УКРАЇНА

(19) UA (11) 4264 (13) U

(51) 7 G06F7/04

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

ОПИС
ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) ПРИСТРІЙ ДЛЯ ОБЧИСЛЕННЯ УСІЧЕНОГО ПЕРЕТВОРЕННЯ ФУР'Є В ОСТАТОЧНИХ КЛАСАХ

1

(21) 2004032321
(22) 30.03.2004
(24) 17.01.2005
(46) 17.01.2005, Бюл. № 1, 2005 р.
(72) Дуденко Сергій Васильович, Рубан Ігор Вікторович, Третяк В'ячеслав Федорович, Сумцов Дмитро Вікторович
(73) Дуденко Сергій Васильович, Рубан Ігор Вікторович, Третяк В'ячеслав Федорович, Сумцов Дмитро Вікторович
(57) Пристрій для обчислення усіченого перетворення Фур'є в остаточних класах, який містить блок оперативної пам'яті, перший, другий, третій та четвертий блоки постійної пам'яті, перший, другий та третій блоки, які реалізують операцію складання по модулю два, перший, другий, третій та четвертий допоміжні блоки постійної пам'яті, перший, другий, третій та четвертий регістри, блок управління, до складу якого входять генератор тактових імпульсів, тригер, лічильник, дешифратор, перший, другий, третій та четвертий елементи І, який відрізняється тим, що додатково введені другий, третій та четвертий блоки постійної пам'яті, перший, другий та третій блоки, які реалізують операцію складання по модулю два, перший, другий, третій та четвертий допоміжні блоки постійної пам'яті, перший, другий, третій та четвертий регістри, вхід запуску пристрою з'єднаний з входом блока управління, вхід дозволу читання блока оперативної пам'яті з'єднаний з першим виходом блока управління, вихід блока оперативної пам'яті з'єднаний з адресними входами першого, другого, третього та четвертого блоків постійної пам'яті, входи дозволу читання першого, другого, третього та четвертого блоків постійної пам'яті з'єднані з другим виходом блока управління, вихід першого блока постійної пам'яті з'єднаний з першим входом першого блока, що реалізує операцію складання по модулю два, вихід другого блока постійної пам'яті з'єднаний з другим входом першого блока, що реалізує операцію складання по модулю два, вихід першого блока, що реалізує операцію складання по модулю два, з'єднаний з першим входом другого блока, що реалізує операцію складання по модулю два, вихід третього блока постійної пам'яті з'єднаний з другим входом другого блока, що реалізує операцію складання по модулю два, вихід

2

другого блока, що реалізує операцію складання по модулю два, з'єднаний з першим входом третього блока, що реалізує операцію складання по модулю два, вихід четвертого блока постійної пам'яті з'єднаний з другим входом третього блока, що реалізує операцію складання по модулю два, вихід третього блока, що реалізує операцію складання по модулю два, з'єднаний з адресними входами першого, другого, третього та четвертого допоміжних блоків постійної пам'яті, входи дозволу читання котрих з'єднані з третім виходом блока управління, вихід першого допоміжного блока постійної пам'яті з'єднаний з входом запису першого регістра, вихід другого допоміжного блока постійної пам'яті з'єднаний з входом запису другого регістра, вихід третього допоміжного блока постійної пам'яті з'єднаний з входом запису третього регістра, вихід четвертого допоміжного блока постійної пам'яті з'єднаний з входом запису четвертого регістра, вхід дозволу запису першого, другого, третього та четвертого регістрів з'єднаний з четвертим виходом блока управління, вхід блока управління з'єднаний з входом переводу тригера в одиницю, вихід тригера з'єднаний з входом генератора тактових імпульсів, вихід якого з'єднаний з рахунковим входом лічильника та другим входом першого, другого, третього та четвертого елементів І, перший вихід лічильника з'єднаний з першим входом дешифратора, другий вихід лічильника з'єднаний з другим входом дешифратора, вихід переповнення лічильника з'єднаний з входом скидання тригера, перший вихід дешифратора з'єднаний з першим входом першого елемента І, другий вихід дешифратора з'єднаний з першим входом другого елемента І, третій вихід дешифратора з'єднаний з першим входом третього елемента І, четвертий вихід дешифратора з'єднаний з першим входом четвертого елемента І, вихід першого елемента І по першому виходу блока управління з'єднаний з входом дозволу читання блока оперативної пам'яті, вихід другого елемента І по другому виходу блока управління з'єднаний з входами управління читанням першого, другого, третього та четвертого блоків постійної пам'яті, вихід третього елемента І по третьому виходу блока управління з'єднаний з входом управління читанням першого, другого, третього та четвертого допоміжних

(19) UA (11) 4264 (13) U

блоків постійної пам'яті, вихід четвертого елемента І по четвертому виходу блока управління з'єднаний з входами управління записом першого, другого, третього та четвертого регістрів.

