



УКРАЇНА

(19) **UA** (11) **130755** (13) **C2**

(51) МПК (2026.01)

G06F 7/00

G06F 7/72 (2006.01)

G06F 11/10 (2006.01)

НАЦІОНАЛЬНИЙ ОРГАН
ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ
ДЕРЖАВНА ОРГАНІЗАЦІЯ
"УКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ОФІС ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ ТА ІННОВАЦІЙ"

(12) ОПИС ДО ПАТЕНТУ НА ВІНАХІД

(21) Номер заявки: а 2023 03129	(72) Винахідник(и): Краснобаєв Віктор Анатолійович (UA), Янко Аліна Сергіївна (UA), Кошман Сергій Олександрович (UA), Ковальчук Дмитро Миколайович (UA)
(22) Дата подання заявки: 27.06.2023	
(24) Дата, з якої є чинними права інтелектуальної власності: 07.05.2026	
(41) Публікація відомостей про заяву: 17.04.2024, Бюл.№ 16	(73) Володілець (володільці): ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В.Н. КАРАЗІНА, пл. Свободи, 4, м. Харків, 61022 (UA)
(46) Публікація відомостей про державну реєстрацію: 06.05.2026, Бюл.№ 18	(56) Перелік документів, взятих до уваги експертизою: UA 50024 U, 25.05.2010 UA 130809 U, 26.12.2018 UA 140865 U, 10.03.2020 UA 106343 C2, 11.08.2014 US 4926374 A, 15.05.1990 WO 2005013117 A1, 10.02.2005 JP 4293665 B2, 08.07.2009 UA 55454 U, 10.12.2010

(54) ПРИСТРІЙ ДЛЯ ДОДАВАННЯ ТА ВІДНІМАННЯ ЛИШКІВ ЧИСЕЛ ЗА МОДУЛЕМ

(57) Реферат:

Пристрій для додавання та віднімання лишків чисел за модулем належить до автоматики та обчислювальної техніки та може бути застосований в комп'ютерних системах і компонентах, що функціонують у непозиційній системі числення залишкових класів. У пристрій, що містить перший і другий вхідні регістри, вихідний регістр, регістр кільцевого зсуву, дешифратор, шифратор, першу та другу групи елементів І, схему порівняння, лічильник імпульсів, генератор імпульсів, елемент заборони додатково введені перший та другий елементи І. Технічний результат: зменшення кількості обладнання пристрою.

UA 130755 C2

Винахід належить до області автоматики та обчислювальної техніки та може бути застосовано в комп'ютерних системах і компонентах, що функціонують у непозиційній системі числення залишкових класів (СЗК).

Відомий аналог для додавання у СЗК (А.с. № 446056 СРСР, G 06 F 7/72, 1971р.). Пристрій містить групу суматорів, перший та другий перетворювачі коду лишку за допоміжним модулем, суматор за допоміжним модулем, схему порівняння та зв'язки між ними.

Недолік аналога - значна кількість обладнання пристрою.

Відомий пристрій - аналог для додавання у СЗК (А.с. № 930317 СРСР, G 06 F 7/72, 1980р.). Пристрій містить групу вхідних регістрів, групу суматорів, групу елементів І, перетворювачі коду лишку за допоміжним модулем, суматор за допоміжним модулем, схему порівняння та зв'язки між ними.

Недолік аналога - значна кількість обладнання пристрою.

Відомий пристрій-аналог для додавання у СЗК (А.с. № 1134942 СРСР, G 06 F 7/72, G 06 F 11/10, 1985р. БВ № 2). Пристрій містить, групу вхідних регістрів, групу суматорів, групу елементів І, перетворювачі коду лишку за допоміжним модулем, комутатор переносу, групу дешифраторів, суматор за допоміжним модулем, блок визначення помилки та зв'язки між ними.

Недолік аналога - значна кількість обладнання пристрою.

Відомий пристрій - аналог для додавання у СЗК (А.с. № 1160408 СРСР, G 06 F 7/72, 1985р. БВ № 21). Пристрій містить групу вхідних регістрів, групу суматорів, групу елементів І, перетворювачі до коду лишку за допоміжним модулем, суматор за допоміжним модулем, схему порівняння та зв'язки між ними.

Недолік аналога - значна кількість обладнання пристрою.

