



УКРАЇНА

(19) UA (11) 14431 (13) U
(51) МПК (2006)
G06F 5/00
G06F 17/14

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 ЗАЛИШКОВИХ КЛАСАХ

1

(21) u200510997

(22) 21.11.2005

(24) 15.05.2006

(46) 15.05.2006, Бюл. № 5, 2006 р.

(72) Дуденко Сергій Васильович, Рубан Ігор Вікторович, Алексєєв Сергій Вікторович, Колмиков Максим Миколайович, Калачова Вероніка Валеріївна
(73) ХАРКІВСЬКИЙ УНІВЕРСИТЕТ ПОВІТРЯНИХ СИЛ ІМЕНІ ІВАНА КОЖЕДУБА

(57) Пристрій для обчислення усіченого перетворення Фур'є в залишкових класах, який містить блок оперативної пам'яті, перший, другий, третій та четвертий блоки постійної пам'яті, перший та другий мультиплексори, блок складання по модулю два, перший, другий, третій, четвертий та п'ятий регістри, блок керування, до складу якого входять генератор тактових імпульсів, перший, другий та третій тригери, перший, другий, третій та четвертий лічильники, дешифратор, перший, другий, третій, четвертий та п'ятий елементи І, формувач фронтів, перший та другий елементи АБО, постійний запам'ятовуючий пристрій, який **відрізняється** тим, що додатково введені перший та другий мультиплексори, п'ятий регістр, до блока керування додатково введені другий, третій та четвертий лічильники, п'ятий елемент І, формувач фронтів, перший та другий елементи АБО, другий та третій тригери, блок постійної пам'яті, вхід запуску пристрою з'єднаний з входом блока керування, адресні входи блока оперативної пам'яті з'єднані з першим виходом блока керування, вхід дозволу читання блока оперативної пам'яті з'єднаний з другим виходом блока керування, 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 керування, вихід першого блока постійної пам'яті з'єднаний з першим входом першого мультиплексора, вихід другого блока постійної пам'яті з'єднаний з другим входом першого мультиплексора, вихід третього блока постійної пам'яті з'єднаний з третім входом першого мультиплексора, вихід четвертого блока постійної пам'яті з'єднаний з четвертим входом першого мультиплексора, адресні входи першого мультиплексора з'єднані з третім

2

виходом блока керування, вихід першого мультиплексора з'єднаний з другим входом блока, що реалізує операцію складання по модулю два, вихід блока, що реалізує операцію складання по модулю два, з'єднаний з входами даних першого, другого, третього та четвертого регістрів, входи дозволу запису першого, другого, третього та четвертого регістрів з'єднані з четвертим виходом блока керування, вихід першого регістра з'єднаний з першим входом другого мультиплексора, вихід другого регістра з'єднаний з другим входом другого мультиплексора, вихід третього регістра з'єднаний з третім входом другого мультиплексора, вихід четвертого регістра з'єднаний з четвертим входом другого мультиплексора, адресні входи другого мультиплексора з'єднані з п'ятим виходом блока керування, вихід другого мультиплексора з'єднаний з входом даних п'ятого регістра, вхід дозволу запису п'ятого регістра з'єднаний з п'ятим виходом блока керування, вихід п'ятого регістра є виходом пристрою та з'єднаний з першим входом блока, що реалізує операцію складання по модулю два, вхід блока керування з'єднаний з входом переводу першого тригера в одиницю, вихід першого тригера з'єднаний з входом генератора тактових імпульсів, вихід якого з'єднаний з рахунковим входом другого лічильника та другими входами другого, третього, четвертого та п'ятого елементів І, вхід скидання першого тригера з'єднаний з виходом переповнення (переносу) першого лічильника, перший вихід другого лічильника (молодший розряд) з'єднаний з першим входом дешифратора (молодший розряд) і першим входом першого елемента І, другий вихід другого лічильника з'єднаний з другим входом дешифратора, третій вихід другого лічильника з'єднаний з третім входом дешифратора, четвертий вихід другого лічильника (старший розряд) з'єднаний з четвертим входом першого елемента І, вихід першого елемента І з'єднаний з входом формувача фронтів, вихід формувача фронтів з'єднаний з входом першого лічильника, входом обнуління другого лічильника, входами обнуління другого та третього тригерів, перший вихід дешифратора з'єднаний з входом переводу другого тригера в одиницю, другий вихід дешифратора з'єднаний з входом переводження тре-

