МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

УКРАЇНА **(19) UA** **(11) 129249** **(13) U**

(51) МПК
G06F 7/72 (2006.01)

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2018 04418**
(22) Дата подання заявки: **23.04.2018**
(24) Дата, з якої є чинними права на корисну модель: **25.10.2018**
(46) Публікація відомостей про видачу патенту: **25.10.2018, Бюл.№ 20**

(72) Винахідник(и):
Краснобаєв Віктор Анатолійович (UA),
Замула Олександр Андрійович (UA),
Рассомахін Сергій Геннадійович (UA),
Янко Аліна Сергіївна (UA)

(73) Власник(и):
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В.Н. КАРАЗІНА,
пл. Свободи, 4, м. Харків, 61022 (UA)

(54) ПРИСТРІЙ ДЛЯ ПІДНЕСЕННЯ ЧИСЕЛ ДО КВАДРАТА У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

(57) Реферат:

Пристрій для піднесення чисел до квадрата у системі залишкових класів (СЗК) містить перший вхідний і перший вихідний регістри, перший дешифратор, першу групу елементів АБО та перший шифратор, крім того, введено (n-1) - н вхідних і вихідних регістрів (n - кількість основ СЗК), (n-1) - н дешифраторів, (n-1) - н груп елементів АБО, та (n-1) - н шифраторів, при цьому і-й ($i=\overline{1,n}$) вхід пристрою підключено до входу і-го вхідного регістра, вихід якого підключено до входу і-го дешифратора, виходи якого попарно підключено до входів відповідних елементів АБО і-ї групи, виходи яких підключено до відповідних входів і-го шифратора, вихід якого підключено до входу і-го вихідного регістра, вихід якого є і-м виходом пристрою, а нульовий вихід і-го дешифратора безпосередньо підключено до нульового входу і-го шифратора.

UA 129249 U

Корисна модель (пристрій) належить до галузі автоматики й обчислювальної техніки та може бути використана в комп'ютерних системах і компонентах, що функціонують у системі залишкових класів (СЗК).

Відомий пристрій (аналог), що містить вхідний та вихідний регістри, елементи АБО та І, дешифратор та ін. (Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М, "Советское радио", 1968, с. 327-340).

Недолік аналога низькі функціональні можливості пристрою. Неможливість виконання операції піднесення чисел до квадрата у СЗК.

Близьким (аналог) за технічною суттю та результатом, що досягається, є "Пристрій для множення в системі залишкових класів" (а.с. № 922731 СРСР, МКИ G 06 F 7/52, 1982, Бюл. № 15), який містить вхідні та вихідний регістри, дешифратори, групи елементів І та АБО, елементи І та АБО, комутатор, суматор за модулем два.

Недолік аналога низькі функціональні можливості пристрою. Неможливість виконання операції піднесення чисел до квадрата у СЗК.

Найбільш близьким (прототипом), за технічною суттю та результатом, що досягається, є корисна модель № 61798 Україна, МПК G 06 F 7/60 (2006.01). Пристрій для піднесення чисел до квадрата за модулем m класу лишків. № u201101245. Заявл. 04.02.2011. Опубл. 25.07.2011, Бюл. № 14. – 6 с. Пристрій містить перетворювач коду, дешифратор, шифратор, елементи АБО та регістри.

Недолік прототипу - низькі функціональні можливості пристрою. Неможливість виконання операції піднесення чисел до квадрата у СЗК.

Задача корисної моделі - підвищення функціональних можливостей пристрою за рахунок виконання операції піднесення чисел до квадрата у СЗК, за рахунок використання наступної властивості $A^2 \pmod m=(n-A)^2 \bmod m$.

Поставлена задача вирішується за рахунок того, що в пристрій, який містить перший вхідний і перший вихідний регістри, перший дешифратор, першу групу елементів АБО та перший шифратор введено (n-1) - н вхідних і вихідних регістрів (n - кількість основ СЗК), (n-1) - н дешифраторів, (n-1) - н груп елементів АБО та (n-1) - н шифраторів, при цьому і-й ($i=\overline{1,n}$) вхід пристрою підключено до входу і-го вхідного регістра, вихід якого підключено до входу і-го дешифратора, виходи якого попарно підключено до входів відповідних елементів АБО і-ї групи, виходи яких підключено до відповідних входів і-го шифратора, вихід якого підключено до входу і-го вихідного регістра, вихід якого є і-м виходом пристрою, а нульовий вихід і-го дешифратора безпосередньо підключено до нульового входу і-го шифратора.