Запропонована корисна модель відноситься до галузі автоматики й обчислювальної техніки і може бути використаний в системах обробки і відображення інформації.

Відомий "Пристрій для обчислення дискретного перетворення Фур'є" [1], який містить інформаційний вхід, перемножувач, комутатор, N/2 обчислювальних модулей (де N - розмір перетворення), кожний з котрих містить k регістрів, тригер, два буферних регістра, два перемножувача, два регістри, два суматора. Крім цього, пристрій містить шину синхронізації, генератор тактових імпульсів, лічильник, дешифратор, елемент І-НІ, вхід завдання режиму, перемножувач, комутатор, два блоки постійної пам'яті.

Недоліком відомого пристрою є те, що він обчислює дискретне перетворення Фур'є комплексного вектору, кожна точка якого складається з дійсної та мнимої частини і тому потребує подвійних обчислень при знаходженні вихідного вектору.

Відомий також "Пристрій для швидкого дійсного перетворення Хартлі-Фур'є" [2], який містить блок синхронізації, два лічильника адреси, блок постійної пам'яті, вхідний регістр, регістр, вихідний регістр, блок пам'яті, два перемножувача, два комутатора, суматор-вичитач, вихідний регістр, комутатор, інформаційний вхід, інформаційний вихід.

Відомий пристрій перетворює коефіцієнти Хартлі в коефіцієнти Фур'є, що вказує на можливість використання пристроїв, які виконують перетворення Хартлі, для обчислення перетворення Фур'є при умові введення додаткових елементів та відповідних зв'язків. Недоліком пристрою є те, що він не виконує обчислень векторів.

Найбільш близьким до запропонованого технічним рішенням, обраним як прототип, є "Пристрій для реалізації швидкого перетворення Хартлі" [3], який містить: блок оперативної пам'яті, блок постійної пам'яті, блок управління, суматор, перемножувач, накопичуваючий суматор Блок управління містить генератор тактових імпульсів, тригер, два лічильники, дешифратор, одновібратор, чотири елементи І.

Недоліком пристрою-прототипу є те, що він обчислює дискретне перетворення Хартлі, яке має аналітичні вирази (1), що відрізняються від виразів для усіченого перетворення Фур'є в остаточних класах (2, 3).

В основу винаходу поставлена задача створити "Пристрій для обчислення усіченого перетворення Фур'є в остаточних класах", який реалізує табличний спосіб знаходження вихідного вектору при реалізації чотирьохточечного усіченого перетворення Фур'є в полі $GF(2^8)$.

Поставлена задача вирішується за рахунок того, що у пристрої-прототипі усунуті суматор, перемножувач, накопичуваючий суматор, та додатково введені другий, третій та четвертий блоки постійної пам'яті, перший, другий та третій блоки, що реалізують операцію складання по модулю два, перший, другий, третій та четвертий допоміжних блока постійної пам'яті, перший, другий, третій та четвертий регістри. В блоці управління усунуті: лічильник, одновібратор та додатково введені нові зв'язки у всьому пристрою.

Технічний результат, який може бути отриманий при здійсненні винаходу, полягає в одержанні технічного засобу для табличного способу знаходження вихідного вектору при реалізації чотирьохточечного усіченого перетворення Фур'є в полі $GF(2^8)$

На Фіг.1 зображена блок-схема запропонованого пристрою.