U
(13)
14431
(11)
UA
(19)

тього тригера в одиницю, третій вихід дешифратора з'єднаний з першим входом першого елемента АБО, четвертий вихід дешифратора з'єднаний з другим входом другого елемента АБО і першим входом другого елемента І, п'ятий вихід дешифратора з'єднаний з другим входом першого елемента АБО, шостий вихід дешифратора з'єднаний з третім входом другого елемента АБО і першим входом третього елемента І, сьомий вихід дешифратора з'єднаний з третім входом першого елемента АБО, восьмий вихід дешифратора з'єднаний з першим входом другого елемента АБО і першим входом четвертого елемента І, дев'ятий вихід дешифратора з'єднаний з четвертим входом першого елемента АБО, десятій вихід дешифратора з'єднаний з четвертим входом другого елемента АБО і першим входом п'ятого елемента І, вихід першого елемента АБО з'єднаний з тактовим входом третього лічильника, вихід другого елемента АБО з'єднаний з тактовим входом четвертого лічильника, виходи четвертого лічильника з'єднані з входами постійного запам'ятовуючого пристрою, вихід першого лічильника (молодший розряд) по першому виходу блока керування з'єднаний з адресним входом (молодший розряд) блока оперативної пам'яті, вихід першого лічильника (старший розряд) по першому виходу блока керування з'єд-

наний з адресним входом (старший розряд) блока оперативної пам'яті, вихід другого тригера по другому виходу блока керування з'єднаний з входом дозволу читання блока оперативної пам'яті, вихід третього тригера по другому виходу блока керування з'єднаний з входами дозволу читання першого, другого, третього та четвертого блоків постійної пам'яті, виходи постійного запам'ятовуючого пристрою по третьому виходу блока керування з'єднані з адресними входами першого мультиплексора, вихід другого елемента І по четвертому виходу блока керування з'єднаний з входом дозволу запису першого регістра, вихід третього елемента І по четвертому виходу блока керування з'єднаний з входом дозволу запису другого регістра, вихід четвертого елемента І по четвертому виходу блока керування з'єднаний з входом дозволу запису третього регістра, вихід п'ятого елемента І по четвертому виходу блока керування з'єднаний з входом дозволу запису п'ятого регістра, виходи третього лічильника по п'ятому виходу блока керування з'єднані з адресними входами другого мультиплексора.

Запропонована корисна модель відноситься до галузі автоматики й обчислювальної техніки і може бути використана в системах кодування даних.

Відомий "Пристрій для реалізації швидкого перетворення Хартлі" [1], який містить блок оперативної пам'яті, блок постійної пам'яті, блок керування, суматор, перемножувач, накопичувач суматор. Блок керування містить: генератор тактових імпульсів, тригер, два лічильники, дешифратор, одновібратор, чотири елемента І.

Недоліком пристрою є те, що він обчислює дискретне перетворення Хартлі, яке має аналітичні вирази, що відрізняються від виразів для усіченого перетворення Фур'є в остаточних класах.

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

Недоліком пристрою є те, що він не виконує обчислень векторів.

Найбільш близьким до запропонованого технічним рішенням, обраним як прототип, є "Пристрій для обчислення усіченого перетворення Фур'є в остаточних класах" [3], 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 керування, до

складу якого входять генератор тактових імпульсів, тригер, лічильник, дешифратор, перший, другий, третій та четвертий елементи І.

Недоліком пристрою-прототипу є те, що він обчислює усічене перетворення Фур'є в остаточних класах табличним способом.

В основу корисної моделі поставлена задача створити "Пристрій для обчислення усіченого перетворення Фур'є в остаточних класах", який реалізує знаходження вихідного вектора при реалізації чотирьохточечного усіченого перетворення Фур'є в полі $GF(2^8)$ математичним способом згідно (1).

