УКРАЇНА

(19) UA (11) 57281 (13) U

(51) МПК (2011.01)
G06F 7/48

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) СУМАТОР ЕЛЕМЕНТІВ ПОЛЯ GF(p^m)

1

(21) u201004903
(22) 23.04.2010
(24) 25.02.2011
(46) 25.02.2011, Бюл.№ 4, 2011 р.
(72) ДИЧКА ІВАН АНДРІЙОВИЧ, ОНАЙ МИКОЛА ВОЛОДИМИРОВИЧ
(73) НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
(57) Суматор елементів поля GF(p^m), що містить шину(1) коду першого операнда, шину (2) коду другого операнда, шину (3) коду модуля, першу (8) та другу (9) групу елементів АБО, комбінаційний суматор (10), схему порівняння кодів (11), шину коду операції (16), групу елементів І (30) та вихід (32) пристрою, який **відрізняється** тим, що додатково містить регістровий запам'ятовувальний пристрій (4) першого операнда та регістровий запам'ятовувальний пристрій (5) другого операнда, регістр (6) модуля, лічильник адрес (7), регістр (12) проміжного результату, двовходовий логічний елемент АБО-НІ (13), індикатор кінцевого стану лічильника (14), блок керування (15), регістровий запам'ятовувальний пристрій (31) результату, при цьому шина(1) коду першого операнда з'єднана з першими n інформаційними входами регістрового запам'ятовувального пристрою (4) першого операнда, шина (2) другого операнда з'єднана з першими n інформаційними входами регістрового запам'ятовувального пристрою (5) другого операнда, шина (3) коду модуля з'єднана з першими n входами регістра (6) модуля, вихід регістрового запам'ятовувального пристрою (4) першого операнда з'єднаний з другим входом першої групи елементів АБО (8), прямий вихід регістрового запам'ятовувального пристрою (5) другого операнда з'єднаний з другим входом другої групи елементів АБО (9), інверсний вихід регістрового запам'ятовувального пристрою (5) другого операнда з'єднаний з першим входом другої групи елементів АБО (9), прямий вихід регістра (6) модуля з'єднаний з четвертим входом другої групи елементів АБО (9), а перші n-1 розрядів прямого виходу регістра (6) модуля з'єднані з другим входом схеми порівняння кодів (11), інверсний вихід регістра (6) модуля з'єднаний з третім входом другої групи елементів АБО (9), виходи першої (8) та другої (9) групи елементів АБО з'єднані з відповідними входами комбінаційного суматора (10), вихід комбінаційного суматора (10) з'єднаний з входом регістра (12) проміжного результату, вихід регістра (12) проміжного результату з'єднаний з першим входом першої групи елементів АБО (8) та з першим входом групи елементів І (30), перші n-1 розрядів виходу регістра (12) проміжного результату з'єднані з першим входом схеми порівняння кодів (11), (n+1)-й розряд (17) регістра (12) проміжного результату з'єднаний з другим входом двовходового логічного елемента АБО-НІ (13) та з другим входом блока керування (15), n-й розряд регістра (12) проміжного результату з'єднаний з першим входом двовходового логічного елемента АБО-НІ (13), вихід (18) двовходового логічного елемента АБО-НІ (13) з'єднаний з третім входом блока керування (15), перший вхід блока керування (15) з'єднаний з шиною (16) коду операції, четвертий вхід блока керування (15) з'єднаний з виходом (19) схеми порівняння кодів (11), п'ятий вхід блока керування (15) з'єднаний з виходом (20) індикатора кінцевого стану лічильника (14), перший вихід (21) блока керування (15) з'єднаний з входом керування видачею коду з регістрового запам'ятовувального пристрою (4) першого операнда, другий вихід (22) блока керування (15) з'єднаний з входом керування видачею коду з регістрового запам'ятовувального пристрою (5) другого операнда, третій вихід (23) блока керування (15) з'єднаний з входом керування видачею інверсного коду з регістрового запам'ятовувального пристрою (5) другого операнда, четвертий вихід (24) блока керування (15) з'єднаний з входом керування видачею коду з регістра (6) модуля, п'ятий вихід (25) блока керування (15) з'єднаний з входом керування видачею інверсного коду з регістра (6) модуля, шостий вихід (26) блока керування (15) з'єднаний з керуючим входом прийому коду в регістр (12) проміжного результату, сьомий вихід (27) блока керування (15) з'єднаний з другим входом групи елементів І (30) та входом керування прийому коду в регістровий запам'ятовувальний пристрій (31) результату, восьмий вихід (28) блока керування (15) з'єднаний з входом вхідного переносу комбінаційного суматора (10), дев'ятий вихід (29) блока керування (15) з'єднаний з синхровходом лічильника адрес (7), перші n розрядів виходу групи елементів І (30) з'єднані з інформаційним входом регістрового запам'ятовува-

2

(19) UA (11) 57281 (13) U

льного пристрою (31) результату, вихід (32) регістрового запам'ятовувального пристрою (31) результату є виходом пристрою.

Корисна модель належить до галузі автоматики та обчислювальної техніки і може бути використана при реалізації додавання та віднімання елементів поля GF(p^m), а саме у спеціалізованих обчислювальних пристроях для побудови швидкодіючих блоків виконання операцій у полях виду GF(p^m), системах криптографічних перетворень, системах цифрового підпису, системах обробки інформації та системах кодування-декодування даних.

Відомий суматор за модулем три [1], що містить шину першого операнда, шину другого операнда, групу елементів І та групу елементів АБО, елементи І та елементи АБО, а також шину результата. Даний пристрій дозволяє виконувати операцію додавання за модулем три. Одним з недоліків його є обмежені функціональні можливості, оскільки цей пристрій дає можливість виконувати тільки операцію додавання і тільки для фіксованого значення модуля, яке дорівнює трьом, а операція віднімання не передбачена. Також недоліком є те, що в якості операндів можуть виступати лише елементи основного поля Галуа, тобто елементи поля GF(p).

Відомий пристрій для додавання та віднімання чисел за модулем [2], що містить шину першого операнда, шину другого операнда, елементи АБО, елементи І, лічильник та шину результата. Недоліком цього пристрою є обмежені функціональні можливості, оскільки він виконує тільки операцію додавання та віднімання двох операндів, які є елементами основного поля Галуа GF(p).

Найбільш близьким за технічною сутністю і результатом, що досягається, є суматор за модулем системи залишкових класів [3], що містить шину першого операнда, шину керування, шину другого операнда, першу групу елементів АБО, блок інвертування коду вхідного операнда, другу групу елементів АБО, регістр першого та другого операнда, комбінаційний суматор, схему порівняння двійкових чисел, шини коду модуля, елемент НІ, першу та другу групи елементів І, шини доповняльного кода значення модуля, третю та четверту групи елементів І, елемент І-НІ, регістр результата, виходи пристрою, при цьому шини першого операнда з'єднані з першими входами першої групи елементів АБО, шини другого операнда з'єднані з входами блока інвертування коду другого вхідного операнда, шина керування з'єднана з керуючим входом блока інвертування коду другого вхідного операнда, виходи блока інвертування коду другого вхідного операнда з'єднані з першими входами другої групи елементів АБО, виходи першої та другої груп елементів АБО з'єднані відповідно з входами регістра першого та другого операндів, виходи регістрів першого та другого операндів з'єднані з відповідними входами комбінаційного суматора, виходи комбінаційного суматора з'єднані з першими входами першої та другої групи елементів І та з першими входами схеми порівняння двійкових чисел, другі входи схеми порівняння двійкових чисел з'єднані з шинами коду модуля, вихід схеми порівняння двійкових чисел з'єднаний з входом елемента НІ та другими входами другої та третьої груп елементів І, вихід елемента НІ з'єднаний з другими входами першої групи елементів І, перші входи третьої групи елементів І з'єднані з шинами значення доповняльного кода модуля, виходи другої та третьої груп елементів І з'єднані з другими входами відповідно першої та другої груп елементів АБО, виходи першої групи елементів І, на яких присутній сигнал значення одиничних розрядів у записі модуля, з'єднані з входами елемента І-НІ, вихід елемента І-НІ з'єднаний з другими входами четвертої групи елементів І, виходи першої групи елементів І з'єднані з першими входами четвертої групи елементів І, виходи четвертої групи елементів І з'єднані з входами вихідного регістра, виходи вихідного регістра є виходами пристрою.

Недоліком цього пристрою є обмежені функціональні можливості, оскільки він виконує операцію додавання тільки коли операндами є елементи основного поля Галуа GF(p), а операція віднімання реалізована тільки для операндів які є елементами основного поля Галуа GF(p), характеристикою якого є число Мерсена. Числами Мерсена називають числа двійковий код яких містить всі одиниці, наприклад, 7,31. Узагальнена формула таких чисел має вигляд $p = 2^n - 1$, де n - будь-яке натуральне число.

В основу корисної моделі покладена задача розширення функціональних можливостей суматора елементів поля GF(p). Поставлена задача вирішується тим, що в суматорі елементів поля GF(p^m), що містить шину 1 кода першого операнда, шину 2 кода другого операнда, шину 3 кода модуля, першу 8 та другу 9 групу елементів АБО, комбінаційний суматор 10, схему порівняння кодів 11, шину кода операції 16, групу елементів І 30 та вихід 32 пристрою, згідно корисної моделі новим є те, що додано регістровий запам'ятовувальний пристрій 4 першого операнда та регістровий запам'ятовувальний пристрій 5 другого операнда, регістр 6 модуля, лічильник адрес 7, регістр 12 проміжного результата, двовходовий логічний елемент АБО-НІ 13, індикатор кінцевого стану лічильника 14, блок керування 15, регістровий запам'ятовувальний пристрій 31 результата, при цьому шина 1 кода першого операнда з'єднана з першими n інформаційними входами ($n =]\log_2 p[$, де] [символ округлення до найближчого більшого цілого числа) регістрового запам'ятовувального пристрою 4 першого операнда, шина 2 другого операнда з'єднана з першими n інформаційними входами регістрового запам'ятовувального пристрою 5 другого операнда, шина 3 кода модуля

