



МІНІСТЕРСТВО
ЕКОНОМІЧНОГО
РОЗВИТКУ І ТОРГІВЛІ
УКРАЇНИ

УКРАЇНА

(19) **UA** (11) **130809** (13) **U**
(51) МПК
G06F 7/72 (2006.01)

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

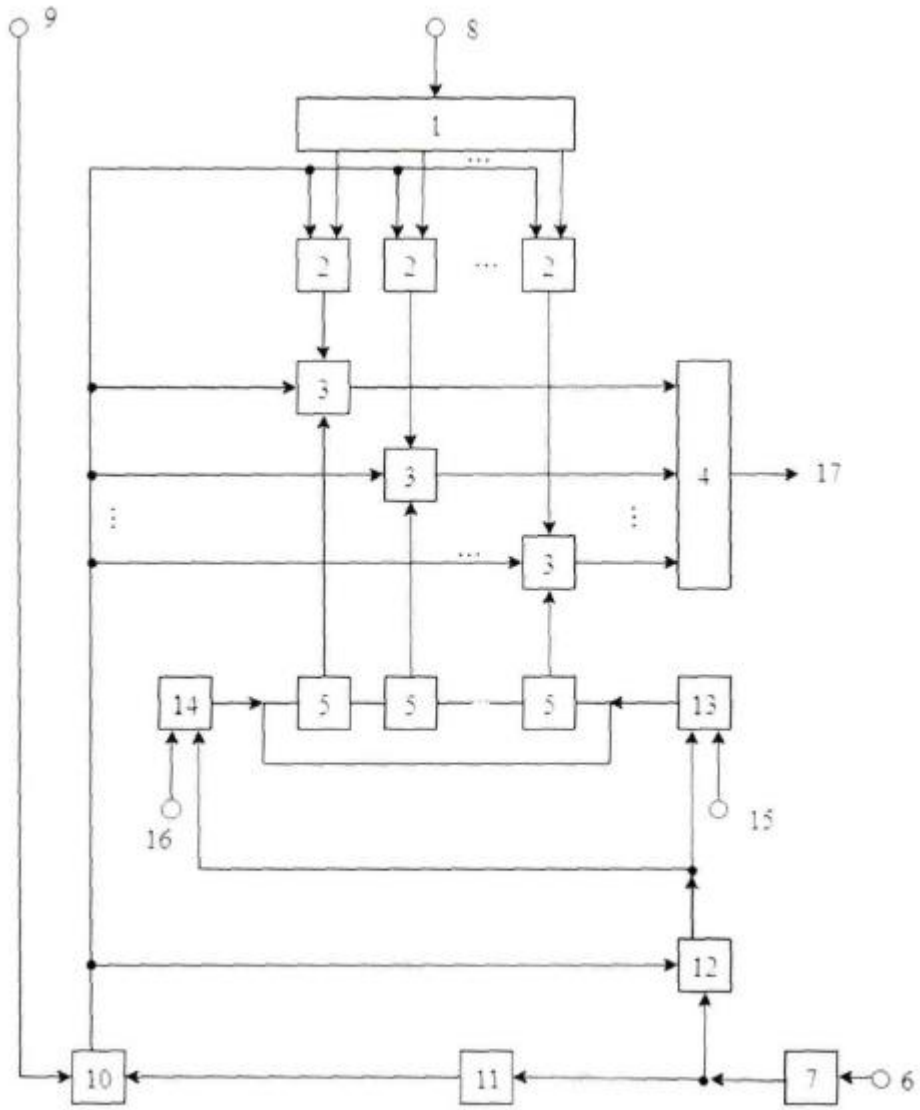
(21) Номер заявки: u 2018 06755	(72) Винахідник(и): Краснобаєв Віктор Анатолійович (UA), Замула Олександр Андрійович (UA), Рассомахін Сергій Геннадійович (UA), Янко Аліна Сергіївна (UA)
(22) Дата подання заявки: 14.06.2018	
(24) Дата, з якої є чинними права на корисну модель: 26.12.2018	(73) Власник(и): ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В.Н. КАРАЗІНА, пл. Свободи, 4, м. Харків, 61022 (UA)
(46) Публікація відомостей про видачу патенту: 26.12.2018, Бюл.№ 24	

