



УКРАЇНА

(19) UA (11) 66645 (13) U
(51) МПК
G06F 7/74 (2006.01)

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під
відповідальність
власника
патенту

(54) ПРИСТРІЙ ДЛЯ ПІДНЕСЕННЯ ЧИСЕЛ ДО КВАДРАТА ЗА МОДУЛЯМИ m_i КЛАСУ ЛИШКІВ

1

2

(21) u201107927

(22) 23.06.2011

(24) 10.01.2012

(46) 10.01.2012, Бюл. № 1, 2012 р.

(72) БАРСОВ ВАЛЕРІЙ ІГОРОВИЧ, ДУГІН МИХАЙЛО ВІТАЛІЙОВИЧ, СОРОКА ЛЕОНІД СТЕПАНОВИЧ, КРАСНОБАЄВ ВІКТОР АНАТОЛІЙОВИЧ, ЗАГУМЕНА КАТЕРИНА ВІКТОРІВНА

(73) УКРАЇНСЬКА ІНЖЕНЕРНО-ПЕДАГОГІЧНА АКАДЕМІЯ

(57) Пристрій для піднесення чисел до квадрата за модулями m_i класу лишків (КЛ), що містить вхідний і вихідний реєстри, перший дешифратор, першу групу із $(m_1-1)/2$ елементів АБО (m_1 - перший модуль КЛ, за яким працює пристрій), перший шифратор, при цьому вхід пристрою підключено до входу вхідного реєстра, а вихід вихідного реєстра є виходом пристрою, виходи першого дешифратора попарно (сума чисел, що надано кожній із пар виходів дорівнює значенню першого m_1 модуля КЛ) підключено до входів відповідних елементів АБО першої групи, виходи яких підключено до відповідних входів першого шифратора, а нульовий вихід першого дешифратора безпосередньо підключено до нульового входу першого шифратора, який **відрізняється** тим, що введено другий та третій дешифратори, другу групу із $m_2/2$ елементів АБО (m_2 - другий модуль КЛ, за яким працює при-

стрій), третю групу із $(m_3-2)/2$ елементів АБО (m_3 - третій модуль КЛ, за яким працює пристрій) та четверту групу елементів АБО, другий та третій шифратори, три групи елементів І, при цьому вихід вхідного реєстра підключено до перших входів елементів І першої, другої та третьої груп, до других входів яких підключено шини подачі сигналів ознак відповідно першого m_1 , другого m_2 та третього m_3 модулів КЛ, а виходи елементів І першої, другої та третьої груп підключено до входів відповідно першого, другого та третього дешифраторів, виходи другого дешифратора попарно (сума чисел, що надано парі виходів, дорівнює значенню другого m_2 модуля КЛ, крім однієї пари виходів, значення шин якої є нульова та $m_2/2$ -я) підключено до входів відповідних елементів АБО другої групи, виходи яких підключено до відповідних входів другого шифратора, виходи третього дешифратора попарно (сума чисел, що надано кожній із пар, дорівнює значенню третього m_3 модуля КЛ) підключено до входів відповідних елементів АБО третьої групи, виходи яких підключено до відповідних входів третього шифратора, а нульовий та $m_3/2$ -й виходи третього дешифратора підключено безпосередньо до відповідних входів третього шифратора, виходи першого, другого та третього шифраторів через елементи АБО четвертої групи підключені до входу вихідного реєстра.

Корисна модель належить до автоматики й обчислювальної техніки та може бути використана в системах та засобах обробки цифрової інформації, що функціонують у непозиційній системі числення класу лишків (КЛ).

Відомий пристрій (аналог), що містить вхідний та вихідний реєстри, 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).

Недоліки аналога - низькі функціональні можливості. Це обумовлено тим, що операція піднесення чисел до квадрата за модулем m КЛ реалізується тільки для m непарного числа.