з'єднана з першими n входами регістра 6 модуля, вихід регістрового запам'ятовувального пристрою 4 першого операнда з'єднаний з другим входом першої групи елементів АБО 8, прямий вихід регістрового запам'ятовувального пристрою 5 другого операнда з'єднаний з другим входом другої групи елементів АБО 9, інверсний вихід регістрового запам'ятовувального пристрою 5 другого операнда з'єднаний з першим входом другої групи елементів АБО 9, прямий вихід регістра 6 модуля з'єднаний з четвертим входом другої групи елементів АБО 9, а перші $n-1$ розрядів прямого виходу регістра 6 модуля з'єднані з другим входом схеми порівняння кодів 11, інверсний вихід регістра 6 модуля з'єднаний з третім входом другої групи елементів АБО 9, виходи першої 8 та другої 9 групи елементів АБО з'єднані з відповідними входами комбінаційного суматора 10, вихід комбінаційного суматора 10 з'єднаний з входом регістра 12 проміжного результата, вихід регістра 12 проміжного результата з'єднаний з першим входом першої групи елементів АБО 8 та з першим входом групи елементів І 30, перші $n-1$ розрядів виходу регістра 12 проміжного результата з'єднані з першим входом схеми порівняння кодів 11, $(n+1)$-й розряд 17 регістра 12 проміжного результата з'єднаний з другим входом двовходового логічного елемента АБО-НІ 13 та з другим входом блока керування 15, п-й розряд регістра 12 проміжного результата з'єднаний з першим входом двовходового логічного елемента АБО-НІ 13, вихід 18 двовходового логічного елемента АБО-НІ 13 з'єднаний з третім входом блока керування 15, перший вхід блока керування 15 з'єднаний з шиною 16 кода операції, четвертий вхід блока керування 15 з'єднаний з виходом 19 схеми порівняння кодів 11, п'ятий вхід блока керування 15 з'єднаний з виходом 20 індикатора кінцевого стану лічильника 14, перший вихід 21 блока керування 15 з'єднаний з входом керування видачею кода з регістрового запам'ятовувального пристрою 4 першого операнда, другий вихід 22 блока керування 15 з'єднаний з входом керування видачею кода з регістрового запам'ятовувального пристрою 5 другого операнда, третій вихід 23 блока керування 15 з'єднаний з входом керування видачею інверсного кода з регістрового запам'ятовувального пристрою 5 другого операнда, четвертий вихід 24 блока керування 15 з'єднаний з входом керування видачею кода з регістра 6 модуля, п'ятий вихід 25 блока керування 15 з'єднаний з входом керування видачею інверсного кода з регістра 6 модуля, шостий вихід 26 блока керування 15 з'єднаний з керуючим входом прийому кода в регістр 12 проміжного результата, сьомий вихід 27 блока керування 15 з'єднаний з другим входом групи елементів І 30 та входом керування прийому кода в регістровий запам'ятовувальний пристрій 31 результата, восьмий вихід 28 блока керування 15 з'єднаний з входом вхідного переноса комбінаційного суматора 10, дев'ятий вихід 29 блока керування 15 з'єднаний з синхровходом лічильника адрес 7, перші n розрядів вихода групи елементів І 30 з'єднані з інформаційним входом регістрового запам'ятовувального пристрою 31 результата, вихід 32 регістрового запам'ятовувального пристрою 31 результата є виходом пристрою.

Введення вказаних ознак дозволяє розширити функціональні можливості пристрою, а саме виконувати операції додавання та віднімання над елементами поля $GF(p^m)$.

Сутність винаходу пояснюється кресленнями.

На Фіг. 1 наведена структурна схема суматора елементів поля $GF(p^m)$, на Фіг. 2 - функціональна схема блока керування 15, на Фіг. 3 - функціональна схема порівняння кодів 11 для $(n-1)$-розрядних двійкових чисел, на Фіг. 4 - позначення на функціональних кресленнях регістрового запам'ятовувального пристрою 4 першого операнда, на Фіг. 5 - позначення на функціональних кресленнях регістрового запам'ятовувального пристрою 5 другого операнда, на Фіг. 6 - позначення на функціональних кресленнях регістрового запам'ятовувального пристрою 31 результата, на Фіг. 7 – приклад побудови індикатора кінцевого стану лічильника (ІКСЛ) для значення степеня т, яке дорівнює 10, на Фіг. 8 - змістова граф-схема алгоритма роботи суматора елементів поля $GF(p^m)$, на Фіг. 9 - закодована граф-схема алгоритма роботи суматора елементів поля $GF(p^m)$.

На Фіг. 1 наведена структурна схема суматора елементів поля $GF(p^m)$, де: 1 - n-розрядна шина кода першого операнда, 2 - n-розрядна шина кода другого операнда, 3 - n-розрядна шина кода модуля, 4 - регістровий запам'ятовувальний пристрій першого операнда з довільною вибіркою даних, який складається з m регістрів розрядність, яких дорівнює $n+1$, 5-регістровий запам'ятовувальний пристрій другого операнда з довільною вибіркою даних, який складається з m регістрів розрядність, яких дорівнює $n+1$, 6- $(n+1)$-розрядний регістр кода модуля, він є регістром з асинхронним записом, синхронною видачею кода та виходами на три стани, 7 - лічильник адрес, 8 - перша група елементів АБО, 9 - друга група елементів АБО, 10 - комбінаційний суматор, 11 - схема порівняння кодів для $(n-1)$-розрядних двійкових чисел, 12 - регістр проміжного результата є регістром з синхронним записом, асинхронною видачею кода та виходами на три стани, 13 - двовходовий логічний елемент АБО-НІ, 14 - індикатор кінцевого стану лічильника (ІКСЛ), 15 - блок керування (Фіг. 2), 16 - шина кода операції (ОР), 17- вихід $(n+1)$-го розряда регістра 12 проміжного результата, 18– вихід двовходового логічного елемента АБО-НІ 13, 19 – вихід схеми порівняння кодів 11, 20- вихід ІКС Л 14, 21- перший вихід блока керування 15, 22 - другий вихід блока керування 15, 23 - третій вихід блока керування 15, 24– четвертий вихід блока керування 15, 25– п'ятий вихід блока керування 15, 26 - шостий вихід блока керування 15, 27 - сьомий вихід блока керування 15, 28– восьмий вихід блока керування 15, 29 – дев'ятий вихід блока керування 15, 30 - група елементів І, 31 - регістровий запам'ятовувальний пристрій результата з довільною вибіркою даних, який складається з т регістрів розрядність, яких дорівнює n, 32 - n-розрядний вихід суматора елементів поля $GF(p^m)$.

Шина 1 кода першого операнда з'єднана з першими n інформаційними входами регістрового запам'ятовувального пристрою 4 першого операнда, шина 2 кода другого операнда з'єднана з першими n інформаційними входами регістрового запам'ятовувального пристрою 5 другого операнда, шина 3 кода модуля з'єднана з першими n входами регістра 6 модуля, вихід регістрового запам'ятовувального пристрою 4 першого операнда з'єднаний з другим входом групи елементів АБО 8, прямий вихід регістрового запам'ятовувального пристрою 5 другого операнда з'єднаний з другим входом другої групи елементів АБО 9, інверсний вихід регістрового запам'ятовувального пристрою 5 другого операнда з'єднаний з першим входом другої групи елементів АБО 9, прямий вихід регістра 6 модуля з'єднаний з четвертим входом другої групи елементів АБО 9, а перші $n-1$ розрядів прямого виходу регістра 6 модуля з'єднані з другим входом схеми порівняння кодів 11, інверсний вихід регістра 6 модуля з'єднаний з третім входом другої групи елементів АБО 9, виходи першої 8 та другої 9 групи елементів АБО з'єднані $(n+1)$-розрядними шинами з відповідними входами комбінаційного суматора 10, вихід комбінаційного суматора 10 з'єднаний $(n+1)$-розрядної шиною з входом регістра 12 проміжного результата, вихід регістра 12 проміжного результата з'єднаний від першої до $(n+1)$-ої шини з першим входом першої групи елементів АБО 8, від першої до n-ої шини - з першим входом групи елементів І 30, від першої до $(n-1)$-ої шини - з першим входом схеми порівняння кодів 11 (Фіг. 3), $(n+1)$-й розряд 17 регістра 12 проміжного результата з'єднаний з другим входом двовходового логічного елемента АБО-НІ 13 та з другим входом блока керування 15, n-й розряд регістра 12 проміжного результата з'єднаний з першим входом двовходового логічного елемента АБО-НІ 13, вихід 18 двовходового логічного елемента АБО-НІ 13 з'єднаний з третім входом блока керування 15, вихід 20 індикатора кінцевого стану лічильника 15 з'єднаний з п'ятим входом блока керування 15, перший вхід блока керування 15 з'єднаний з шиною 16 кода операції, четвертий вхід блока керування 15 з'єднаний з виходом 19 схеми порівняння кодів 11 (Фіг. 3), перший вихід 21 блока керування 15 з'єднаний з входом керування видачею кода з регістрового запам'ятовувального пристрою 4 першого операнда, другий вихід 22 блока керування 15 з'єднаний з входом керування видачею кода з регістрового запам'ятовувального пристрою 5 другого операнда, третій вихід 23 блока керування 15 з'єднаний з входом керування видачею інверсного кода з регістрового запам'ятовувального пристрою 5 другого опернада, четвертий вихід 24 блока керування 15 з'єднаний з входом керування видачею кода з регістра 6 модуля, п'ятий вихід 25 блока керування 15 з'єднаний з входом керування видачею інверсного кода з регістра 6 модуля, шостий вихід 26 блока керування 15 з'єднаний з керуючим входом прийому кода в регістр 12 проміжного результата, сьомий вихід 27 блока керування 15 з'єднаний з другим входом групи елементів 130 та входом керування прийому кода в регістровий запам'ятовувальний пристрій 31 результата, восьмий вихід 28 блока керування 15 з'єднаний з входом вхідного переноса комбінаційного суматора 10, дев'ятий вихід 29 блока керування 15 з'єднаний з синхровходом лічильника адрес 7, перші n розрядів виходa групи елементів І 30 з'єднані з інформаційним входом регістрового запам'ятовувального пристрою 31 результата, вихід 32 регістрового запам'ятовувального пристрою 31 результата є виходом пристрою.

На Фіг. 2 наведена функціональна схема блока керування 15, де: 16-однорозрядна шина кода операції, 17 - однорозрядна шина на яку подається результат виконання першої умови, а саме наявність одиниці в $(n+1)$-му розряді проміжного результата, 18 - однорозрядна шина на яку подається результат виконання другої умови, а саме наявність нулів в $(n+1)$-му та n-му розряді проміжного результата, 19 - однорозрядна шина на яку подається результат виконання третьої умови, а саме вихід схеми порівняння кодів 11, 20 – однорозрядна шина на яку подається результат виконання четвертої умови, а саме вихід ІКСЛ 14, 33-35- одновходові логічні елементи І-НІ, 36 - трьохвходовий логічний елементи І, 37 - 42 - двовходові логічні елементи І, 43 - трьохвходовий логічний елементи І, 44 - 47 - двовходові логічні елементи І, 48 – семивходовий логічний елемент АБО, 49 -шестивходовий логічний елемент АБО, 50 - п'ятивходовий логічний елемент АБО, 51- шестивходовий логічний елемент АБО, 52-55- D-тригери, інверсні S-входи D-тригерів є входами встановлення в одиницю значень D-тригерів, інверсні R-входи D-тригерів є входами встановлення в нуль значень D-тригерів, С - синхровхід D-тригерів, D - інформаційні входи D-тригерів, 56 - дешифратор на чотири входи, z_0-z_{10} - перші одинадцять виходів дешифратора, 57 - трьохвходовий логічний елементи АБО, 58 - 60 -двовходові логічні елементи АБО, 21 - однорозрядна шина, яка є першим виходом блока керування 15, 22 - однорозрядна шина, яке є другим виходом блока керування 15, 23- однорозрядна шина, яка є третім виходом блока керування 15, 24- однорозрядна шина, яка четвертим виходом блока керування 15, 25- однорозрядна шина, яка є п'ятим виходом блока керування 15, 26- однорозрядна шина, яка є шостим виходом блока керування 15, 27- однорозрядна шина, яка є сьомим виходом блока керування 15, 28- однорозрядна шина, яка є восьмим виходом блока керування 15, 29- однорозрядна шина, яка є дев'ятим виходом блока керування 15.