Поставлена задача вирішується за рахунок того, що у пристрої-прототипі усунути другий та третій блоки, які реалізують операцію складання по модулю два, перший, другий, третій та четвертий допоміжні блоки постійної пам'яті, та додатково введені перший та другий мультиплексори, п'ятий регістр. До блока керування додатково введені другий, третій та четвертий лічильники, п'ятий елемент І, формувач фронтів, перший та другий елементи АБО, другий та третій тригери, блок постійної пам'яті. Також додатково введені нові зв'язки у всьому пристрої.

Технічний результат, який може бути отриманий при використанні корисної моделі, полягає в одержанні технічного засобу для знаходження вихідного вектора при реалізації чотирьохточечного усіченого перетворення Фур'є в полі $GF(2^8)$ математичним способом.

На Фіг.1 приведена блок-схема запропонованого пристрою.

На Фіг.2 приведена блок-схема блока керу-

вання запропонованого пристрою.

Запропонований пристрій для обчислення усіченого перетворення Фур'є в остаточних класах містить блок оперативної пам'яті 1, перший, другий, третій та четвертий блоки постійної пам'яті 2-5, блок керування 6, перший мультиплексор 7, блок складання по модулю два 8, перший, другий, третій та четвертий регістри 9-12, другий мультиплексор 13, п'ятий регістр 14, вхід запуску 15, вихід 16, причому вхід запуску 15 пристрою з'єднаний з входом блока керування. Адресні входи блока оперативної пам'яті 1 з'єднані з виходом 17 блока керування. Вхід дозволу читання блока оперативної пам'яті 1 з'єднаний з виходом 18 блока керування. Вихід блока 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 18 блока керування. Вихід блока постійної пам'яті 2 з'єднаний з першим входом мультиплексора 7. Вихід блока постійної пам'яті 3 з'єднаний з другим входом мультиплексора 7. Вихід блока постійної пам'яті 4 з'єднаний з третім входом мультиплексора 7. Вихід блока постійної пам'яті 5 з'єднаний з четвертим входом мультиплексора 7. Адресні входи мультиплексора 7 з'єднані з виходом 19 блока керування. Вихід мультиплексора 7 з'єднаний з другим входом блока 8, що реалізує операцію складання по модулю два. Вихід блока 8, що реалізує операцію складання по модулю два, з'єднаний з входами даних регістрів 9-12. Входи дозволу запису регістрів 9-12 з'єднані з виходом 20 блока керування. Вихід регістра 9 з'єднаний з першим входом мультиплексора 13. Вихід регістра 10 з'єднаний з другим входом мультиплексора 13. Вихід регістра 11 з'єднаний з третім входом мультиплексора 13. Вихід регістра 12 з'єднаний з четвертим входом мультиплексора 13. Адресні входи мультиплексора 13 з'єднані з виходом 21 блока керування. Вихід мультиплексора 13 з'єднаний з входом даних регістра 14. Вхід дозволу запису регістра 14 з'єднаний з виходом 21 блока керування. Вихід регістра 14 є виходом 16 пристрою та з'єднаний з першим входом блока 8, що реалізує операцію складання по модулю два.

Блок керування 6 пристрою для обчислення усіченого перетворення Фур'є в остаточних класах містить: генератор тактових імпульсів 22, перший тригер 23, перший та другий лічильники 24 і 25, дешифратор 26, перший елемент І 27, формувач фронтів 28, перший та другий елементи АБО 29 і 30, третій та четвертий лічильники 31 і 32, другий та третій тригери 33 і 34, постійний запам'ятовуючий пристрій 35, другий, третій, четвертий та п'ятий елементи І 36-39, причому вхід 15 блока керування з'єднаний з входом переводу тригера 23 в одиницю, вихід тригера 23 з'єднаний з входом генератора тактових імпульсів 22, вихід якого з'єднаний з рахунковим входом лічильника 25 та другими входами елементів І 36-39. Вхід скидання тригера 23 з'єднаний з виходом переповнення (переносу) лічильника 24. Перший вихід лічильника 25 (молодший розряд) з'єднаний з першим входом дешифратора 26 (молодший розряд) і першим входом елемента І 27. Другий вихід лічильника 25 з'єднаний з другим входом дешифратора 26. Третій вихід лічильника 25 з'єднаний з третім входом