(54) ПРИСТРІЙ ДЛЯ ДОДАВАННЯ ТА ВІДНІМАННЯ ЛИШКІВ a_i І b_i ЗА МОДУЛЕМ m_i ЧИСЛА, ЩО ПРЕДСТАВЛЕНЕ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

(57) Реферат:

Пристрій для додавання та віднімання лишків a_i і b_i за модулем m_i числа, що представлено у системі залишкових класів, містить дешифратор, групу ключових елементів, групу елементів I , перший і другий елементи I , генератор імпульсів, лічильник, регістр кільцевого зсуву (РКЗ), схему порівняння, елемент АБО, виходи дешифратора є першими входами відповідних ключових елементів групи, виходи яких підключено до перших входів відповідно елементів I групи, виходи яких підключено до входів елемента АБО, виходи розрядів кільцевого регістра зсуву підключено до других входів відповідних елементів I групи, перша керуюча шина пристрою підключена до входу генератора імпульсів. При цьому введено вентильний елемент, а перший інформаційний вхід пристрою є входом дешифратора, а другий інформаційний вхід пристрою є першим входом схеми порівняння, другим входом якої є вихід лічильника, а вихід генератора імпульсів підключено до входу лічильника та до першого (інформаційного) входу вентильного елемента, вихід якого підключено до перших входів першого та другого елементів I , виходи яких підключені відповідно до першого та другого керуючих входів РКЗ, до других входів першого та другого елементів I підключені відповідно друга та третя керуючі шини пристрою, а вихід схеми порівняння підключено до другого входу вентильного елемента.

UA 130809 U



Фиг. 1

Корисна модель (пристрій) 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 пристрій (аналог) для додавання у СЗК (А.с. № 446056 СРСР, G06F 7/72, 1971р.).
5 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 - низькі функціональні можливості, що обумовлені неможливістю безпосередньо виконувати одночасно арифметичні операції додавання і віднімання лишків a_i і b_i за модулем m_i числа у СЗК.

10 Відомий пристрій (аналог) для додавання у СЗК (А.с. № 930317 СРСР, G06F 7/72, 1980 р.). Пристрій містить, групу вхідних регістрів, групу суматорів, групу елементів I, перетворювачі коду лишку за допоміжним модулем, суматор за допоміжним модулем, схему порівняння та зв'язки між ними.

15 Недолік аналога - низькі функціональні можливості, що обумовлені неможливістю безпосередньо виконувати одночасно арифметичні операції додавання і віднімання лишків a_i і b_i за модулем m_i числа у СЗК.

20 Відомий пристрій (аналог) для додавання у СЗК (А.с. № 1134942 СРСР, G06F 7/72, G06F 11/10, 1985 р. БВ № 2). Пристрій містить, групу вхідних регістрів, групу суматорів, групу елементів I, перетворювачі коду лишку за допоміжним модулем, комутатор переносу, групу дешифраторів, суматор за допоміжним модулем, блок визначення помилки та зв'язки між ними.

Недолік аналога - низькі функціональні можливості, що обумовлені неможливістю безпосередньо виконувати одночасно арифметичні операції додавання і віднімання лишків a_i і b_i за модулем m_i числа у СЗК.

25 Відомий пристрій (аналог) для додавання у СЗК (А.с. № 1160408 СРСР, G06F 7/72, 1985р. БВ № 21). Пристрій містить, групу вхідних регістрів, групу суматорів, групу елементів I, перетворювачі до коду лишку за допоміжним модулем, суматор за допоміжним модулем, схему порівняння та зв'язки між ними.

30 Недолік аналога - низькі функціональні можливості, що обумовлені неможливістю безпосередньо виконувати одночасно арифметичні операції додавання і віднімання лишків a_i і b_i за модулем m_i числа у СЗК.

Найбільш близьким за технічною суттю (найближчим аналогом) до запропонованої корисної моделі є пристрій для складання чисел за модулем m_i модулярної системи числення (патент № 50024 України, G06F 7/72. Б. В. № 10, 2010р.). Пристрій містить перший і другий вхідні регістри, вихідний регістр дешифратор, групу ключових елементів, групу елементів I, елемент АБО, генератор імпульсів, перемножувач частоти, лічильник, кільцевий регістр зсуву, схему порівняння, чотири елементи I, 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 вхідних відповідних елементів I 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 I, вихід першого елемента I підключено до входу лічильника, вихід якого підключено до других входів ключових елементів групи та до других входів елементів I групи, а також до других входів першого і другого елементів I, вихід другого елемента підключено до входу перемножувача частоти, а виходи розрядів кільцевого регістра зсуву підключено до третіх входів відповідних елементів I 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 I, виходи яких підключено до відповідно першого і другого входів кільцевого регістра зсуву, а до других входів третього і четвертого елементів I підключено відповідно друга і третя керуючі шини пристрою.