Технічний результат, який може бути отриманий при використанні запропонованої корисної моделі, полягає в підвищення функціональних можливостей пристрою за рахунок виконання операції піднесення чисел до квадрата у СЗК.

На кресленні (фіг. 1) приведена блок-схема запропонованого пристрою, де: 1_1-1_n входи пристрою; 2_1-2_n - вхідні регістри; 3_1-3_n - дешифратори (пристрої для перетворення лишків a_i числа $A=(a_1, a_2,\ldots, a_n)$ у СЗК з двійкового коду в унітарний); 4_1-4_n групи двоходових елементів (вихідні шини дешифраторів 3_1-3_n попарно об'єднуються таким чином, щоб сума чисел, що надана кожній із пар виходів 3_1-3_n дорівнювала значенню модуля m_i СЗК) АБО; 5_i-5_n - шифратори (пристрої для перетворення унітарного коду числа в двійковий); 6_1-6_n - вихідні регістри; 7_1-7_n - виходи пристрою.

Входи 1_1-1_n пристрою підключено до входів відповідних вхідних регістрів 2_1-2_n, вихід яких підключено до входів відповідних дешифраторів 3_1-3_n. Виходи дешифраторів 3_1-3_n попарно підключено до входів відповідних елементів АБО груп 4_1-4_n, виходи яких підключено до відповідних входів шифраторів 5_1-5_n, виходи яких підключено до входів відповідних вихідних регістрів 6_1-6_n, виходи 7_1-7_n яких є виходом пристрою. Нульовий вихід дешифраторів 3_1-3_n підключено до нульового входу шифраторів 5_1-5_n.

Пристрій працює наступним чином. До входів 1_1-1_n пристрою надходить число $A=(a_1, a_2,\ldots, a_n)$ у СЗК, яке необхідно піднести до квадрата. Тобто, окремий лишок a_i числа $A=(a_1, a_2,\ldots, a_n)$ у двійковому коді надходить до відповідного регістра 2_1-2_n. Дешифратори 3_1-3_n перетворюють лишки a_i числа $A=(a_1, a_2,\ldots, a_n)$ в унітарний код, сигнали якого через відповідні елементи 4_1-4_n АБО групи надходять на відповідні входи шифраторів 5_1-5_n. Номери входів довільного і-го шифратора 5, для лишку a_i за модулем m_i СЗК відповідають значенням: 0, 1, $2^2(\mathrm{mod} m_i)$, $3^2(\mathrm{mod} m_i)$, $4^2(\mathrm{mod} m_i)$, … і т.д. З виходу шифраторів, 5_1-5_n результат операції A^2 в двійковому коді через вихідні регістри 6_1-6_n надходить на виходи 7_1-7_n пристрою.

Розглянемо приклад (фіг. 2) конкретного виконання пристроєм операції піднесення числа $A=(a_1, a_2, a_3)=(10, 011, 001)$ у СЗК до квадрата. Нехай СЗК задана наступними основами $m_1=3$,

m_2=5, m_3=7. У таблицях 1-3 дано схеми отримання квадратів a_i^2 лишків вихідного числа А=(10, 011, 001).

Таблиця 1

Схема реалізації операції $a_1^2(\mathrm{mod}\, m_1) = 2^2(\mathrm{mod}\, 3)$

Номер пари шин дешифратора 3_1	Значення, що призначаються парі вихідних шин дешифратора 3_1	Значення, що призначаються вихідним шинам шифратора 5_1	Значення, що призначаються вихідним шинам шифратора 5_1
0	0	0	00
1	1,2	1	01

Таблиця 2

Схема реалізації операції $a_2^2(\mathrm{mod}\, m_2) = 3^2(\mathrm{mod}\, 5)$

Номер пари шин дешифратора 3	Значення, що призначаються парі вихідних шин дешифратора 3	Значення, що призначаються вихідним шинам шифратора 5_2	Значення, що призначаються вихідним шинам шифратора 5_2
0	0	0	000
1	1,4	1	001
2	2,3	4	100

