УДК 638.322

О.К. ТЕСЛЕНКО, О.М. ЛАВСЬКИЙ

Національний технічний університет України "КПІ", Київ

СИНТЕЗ 2-ГРУП НА ЛОГІЧНИХ ЕЛЕМЕНТАХ

Проведено аналіз можливості реалізації групових операцій над двійковими кортежами довільної розрядності (2-груп) на логічній мережі фіксованої структури і лінійної складності, та визначені логічні функції мережі. За допомогою програмного інструментарію одержані результати підтверджені експериментально. Доведено, що на ЛМ лінійної складності із структурою суматора при будь якій розрядності більшою за 3 можна реалізувати лише 16 різних групових операцій, 8 із яких є найпростішими та ізоморфні порозрядній операції xor, а інші 8 ізоморфні операції додавання по модулю 2n.

Ключові слова: *логічні мережі, групові операції, суматор, ізоморфізм.*

Вступ

Арифметичні блоки сучасного комп'ютера в основному побудовані на базі чотирьох операцій – додавання, множення, а також їх зворотних - віднімання та ділення. Ці операції складають деякий обчислювальний фундамент, розвинений математичний апарат дозволяє знаходити їх суперпозиції для обчислення значної кількості функцій, що зустрічаються в прикладних задачах.

Проте ми зовсім не зобов'язані обмежувати себе цими чотирма операціями. Можливо вдасться знайти такі операції, які б виконувались так само швидко, але при цьому дозволяли б вирішувати ряд задач ефективніше.

Ми пропонуємо вирішувати поставлену проблему виходячи з критерію простоти реалізації на логічних елементах, що забезпечить малий час перехідних процесів в схемі, тобто час отримання результату операції. Також пропонуємо обмежитися класом групових операцій (який включає додавання і множення), зважаючи на його виключну корисність і вивченість.

Задача даної статті полягає в дослідженні можливостей регулярних логічних мереж лінійної складності для реалізації групових операцій довільної розрядності (2-груп).

1. Основні визначення

Регулярна логічна мережа (ЛМ) лінійної складності – сукупність поєднаних між собою однакових конструктивних модулів (КМ) із настроюваних (на будь-яку таблицю істинності) булевих функцій відповідного числа змінних. При цьому виділимо вхідні (позначатимемо X^n і Y^n) та вихідні (позначатимемо Z^n) кортежі (впорядковані набори) булевих змінних. ($X^n = \langle x_1,x_2,\ldots,x_n\rangle$, $Y^n = \langle y_1,y_2,\ldots,y_n\rangle$, $Z^n = \langle z_1,z_2,\ldots,z_n\rangle$), n – натуральне число. Фактично кортежі X^n і Y^n – це кортежі незалежних булевих змінних, а Z^n – це кортежі булевих функцій. При конкретних значеннях булевих змінних утворюються кортежі значень змінних, які будемо позначати першими буквами латинського алфавіту, наприклад $A^n = \langle a_1,a_2,\ldots,a_n\rangle$. Множину всіх n-розрядних кортежів позначимо E^n. Лінійна складність ЛМ забезпечується використанням в ній рівно n конструктивних модулів.

На рис. 1 зображена регулярна однонаправлена логічна мережа лінійної складності. В літературі вказана логічна мережа має також назву одновимірний однонаправлений регулярний каскад конструктивних модулів або логічна мережа зі структурою суматора. Зрозуміло, що така ЛМ – просто комбінаційна схема.

