висновок, що синтез суматору за модулем $m_i = 53$ (рис. 15) проведений вірно!

Пример 4. Пусть $m_i = 97$. Этапы синтеза сумматора по модулю СОК следующие

1. У відповідності зі значенням модулю, $m_i = 97$ визначимо кількість *n* ДОС суматора за модулем $M = 2^n - 1$. Для модулю $m_i = 97$ маємо, що $n = \left\lceil \log_2 (m_i - 1) \right\rceil + 1 = \left\lceil \log_2 (97 - 1) \right\rceil + 1 = 7$. Структура суматору по модулю $M = 2^n - 1 = 2^7 - 1 = 127$ має вигляд, який представлений на рис. 18.

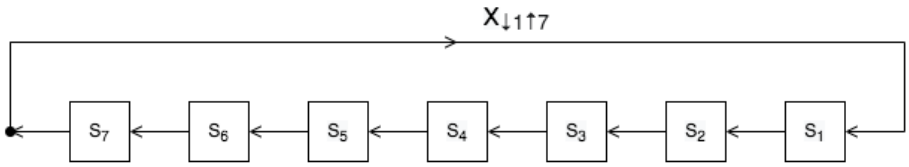

Рис. 18 – Вихідна структура суматора за модулем $M = 2^7 - 1$

2. Модуль $m_i = 97$ в двійковому коді $S_7 S_6 S_5 S_4 S_3 S_2 S_1$ представляється у вигляді 1100001, тобто $S_7 = 1, S_6 = 1, S_5 = S_4 = S_3 = S_2 = 0, S_1 = 1$.

3. На підставі отриманих результатів, структура суматора по модулю $m_i = 97$ представлена на рис. 19.

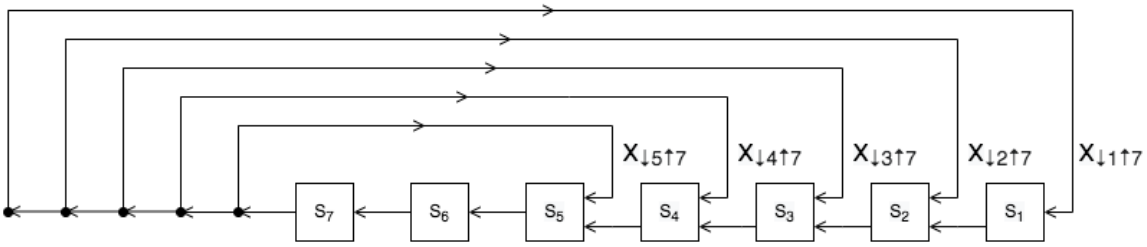

Рис. 19 – Структура суматора за модулем $m_i = 97$

Відповідно до отриманих результатів в суматор за модулем $M = 2^7 - 1$ введені 4 додаткові зв'язку: - $X_{\downarrow 5 \uparrow 7}, X_{\downarrow 4 \uparrow 7}, X_{\downarrow 3 \uparrow 7}, X_{\downarrow 2 \uparrow 7}$. Для перевірки правильності створеної структури суматору за модулем $m_i = 97$, визначимо значення модуля для створеної структури (*див. рис. 19*). Перша частина структури суматора (*рис. 19*) представлена на рис. 20.

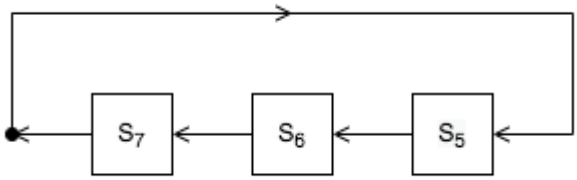

Рис. 20 – Перша частина структури суматора за модулем $m_i = 97$

Для першої частини структури суматора модуль M_1 визначається наступним чином $M_1 = \tau_7 \cdot \tau_6 \cdot \tau_5 - 1$.

Друга частина структури суматора представлена на рис. 21.