Близьким за технічною суттю та результатом (аналог), що досягається, є «Пристрій для мно-

ження в системі залишкових класів» [а. с. № 922731 СРСР, МПК G06F7/52, 1982, Бюл. № 15], який містить вхідні та вихідні реєстри, дешифратори, групи елементів І та АБО, елементи І та АБО, комутатор, суматор за модулем два.

Недолік аналога - низькі функціональні можливості. Це обумовлено тим, що операція піднесення чисел до квадрата за модулем m_i КЛ реалізується тільки для m_i непарного числа.

Найбільш близьким за технічною суттю та результатом (прототип), що досягається, є «Пристрій для піднесення чисел до квадрата за модулем m модулярної системи числення» (Патент на корисну модель № 51512, Україна, МПК G06F7/74, 2010, Бюл. № 14).

UA (19) 66645 (13) U

Вхід пристрою підключено до входу вхідного регістра, вихід якого підключено до входу дешифраторів. Виходи дешифратора попарно, так, що сума чисел, що надана кожній із пар виходів, дорівнює значенню першого m_1 модуля КЛ, підключено до входів відповідних елементів АБО групи. Вихід вихідного регістра є виходом пристрою. Виходи елементів АБО групи підключено до відповідних входів шифратора, вихід якого підключено до входу вихідного регістра. Нульовий вихід шифратора підключено до нульового входу шифратора.

Недолік прототипу - низькі функціональні можливості. Це обумовлено тим, що операція піднесення чисел до квадрата за модулем m_i КЛ реалізується тільки для m_i непарного числа.

Задача корисної моделі - розширення функціональних можливостей пристрою за рахунок виконання операції піднесення чисел до квадрата за усіма можливими модулями m_i КЛ: для m непарного та m парного чисел.

Технічний результат, який може бути отриманий при використанні корисної моделі, полягає в одержанні технічного засобу для піднесення чисел до квадрата за довільними модулями m_i КЛ.

Поставлена задача вирішується тим, що в пристрій, який містить вхідний і вихідний регістри, перший дешифратор, першу групу із $(m_1-1)/2$ елементів АБО (m_1 - перший модуль КЛ, за яким працює пристрій), перший шифратор, введено другий та третій дешифратори, другу групу із $m_2/2$ елементів АБО (m_2 - другий модуль КЛ, за яким працює пристрій), третю групу із $(m_3-2)/2$ елементів АБО (m_3 - третій модуль КЛ, за яким працює пристрій) та четверту групу елементів АБО, другий та третій шифратори, три групи елементів І. При цьому вхід пристрою підключено до входу вхідного регістра, а вихід вихідного регістра є виходом пристрою, виходи першого дешифратора попарно (сума чисел, що надано кожній із пар виходів, дорівнює значенню першого m_1 модуля КЛ) підключено до входів відповідних елементів АБО першої групи, виходи яких підключено до відповідних входів першого шифратора, а нульовий вихід першого дешифратора безпосередньо підключено до нульового входу першого шифратора. Вихід вхідного регістра підключено до перших входів елементів І першої, другої та третьої груп, до других входів яких підключено шини подачі сигналів ознак відповідно першого m_1 , другого m_2 та третього m_3 модулів КЛ, а виходи елементів І першої, другої та третьої груп підключено до входів відповідно першого, другого та третього дешифраторів. Виходи другого дешифратора попарно (сума чисел, що надано парі виходів, дорівнює значенню другого m_2 модуля КЛ, крім однієї пари виходів, значення шин якої є нульова та $m_2/2$ -я) підключено до входів відповідних елементів АБО другої групи, виходи яких підключено до відповідних входів другого шифратора. Виходи третього дешифратора попарно (сума чисел, що надано кожній із пар, дорівнює значенню третього m_3 модуля КЛ) підключено до входів відповідних елементів АБО третьої групи, виходи яких підключено до відповідних входів третього шифратора, а нульовий та $m_3/2$ -й виходи третього дешифратора підключено безпосередньо до від-

повідних входів третього шифратора. Виходи першого, другого та третього шифраторів через елементи АБО четвертої групи підключені до входу вихідного регістра.

