



УКРАЇНА

(19) UA

(11) 160091

(13) U

(51) МПК

G06F 7/04 (2006.01)

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

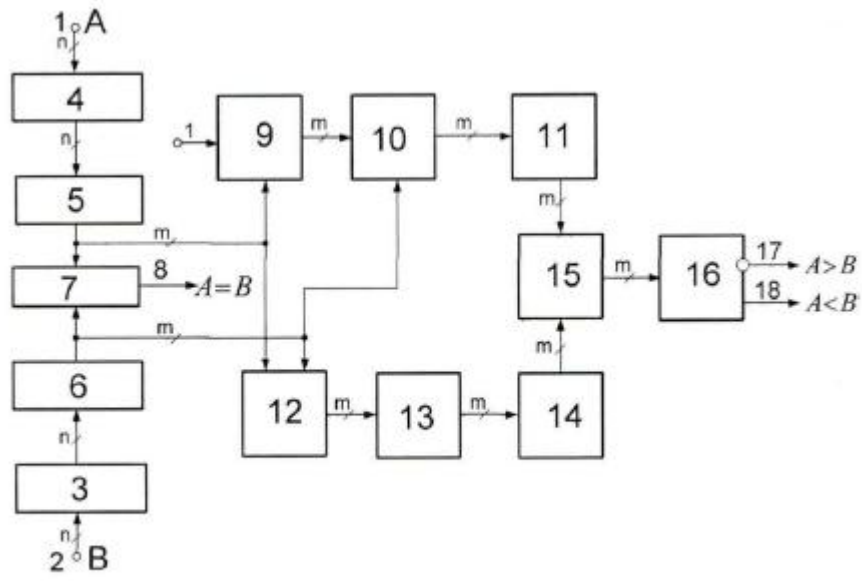
(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: u 2024 04328	(72) Винахідник(и): Николайчук Ярослав Миколайович (UA), Якименко Ігор Зіновійович (UA), Івасьєв Степан Володимирович (UA), Грига Володимир Михайлович (UA)
(22) Дата подання заявки: 03.09.2024	
(24) Дата, з якої є чинними права інтелектуальної власності: 07.08.2025	
(46) Публікація відомостей про державну реєстрацію: 06.08.2025, Бюл.№ 32	(73) Володілець (володільці): Николайчук Ярослав Миколайович, вул. В. Великого, 14а, м. Надвірна, Івано-Франківська обл., 78400 (UA), Якименко Ігор Зіновійович, вул. Волинська, 19а, с. Підгородне, Тернопільська обл., 47751 (UA), Івасьєв Степан Володимирович, вул. Чехова, 8, м. Надвірна, Тернопільська обл., 46003 (UA), Грига Володимир Михайлович, вул. Івана Богуна, 12, м. Надвірна, Івано-Франківська обл., 78400 (UA)

(54) ПРИСТРІЙ ПОРІВНЯННЯ ДАНИХ, ПРЕДСТАВЛЕНИХ У НЕПОЗИЦІЙНІЙ СИСТЕМІ ЧИСЛЕННЯ КЛАСУ ЛИШКІВ**(57) Реферат:**

Пристрій порівняння даних, представлених у непозиційній системі числення класу лишків, містить перший та другий інформаційні входи чисел (A і B) з'єднані з відповідними входами першого та другого регістрів, виходи яких з'єднані з входами відповідних суматорів, схему порівняння однопорядкового коду, логічні елементи І, АБО та НЕ, які з'єднані між собою відповідним чином, перший $A=B$, другий $A>B$ та третій $A<B$ вихідні канали, які є відповідними виходами пристрою. Додатково вихідні n-розрядні виходи першого регістра з'єднані з відповідними входами першого шифратора коду (R-C) у m-розрядний код (H-C), виходи якого з'єднані з першими входами першого та другого матрично-модульних суматорів (ММС), та першими входами схеми порівняння однопорядкових (H-C)-кодів, вихід якої є першим виходом пристрою $A=B$. Додатково (H-C)-код логічної 1 з'єднаний з другими входами першого ММС, виходи якого з'єднані з першими входами третього ММС, виходи якого з'єднані з відповідними входами першого квадратора, виходи якого з'єднані з першими входами багаторозрядного четвертого ММС. Додатково n-розрядні виходи другого регістра з'єднані з відповідними входами другого шифратора коду (R-C) у m-розрядний код (H-C) виходи якого з'єднані з другими входами схеми порівняння однопорядкових (H-C)-кодів та відповідними другими входами другого та третього ММС, виходи якого з'єднані з відповідними входами другого квадратора, виходи якого з'єднані з відповідними входами кодового інвертора, виходи якого з'єднані з відповідними другими входами четвертого ММС, виходи якого з'єднані з відповідними входами третього шифратора, інверсний вихід якого $A>B$ є другим виходом пристрою. Прямий вихід $A<B$ третім виходом пристрою.