На Фіг.2 зображена блок-схема блоку управління запропонованого пристрою

Запропонований пристрій для обчислення усіченого перетворення Фур'є в остаточних класах (Фіг.1) містить блок оперативної пам'яті 1, чотири блоки постійної пам'яті 2-5, блок управління 6, три блоки, що реалізують операцію складання по модулю два 7-9, чотири допоміжних блоки постійної пам'яті 10-13, чотири регістра 14-17, вхід запуску 18, вихід 19, причому вхід запуску пристрою 18 з'єднаний з входом блоку управління. Вхід дозволу читання блоку оперативної пам'яті 1 з'єднаний з виходом блоку управління 20. Вихід блоку оперативної пам'яті 1 з'єднаний з адресними входами блоків постійної пам'яті 2-5 Входи дозволу читання блоків постійної пам'яті 2-5 з'єднані з виходом блоку управління 21. Вихід блоку постійної пам'яті 2 з'єднаний з першим входом блоку 7, що реалізує операцію складання по модулю два Вихід блоку постійної пам'яті 3 з'єднаний з другим входом блоку 7, що реалізує операцію складання по модулю два. Вихід блоку 7, що реалізує операцію складання по модулю два, з'єднаний з першим входом блоку 8, що реалізує операцію складання по модулю два. Вихід блоку постійної пам'яті 4 з'єднаний з другим входом блоку 8, що реалізує операцію складання по модулю два. Вихід блоку 8, що реалізує операцію складання по модулю два, з'єднаний з першим входом блоку 9, що реалізує операцію складання по модулю два. Вихід блоку постійної пам'яті 5 з'єднаний з другим входом блоку 9, що реалізує операцію складання по модулю два. Вихід блоку 9, що реалізує операцію складання по модулю два, з'єднаний з адресними входами допоміжних блоків постійної пам'яті 10-13 Входи дозволу допоміжних блоків постійної пам'яті 10-13 з'єднані з виходом блоку управління 22. Вихід до-

поміжного блоку постійної пам'яті 10 з'єднаний з входом запису регістру 14. Вихід допоміжного блоку постійної пам'яті 11 з'єднаний з входом запису регістру 15. Вихід допоміжного блоку постійної пам'яті 12 з'єднаний з входом запису регістру 16 Вихід допоміжного блоку постійної пам'яті 13 з'єднаний з входом запису регістру 17. Входи дозволу запису регістрів 14-17 з'єднаний з виходом блоку управління 23.

Блок управління 6 пристрою для обчислення усіченого перетворення Фур'є в остаточних класах (Фіг.2) містить тригер 24, генератор тактових імпульсів 25, лічильник 26, дешифратор 27, чотири елемента І 28-31, причому вхід блоку управління 18 з'єднаний з входом переводу тригера 24 в одиницю, вихід тригеру з'єднаний з входом генератору тактових імпульсів 25, вихід якого з'єднаний з рахунковим входом лічильника 26 та другими входами елементів І 28-31. Перший вихід лічильника 26 (молодший розряд) з'єднаний з першим входом дешифратора 27 (молодший розряд). Другий вихід лічильника 26 (старший розряд) з'єднаний з другим входом дешифратора 27 (старший розряд). Вихід переповнення лічильника 26 (переносу) з'єднаний з входом скидання тригера 24. Перший вихід дешифратора 27 з'єднаний з першим входом елемента І 28, другий вихід дешифратора 27 з'єднаний з першим входом елемента І 29, третій вихід дешифратора 27 з'єднаний з першим входом елемента І 30, четвертий вихід дешифратора 27 з'єднаний з першим входом елемента 131. Вихід елемента І 28 по виходу 20 блоку управління 6 з'єднаний з входом дозволу читання блоку оперативної пам'яті 1. Вихід елемента І 29 по виходу 21 блоку управління 6 з'єднаний з входами управління читанням блоків постійної пам'яті 2-5. Вихід елемента І 30 по виходу 22 блоку управління 6 з'єднаний з входом управління читанням допоміжних блоків постійної пам'яті 10-13. Вихід елемента І 31 по виходу 23 блоку управління 6 з'єднаний з входами управління записом регістрів 14-17

Робота запропонованого пристрою полягає в наступному. Перед початком роботи в блок оперативної пам'яті 1 записаний вхідний вектор

$v=\{v_1, v_2, v_3, v_4\}$ в двійковому коді, причому $V_i \in GF(2^8)$.

В блок постійної пам'яті 2 за адресою v_1=0-255 записані результати множення в $GF(2^8)$ у виді

$$\{P(v_1 \cdot 52) \otimes P(v_1 \cdot 103) \otimes P(v_1 \cdot 154) \otimes P(v_1 \cdot 205)\}$$

де P(X) - перехід від десяткового представлення елемента поля $GF(2^8)$ до двійкового представлення; ⊗ - знак конкатенації результатів множення.

