УДК 638.322

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

Національний технічний університет України «КПІ», Київ

ВЛАСТИВОСТІ ПОВНИХ ПІДСТАНОВОК, ЯКІ РЕАЛІЗУЮТЬСЯ НАЙПРОСТІШИМ ОДНОНАПРАВЛЕНИМ РЕГУЛЯРНИМ ОДНОВИМІРНИМ КАСКАДОМ КОНСТРУКТИВНИХ МОДУЛІВ

Приводяться результати дослідження реалізації підстановок на множині {0,1,…,2^n-1} за допомогою регулярної логічної мережі лінійної структури – одновимірних каскадах конструктивних модулів (ОККМ). Показано існування 30 функціонально різних одновимірний каскад конструктивних модулів, на яких реалізуються 48 підстановок при будь яких n>2. Досліджені циклічні властивості вказаних підстановок. Розглянуті та експериментальним шляхом обґрунтовані перспективи застосування одержаних результатів, спрямовані подальші напрямки.

***Ключові слова**: підстановки, логічна мережа, регулярна структура, кількісні характеристики, циклічні властивості, приклади застосування.*

Вступ

З розвитком технології ПЛІС зросла актуальність створення та застосування нових базових перетворень інформації та відповідних параметричних блоків для комп'ютерних пристроїв. До таких базових перетворень можна віднести підстановки, які досить часто застосовуються в математиці, але в інформаційних технологіях їх застосування обмежується окремими випадками, наприклад, в криптографічних перетвореннях. Такий стан речей зумовлений, насамперед, недостатністю методів та 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 числа. Для реалізації підстановок довільної розрядності можна використовувати логічну мережу (мережу із булевих функцій) з лінійною складністю 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 первісних виходах КМ залежать:

– від m булевих змінних, які репрезентують m поточних розрядів аргументу підстановки та подаються на первісні входи КМ;

– від k_r булевих змінних, які подаються на k_r правих бокових входів модуля;

– від k_l булевих змінних, які подаються на k_l лівих бокових входів модуля.

Окрім того, кожний КМ на лівих бокових виходах реалізує k_r булевих функцій, які залежать від m первісних булевих змінних та k_r змінних на правих бокових входах. На правих бокових виходах КМ реалізуються k_l булевих функцій, які залежать від первісних булевих змінних та k_l 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]. Відмітимо, 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. Було 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 шляхом 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 в відповідний бік типи (2а, 2а).

1. Постановка задачі дослідження

Далі розглядається задача дослідження структур найпростіших регулярних однонаправлених ОККМ, кількісних характеристик каскадів, кількісних характеристик та властивостей підстановок, які реалізуються такими ОККМ

2. Основна частина

На рис. 1 приведена структура найпростішого регулярного однонаправленого ОККМ та структура КМ.

Кожний КМ каскаду описується двома логічними функціями від двох змінних – $f_o(x,r)$ $f_r(x,r)$. Для ідентифікації КМ будемо використовувати два десяткові числа, які відповідають двійковому коду значень булевих функцій від двох змінних із таблиць істинності.

Наприклад, нехай $f_o(x,r) = x + r$ (+ – тут і надалі позначення функції xor), $f_r(x,r) = x$ and (not r), тоді відповідний КМ буде позначатись КМ(6,4). Для ідентифікації однонаправленого ОККМ в цілому необхідно вказувати напрям зв'язків між КМ – в бік старших розрядів, наприклад, ОККМ (6,4,с) (як показано на рис. 1), або в бік молодших розрядів – ОККМ(6,4,м).

Для ідентифікації підстановок необхідно до ідентифікатора ОККМ добавити значення змінної r_0 , яку будемо називати змінною налагодження, наприклад, П (6,4,с,0).

Згідно з [3] для реалізації на однонаправленому простому каскаді повних підстановок необхідно і достатньо, щоб кожний КМ в бік зв'язку з попереднім мав типи (2a,2a). Це означає, що при обох значеннях змінної на боковому вході r КМ реалізовував повні підстановки на множині Q_m. При m=1 таких підстановок лише дві – x та not x. Звідси випливає, що можливі лише наступні дві функції $f_o(x,r) = x+r$ та $f_o(x,r) = x+r+1$. Теоретично можливі також функції $f_o(x,r)= x$ та $f_o(x,r)=$ not x, але при цьому ОККМ фактично є тривіальним та може реалізувати при будь яких $f_r(x,r)$ лише наступні підстановки – тотожну підстановку та порозрядну інверсію. Підстановки, які можуть бути реалізовані на тривіальних ОККМ будемо надалі називати тривіальними.