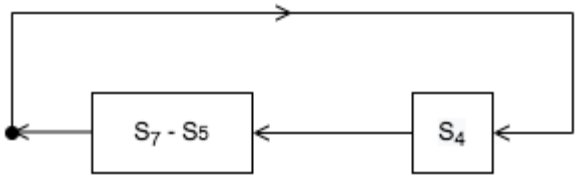

Рис. 21 – Друга частина структури суматора за модулем $m_i = 97$

Для 2-ої частини структури відповідного суматора модуль M_2 визначається, як $M_2 = M_1 \cdot \tau_4 - 1$.

Третя частина структури суматора представлена на рис. 22.

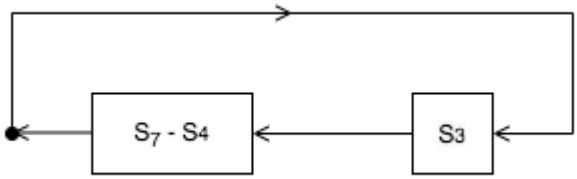

Рис. 22 – Третя частина структури суматора за модулем $m_i = 97$

Для третьої частини структури суматора, модуль M_3 визначається, як $M_3 = M_2 \cdot \tau_3 - 1$.

Четверта частина структури суматора представлена на рис. 23. Для неї модуль M_4 визначається, як $M_4 = M_3 \cdot \tau_2 - 1$.

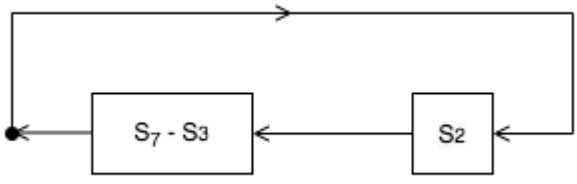

Рис. 23 – Четверта частина структури суматора за модулем $m_i = 97$

П'ята частина структури суматора представлена на рис. 24.

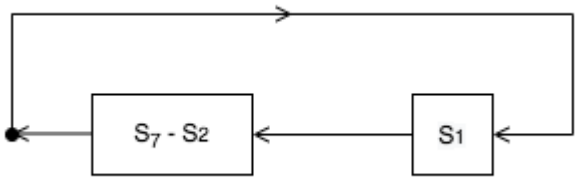

Рис. 24 – П'ята частина структури суматора за модулем $m_i = 97$

Для п'ятої частини структури суматора, модуль M_5 визначається, як $M_5 = M_4 \cdot \tau_1 - 1$.

Визначимо значення модуля m_i:

- $M_1 = \tau_7 \cdot \tau_6 \cdot \tau_5 - 1$ *(див. рис. 20)*;
- $M_2 = M_1 \cdot \tau_4 - 1 = (\tau_7 \cdot \tau_6 \cdot \tau_5 - 1) \cdot \tau_4 - 1$ *(див. рис. 21)*;
- $M_3 = M_2 \cdot \tau_3 - 1 = \left[(\tau_7 \cdot \tau_6 \cdot \tau_5 - 1)\tau_4 - 1\right]\tau_3 - 1$ *(див. рис. 22)*;
- $M_4 = M_3 \cdot \tau_2 - 1 = \left\{\left[(\tau_7 \cdot \tau_6 \cdot \tau_5 - 1) \cdot \tau_4 - 1\right] \cdot \tau_3 - 1\right\} \cdot \tau_2 - 1$ *(см. рис. 23)*;
- $M_5 = M_4 \cdot \tau_1 - 1 = \left(\left\{\left[(\tau_7 \cdot \tau_6 \cdot \tau_5 - 1) \cdot \tau_4 - 1\right] \cdot \tau_3 - 1\right\} \cdot \tau_2 - 1\right) \cdot \tau_1 - 1$ *(см. рис. 24)*.

В цьому випадку можна представити вираз для визначення значення модуля m_i у наступному вигляді: $m_i = m_5 = \left(\left\{\left[(2 \cdot 2 \cdot 2 - 1) \cdot 2 - 1\right] \cdot 2 - 1\right\} \cdot 2 - 1\right) \cdot 2 - 1 = 97$.