50 Недолік найближчого аналога - низькі функціональні можливості, що обумовлені неможливістю безпосередньо виконувати одночасно арифметичні операції додавання і віднімання лишків a_i і b_i за модулем m_i числа у СЗК.

55 В основу запропонованої корисної моделі поставлено задачу (мету) розширення функціональних можливостей пристрою за рахунок спроможності безпосередньо виконувати одночасно арифметичні операції додавання і віднімання лишків a_i і b_i за модулем m_i числа у СЗК.

60 Поставлена задача (досягнення мети) вирішується тим, що пристрій містить дешифратор, групу ключових елементів, групу елементів I, перший і другий елементи I, генератор імпульсів, лічильник, регістр кільцевого зсуву (РКЗ), схему порівняння, елемент АБО, при цьому виходи

дешифратора є першими входами відповідних ключових елементів групи, виходи яких підключено до перших входів відповідно елементів I групи, виходи яких підключено до входів елемента АБО, виходи розрядів кільцевого регістру зсуву підключено до других входів відповідних елементів I групи, перша керуюча шина пристрою підключена до входу генератора імпульсів. В пристрій введено вентиляльний елемент при цьому, перший інформаційний вхід пристрою є входом дешифратора, а другий інформаційний вхід пристрою є першим входом схеми порівняння, другим входом якої є вихід лічильника, а вихід генератора імпульсів підключено до входу лічильника та до першого (інформаційного) входу вентиляльного елемента, вихід якого підключено до перших входів першого та другого елементів I, виходи яких підключені відповідно до першого та другого керуючих входів РКЗ, до других входів першого та другого елементів I підключені відповідно друга та третя керуючі шини пристрою, а вихід схеми порівняння підключено до другого (забороненого) входу вентиляльного елемента, а також до других входів ключових елементів групи і до третіх входів елементів I групи, вихід елемента АБО є виходом пристрою.

Введення вказаних ознак дозволяє розширити функціональні можливості запропонованої корисної моделі (пристрою) за рахунок спроможності безпосередньо виконувати одночасно дві арифметичні операції додавання і віднімання лишків a_i і b_i за модулем m_i числа у СЗК.

На фіг. 1 представлена блок-схема корисної моделі, де: 1 - дешифратор (пристрій для перетворення двійкового коду в унітарний); 2 - група ключових елементів; 3 - група елементів / перший; 4 - елемент АБО; 5 - регістр кільцевого зсуву (РКЗ); 6 - перша керуюча шина пристрою; 7 - генератор імпульсів; 8 - перший інформаційний вхід пристрою; 9 - другий інформаційний вхід пристрою; 10 - схема порівняння; 11 - лічильник імпульсів; 12 - вентиляльний елемент; 13, 14 - перший і другий елементи I; 15 та 16 - друга (шина подачі сигналу ознаки арифметичної операції додавання) та третя (шина подачі сигналу ознаки арифметичної операції віднімання) керуючі шини пристрою; 17 - вихід пристрою.

Виходи дешифратора 1 є першими входами відповідних ключових елементів групи 2, виходи яких підключено до перших входів відповідно елементів I групи 3, виходи яких підключено до входів елемента АБО 4. Виходи розрядів РКЗ 5 підключено до других входів відповідних елементів I групи 3. Перша 6 керуюча шина пристрою підключена до входу генератора імпульсів 7. Перший 8 інформаційний вхід пристрою є входом дешифратора 1, а другий 9 інформаційний вхід пристрою є першим входом схеми порівняння 10, другим входом якої є вихід лічильника 11. Вихід генератора 7 імпульсів підключено до входу лічильника 11 та до першого (інформаційного) входу вентиляльного елемента 12, вихід якого підключено до перших входів першого 13 та другого 14 елементів I, виходи яких підключені відповідно до першого та другого керуючих входів РКЗ 5. До других входів першого 13 та другого 14 елементів I підключені відповідно друга 15 та третя 16 керуючі шини пристрою. Вихід схеми порівняння 10 підключено до другого (забороненого) входу вентиляльного елемента 12, а також до других входів ключових елементів групи 2 і до третіх входів елементів I групи 3. Вихід елемента АБО 4 є виходом 17 пристрою.