Отже, максимальна кількість різних КМ визначається як 2*16=32, відповідно максимальна кількість різних ОККМ – 64. Кожний з ОККМ реалізує дві підстановки при $r_0=0$ та $r_0=1$, тому максимальна кількість різних підстановок не перевищує 128 при будь яких n. Визначимо реальну кількість різних повних підстановок, які реалізуються на найпростіших однонаправлених регулярних ОККМ. Розглянемо кортеж $<f_n,\ldots,f_i,\ldots,f_2,f_1>$ (впорядкований набір) булевих функцій, які реалізуються на первісних виходах каскаду. В випадку напрямку зв'язків між КМ в сторону старших розрядів маємо кортеж $<f_n(x_n,\ldots,x_1,r_0),\ldots, f_i(x_i,\ldots,x_1,r_0),\ldots, f_2(x_2,x_1,r_0), f_1(x_1,r_0)>$, а в випадку напрямку зв'язків в сторону молодших розрядів – кортеж

$$<f_n(x_n,r_0),\ldots, f_i(x_n,\ldots,x_i,r_0),\ldots,$$
$$f_2(x_n,\ldots,x_2,r_0), f_1(x_n,\ldots,x_1,r_0)>.$$

Два кортежі функцій однакові, якщо однакові функції, які розміщуються в кортежі на однакових позиціях.

Очевидним є наступне твердження.

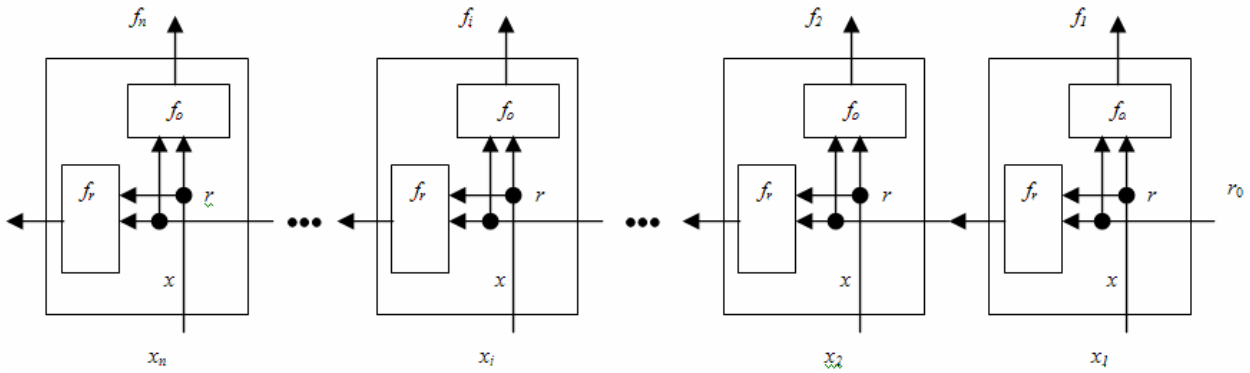

Рис. 1. Найпростіший регулярний однонаправлений ОККМ

Твердження 1. Різні кортежі функцій реалізують різні підстановки, і навпаки - різні підстановки реалізуються різними кортежами.

Із Твердження 1 випливає, що кількість різних підстановок дорівнює кількості різних кортежів функцій. Для визначення кількості різних кортежів функцій, які реалізуються ОККМ, розглянемо поняття спряженості КМ.

Нехай один із КМ (позначимо КМ1) реалізує функції $f_o(x,r)$ та $f_r(x,r)$, а другий (позначимо КМ2) – функції $g_o(x,r)$ та $g_r(x,r)$. КМ1 та КМ2 будемо називати спряженими, якщо

$$g_r(x,r) = \text{not } f_r(x, \text{not } r),\ g_o(x,r) = f_o(x,\text{not } r). \qquad (1)$$

ОККМ, побудовані із спряжених КМ будемо називати спряженими. Аналогічно, будемо називати спряженими функції $f_o(x,r)$ та $g_o(x,r)$, також функції $f_r(x,r)$ та $g_r(x,r)$.

Твердження 2. Якщо два ОККМ є спряженими, то вони реалізують однакові підстановки.