UA 160091 U



Фиг. 1

Пристрій належить до галузі автоматики та обчислювальної техніки і може бути застосований в інформаційно-телекомунікаційних системах, що працюють у непозиційній системі числення класу лишків (КЛ), а також при реалізації криптографічних перетворень у полях Галуа.

Відомий пристрій для порівняння даних, що представлені у класі лишків [Патент України на корисну модель № 73379. Пристрій для порівняння даних, що представлені у класі лишків. Бюл. № 18, 2012], що містить перший та другий інформаційні входи (А, В), з'єднані з відповідними входами першого та другого регістрів, виходи яких з'єднані з входами відповідних суматорів, схему порівняння однопорядкового коду, логічні елементи І, АБО та НЕ, які з'єднані між собою відповідним чином, перший (А=В), другий (А>В) та третій (А<В) вихідні канали, які є відповідними виходами пристрою.

Недолік такого пристрою полягає в тому, що пристрій не в усіх випадках достовірно визначає результат порівняння двох чисел А і В у КЛ з максимальною точністю порівняння $W_{\max}=1$.

Відомий найближчий аналог - пристрій для порівняння даних, що представлені у непозиційній системі числення класу лишків [Патент України на корисну модель № 79587. Пристрій для порівняння даних, що представлені в непозиційній системі числення класу лишків. Бюл. № 8, 2013], що містить перші та другі інформаційні входи чисел (А, В) з'єднані з відповідними входами першого та другого регістрів, виходи яких з'єднані з входами відповідних суматорів, схему порівняння однопорядкового коду, логічні елементи І, АБО та НЕ, які з'єднані між собою відповідним чином, перший (А=В), другий (А>В) та третій (А<В) вихідні канали, які є відповідними виходами пристрою.

Недоліками такого пристрою є висока алгоритмічно-арифметична складність процесів порівняння чисел представлених у КЛ та низька швидкодія.

Іншим недоліком такого пристрою є надлишковість апаратного обладнання, що обумовлено паралельним визначенням ознак (А>В) та (А<В). Оскільки результати порівняння чисел (А>В) та (А<В) є взаємновиключними. Тобто, достатньо визначити тільки один результат порівняння чисел (А>В) у КЛ, інакше, однозначно (А<В).

Недоліком такого пристрою є представлення вхідних даних у кодах Радемахера-Крестенсона (R-C), що потребує застосовувати як суматори двійкові Рі-розрядні суматори з наскрізними переносами та заміни операцій віднімання операцією додавання доповнюючих двійкових кодів лишків $(a_i + b_i) \bmod P_i$, якщо $(a_i > b_i)$ [Патент України на корисну модель № 117789. Пристрій додавання багаторозрядних двійкових чисел. Бюл. № 13, 2017].

В основу корисної моделі поставлена задача спрощення алгоритму порівняння чисел А і В у КЛ шляхом додаткового представлення вхідних значень А і В у кодах Хаара-Крестенсона (H-C) та визначення наступних числових значень: $A \oplus B = 1(A = B)$; $(A - B)^2 = S_0$; $[(A+1)-B]^2 = S_x$; $D = (S_0 + S_x) \bmod P_0$, $P_0 = (P_1 \times P_2 \times \dots \times P_k)$, k - кількість модулів P_i . Якщо вихід шифратора $D=0$ то (А>В), інакше (А<В).

