УДК 519.67

А. Батюк, В. Кожан*
Національний університет ”Львівська політехніка”, кафедра АСУ
*Фізико-механічний інститут ім.Г.В.Карпенка НАНУ

ШВИДКІ ПОМНОЖУВАЧІ ПОЛІНОМІВ

Розглянуто задачу множення розріджених поліномів та поліномів над полями Галуа GF(2^m), запропоновано алгоритми та структури спеціалізованих помножувачів для їх реалізації.

This paper presents a new algorithm for perfoming fast multiplication in GF(2^m) and sparse polynomials. The designs are highly regular, modular, and well-suited for VLSI implementation.

При розв’язанні багатьох задач кодування для стиску інформації, а також виявлення і виправлення помилок в криптографічних алгоритмах, в області зв’язку, цифровій обробці сигналів тощо розглядають реалізації операцій над поліномами. Існує потреба в алгоритмах, які можна було б реалізувати з використанням надвеликих інтегральних схем (НВІС) технології [1, 2].

Поля Галуа привернули велику увагу через своє практичне використання в області кодування, зв’язку, в теорії перемикальних схем, цифровій обробці сигналів тощо. Скінченні поля застосовують у конструкціях багатьох кодів, які виправляють помилки, в кодувальних і декодувальних схемах Reed-Solomon кодів, в криптографічних алгоритмах. Скінченне поле $GF(2^m)$ складається з елементів, які можна подати декількома еквівалентними формами, зокрема за допомогою поліномів, степінь яких не перевищує $m-1$ з коефіцієнтами з поля $GF(2)$. Тоді операції над поліномами проводять за модулем незвідного многочлена $F(x)$ степені m, який є породжуючим для поля $GF(2^m)$.

Існує необхідність в хороших алгоритмах множення в скінченних полях, які можна було б легко реалізувати за допомогою НВІС технології. Існує ряд схем реалізації множення елементів у скінченних полях, але не всі вони підходять для реалізації у НВІС системах через відсутність паралельності, однорідності і модульності або складність управління і топології зв’язків. Використаємо підхід, запропонований раніше в [4].

Два елементи поля $GF(2^m)$: множник $A(x)=\sum_{i=0}^{m-1} a_i x^i$ і множене $B(x)=\sum_{i=0}^{m-1} b_i x^i x$ множимо за модулем незвідного многочлена $F(x)=x^m+f_{m-1}x^{m-1}+\ldots+f_1x+1$: $A(x)\cdot B(x) \bmod F(x)$.

Добуток подамо у вигляді $P(x)=\sum_{i=0}^{m-1} p_i x^i$,

$$\begin{aligned} P(x) &= A(x)\cdot B(x) \bmod F(x) = A(x)\cdot\left\{b_{m-1}x^{m-1}+\ldots+b_1x+b_0\right\} \bmod F(x) = \\ &= \left\{A(x)b_{m-1}x^{m-1} \bmod F(x)+\ldots+A(x)b_0 \bmod F(x)\right\} \bmod F(x). \end{aligned} \quad (1)$$

Розписавши кожен із термів (1), отримаємо:

$$K_i(x)=P_i(x)\cdot x^{m-i-1} \bmod F(x), \text{ де } P_i(x)=\left[P_{i-1}(x)+A(x)\cdot b_{m-i}\right] \bmod F(x)\cdot x;\ i=\overline{1,m}. \quad (2)$$

