УДК 638.322

В.П. ТАРАСЕНКО, О.К. ТЕСЛЕНКО, О.Ю. ЯНОВСЬКА

Національний технічний університет України «КПІ», Україна

МОЖЛИВОСТІ НАЙПРОСТІШИХ ДВОНАПРАВЛЕНИХ РЕГУЛЯРНИХ ОДНОВИМІРНИХ КАСКАДІВ КОНСТРУКТИВНИХ МОДУЛІВ ЩОДО РЕАЛІЗАЦІЇ РІЗНИХ ПОВНИХ ПІДСТАНОВОК

Приводяться результати дослідження кількісних показників реалізації підстановок на множині $\{0,1,\ldots,2^n-1\}$ за допомогою регулярної логічної мережі лінійної структури – одновимірного двонаправленого каскаду конструктивних модулів (ОККМ). Розглядається задача дослідження структур найпростіших регулярних двонаправлених ОККМ. На вказаній логічній мережі додатково можуть бути реалізовані повні підстановки будь якої розрядності із значень елементів декількох арифметичних прогресій. При співпадінні значень елементів цих арифметичних прогресій кількість різних підстановок збільшується до максимально можливого значення, яке дорівнює 850.

Ключові слова: *підстановки, логічна мережа, регулярна структура, кількісні характеристики.*

Вступ

З розвитком технології ПЛІС зросла актуальність застосування для комп'ютерних пристроїв базових перетворень інформації та відповідних блоків з параметричним їх налаштуванням. До таких базових перетворень можна віднести підстановки, які досить часто застосовуються в математиці, але в інформаційних технологіях їх застосування обмежується окремими випадками, наприклад, криптографічними перетвореннями. Такий стан зумовлений, насамперед, недостатністю інженерних методик апаратної реалізації підстановок та недостатньо вивченими властивостями підстановок, зокрема підстановок довільної розрядності, які допускають просту реалізацію. Під повною підстановкою, згідно з [1], розуміють підстановку, яка визначена на всіх 2^n значеннях n-розрядного двійкового операнда. Для реалізації підстановок довільної розрядності можна використовувати логічну мережу (мережу із булевих функцій) з лінійною залежністю складності від кількості розрядів – одновимірний каскад конструктивних модулів (ОККМ).

В загальному випадку кожний конструктивний модуль (КМ) каскаду на первинних виходах реалізує m булевих функцій, які репрезентують m поточних розрядів підстановки. Булеві функції на первинних виходах КМ залежать від:

- m булевих змінних, які репрезентують m поточних розрядів аргументу підстановки та подаються на первинні входи КМ,
- k_r булевих змінних, які подаються на k_r правих бокових входів КМ,
- k_l булевих змінних, які подаються на k_l лівих бокових входів КМ.

Крім того, кожний КМ на лівих бокових виходах реалізує k_r булевих функцій, які залежать від m первинних булевих змінних та k_r змінних на правих бокових входах. На правих бокових виходах КМ реалізуються k_l булевих функцій, які залежать від первинних булевих змінних та k_{ll} змінних на лівих бокових входах.

Якщо всі КМ каскаду однакові, то такий каскад називають регулярним. Якщо $k_r = k_l = 1$, то ОККМ називають, простим. Якщо в простому ОККМ для всіх КМ m=1, то такий каскад називають найпростішим. Якщо $k_r \neq 0$ та $k_l \neq 0$, то такий ОККМ називають двонаправленим. Якщо $k_r = 0$ або $k_l = 0$, то такий ОККМ називають однонаправленим. Якщо $k_r = k_l = 0$, то такий каскад називають тривіальним [1]. Зауважимо, що в алгоритмах симетричних криптографічних перетворень DES, AES, ГОСТ 28147-89 для формування багаторозрядних повних підстановок фактично використовуються наступні ОККМ: тривіальні регулярні (m=8, AES), тривіальні нерегулярні (m=4, ГОСТ), прості двонаправлені нерегулярні ОККМ (m=4, DES).

В [2] на основі аналізу каскаду із двох КМ були визначені властивості КМ, які необхідні і достатні для реалізації каскадом повної підстановки. Визначено 6 типів структур КМ позначених як 2а, 3а, 2б, 3б, 2в та 3в. В [3] проаналізовані методи реалізації багаторозрядних повних підстановок на простих ОККМ як ітеративного процесу, де на кожному кроці ітерації ОККМ доповнюється одним КМ. Було показано, що для реалізації багаторозрядних повних

підстановок на кожному кроці ітерації достатньо, щоб КМ, який підключається до ОККМ, мав тип (2а,2а) в відповідний бік.

Постановка задачі дослідження. Далі розглядається задача дослідження структур найпростіших регулярних двонаправлених ОККМ з метою встановлення кількісних характеристик підстановок, які реалізуються такими ОККМ.