дешифратора 26. Четвертий вихід лічильника 25 (старший розряд) з'єднаний з четвертим входом дешифратора 26 (старший розряд) і другим входом елемента І 27. Вихід елемента І 27 з'єднаний з входом формувача фронтів 28. Вихід формувача фронтів 28 з'єднаний з входом лічильника 24, входом обнуління лічильника 25, входами обнуління тригерів 33 і 34. Перший вихід дешифратора 26 з'єднаний з входом переводу тригера 33 в одиницю, другий вихід дешифратора 26 з'єднаний з входом переводу тригера 34 в одиницю, третій вихід дешифратора 26 з'єднаний з першим входом елемента АБО 29, четвертий вихід дешифратора 26 з'єднаний з другим входом елемента АБО 30 і першим входом елемента І 36, п'ятий вихід дешифратора 26 з'єднаний з другим входом елемента АБО 29, шостий вихід дешифратора 26 з'єднаний з третім входом елемента АБО 30 і першим входом елемента І 37, сьомий вихід дешифратора 26 з'єднаний з третім входом елемента АБО 29, восьмий вихід дешифратора 26 з'єднаний з першим входом елемента АБО 30 і першим входом елемента І 38, дев'ятий вихід дешифратора 26 з'єднаний з четвертим входом елемента АБО 29, десятий вихід дешифратора 26 з'єднаний з четвертим входом елемента АБО 30 і першим входом елемента І 39. Вихід елемента АБО 29 з'єднаний з тактовим входом лічильника 31. Вихід елемента АБО 30 з'єднаний з тактовим входом лічильника 32. Виходи лічильника 32 з'єднані з входами постійного запам'ятовуючого пристрою 35. Вихід лічильника 24 (молодший розряд) по виходу 17 блока керування 6 з'єднаний з адресним входом (молодший розряд) блока оперативної пам'яті 1. Вихід лічильника 24 (старший розряд) по виходу 17 блока керування 6 з'єднаний з адресним входом (старший розряд) блока оперативної пам'яті 1. Вихід тригера 33 по виходу 18 блока керування 6 з'єднаний з входом дозволу читання блока оперативної пам'яті 1. Вихід тригера 34 по виходу 18 блока керування 6 з'єднаний з входами дозволу читання блоків постійної пам'яті 2-5. Виходи постійного запам'ятовуючого пристрою 35 по виходу 19 блока керування 6 з'єднані з адресними входами мультиплексора 7. Вихід елемента І 36 по виходу 20 блока керування 6 з'єднаний з входом дозволу запису регістра 9. Вихід елемента І 37 по виходу 20 блока керування 6 з'єднаний з входом дозволу запису регістра 10. Вихід елемента І 38 по виходу 20 блока керування 6 з'єднаний з входом дозволу запису регістра 11. Вихід елемента І 39 по виходу 20 блока керування 6 з'єднаний з входом дозволу запису регістра 12. Вихід елемента АБО 29 по виходу 21 блока керування 6 з'єднаний з входом дозволу запису регістра 14. Виходи лічильника 31 по виходу 21 блока керування 6 з'єднані з адресними входами мультиплексора 13.

Робота запропонованого пристрою здійснюється за 4 цикли по 10 тактів у кожному та 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 $v_i = 0 \div 255$ записані результати множення в $GF(2^8)$ у виді

$$\{P(v_i \cdot 52)\},$$

де $P(X)$ - перехід від десяткового представ-

лення елемента поля $GF(2^8)$ до двійкового представлення.

В блок постійної пам'яті 3 за адресою $v_i=0÷255$ записані результати

$\{P(v_i \cdot 103)\}$.

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

$\{P(v_i \cdot 154)\}$.

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

$\{P(v_i \cdot 205)\}$.