Нехай $A(x)=(a_{m-1},\ldots,a_1,a_0)$, $B(x)=(b_{m-1},\ldots,b_1,b_0)$, $F(x)=(1,f_{m-1},\ldots,f_1,f_0)$, $P(x)=(p_{m-1},\ldots,p_1,p_0)$ – бінарні вектори. Для реалізації (2) скористаємось алгоритмом, поданим на рис. 1. Початкове значення лічильника I дорівнює степені $F-1$. Елемент *A* сумується з частковим добутком *P*, якщо поточний біт *B b=1*. F з частковим добутком *P* , якщо старший розряд часткового добутку *CP(P*) дорівнює 1. Сумування відбувається за модулем 2. Часткові добутки, які обчислюються кожною коміркою, подаються рекурентною формулою

$$P_j^i = P_{j-1}^{i-1} + P_N^{i-1} f_j + b_{N-1} \cdot a_{j,} \text{ де } 0 \le i, j \le N, N = m-1. \quad (3)$$

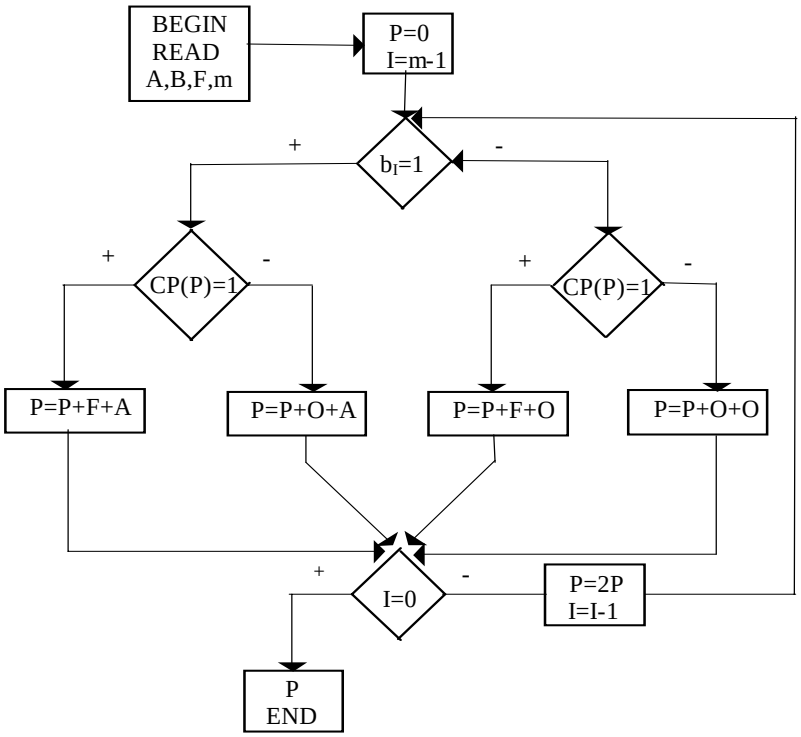


Рис. 1. Алгоритм множення в скінченних полях Галуа GF(2^m)

Опишемо роботу обчислювального масиву (рис. 2.) В початковий момент часу коефіцієнти множника $A(x)$: $a_1,a_2,\ldots,a_N$ записуються через вхід *a* в буфер 3 обчислювальної комірки 1 (рис. 3) і зберігаються до кінця. Коефіцієнти многочлена *F* через вхід *f* записуються в буфер 4. Коефіцієнти множеного $B(x)$: $b_1,b_2,\ldots,b_N$ подаються з інтервалом в один такт, починаючи з старших розрядів на вхід B_{bx} крайньої лівої комірки (старший розряд). На вхід P_{bx} крайньої правої комірки (молодший розряд) постійно надходять логічні «*0*». Розряди часткових добутків зберігаються в буфері 2. При цьому старший розряд часткового добутку використовується для визначення решти таких розрядів, оскільки його значення із затримкою на один такт подається на вхід S_{bx} крайньої лівої комірки, а потім розповсюджується по всіх комірках масиву в міру просування розрядів множеного. На кожному такті роботи комірки визначається значення відповідного розряду часткового добутку шляхом реалізації логічної функції (3). На виході масиву через *2N* тактів роботи з'явиться значення старшого розряду добутку *P(x)*. Наступні значення розрядів *P(x*) на виході будуть з'являтись через кожний такт роботи. Це дає можливість використовувати вказану особливість для розв'язання двох аналогічних задач одночасно. Для цього на вхід B_{bx} подаються в пос-

лідовному порядку коефіцієнти множеного $B_1(x)$ і $B_2(x)$, а на виході пристрою через $2N$ тактів роботи на кожному непарному такті виникають коефіцієнти добутку поліномів $A(x)B_1(x)$, а на кожному парному такті – добуток поліномів $A(x)B_2(x)$.