Поставлена задача вирішується тим, що у пристрої порівняння даних, представлених у непозиційній системі числення КЛ, містить перший та другий інформаційні входи чисел (А і В), з'єднані з відповідними входами першого та другого регістрів, виходи яких з'єднані з входами відповідних суматорів, схему порівняння однопорядкового коду, логічні елементи І, АБО та НЕ, які з'єднані між собою відповідним чином, перший А=В, другий А>В та третій А<В вихідні канали, які є відповідними виходами пристрою, згідно з корисною моделлю, додатково вихідні n-розрядні виходи першого регістра з'єднані з відповідними входами першого шифратора коду (R-C) у m-розрядний код (H-C), m-розрядні виходи якого з'єднані з першими входами першого та другого матрично-модульних суматорів (ММС) та першими входами схеми порівняння однопорядкових (H-C)-кодів, вихід якої є першим виходом пристрою А=В, додатково (H-C)-код логічної "1" з'єднаний з другими входами першого ММС, виходи якого з'єднані з першими входами третього ММС, виходи якого з'єднані з відповідними входами першого квадратора, виходи якого з'єднані з першими входами четвертого ММС, додатково n-розрядні виходи другого регістра з'єднані з відповідними входами другого шифратора коду (R-C) у m-розрядний код (H-C), виходи якого з'єднані з другими входами схеми порівняння однопорядкових (H-C)-кодів та відповідними другими входами другого та третього ММС, виходи якого з'єднані з відповідними входами другого квадратора, виходи якого з'єднані з відповідними входами кодового інвертора, виходи якого з'єднані з відповідними другими входами багаторозрядного четвертого ММС, виходи якого з'єднані з відповідними входами третього шифратора, інверсний вихід якого А>В є другим виходом пристрою, а прямий вихід А<В, відповідно, третім виходом пристрою.

Корисна модель ілюструється кресленням, де на фіг. 1 показана структура пристрою порівняння даних, представлених у непозиційній системі класу лишків, що містить: 1,2 - перші та другі інформаційні входи пристрою чисел A і B; 3,4 - перший та другий регістри пам'яті (II-C)-кодів чисел A і B; 5,6 - перший та другий шифратори n-розрядних (R-C)-кодів у m-розрядні (H-C)-коди (фіг. 2); 7- схему порівняння однопорядкових m-розрядних (H-C)-кодів (фіг. 3); 8 - перший вихід пристрою (A=B); 9,10,12-m-розрядні ММС (фіг. 4); 11,13 - модульні квадратори (фіг. 5); 14 - кодовий інвертор (фіг. 6); 15 - багаторозрядний ММС з вихідним шифратором 16 (фіг. 7); 17,18 - другий A>B та третій A<B виходи пристрою.

При застосуванні інших наборів модулів для процесорів більшої розрядності (8,16, 32,...) структурні схеми компонентів пристрою будуються аналогічно.

У таблиці 1 представлена реалізація алгоритму порівняння чисел у КЛ.

Таблица 1

Алгоритм порівняння чисел у кодах лишків

τ	Регістр A $A=(a_1, a_2, \dots, a_n)_{(R-C)}$		Регістр B $B=(b_1, b_2, \dots, b_n)_{(R-C)}$	τ
2	$A=(a_1, a_2, \dots, a_n)_{(R-C)}$		$B=(b_1, b_2, \dots, b_n)_{(R-C)}$	2
1	$A=(a_1, a_2, \dots, a_m)_{(H-C)}$		$B=(b_1, b_2, \dots, b_m)_{(H-C)}$	1
1	$(A+1) \bmod P_0$	$A \oplus B = 1$ 0 1	$(A-B) \bmod P_0$	1
2	$[(A+1)-B] \bmod P_0$		$S_0 = (A-B)^2 \bmod P_0$	2
1	$S_x = [(A+1)-B]^2 \bmod P_0$		$S_0 = (P_0 - S_0) \bmod P_0$	1
2		$D = (S_x + S_0) \bmod P_0$ $D = 1 \quad D = 0$		2
1		$A < B \quad A > B$		1
10			Сума τ (мікротактів)	10

Алгоритм порівняння чисел A і B представлений в (H-C)-кодах на прикладі застосування 5-розрядного двійкового процесора. Тобто діапазони зміни різниць чисел A і B відбуваються в границях (0÷31), що відповідає кодам (00000÷11111) у двійковій системі числення. Оскільки у алгоритмі порівняння чисел A і B у КЛ, згідно з табл.1 є операція піднесення до квадрату $[(A+1)-B]^2$, для однозначного виконання цієї операції у (H-C)-кодах, вибраний добуток взаємно-простих модулів ($P_0 = P_1 \times P_2 \times \dots \times P_m$) повинен перевищувати число $32=1024$.