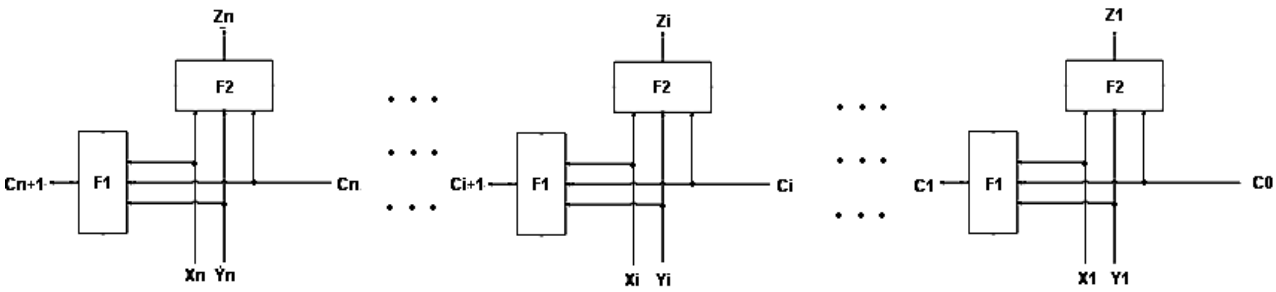

Рис. 1. Регулярна одно направлена логічна мережа лінійної складності

ЛМ на рис.1 складається із сукупності однакових КМ, структура яких визначається булевою функцією F_2 на первинному виході КМ та булевою функцією F_1 на боковому виході, тобто $z_i = F_2\ (x_i, y_i, c_i)$, $c_{i+1} = F_1\ (x_i, y_i, c_i)$, i=1,2,…,n, $c_0 \in \{0,1\}$ – константа налагоджування.

Скінчена група (надалі група)– множина E^n з визначеною на ній операцією (позначимо °) від двох змінних. Операція має задовольняти умовам асоціативності, існування нейтрального елемента (одиниця групи), який будемо позначати як кортеж $O^n = <o_1, o_2, \ldots, o_n>$ та існування оберненого елемента [2]. Відмітимо наступні властивості групової операції

$$\forall(A^n, B^n, D^n \in E^n,\ B^n \neq D^n) |\ A^n \circ B^n \neq A^n \circ D^n \quad \text{та} \quad B^n \circ A^n \neq D^n \circ A^n, \tag{1}$$

$$\forall(A^n, B^n, D^n \in E^n) \mid (A^n \circ B^n) \circ D^n = A^n \circ (B^n \circ D^n)$$

$$\forall(A^n \in E^n)\ \exists(O^n \in E^n) \mid O^n \circ A^n = A^n \quad \text{та} \quad A^n \circ O^n = A^n.$$

2. Оцінка кількості груп порядку 2^n

Перед тим, як розв'язувати поставлену задачу, корисно оцінити її об'єм. В табл. 1 наведені точні дані для кількостей попарно не ізоморфних груп різних порядків [3] .

Таблиця 1

Неізоморфні групи малого порядку

Порядок групи	Всього	Абелевих
$2^0=1$	1	1
$2^1=2$	1	1
$2^2=4$	2	2
$2^3=8$	5	3
$2^4=16$	14	5
$2^5=32$	51	7
$2^6=64$	267	11
$2^7=128$	2328	15
$2^8=256$	56092	22
$2^9=512$	10494213	30
$2^{10}=1024$	49487365422	42

Бачимо, що обсяг задачі вже для восьми розрядів завеликий для повного аналізу.

Кількість не ізоморфних груп порядку p^n, де p – просте, має асимптотику: [4]

$$p^{\frac{2}{27}n^3+O(n^{\frac{8}{3}})}$$

зокрема при p = 2 маємо

$$p(n) = 2^{\frac{2}{27}n^3+O(n^{\frac{8}{3}})}.$$

Кількість неізоморфних абелевих груп порядку p^n (p – просте) дорівнює числу розбиттів P(n) числа n. Асимптотика: [2]

$$P(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}.$$

Ці дві функції зростають дуже швидко, причому до нескінченності, тому намагатися дослідити всі групи окремого порядку не має сенсу для великих n - це стає просто фізично не можливо. Таким чином, прив'язка досліджень до конкретних структур логічної мережі обґрунтована.

Зазначимо, що подібний характер залежності кількості 2-груп від порядку не має місця для всіх груп. Наприклад, для порядків, які являються простими числами, з точністю до ізоморфізму, існує лише одна група.

3. Елементарні (найпростіші) групові операції на ЛМ зі структурою суматора

Загальновідомо, що булеві операції x+y (операція **xor**) та x+y+1 (операція **not xor**), де знаком + позначена операція суми по модулю 2, є груповими на множині $\mathbf{E^1}$. Звідси випливає, що ЛМ на n розрядів, де $z_i = x_i + y_i$, або $z_i = x_i + y_i + 1$, i=1,2,…,n, реалізує групову операцію на множині $\mathbf{E^n}$. Всього може бути 2^n таких операцій, всі вони ізоморфні одна одній. Кожний елемент в множині $\mathbf{E^n}$ має порядок в групі, який дорівнює 2, і відповідно є оберненим сам до себе.