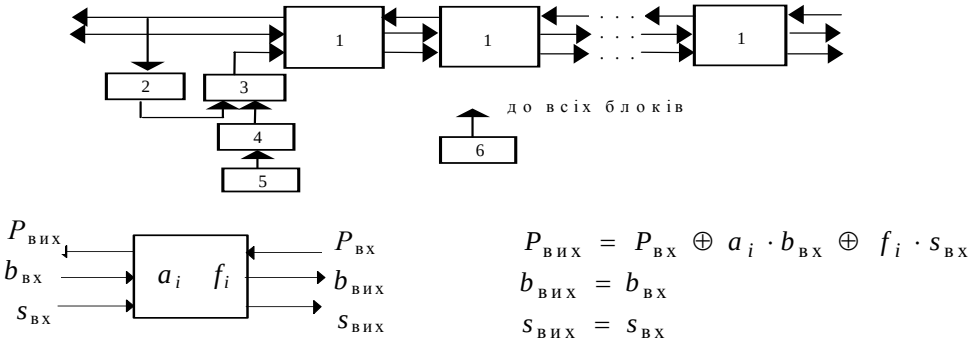


Рис. 2. Множення елементів у полях Галуа $F(2^m)$: 1 – обчислювальна комірка; 2 – блок затримки; 3 – логічний елемент АБО; 4 – схема порівняння; 5 – ГТІ

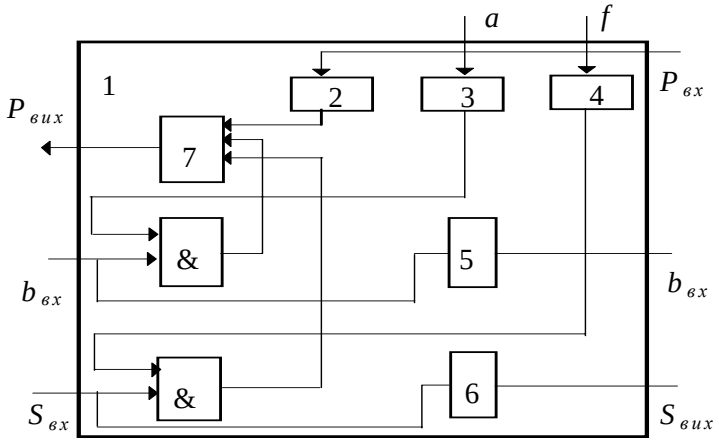


Рис. 3. Обчислювальна комірка: 2 - 6 – буфери; 7 – суматор за модулем 2

Запропонований обчислювач за високої швидкодії простий і однорідний, що дозволяє скоротити схемотехнічні затрати і легко нарощувати його зі збільшенням розмірності задачі. Крім того, регулярність і локальність зв'язків, автоматичний режим управління дає можливість ефективно використовувати НВІС - технологію при його виготовленні.

Під час розв'язання багатьох задач зондування, математичної фізики, лінійної алгебри, теорії кодування розглядають задачі реалізації арифметичних операцій над поліномами [1, 2]. Необхідно розрізняти модель поліномів, в якій припускається, що більшість коефіцієнтів відмінні від нуля (щільна модель), і модель, де більшість коефіцієнтів дорівнює нулю (розріджена модель). Нижче наведено результати досліджень розв'язання задачі множення поліномів [3].