При реалізації операції піднесення чисел до квадрата за парним m_i модулем КЛ слід окремо розглянути два можливих варіанти: для $m_i/2$ парного та $m_i/2$ непарного чисел.

Перший варіант. Для $m_2=2n$ парного та $m_2/2$ також парного чисел. В цьому випадку $\frac{m_2}{2}$ - ціле

число і тому маємо $\left(\frac{m_2}{2}\right)^2 = \frac{m_2}{4} \cdot m_2 \equiv 0 \pmod{m_2}$.

Для першого варіанта вихідна шина другого де-

шифратора, що відповідає значенню $\frac{m_2}{2}$, одноразово з нульовою шиною, через нульовий елемент АБО підключені до нульового входу другого шифратора. Таким чином, алгоритм функціонування пристрою (корисної моделі), у відповідності до першого варіанта, визначається наступним математичним співвідношенням:

$$\left(\frac{m_2}{2}\right)^2 \equiv 0 \pmod{m_2}. \quad (1)$$

Вираз (1) покладено в основу алгоритму для визначення значення $A^2 \pmod{m_2}$. В таблиці 5 представлено приклад алгоритму визначення $A^2 \pmod{m_2}$ для модуля $m_2=12$ ($m_2/2=6$).

Другий варіант для $m_3=2n$ парного та $m_3/2$ непарного чисел. Для цього варіанта виконується умова:

$$\left(\frac{m_3}{2}\right)^2 \equiv \frac{m_3}{2} \pmod{m_3}. \quad (2)$$

Дійсно, вираз (2) легко представити у вигляді:

$$\frac{m_3}{2} \cdot \left(\frac{m_3}{2} - 1\right) \equiv 0 \pmod{\frac{m_3}{2} \cdot 2}. \quad (3)$$

З теорії чисел відомо, що порівняння $A \equiv B \pmod{m_i}$ двох чисел A і B за модулем m_i рівнозначно подільності числа $A-B$ на модуль m_i . З виразу

(3) випливає, що число $m_3 = \frac{m_3}{2} \cdot 2$ є дільник виразу $\frac{m_3}{2} \cdot \left(\frac{m_3}{2} - 1\right)$.

Дійсно, перший співмножник $\frac{m_3}{2}$ добутку (3)

ділиться на $\frac{m_3}{2}$, а другий $\frac{m_3}{2} - 1$ співмножник - ділиться на два, так як за умовою (другий варіант) значення $\frac{m_3}{2}$ - непарне число. Таким чином, рівняння (3) справедливе.

Вираз (2) покладено в основу алгоритму для визначення значення $A^2 \pmod{m_3}$. В таблиці 6 представлено приклад алгоритму визначення значення $A^2 \pmod{m_3}$ для модуля $m_3=14$ ($m_3/2=7$).

На кресленні (фіг. 1) наведена блок-схема запропонованого пристрою, де: 1 - вхід пристрою; 2 - вхідний регістр; 3, 4 і 5 - перша, друга і третя групи елементів І; 6, 7 і 8 - шини подачі сигналів ознак відповідно першого m_1 , другого m_2 і третього m_3 модулів КЛ; 9, 10 і 11 - перший, другий і третій дешифратори (пристрій для перетворення числа з двійкового коду в унітарний); 12 - перша група двох входних елементів АБО; 13 - перший шифратор (пристрій для перетворення унітарного коду числа в двійковий); 14 - друга група двох входних елементів АБО; 15 - другий шифратор; 16 - третя група двох входних елементів АБО; 17 - третій шифратор; 18 - четверта група елементів АБО; 19 - вихідний регістр; 20 - вихід пристрою.