Роботу пристрою будемо розглядати у двох режимах (фіг. 1). Вихідне значення вмісту розрядів РКЗ 5 зазначене на фіг. 2.

Перший режим. Визначення $(a_i + b_i) \bmod m_i$. При цьому вихідне значення вмісту розрядів РКЗ 5 і напрям зсуву (присутній сигнал шини 15) розрядів РКЗ 5 зазначене на фіг. 3.

Пристрій функціонує наступним чином. Перше a_i число у двійковому кодi за шиною першого інформаційного входу пристрою 8 надходить до входу дешифратора 1, з виходу якого число a_i в унітарному кодi надходить до першого входу a_i -го $i = 0, m_i - 1$ ключового елемента 2, що визначає a_i -й розряд РКЗ 5, з якого у подальшому буде визначатися результат операції $(a_i + b_i) \bmod m_i$ (вихід a_i -го 2 ключового елемента відкриває a_i -й елемент I групи 3). Друге число b_i у двійковому кодi за шиною другого інформаційного входу пристрою 9 поступає до першого входу схеми порівняння 10. Сигнал першої 6 керуючої шини пристрою запускає генератор 7 імпульсів, з виходу якого імпульси надходять до входу лічильника імпульсів 11, з виходу якого його вміст надходить до другого входу схеми порівняння 10. Одночасно, через відкритий вентиляльний елемент 12, відкритий перший 13 елемент I, імпульси надходять до входу РКЗ 5, що приводить до зсуву його вмісту у позитивному (проти часової стрілки) напрямку на b_i розрядів РКЗ 5. Якщо у лічильнику 11 міститься значення b_i , тоді вихідний сигнал схеми 10 порівняння відкриває a_i -й ключовий елемент групи 2 та a_i -й елемент I 3, а також закриває вентиляльний елемент 12. В цьому випадку вміст $(a_i + b_i) \bmod m_i$, a_i -го розряду РКЗ 5 через a_i -й елемент I 3, через елемент АБО 4 надходить до виходу 17 пристрою.

Другий режим. Визначення $(a_i - b_i) \bmod m_i$. При цьому вихідне значення вмісту розрядів РКЗ 5 і напрям зсуву (присутній сигнал шини 16) розрядів РКЗ 5 зазначені на фіг. 4.

Для другого режиму функціонування пристрою через відкритий вентиляльний елемент 12, відкритий другий 14 елемент I, імпульси надходять до входу РКЗ 5, зрушуючи його вміст у негативному (за часової стрілки) напрямку на b_i розрядів РКЗ 5. В цьому випадку вміст $(a_i - b_i) \bmod m_i$ a_i -го розряду РКЗ 5 через a_i -й елемент I 3, через елемент АБО 4 надходить до виходу 17 пристрою.

Розглянемо приклади конкретного виконання операцій $(a_i + b_i) \bmod m_i$ і $(a_i - b_i) \bmod m_i$ для $m_i = 5$. В цьому випадку вихідний зміст розрядів РКЗ 5 для першого та другого режимів функціонування пристрою представлено на фіг. 5 і фіг. 6 відповідно.

Приклад 1. Необхідно визначити результат операції $(a_i + b_i) \bmod m_i$ для $(a_i = 010, b_i = 011)$. Перше число $a_i = 010$ визначає другий розряд РКЗ 5, за вмістом якого визначається результат операції $(a_i + b_i) \bmod m_i$. Перше число $a_i = 010$ за шиною 8 надходить до входу дешифратора 1, з виходу якого число $a_i = 010$ в унітарному коді, що відповідає значенню два, надходить на перший вхід другого ключового елемента 2, з виходу якого надходить на перший вхід другого елемента I групи 3. Друге число $b_i = 011$ за шиною другого інформаційного входу пристрою 9 значення 010 надходить на перший вхід схеми порівняння 10. Сигнал шини 6 запускає генератор 7 імпульсів, що дає зсув значення вихідних (фіг. 7) розрядів РКЗ 5 у негативному напрямку на три ($b_i = 011$) розряди.

Таким чином, значення 000 другого ($a_i = 010$) розряду РКЗ 5 через другий елемент I 3, через елемент АБО 4 надходить на вихід 17 пристрою.