Розріджений поліном $P(x) = \sum_{i=1}^{n} a_i x^{j_i}$ задаватимемо списком пар, які складаються з ненульового коефіцієнта і показника степеня змінної x: $(a_1, j_1), (a_2, j_2), \ldots, (a_n, j_n)$, де j_i задовольняють умови:

1. $\forall k, l \in N \quad j_k \neq j_l$.
2. $j_i > j_{i+1}$, $\quad 1 \leq i < n$.

При множенні так поданих поліномів знаходимо добутки пар і розміщуємо їх за показниками (тобто за другими компонентами пар), об'єднуючи всі члени з однаковими показниками. Наведемо неформальний алгоритм множення розріджених поліномів, зображених так:

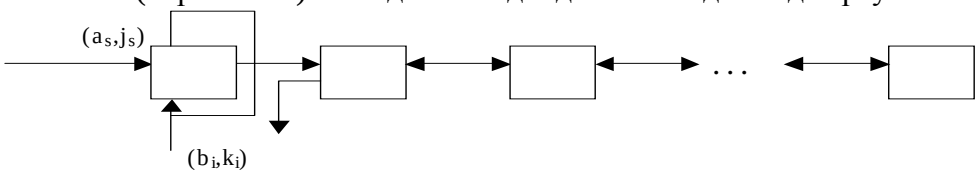
Вхід. Поліноми $f(x)=\sum_{i=1}^{m} a_i x^{j_i}$ і $g(x)=\sum_{i=1}^{n} b_i x^{k_i}$ подаються списками пар

$$(a_1, j_1),\ (a_2, j_2),\ldots,(a_m, j_m) \quad \text{і} \quad (b_1, k_1),\ (b_2, k_2),\ldots,(b_n, k_n).$$

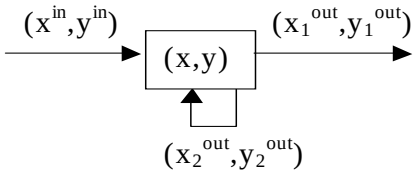
Вихід. Поліном $f(x)g(x)=\sum_{i=1}^{p} c_i x^{l_i}$, зображений за допомогою списку пар

$$(c_1, l_1),\ (c_2, l_2),\ldots,(c_p, l_p),\ \text{де}\ \ c_i > c_{i+1},\ \ 1 \le i < p.$$

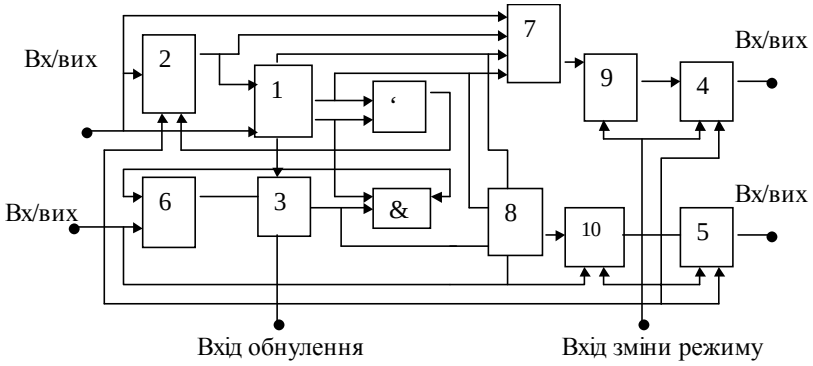
На рис. 4 наведено структурну схему лінійного масиву для множення розріджених поліномів. На один із входів комірки-множника послідовно через кожні X тактів, де X – кількість членів полінома-множеного, налдходять коефіцієнти полінома-множника, заданого у вигляді списку пар ненульових коефіцієнтів і відповідних показників степенів. На інший вхід множника поступають потактно пари коефіцієнтів полінома-множеного. Результати множення (пари чисел) послідовно надходять на вхід-вихід сортуючої комірки.