Реалізація вказаних операцій простіша ніж в ЛМ зі структурою суматора. Легко перевірити, що ЛМ зі структурою суматора при відповідних функціях F_1 та F_2 та значенні c_0 із-за регулярності структури може реалізувати лише шість із 2^n найпростіших групових операцій:

1) порозрядну **xor,**
2) порозрядну **not xor,**
3) $z_i = x_i + y_i$ при парних i та $z_i = x_i + y_i + 1$ при непарних i,
4) $z_i = x_i + y_i + 1$ при парних i та $z_i = x_i + y_i$ при непарних i,
5) $z_i = x_i + y_i$ при i= i=2,3…,n, $z_1 = x_1 + y_1 + 1$,
6) $z_i = x_i + y_i + 1$ при i= i=2,3…,n, $z_1 = x_1 + y_1$,

4. Інші групові операції на ЛМ зі структурою суматора

Станом ЛМ називатимемо комбінаційну схему, яка реалізується цією ЛМ при конкретно визначених (детермінованих) булевих функціях. В випадку логічної мережі зі структурою суматора кількість станів ЛМ визначається кількістю різних пар функцій F_1 та F_2 і дорівнює $C_1(n)=2^{16}$.

Стани ЛМ називатимемо різними, якщо вони визначені різними функціями F_1 та F_2.

Зрозуміло, що різні стани можуть реалізовувати одну й ту саму операцію, тобто значення $C_1(n)$

можна розглядати лише як верхню оцінку кількості різних операцій.

Твердження 1. Для будь якого стану ЛМ зі структурою суматора існує тотожній стан, тобто стан при якому реалізується одна і та ж операція. Доведення ґрунтується на тому факті, що введення двох інверторів між КМ не призводить до зміни операції. Таким чином для будь якого стану, який задається функціями F_2 (x_i, y_i,c_i), та F_1 (x_i, y_i,c_i), тотожним буде стан із функціями F'_1 (x_i, y_i,c_i) = not F_1 (x_i, y_i,not c_i) , F'_2 (x_i, y_i,c_i) = F_2 (x_i, y_i,not c_i), крім того c'_0 = not c_0 .

В випадку реалізації групових операцій верхню оцінку їх кількості можна зменшити ще суттєвіше.

Твердження 2. Існує не більше двох дочірніх функцій $F_2(x,y,const)$ ($const \in \{0,1\}$) при яких логічна мережа зі структурою суматора реалізує групову операцію на множині $\mathbf{E^n}$.Оскільки всі КМ мережі одинакові, то не порушуючи загальності, розглянемо згідно з (1) властивості функцій КМ в n-ному розряді. Нехай кортежі B≠D і відрізняються лише в старшому (n-ному) розряді. Позначимо $A^n = <a_n,A^{n-1}>$, $B^n = <b_n,B^{n-1}>$ $D^n = <d_n,D^{n-1}>$. Тоді $B^{n-1} = D^{n-1}$, $b_n \neq d_n$, $A^{n-1} \circ B^{n-1} = A^{n-1} \circ D^{n-1}$, c_{n-1} = const. Для виконання (1) необхідно, щоб

$$F_2(a_n, b_n,const) \neq F_2(a_n, d_n,const) \text{ і}$$
$$F_2(b_n,a_n,const) \neq F_2(d_n, a_n,const)$$

при будь яких a_n та const (a_n , const $\in \{0,1\}$). Звідси випливає, що $F_2(x,y,const) = x+y$, або $F_2(x,y,const) = x+y+1$. Доведення завершено.

Отже можливі лише дві наступні функції F_2 - $F_2(x,y,c)$ = ((x+y) **and not** c) or ((x+y+1) and c)) та $F_2(x,y,c)$ = ((x+y) **and** c) or ((x+y+1) and **not** c)) або $F_2(x,y,c) = x+y+c$ та $F_2(x,y,c) = x+y+c+1$. Але згідно з **Твердженням 1** для цих функцій існують функції F_1, які будуть утворювати тотожній стан, тому в подальшому має сенс розглядати лише одну із них, наприклад $F_2(x,y,c) = x+y+c$. Зауважимо, що в випадку, наприклад,

$F_2(x,y,c)$ = ((x+y) **and** c) or ((x+y) and **not** c))

функція F_2 не буде залежати від c , а ЛМ буде реалізовувати найпростішу операцію.