Виконаємо алгоритм порівняння чисел A і B у системі взаємно-простих модулів ($P_1=2, P_2=5, P_3=9, P_4=13$), добуток яких ($P_0=2 \times 5 \times 9 \times 13=1170 > 1024$).

Наведемо приклад реалізації алгоритму порівняння чисел A і B, представлених у десятковій системі числення.

Нехай $A=27_{10}$; $B=24_{10}$ результатом їх порівняння згідно з алгоритмом, представленим в таблиці 1.

- $S_x = [(27+1)-24]^2 = 16 (A > B)$;
- $S_x = [(24+1)-27]^2 = 4 (A < B)$;
- $S_0 = (27-24)^2 = 9 (A > B)$;
- $S_0 = (24-27)^2 = 9 (A < B)$;
- $(A-B)^2 = P_0 - (A-B)^2 = 1170 - 9 = 1161$;
- $(S_0 + S_x) \bmod P_0 = (1161 + 16) \bmod 1170 = 7 (A > B)$;
- $(S_0 + S_x) \bmod P_0 = (1161 + 4) \bmod 1170 = 1165 (A < B)$.

При зростанні різниць між числами A і B у діапазоні від (1÷31), якщо $A > B$ на виході 3-го шифратора формуються логічні сигнали '0' то ($A > B$), інакше ($A < B$).

У таблиці 2 приведені вихідні дані у 10-й системі числення алгоритму порівняння чисел у кодах лишків для 5-розрядного процесора.

Таблиця 2

Вихідні дані у 10-ій системі числення алгоритму порівняння чисел у кодах лишків

A-B	$(A < B)S_x \leftarrow S_0 \rightarrow +S_x(A > B)$	A>B
1	0-1-4	3
2	1-4-9	5
3	4-9-16	7
	...	
31	900-961-1024	63

Всі обчислювальні операції у пристрої виконуються у (Н-С)-кодах базису Хаара-Крестенсона. У багаторозрядному четвертому ММС (фіг.5) реалізується операція матрично-модульного додавання відповідним з'єднанням виходів логічних елементів І-НЕ та додатковим введенням інверторів, які формують прямі вихідні коди результатів із затримкою сигналів 2 мікротакти.

Згідно табл. 1 загальна затримка сигналів у пристрої порівняння $\tau=10$ (мікротактів).

Апаратна складність 5-розрядного процесора розраховується згідно з виразом:

$$A=A_1+A_2+A_3+A_4+A_5+A_6,$$

де A_1 - апаратна складність першого та другого n-розрядних регістрів,

$A_1=4 \times (1+3+4+4)=48V$ (вентилів); A_2 - апаратна складність першого та другого шифратора, $A_2=2 \times 29=58V$; A_3 - схема порівняння однопорядкових (Н-С)-кодів, $A_3=3 \times 29=87V$; A_4 - апаратна складність 1, 2, 3, 4 m-розрядних ММС, $A_4=4 \times (2^2+5^2+9^2+13^2)=1116V$; A_5 - апаратна складність першого та другого квадраторів, $A_5=2 \times (2+5+9+13)=58V$; A_6 - апаратна складність третього шифратора, $A_6=31V$.

Сумарна апаратна складність удосконаленого пристрою складає: $A=48+58+87+1116+58+31=1398V$ (вентилів).

Для запису вхідних даних (А і В) у кодах (R-C) в регістри пам'яті застосовується сигнал синхронізації S_x , який в описі корисної моделі не вказаний.