Регістри 9-12, регістр 14, тригер 23, лічильники 24, 25, 31, 32, тригери 33 і 34 у нульовому стані.

На виході дешифратора 26 під час роботи пристрою формується унітарний код такту, причому рівень "1" буде тільки на одному з його виходів.

Постійний запам'ятовуючий пристрій 35 містить для кожного з тактів 4, 6, 8, 10 циклів 1-4 адреси, що використовуються для адресації мультиплексора 7 з метою здійснення математичного способу знаходження вихідного вектора при реалізації чотирьохточечного усіченого перетворення Фур'є в полі $GF(2^8)$.

По сигналу "Запуск обробки", що надходить по входу 15 пристрою, тригер 23 встановлюється в одиничний стан, сигнал "1" з виходу тригера 23 надходить на вхід генератора тактових імпульсів 22, що починає формувати послідовність тактових імпульсів, що надходять на рахунковий вхід лічильника 25 та другі входи елементів І 36-І 39.

Цикл 1.

На першому такті формується рівень "1" на першому виході дешифратора 26, що встановлює тригер 33 в одиницю. Рівень "1" з виходу тригера 33 через вихід 18 блока керування 6 поступає на вхід дозволу читання блока оперативної пам'яті 1, на виході якого формується двійкове представлення числа v_1 .

На другому такті формується рівень "1" на другому виході дешифратора 26, що встановлює тригер 34 в одиницю. Рівень "1" з виходу тригера 34 через вихід 18 блока керування 6 поступає на входи дозволу читання блоків постійної пам'яті 2-5. При цьому на виході блока постійної пам'яті 2 формується двійкове представлення результату множення $v_1 \cdot 52$ у полі $GF(2^8)$, на виході блока постійної пам'яті 3 - двійкове представлення результату множення $v_1 \cdot 103$ у полі $GF(2^8)$, на виході блока постійної пам'яті 4 - двійкове представлення результату множення $v_1 \cdot 154$ у полі $GF(2^8)$, на виході блока постійної пам'яті 5 - двійкове представлення результату множення $v_1 \cdot 205$ у полі $GF(2^8)$. Двійкове представлення результату множення з виходу відповідного блока постійної пам'яті (2-5) через мультиплексор 7 поступає на другий вхід блока 8. З виходу блока 8 результат складання по модулю 2 результату множення зі значенням, що міститься на виході регістра 14, поступає на входи даних регістрів 9-12.

На третьому такті формується рівень "1" на третьому виході дешифратора 26, що з виходу елемента АБО 29 через вихід 21 блока керування 6 по передньому фронту імпульсу в регістр 14 через мультиплексор 13 записує значення, що міститься у регістрі 9. По задньому фронту імпульсу з

виходу елемента АБО 29 лічильник 31 збільшує своє значення на одиницю. Двійковий код з виходу лічильника 31 через вихід 21 блока керування 6 поступає на адресні входи мультиплексора 13 та комується на вхід даних регістра 14 вихід регістра 10.

На четвертому такті формується рівень "1" на четвертому виході дешифратора 26, що з виходу елемента І 36 через вихід 20 блока керування 6 записує до регістра 9 результат складання по модулю 2 результату множення v_1 у полі $GF(2^8)$ зі значенням, що міститься на виході регістра 14. Рівень "1" з четвертого виходу дешифратора 26 поступає на елемент АБО 30. По передньому фронту імпульсу з виходу елемента АБО 30 лічильник 32 збільшує своє значення на одиницю. При цьому з виходу постійного запам'ятовуючого пристрою 35 через вихід 19 блока керування 6 на адресних входах мультиплексора 7 встановлюється новий адрес і двійкове представлення результату множення з виходу відповідного блока постійної пам'яті 2-5 через мультиплексор 7 поступає на другий вхід блока 8. З виходу блока 8 результат складання по модулю 2 результату множення з значенням, що міститься на виході регістра 14, поступає на входи даних регістрів 9-12.