Дійсно, для i=1,2,…,n маємо $f_i(x_i, x_{i-1},\ldots, x_1,r_0) = f_o(x_i, f_r(x_{i-1}, f_r(x_{i-2},\ldots f_r(x_1,r_0)\ldots)))$. Розглянемо функцію $g_i(x_i, x_{i-1},\ldots, x_1,\text{not } r_0) = g_o(x_i, g_r(x_{i-1}, g_r(x_{i-2},\ldots g_r(x_1, \text{not } r_0)\ldots)))$. Виходячи з (1) маємо $g_r(x_1,\text{not } r_0) = \text{not } f_r(x_1, r_0)$, $g_r(x_2,g_r(x_1,\text{not } r_0)) = g_r(x_2, \text{not } f_r(x_1, r_0)) = \text{not } f_r(x_2, f_r(x_1, r_0))$ і т.д., тобто $g_r(x_{i-1}, g_r(x_{i-2},\ldots g_r(x_1, \text{not } r_0)\ldots))) = \text{not } f_r(x_{i-1}, f_r(x_{i-2},\ldots f_r(x_1,r_0)\ldots))$, звідси $g_o(x_i, \text{not } f_r(x_{i-1}, f_r(x_{i-2},\ldots f_r(x_1,r_0)\ldots))) = f_o(x_i, f_r(x_{i-1}, f_r(x_{i-2},\ldots f_r(x_1,r_0)\ldots)))$, тобто

$f_i(x_i, x_{i-1},\ldots, x_1,r_0) = g_i(x_i, x_{i-1},\ldots, x_1,\text{not } r_0)$.

Твердження 3. Серед ОККМ, які розглядаються, відсутні спряжені самі з собою.

Дійсно, дві можливі функції КМ $f_o(x,r) = x + r$ та $f_o(x,r) = x + r+1$ не спряжені самі з собою (але спряжені між собою).

Отже спряжені ОККМ реалізують однакові підстановки при протилежних значеннях r_0, що згідно з Твердженням 3, вдвічі зменшує максимальну оцінку фактично (функціонально) різних ОККМ, тобто 16 при напрямку зв'язків між КМ в бік старших розрядів та 16 – в бік молодших (всього 32). В табл. 1 подано перелік спряжених КМ.

Таблиця 1

Перелік спряжених КМ

КМ(9,0)	КМ(6,15)	$f_r(x,0) = 0$.
КМ(9,1)	КМ(6,13)	
КМ(9,2)	КМ(6,14)	$f_r(x,0) = 0$
КМ(9,3)	КМ(6,12)	
КМ(9,4)	КМ(6,7)	
КМ(9,5)*	КМ(6,5)	
КМ(9,6)	КМ(6,6)	
КМ(9,7)	КМ(6,4)	
КМ(9,8)	КМ(6,11)	$f_r(x,0) = 0$
КМ(9,9)	КМ(6,9)	
КМ(9,10)*	КМ(6,10)	$f_r(x,0) = 0$ $f_r(x,1) = 1$
КМ(9,11)	КМ(6,8)	$f_r(x,1) = 1$
КМ(9,12)	КМ(6,3)	
КМ(9,13)	КМ(6,1)	
КМ(9,14)	КМ(6,2)	$f_r(x,1) = 1$
КМ(9,15)	КМ(6,0)	$f_r(x,1) = 1$

Не порушуючи загальності викладу, КМ з функцією $f_o(x,r) = x + r$ (другий стовпчик табл. 1) в подальшому розглядати не будемо.

Розглянемо КМ з $f_r(x,r) = r$ та $f_r(x,r) = \text{not } r$ (позначені * в табл. 1). ОККМ з таких КМ фактично тривіальні, та реалізують або тотожну підстановку, або підстановки, в яких результат є інверсією парних або непарних розрядів аргументів (підстановки типу «гребінець»), в залежності від r_0. Відповідно будуть функціонально однакові ОККМ зі зв'язками між КМ в різні боки. Таким чином результуюча кількість функціонально різних ОККМ – 30 при всіх n>1, а кількість різних підстановок – не більше 60. Для визначення кількості різних підстановок необхідно врахувати наявність функцій $f_r(x,r)$, які зберігають значення r_0, тобто $f_r(x,r_0) = r_0$. Таких функцій 8, при чотирьох із них ($r_0 =0$) реалізується порозрядна інверсія, при інших чотирьох ($r_0 =1$) – тотожна підстановка. Враховуючи особливості КМ(9,10), із табл. 1 випливає, що кількість різних підстановок, які реалізуються будь якими найпростішими однонаправленими регулярними ОККМ не перевищує 48. До розглянутих раніше тривіальних підстановок (тотожну, порозрядну інверсію та дві типу «гребінець») необхідно додати ще чотири тривіальні підстановки, які реалізуються каскадами із КМ(9,0) або КМ(9,15) – П(9,0,с,1), П(9,0,м,1) П(9,15,с,0) П(9,15,м,0).