Таблиця 3

Схема реалізації операції $a_3^2(\mathrm{mod}\, m_3) = 1^2(\mathrm{mod}\, 7)$

Номер пари шин дешифратора 3	Значення, що призначаються парі вихідних шин дешифратора 3	Значення, що призначаються вихідним шинам шифратора 5	Значення, що призначаються вихідним шинам шифратора 5
0	0	0	000
1	1,6	1	011
2	2,5	4	100
3	3,4	2	010

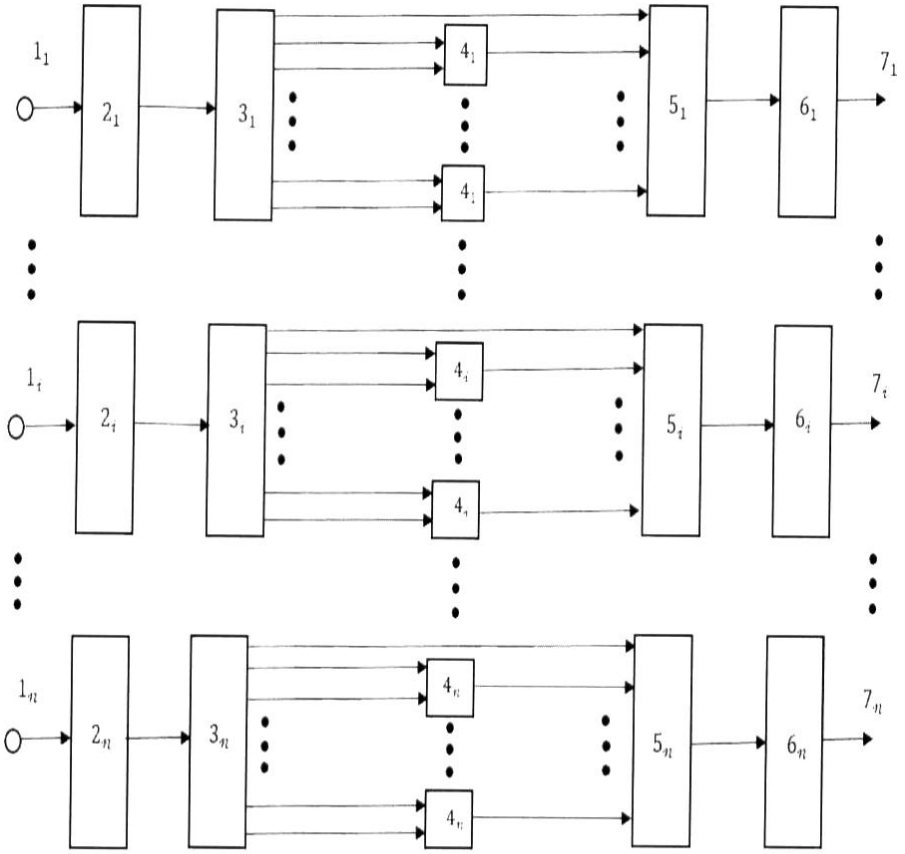
До входів 1_1-1_3 надходить число А=(10, 011, 001). До першого вхідного регістра 2_1 надходить значення першого лишку a_1=10 числа А=(10, 011, 001), до другого вхідного регістра 2_2 надходить значення другого лишку a_2=011, а до третього вхідного регістра 2, надходить значення третього лишку a_3=001. У відповідності зі схемами реалізації операції a_i^2 ($\mathrm{mod} m_i$) (табл. 1-3), у першому 6_1 вихідному регістрі маємо значення 01, у другому 6_2 вихідному регістрі маємо значення 100, а у третьому 6_3 вихідному регістрі маємо значення 001. Таким чином, на виході 7_1-7_3 пристрою маємо результат операції A^2=(01, 100, 001).