Таким чином, синтез суматора за модулем $m_i = 97$ (*рис. 19*) виконаний правильно.

7 Висновки

1. В роботі запропонований алгоритм побудови суматорів за модулем m_i СЗК.

2. Запропонований алгоритм заснований на використанні вже існуючих позиційних суматорів за модулем $M = 2^n - 1$ (що складаються із сукупності послідовно розташованих двійкових однорозрядних суматорів), за допомогою введення та подальшої реалізації, додаткових міжрозрядних зв'язків (*виду* $X_{\downarrow i \uparrow j}$).

3. Авторами роботи сформульовані правила введення додаткових міжрозрядних зв'язків виду $X_{\downarrow i \uparrow j}$. Підкреслено, що використання додаткових зв'язків *(на основі структури суматора за модулем* $M = 2^n - 1$*)*, дозволяє синтезувати суматор, який реалізує операцію додавання двох залишків a_i та b_i чисел.

4. Сукупність із k суматорів за модулем, представляє собою суматор двох чисел $A = (a_1 \| a_2 \| ... \| a_i \| ... \| a_k)$ та $B = (b_1 \| b_2 \| ... \| b_i \| ... \| b_k)$ в СЗК.

5. Розглянуті в межах цієї статті приклади побудови двійкових суматорів для різних значень модулів m_i СЗК, підтверджують можливість практичного використання запропонованого алгоритму.

Посилання

[1] V. A. Krasnobayev, A. A. Kuznetsov, S. A. Koshman, and K. O. Kuznetsova "A method for implementing the operation of modulo addition of the residues of two numbers in the residue number system", Cybernetics and Systems Analysis, Vol. 56, No. 6, November, 2020, 1029-1038. https://doi.org/10.1007/s10559-020-00323-9.

[2] Krasnobayev V. A., Yanko A. S., Koshman S. A. A Method for arithmetic comparison of data represented in a residue number of system // Cybernetics and Systems Analysis. – January 2016. – Vol. 52, Is. 1, pp. 145-150.

[3] Krasnobayev V. A. and Koshman S. A. Method for implementing the arithmetic operation of addition in residue number system based on the use of the principle of circular shift // Cybernetics and Systems Analysis. – July, 2019. – Vol. 55, Is. 4, pp. 692-698.

[4] Bayoumi M.A., Jullien G.A., Miller W.C. A VLSI Implementation of Residue. Adders IEEE Trans. on Circuits and Systems. 1987. Vol. 34, № 3. pp. 284-288.

[5] Azadeh Safari, James Nugent, Yinan Kong. Novel implementation of full adder based scaling in Residue Number Systems. IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS). 4-7 Aug. 2013. pp. 657–660.

[6] Shugang Wei. Fast signed-digit arithmetic circuits for residue number systems. IEEE International Conference on Electronics, Circuits, and Systems (ICECS). 6-9 Dec. 2015. pp. 344 – 347.
[7] P.V. Ananda Mohan. Residue Number Systems: Theory and Applications. Birkhäuser Basel: Springer International Publishing Switzerland, 2016. - 351 P.

Рецензент: Вячеслав Калашников, д.ф.-м.н., проф., Технологический университет Монтеррея, Монтеррей, Мексика.
E-mail: kalash@itesm.mx

Поступила: Февраль 2021.

Авторы:
Михаил Багмут, аспирант кафедры Безопасности информационных систем и технологий, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: Mikhail56@ukr.net

Екатерина Кузнецова, студентка кафедры Безопасности информационных систем и технологий, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: kate7smith12@gmail.com

Людмила Горбачова, студентка кафедры Безопасности информационных систем и технологий, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: lusyag23@gmail.com

Алгоритм построения структуры сумматора двух остатков чисел по модулю.