Наступним кроком є визначення функцій F_1 при яких буде реалізовуватись групова операція. Кількість станів, які необхідно аналізувати зменшилось до 252 (якщо F_1 = const, або F_1 = c, або F_1 = **not** c ЛМ реалізує найпростішу групову операцію).

Нехай n-розрядна операція є груповою. Розглянемо умови, при яких n+1 – розрядна операція також буде груповою. Позначимо

$$Z_1^{n+1} = (X^{n+1} \circ Y^{n+1}) \circ U^{n+1}, \; Z_2^{n+1} = X^{n+1} \circ (Y^{n+1} \circ U^{n+1}),$$
$$Z_1^{n+1} = <z_{n+1}, Z_1^n> , \; Z_2^{n+1} = <z'_{n+1}, Z_2^n>.$$

Оскільки n-розрядна операція є груповою то $Z_1^n = Z_2^n = Z^n$ (див рис.3). Для рівності Z_1^{n+1} та Z_2^{n+1} необхідна і достатня рівність

$$z_{n+1} = z'_{n+1}. \qquad (2)$$

Враховуючи, що згідно з попереднім $F_2(x,y,c)$ = = x+y+c, маємо

$$z_{n+1} = F_2(F_2 (x_{n+1},y_{n+1},p_{11}),u_{n+1},p_{12}) =$$
$$= x_{n+1}+y_{n+1}+p_{11}+u_{n+1}+p_{12}.$$

Аналогічно

$$z'_{n+1} = F_2(x_{n+1}, F_2(y_{n+1},u_{n+1} ,p_{21}), p_{22}) =$$
$$= x_{n+1}+y_{n+1}+p_{21}+u_{n+1}+p_{22}.$$

Для виконання (2) необхідно і достатньо, щоб

$$p_{11}+p_{12}= p_{21}+p_{22}. \qquad (3)$$

при будь яких значеннях X^n,Y^n та U^n

Нехай n=1. Тоді

$p_{11} = F_1(x_1,y_1,c_0)$, $p_{12}=F_1(x_1+y_1+c_0,u_1,c_0)$,

$p_{21} = F_1(y_1, u_1,c_0)$, $p_{22} = F_1(x_1, y_1+u_1+c_0 ,c_0)$.

Маємо

$$F_1(x_1,y_1,c_0) + F_1(x_1+y_1+c_0,u_1,c_0) =$$
$$= F_1(y_1, u_1,c_0) + F_1(x_1, y_1+u_1+c_0 ,c_0). \qquad (4)$$

При c_0 =0 із (4) випливає, що для виконання (3) необхідно, щоб $F_1(0,0,0) = F_1(0,1,0) = F_1(1,0,0)$. Значення $F_1(1,1,0)$ – довільне.

При c_0 =1 із (4) випливає, що для виконання (3) необхідно, щоб $F_1(1,1,1) = F_1(1,0,1) = F_1(0,1,1)$. Значення $F_1(0,0,1)$ – довільне.

Отже, верхня оцінка кількості різних функцій F_1 знизилась до 16, при цьому, як і раніше, в це число входить не менше чотирьох функцій, при яких реалізуються найпростіші операції.

Проводячи аналогічний аналіз для 2-х, 3-х та 4-х КМ ми прийшли до висновку, що бокова функція F_1 для не найпростіших операцій має реалізовувати мажоритарний вентиль (функцію переносу), тобто F_1 (x_i, y_i,c_i) = $x_iy_i \vee x_ic_i \vee y_ic_i$ або його інверсію, тобто F_1 (x_i, y_i,c_i) = not($x_iy_i \vee x_ic_i \vee y_ic_i$). За індукцією цей результат легко довести для будь якої розрядності n.

Таким чином, кількість функцій F_1 зводиться до двох, а, враховуючи різні значення c_0, кількість не простих групових операцій будь-якої розрядності ЛМ зі структурою суматора буде дорівнювати 4.