Перевірка. Значення А=(10, 011, 001) у двійковій позиційній системі числення (ПСЧ) дорівнює величині 8. З другого боку, 8^2=64. Значення 64 у СЗК з основами m_1=3, m_2=5, m_3=7 дорівнює A^2=(01, 100, 001). Тобто, результат операції піднесення числа А=(a_1, a_2, a_3)=(10, 011, 001) у СЗК до квадрата правильний.

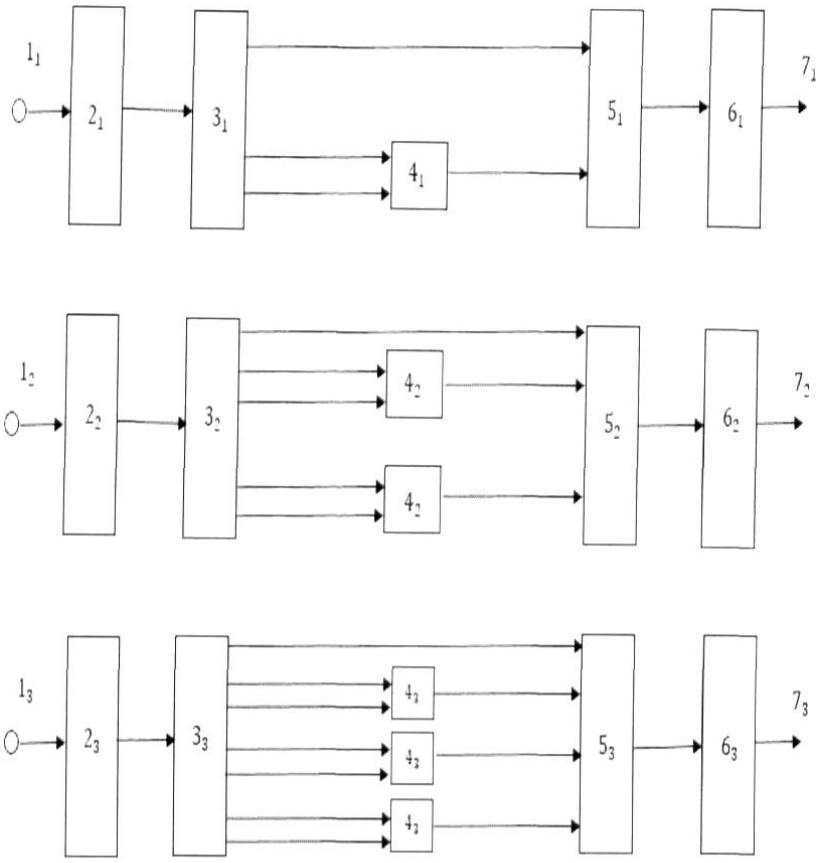
Таким чином, запропонована корисна модель дозволяє підвищити функціональні можливості пристрою за рахунок виконання операції піднесення чисел до квадрата у СЗК, на основі використання числової властивості $A^2(\mathrm{mod} m)=(m-A)^2\ \mathrm{mod} m$, при збереженні всіх технічних характеристик пристрою.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Пристрій для піднесення чисел до квадрата у системі залишкових класів (СЗК), що містить перший вхідний і перший вихідний регістри, перший дешифратор, першу групу елементів АБО, та перший шифратор, який **відрізняється** тим, що введено (n-1) - н вхідних і вихідних регістрів (n - кількість основ СЗК), (n-1) - н дешифраторів, (n-1) - н груп елементів АБО, та (n-1) - н шифраторів, при цьому і-й ($i=\overline{1,n}$) вхід пристрою підключено до входу і-го вхідного регістра, вихід якого підключено до входу і-го дешифратора, виходи якого попарно підключено до входів відповідних елементів АБО і-ї групи, виходи яких підключено до відповідних входів і-го шифратора, вихід якого підключено до входу і-го вихідного регістра, вихід якого є і-м виходом пристрою, а нульовий вихід і-го дешифратора безпосередньо підключено до нульового входу і-го шифратора.



Фіг. 1



Фіг. 2

Комп'ютерна верстка І. Мироненко

Міністерство економічного розвитку і торгівлі України, вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

ДП “Український інститут інтелектуальної власності”, вул. Глазунова, 1, м. Київ – 42, 01601