Вхід 1 пристрою підключено до входу вхідного регістра 2, вихід якого підключено до перших входів елементів І першої 3, другої 4 та третьої 5 груп, до других входів яких підключено шини 6, 7 і 8 подачі сигналів ознак відповідно першого m_1 , другого m_2 та третього m_3 модулів КЛ. Виходи елементів І першої 3, другої 4 та третьої 5 груп підключено до входів відповідно першого 9, другого 10 та третього 11 дешифраторів. Виходи першого 9 дешифратора попарно (сума чисел, що надано кожній із пари виходів, дорівнює значенню першого m_1 модуля КЛ) підключено до входів відповідних елементів АБО першої 12 групи, виходи яких підключено до відповідних входів першого 13 шифратора, а нульовий вихід першого 9 дешифратора безпосередньо підключено до нульового входу першого 13 шифратора. Виходи другого 10 дешифратора попарно (сума чисел, що надано кожній із пари виходів, дорівнює значенню другого m_2 модуля КЛ, крім однієї пари виходів, значення шин якої є нульова та $m_2/2$ -я) підключено до входів відповідних еле-

ментів АБО другої 14 групи, виходи яких підключено до відповідних входів другого 15 шифратора. Виходи третього 11 дешифратора попарно (сума чисел, що надано кожній із пари виходів, дорівнює значенню першого m_1 модуля КЛ) підключено до входів відповідних елементів АБО третьої 16 групи, виходи яких підключено до відповідних входів третього 17 шифратора, а нульовий та $m_2/2$ -й виходи третього 11 дешифратора підключено безпосередньо до нульового входу третього 17 шифратора. Виходи першого 13, другого 15 і третього 17 шифраторів через елементи АБО четвертої 18 групи підключені до входу вихідного регістра 19, вихід 20 якого є виходом пристрою.

Розглянемо процес функціонування корисної моделі у трьох можливих режимах роботи.

Перший режим. При m_1 непарне число (прототип). Дивись креслення (фіг. 1, 2) і табл. 1. Присутній сигнал шини 6.

Пристрій працює наступним чином. За входом 1 через регістр 2, відкриті елементи І першої 3 групи число A ($0 \leq A \leq m_1 - 1$) у двійковому коді надходить на вхід першого дешифратора 9 (фіг. 2). Дешифратор 9 перетворює число A в унітарний код, сигнал якого через відповідний елемент АБО першої 12 групи надходить на відповідний вхід першого 13 шифратора (табл. 1). Номери входів шифратора 13 відповідають значенням: 0, 1, 2²

$$(\text{mod } m), 3^2(\text{mod } m), 4^2(\text{mod } m), \dots, \left(\left[\frac{m}{2}\right]\right)^2 (\text{mod } m).$$

З виходу шифратора 13 результат операції $A^2 (\text{mod } m_1)$ в двійковому коді через четверту 18 групу елементів АБО, регістр 19 надходить на вихід 20 пристрою.

Таблиця 1

| | | | | | | | |
|------------------------------|-------------------------|---|---|-----|---|-----|-------------|
| Входи шифратора 13 (m_1) | 0 | 1 | 2 | ... | i | ... | $(m_1-1)/2$ |
| Виходи шифратора 13 | $A^2 (\text{mod } m_1)$ | | | | | | |

Таблиця 2

| | | | | | | | |
|------------------------------|-------------------------|---|---|-----|---|-----|-------------|
| Входи шифратора 15 (m_2) | 0 | 1 | 2 | ... | i | ... | $(m_2-2)/2$ |
| Виходи шифратора 15 | $A^2 (\text{mod } m_2)$ | | | | | | |

Таблиця 3

| | | | | | | | |
|------------------------------|-------------------------|---|---|-----|---|-----|-----------|
| Входи шифратора 17 (m_3) | 0 | 1 | 2 | ... | i | ... | $(m_3)/2$ |
| Виходи шифратора 17 | $A^2 (\text{mod } m_3)$ | | | | | | |

Другий режим. При m_2 парне число (варіант 1). Дивись креслення (фіг. 1, 2) і табл. 2. Присутній сигнал шини 7.