Близьким за технічною суттю-аналогом до запропонованого винаходу є пристрій для складання чисел за модулем m модулярної системи числення (Патент № 50024 України, G 06 F 7/72. Б. В. № 10, 2010 р.). Пристрій містить перший і другий вхідні регістри, вихідний регістр дешифратор, групу ключових елементів, групу елементів І, елемент АБО, генератор імпульсів, перемножувач частоти, лічильник, кільцевий регістр зсуву, схему порівняння, чотири елементи І, причому, перший інформаційний вхід пристрою є входом першого вхідного регістра, вихід якого є входом дешифратора, виходи якого є першими входами відповідних ключових елементів, виходи яких підключено до перших входів відповідних елементів І групи, виходи яких через елемент АБО підключено до входу вихідного регістра, вихід якого є виходом пристрою, першу керуючу шину пристрою підключено до входу генератора імпульсів, вихід якого підключено до перших входів першого і другого елементів І, вихід першого елемента І підключено до входу лічильника, вихід якого підключено до других входів ключових елементів групи та до других входів елементів І групи, а також до других входів першого і другого елементів І, вихід другого елемента І підключено до входу перемножувача частоти, а виходи розрядів кільцевого регістра зсуву підключено до третіх входів відповідних елементів І групи, а другий інформаційний вхід пристрою підключено до входу другого вхідного регістра, вихід другого вхідного регістра підключено до другого входу схеми порівняння, а вихід перемножувача частоти є першими входами третього і четвертого елементів І, виходи яких підключено до відповідно першого і другого входів кільцевого регістра зсуву, а до других входів третього і четвертого елементів І підключено відповідно друга і третя керуючі шини пристрою.

Недолік аналога - значна кількість обладнання пристрою.

Найбільш близьким аналогом до запропонованого винаходу є пристрій для додавання і віднімання чисел за модулем m модулярної системи числення на основі кільцевого зсуву. Патент № 55454 (заявка u201008060) України, МПК (2009) G 06 F 7/00. Бюл. № 23 від 10.12. 2010р. Пристрій містить перший і другий вхідні регістри, вихідний регістр, перший дешифратор, перший шифратор, кільцевий регістр зсуву (КРЗ), першу, другу та третю групи елементів І, першу групу елементів АБО, схему порівняння (СП), лічильник імпульсів (ЛІ) і елемент заборони (ЕЗ), другий дешифратор, другий шифратор, другу групу елементів АБО, четверту та п'яту групи елементів І. При цьому перший і другий інформаційні входи пристрою підключено до входів відповідно першого та другого вхідних регістрів, виходи розрядів КРЗ підключено до перших входів елементів І першої групи, а вихід вихідного регістра є виходом пристрою, керуючий вхід пристрою підключено до першого входу ЕЗ, вихід якого підключено до першого входу ЕЗ, вихід якого підключено до керуючого входу КРЗ та до входу ЛІ, вихід якого підключено до перших входів СП, виходи якої підключено до других входів елементів І першої групи, а також до другого (забороненого) входу ЕЗ. Вихід другого вхідного регістра підключено до других входів СП, а виходи елементів І першої групи підключено до перших входів елементів І другої та третьої груп, виходи яких підключено до входів відповідно першого та другого шифраторів, виходи яких через елементи АБО першої групи підключено до входу вихідного регістра. Виходи

першого вхідного регістра підключено до перших входів елементів I четвертої та п'ятої груп, виходи яких підключено до входів відповідно першого та другого дешифраторів, виходи яких через елементи АБО другої групи підключено до входів відповідних розрядів РКЗ. До других входів елементів I другої та четвертої груп підключена шина подачі сигналу ознаки операції "додавання", а до других входів елементів I третьої та п'ятої груп підключена шина подачі сигналу ознаки операції "віднімання".

Недолік прототипу - значна кількість обладнання пристрою. Недолік пристрою-прототипу, в першу чергу, обумовлено наявністю двох шифраторів, двох дешифраторів, п'яти груп елементів I, груп елементів АБО та ін.

В основу запропонованого винаходу поставлена задача зменшення кількості обладнання пристрою.

Поставлена задача вирішується тим, що пристрій для додавання та віднімання лишків чисел за модулем містить перший і другий вхідні регістри, вихідний регістр, регістр кільцевого зсуву (РКЗ), дешифратор, шифратор, першу та другу групи елементів I, схему порівняння (СП), лічильник імпульсів (ЛІ), генератор імпульсів (ГІ), елемент заборони (ЕЗ), при цьому, перший і другий інформаційні входи пристрою підключено до входів відповідно першого та другого вхідних регістрів, вихід другого вхідного регістра підключено до першого входу СП, до другого входу якої підключено вихід ЛІ, керуючий вхід пристрою підключено до входу ГІ, вихід якого підключено до першого (інформаційного) входу ЕЗ, а також підключено до входу ЛІ, а вихід вихідного регістра є виходом пристрою. В пристрій введено перший та другий елементи I, при цьому вихід першого вхідного регістра підключено до входу дешифратора, а вихід шифратора підключено до входу вихідного регістра, вихід ЕЗ підключено до перших входів першого та другого елементів I, до других входів яких підключено входи подачі сигналів ознак, відповідно, операцій додавання і віднімання, а виходи першого та другого елементів I підключено відповідно до першого ("Додавання") та другого ("Віднімання") керуючих входів РКЗ, виходи дешифратора підключено до перших входів відповідних елементів I першої групи, виходи яких підключено до перших входів відповідних елементів I другої групи, а виходи розрядів РКЗ підключено до других входів відповідних елементів I другої групи, вихід СП підключено до другого (забороненого) входу ЕЗ, а також підключено до других входів елементів I першої групи і підключено до третіх входів елементів I другої групи, а виходи елементів I другої групи підключено до входів шифратора.