а



$$(x_2^{out}, y_2^{out}) = \begin{cases} \max\limits_{y}\left\{\left(x^{in}, y^{in}\right), (x, y)\right\}, & y^{in} \neq y; \\ \left(x^{in} + x, y\right), & y^{in} = y, \end{cases} \qquad \left(x_1^{out}, y_1^{out}\right) = \min\limits_{y}\left\{\left(x^{in}, y^{in}\right), (x, y)\right\}$$



б

Рис.4. Процесорний масив для множення розріджених поліномів: а – структурна схема; б – сортуюча комірка: 1 – блок порівняння, 2 – 5 – регістри, 6 – суматор, 7 – 10 – комутатори

Сортуюча комірка працює так. Блок порівняння 1 виконує порівняння показника степені, який надійшов із записаним у регістр 2. Якщо показник степені, що надійшов більший, то виконується перезапис вмістимого регістрів 2 і 3 у відповідні регістри 4 і 5, а в регістри 2 і 3 записується відповідно показник степені і коефіцієнт, що надійшли. Якщо показник степені менший від записаного, то записується показник степені і коефіцієнта, що надійшли в регістри 4 і 5 із збереженням інформації в регістрах 2 і 3. Якщо ж показники степенів однакові, то додається коефіцієнт, що надійшов із записаним в регістр 3, і записується результат додавання і показника степені відповідно в регістри 3 і 2. Вивантаження результатів проходить в напрямку, зворотному до напрямку надходження даних.

Підвищити швидкодію пристрою можна, організувавши паралельний вивід інформації. Зауважимо, що якщо при знаходженні добутків довільних поліномів кількість членів результуючого полінома менша, ніж розмірність процесорного масиву, то можна досягти виграшу у швидкодії за рахунок зменшення кількості працюючих комірок процесорного масиву.

Розглянемо наступний проект матричного помножувача, який являє собою *nxn* - масив $N=n^2$ однорідних обчислювальних комірок з такими зв'язками (рис. 5):

Y_1, Y_2, X_1, X_2 – вертикальні та горизонтальні керуючі входи;

$Y_1(n-1)$ – вхід управління з попередньої комірки;

$Y_1(n+1)$ – вихід управління наступної комірки;

Y – вхід управління режимом роботи;

TI – вхід тактових імпульсів;

a,b,c_1 – інформаційні входи ;

c_2 – інформаційний вихід;

d_1,d_2 – вхід і вихід обміну керуючими сигналами між комірками.

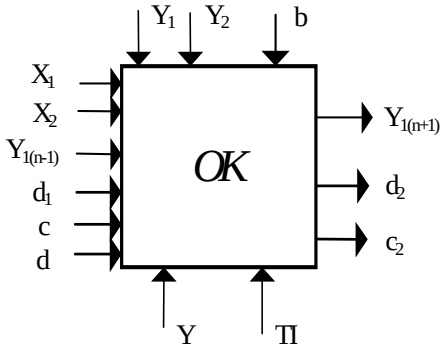


Рис. 5. Обчислювальна комірка

Зв'язок комірки із сусідніми встановлюється за допомогою керуючих входів X_1, X_2, Y_1, Y_2 . Комірка може працювати в таких режимах:

1) режим множення пар послідовностей, які надходять на входи *a* і *b* . Виключення режиму проводиться сигналом *Y* ;

2) режим тасування. Проводиться інформаційний обмін з сусідньою коміркою;

3) активний режим. За необхідності спрацьовує сигнал d_2, який дозволяє обмінюватися інформацією із сусідньою коміркою. При збігуі показників степеня (других компонентів пар) виконується додавання коефіцієнтів (перших компонентів). Активізація обчислювальної комірки проводиться керуючими сигналами X_2 і Y_1.