1. Основна частина

На рис. 1 показані структура найпростішого регулярного двонаправленого ОККМ та структура КМ. Значення сигналу на первинному виході такого КМ fo залежить від значень сигналів на первинному вході x та на лівому та правому бокових входах h, r. Значення сигналу на лівому боковому виході fr залежить від значення первинної змінної x та від значення сигналу на правому боковому вході r. Відповідно значення на правому боковому виході fh залежить від значення первинної змінної x та від значення на лівому боковому вході h.

Оскільки всі КМ каскаду є однаковими, то для опису кожного КМ i, як наслідок, каскаду в цілому, необхідно застосовувати одну логічну функцію трьох змінних fo(x,h,r) та дві логічні функції двох змінних fr(x,r) та fh(x,h).

Таким чином, кількість різних КМ i, відповідно ОККМ, дорівнює 216, а кількість різних повних підстановок – не більшою за 218 .

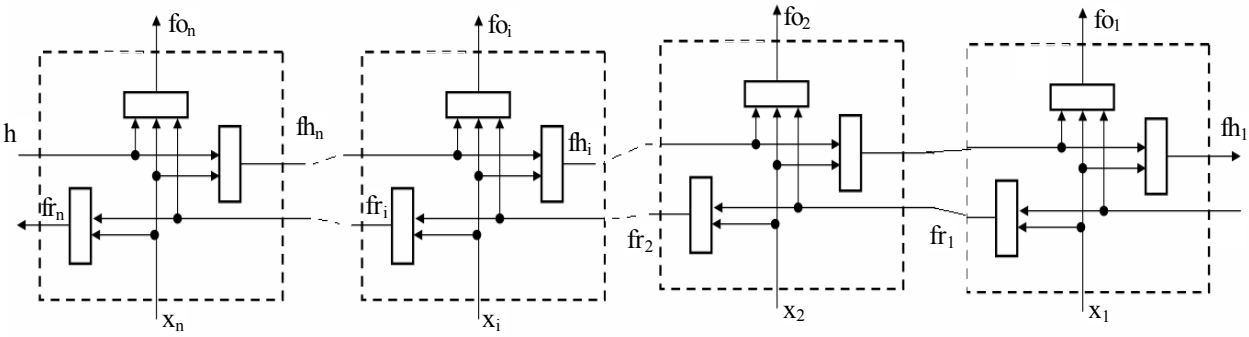

Рис. 1. Структура найпростішого ОККМ

В залежності від комбінації функцій на первинному та бокових виходах КМ характеризується комбінацією лівих та правих типів, які визначають його властивості щодо реалізації на ОККМ повних підстановок.

В табл. 1 показані можливі типи КМ при m=1, де використані наступні позначення:

0, 1 – функції є будь-якими константами (або 0, або 1);

x, $\overline{x}$ - функції є будь- якими не константами (або x, або $\overline{x}$);

0 (1) 0 (1) – функції є одинакові константи;

0 (1) 1 (0) – функції є різні константи;

x($\overline{x}$) x($\overline{x}$) - функції є одинакові не константи;

x($\overline{x}$) $\overline{x}$ (x) - функції є різні не константи.

Отже КМ можна позначать наступним чином:

(ЛТ0, ЛТ1, ПТ0 ПТ1),

де ЛТ0 - лівосторонній тип, при умові, що на правий боковий вхід поступає 0,

ЛТ1 - лівосторонній тип, при умові, що на правий боковий вхід поступає 1,

ПТ0 - правосторонній тип, при умові, що на лівий боковий вхід поступає 0,

ПТ1 – правосторонній тип, при умові, що на лівий боковий вхід поступає 1, наприклад (2а1, 2а2, 2б, 2а1).

Таблиця 1

Можливі типи КМ при m=1

fo(x,0,0)	fo(x,1,0)	fr(x,0)	ЛТ0
fo(x,0,1)	fo(x,1,1)	fr (x,1)	ЛТ1
fo(x,0,0)	fo(x,0,1)	fh(x,0)	ПТ0
fo(x,1,0)	fo(x,1,1)	fh (x,1)	ПТ1
0 , 1	0 , 1	0 , 1	-
0 (1)	0 (1)	x, $\overline{x}$	-
0 (1)	1 (0)	x, $\overline{x}$	Тип 2в
0 , 1	x, $\overline{x}$	0 , 1	-
0 , 1	x, $\overline{x}$	x, $\overline{x}$	-
x, $\overline{x}$	0 , 1	0 , 1	-
x, $\overline{x}$	0 , 1	x, $\overline{x}$	-
x, $\overline{x}$	x, $\overline{x}$	0 , 1	Тип 2а1
x($\overline{x}$)	x($\overline{x}$)	x, $\overline{x}$	Тип 2а2
x($\overline{x}$)	$\overline{x}$ (x)	x, $\overline{x}$	Тип 2б

Для КМ найпростіших ОККМ (m=1) властиве наступне:

- якщо один з типів 2в, то всі інші – також 2в;
- із можливих 3^4 комбінацій типів 2а1,2а2 та

2б не існують наступні 8 комбінацій типів:

(2а2,2а2,2а2,2б), (2а2,2а2,2б,2а2),
(2а2,2б,2а2,2а2), (2б,2а2,2а2,2а2),
(2б,2б,2б,2а2), (2б,2б,2а2,2б),
(2б,2а2,2б,2б), (2а2,2б,2б,2б).