До входу логічного елемента І-НІ 33 п'єднана шина з сигналом першої умови 17, до входу логічного елемента І-НІ 34 під'єднана шина третьої умови 19, до входу логічного елемента І-НІ 35 під'єднана шина другої умови 18, вихід логічного елемента І-НІ 33 з'єднано з другим входом логічного елемента І 36, перший вхід логічного елемента І 36 з'єднано з другим виходом (z_2) дешифратора 56, до третього входа логічного елемента 136 під'єднано шину другої умови 18, перший вхід логі-

чного елемента 137 з'єднано з третім виходом (z_3) дешифратора 56, другий вхід логічного елемента І 37 під'єднано до шини третьої умови 19, перший вхід логічного елемента І 38 з'єднано з виходом логічного елемента І-НІ 33, другий вхід логічного елемента 138 з'єднано з шостим виходом (z_6) дешифратора 56, перший вхід логічного елемента І 39 з'єднано з нульовим виходом (z_0) дешифратора 56, другий вхід логічного елемента І 39 під'єднано до шини 16 кода операції, перший вхід логічного елемента І 40 з'єднано з другим виходом (z_2) дешифратора 56, другий вхід логічного елемента І 40 під'єднано до шини 17 першої умови, перший вхід логічного елемента І 41 з'єднано з третім виходом (z_3) дешифратора 56, другий вхід логічного елемента І 41 з'єднано з виходом логічного елемента І-НІ 34, перший вхід логічного елемента І 42 з'єднано з шостим виходом (z_6) дешифратора 56, другий вхід логічного елемента І 42 під'єднано до шини 17 першої умови, перший вхід логічного елемента 143 з'єднано з другим виходом (z_2) дешифратора 56, другий вхід логічного елемента 143 з'єднано з виходом логічного елемента І-НІ 33, третій вхід логічного елемента І 43 з'єднано з виходом логічного елемента І-НІ 35, перший вхід логічного елемента І 44 під'єднано до шини 20 четвертої умови, другий вхід логічного елемента І 44 з'єднано з дев'ятим виходом (z_9) дешифратора 56, перший вхід логічного елемента І 45 під'єднано до шини 16 кода операції, другий вхід логічного елемента І 45 з'єднано з десятим виходом (z_{10}) дешифратора 56, перший вхід логічного елемента І 46 з'єднано з другим виходом (z_2) дешифратора 56, другий вхід логічного елемента І 46 з'єднано з виходом логічного елемента І-НІ 33, перший вхід логічного елемента І 47 з'єднано з третім виходом (z_3) дешифратора 56, другий вхід логічного елемента І 47 під'єднано до шини 19 третьої умови, перший вхід логічного елемента АБО 48 з'єднано з четвертим виходом (z_4) дешифратора 56, другий вхід логічного елемента АБО 48 з'єднано з виходом логічного елемента 136, третій вхід логічного елемента АБО 48 з'єднано з сьомим виходом (z_7) дешифратора 56, четвертий вхід логічного елемента АБО 48 з'єднано з восьмим виходом (z_8) дешифратора 56, п'ятий вхід логічного елемента АБО 48 з'єднано з виходом логічного елемента І 37, шостий вхід логічного елемента АБО 48 з'єднано з виходом логічного елемента І 38, сьомий вхід логічного елемента АБО 48 з'єднано з виходом логічного елемента 144, перший вхід логічного елемента АБО 49 з'єднано з виходом логічного елемента І 39, другий вхід логічного елемента АБО 49 з'єднано з виходом логічного елемента 140, третій вхід логічного елемента АБО 49 з'єднано з виходом логічного елемента 141, четвертий вхід логічного елемента АБО 49 з'єднано з виходом логічного елемента І 42, п'ятий вхід логічного елемента АБО 49 з'єднано з виходом логічного елемента І 45, шостий вхід логічного елемента АБО 49 з'єднано з п'ятим виходом (z_5) дешифратора 56, перший вхід логічного елемента АБО 50 з'єднано з першим виходом (z_1) дешифратора 56, другий вхід логічного елемента АБО 50 з'єднано з виходом логічного елемента І 42, третій вхід логічного елемента АБО 50 з'єднано з п'ятим виходом (z_5) дешифратора 56, четвертий вхід логічного елемента АБО 50 з'єднано з виходом логічного елемента І 43, п'ятий вхід логічного елемента АБО 50 з'єднано з виходом логічного елемента 144, перший вхід логічного елемента АБО 51 з'єднано з нульовим виходом (z_0) дешифратора 56, другий вхід логічного елемента АБО 51 з'єднано з восьмим виходом (z_8) дешифратора 56, третій вхід логічного елемента АБО 51 з'єднано з десятим виходом (Z_{10}) дешифратора 56, четвертий вхід логічного елемента АБО 51 з'єднано з шостим виходом (z_6) дешифратора 56, п'ятий вхід логічного елемента АБО 51 з'єднано з виходом логічного елемента І 46, шостий вхід логічного елемента АБО 51 з'єднано з виходом логічного елемента І 47, вихід логічного елемента АБО 48 з'єднано з D-входом третього D-тригера 55, вихід логічного елемента АБО 49 з'єднано з D-входом другого D-тригера 54, вихід логічного елемента АБО 50 з'єднано з D-входом першого D-тригера 53, вихід логічного елемента АБО 51 з'єднано з D-входом нульового D-тригера 52, прямі виходи D-тригерів (Q_0, Q_1, Q_2, Q_3) під'єднані до відповідних входів дешифратора 56, перший вхід логічного елемента АБО 57 з'єднано з восьмим виходом (z_8) дешифратора 56, другий вхід логічного елемента АБО 57 з'єднано з другим виходом (z_2) дешифратора 56, третій вхід логічного елемента АБО 57 з'єднано з шостим виходом (z_6) дешифратора 56, вихід 26 логічного елемента АБО 57 є шостим виходом (y_6) блока керування 15, перший вхід логічного елемента АБО 58 з'єднано з першим виходом (z_5) дешифратора 56, другий вхід логічного елемента АБО 58 з'єднано з п'ятим виходом (z_5) дешифратора 56, вихід 21 логічного елемента АБО 58 є першим виходом (y_1) блока керування 15, перший вхід логічного елемента АБО 59 з'єднано з третім виходом (z_3) дешифратора 56, другий вхід логічного елемента АБО 59 з'єднано з сьомим виходом (z_7) дешифратора 56, вихід 24 логічного елемента АБО 59 є четвертим виходом (y_4) блока керування 15, перший вхід логічного елемента АБО 60 з'єднано з четвертим виходом (z_4) дешифратора 56, другий вхід логічного елемента АБО 50 з'єднано з п'ятим виходом (z_5) дешифратора 56, вихід 28 логічного елемента АБО 60 є восьмим виходом (y_8) блока керування 15, перший вихід (z_1) дешифратора 56 є другим виходом 22 (y_2) блока керування 15, четвертий вихід (z_4) дешифратора 56 є п'ятим виходом 25 (y_5) блока керування 15, п'ятий вихід (z_5) дешифратора 56 є третім виходом 23 (уз) блока керування 15, дев'ятий вихід (z_9) дешифратора 56 є сьомим виходом 27 (y_7) блока керування 15, десятий вихід (z_{10}) дешифратора 56 є дев'ятим виходом 29 (y_9) блока керування 15.

На Фіг. 3 наведена функціональна схема порівняння кодів 11 призначена для порівняння $(n-1)$-розрядних двійкових чисел. Схема порівняння кодів 11 складається з $n-1$ двовходового логічного елемента І-НІ (65.1 - 65. $n-2$, 66. $(n-1)$), одного трьохвходового логічного елемента І-НІ (66. $n-2$), одного чотирьохвходового логічного елемента І-НІ (66. $n-3$), ..., одного $(n-2)$-входового логічного

елемента І-НІ (66.3), двох $(n-1)$-входових логічних елементів І-НІ (66.2, 67) і одного n-входового логічного елемента І-НІ (66.1). Вхід 62 є входом прямого кода проміжного результата, 62.і означає, що на цей вхід подається і-ий розряд кода з регістра 12 проміжного результата, вхід 61 є інверсним значенням кода модуля, 61.і означає, що на цей вхід подається і-ий розряд інверсного значення кода модуля, вхід 63 є входом прямого кода модуля, 63.і означає, що на цей вхід подається і-ий розряд значення кода модуля, вхід 64 є інверсним значенням кода з регістра 12 проміжного результата, 64.і означає, що на цей вхід подається і-ий розряд інверсного значення проміжного результата. Вихід 19 є виходом схеми порівняння кодів 11.

На Фіг. 4 наведено позначення на функціональних кресленнях регістрового запам'ятовувального пристрою ($РЗП_1$) 4 першого операнда. Даний РЗП має організацію пам'яті $m \times n+1$, тобто m регістрів з довільною вибіркою даних по $n+1$ розрядів кожний, де DI_1 (Data Input) - вхід даних, A (Adress) - адресний вхід, RD - вхід керування видачею даних, DO_1 (Data Output) - вихід даних. Адресний вхід (А) з'єднано шиною розрядністю $\log_2 m$ з виходом лічильника адрес 7. До входу даних (DI) під'єднано n -розрядну шину 1 кода першого операнда, вхід керування видачею даних (RD) з'єднано однорозрядною шиною з першим виходом 21 блока керування 15, вихід даних (DO_1) з'єднано $(n+1)$-розрядною шиною з другим входом першої групи елементів АБО 8.

На Фіг. 5 наведено позначення на функціональних кресленнях регістрового запам'ятовувального пристрою ($РЗП_2$) 5 другого операнда. Даний РЗП має організацію пам'яті $m \times n+1$ тобто m регістрів з довільною вибіркою даних по $n+1$ розрядів, де DI (Data Input) - вхід даних, A (Adress) - адресний вхід, RD_1 - вхід керування видачею прямого коду даних, RD_2 - вхід керування видачею інверсного коду даних, DO_2 (Data Output) - вихід, на який видається прямий код даних, DO_2 (Data Output) - вихід, на який видається інверсний код даних. Адресний вхід (А) з'єднано шиною розрядністю $\log_2 m$ з виходом лічильника адрес 7. До входу даних (DI) під'єднано n-розрядну шину кода другого операнда, вхід керування видачею прямого кода даних (RD_1) з'єднано однорозрядною шиною з другим виходом 22 блока керування 15, вхід керування видачею інверсного кода даних (RD_2) з'єднано однорозрядною шиною з третім виходом 23 блока керування 15, вихід прямого кода даних (DO_2) з'єднано $(n+1)$-розрядною шиною з другим входом другої групи елементів АБО 9, вихід інверсногго кода даних (DO_3) з'єднано $(n+1)$-розрядною шиною з першим входом другої групи елементів АБО 9.