Введення вказаних ознак дозволяє зменшити кількість обладнання пристрою при збереженні всіх функціональних і технічних можливостей пристрою-прототипу. Кількість обладнання зменшується в основному за рахунок скорочення шифратора, дешифратора та трьох груп елементів I.

На кресленні представлена блок-схема винаходу, де: 1, 2 - перший та другий інформаційні входи пристрою; 3, 4 - перший та другий вхідні регістри; 5 - схема порівняння (СП); 6 - лічильник імпульсів (ЛІ); 7 - керуючий вхід пристрою; 8 - генератор імпульсів (ГІ); 9 - елемент заборони (ЕЗ); 10 - вихідний регістр; 11 - вихід пристрою; 12 - дешифратор (пристрій для перетворення двійкового коду до унітарного коду); 13 - шифратор (пристрій для перетворення унітарного коду до двійкового коду); 14, 15 - перший і другий елементи I; 16 - вхід подачі сигналу ознаки арифметичної операції додавання; 17 - вхід подачі сигналу ознаки арифметичної операції віднімання; 18, 19 - керуючі входи "Додавання" та "Віднімання" регістра кільцевого зсуву 20; 20 - регістр кільцевого зсуву (РКЗ); 21, 22 - перша та друга групи елементів I.

Перший 1 та другий 2 інформаційні входи пристрою підключено до входів відповідно першого 3 та другого 4 вхідних регістрів, вихід другого 4 вхідного регістра підключено до першого входу СП 5, до другого входу якої підключено вихід ЛІ 6, керуючий вхід 7 пристрою підключено до входу ГІ 8, вихід якого підключено до першого (інформаційного) входу ЕЗ 9, а також підключено до входу ЛІ 6, вихід вихідного регістра 10 є виходом 11 пристрою. Вихід першого 3 вхідного регістра підключено до входу дешифратора 12, а вихід шифратора 13 підключено до входу вихідного 10 регістра, вихід ЕЗ 9 підключено до перших входів першого 14 та другого 15 елементів I, до других входів яких підключено входи 16 та 17 подачі сигналів ознак відповідно операцій додавання і віднімання. Виходи першого 14 та другого 15 елементів I підключено, відповідно, до першого ("Додавання") 18 та другого ("Віднімання") 19 керуючих входів РКЗ 20. Виходи дешифратора 12 підключено до перших входів відповідних елементів I першої 21 групи, виходи яких підключено до перших входів відповідних елементів I другої 22 групи. Виходи розрядів РКЗ 20 підключено до других входів відповідних елементів I другої 22 групи. Вихід СП 5 підключено до другого (забороненого) входу ЕЗ 9, а також підключено до других входів елементів I першої 21 групи і підключено до третіх входів елементів I другої 22 групи, а виходи елементів I другої 22 групи підключено до входів шифратора 13.

Роботу пристрою будемо розглядати у двох режимах (креслення): перший (визначення значення $(a_i+b_i) \bmod m_i$ модульного додавання) та другий (визначення значення $(a_i-b_i) \bmod m_i$ модульного віднімання) режими.

Початкове вихідне значення вмісту та напрям (у позитивному напрямку, тобто проти часової стрілки або у негативному напрямку, тобто за часовою стрілкою) зсуву двійкових розрядів РКЗ 20 буде мати наступний вигляд (схема 1).

Схема 1. Вихідне значення вмісту та напрям зсуву двійкових розрядів РКЗ 20

Перший режим. Визначення значення суми $(a_i+b_i) \bmod m_i$. При цьому початкове вихідне значення вмісту розрядів РКЗ 20 і напрям (у позитивному напрямку, тобто проти часової стрілки) зсуву (присутній сигнал шини 16) розрядів РКЗ 20 буде мати наступний вигляд (схема 2)

Схема 2. Вихідне значення вмісту та напрям зсуву двійкових розрядів РКЗ 20 при реалізації $(a_i+b_i) \bmod m_i$