Пристрій працює наступним чином. За входом 1 через регістр 2, відкриті елементи І другої 4 групи число A ($0 \leq A \leq m_2 - 1$) у двійковому коді надходить на вхід другого дешифратора 10 (фіг. 2). Дешифратор 10 перетворює число A в унітарний код, сигнал якого через відповідний елемент АБО другої 14 групи надходить на відповідний вхід другого 15 шифратора (табл. 2). Номери входів шифратора 15 відповідають значенням $A^2 (\text{mod } m_2)$. З виходу шифратора 15 результат операції $A^2 (\text{mod } m_2)$ в

двійковому коді через четверту 18 групу елементів АБО, регістр 19 надходить на вихід 20 пристрою.

Третій режим. При m_3 парне число (варіант 3). Дивись креслення (фіг. 1, 2) і табл. 3. Присутній сигнал шини 8.

Пристрій працює наступним чином. За входом 1 через регістр 2, відкриті елементи І третьої 5 групи число A ($0 \leq A \leq m_3 - 1$) у двійковому коді надходить на вхід третього дешифратора 11 (фіг. 2). Дешифратор 11 перетворює число A в унітарний код, сигнал якого через відповідний елемент АБО третьої 16 групи надходить на відповідний вхід третього 17 шифратора (табл. 3). Номери входів

шифратора 13 відповідають значенням $A^2 \pmod{m_3}$. З виходу шифратора 17 результат операції $A^2 \pmod{m_3}$ в двійковому коді через четверту 18 групу елементів АБО, регістр 19 надходить на вихід 20 пристрою.

Розглянемо приклади конкретного виконання пристроєм операції $A^2 \pmod{m_1}$.

Перший режим. При $m_1=11$ - непарне число, $A=8$ (1000) дивись креслення (фіг. 3, 4) і табл. 4. Присутній сигнал шини 6.

Таблиця 4

Реалізація операції $A^2 \pmod{11}$ (прототип, m_1)

| Номер пари вихідних шин дешифратора 9 | Значення, що призначають парі вихідних шин дешифратора 9 | Значення, що призначаються вхідним шинам шифратора 13 | Значення, що призначаються вихідним шинам шифратора 13 |
|---------------------------------------|--|---|--|
| 0 | 0 | 0 | 0000 |
| 1 | 1,10 | 1 | 0001 |
| 2 | 2,9 | 4 | 0100 |
| 3 | 3,8 | 9 | 1001 |
| 4 | 4,7 | 5 | 0101 |
| 5 | 5,6 | 3 | 0011 |

Пристрій працює наступним чином. За входом 1 через регістр 2, відкриті елементи I першої 3 групи число $A=1000$ у двійковому коді надходить на восьмий вхід першого дешифратора 9. Дешифратор 9 перетворює число A в унітарний код $A=8$, сигнал якого через третій (табл. 4) елемент АБО першої 12 групи надходить на дев'ятий вхід першого 13 шифратора (табл. 4). З виходу шифратора

13 результат операції $A \pmod{m_1}=1001$ у двійковому коді через четверту 18 групу елементів АБО, регістр 19 надходить на вихід 20 пристрою.

Перевірка: $A \pmod{m_1}=8 \pmod{11}=9$.

Другий режим. При $m_2 = 12$ - парне число (варіант 1), $A = 8$ (1000). Дивись креслення (фіг. 3, 4) і табл. 5. Присутній сигнал шини 7.

Таблиця 5

Реалізація операції $A^2 \pmod{12}$ (варіант 1, m_2)

| Номер пари вихідних шин дешифратора 10 | Значення, що призначають парі вихідних шин дешифратора 10 | Значення $A^2 \pmod{12}$, що призначаються вхідним шинам шифратора 15 | Значення, що призначаються вихідним шинам шифратора 15 |
|--|---|--|--|
| 0 | 0,6 | 0 | 0000 |
| 1 | 1,11 | 1 | 0001 |
| 2 | 2,10 | 4 | 0100 |
| 3 | 3,9 | 9 | 1001 |
| 4 | 4,8 | 4 | 0100 |
| 5 | 5,7 | 1 | 0001 |

Пристрій працює наступним чином. За входом 1 через регістр 2, відкриті елементи I другої 4 групи число $A=1000$ у двійковому коді надходить на восьмий вхід другого дешифратора 10. Дешифратор 10 перетворює число A в унітарний код $A=8$, сигнал якого через четвертий елемент АБО другої 14 групи надходить на четвертий вхід другого 15 шифратора (табл. 5). З виходу шифратора 15 ре-

зультат операції $A^2 \pmod{m_2}=0100$ в двійковому коді через четверту 18 групу елементів АБО, регістр 19 надходить на вихід 20 пристрою.