Згідно з [3] для реалізації повних підстановок на двонаправленому простому каскаді достатньо, щоб кожний КМ мав тип (2а, 2а) принаймні в один бік. Це означає, що при обох значеннях змінної на боковому вході r (або h) КМ повинен реалізовувати повні підстановки на множині Q_m всіх можливих значень булевих змінних. При m=1 таких підстановок лише дві – x та not x. Враховуючи значення бокових змінних, виходить, що такі КМ можуть реалізувати 16 різних первинних функцій, що представлені в табл. 2.

Таблиця 2

Перелік первинних функцій КМ при m=1

№ з/п	Повна ДНФ $f_o(x,r,h)$	Можлива мінімізація	Коментар
1	$(\bar{x}\wedge\bar{h}\wedge\bar{r})\vee(\bar{x}\wedge\bar{h}\wedge r)\vee(\bar{x}\wedge h\wedge\bar{r})\vee(\bar{x}\wedge h\wedge r)$	$\bar{x}$	Тривіальна підстановка
2	$(x\wedge\bar{h}\wedge\bar{r})\vee(x\wedge\bar{h}\wedge r)\vee(x\wedge h\wedge\bar{r})\vee(x\wedge h\wedge r)$	x	Тривіальна підстановка
3	$(x\wedge\bar{h}\wedge\bar{r})\vee(x\wedge\bar{h}\wedge r)\vee(\bar{x}\wedge h\wedge\bar{r})\vee(\bar{x}\wedge h\wedge r)$	$(x\wedge\bar{h})\vee(\bar{x}\wedge h)$	Не залежить від r – односторонній каскад
4	$(\bar{x}\wedge\bar{h}\wedge\bar{r})\vee(\bar{x}\wedge\bar{h}\wedge r)\vee(x\wedge h\wedge\bar{r})\vee(x\wedge h\wedge r)$	$(x\wedge h)\vee(\bar{x}\wedge\bar{h})$	Не залежить від r – односторонній каскад
5	$(x\wedge\bar{h}\wedge\bar{r})\vee(\bar{x}\wedge\bar{h}\wedge r)\vee(x\wedge h\wedge\bar{r})\vee(\bar{x}\wedge h\wedge r)$	$(x\wedge\bar{r})\vee(\bar{x}\wedge r)$	Не залежить від h – односторонній каскад
6	$(\bar{x}\wedge\bar{h}\wedge\bar{r})\vee(x\wedge\bar{h}\wedge r)\vee(\bar{x}\wedge h\wedge\bar{r})\vee(x\wedge h\wedge r)$	$(x\wedge r)\vee(\bar{x}\wedge\bar{r})$	Не залежить від h – односторонній каскад
7	$(x\wedge\bar{h}\wedge\bar{r})\vee(\bar{x}\wedge\bar{h}\wedge r)\vee(\bar{x}\wedge h\wedge\bar{r})\vee(\bar{x}\wedge h\wedge r)$	$x+(\bar{h}\wedge\bar{r})+1$	Спряжена з функціями 8, 9, 10
8	$(\bar{x}\wedge\bar{h}\wedge\bar{r})\vee(x\wedge\bar{h}\wedge r)\vee(\bar{x}\wedge h\wedge\bar{r})\vee(\bar{x}\wedge h\wedge r)$	$x+(\bar{h}\wedge r)+1$	Спряжена з функціями 7, 9, 10
9	$(\bar{x}\ \bar{x}\wedge\bar{h}\wedge\bar{r})\vee(\bar{x}\wedge\bar{h}\wedge r)\vee(x\wedge h\wedge\bar{r})\vee(\bar{x}\wedge h\wedge r)$	$x+(h\wedge\bar{r})+1$	Спряжена з функціями 7, 8, 10
10	$(\bar{x}\wedge\bar{h}\wedge\bar{r})\vee(\bar{x}\wedge\bar{h}\wedge r)\vee(\bar{x}\wedge h\wedge\bar{r})\vee(x\wedge h\wedge r)$	$x+(h\wedge r)++1$	Спряжена з функціями 7, 8, 9
11	$(\bar{x}\wedge\bar{h}\wedge\bar{r})\vee(x\wedge\bar{h}\wedge r)\vee(x\wedge h\wedge\bar{r})\vee(x\wedge h\wedge r)$	$x+(\bar{h}\wedge\bar{r})$	Спряжена з функціями 12, 13, 14
12	$(x\wedge\bar{h}\wedge\bar{r})\vee(\bar{x}\wedge\bar{h}\wedge r)\vee(x\wedge h\wedge\bar{r})\vee(x\wedge h\wedge r)$	$x+(\bar{h}\wedge r)$	Спряжена з функціями 11, 13, 14
13	$(x\wedge\bar{h}\wedge\bar{r})\vee(x\wedge\bar{h}\wedge r)\vee(\bar{x}\wedge h\wedge\bar{r})\vee(x\wedge h\wedge r)$	$x+(h\wedge\bar{r})$	Спряжена з функціями 11, 12, 14
14	$(x\wedge\bar{h}\wedge\bar{r})\vee(x\wedge\bar{h}\wedge r)\vee(x\wedge h\wedge\bar{r})\vee(\bar{x}\wedge h\wedge r)$	$x+(h\wedge r)$	Спряжена з функціями 11, 12, 13
15	$(x\wedge\bar{h}\wedge\bar{r})\vee(\bar{x}\wedge\bar{h}\wedge r)\vee(\bar{x}\wedge h\wedge\bar{r})\vee(x\wedge h\wedge r)$	x+h+r	Спряжена з функціями 15 та 16
16	$(\bar{x}\wedge\bar{h}\wedge\bar{r})\vee(x\wedge\bar{h}\wedge r)\vee(x\wedge h\wedge\bar{r})\vee(\bar{x}\wedge h\wedge r)$	x+h+r+1	Спряжена з функціями 15 та 16