На Фіг. 6 наведено позначення на функціональних кресленнях регістрового запам'ятовувального пристрою ($РЗП_3$) 31 результата. Даний РЗП має організацію пам'яті $m \times n$, тобто m регістрів з довільною вибіркою даних по п розрядів, де DI (Data Input) - вхід даних, A (Adress) - адресний вхід, WR - вхід керування прийомом даних, DO_4 (Data Output) - вихід даних. Адресний вхід (А) з'єднано шиною розрядністю $\log_2 m$ з виходом лічильника адрес 7. Вхід даних (DI) з'єднано n-розрядною шиною з виходом групи елементів І 30, вхід керування прийомом даних (WR) з'єднано однорозрядною шиною з сьомим виходом 27 блока керування 15, до виходу даних (DO) під'єднано n-розрядну шину, яка є виходом пристрою 32.

На Фіг. 7 наведено приклад побудови індикатора кінцевого стану лічильника (ІКСЛ) 14 для значення степеня $m-1$, яке дорівнює 9. Adr.O-Adr3 це відповідні розряди виходу лічильника адрес 7. Коли на виході лічильника адрес 7 отримуємо значення степеня $m-1$, яке дорівнює 9, тоІКСЛ видає на вихід 20 одиничний сигнал. Вихід 20 ІКСЛ з'єднано з п'ятим входом блока керування 15. ІКСЛ по суті є логічним елементом І на $\log_2 m$ входів, деякі з яких є інверсними. Інверсними є ті входи ІКСЛ, відповідні розряди у двійковому записі числа $m-1$, яких є нульовими. Тобто для $m-1=9$ двійкове подання буде 1001_2, отже, щоб видати на вихід 20 одиничний сигнал потрібен ІКСЛ на чотири входи (Adr.0, Adr.I, Adr.2, Adr.3), в якому нульовий і третій вхід є інверсними. Зауважемо, що в загальному випадку ІКСЛ може бути схемою порівняння двійкових чисел розрядності $\log_2 m$, перший вхід якої буде з'єднано з виходом лічильника адрес 7, а на другий вхід буде подаватися константа, яка дорівнює $m-1$. Але введення додаткової схеми порівняння кодів несе за собою значні апаратні витрати, тому в якості ІКСЛ пропонується використовувати логічний елемент І з прямими та інверсними входами, кількість, яких дорівнює $\log_2 m$.

На Фіг. 8 наведена змістова граф-схема алгоритма роботи суматора, яка містить вершини Початок і Кінець, операторні вершини (прямокутники) та умовні вершини (ромби). Розглянемо скорочення, які використані на цій граф-схемі алгоритма: ОР - код операції, ADD - операція додавання, SUB -операція віднімання, $ВК_{РЗП1}$ - видача кода з регістрового запам'ятовувального пристрою 4 першого операнда, $ВК_{РЗП2}$ - видача прямого кода з регістрового запам'ятовувального пристрою 5 другого операнда, $ВІК_{РЗП2}$ - видача інверсного кода з регістрового запам'ятовувального пристрою 5 другого операнда, $ПК_{пр}$ - прийом кода в регістр 12 проміжного результата, α - перша умова, β - друга умова, $ВК_Р$ - видача кода з регістра 6, γ - третя умова, δ - четверта умова, $ВІК_Р$ - видача інверсного кода з регістра 6, "+1"- сигнал вхідного переноса комбінаційного суматора 10, $ВК_{Рез}$ - видача результата на вхід регістрового запам'ятовувального пристрою 31 та сигнал запису отриманого результата у даний РЗП, $CLK_{АС}$ -сигнал інкрементації лічильника адрес 7.

На Фіг. 9 наведена закодована граф-схема алгоритма роботи суматора, де сигнал $ВК_{РЗП1}$ позначено як y_1, $ВК_{РЗП2}$ - y_2, $ВІК_{РЗП2}$ - y_3, $ВК_р$- y_4, $ВІК_р$- y_5, $ПК_{пр}$- y_6, $ВК_{Рез}$- y_7, «+1»- y_8, $CLK_{АС}$- y_9, а операторні вершини позначено від z_0 до z_{10} відповідно.

Розрізняють два види скінченних полів:

• поле, кількість елементів якого є простим числом. Таке поле позначають GF(p), де p-просте число. Операції в такому полі виконують за модулем простого числа p;

• поле, кількість елементів якого є степенем простого числа. Таке поле позначають GF(p^m), де p - просте число, а m- величина степеня. Операції над елементами такого поля виконують за модулем незвідного многочлена степеня m.

Коефіцієнти незвідного многочлена степеня т належать множині {0,1,2,...,p}. Операції над коефіцієнтами виконують за модулем простого числа p.

GF(p^m) є розширенням поля GF(p). Величину p називають характеристикою поля.

Елементи поля GF(p^m) можна подавати у десятковому вигляді, у вигляді степеня примітивного елемента поля, у вигляді многочлена. Ці подання є ізоморфними. У десятковому вигляді елементами GF(p^m) є числа {0,1, 2,..., p^m-1}. Але для підсумовування зручно користуватись многочленним поданням елементів, тому надалі будемо використовувати многочленне подання.

Наприклад, у полі GF(23^4) при незвідному многочлені x^4+19x^3+1 елементу 157912 (десяткове подання) відповідає α^{73} (степеневе подання) та $12x^3+22x^3+11x^2+17$ (многочленне подання), де α - примітивний елемент поля. Для цього поля $p=23, m=4$.

Суматор елементів поля GF(p^m) забезпечує виконання двох операцій:

• додавання;

• віднімання.

Для виконання цих операцій над многочленним поданням елементів поля GF(p^m) необхідно виконати почергове підсумовування відповідних коефіцієнтів операндів за модулем простого числа p.

$$A(x)=\sum_{i=0}^{m-1}A_i x^i$$

Нехай - перший операнд, $B(x)=\sum_{i=0}^{m-1}B_i x^i$ $C(x)=\sum_{i=0}^{m-1}C_i x^i$ - другий операнд, - результат виконання операції, а p - модуль за яким виконуються операції над коефіцієнтами многочленного подання елементів поля.

Очевидно, що:

$$C(x)=A(x)\pm B(x)=\sum_{i=0}^{m-1}A_i x^i \pm \sum_{i=0}^{m-1}B_i x^i=\sum_{i=0}^{m-1}(A_i\pm B_i)x^i=\sum_{i=0}^{m-1}C_i x^i$$

.

Розглянемо, як виконуються операції для одного коефіцієнта.

Коефіцієнти A_i, B_i, C_i є елементами поля GF(p), тобто $A_i, B_i, C_i \in \{0,1,2,...,p-1\}$.

Операцію віднімання $C_i=(A_i-B_i)\,\mathrm{mod}\,p$ реалізуємо як

$$C_i=(A_i+B_{i\,пр})\,\mathrm{mod}\,p,$$

де $B_{i\,пр}$ - елемент поля GF(p), протилежний до елемента B_i, $B_{i\,пр}=p-B_i$. Зрозуміло, що $B_i+B_{i\,пр}=p$.

Вираз $B_{i\,пр}=p-B_i$ реалізуємо як $B_{i\,пр}=p+B_{i\,доп}$, де $B_{i\,доп}$ - доповнення величини B_i до 2^n (доповняльний код величини B_i), тобто $B_{i\,пр}=p-B_i=p+(2^n-B_i)=p+\bar{B}_i+1$, де $\bar{B}_i$ - інверсний код величини B_i.

Тоді $C_i=(A_i-B_i)\,\mathrm{mod}\,p=(A_i+p+\bar{B}_i+1)\,\mathrm{mod}\,p$.

Отже, величина C_i дорівнює:

$$C_i=\begin{cases}(A_i+B_i)\,\mathrm{mod}\,p, & \text{якщо } OP=0;\\ \left(A_i+\bar{B}_i+1\right)\mathrm{mod}\,p, & \text{якщо } OP=1;\end{cases}$$

Схема порівняння кодів 11 (Фіг. 3) призначена для порівняння $n-1$ молодших розрядів результата підсумовування коефіцієнтів $C_i=(A_i\pm B_i)$, (який з виходу регістра 12 проміжного результата поступає на перші входи схеми порівняння кодів 11) з $n-1$ молодшими розрядами модуля, за яким виконуються операції над коефіцієнтами многочленного подання елементів поля. На виході схеми порівняння кодів 11 (Фіг. 3) з'являється сигнал, якщо $n-1$ молодших розрядів результата підсумовування коефіцієнтів менше за $n-1$ молодших розрядів модуля.

Порівняно з прототипом [3], кількість входів схеми порівняння кодів 11 (Фіг. 3) зменшена з $(n+1)$-го до $(n-1)$-го, що дає можливість зменшити апаратні витрати на: два двовходових елемента І-НІ, один $(n+2)$-входовий елемент І-НІ і один $(n+1)$-входовий елемент І-НІ, а також зменшити кількість входів одного елемента І-НІ з $n+1$ до $n-1$. Це стає зрозумілим, якщо докладніше розглянути схему порівняння кодів 11 (Фіг. 3).

У загальному випадку схема порівняння кодів реалізує такий вираз:

$$H_M(C_i,p)=\overline{c_n p_n}\bigvee_{j=n-1}^{1}\bar{c}_j p_j \,\&\, \bigvee_{k=n}^{j+1}\left(\bar{c}_k\vee p_k\right),$$

де під c_j та c_k мається на увазі j-ий та k-ий двійковий розряд і-го коефіцієнта результата виконання операції відповідно; p_j та p_k -j-ий та k-ий двійковий розряд значення модуля p відповідно.

Представимо цю формулу у вигляді придатному для схемотехнічної реалізації на елементах І-НІ:

$$H_M(C_i,p)=\overline{\overline{c_n p_n}\bigvee_{j=n-1}^{1}\bar{c}_j p_j \,\&\, \bigvee_{k=n}^{j+1}\left(\bar{c}_k\vee p_k\right)}=\overline{\overline{c_n p_n}\,\&\bigvee_{j=n-1}^{1}\bar{c}_j p_j \,\&\, \bigvee_{k=n}^{j+1}\overline{c_k p_k}}.$$

Якщо взяти схему порівняння кодів для $(n-1)$ -розрядних чисел (Фіг. 3), то формула набуває вигляду:

$$H_M(C_i,p) = \overline{\overline{c_{n-1}}\,p_n \;\&_{j=n-2}^{1}\; \overline{c_j}\,p_j \;\&_{k=n-1}^{j+1}\; \overline{c_k}\,\overline{p_k}}.$$

Блок керування 15 (Фіг. 2) побудований, як автомат Мура. Процес синтезу блока керування 15 (Фіг. 2) починається з побудови змістової (Фіг. 8) та закодованої (Фіг. 9) граф-схеми алгоритма роботи суматора елементів поля GF(p^m).