4) пасивний режим. ОК знаходиться в стані очікування керуючого сигналу d_1 з сусідньої активної ОК. Після надходження сигналу проходить обмін інформацією з сусідньою коміркою, в протилежному випадку ОК зберігає свою інформацію;

5) режим вивантаження. Проходить об'єднання всіх ОК по стовпцях і по кожному такту - зсув матриці даних посрядково вниз.

Отже, кожна комірка виконує множення, перестановку, порівняння-перестановку, порівняння-додавання.

Робота помножувача описується таким алгоритмом:

1. Множення коефіцієнтів: формування в кожній процесорній комірці пари виду $(a_r b_i, j_r + q_i)$, $i,r = \overline{1,n}$; де a_r, b_i (j_r, q_i) – коефіцієнти (показники степеня) вхідних поліномів.

2. Перетасування кожного рядка масиву розмірності *nxn* , тобто перестановка стовпців за повним перетасуванням.

3. Сортування подвійних стовпців, тобто підмасивів розмірності *nx2* в змієподібному порядку за допомогою непарно-парного транспозитивного сортування. По ходу сортування підсумовуються коефіцієнти з однаковими показниками степеня.

4. Сортування масиву розмірності *nxn*, за допомогою непарно-парного транспозитивного сортування в змієподібному порядку. По ходу сортування додаються коефіцієнти з однаковими показниками степеня.

Для сортування використовуються алгоритм MERGE [3], який базується на алгоритмі злиття підмасивів і складається з повної перетасовки і парно-непарного сортування. На рис. 6 схматично показано роботу помножувача. Другий крок алгоритму – операція перетасовування перетворює послідовність $Z_1, Z_2, \ldots, Z_{2n}$ в повну перетасовану послідовність $Z_1, Z_{n+1}, Z_2, Z_{n+2}, \ldots, Z_n$. Змієподібне сортування подвійних стовпців зверху вниз у порядку зростання проходить на базі непарно-парного сортування. На непарному (парному) покроковому алгоритмі всі елементи послідовності, які мають непарні (парні) записи, порівнюються зі своїми наступними елементами і міняються місцями, якщо $\left\{Z_i > Z_{i+1},\ i = \overline{1,n-1}\right\}$. Парно-непарні кроки виконуються в порядку чергування. Якщо елементи, що порівнюються, збігаються (за другими компонентами пар) , то додаються перші компоненти елементів, які порівнюються, і записуються на місце першого. Другий елемент (пара) при цьому позначається *(0,0).* На рис.6 проілюстровані відповідні кроки транспозитивного сортування двох подвійних стовпців *4x2* масиву елементів розмірності *4x4*. Час T , необхідний для множення двох розріджених поліномів порядку n за розглядуваним алгоритмом – $T = 4.5n$.