Таким чином, кількість різних функцій fo(x,r,h) зменшилась до 10, оскільки при двох із них реалізуються тривіальні підстановки (функція fo(x,r,h) не залежить від r та h), а при 4-х – реалізуються підстановки однонаправленого каскаду (функція fo(x,r,h) не залежить від r або h).

Очевидно, що різні кортежі функцій реалізують різні підстановки, і навпаки - різні підстановки реалізуються різними кортежами. Таким чином, кількість різних підстановок дорівнює кількості різних кортежів функцій. Для визначення кількості різних кортежів функцій, які реалізуються ОККМ, розглянемо поняття спряженого КМ. Нехай один із КМ (позначимо КМ1) реалізує функції fo(x,r,h) та fr(x,r), fh(x,h) а другий (позначимо КМ2) – функції g0(x,r,h) та gr(x,r), gh(x,h). КМ1 та КМ2 будемо називати спряженими, якщо:

$$gr(x,r) = \text{not } fr(x, \text{not } r),$$
$$gh(x,h) = fh(x,h),$$
$$go(x,r,h) = fo(x, \text{not } r, h), \quad (1)$$

або

$$gr(x,r) = fr(x,r),$$
$$gh(x, h) = \text{not } fh(x, \text{not } h),$$
$$go(x,r,h) = fo(x, r, \text{not } h), \quad (2)$$

або

$$gr(x,r) = \text{not } fr(x, \text{not } r),$$
$$gh(x, h) = \text{not } fh(x, \text{not } h),$$
$$go(x,r,h) = fo(x, \text{not } r, \text{not } h)\ . \quad (3)$$

Отже, для одного КМ може існувати 3 спряжені КМ.

ОККМ, побудовані із спряжених КМ будемо називати спряженими. Аналогічно, будемо називати спряженими функції fo(x,r,h) та go(x,r,h), також функції fr(x,r) та gr(x,r), fh(x,h) та gh(x,h).

Якщо ОККМ є спряженими, то вони реалізують однакові підстановки. Доведемо це.

Нехай ОККМ складається з п КМ. Розглянемо функції двох ОККМ, що є спряженими:

$$F(x_n, x_{n-1},\ldots, x_1, r0\ , h0)$$
$$\text{та } G(x_n, x_{n-1},\ldots, x1,\text{not } r0,h0).$$

Співпадіння підстановок можливо лише при умові співпадіння функцій на виходах всіх КМ ОККМ. Розглянемо спочатку функції крайніх КМ

$$fn(x_n,x_{n-1},\ldots,x_1,r0,h0) =$$
$$= fo(x_n,fr(x_{n-1},fr(x_{n-2}\ldots,fr(x_1,r0)\ldots)),h0).$$

Функція спряженого ОККМ

$$gn(x_n, x_{n-1},\ldots, x_1,\text{not } r0,h0) =$$
$$=go(x_n, gr(x_{n-1}, gr(x_{n-2},\ldots gr(x_1,\text{not } r0)\ldots)),h0).$$