Властивості підстановок. Однією з важливих властивостей підстановок є їх циклічність. Наприклад, підстановка П(9,6,с,1) при n=3 має наступні 4 цикли [(1,7,5,3), (2,6),(0),(4)]. Тут і надалі цикли підстановки будемо записувати в круглих дужках, а список циклів – в квадратних. Цикли репрезентують множину пар підстановки, де аргументом пари є будь який елемент циклу, а значенням пари – наступний елемент в списку циклу –значення підстановки на даному аргументі. Наступний елементом для останнього є перший елемент списку. Наприклад, для циклу (1,7,5,3) маємо наступну множину пар підстановки {(1,7),(7,5),(5,3),(3,1)}. Серед циклів можуть бути точки нерухомості – одноелементні цикли, коли аргумент та значення підстановки співпадають. Тотожна підстановка містить лише точки нерухомості, інші тривіальні підстановки містять лише двохелементні цикли при будь яких n.

Теоретичний та практичний інтерес має характер циклічності інших 40 підстановок, в залежності від n. КМ з $f_o(x,r) = x + r+1$ при r=0 має цикл [(0,1)], а при r=1 – цикли [(0,0),(1,1)]. Відповідно існують наступні множини пар підстановки $M_0 = \{(0,1),(1,0)\}$ при r=0 та $M_1 = \{(0,0),(1,1)\}$ при r=1. Нехай при $n \le 1$ ОККМ реалізує підстановку, в якій є цикл $(a_1,a_2,\ldots,a_t)$, $a_i \in Q_n$., i=1,2,…,t. Послідовність бокових значень $(f_{rn}(a_1), f_{rn}(a_2),\ldots, f_{rn}(a_t))$, де f_{rn} – функція на боковому виході ОККМ, розбиває цикл на лан-

цюги – множини зчеплених пар підстановки в межах незмінного значення цієї функції для аргументів пар. Шляхом об'єднання ланцюгів, які утворені одним і тим значенням f_{rn} утворюються множини T_0 та T_1.

Наприклад, для підстановки П(9,6,с,1) при n=3 та циклу (1,7,5,3) маємо наступну послідовність бокових значень (0011) та ланцюги {(1,7),(7,5)}, {(5,3),(3,1)}.

В даному випадку

$$T_0 = \{(1,7),(7,5)\},\ T_1 = \{(5,3),(3,1)\}.$$

Шляхом декартового добутку $M_0 \times T_0$ та $M_1 \times T_1$ формуються ланцюги циклів n+1 – розрядної підстановки.

В даному випадку операція множення – це конкатенація аргументів з аргументами та значень із значеннями двох пар підстановок.

Нехай $\{(a_x,a_{x+1}),(a_{x+1},a_{x+2}),\ldots,(a_{x+y},a_{x+y+1})\}$ – ланцюг із T_1 на у елементів, утворений із циклу $(a_1,a_2,\ldots,a_t)$.

В результаті декартового добутку будуть сформовані наступні ланцюги:

$\{(0a_x,0a_{x+1}),(0a_{x+1},0a_{x+2}),\ldots,(0a_{x+y},0a_{x+y+1})\}$ та

$\{(1a_x,1a_{x+1}),(1a_{x+1},1a_{x+2}),\ldots,(1a_{x+y},1a_{x+y+1})\}$.

Нехай, далі, $\{(a_u,a_{u+1}),(a_{u+1},a_{u+2}),\ldots,(a_{u+y},a_{u+w+1})\}$ ланцюг із T_0 на w елементів. Будуть сформовані наступні ланцюги:

$\{(0a_u,1a_{u+1}),(1a_{u+1},0a_{u+2}),\ldots,(ja_{u+y},ka_{u+w+1})\}$ та

$\{(1a_u,0a_{u+1}),(0a_{u+1},1a_{u+2}),\ldots,(ka_{u+y},ja_{u+w+1})\}$,

де j=1, k=0, якщо w парне та j=0, k=1, якщо непарне.

Не важко бачити, що із одержаних ланцюгів буде створено два цикли довжиною t елементів, якщо кількість нульових значень $f_{rn}(a_i)$ (i=1,2,…,t) парне, або один цикл на t*2 телементів, якщо непарне.