Сумарна затримка сигналів у відомому пристрої визначається згідно з виразом:

$$\tau=\tau_1+\tau_2+\tau_3+\tau_4+\tau_5,$$

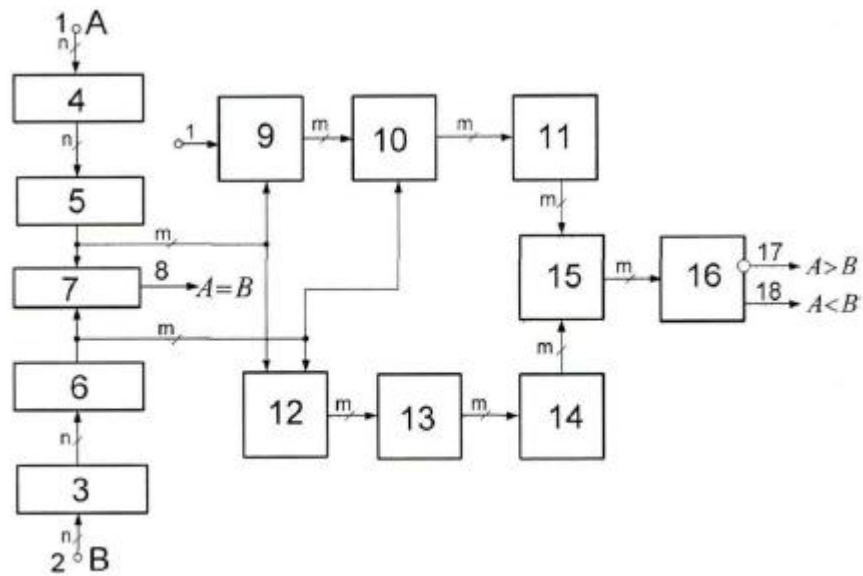
де τ_1 - затримка сигналів у регістрах пам'яті, $\tau_1=2\tau$ (мікротакти); τ_2 - затримка сигналів у 3-розрядному двійковому суматорі, $\tau_2=6\tau$, τ_3 - затримка сигналів у схемі порівняння однопорядкового коду, $\tau_3=4\tau$; τ_4 - затримка сигналів у мультиплексорі, $\tau_4=3\tau$, τ_5 - затримка сигналів у 5-и послідовно з'єднаних логічних елементах, $\tau_5=5\tau$.

Сумарна затримка сигналів у відомому пристрої складає: $\tau=2+6+4+3+5=20\tau$. Таким чином, підвищення швидкодії запропонованого пристрою, відповідно, складає $k=20/10=2$ рази.