Виходячи з (1) маємо

$$gr(x_1,\text{not } r0) = \text{not } fr(x^1, r0),\ gr(x^2,gr(x^1,\text{not } r0)) =$$
$$= gr(x^2, \text{not } fr(x^1, r0)) = \text{not fr } (x^2, fr(x^1, r0)) \text{ і т.д.,}$$

тобто

$$gr(x_{n-1}, gr(x_{n-2},\ldots gr(x_1,\text{not } r0)\ldots))) =$$
$$= \text{not } fr(x_{n-1}, fr(x_{n-2},\ldots fr(x_1,r0)\ldots)),$$

звідси

$$go(xn, \text{not } fr(x_{n-1}, fr(x_{n-2},\ldots fr(x_1,r0)\ldots)), h0) =$$
$$= fo(x_i, fr(x_{i-1}, fr(x_{i-2},\ldots fr(x_1,r0)\ldots)),h0),$$

тобто

$$fn(x_n, x_{n-1},\ldots, x_1,r0,h0) =$$
$$= gn(x_n, x_{n-1},\ldots, x_1,\text{not } r0,h0).$$

Аналогічно для первинної функції іншого крайнього модуля:

$$f1(x_n, x_{n-1},\ldots, x_1,r0,h0) = fo(x_1,h0, fh(x_2, r0, fh(x3,\ldots$$
$$fh(x_n,h0)\ldots))).$$

Функція

$$g1(x_n, x_{n-1},\ldots, x_1,\text{not } r0,h0)=$$
$$= go(x_1, \text{not } r0, gh(x_2, gh(x_3,\ldots gh(x_n,h0)\ldots))).$$

Згідно умови спряженості (1)

$$f1(x_1, \text{not } r0, fh(x_3,\ldots fh(x_n,h0)\ldots))=$$
$$= g1(x_1, \text{not } r0, gh(x_3,\ldots gh(x_n,h0)\ldots))).\ fr(x_1,r0)\ldots)),$$

звідси

$$go(x_n, \text{not } fr(x_{n-1}, fr(x_{n-2},\ldots fr(x_1,r0)\ldots)),$$
$$fh(x_2, fh(x_3,\ldots fh(x_1,\text{not } r0)\ldots))) =$$
$$=fo(x_i, fr(x_{i-1}, fr(x_{i-2},\ldots fr(x_1,r0)\ldots)),$$
$$fh(x_2, fh(x_3,\ldots fh(x_1,\text{not } h0)\ldots))),$$

тобто f

$$i(x_n, x_{n-1},\ldots, x_1,r0,h0) =$$
$$= gn(x_n, x_{n-1},\ldots, x_1,\text{not } r0,h0).$$

Стосовно функцій центральних модулів, то для і-го модуля i=2,…,n-1 маємо

$$fi(x_n, x_{n-1},\ldots, x_i\ldots, x_1,r0\ ,h0) =$$
$$= fo(x_i, fr(x_{i-1}, fr(x_{i-2},\ldots fr(x_1,r0)\ldots)),$$
$$fh(x2, fh(x_3,\ldots fh(x_1,\text{not } r0)\ldots))).$$

Розглянемо функцію

$$gi(x_n, x_{n-1},\ldots, x_1, \text{not } r0, h0) =$$
$$= go(x_n, gr(x_{n-1}, gr(x_{n-2},\ldots gr(x_1,\text{not } r0)\ldots)),$$
$$gh(x_2, gh(x_3,\ldots gh(x_1,h0)\ldots))).$$

Виходячи з (1) маємо

$$gr(x_1,\text{not } r0) = \text{not } fr(x_1, r0),\ gr(x_2,gr(x_1,\text{not } r0)) =$$
$$= gr(x_2, \text{not } fr(x_1, r0)) = \text{not fr } (x_2, fr(x_1, r0)) \text{ і т.д.,}$$

тобто

$$gr(x_{n-1}, gr(x_{n-2},\ldots gr(x_1,\text{not } r0)\ldots))) =$$
$$= \text{not } fr(x_{n-1}, fr(x_{n-2},\ldots fr(x_1,r0)\ldots)),$$

звідси

$$go(xn, \text{not } fr(x_{n-1}, fr(x_{n-2},\ldots fr(x_1,r0)\ldots)),$$
$$fh(x_2, fh(x_3,\ldots fh(x_1,\text{not } r0)\ldots))) =$$
$$fo(x_i, fr(x_{i-1}, fr(x_{i-2},\ldots fr(x_1,r0)\ldots)),$$
$$fh(x_2, fh(x_3,\ldots fh(x_1,\text{not } h0)\ldots))),$$

тобто

$$fi(x_n, x_{n-1},\ldots, x_1,r0,h0) =$$
$$= gn(x_n, x_{n-1},\ldots, x_1,\text{not } r0,h0).$$

Співпадіння функцій спряжених ОККМ згідно (2) і (3) доводиться аналогічно.