Пристрій функціонує наступним чином. Перший a_i і другий b_i лишки чисел за відповідними входами пристрою 1 і 2 у двійковому коді надходять до першого 3 і другого 4 вхідних регістрів. З виходу регістра 3 значення a_i надходить до входу дешифратора 12, з виходу якого унітарний код, що відповідає значенню a_i , надходить до перших входів елементів I першої 21 групи. Другий лишок b_i у двійковому коді надходить до перших входів схеми порівняння 5. З початку роботи, сигнал керуючого входу 7 пристрою надходить до входу ПІ 8, з виходу якого імпульси надходять на вхід ЛІ 6 та на керуючий вхід КРЗ 9, що забезпечує зсув вихідного вмісту двійкових розрядів КРЗ 20 на b_i двійкових розрядів у негативному (за часовою стрілкою) напрямку (присутній сигнал шини 16). При наявності у ЛІ 6 числового значення b_i вихідний сигнал ("Рівно") СП 5 закриває елемент 9 заборони та забороняє подачу імпульсів до КРЗ 20 і одночасно відкриває елементи I першої 21 та другої 22 груп. В цьому випадку вміст КРЗ 20 через відкриті елементи I другої 22 групи надходить до входу шифратора 13, з виходу якого значення $(a_i+b_i) \bmod m_i$ результату операції модульного додавання надходить до входу вихідного 10 регістра.

Другий режим. Визначення значення величини $(a_i-b_i) \bmod m_i$. При цьому початкове вихідне значення вмісту розрядів РКЗ 20 і напрям зсуву (присутній сигнал шини 17) розрядів РКЗ 19 буде мати наступний вигляд (схема 3)

Схема 3. Вихідне значення вмісту та напрям зсуву двійкових розрядів РКЗ 20 при реалізації $(a_i-b_i) \bmod m_i$

Для другого режиму функціонування пристрою імпульси надходять до входу РКЗ 20, зрушуючи його вміст у негативному (за часовою стрілкою) напрямку на b_i двійкових розрядів РКЗ 20. В цьому випадку вміст КРЗ 20, через відкриті елементи I другої 22 групи, надходить до входу шифратора 12, з виходу якого значення $(a_i-b_i) \bmod m_i$ результату операції модульного віднімання надходить до входу вихідного 10 регістра.

Розглянемо приклади конкретного виконання операцій $(a_i+b_i) \bmod m_i$ і $(a_i-b_i) \bmod m_i$ (схема 5) для $m_i=5$. В таблиці позначено означені величини першого a_i та другого доданків b_i .

Таблиця

Значення доданків

Значення доданків a_i та b_i		
У десятковому коді	У двійковому коді	В унітарному коді
0	000	00001
1	001	00010
2	010	00100
3	011	01000
4	100	10000

Перший режим

Приклад 1. Необхідно визначити результат операції $(a_i+b_i) \bmod m_i$ для $a_i=011$, $b_i=100$ (див. фіг. 1). Перший лишок $a_i=011$ визначає вихідне значення вмісту РКЗ 20 (третій розряд РКЗ 20), що відповідає значенню унітарного коду 01000 (таблиця). Другий лишок $b_i=100$ визначає кількість (чотири) зсувів двійкових розрядів РКЗ 20 у позитивному напрямку. Таким чином, у розрядах РКЗ міститься значення першого $a_i=011$ доданку в унітарному коді, тобто, значення 01000. Після чотирьох ($b_i=100$) зсувів розрядів РКЗ 20, отримуємо у розрядах РКЗ 20 наступне значення

Схема 4

На схемі 4 представлено унітарний код 00100, що міститься у РКЗ 20 після чотирьох $b_i=100$ зсувів двійкових розрядів. Значення унітарного коду 00100 через відкриті елементи I другої 22 групи надходить до входу шифратора 13, з виходу якого значення 010 надходить до входу вихідного 10 регістра (таблиця).

5 Перевірка: $(a_i+b_i)\bmod m_i=(011+100)=010(\bmod 5)$ (таблиця).

Приклад 2. Необхідно визначити результат операції $(a_i+b_i)\bmod m_i$ для $a_i=100$, $b_i=100$ (див. фіг. 1).). Перший лишок $a_i=100$ визначає вихідне значення вмісту РКЗ 20 (четвертий розряд РКС 20), що відповідає значенню унітарного коду 10000 (таблиця). Другий лишок $b_i=100$ визначає кількість (чотири) зсувів двійкових розрядів РКЗ 20 у позитивному напрямку. Таким чином, у розрядах РКЗ міститься значення першого $a_i=100$ доданку в унітарному коді, тобто, значення 01000. Після чотирьох ($b_i=100$) зсувів розрядів РКЗ 20, отримуємо у розрядах РКЗ 20 наступне значення

Схема 5

Перевірка: $(a_i+b_i)\bmod m_i=(100+100)=011(\bmod 5)$ (таблиця).