По закодованій граф-схемі алгоритма (Фіг. 9) будується структурна таблиця переходів автомата Мура (табл. 1).

Таблиця

Вихідний стан	Код вихідного стану				Керуючі сигнали	Стан переходу	Код стану переходу				Логічні умови					Функції збудження			
	$Q_3(t)$	$Q_2(t)$	$Q_1(t)$	$Q_0(t)$			$Q_3(t+1)$	$Q_2(t+1)$	$Q_1(t+1)$	$Q_0(t+1)$	ОР	α	β	γ	δ	D_3	D_2	D_1	D_0
z_0	0	0	0	0		z_1	0	0	0	1	0	*	*	*	*	0	0	0	1
						z_5	0	1	0	1	1	*	*	*	*	0	1	0	1
z_1	0	0	0	1	y_1, y_2	z_2	0	0	1	0	*	*	*		*	0	0	1	0
z_2	0	0	1	0	y_6	z_3	0	0	1	1	*	0	0		*	0	0	1	1
						z_4	0	1	0	0	*	1	*	*	*	0	1	0	0
						z_9	1	0	0	1	*	0	1			1	0	0	1
z_3	0	0	1	1	y_4	z_4	0	1	0	0	*	*	*	0	*	0	1	0	0
						z_9	1	0	0	1	*	*		1		1	0	0	1
z_4	0	1	0	0	y_5, y_8	z_8	1	0	0	0	*	*	*	*	*	1	0	0	0
z_5	0	1	0	1	y_1, y_3, y_8	z_6	0	1	1	0	*	*	*	*		0	1	1	0
z_6	0	1	1	0	y_6	z_7	0	1	1	1	*	1	*	*	*	0	1	1	1
						z_9	1	0	0	1	*	0	*	*	*	1	0	0	1
z_7	0	1	1	1	y_4	z_8	1	0	0	0	*	*	*	*	*	1	0	0	0
z_8	1	0	0	0	y_6	z_9	1	0	0	1	*	*		*	*	1	0	0	1
z_9	1	0	0	1	y_7	z_0	0	0	0	0	*	*	*	*	0	0	0	0	0
						z_{10}	1	0	1	0	*	*	*	*	1	1	0	1	0
z_{10}	1	0	1	0	y_9	z_1	0	0	0	1	0	*			*	0	0	0	1
						z_5	0	1	0	1	1	*	*	*	*	0	1	0	1

За побудованою структурною таблицею переходів автомата Мура визначаємо функції збудження D-тригерів:

$$D_3 = z_2\overline{\alpha\beta} \vee z_3\gamma \vee z_6\overline{\alpha} \vee z_9\delta \vee z_4 \vee z_7 \vee z_8;$$

$$D_2 = z_0 OP \vee z_2\alpha \vee z_3\overline{\gamma} \vee z_6\alpha \vee z_{10}OP \vee z_5;$$

$$D_1 = z_2\overline{\alpha\beta} \vee z_6\alpha \vee z_9\delta \vee z_1 \vee z_5;$$

$$D_0 = z_2\overline{\alpha} \vee z_3\gamma \vee z_0 \vee z_6 \vee z_8 \vee z_{10};$$

В залежності від станів автомата Мура функції виходів блока керування 15 набувають такого вигляду:

$$y_1 = z_1 \vee z_5; y_2 = z_1; y_3 = z_5; y_4 = z_3 \vee z_7; y_5 = z_4; y_6 = z_2 \vee z_6 \vee z_8; y_7 = z_9; y_8 = z_4 \vee z_5; y_9 = z_{10}.$$

За наведеними функціями збудження D-тригерів та функціями виходів блока керування 15 легко будуємо функціональну схему блока керування 15 (Фіг. 2).

Розглянемо як функціонує блок керування 15 (Фіг. 2). Блок керування 15 спочатку знаходиться в стані z_0 (початковий стан), далі, в залежності від вхідних сигналів, за граф-схемою алгоритма (Фіг. 8 та Фіг. 9) він переходить з одного стану в інший і формує на своїх виходах відповідні сигнали керування. В кінці алгоритма блок керування 15 повертається в початковий стан z_0.

Розглянемо, як працює суматор елементів поля GF(p^m). Логіку роботи суматора елементів поля GF(p^m), яка представлена змістовою (Фіг. 8) та закодованою (Фіг. 9) граф-схемою алгоритма роботи забезпечує блок керування 15. Значення вхідних операндів та значення модуля надходять відповідно на шину 1 кода першого операнда, шину 2 кода другого операнда та шину 3 кода модуля і записуються у відповідні РЗП та регістр. Регістровий запам'ятовувальний пристрій 4 першого операнда, регістровий запам'ятовувальний пристрій 5 другого операнда є РЗП з довільним доступом. Кожен операнд у многочленному поданні представлений m коефіцієнтами від нульового до $(m-1)$-го, адреса коефіцієнта у певному РЗП буде дорівнювати його вазі в даному елементі поля GF(p^m) відповідно від 0 до $m-1$. Регістр 6 модуля є регістром з асинхронним записом, тому після надходження значення на шину воно буде відразу записане у регістр. Лічильник адрес 7 на початку роботи встановлений в нульовий стан. На вхід 16 блока керування 15 надходить значення кода операції (ОР).

Далі блок керування 15 аналізує код операції:

1. Якщо ОР - 0, то треба виконувати операцію додавання двох операндів. Блок керування 15 формує сигнали 21 та 22 видачі прямого кода першого коефіцієнта з РЗП першого 4 та другого 5 операнда. Перший коефіцієнт першого операнда через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, перший

коефіцієнт другого операнда через другу 9 групу елементів АБО надходить на другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах. З виходу комбінаційного суматора 10 результат потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 прийому кода в регістр 12 проміжного результата. Далі блок керування 15 аналізує дві умови (α та β), де α дорівнює одиниці коли старший $(n+1)$-ий розряд регістра 12 проміжного результата дорівнює 1, а β дорівнює одиниці коли два старших, $(n+1)$-ий та n-й, розряди регістра 12 проміжного результата дорівнюють 0. Потім в залежності від значення умов α та β блок керування 15 формує певні сигнали, а саме:

• Якщо умова α дорівнює 0, а умова β дорівнює 1, то отримано результат додавання коефіцієнтів, який не вимагає корекції, оскільки він менше за значення модуля. В цьому випадку блок керування 15 формує сигнал 27 відкривання групи елементів 130, на другому вході яких знаходиться значення суми двох коефіцієнтів. Через групу елементів 130 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується у відповідний регістр (згідно поточного стану лічильника адрес 7) даного РЗП.

• Якщо умова α дорівнює 0 і умова β дорівнює 0, то без залучення схеми порівняння кодів 11 не можна визначити чи є отриманий результат меншим від значення модуля, тому блок керуваня 15 формує сигнал 24 видачі прямого кода з регістра 6 модуля. Перші $n-1$ розрядів значення модуля надходять на другий вхід схеми порівняння кодів 11, а на першому вході вже присутні перші $n-1$ розрядів отриманого результата додавання коефіцієнтів. Далі схема порівняння кодів 11 формує на виході 19 значення третьої умови γ:

Якщо $\gamma=1$, то це означає, що отриманий результат не вимагає корекції, оскільки він менше за значення модуля, тоді блок керування 15 формує сигнал 27 відкривання групи елементів І 30, на другому вході яких знаходиться значення суми двох коефіцієнтів. Через групу елементів І 30 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується у відповідний регістр (згідно поточного стану лічильника адрес 7) даного РЗП.

Якщо $\gamma=0$, то це означає, що отриманий результат вимагає корекції, оскільки він дорівнює або більше за значення модуля, тоді блок керування 15 формує сигнал 25 видачі інверсного кода з регістра 6 модуля і сигнал 28 вхідного переноса комбінаційного суматора 10. Проміжний результат з виходів регістра 12 проміжного результата через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, інверсний код модуля через другу 9 групу елементів АБО надходить на другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах з урахуванням вхідного переноса. З виходу комбінаційного суматора 10 результат потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 прийому кода в регістр 12 проміжного результата. Далі блок керування 15 формує сигнал 27 відкривання групи елементів 130, на другому вході яких знаходиться значення суми двох коефіцієнтів. З виходів групи елементів 130 результат потрапляє на вхід регістрового

запам'ятовувального пристрою 31 і записується у відповідний регістр (згідно поточного стану лічильника адрес 7) даного РЗП.

• Якщо умова α дорівнює 1, то отримано результат, який вимагає корекції, оскільки він більше за значення модуля, тоді блок керування 15 формує сигнал 25 видачі інверсного кода з регістра 6 модуля і сигнал 28 вхідного переноса комбінаційного суматора 10. Проміжний результат з виходів регістра 12 проміжного результата через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, інверсний код модуля через другу 9 групу елементів АБО надходить на другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах з урахуванням вхідного переноса. З виходу комбінаційного суматора 10 результат потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 прийому кода в регістр 12 проміжного результата. Далі блок керування 15 формує сигнал 27 відкривання групи елементів І 30, на другому вході яких знаходиться значення суми двох коефіцієнтів. З виходів групи елементів І 30 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується у відповідний регістр (згідно поточного стану лічильника адрес 7) даного РЗП.

Далі блок керування 15 аналізує значення четвертої умови δ, а саме: якщо $\delta=0$, то це означає, що значення лічильника адрес 7 менше за значення степеня $m-1$ і потрібно переходити до наступного коефіцієнта операндів. В цьому випадку блок керування 15 видає сигнал 29 (CLK_{AC}) для інкрементації лічильника адрес 7, потім виконуємо операцію додавання для чергових коефіцієнтів у відповідності до сформованого лічильником адрес значення адреси; якщо $\delta=1$, то це означає, що значення лічильника адрес 7 дорівнює значенню степеня $m-1$ і ми в регістровому запам'ятовувальному пристрої 31 отримали результат додавання двох елементів поля $GF(p^m)$.

2. Якщо ОР=1, то треба виконувати операцію віднімання двох операндів. Блок керування 15 формує сигнали 21 видачі прямого кода першого коефіцієнта з РЗП першого 4 операнда та сигнал 23 видачі інверсного кода першого коефіцієнта з РЗП другого 5 операнда, а також сигнал 28 вхідного переноса комбінаційного суматора 10. Перший коефіцієнт першого операнда через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, перший коефіцієнт другого

операнда через другу 9 групу елементів АБО надходить на другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах з урахуванням вхідного переноса. З виходу комбінаційного суматора 10 результат потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 прийому кода в регістр 12 проміжного результата. Далі блок керування 15 аналізує значення умови α, де α дорівнює одиниці коли старший $(n+1)$-ий розряд регістра 12 проміжного результата дорівнює 1:

• Якщо умова α дорівнює 0, то отримано результат, який не вимагає корекції, оскільки він менше за значення модуля. Блок керування 15 формує сигнал 27 відкривання групи елементів 130, на другому вході яких знаходиться значення різниці двох коефіцієнтів. Через групу елементів 130 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується у відповідний регістр (згідно поточного стану лічильника адрес 7) даного РЗП.