Перевірка: $(a_i + b_i) \bmod m_i = (010 + 011) = 000 \pmod{5}$.

Приклад 2. Необхідно визначити результат операції $(a_i - b_i) \bmod m_i$ для $a_i = 010, b_i = 011$ (див. фіг. 8). Перше число $a_i = 010$ визначає вміст другого розряду РКЗ 5, з якого визначається результат операції $(a_i - b_i) \bmod m_i$. На вхід 9 подається значення $b_i = 011$. В цьому випадку кількість зсуву розрядів РКЗ 5, в негативному (за часовою стрілкою) напрямку, дорівнює трьом.

Результат операції 100, що міститься у другому розряді РКЗ 5, через елемент АБО 4 надходить до виходу 17 пристрою.

Перевірка: $(a_i - b_i) \bmod m_i = (010 - 011) = 100 \pmod{5}$.

Таким чином, запропонована корисна модель дозволяє суттєво розширити функціональні можливості пристрою-найближчого аналога. Це здійснюється за рахунок можливості додатково до реалізації операції додавання лишків a_i і b_i за модулем m_i виконання операції віднімання лишків a_i і b_i за модулем m_i чисел у СЗК. В цьому випадку, при необхідності, запропонована корисна модель може безпосередньо виконувати дві арифметичні операції: додавання $(a_i + b_i) \bmod m_i$ та віднімання $(a_i - b_i) \bmod m_i$ лишків a_i і b_i за модулем m_i чисел $A = (a_1, a_2, \dots, a_n)$ і $B = (b_1, b_2, \dots, b_n)$, що представлені у СЗК.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Пристрій для додавання та віднімання лишків a_i і b_i за модулем m_i числа, що представлене у системі залишкових класів, що містить дешифратор, групу ключових елементів, групу елементів I, перший і другий елементи I, генератор імпульсів, лічильник, регістр кільцевого зсуву (РКЗ), схему порівняння, елемент АБО, при цьому виходи дешифратора є першими входами відповідних ключових елементів групи, виходи яких підключено до перших входів відповідно елементів I групи, виходи яких підключено до входів елемента АБО, виходи розрядів кільцевого регістра зсуву підключено до других входів відповідних елементів I групи, перша керуюча шина пристрою підключена до входу генератора імпульсів, який **відрізняється** тим, що введено вентиляльний елемент, при цьому перший інформаційний вхід пристрою є входом дешифратора, а другий інформаційний вхід пристрою є першим входом схеми порівняння, другим входом якої є вихід лічильника, а вихід генератора імпульсів підключено до входу лічильника та до першого (інформаційного) входу вентиляльного елемента, вихід якого підключено до перших входів першого та другого елементів I, виходи яких підключені відповідно до першого та другого керуючих входів РКЗ, до других входів першого та другого елементів I підключені відповідно друга та третя керуючі шини пристрою, а вихід схеми порівняння підключено до другого (забороненого) входу вентиляльного елемента, а також до других входів ключових елементів групи і до третіх входів елементів I групи, вихід елемента АБО є виходом пристрою.