15 Другий режим

Приклад 3. Необхідно визначити результат операції $(a_i-b_i)\bmod m_i$ для $a_i=011$, $b_i=100$ (креслення, таблиця). Перший лишок $a_i=011$ визначає вихідне значення вмісту РКЗ 20, що відповідає значенню унітарного коду 01000 (таблиця). Другий лишок $b_i=100$ визначає кількість (чотири) зсувів двійкових розрядів РКЗ 20 у негативному напрямку (присутній сигнал шини 17).

20 Схема 6

На схемі 6 остаточно представлено унітарний код 10000, що міститься у РКЗ 20 після чотирьох зсувів двійкових розрядів. Значення унітарного коду 10000 через відкриті елементи I другої 22 групи надходить до входу шифратора 13, з виходу якого значення 100 (таблиця) надходить до входу вихідного 10 регістра.

25 Перевірка: $(a_i-b_i)\bmod m_i=(011-100)=100(\bmod 5)$.

Приклад 4. Необхідно визначити результат операції $(a_i-b_i)\bmod m_i$ для $a_i=000$, $b_i=100$ (креслення, таблиця). Перший лишок $a_i=000$ визначає вихідне значення вмісту РКЗ 20, що відповідає значенню унітарного коду 0000 (таблиця).

Схема 7

30 Другий лишок $b_i=100$ визначає кількість (чотири) зсувів двійкових розрядів РКЗ 20 у негативному напрямку (присутній сигнал шини 17).

Перевірка: $(a_i-b_i)\bmod m_i=(000-100)=001(\bmod 5)$.

Наведені приклади реалізації модульних операцій підтверджують достовірність отримання результатів за допомогою запропонованого винаходу.

35 Запропонований винахід дозволяє суттєво зменшити кількість обладнання пристрою при збереженні всіх функціональних і технічних можливостей пристрою-прототипу. Кількість обладнання зменшується в основному за рахунок скорочення елементів шифратора, елементів дешифратора та виключення з прототипу трьох груп елементів I.

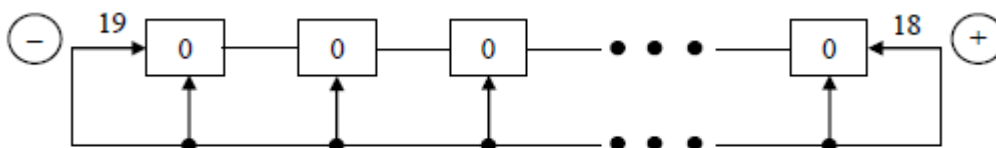


Схема 1. Вихідне значення вмісту та напрям зсуву двійкових розрядів РКЗ 20

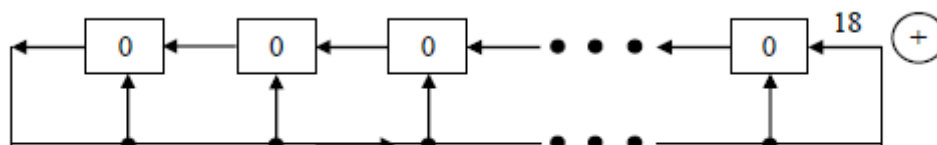


Схема 2. Вихідне значення вмісту та напрям зсуву двійкових розрядів РКЗ 20 при реалізації $(a_i + b_i) \bmod m_i$

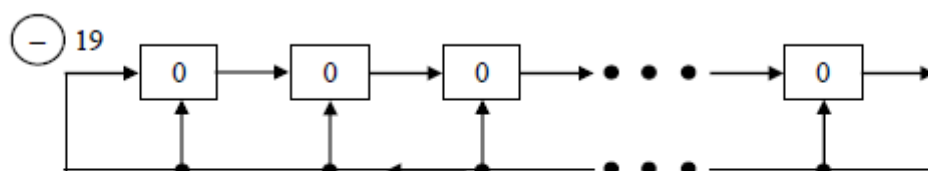
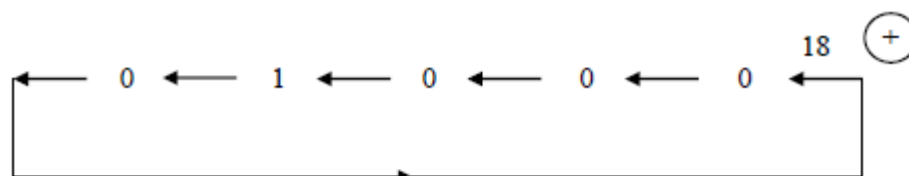
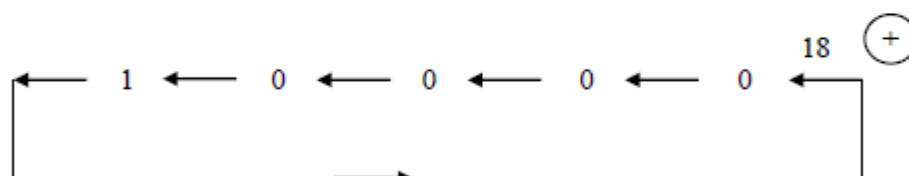