Серед визначених (табл. 2) 10 функцій fo(x,r,h) існують два класи функцій, де будь які дві функції із класу спряжені між собою.

До першого класу відносяться функції $x+(\overline{h} \wedge \overline{r})$, $x+(h\wedge \overline{r})$, $x+(h\wedge \overline{r})$ та $x+(h\wedge r)$.

До другого відносяться функції, які є інверсією функцій першого класу. До третього класу функцій віднесемо функції x+h+r і x+h+r+1. Ці функції спряжені самі з собою та спряжені між собою.

Отже, при повному переборі значень бокових змінних (значень налагодження) та повному переборі всіх бокових функцій, які реалізуються на двонаправленому ОККМ, для реалізації всіх повних підстановок достатньо використання лише однієї функції із вказаних трьох класів, тобто кількість різних підстановок не може бути більшою за 3×210. Не порушуючи загальності, виберемо для подальшого аналізу функції

$$fo(x,r,h)= x+(h\wedge r),\ fo(x,r,h)= x+(h\wedge r)+1,$$
$$fo(x,r,h)= x+h+r.$$

Подальше уточнення кількості різних підстановок полягає в обмежені можливих комбінацій бокових функцій та значень бокових змінних. Такі обмеження, перш за все, полягають в забезпеченні реалізації повних підстановок при будь якій кількості КМ в ОККМ, що безумовно може мати місце лише при наявності обох правосторонніх або обох лівосторонніх типів 2а. В табл. 3 та 4 показано всі можливі типи для КМ з вибраними функціями fo(x,r,h) та темним фоном виділені КМ, які не мають вказаної властивості. Звідси випливає, що кількість різних підстановок, які реалізуються на двонаправленому ОККМ суттєво зменшується. Крім того, на підрахунок кількості різних підстановок впливають випадки, коли бокові функції є наступними:

$$fr(x,r)=const,\ fr(x,r) =r,\ fr(x,r) = not\ r,$$
$$fr(x,r) = x,\ fr(x,r) = not\ x\ ,\ fr(x,0) =0,\ fr(x,1) =1.$$

Аналогічно для функцій fh(x,h) . Це ускладнює аналітичне визначення точної оцінки кількості різних підстановок та потребує використання експериментальних даних.

3. Експериментальна частина

Для проведення експериментів був розроблений програмний інструментарій, в якому шляхом повного перебору всіх 2^{16} КМ та чотирьох можливих значень змінних налагодження аналізувалась реалізація повних підстановок на ОККМ, які складались від 2 до 12 КМ. В результаті проведених експериментів встановлено наступне.

Підтверджено наявність спряжених ОККМ та достатність вибору лише трьох функцій $f_o(x,r,h)$ для реалізації повних підстановок при будь якій розрядності.

Загальна кількість підстановок, які реалізуються при будь якій розрядності, дорівнює 814 та розбивається на наступні три групи. До першої із них належать 48 підстановок, які співпадають з підстановками односторонніх каскадів, що з одного боку підтверджує результат, наведений в [4], а з іншого боку підтверджує достовірність результатів програмного інструментарію.

Таблиця 3

Можливі типи КМ з первинними функціями, які належать до первого та другого класів

$f_h(0,x)$	$f_h(1,x)$	$f_r(0,x)$	$f_r(1,x)$	Типи КМ при $f_o(x,r,h)= x+(h\wedge r)$, або $f_o(x,r,h)= x+(h\wedge r)+1$
const	const	const	const	2а1, 2а1, 2а1, 2а1
const	const	const	x, $\overline{x}$	2а1, 2а1, 2а1, 2б
const	const	x, $\overline{x}$	const	2а1, 2а1, 2а2, 2а1
const	const	x, $\overline{x}$	x, $\overline{x}$	2а1, 2а1, 2а2, 2б
const	x, $\overline{x}$	const	const	2а1, 2б, 2а1, 2а1
const	x, $\overline{x}$	const	x, $\overline{x}$	2а1, 2б, 2а1, 2б
const	x, $\overline{x}$	x, $\overline{x}$	const	2а1, 2б, 2а2, 2а1
const	x, $\overline{x}$	x, $\overline{x}$	x, $\overline{x}$	2а1, 2б, 2а2, 2б
x, $\overline{x}$	const	const	const	2а2, 2а1, 2а1, 2а1
x, $\overline{x}$	const	const	x, $\overline{x}$	2а2, 2а1, 2а1, 2б
x, $\overline{x}$	const	x, $\overline{x}$	const	2а2, 2а1, 2а2, 2а1
x, $\overline{x}$	const	x, $\overline{x}$	x, $\overline{x}$	2а1, 2а1, 2а2, 2б
x, $\overline{x}$	x, $\overline{x}$	const	const	2а2, 2б, 2а1, 2а1
x, $\overline{x}$	x, $\overline{x}$	const	x, $\overline{x}$	2а2, 2б, 2а1, 2б
x, $\overline{x}$	x, $\overline{x}$	x, $\overline{x}$	const	2а2, 2б, 2а2, 2а1
x, $\overline{x}$	x, $\overline{x}$	x, $\overline{x}$	x, $\overline{x}$	2а2, 2б, 2а2, 2б