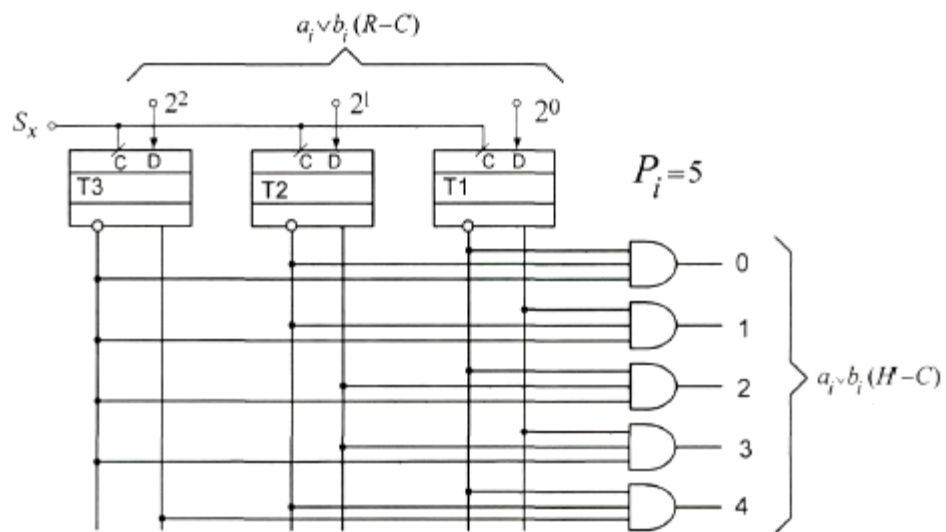
ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Пристрій порівняння даних, представлених у непоозиційній системі числення класу лишків, який містить перший та другий інформаційні входи чисел (А і В), з'єднані з відповідними входами першого та другого регістрів, виходи яких з'єднані з входами відповідних суматорів, схему порівняння однопорядкового коду, логічні елементи І, АБО та ІІ, які з'єднані між собою відповідним чином, перший $A=B$, другий $A>B$ та третій $A<B$ вихідні канали, які є відповідними виходами пристрою, який **відрізняється** тим, що додатково вихідні n-розрядні виходи першого регістра з'єднані з відповідними входами першого шифратора коду (R-C) у m-розрядний код (Н-С), виходи якого з'єднані з першими входами першого та другого матрично-модульних суматорів (ММС) та першими входами схеми порівняння однопорядкових (Н-С)-кодів, вихід якої є першим виходом пристрою $A=B$, додатково (Н-С)-код логічної 1 з'єднаний з другими входами першого ММС, виходи якого з'єднані з першими входами третього ММС, виходи якого з'єднані з відповідними входами першого квадратора, виходи якого з'єднані з першими входами багаторозрядного четвертого ММС, додатково n-розрядні виходи другого регістра з'єднані з відповідними входами другого шифратора коду (R-C) у m-розрядний код (Н-С), виходи якого з'єднані з другими входами схеми порівняння однопорядкових (Н-С)-кодів, та відповідними другими входами другого та третього ММС, виходи якого з'єднані з відповідними входами другого квадратора, виходи якого з'єднані з відповідними входами кодового інвертора, виходи якого з'єднані з відповідними другими входами четвертого ММС, виходи якого з'єднані з

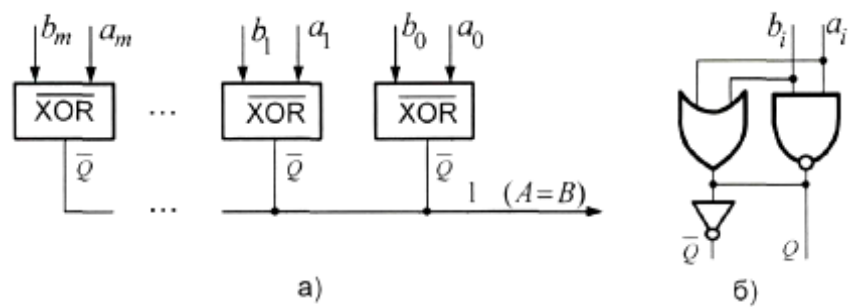
відповідними входами третього шифратора, інверсний вихід якого $A > B$ є другим виходом пристрою, а прямий вихід $A < B$ третім виходом пристрою.



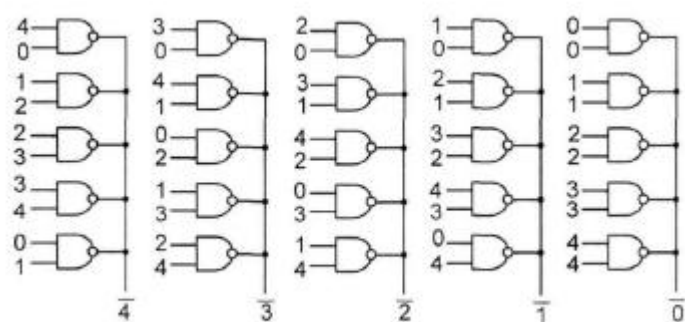
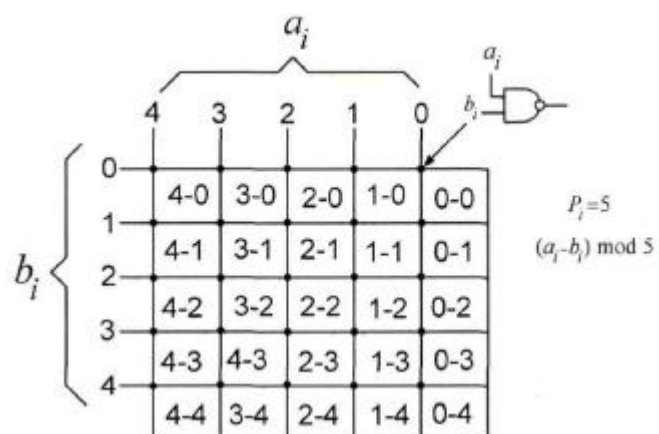
Фиг. 1