В блок постійної пам'яті 3 за адресою v_2=0-255 записані результати

$$\{P(v_2 \cdot 103) \otimes P(v_2 \cdot 205) \otimes P(v_2 \cdot 52) \otimes P(v_2 \cdot 154)\}$$

В блок постійної пам'яті 4 за адресою a_3=0÷255 записані результати

$$\{P(v_3 \cdot 154) \otimes P(v_3 \cdot 52) \otimes P(v_3 \cdot 205) \otimes P(v_3 \cdot 103)\}.$$

В блок постійної пам'яті 5 за адресою a_4=0÷255 записані результати

$$\{P(v_4 \cdot 205) \otimes P(v_4 \cdot 154) \otimes P(v_4 \cdot 103) \otimes P(v_4 \cdot 52)\}.$$

Регістри 14-17, тригер 24 і лічильник тактів 26 у нульовому стані. В блоки допоміжної постійної пам'яті 10-13 за адресою a_1=0÷255 записані результати операції ОР (a_1) - зворотного переходу від двійкового представлення елемента поля $GF(2^8)$ до десяткового представлення.

По сигналу "Запуск обробки", що надходить по входу пристрою 18, тригер 24 встановлюється в одиничний стан, сигнал "1" з виходу тригера 24 надходить на вхід генератора тактових імпульсів 25, що починає формувати послідовність тактових імпульсів, що надходять на рахунковий вхід лічильника тактів 26 та другі входи елементів 128-131. На виході дешифратора 27 формується унітарний код такту, причому рівень "1" буде тільки на одному з чотирьох його виходів, з'єднаних з першими входами відповідних елементів І 28 - І 31.

На першому такті формується рівень "1" на першому виході дешифратора 27, що дозволяє проходження тактового імпульсу з генератора 25 через вихід 20 блоку управління 6 на вхід дозволу читання блоку постійної пам'яті 1, на виході якого формується вектор v.

На другому такті при надходженні через елемент І 29 виходу 21 блоку управління 6 тактового імпульсу вектор v з виходу блоку оперативної пам'яті 1 подається на адресні входи блоків постійної пам'яті у такому виді:

v_1 (розряди 0-7) на адресний вхід блоку постійної пам'яті 2,

v_2 (розряди 8-15) на адресний вхід блоку постійної пам'яті 3,

v_3 (розряди 16-23) на адресний вхід блоку постійної пам'яті 4,

v_4 (розряди 24-31) на адресний вхід блоку постійної пам'яті 5.

На третьому такті результат складання в блоках 7-9, що реалізують операцію складання по модулю два, надходить на адресні входи допоміжних блоків постійної пам'яті 10-13, а при надходженні через елемент І 30 виходу 22 блоку управління 6 тактового імпульсу на виходах допоміжних блоків постійної пам'яті 10-13 формуються відповідні коди у такому виді:

допоміжний блок постійної пам'яті 10 - розряди 0-7,

допоміжний блок постійної пам'яті 11 - розряди 8-15,

допоміжний блок постійної пам'яті 12 - розряди 16-23,

допоміжний блок постійної пам'яті 13 – розряди 24-31.

На четвертому такті при надходженні через елемент І 31 виходу 23 блоку управління 6 тактового імпульсу дозволяється запис у регістри 14-17.

Після завершення останнього такту на виході переповнення лічильника тактів 26 формується рівень "1", що скидає тригер 24 у нульовий стан, а пристрій повертається у початковий стан, при цьому з виходу пристрою 19 повинний бути зчитаний остаточний результат - вихідний вектор V:

V_1 - розряди 0-7, V_2 - розряди 8-15, V_3 - розряди 16-23, V_4 - розряди 24-31.

Перетворення Хартлі дійсної функції $f(\tau), \tau = 0,1,..,N-1$ є сума косинусного та синусного перетворень

$$H(v) = N^{-1}\sum_{\tau=0}^{N-1} f(\tau)\,cas(2\pi v\tau/N),\ v = \overline{0,N-1} \quad (1)$$

де $cas(\Theta) = \cos(\Theta) + \sin(\Theta)$.

Усічене перетворення Фур'є в остаточних класах визначено [4].

$$V_j = \sum_{i=1}^{n-1} w^{ij}\cdot v_i \quad (2)$$

$$v_i = \left(\frac{1}{n \bmod p}\right)\sum_{j=1}^{n-1}\left(w^{-ij}\oplus L\right)\cdot V_j \quad (3)$$

де w - елемент порядку n у полі GF (q^m), $\oplus$ - операція складання у полі, L= -1. Існує два способу знаходження вихідного вектора за виразами (2, 3):

1. Математичний спосіб, який полягає у виконанні усіх математичних операцій згідно аналітичних виразів.