Таблиця 4

Можливі типи КМ з первинними функціями, які належать до третього класу

$f_h(0,x)$	$f_h(1,x)$	$f_r(0,x)$	$f_r(1,x)$	Типи КМ при $f_o(x,r,h)= x+h+r$
const	const	const	const	2а1, 2а1, 2а1, 2а1
const	const	const	x, $\bar{x}$	2а1, 2а1, 2а1, 2б
const	const	x, $\bar{x}$	const	2а1, 2а1, 2б, 2а1
const	const	x, $\bar{x}$	x, $\bar{x}$	2а1, 2а1, 2б, 2б
const	x, $\bar{x}$	const	const	2а1, 2б, 2а1, 2а1
const	x, $\bar{x}$	const	x, $\bar{x}$	2а1, 2б, 2а1, 2б
const	x, $\bar{x}$	x, $\bar{x}$	const	2а1, 2б, 2б, 2а1
const	x, $\bar{x}$	x, $\bar{x}$	x, $\bar{x}$	2а1, 2б, 2б, 2б
x, $\bar{x}$	const	const	const	2б, 2а1, 2а1, 2а1
x, $\bar{x}$	const	const	x, $\bar{x}$	2б, 2а1, 2а1, 2б
x, $\bar{x}$	const	x, $\bar{x}$	const	2б, 2а1, 2б, 2а1
x, $\bar{x}$	const	x, $\bar{x}$	x, $\bar{x}$	2б, 2а1, 2б, 2б
x, $\bar{x}$	x, $\bar{x}$	const	const	2б, 2б, 2а1, 2а1
x, $\bar{x}$	x, $\bar{x}$	const	x, $\bar{x}$	2б, 2б, 2а1, 2б
x, $\bar{x}$	x, $\bar{x}$	x, $\bar{x}$	const	2б, 2б, 2б, 2а1
x, $\bar{x}$	x, $\bar{x}$	x, $\bar{x}$	x, $\bar{x}$	2б, 2б, 2б, 2б

Слід відзначити, що до цієї групи належать підстановки, які реалізуються на таких ОККМ де, принаймні в одному із напрямів, значення на бокових виходах КМ незмінне та дорівнює значенню змінної налагодження, наприклад, при $fr(x,r) =r$. До другої групи належить 190 підстановок, які реалізуються при умові, що в відповідних ОККМ, принаймні в одному із напрямів, значення на бокових виходах КМ незмінне та дорівнює протилежному значенню змінної налагодження. До третьої групи належить 576 підстановок, які можна вважати дійсними підстановками двонаправлених каскадів.

Експериментальні дослідження також показали існування КМ, при з'єднанні яких в ОККМ повні підстановки реалізуються тільки при відповідних значеннях розрядності. Це стосується КМ з типами (2б,2б,2б,2б) або (2в,2в,2в,2в). Так ОККМ на КМ з $f_o(x,r,h)= x+h+r$ і $f_r(x,r) = x$ $f_h(x,h)= x$ або $f_h(x,h)=$not x реалізує повні підстановки при значенні n, які відповідають елементам наступних арифметичних прогресій - $n=3+3\times j$ або $n=4+3\times j$ ($j=0,1,\ldots$), що додає ще 8 оригінальних повних підстановок з указаною розрядністю. КМ з типами (2в,2в,2в,2в) дають можливість реалізовувати ще 28 повних оригінальних підстановок при парних значеннях n або при значеннях n, які відповідають елементам наступних арифметичних прогресій - $n=2+3\times j$ та $3+3\times j$. Загальна кількість різних КМ та відповідно двонаправлених ОККМ, за допомогою яких реалізуються вказані підстановки дорівнює 350.

Висновки

На логічній мережі лінійної складності – найпростіших регулярних двонаправлених каскадах КМ - можна реалізувати 814 різних повних підстановок з будь-якою розрядністю $n \geq 1$. Для реалізації всіх вказаних підстановок достатньо використовувати КМ, в яких на первинному виході із загальної кількості функцій від трьох змінних реалізується лише три різні функції $f_o(x,r,h)$.

Крім того, на вказаній логічній мережі додатково можуть бути реалізовані повні підстановки будь якої розрядності із значень елементів декількох арифметичних прогресій. При співпадінні значень елементів цих арифметичних прогресій кількість різних підстановок збільшується до максимально можливого значення, яке дорівнює 850.