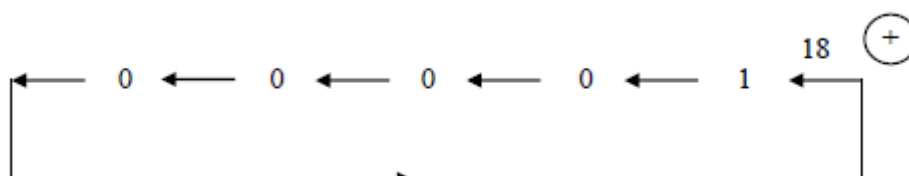
Схема 3. Вихідне значення вмісту та напрям зсуву двійкових розрядів РКЗ 20 при реалізації $(a_i - b_i) \bmod m_i$



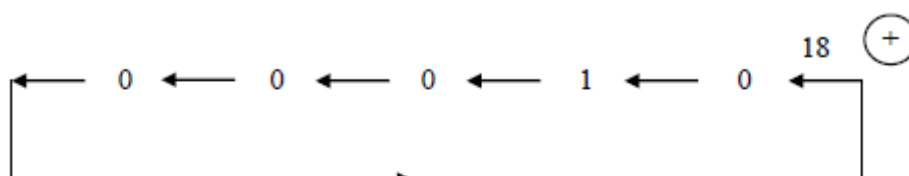
Вихідне значення РКЗ 20 $b_i = 0$



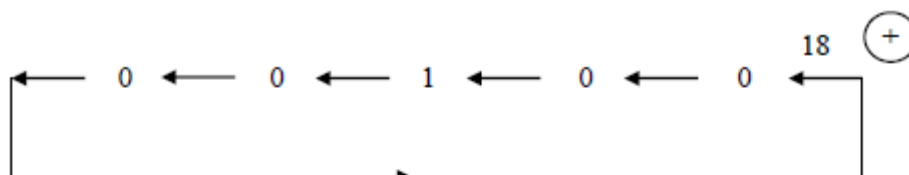
Перший зсув $b_i = 1$



Другий зсув $b_i = 2$

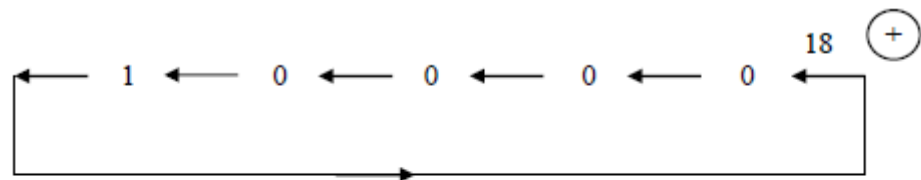


Третій зсув $b_i = 3$

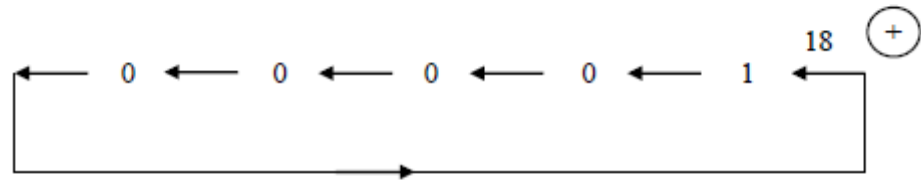


Четвертий зсув $b_i = 4$. Результат операції

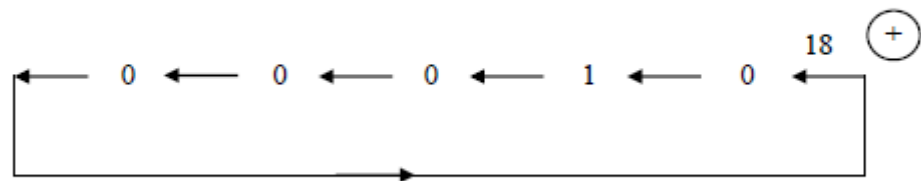
Схема 4



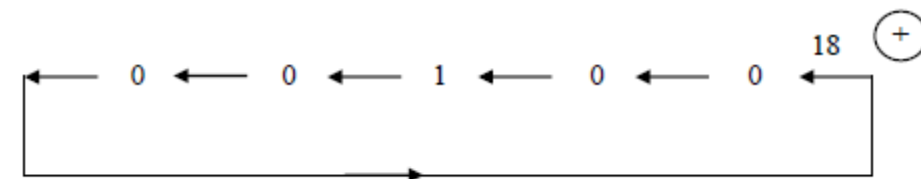
Вихідне значення КРЗ 20 $b_i = 0$



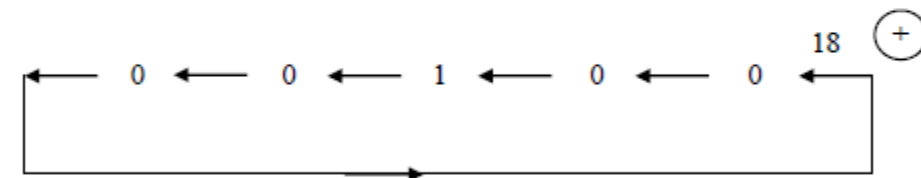
Перший зсув $b_i = 1$



Другий зсув $b_i = 2$

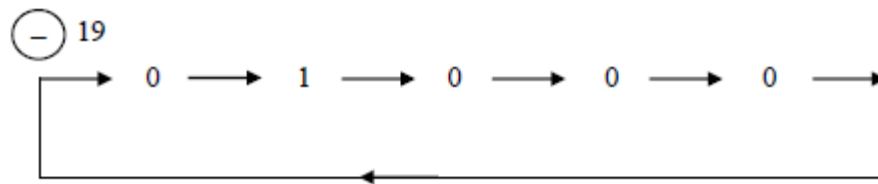


Третій зсув $b_i = 3$

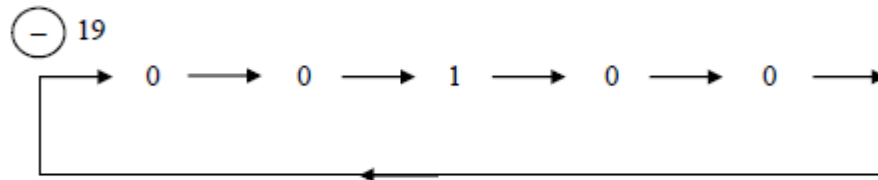


Четвертий зсув $b_i = 4$. Результат операції

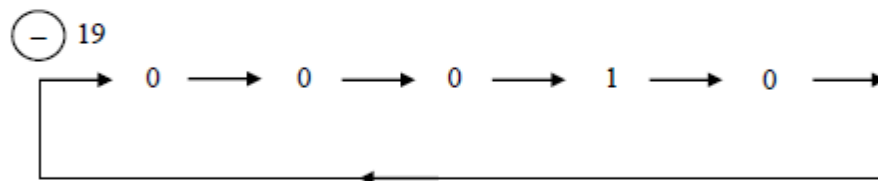
Схема 5



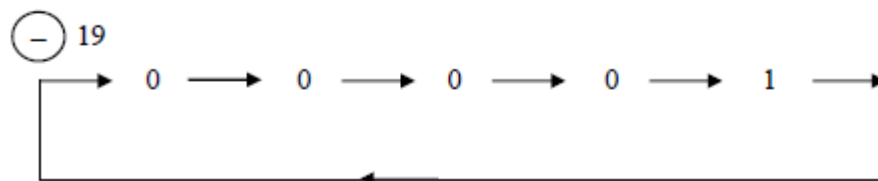
Вихідне значення КРЗ 20 $b_i = 0$