• Якщо умова α дорівнює 1, то отримано результат, який вимагає корекції, оскільки значення першого операнда було менше за значення другого ми отримали «від'ємний» результат. Для корекції результата необхідно до нього додати значення модуля. Блок керування 15 формує сигнал 24 видачі прямого кода з регістра 6 модуля. Проміжний результат з виходів регістра 12 проміжного результата через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, прямий код модуля через другу 9 групу елементів АБО надходить на другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах. З виходу комбінаційного суматора 10 результат потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 прийому кода в регістр 12 проміжного результата. Далі блок керування 15 формує сигнал 27 відкривання групи елементів 130, на другому вході яких знаходиться значення різниці двох операндів. З виходів групи елементів І 30 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується у відповідний регістр (згідно поточного стану лічильника адрес 7) даного РЗП.

Далі блок керування 15 аналізує значення четвертої умови δ, а саме: якщо $\delta = 0$, то це означає, що значення лічильника адрес 7 менше за значення степеня $m-1$ потрібно виконувати операцію віднімання над наступними коефіцієнтами операндів. В цьому випадку блок керування 15 видає сигнал 29 (CLK_{AC}) для інкрементації лічильника адрес 7, потім виконуємо операцію відніманя для чергових коефіцієнтів у відповідності до сформованого лічильником адрес значення адреси; якщо $\delta = 1$, то це означає, що значення лічильника адрес 7 дорівнює значенню степеня $m-1$ і ми в регістровому запам'ятовувальному пристрої 31 отримали результат віднімання двох елементів поля $GF(p^m)$.

Наведемо приклади роботи суматора елементів поля $GF(p^m)$ при виконанні операцій додавання та віднімання для модуля $p = 23_{10} = 10111_2$ та степеня $m = 4_{10} = 100_2$, тобто приклади роботи суматора елементів поля $GF(23^4)$.

Приклад 1

Нехай є два елементи поля $GF(23^4)$: A = 102503, B = 79072.

Елементам A і B відповідає таке многочленне подання: $A(x)=8x^3+9x^2+17x+15$, $B(x)=6x^3+11x^2+10x+21$.

Виконаємо операцію додавання (ОР = 0): A + B.

В $РЗП_1$ та $РЗП_2$ коефіцієнти многочленного подання будуть розміщені таким чином, як показано в табл. 2 (елементі) та табл. 3 (елементВ). Жирним в даних таблицях позначено $(n+1)$-і розряди, в даному прикладі це п'яті розряди, першого та другого операндів, які беруть участь у визначенні знаку проміжного результату, тобто проміжний результат є додатним чи від'ємним.

Таблиця 2

Адреса	Значення
00	$15_{10} = 001111_2$
01	$17_{10} = 010001_2$
10	$9_{10} = 001001_2$
11	$8_{10} = 001000_2$

Таблиця 3

Адреса	Значення
00	$21_{10} = 010101_2$
01	$10_{10} = 001010_2$
10	11,o = 001011_2
11	$6_{10} = 000110_2$

На вхід 16 блока керування 15 надходить значення кода операції (ОР).

Код операції дорівнює 0, отже треба виконувати операцію додавання двох операндів. Лічильник адрес 7 встановлений в нульовий стан. Блок керування 15 формує сигнали 21 (y_1, $ВК_{РЗП1}$) та 22 (y_2, $ВК_{РЗП2}$) видачі прямого кода коефіцієнтів (A_0 та B_0), які знаходяться за нульовою адресою в РЗП першого та другого операнда. Зчитаний коефіцієнт першого операнда ($A_0 = 15_{10} = 001111_2$) через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, зчитаний коефіцієнт другого операнда ($B_0 = 21_{10} = 010101_2$) через другу 9 групу елементів АБО надходить на другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах (001111 та 010101). З виходу комбінаційного суматора 10 результат $C_0 = 100100$ потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 (y_6,

$ПК_{пр}$) прийому кода в регістр 12 проміжного результата. Далі значення п'ятого розряда (умова $\alpha = c_5 = 1$) регістра 12 проміжного результата поступає на відповідний вхід блока керування 15. Рівність одиниці старшого розряду отриманого результату означає, що потрібно виконати корекцію. Отримавши одиничне значення умови а блок керування 15 формує сигнал 25 (y_5, $ВІК_Р$) для видачі інверсного кода з регістра 6 та сигнал 28 (y_8,+1), який є вхідним переносом для комбінаційного суматора 10. Далі виконується підсумовування першого операнда (отримане значення суми C_0 = 100100) та другого операнда (проінвертоване значення модуля $\bar{p}$ = 101000) з урахуванням вхідного переноса. На виході комбінаційного суматора 10 отримуємо наступний результат C_0 = 001101. Далі блок керування 15 видає сигнал 26 (y_6, $ПКр_{П}р$) прийому кода в регістр 12 проміжного результата і результат з виходів комбінаційного суматор 10 записується в регістр 12 проміжного результата. В наступному такті формується сигнал 27 (y_7, $ВК_{Рез}$) відкривання «защіпки» 30 (групи елементів І) на другому вході якої знаходиться значення результату підсумовування двох коефіцієнтів. З виходів групи елементів 130 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується в нульовий регістр (згідно поточного стану лічильника адрес 7) даного РЗП. Далі блок керування 15 аналізує значення четвертої умови δ. Індикатор кінцевого стану лічильника формує значення δ яке дорівнює 0, це означає, що значення лічильника адрес 7 менше за значення степеня $m-1=3$ і потрібно переходити до наступного коефіцієнта операндів. В цьому випадку блок керування 15 видає сигнал 29 (y_9, CLK_{AC}) для інкрементації лічильника адрес 7. Лічильник адрес 7 переходить у стан 01_2.

Блок керування 15 формує сигнали 21 (y_1, $ВК_{РЗш}$) та 22 (y_2, ВКрзт) видачі прямого кода коефіцієнтів (A_1 та B_1), які знаходяться за одиничною адресою в РЗП першого та другого операнда. Зчитаний коефіцієнт першого операнда (A_1 = 17_{10} = 010001_2) через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, зчитаний коефіцієнт другого операнда (B_1 =10_{10} = 001010_2) через другу 9 групу елементів АБО надходить на другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах (010001 та 001010). З виходу комбінаційного суматора 10 результат C_1 =011011 потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 (y_6, $ПК_{рпр}$) прийому кода в регістр 12 проміжного результата. Далі значення п'ятого розряда (умова $\alpha = c_5 = 0$) регістра 12 проміжного результата поступає на відповідний вхід блока керування 15, а також на перший вхід логічного елемента АБО-НІ 13, на другий вхід логічного елемента АБО-НІ 13 поступає значення четвертого розряда ($c_4 = 1$) регістра 12 проміжного результата, на виході логічного елемента АБО-НІ 13 отримуємо значення умови $\beta = \overline{0 \vee 1} = 0$, яке надходить на відповідний вхід блока керування 15. Аналізуючи умови α та β блок керування 13 формує сигнал 24 (y_4, , $ВК_Р$) видачі прямого кода з регістра 6. На схемі порівняння кодів 11 виконується порівняння чотирьох молодших розрядів результата підсумовування коефіцієнтів та модуля. Схема порівняння кодів 11 формує значення третьої умови γ, яке дорівнює 0, тобто перший операнд (значення суми) більше або дорівнює другому операнду (значення модуля). Отримавши на четвертий вхід нульове значення третьої умови γ блок керування 15 формує сигнал 25 (y_5, , $ВІК_р$) видачі інверсного кода з регістра 6 модуля та сигнал 28 (y_8 ,+1), який є вхідним переносом для комбінаційного суматора 10. Далі виконується підсумовування першого операнда (отримане значення суми C_1=011011) та другого операнда (проінвертоване значення модуля $\bar{p}$ = 101000) з урахуванням вхідного переноса. На виході комбінаційного суматора 10 отримуємо наступний результат C_1=000100. Далі блок керування 15 видає сигнал 26 (y_6 , $ПК_{пр}$) прийому кода в регістр 12 проміжного результата і результат з виходів комбінаційного суматор 10 записується в регістр 12 проміжного результата. В наступному такті формується сигнал 27 (y_7 , $ВК_{Рез}$) відкривання «защіпки» 30 (групи елементів І) на другому вході якої знаходиться значення результату підсумовування двох коефіцієнтів. З виходів групи елементів 130 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується в регістр з одиничною адресою (згідно поточного стану лічильника адрес 7) даного РЗП. Далі блок керування 15 аналізує значення четвертої умови δ. Індикатор кінцевого стану лічильника формує значення δ яке дорівнює 0, це означає, що значення лічильника адрес 7 менше за значення степеня $m-1=3$ і потрібно переходити до наступного коефіцієнта операндів. В цьому випадку блок керування 15 видає сигнал 29 (y_9, CLK_{AC}) для інкрементації лічильника адрес 7. Лічильник адрес 7 переходить у стан 10_2.

Блок керування 15 формує сигнали 21 (y_1, $ВК_{РЗП1}$) та 22 (y_2, $ВК_{РЗП2}$) видачі прямого кода коефіцієнтів (A_2 та B_2), які знаходяться за адресою 2 в РЗП першого та другого операнда. Зчитаний коефіцієнт першого операнда (A_2 =9_{10}= 001001_2) через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, зчитаний коефіцієнт другого операнда (B_2= 11_{10} = 001011_2) через другу 9 групу елементів АБО надходить на

другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах (001001 та 001011). З виходу комбінаційного суматора 10 результат C_2 = 010100 потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 (y_6, $ПК_{пр}$) прийому кода в регістр 12 проміжного результата. Далі значення п'ятого розряда (умова $\alpha = c_5 = 0$) регістра 12 проміжного результата поступає на відповідний вхід блока керування 15, а також на перший вхід логічного елемента АБО-НІ 13, на другий вхід логічного елемента АБО-НІ 13 поступає значення четвертого розряда ($c_4 = 1$) регістра 12 проміжного результата, на виході логічного елемента АБО-НІ 13 отримуємо значення умови $\beta = \overline{0 \vee 1} = 0$, яке надходить на відповідний вхід блока керування 15. Аналізуючи умови α та β блок керування 15 формує сигнал 24 (y_4, $ВК_Р$) видачі прямого кода з регістра 6. На схемі порівняння кодів 11 виконується порівняння чотирьох молодших розрядів результата суми операндів та модуля p. Схема порівняння кодів 11 формує значення третьої умови γ, яке дорівнює 1, тобто перший операнд (значення суми) менше другого операнда (значення модуля p). Значення третьої умови γ надходить відповідно на четвертий вхід блока керування 15. Отримавши на четвертий вхід одиничне значення третьої умови блок керування 15 формує сигнал 27 (y_7, $ВК_{Рез}$) відкривання «защіпки» 30 (групи елементів І) на другому вході якої знаходиться значення результату підсумовування двох коефіцієнтів. З виходів групи елементів 130 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується в регістр з адресою 2 (згідно поточного стану лічильника адрес 7) даного РЗП. Далі блок керування 15 аналізує значення четвертої умови δ. Індикатор кінцевого стану лічильника формує значення δ яке дорівнює 0, це означає, що значення лічильника адрес 7 менше за значення степеня $m-1$ і потрібно переходити до наступного коефіцієнта операндів. В цьому випадку блок керування 15 видає сигнал 29 (y_9, $CLK_{АС}$) для інкрементації лічильника адрес 7. Лічильник адрес 7 переходить у стан 11_2.