Слід зазначити, що при $F_2(x,y,c) = x+y+c+1$ будуть реалізовані такі ж самі 4 операції.

5. Аналіз операцій

Запишемо операції звичайної суми та суми з інверсією переносу (позначатимемо «⊙») в рекурентному вигляді.

- для «⊙»: $z_i = x_i \oplus y_i \oplus c_i$, $c_i = \overline{x_i \# y_i \# c_{i-1}}$ (# - мажоранта), i=1..n.

- для «+»: $z_i = x_i \oplus y_i \oplus c_i$, $c_i = x_i \# y_i \# c_{i-1}$ (# - мажоранта), i=1..n.

+ та ⊙ – ізоморфні при всіх n. Доведемо це.

Нехай $X^n = <x_1,x_2,\ldots,x_n>$, позначимо через $W(X^n)$ кортеж, отриманий з X^n інверсією біт з пар-

ними номерами. Відзначимо, що $W: E^n \to E^n$ та $W(W(X^n)) = X^n$.

Покажемо, що $W(X^n) \odot W(Y^n) = W(X^n + Y^n)$. Дійсно (штрихом позначені результати для $\odot$, без штриха – для +):

$$c_0' = c_0 = 0;$$

$$z_1' = x_1 \oplus y_1 \oplus c_0' = x_1 \oplus y_1;$$

$$z_1 = x_1 \oplus y_1 \oplus c_0 = x_1 \oplus y_1; z_1' = z_1;$$

$$c_1' = \overline{x_1 \# y_1 \# c_0'};\ c_1 = x_1 \# y_1 \# c_0;\ c_1' = \overline{c_1};$$

$$z_2' = \overline{x_2} \oplus \overline{y_2} \oplus c_1' = \overline{x_2} \oplus \overline{y_2} \oplus \overline{c_1};$$

$$z_2 = x_2 \oplus y_2 \oplus c_1; z_2' = \overline{z_2};$$

$$c_2' = \overline{\overline{x_2} \# \overline{y_2} \# c_1'} = \overline{\overline{x_2} \# \overline{y_2} \# \overline{c_1}} = x_2 \# y_2 \# c_1;$$

$$c_2 = x_2 \# y_2 \# c_1; c_2' = c_2;$$

…

$$c_{2i}' = c_{2i};$$

$$z_{2i+1}' = z_{2i+1};$$

$$c_{2i+1}' = \overline{c_{2i+1}};$$

$$z_{2i+2}' = \overline{z_{2i+2}}$$ і т.д. до n.

А оскільки $W(W(X^n)) = X^n$, то

$$\forall X^n, Y^n, Z^n \in E^n;$$

$$(X^n + Y^n = Z^n \Leftrightarrow W(X^n) \odot W(Y^n) = W(Z^n)),$$

що є умовою ізоморфності, тобто відповідність $X^n \leftrightarrow W(X^n)$ встановлює ізоморфізм між операціями + та $\odot$.

Для випадку $c_0 = 1$ матимемо додатково операції x+y+1 та $x \odot (y+1)$. Операції x+y(mod n) та x+y+1(mod n) також ізоморфні між собою. Відповідність $x \leftrightarrow x-1$ задає ізоморфізм, оскільки:

$$(x-1)+(y-1)+1(\text{mod n}) = ((x+y)-1)+1(\text{mod n}).$$

Аналогічно для операцій $x \odot (y+1)$ та $x \odot y$.

А оскільки відношення ізоморфності є транзитивним, то ми встановлюємо, що всі чотири операції (а саме: x+y, $x \odot y$, x+y+1 та $x \odot (y+1)$) ізоморфні між собою.

На рис. 2 зображено ЛМ, коли зв'язки між КМ йдуть зліва направо.

Очевидно, що ми отримаємо з точністю до ізоморфізму (достатньо перенумерувати розряди) ті самі операції, що і в випадку ЛМ із зв'язками, які йдуть справа наліво, тобто загальна кількість операцій дорівнює 10. Із 6 простих 4 тотожні раніше розглянутим.