Аннотация. Известно, что задача построения структуры сумматора, который работает по произвольному модулю m_i и выполнен на логических элементах с двумя устойчивыми состояниями, является актуальной научно-прикладной задачей. Данный тип сумматора используется, как в позиционной двоичной системе счисления *(ПСС),* так и в непозиционной системе счисления в остаточных классах *(СОК).* Если остатки a_i и b_i чисел $A = (a_1||a_2||...||a_i||...||a_k)$ и $B = (b_1||b_2||...||b_i||...||b_k)$, представленных в СОК, даны в двоичной ПСС, тогда сумматор двух остатков a_i и b_i по модулю m_i , представляет собой совокупность из $n = [log_2(m_i - 1)+1]$ двоичных одноразрядных сумматоров (*ДОС*). При этом все ДОС объединены между собой связями, подобно связям позиционных двоичных сумматоров. Целью статьи является разработка алгоритма построения структуры сумматора двух остатков a_i и b_i , чисел *A* и *B,* для произвольного значения m_i модуля СОК. Этот процесс реализован, путем организации новых межразрядных связей ДОС, с использованием позиционного сумматора по модулю $M = 2^n–1$. Отмечено, что существуют специальные наборы модулей, которые применяются при обработке данных в СОК. Так, при выполнении операции модульного сложения остатков чисел, может использоваться один из *3-х* взаимно попарно простых чисел *(вида* $M = 2^n - 1$, $M = 2^n$ *или* $M = 2^n + 1$*).* Показано, что для синтеза сумматора по модулю m_i СОК, в структуре сумматора по модулю *M,* необходимо соответствующим образом сформировать дополнительные связи.

Ключевые слова: непозиционная система счисления; однобитовый сумматор; система счисления остатков; сумматор остатков; целочисленные арифметические операции.

Reviewer: Vyacheslav Kalashnikov, Doctor of Sciences (Physics and Mathematics), Full Prof., Department of Systems and Industrial Engineering, Campus Monterrey, Monterrey, Mexico.
E-mail: kalash@itesm.mx

Received: February 2021.

Authors:
Mykhailo Bagmut, graduate student of the Department of Security of Information Systems and Technologies, Kharkiv National University named after V.N. Karazin, Kharkiv, Ukraine.
E-mail: Mikhail56@ukr.net

Katerina Kuznetsova, student of the Department of Security of Information Systems and Technologies, Kharkiv National University named after V.N. Karazin, Kharkiv, Ukraine.
E-mail: kate7smith12@gmail.com

Ludmila Gorbachova, student of the Department of Security of Information Systems and Technologies, Kharkiv National University named after V.N. Karazin, Kharkiv, Ukraine.
E-mail: lusyag23@gmail.com

Algorithm for constructing the adder of residues of two numbers modulus.

Abstract. An urgent scientific and applied problem is the problem of constructing the adder structure, which is performed on logical elements with two stable states and operates according to an arbitrary modulo m_i. This type of adder is used both in the positional binary number system *(PNS)* and in the non-positional number system in residual classes *(RNS).* If the residuals a_i and b_i of numbers $A = (a_1||a_2||...||a_i||...||a_k)$ and $B = (b_1||b_2||...||b_i||...||b_k)$, represented in the RNS are given in a binary PNS, then the adder of two

residuals a_i and b_i modulo m_i is a set of $n = [log_2(m_i - 1)+1]$ binary one-bit adders (*BOBA*). Simultaneously, all BOBA are connected as positional binary adders. The purpose of the article is to develop an algorithm for constructing the adder structure of two residuals a_i and b_i of numbers *A* and *B* for an arbitrary modular value m_i of RNS. This process is realized by organizing new inter-bit connections of BOBA, using a positional adder modulo $M = 2^n - 1$. It is noted, that there are special sets of modules that are used when processing data in RNS. So, when performing the operation of modular addition of the remainders of numbers, one of three mutually pairwise primes (of the form $M = 2^n - 1$, $M = 2^n$ or $M = 2^n + 1$) can be used. It is shown that in order to synthesize an adder modulo m_i RNS, in the adder structure modulo *M*, it is necessary to appropriately form the additional connections.

Keywords: non-positional number system; single-bit adder; balance system; balance adder; integer arithmetic operations.