2. Табличний спосіб, який полягає в тому, що строяться (n-1) таблиць, які складаються з 2^m елементів, розміру m(n-1) біт, а вихідний вектор отримується шляхом складання елементів таблиць, які відповідають точкам вхідного вектору.

Чотирьохточечне перетворення у полі GF (2^8) визначено

$$\begin{vmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \end{vmatrix} = \begin{vmatrix} 52 & 103 & 154 & 205 \\ 103 & 205 & 52 & 154 \\ 154 & 52 & 205 & 103 \\ 205 & 154 & 103 & 52 \end{vmatrix} \cdot \begin{vmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{vmatrix} \quad (4)$$

яке згідно табличного способу виконується за чотири такти таким чином:

1. З блоку оперативної пам'яті витягається вхідний вектор v={v_1, v_2, v_3, v_4},

причому $v_i \in GF(2^8)$ і надходить на адресні входи блоків постійної пам'яті:

v_1 - на адресний вхід першого блоку постійної пам'яті,

v_2 - на адресний вхід другого блоку постійної пам'яті,

v_3 - на адресний вхід третього блоку постійної пам'яті,

v_4 - на адресний вхід четвертого блоку постійної пам'яті.

2. На виходах блоків постійної пам'яті формується 32-розрядні коди K_i, які відповідають виконанню операцій:

в першому блоці - $K_1 = \{P(v_1\cdot 52)\otimes P(v_1\cdot 103)\otimes P(v_1\cdot 154)\otimes P(v_1\cdot 205)\}$,

в другому блоці - $K_2 = \{P(v_2\cdot 103)\otimes P(v_2\cdot 205)\otimes P(v_2\cdot 52)\otimes P(v_2\cdot 154)\}$,

в третьому блоці - $K_3 = \{P(v_3\cdot 154)\otimes P(v_3\cdot 52)\otimes P(v_3\cdot 205)\otimes P(v_3\cdot 103)\}$,

в четвертому блоці - $K_4 = \{P(v_4\cdot 205)\otimes P(v_4\cdot 154)\otimes P(v_4\cdot 103)\otimes P(v_4\cdot 52)\}$,

де P(X) - перехід від десяткового представлення елемента поля $GF(2^8)$ до двійкового представлення; $\otimes$ - знак конкатенації результатів множення.

3. В блоках, що реалізують складання по модулю два формується результат $K_1\oplus K_2\oplus K_3\oplus K_4$, який поступає на адресні входи допоміжних блоків постійної пам'яті:

розряди 0-7 на вхід першого допоміжного блоку постійної пам'яті,

розряди 8-15 на вхід другого допоміжного блоку постійної пам'яті,

розряди 16-23 на вхід третього допоміжного блоку постійної пам'яті,

розряди 24-31 на вхід четвертого допоміжного блоку постійної пам'яті.

На виходах допоміжних блоків постійної пам'яті формуються коди, які відповідають результату операції OP (X) - зворотного переходу від двійкового представлення елемента поля $GF(2^8)$ до десяткового.

4. З виходів допоміжних блоків постійної пам'яті результат заноситься до регістрів. На виходах регістрів формується результат: перший регістр – V_1, другий регістр – V_2, третій регістр – V_3, четвертий регістр – V_4.