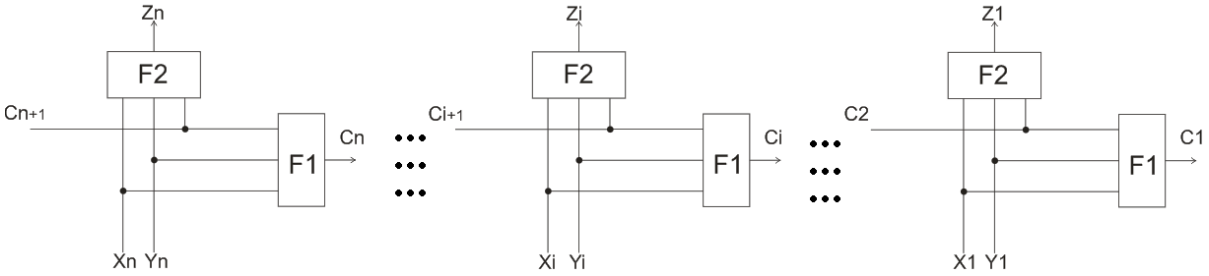

Рис. 2. Зворотній порядок зв'язків

6. Допоміжне положення

Розглянемо як виразиться n+1-розрядна операція ° для трьох операндів через її n-розрядний аналог (рис. 3).

$$(A^{n+1} \circ B^{n+1}) \circ C^{n+1} = (\langle a_{n+1}, A^n \rangle \circ \langle b_{n+1}, B^n \rangle) \circ \langle c_{n+1}, C^n \rangle =$$
$$= \langle F_2(a_{n+1}, b_{n+1}, p_n(A^n, B^n)), A^n \circ B^n \rangle \circ \langle c_{n+1}, C^n \rangle =$$
$$= \langle F_2(F_2(a_{n+1}, b_{n+1}, p_n(A^n, B^n)), c_{n+1},$$
$$p_n(A^n \circ B^n, C^n), (A^n \circ B^n) \circ C^n \rangle; \quad (5)$$

$$A^{n+1} \circ (B^{n+1} \circ C^{n+1}) = \langle a_{n+1}, A^n \rangle \circ (\langle b_{n+1}, B^n \rangle \circ \langle c_{n+1}, C^n \rangle) =$$
$$= \langle a_{n+1}, A^n \rangle \circ (\langle F_2(b_{n+1}, c_{n+1}, p_n(B^n, C^n)), B^n \circ C^n \rangle =$$
$$= \langle F_2(a_{n+1}, F_2(b_{n+1}, c_{n+1}, p_n(B^n, C^n)),$$
$$p_n(A^n, B^n \circ C^n), A^n \circ (B^n \circ C^n) \rangle. \quad (6)$$

Якщо n+1-розрядна операція ° асоціативна, то (5) ≡ (6), тому $(A^n \circ B^n) \circ C^n = A^n \circ (B^n \circ C^n)$, тобто n-розрядна операція ° також є асоціативною. Легко також показати, що, якщо n+1-розрядна операція ° має зворотні та нейтральний елементи, то n- розрядна операція ° також має зворотні та нейтральний елементи (бо молодші розряди не залежать від старших). Фактично це означає, що, якщо n+1-розрядна операція ° є груповою, то і будь-яка її молодша «підоперація» теж групова.

7. Програмний інструмент

Для перевірки теоретичних досліджень було розроблено програмний інструмент, який виконує повний перебір всіх станів ЛМ при фіксованій розрядності. Цей інструмент буде корисним для перевірки теоретичних даних, особливо коли в майбутньому досліджуватимемо складніші структури ЛМ.

Вище було показано, що якщо логічна мережа зі структурою суматора в деякому стані реалізує групову операцію над операндами розрядності n+1, то її молодша частина реалізує групову операцію над операндами розрядності n.