Перевірка: $A \pmod{m_2}=8 \pmod{12}=4$.

Третій режим. При $m_3=14$ парне число (варіант 2), $A=8$ (1000) Дивись креслення (фіг. 3, 4) і табл. 6. Присутній сигнал шини 8.

Таблиця 6

Реалізація операції $A^2 \pmod{14}$ (варіант 2, m_3)

| Номер пари вихідних шин дешифратора 11 | Значення, що призначають парі вихідних шин дешифратора 11 | Значення $A^2 \pmod{14}$, що призначаються вхідним шинам шифратора 17 | Значення, що призначаються вихідним шинам шифратора 17 |
|--|---|--|--|
| 0 | 0,6 | 0 | 0000 |
| 1 | 1,13 | 1 | 0001 |
| 2 | 2,12 | 4 | 0100 |
| 3 | 3,11 | 9 | 1001 |
| 4 | 4,10 | 2 | 0010 |
| 5 | 5,9 | 11 | 1011 |
| 6 | 6,8 | 8 | 1000 |
| 7 | 7 | 7 | 0111 |

Пристрій працює наступним чином. За входом 1 через регістр 2, відкриті елементи І третьої 5 групи число $A=1000$ у двійковому коді надходить на вхід третього дешифратора 11. Дешифратор 11 перетворює число A в унітарний код $A=8$, сигнал якого через шостий елемент АБО третьої 16 групи надходить на восьмий вхід третього 17 шифратора (табл. 6). З виходу шифратора 17 результат операції $A^2 \pmod{m_3}=1000$ у двійковому коді через четверту 18 групу елементів АБО, регістр 19 надходить на вихід 20 пристрою.

Перевірка: $A^2 \pmod{m_3}=A^2 \pmod{14}=8$.

Таким чином, запропонована корисна модель дозволяє розширити (у порівнянні з прототипом) функціональні можливості корисної моделі за ра-

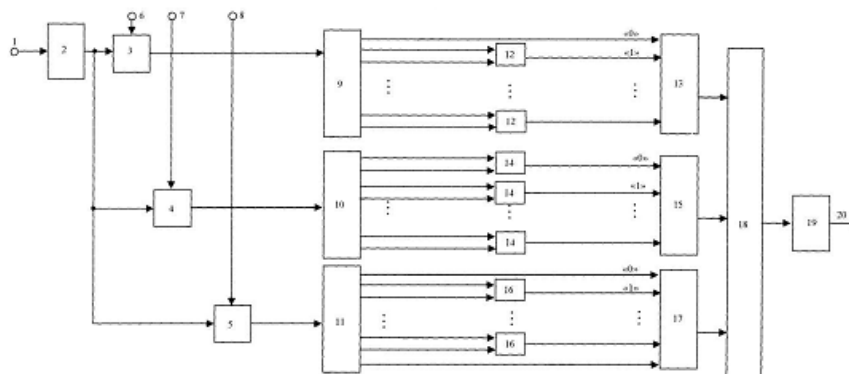
хунок виконання операції $A^2 \pmod{m_i}$ піднесення чисел до квадрата за всіма можливими модулями m_i КЛ. Це, у свою чергу, дає можливість підвищити коефіцієнт використання обладнання пристрою для піднесення чисел до квадрата за модулями m_i класу лишків.