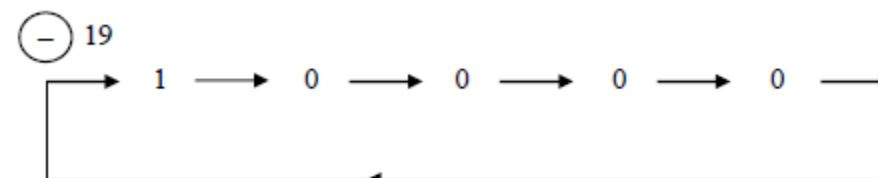
Перший зсув $b_i = 1$



Другий зсув $b_i = 2$

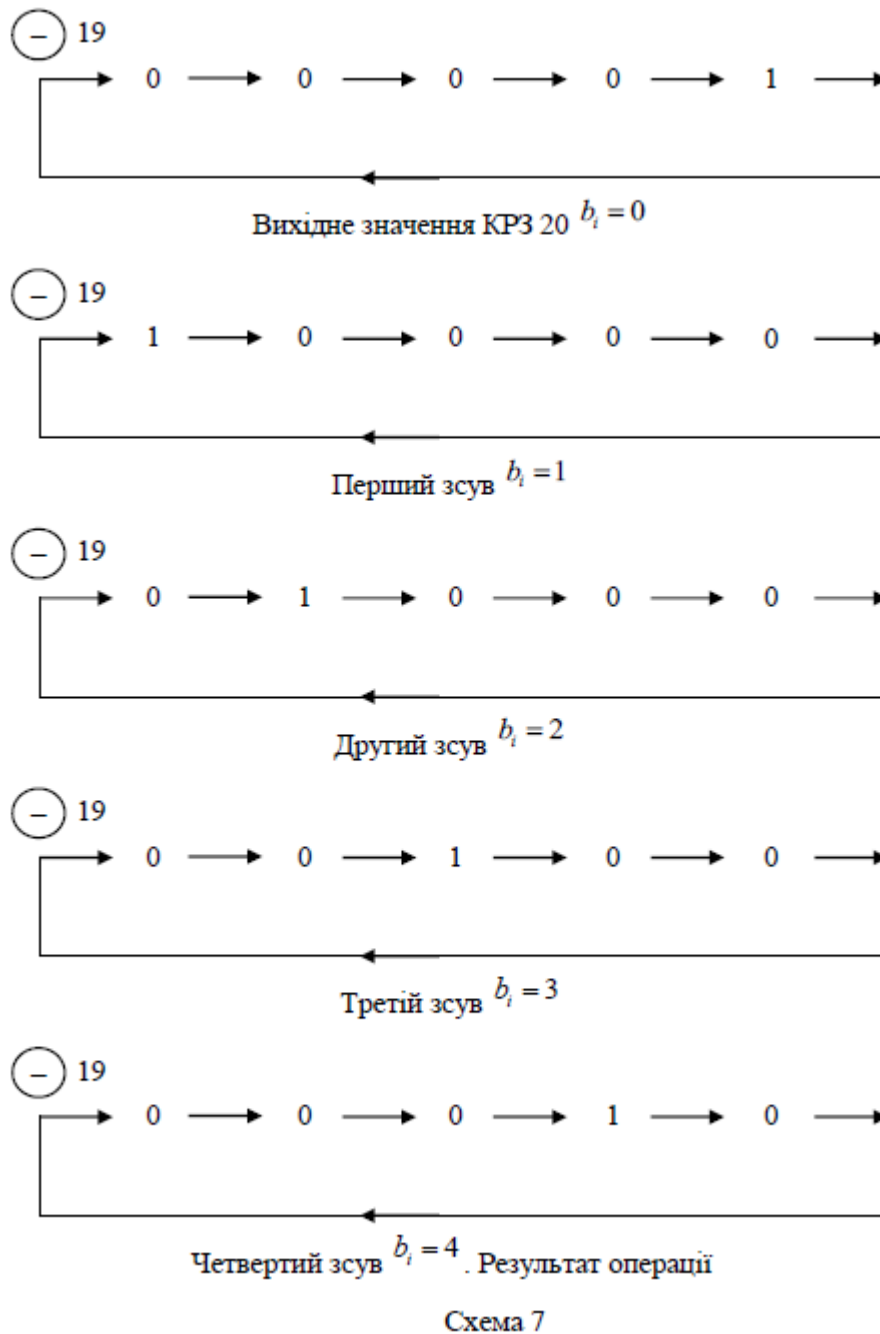


Третій зсув $b_i = 3$



Четвертий зсув $b_i = 4$. Результат операції

Схема 6



ФОРМУЛА ВИНАХОДУ

- 5 Пристрій для додавання та віднімання лишків чисел за модулем, що містить перший і другий вхідні регістри, вихідний регістр, регістр кільцевого зсуву (РКЗ), дешифратор, шифратор, першу та другу групи елементів І, схему порівняння (СП), лічильник імпульсів (ЛІ), генератор імпульсів (ГІ), елемент заборони (ЕЗ), при цьому перший і другий інформаційні входи пристрою підключено до входів, відповідно, першого та другого вхідних регістрів, вихід другого вхідного
- 10 регістра підключено до першого входу СП, до другого входу якої підключено вихід ЛІ, керуючий вхід пристрою підключено до входу ГІ, вихід якого підключено до першого, інформаційного, входу ЕЗ, а також підключено до входу ЛІ, вихід вихідного регістра є виходом пристрою, який **відрізняється** тим, що введено перший та другий елементи І, при цьому вихід першого вхідного регістра підключено до входу дешифратора, а вихід шифратора підключено до входу вихідного регістра, вихід ЕЗ підключено до перших входів першого та другого елементів І, до других входів яких підключено входи подачі сигналів ознак, відповідно, операцій додавання і віднімання, а виходи першого та другого елементів І підключено, відповідно, до першого,
- 15

- "Додавання", та другого, "Віднімання", керуючих входів РКЗ, виходи дешифратора підключено до перших входів відповідних елементів I першої групи, виходи яких підключено до перших входів відповідних елементів I другої групи, а виходи розрядів РКЗ підключено до других входів відповідних елементів I другої групи, вихід СП підключено до другого, забороненого, входу ЕЗ, а також підключено до других входів елементів I першої групи і підключено до третіх входів елементів I другої групи, а виходи елементів I другої групи підключено до входів шифратора.
- 5