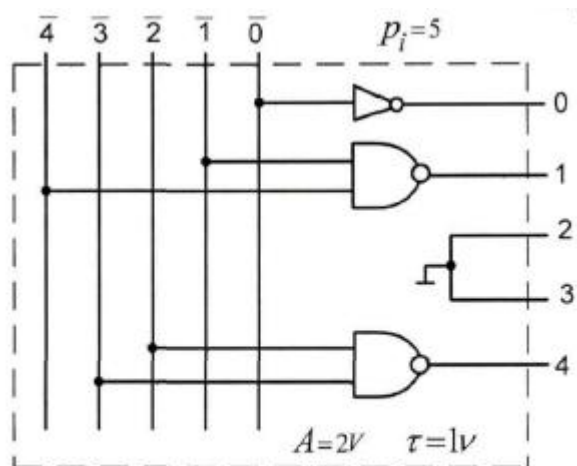
Фиг. 2



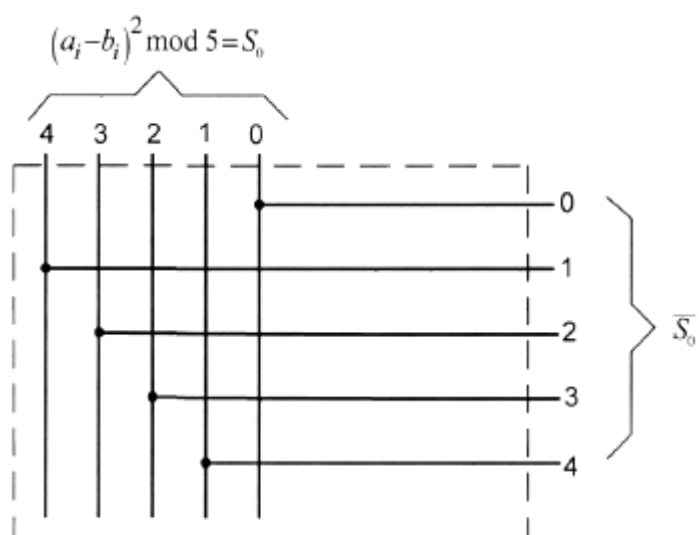
Фиг. 3



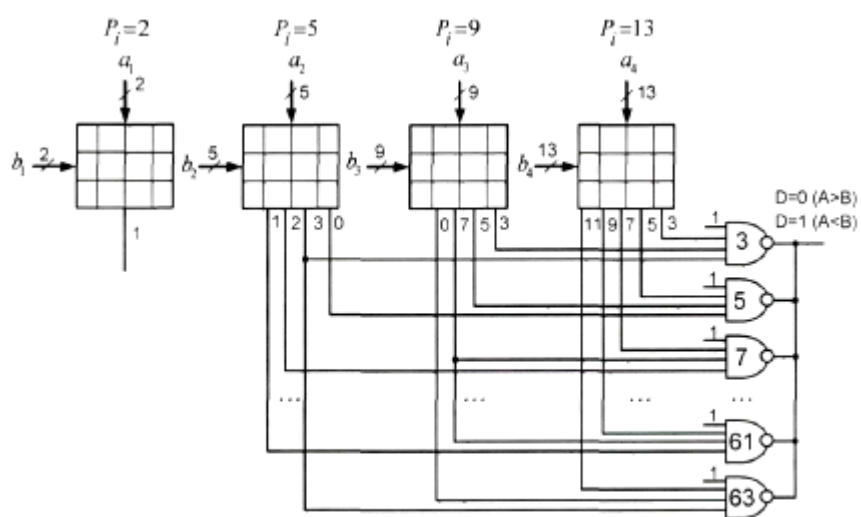
Фиг. 4



Фиг. 5



Фиг. 6



Фиг. 7