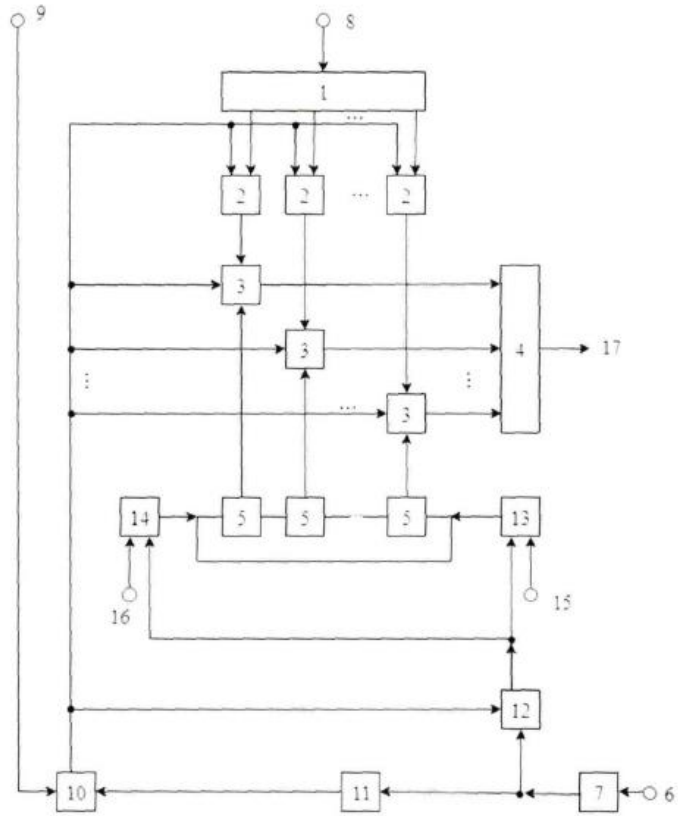


Fig. 1

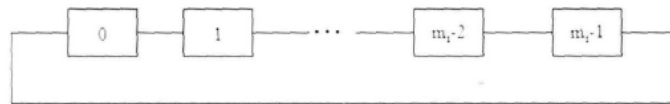


Fig. 2

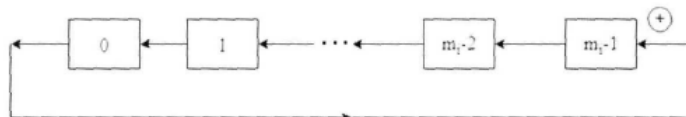


Fig. 3

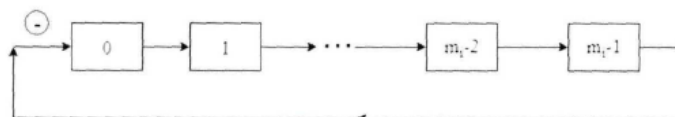


Fig. 4

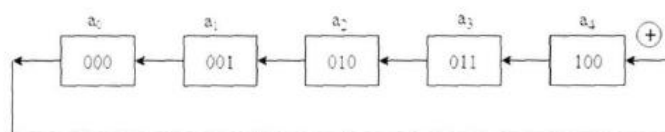
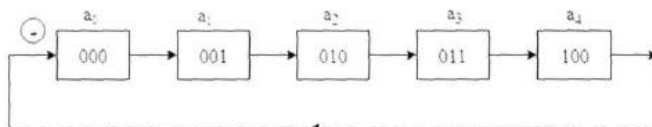
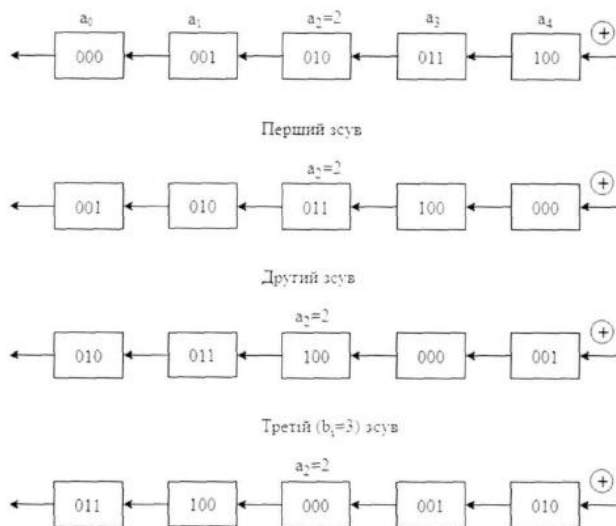


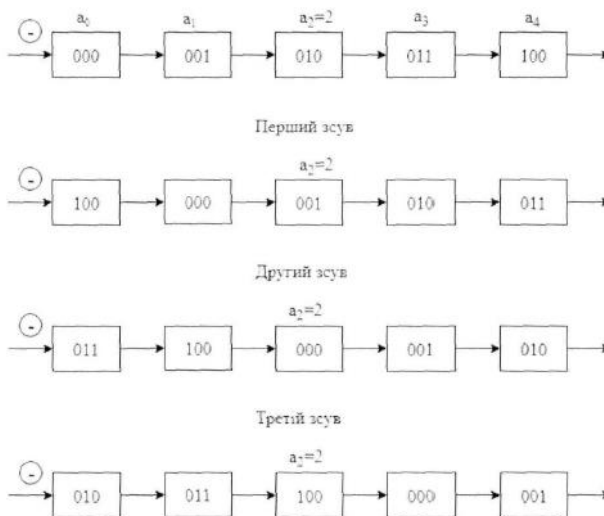
Fig. 5



Фиг. 6



Фиг. 7



Фиг. 8