Блок керування 15 формує сигнали 21 (y_1, $ВК_{РЗПі}$) та 22 (y_2, $ВК_{РЗП2}$) видачі прямого кода коефіцієнтів (A_3 та B_3), які знаходяться за адресою 3 в РЗП першого та другого операнда. Зчитаний коефіцієнт першого операнда ($A_3 = 8_{10} = 001000_2$) через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, зчитаний коефіцієнт другого операнда ($B_3 = 6_{10} = 000110_2$) через другу 9 групу елементів АБО надходить на другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах (001000 та 000110). З виходу комбінаційного суматора 10 результат C_3 = 001110 потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 (y_6, $ПК_{пр}$) прийому кода в регістр 12 проміжного результата. Далі значення п'ятого розряда (умова $\alpha = c_5 = 0$) регістра 12 проміжного результата поступає на відповідний вхід блока керування 15, а також на перший вхід логічного елемента АБО-НІ 13, на другий вхід логічного елемента АБО-НІ 13 поступає четвертий розряд ($c_4 = 0$) регістра 12 проміжного результата, на виході логічного елемента АБО-НІ 13 отримуємо значення умови $\beta = \overline{0 \vee 1} = 1$, яке надходить на відповідний вхід блока керування 15. Аналізуючи умови α та β блок керування 15 формує сигнал 27 (y_7, $ВК_{Рез}$) відкривання «защіпки» 30 (групи елементів І) на другому вході якої знаходиться значення результата підсумовування двох коефіцієнтів. З виходів групи елементів 130 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується в регістр з адресою 3 (згідно поточного стану лічильника адрес 7) даного РЗП. Далі блок керування 15 аналізує значення четвертої умови δ. Індикатор кінцевого стану лічильника формує значення δ яке дорівнює 1, це означає, що значення лічильника адрес 7 дорівнює значенню степеня $m-1=3$ і ми в регістровому запам'ятовувальному пристрої 31 отримали результат додавання двох елементів поля $GF(23^4)$. В табл. 4 показано яким чином буде записано результат додавання в $РЗП_3$.

Таблиця 4

Адреса	Значення
00	13_{10} = 0110I2
01	$4_{10} = 00100_2$
10	$20_{10}= 10100_2$
11	$14_{10} = 01110_2$

Приклад 2

Нехай є два елементи поля $GF(23^4)$: A = 43314, B = 185873.

Елементам A і B відповідає таке многочленне подання: $A(x) = 3x^3 + 12x^2 + 20x + 5$, $B(x) = 15x^3 + 6x^2 + 8x + 10$.

Виконаємо операцію віднімання (ОР = 1): A - B.

В $РЗП_1$ та $РЗП_2$ коефіцієнти многочленного подання будуть розміщені таким чином, як показано в табл. 5 (елементі) та табл. 6 (елемент B). Жирним в даних таблицях позначено $(n+1)$-і розряди, в даному прикладі це п'яті розряди, першого та другого операндів, які беруть участь у визначенні знаку проміжного результату, тобто проміжний результат є додатним чи від'ємним.

Таблиця 5

Адреса	Значення
00	5_{10} = 00010I2
01	$20_{10} = 010100_2$
10	$12_{10} = 001100_2$
11	$3_{10} = 000011_2$

Таблиця 6

Адреса	Значення
00	$10_{10} = 001010_2$
01	$8_{10} = 001000_2$
10	$6_{10} = 000110_2$
11	$15_{10} = 001111_2$

На вхід 16 блока керування 15 надходить значення кода операції (ОР). Код операції дорівнює 1, отже треба виконувати операцію віднімання двох операндів. Лічильник адрес 7 встановлений в нульовий стан.

Блок керування 15 формує сигнали 21 (y_1, $ВК_{РЗП1}$) видачі прямого кода коефіцієнта (A_0), який знаходиться за нульовою адресою в РЗП першого операнда та сигнал 23 (y_3, $ВІК_{РЗП2}$) видачі інверсного кода коефіцієнта (B_0), який знаходиться за нульовою адресою в РЗП другого операнда і формує сигнал 28 (y_8, +1), який є вхідним переносом для комбінаційного суматора 10. Зчитаний коефіцієнт першого операнда (A_0= 5_{10} = 000101_2) через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, зчитаний проінвертований коефіцієнт другого операнда ($\overline{B_0}$ = 110101_2) через другу 9 групу елементів АБО надходить на другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах (000101 та 110101) з урахуванням вхідного переноса. З виходу комбінаційного суматора 10 результат C_0 =111011 потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 (y_6, $ПК_{пр}$) прийому кода в регістр 12 проміжного результата. Далі значення п'ятого розряда (умова $\alpha = c_5 = 1$) регістра 12 проміжного результата поступає на відповідний вхід блока керування 15. Аналізуючи умову α блок керування 15 формує сигнал 24 (y_4, $ВК_Р$) видачі прямого кода з регістра 6. На комбінаційному суматорі 10 відбувається підсумовування першого операнда (отриманий результат C_0 = 111011) та значення модуля, яке дорівнює 010111. На виході комбінаційного суматора 10 отримуємо результат C_0 = 010010. Далі блок керування 15 видає сигнал 26 (y_6, $ПК_{пр}$) прийому кода в регістр 12 проміжного результата і результат з виходів комбінаційного суматора 10 записується в регістр 12 проміжного результата. В наступному такті формується сигнал 27 (y_7, $ВК_{Рез}$) відкривання «защіпки» 30 (групи елементів І) на другому вході якої знаходиться значення результату підсумовування двох коефіцієнтів. З виходів групи елементів 130 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується в регістр з адресою 00_2 (згідно поточного стану лічильника адрес 7) даного РЗП. Далі блок керування 15 аналізує значення четвертої умови δ. Індикатор кінцевого стану лічильника формує значення δ яке дорівнює 0, це означає, що значення лічильника адрес 7 менше за значення степеня $m-1=3$ і потрібно переходити до наступного коефіцієнта операндів. В цьому випадку блок керування 15 видає сигнал 29 (y_9, CLK_{AC}) для інкрементації лічильника адрес 7. Лічильник адрес 7 переходить у стан 01_2.

Блок керування 15 формує сигнали 21 (y_1, $ВК_{РЗП1}$) видачі прямого кода коефіцієнта (A_1), який знаходиться за одиничною адресою в РЗП першого операнда та сигнал 23 (y_3, $ВІК_{РЗт}$) видачі інверсного кода коефіцієнта (B_1), який знаходиться за одиничною адресою в РЗП другого операнда і формує сигнал 28 (y_8, +1), який є вхідним переносом для комбінаційного суматора 10. Зчитаний коефіцієнт першого операнда (A_1 = 20_{10} – 010100_2) через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, зчитаний проінвертований коефіцієнт другого операнда ($\overline{B_1}$ = 110111_2) через другу 9 групу елементів АБО надходить на другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах (010100 та 110111) з урахуванням вхідного переноса. З виходу комбінаційного суматора 10 результат C_1= 001100 потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 (y_6, $ПК_{пр}$) прийому кода в регістр 12 проміжного результата. Далі значення п'ятого розряда (умова $\alpha = c_5 = 0$) регістра 12 проміжного результата поступає на вхід блока керування 15. Аналізуючи умову α блок керування 15 формує сигнал 27 (y_7, $ВК_{Рез}$) відкривання «защіпки» 30 (групи елементів І) на другому вході якої знаходиться значення результату підсумовування двох коефіцієнтів. З виходів групи елементів 130 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується в регістр з адресою 01_2 (згідно поточного стану лічильника адрес 7) даного РЗП. Далі блок керування 15 аналізує значення четвертої умови δ. Індикатор кінцевого стану лічильника формує значення δ яке дорівнює 0, це означає, що значення лічильника адрес 7 менше за значення степеня $m-1=3$ і потрібно переходити до наступного коефіцієнта операндів. В цьому випад-

ку блок керування 15 видає сигнал 29 (y_9, CLK_{AC}) для інкрементації лічильника адрес 7. Лічильник адрес 7 переходить у стан 10_2.

Блок керування 15 формує сигнали 21 (y_1, $ВК_{РЗП1}$) видачі прямого кода коефіцієнта (A_2), який знаходиться за адресою 2 в РЗП першого операнда та сигнал 23 (y_3, ВІК $_{РЗП2}$) видачі інверсного кода коефіцієнта (B_2), який знаходиться за адресою 2 в РЗП другого операнда і формує сигнал 28 (y_8, +1), який є вхідним переносом для комбінаційного суматора 10. Зчитаний коефіцієнт першого операнда (A_2= 12_{10} = 001100_2) через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, зчитаний проінвертований коефіцієнт другого операнда ($\bar{B}_2$ =111001_2) через другу 9 групу елементів АБО надходить на другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах (001100 та 111001) з урахуванням вхідного переноса. З виходу комбінаційного суматора 10 результат C_2 = 000110 потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 (y_6, $ПК_{пр}$) прийому кода в регістр 12 проміжного результата. Далі значення п'ятого розряда (умова $\alpha = c_5 = 0$) регістра 12 проміжного результата поступає на вхід блока керування 15. Аналізуючи умову а блок керування 15 формує сигнал 27 (y_7, $ВК_{Рез}$) відкривання «защіпки» 30 (групи елементів І) на другому вході якої знаходиться значення результату підсумовування двох коефіцієнтів. З виходів групи елементів 130 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується в регістр з адресою 01_2 (згідно поточного стану лічильника адрес 7) даного РЗП. Далі блок керування 15 аналізує значення четвертої умови δ. Індикатор кінцевого стану лічильника формує значення δ яке дорівнює 0, це означає, що значення лічильника адрес 7 менше за значення степеня $m-1=3$ і потрібно переходити до наступного коефіцієнта операндів. В цьому випадку блок керування 15 видає сигнал 29 (y_9, CLK_{AC}) для інкрементації лічильника адрес 7. Лічильник адрес 7 переходить у стан 11_2.