На п'ятому такті формується рівень "1" на п'ятому виході дешифратора 26, що з виходу елемента АБО 29 через вихід 21 блока керування 6 по передньому фронту імпульсу в регістр 14 через мультиплексор 13 записує значення, що міститься у регістрі 10. По задньому фронту імпульсу з виходу елемента АБО 29 лічильник 31 збільшує своє значення на одиницю. Двійковий код з виходу лічильника 31 через вихід 21 блока керування 6 поступає на адресні входи мультиплексора 13 та комується на вхід даних регістра 14 вихід регістра 11.

На шостому такті формується рівень "1" на шостому виході дешифратора 26, що з виходу елемента І 37 через вихід 20 блока керування 6 записує до регістра 10 результат складання по модулю 2 результату множення v_1 у полі $GF(2^8)$ зі значенням, що міститься на виході регістра 14. Рівень "1" з шостого виходу дешифратора 26 поступає на елемент АБО 30. По передньому фронту імпульсу з виходу елемента АБО 30 лічильник 32 збільшує своє значення на одиницю. При цьому з виходу постійного запам'ятовуючого пристрою 35 через вихід 19 блока керування 6 на адресних входах мультиплексора 7 встановлюється новий адрес і двійкове представлення результату множення з виходу відповідного блока постійної пам'яті 2-5 через мультиплексор 7 поступає на другий вхід блока 8. З виходу блока 8 результат складання по модулю 2 результату множення зі значенням, що міститься на виході регістра 14, поступає на входи даних регістрів 9-12.

На сьомому такті формується рівень "1" на сьомому виході дешифратора 26, що з виходу елемента АБО 29 через вихід 21 блока керування 6 по передньому фронту імпульсу в регістр 14 через мультиплексор 13 записує значення, що міститься у регістрі 11. По задньому фронту імпульсу з виходу елемента АБО 29 лічильник 31 збільшує своє значення на одиницю. Двійковий код з виходу лічильника 31 через вихід 21 блока керування 6

поступає на адресні входи мультиплексора 13 та комутує на вхід даних регістра 14 вихід регістра 12.

На восьмому такті формується рівень "1" на восьмому виході дешифратора 26, що з виходу елемента І 38 через вихід 20 блока керування 6 записує до регістра 11 результат складання по модулю 2 результату множення v_1 у полі $GF(2^8)$ зі значенням, що міститься на виході регістра 14. Рівень "1" з восьмого виходу дешифратора 26 поступає на елемент АБО 30. По передньому фронту імпульсу з виходу елемента АБО 30 лічильник 32 збільшує своє значення на одиницю. При цьому з виходу постійного запам'ятовуючого пристрою 35 через вихід 19 блока керування 6 на адресних входах мультиплексора 7 встановлюється новий адрес і двійкове представлення результату множення з виходу відповідного блока постійної пам'яті 2-5 через мультиплексор 7 поступає на другий вхід блока 8. З виходу блока 8 результат складання по модулю 2 результату множення зі значенням, що міститься на виході регістра 14, поступає на входи даних регістрів 9-12.

На дев'ятому такті формується рівень "1" на дев'ятому виході дешифратора 26, що з виходу елемента АБО 29 через вихід 21 блока керування 6 по передньому фронту імпульсу в регістр 14 через мультиплексор 13 записує значення, що міститься у регістрі 12. По задньому фронту імпульсу з виходу елемента АБО 29 лічильник 31 встановлюється в 0. Двійковий код з виходу лічильника 31 через вихід 21 блока керування 6 поступає на адресні входи мультиплексора 13 та комутує на вхід даних регістра 14 вихід регістра 9.