Джерела інформації

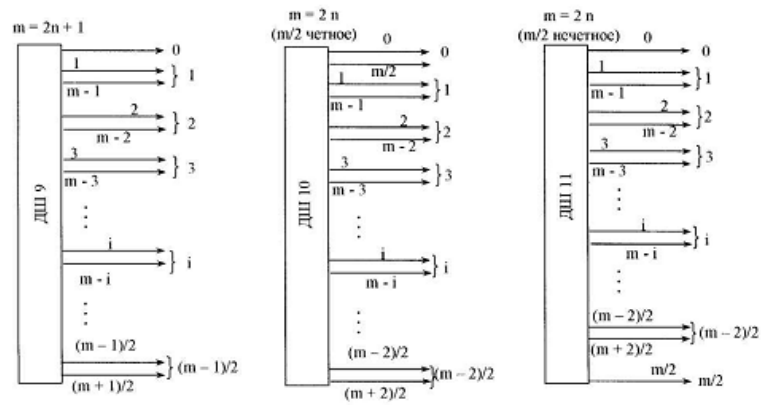
1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М.:Советское радио, 1968. - с. 327-340.

2. А.с. № 922731 СРСР, МПК G06F7/52, 1982, Бюл. № 15.

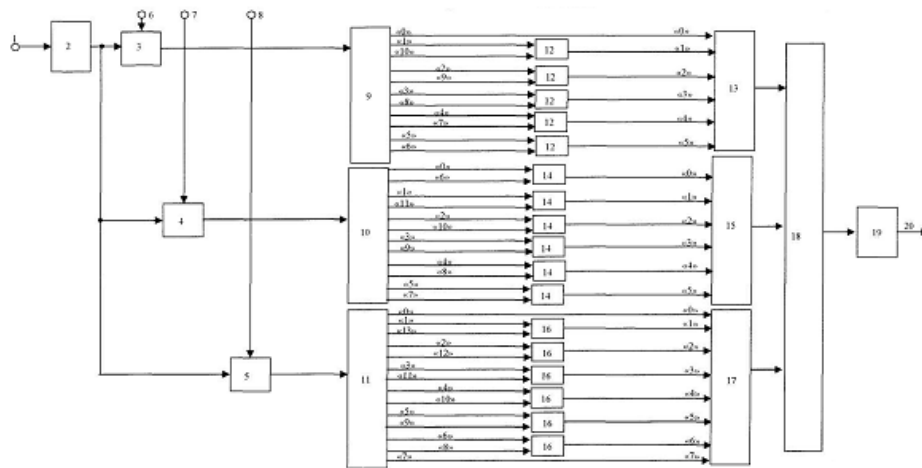
3. Патент на корисну модель № 51512, Україна, МПК G06F7/74, 2010, Бюл. № 14.



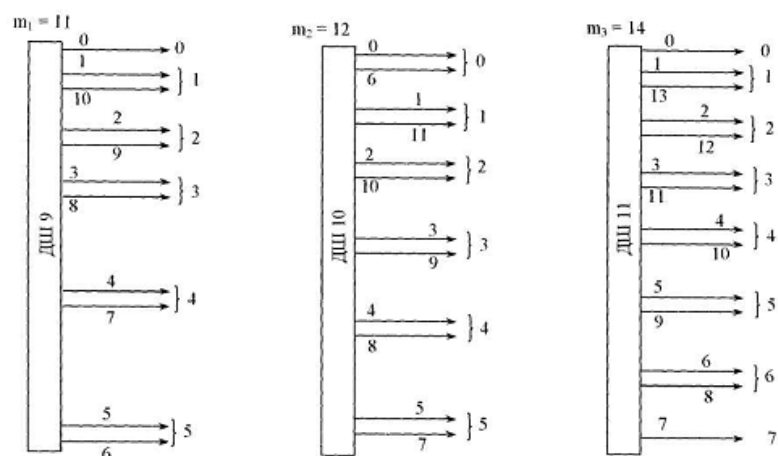
Фиг. 1



Фиг. 2



Фиг. 3



Фиг. 4