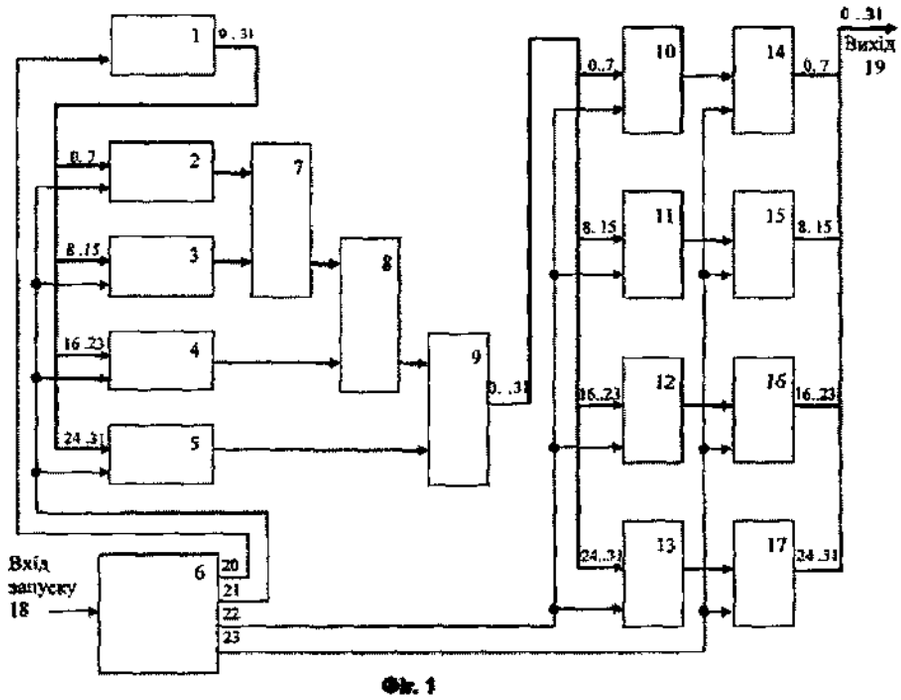
Джерела інформації

1. А.с. 1575202 СССР, МКИ G06F15/332. Устройство для вычисления дискретного преобразования Фурье. Ю.С. Каневский, Д.В. Корчев, И.А. Коноплицкий. - №4450024; Заявл. 30.05.88, Опубл 30.06.90, Бюл. №24.

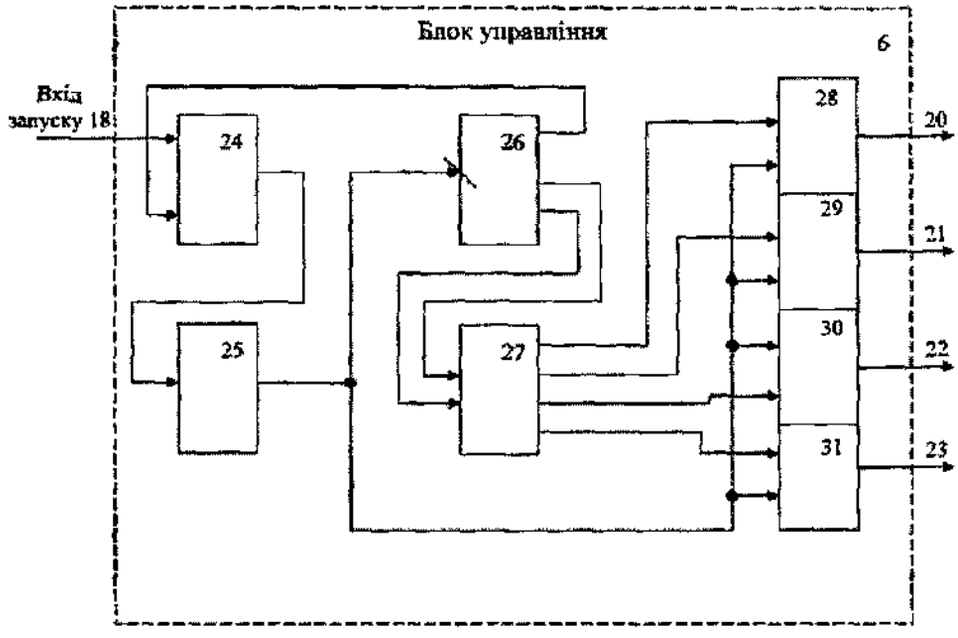
2. А.с. 1569847 СССР, МКИ G06F15/332. Устройство для быстрого действительного преобразования Хартли - Фурье С.Н. Демиденко, Э.Б. Куновский, О.В. Малашонок, Е.М. Левин. - №4473106, Заявл. 10.08.88, Опубл 7.06.90, Бюл. №21.

3. Деклараційний патент №58743 А України, 5МПК G06F07/04. Пристрій для реалізації швидкого перетворення Хартлі Дуденко С.В., Рубан І.В., Голубнічий Д.Ю., Корольова Н.А. Заявл. 1.10.2002, Опубл. 15.08.2003, Бюл. №8. - 4с.ил.

4. Рубан И.В., Дуденко С.В. Оптимизация теоретико-числовых преобразований // Інформаційно-керуючи системи на залізничному транспорті. - 2002. - №6. -С.47-49.



Фіг. 1



Фіг. 2

Комп'ютерна верстка Н Лисенко Підписне Тираж 37 прим

Міністерство освіти і науки України

Державний департамент інтелектуальної власності, вул. Урицького, 45, м Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул Глазунова, 1, м Київ – 42, 01601