На десятому такті формується рівень "1" на десятому виході дешифратора 26, що з виходу елемента І 39 через вихід 20 блока керування 6 записує до регістра 12 результат складання по модулю 2 результату множення v_1 у полі $GF(2^8)$ зі значенням, що міститься на виході регістра 14. Рівень "1" з десятого виходу дешифратора 26 поступає на елемент АБО 30. По передньому фронту імпульсу з виходу елемента АБО 30 лічильник 32 збільшує своє значення на одиницю. При цьому з виходу постійного запам'ятовуючого пристрою 35 через вихід 19 блока керування 6 на адресних входах мультиплексора 7 встановлюється новий адрес і двійкове представлення результату множення з виходу відповідного блока постійної пам'яті 2-5 через мультиплексор 7 поступає на другий вхід блока 8. З виходу блока 8 результат складання по модулю 2 результату множення зі значенням, що міститься на виході регістра 14, поступає на входи даних регістрів 9-12. По задньому фронту імпульсу з виходу елемента І 27 через формувач фронтів 28 здійснюється збільшення на одиницю лічильника 24, обнуління лічильника 25 та встановлення в "0" тригерів 33 і 34. Двійковий код з виходу лічильника 24 через вихід 17 блока керування 6 встановлює на адресних входах блока оперативної пам'яті 1 адресу для зчитування двійкового

представлення числа v_2 .

Цикл 2 здійснюється аналогічно циклу 1 за винятком того, що всі операції здійснюються з використанням двійкового представлення числа v_2 .

Цикл 3 здійснюється аналогічно циклу 1 за винятком того, що всі операції здійснюються з використанням двійкового представлення числа v_3 .

Цикл 4 здійснюється аналогічно циклу 1 за винятком того, що всі операції здійснюються з використанням двійкового представлення числа v_4 .

Після завершення останнього такту четвертого циклу на виході переповнення лічильника 24 формується рівень "1", що скидає тригер 23 у нульовий стан, а пристрій повертається у початковий стан, при цьому з виходу 16 пристрою повинний бути зчитаний остаточний результат.

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

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

$$v_i = \left(\frac{1}{n \bmod p} \right) \sum_{j=1}^{n-1} (w^{-ij} \oplus L) \cdot V_j, \quad (2)$$

де w - елемент порядку n у полі $GF(q^m)$;

$\oplus$ - операція складання у полі;

$L = -1$.

Існує два способу знаходження вихідного вектора:

1. Математичний спосіб, який полягає у використанні усіх математичних операцій згідно (1).

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

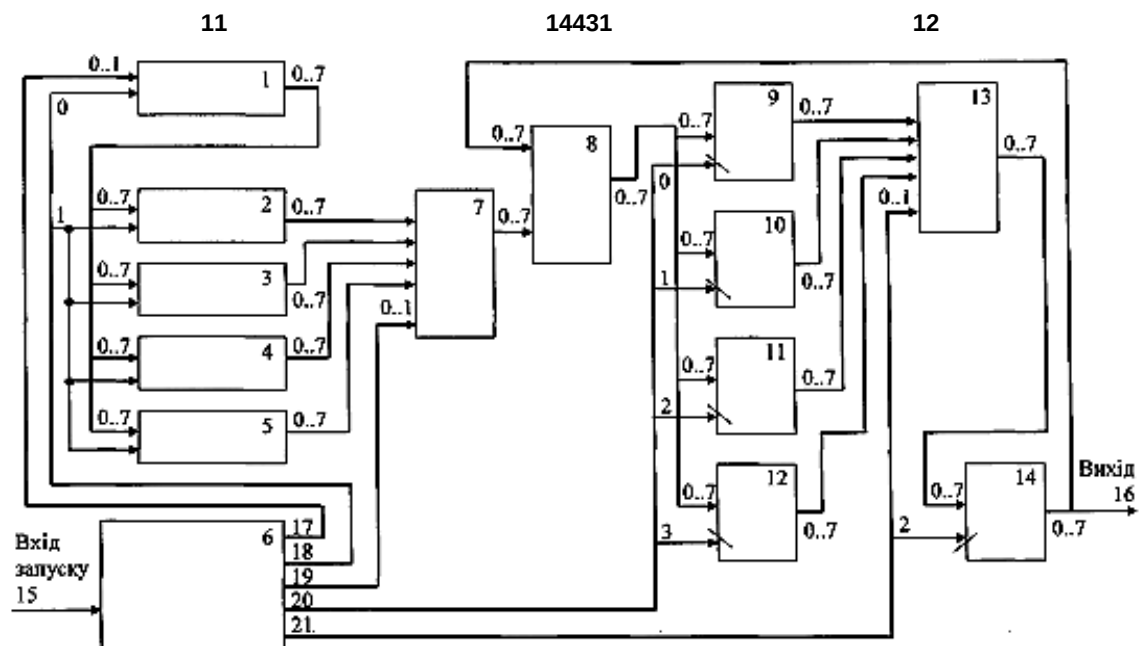
Джерела інформації:

1. Деклараційний патент №58743А України, 7МПК G06F7/04. Пристрій для реалізації швидкого перетворення Хартлі /Дуденко С.В., Рубан І.В., Голубнічий Д.Ю., Корольова Н.А. -№20021107777; Заяв. 1.10.2002, Опубл. 15.08.2003, Бюл. №8. -4с. ил.

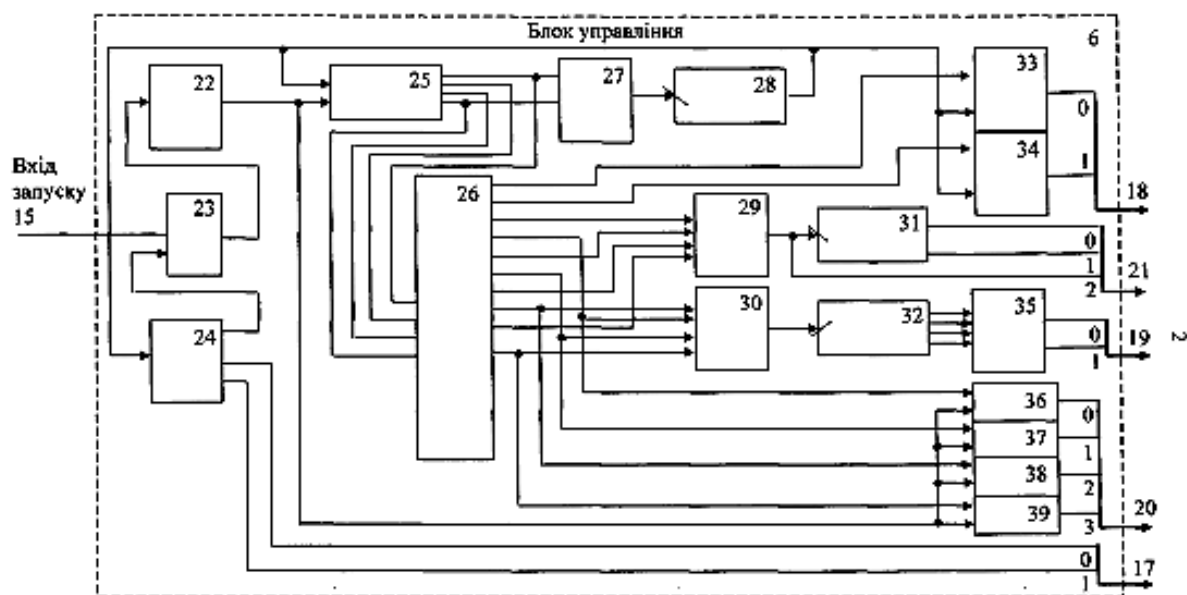
2. А.с. 1569847 СССР, МКИ G06F15/332. Устройство для быстрого действительного преобразования Хартли-Фур'є /С.Н. Демиденко, Э.Б. Куновский, О.В. Малашонок, Е.М. Левин. -№4473106; Заяв. 10.08.88, Опубл. 7.06.90, Бюл. №21.

3. Деклараційний патент №4264U України, 7МПК G06F7/04. Пристрій для обчислення усіченого перетворення Фур'є в остаточних класах /Дуденко С.В., Рубан І.В., Третяк В.Ф., Сумцов Д.В. -№2004032321; Заяв. 30.03.2004, Опубл. 17.01.2005, Бюл. №1. -4с. ил.

4. Рубан І.В., Дуденко С.В. Оптимизация теоретико-числовых преобразований //Информационно-керуючі системи на залізничному транспорті. - 2002. -№6. -С.47-49.



Фиг. 1



Фиг. 2