Блок керування 15 формує сигнали 21 (y_1, $ВК_{РЗП1}$) видачі прямого кода коефіцієнта (A_3), який знаходиться за адресою 3 в РЗП першого операнда та сигнал 23 (y_3, ВІК $ВК_{РЗП2}$) видачі інверсного кода коефіцієнта (B_3), який знаходиться за адресою 3 в РЗП другого операнда і формує сигнал 28 (y_8, +1), який є вхідним переносом для комбінаційного суматора 10. Зчитаний коефіцієнт першого операнда (A_3 = 3_{10} = 000011_2) через першу 8 групу елементів АБО надходить на перший вхід комбінаціного суматора 10, зчитаний проінвертований коефіцієнт другого операнда ($\bar{B}_3$ = 110000_2) через другу 9 групу елементів АБО надходить на другий вхід комбінаційного суматора 10. На комбінаційному суматорі 10 виконується підсумовування двійкових кодів, які присутні на першому та другому входах (000011 та 110000) з урахуванням вхідного переноса. З виходу комбінаційного суматора 10 результат C_3 = 110100 потрапляє на вхід регістра 12 проміжного результата. Блок керування 15 формує сигнал 26 (y_6, $ПК_{пр}$) прийому кода в регістр 12 проміжного результата. Далі значення п'ятого розряда (умова $\alpha = c_5 = 1$) регістра 12 проміжного результата поступає на відповідний вхід блока керування 15. Аналізуючи умову а блок керування 15 формує сигнал 24 (y_4, $ВК_р$) видачі прямого кода з регістра 6. На комбінаційному суматорі 10 відбувається підсумовування першого операнда (отриманий результат C_3 = 110100) та значення модуля, яке дорівнює 010111. На виході комбінаційного суматора 10 отримуємо результат C_3 = 001011. Далі блок керування 15 видає сигнал 26 (y_6, $ПК_{пр}$) прийому кода в регістр 12 проміжного результата і результат з виходів комбінаційного суматора 10 записується в регістр 12 проміжного результата. В наступному такті формується сигнал 27 (y_7, $ВК_{Рез}$) відкривання «защіпки» 30 (групи елементів І) на другому вході якої знаходиться значення результату підсумовування двох коефіцієнтів. З виходів групи елементів 130 результат потрапляє на вхід регістрового запам'ятовувального пристрою 31 і записується в регістр з адресою 11_2 (згідно поточного стану лічильника адрес 7) даного РЗП. Далі блок керування 15 аналізує значення четвертої умови S. Індикатор кінцевого стану лічильника формує значення д яке дорівнює 1, це означає, що значення лічильника адрес 7 дорівнює значенню степеня $m-1=3$ і ми в регістровому запам'ятовувальному пристрої 31 отримали результат віднімання двох елементів поля $GF(23^4)$. В табл. 7 показано яким чином буде записано результат віднімання в $РЗП_3$.

Таблиця 7

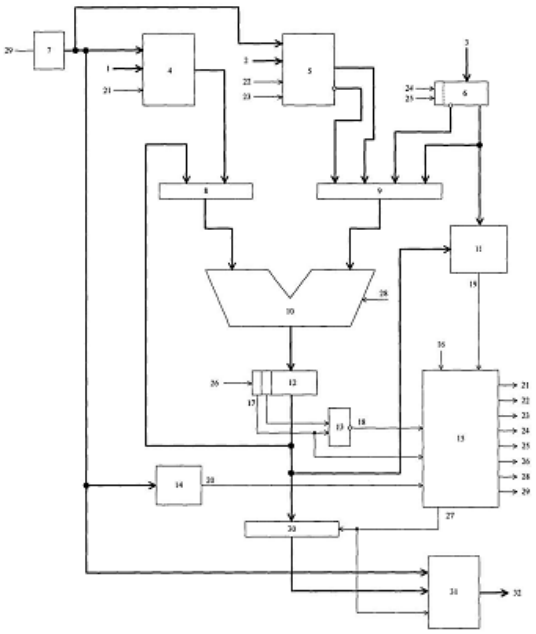
Адреса	Значення
00	18_{10}= 10010_2
01	12_{10} = 01100_2
10	6_{10} = 00110_2
11	11_{10} = 01011_2

Джерела інформації:

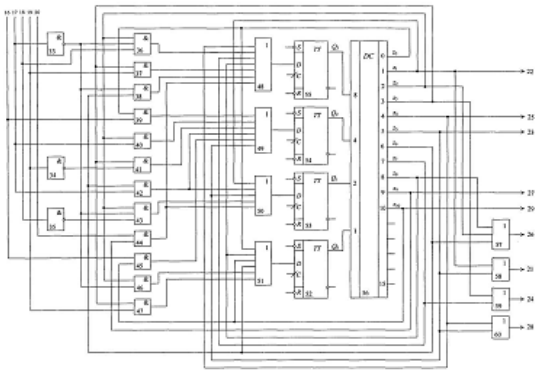
1. СССР, Авторское свидетельство №1401452, МПК G06F 7/49; Изобретатель О.Н. Музыченко; №4144092/24-24, Дата подачи 04.11.1986; Дата публ. 07.06.1988, Бюл. №21; Сумматор по модулю три.

2. Россия, Патент №2156998, МІЖ G06F 7/49, G06F 7/72; Заявитель Воронежский государственный технический университет; №99102011/09, Дата подачи 02.02.1999; Дата публ. 27.09.2000; Устройство для сложения и вычитания чисел по модулю.

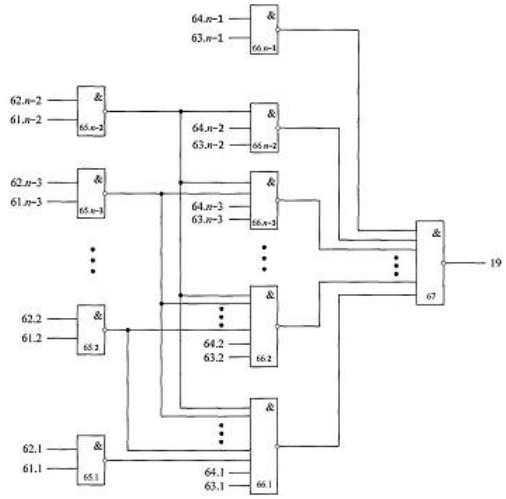
3. Україна, Патент №86637, МПК G06F 7/50; Заявники Фурман Ілля Олександрович; Кошман Сергій Олександрович; Деренько Микола Семенович; Краснобаев Віктор Анатолійович; № a200701744, Дата подачі 19.02.2007; Дата публ. 12.05.2009, бюл. №9; Суматор по модулю т системи залишкових класів.



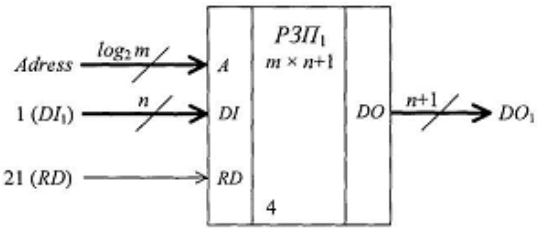
Фіг. 1



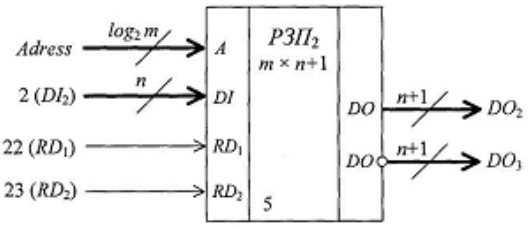
Фіг. 2



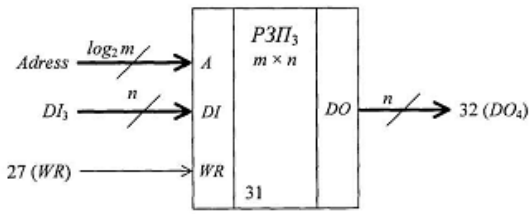
Фіг. 3



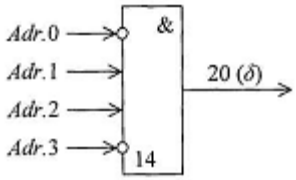
Фіг. 4



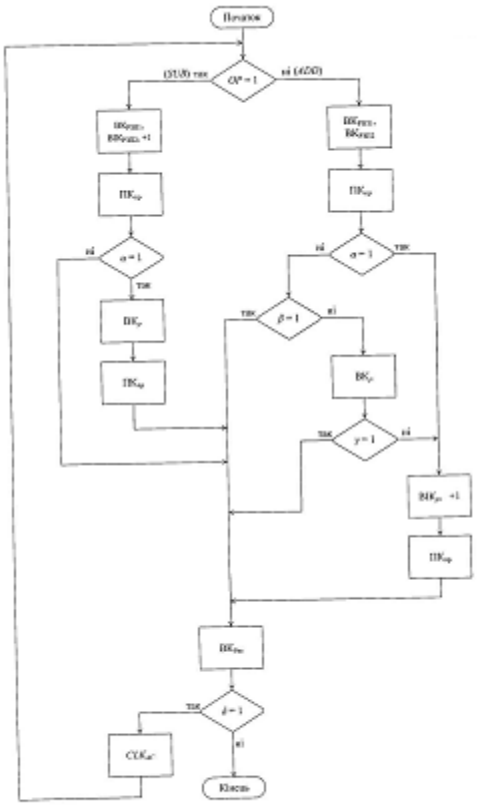
Фіг. 5



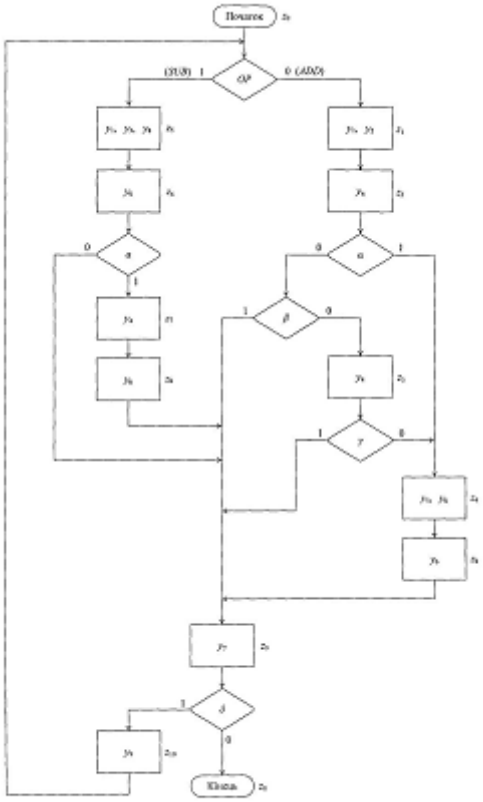
Фіг. 6



Фіг. 7



Фіг. 8



Фіг. 9

Комп'ютерна верстка Д. Шеверун Підписне Тираж 23 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