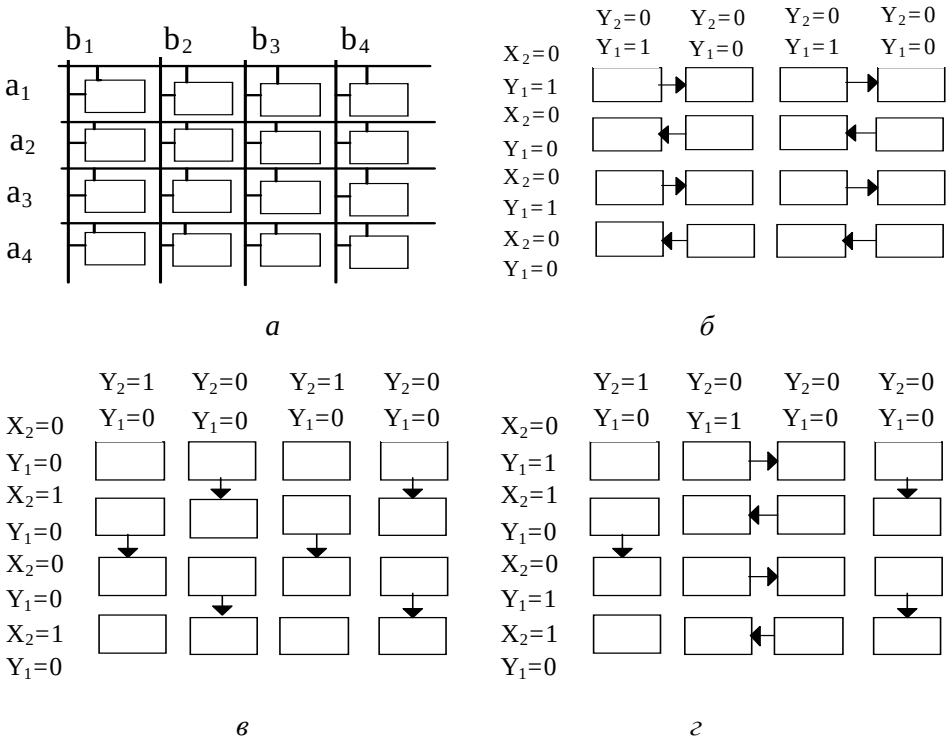


Рис. 6. Матриця процесорних елементів розмірності 4x4

Отже, запропонований підхід дозволяє суттєво скоротити час реалізації алгоритму порівняно з традиційними підходами (n^2), а також отримувати конвеєрні алгоритми, які добре реалізуються з використанням технології НВІС.

1. Кожан В.П., Деркач Б.Т. Множення в кільці многочленів. // Автоматика-97. Т .4, – С. 27. 2. Кун С. Матричные процессоры и на СБИС — М., 1991. – 672 с. 3. Land.H.W. e.a. Systolic Sorting on Mesh-connected Network.// IEEE Trans. On Comput.– 1985. – С-35, – №6. – P. 531 – 542. 4. Scott P.A., Tavares S.E., Peppard L.E. A Fast VLSI Multiplier for GF(2) // IEEE al on Selected Areas in Communications. – 1996. – Sac-4, – №1, – P. 62 – 65.

УДК 681.333

В. Отенко, Л. Пархуць, З. Стрілецький
Національний університет "Львівська політехніка",
кафедра АВ

ПРИСТРІЙ ДЛЯ ВИЗНАЧЕННЯ СЕРЕДНЬОГО АРИФМЕТИЧНОГО ЗНАЧЕННЯ ВИМІРЮВАНИХ ВЕЛИЧИН

Розглянуто пристрій для визначення середнього арифметичного значення вимірюваних величин, інформативний сигнал від яких представлений число-імпульсним кодом.

In the article the device for definition of arithmetic mean of value of stimuluss is reviewed, the intelligence signal which one is shown by a number-pulse-code.

На практиці часто виникає потреба визначення середнього значення виміряної температури, вологості, освітлення, тиску, електричних чи інших фізичних величин у великих за об'ємом приміщеннях або для кількох рознесених у просторі об'єктів, причому контроль за вимірюваною величиною в різних точках здійснюють окремими сенсорами. Найзручніше для цього використати сенсори з частотним представленням виміряної інформації, які мають високу стабільність параметрів, завадостійкість, надійність і можуть передавати результат вимірювання на значні відстані [1, 2]. В таких випадках для знаходження середнього значення виміряної величини може бути використаний пристрій, що розглядається у даній статті [3].

Даний пристрій дозволяє визначати миттєве середнє значення кількості імпульсів у число-імпульсних послідовностях вимірюваних сигналів для довільної кількості каналів вимірювання. При цьому його універсальність полягає в тому, що він автоматично визначає кількість підключених каналів вимірювання, а також автоматично визначає справність чи несправність кожного каналу. Якщо один чи кілька каналів вимірювання вимкнені або випадково стали несправними (наприклад, через обрив чи пошкодження лінії з'єднання сенсора та пристрою), то середнє арифметичне значення буде визначатися лише серед працюючої кількості каналів. У разі необхідності пристрій може визначати наявність