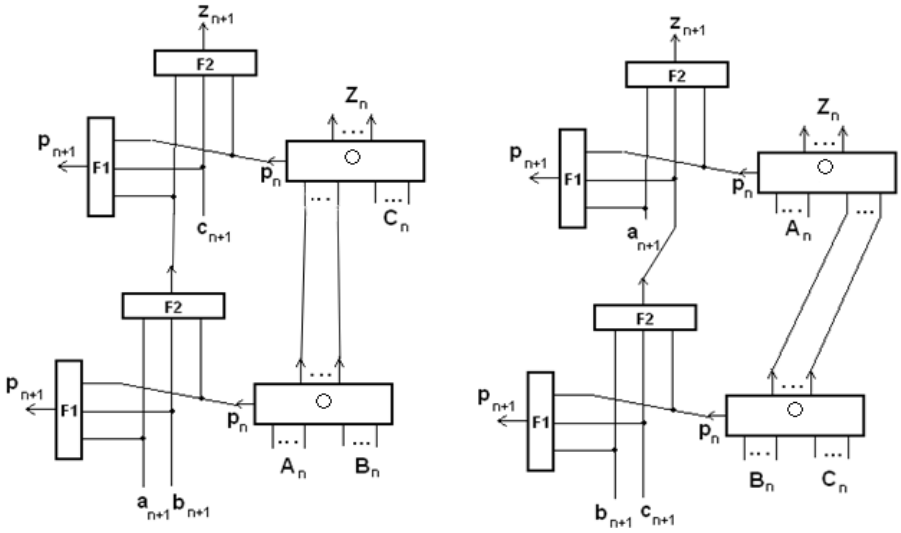

Рис. 3. З'єднання ЛМ для перевірки асоціативності

Звідси випливає коректність наступного алгоритму пошуку групових операцій для цієї ЛМ:

1) n := 1;

2) знайти перебором групові операції розрядності n;

3) n:=n+1, якщо на попередніх двох ітераціях ми отримали однакову кількість операцій, або N перевищило деяке фіксоване значення (захист від зависання), то завершити алгоритм, інакше перейти на 2.

Так ми отримаємо деякий набір операцій, для кожної з яких потрібно виконати дослідження. При більших значеннях N нових операцій не існуватиме.

Звичайно такий перебір (2^{16} варіантів) потрібно виконувати на швидкому комп'ютері.

Швидкість роботи програми

Залежність часу пошуку від розрядності

$$g_{ЗАГ}(n) < 3\times 2^{2r-1} + 2^{3r+2} \sim 4\times 8^{r}.$$

Як бачимо повний перебір є надзвичайно повільним, тому для більш складних випадків необхідно визначити способи скорочення простору перебору.

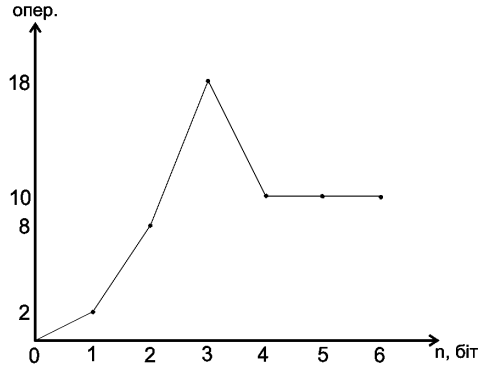

Рис. 4. Кількість операцій

На рис.4 результати кількостей операцій для різних n (не враховуючи ізоморфізм операцій).

В табл.2 наведені, одержані програмним шляхом, пари функцій F_1 та F_2, які задають операції. Операції з номерами 1,2,4,6,8,10 є найпростішими ізоморфними. Операцій 3,5,7,9 ізоморфні сумі. Як бачимо, теоретичні та емпіричні результати співпадають.

Таблиця 2

Результати пошуку групових операцій

№			1		2		3		4		5		6		7		8		9		10	
x_i	y_i	c_i	F_1	F_2	F_1	F_2	F_1	F_2	F_1	F_2	F_1	F_2	F_1	F_2	F_1	F_2	F_1	F_2	F_1	F_2	F_1	F_2
0	0	0	0	0	0	1	**1**	**1**	1	1	**0**	**1**	1	1	**1**	**0**	1	0	**0**	**0**	1	0
0	0	1	0	0	0	0	**1**	**0**	0	0	**0**	**0**	1	0	**1**	**1**	0	1	**0**	**1**	1	1
0	1	0	0	1	0	0	**0**	**0**	1	0	**1**	**0**	1	0	**1**	**1**	1	1	**0**	**1**	1	1
0	1	1	0	0	0	0	**1**	**1**	0	1	**0**	**1**	1	1	**0**	**0**	0	0	**1**	**0**	1	0
1	0	0	0	1	0	0	**0**	**0**	1	0	**1**	**0**	1	0	**1**	**1**	1	1	**0**	**1**	1	1
1	0	1	0	0	0	0	**1**	**1**	0	1	**0**	**1**	1	1	**0**	**0**	0	0	**1**	**0**	1	0
1	1	0	0	0	0	1	**0**	**1**	1	1	**1**	**1**	1	1	**0**	**0**	1	0	**1**	**0**	1	0
1	1	1	0	0	0	0	**0**	**0**	0	0	**1**	**0**	1	0	**0**	**1**	0	1	**1**	**1**	1	1