Кількість підстановок, обернені до яких також реалізуються на двонаправлених каскадах, дорівнює 610.

Збільшення більш ніж на порядок кількості підстановок порівняно з їх кількістю для найпростіших регулярних однонаправлених каскадів дозволяє при незначних додаткових апаратних витратах суттєво розширити можливості практичного застосування логічних мереж лінійної складності.

Враховуючи наявність розвинутого апарату алгебри підстановок, напрямком подальших досліджень може бути визначення кількості різних підстановок на логічних мережах прямокутної структури, утворюваних шляхом об'єднання мереж лінійної структури.

Література

1. Тарасенко, В.П. Проблеми апаратної реалізації підстановок [Текст] / В.П. Тарасенко, О.К. Тесленко, О.Ю. Яновська // Наукові записки УНДІЗ. – 2007. – № 2. – С. 52 – 58.

2. Тарасенко, В.П. Реалізація повних підстановок на простому двох модульному каскаді конструктивних модулів [Текст] / В.П. Тарасенко, О.К. Тесленко, О.Ю. Яновська // Інформаційні технології та комп'ютерна інженерія. – 2008. – №1(11). – С. 88 – 97.

3. Тарасенко, В.П. Реалізація повних підстановок за допомогою багатомодульного каскаду найпростіших конструктивних модулів [Текст] / В.П. Тарасенко, О.К. Тесленко, О.Ю. Яновська // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: наук.-техн. зб. Національного технічного університету України «Київський політехнічний інститут». – 2008. – Вип. 2 (17). – С. 49–55.

4. Тарасенко, В.П. Властивості повних підстановок, які реалізуються найпростішим однонаправленим регулярним ОККМ [Текст] / В.П Тарасенко, О.К. Тесленко, О.Ю. Яновська // Радіоелектронні і комп'ютерні системи. – 2010. – №6. – С. 123 – 128.

Надійшла в редакцію 23.02.2012

Рецензент: д-р техн. наук, проф., проф. каф. експериментальних досліджень Є.Т. Володарський, Національний технічний університет України «Київський політехнічний інститут», Київ.

ВОЗМОЖНОСТИ ПРОСТЕЙШИХ ДВУНАПРАВЛЕНЫХ РЕГУЛЯРНЫХ ОДНОМЕРНЫХ КАСКАДОВ КОНСТРУКТИВНЫХ МОДУЛЕЙ ОТНОСИТЕЛЬНО РЕАЛИЗАЦИИ РАЗЛИЧНІХ ПОЛНЫХ ПОДСТАНОВОК

В.П. Тарасенко, А.К. Тесленко, Е.Ю. Яновская

Приводятся результаты исследования количественных характеристик реализации подстановок на множестве $\{0,1,\ldots,2^n-1\}$ с помощью регулярной логической структуры – одномерных двунаправленных каскадах конструктивных модулей (ОККМ). Рассматривается задача исследования структур простых регулярных двунаправленных ОККМ. На указанной логической сети дополнительно могут быть реализованы полные подстановки любой разрядности из значений элементов нескольких арифметических прогрессий. При совпадении значений элементов этих арифметических прогрессий количество различных подстановок увеличивается до максимально возможного значения, которое равна 850.

Ключевые слова: подстановки, логическая сеть, регулярная структура, количественные характеристики.

THE POSSIBILITIES OF THE SIMPLEST TWO-DIRECTIONAL REGULAR ONE-DIMENSIONAL CASCADES OF CONSTRUCTIVE MODULES CONCERNING THE REALIZATION OF THE DIFFERENT COMPLETE PERMUTATIONS

V.P. Tarasenko, O.K. Teslenko, O.Yu. Ianovska

There are represented results concerning the number of different complete permutations on a set $\{0,1,\ldots,2^n-1\}$ realised with help of regular logical structure - one-dimensional cascade of constructive modules (OCCM). The problem of studying the structure of simple regular MRCS. In this logical network can be implemented in addition complete substitution of digits of the values of several elements of arithmetic progressions. If the values match the elements of arithmetic progressions of the various permutations of increases to the maximum possible value, which is equal to 850.

Key words: permutations, logical network, regular structure, quantititve characteristics.

Тарасенко Володимир Петрович – д-р техн. наук, проф., зав. каф. спеціалізованих комп'ютерних систем НТУУ «КПІ», e-mail: vtarasen@scs.ntu-kpi.kiev.ua.

Тесленко Олександр Кирилович – канд. техн. наук, доц. каф. спеціалізованих комп'ютерних систем НТУУ «КПІ», e-mail: teslenko@scs.ntu-kpi.kiev.ua.

Яновська Олена Юріївна – аспірант каф. спеціалізованих комп'ютерних систем НТУУ «КПІ», e-mail: yanovskaya@voliacable.com.