Висновки

На ЛМ лінійної складності із структурою сумматора при будь якій розрядності більшою за 3 можна реалізувати лише 16 різних групових операцій, 8 із яких є найпростішими та ізоморфні порозрядній операції **xor,** а інші 8 ізоморфні операції додавання по модулю 2^n.

Оскільки ізоморфні перетворення для 6 із 8 операцій потребують при їх реалізації на базі стандартних суматорів додаткових апаратних витрат, то безпосередня реалізація цих 6 операцій на ЛМ може мати практичне значення. Тим більш, що математичні властивості цих операцій аналогічні операції додавання.

Одержані результати є основою для подальших досліджень в напрямку ускладнення структури логічної мережі, наприклад, шляхом використання двонаправлених структур та збільшення розрядності КМ.

Літтература

1. Курош, А.Г. Теория групп [Текст] / А.Г. Курош. – М.: Наука, 1967. – 711 с.

2. Abelian Group [Electronic resource]. – Access mode: http://www.mathworld.wolfram.com/AbelianGroup.html. – 10.03.2012.

3. Conway, J.H. Counting groups: gnus, moas and other exotica [Text] / J.H. Conway, H. Dietrich, E.A. O'Brien // Mathematical Intelligencer. – 2008. – V. 30. – P. 6 – 15.

4. Sims, C.C. Enumerating p–groups [Text] / C.C. Sims // Proc. London Math. Soc. – 1965. – P. 151 – 166.

Надійшла до редакції 12.03.2012

Рецензент: д-р техн. наук, ст. наук. співр. В.М. Опанасенко, Інститут кібернетики ім. В.М. Глушкова, Київ, Україна.

СИНТЕЗ 2-ГРУПП НА ЛОГИЧЕСКИХ ЭЛЕМЕНТАХ

А.К. Тесленко, О.Н. Лавский

Проведен анализ возможности реализации групповых операций над двоичными кортежами произвольной разрядности (2-груп) на логической сети фиксированной структуры линейной сложности и определены логические функции сети. С помощью программного инструментария полученные результаты подтверждены экспериментально. Доказано, что на ЛМ линейной сложности со структурой сумматора при будь какой разрядности большей за 3 можно реализовать лишь 16 разных групповых операций, 8 из которых является самыми простыми и изоморфные поразрядной операции xor, а другие 8 изоморфные операции добавления по модулю 2n.

Ключевые слова: логическая сеть, групповые операции, сумматор, изоморфизм.

SYNTHESIS OF 2-GROUPS ON THE LOGIC ELEMENTS

O.K. Teslenko, O.M. Lavsky

The aim is to determine whether the synthesis of group operations on binary vectors (2 groups) with a fixed structure of the connections between logic elements, which introduce the concepts of the logical network and constructive module. The use of such operations in computer systems can increase the computing speed of various algorithms. With the software tool study the structure of the adder are presented and analyzed the results. It is well-proven that on LM of linear complication with the structure of summator at be what bit after 3 it is possible greater to realize only 16 different group operations, 8 from which is the simplest and isomorphous bit manipulation of xor, and other 8 isomorphous operations of addition on the module of 2n.

Key words: logic network, group operations, adder, an isomorphism.

Теленко Олександр Кирилович – канд. техн. наук, с.н.с, доц. кафедри СКС Національного технічного університету України "Київський політехнічний інститут" e-mail:teslenko@scs.ntu-kpi.kiev.ua.

Лавський Олег Миколайович – магістрант кафедри СКС Національного технічного університету України "Київський політехнічний інститут", e-mail: notiq@yandex.ru.