В прикладі, що розглядається, маємо

$$M_0 \times T_0 = \{\{(01,17),(17,05)\},\{(11,07),(07,15)\}\};$$

$$M_1 \times T_1 = \{\{(05,03),(03,01)\},\{(15,13),(13,11)\}\}.$$

Тоді на базі циклу (1,7,5,3) формуються наступні два цикли – (01,17,05,03) та (11,07,15,13).

На основі розглянутого випливає справедливість наступного Твердження 4.

Твердження 4. Всі підстановки, які реалізуються найпростішими однонаправленими регулярними ОККМ при будь яких n мають цикли з довжиною, рівною степеням 2. Подвоєння довжин циклів з ростом n відбувається при умові, що функція на боковому виході ОККМ розбиває цикл підстановки попередньої ітерації на непарні частини.

3. Експериментальна частина

Для підтвердження достовірності одержаних результатів та подальших досліджень експериментальним шляхом, розроблено ряд програмних інструментів.

Перший із них (Regular) шляхом простого перебору всіх можливих КМ та моделювання регулярних ОККМ(с) та ОККМ(м) при $r_0=0$ та $r_0=1$ визначив наявність 48 різних повних підстановок при n>2. При n=2 кількість різних підстановок 12.

Це пояснюється тим, що функція на боковому вході другого КМ фактично залежить від однієї змінної, тому максимальна кількість підстановок – 2*4*2=16.

Маємо 8 кортежів функцій при напрямку зв'язків між КМ в сторону старших розрядів

$$\mathbf{< x_2, x_1>,< x_2+1, x_1>,}< x_2+ x_1, x_1>,$$
$$< x_2+ x_1+1, x_1>, < \mathbf{x_2, x_1+1}>,< x_2+1, x_1+1>,$$
$$< x_2+ x_1, x_1+1>,< x_2+ x_1+1, x_1+1>,$$

та 8 кортежів – в сорону молодших

$$\mathbf{< x_2, x_1>}, < \mathbf{x_2, x_1+1}>,< x_2, x_1+ x_2>,$$
$$< x_2, x_1+ x_2+1>, < \mathbf{x_2+1, x_1}>, < x_2+1, x_1+1>,$$
$$< x_2 +1,x_2+ x_1>,< x_2 +1, x_2+x_1+1>.$$

Чотири кортежі співпадають, що підтверджує експериментальний результат. Встановлено, також, що кількість функціонально різних ОККМ при n>1 дорівнює 30, що відповідає аналітичним результатам.

За допомогою другого програмного інструменту (Cycles) досліджувались циклічні властивості підстановок. Експериментально встановлена достовірність Твердження 4.

Підтверджено припущення, що циклічність підстановок (загальна кількість циклів, та кількість елементів у циклах) не залежить від напрямку зв'язків в ОККМ при одних і тих КМ.

Встановлено наступні особливості нетривіальних підстановок. Ряд підстановок мають цикл довжиною 2^n. Крім загально відомих реалізацій інкременту П(9,11,с,0) (інкременту зі старших розрядів П(9,11,м,0)) та декременту П(9,14,с,0) (декременту зі старших розрядів П(9,11,с,0)) цикл довжиною 2^n мають також наступні підстановки П(9,4,с,0), П(9,1,с,0), П(9,4,м,0), П(9,1,м,0) з більш складною залежністю між вхідними та вихідними значеннями.

Підстановки П(9,4,с,1), П(9,1,с,1), П(9,4,м,1), П(9,1,м,1) мають по два цикли довжиною 2^{n-1} . Ряд підстановок (наприклад П(9,3,с,0), П(9,3,м,0) мають однакову кількістю елементів у всіх циклах, яка поступово (не прямо пропорційно) зростає з ростом n. Ряд підстановок (наприклад П(9,3,с,1), П(9,3,м,1) мають цикли з довжиною всіх степенів 2 із діапазону, який поступово змінюється з ростом n.

Нарешті підстановки П(9,7,с,0), П(9,7,м,0), П(9,7,с,1), П(9,7,м,1),П(9,8,с,1), П(9,8,м,1),П(9,13,с,0), П(9,13,с,1), П(9,13,м,0), П(9,13,м,1) при будь яких n мають цикли довжиною не більше за 2 і не є тривіальними.

Таблиця 2

Таблиця значень від 7 змінних

				x_7	0	0	0	0	1	1	1	1
				x_6	0	0	1	1	0	0	1	1
x_4	x_3	x_2	x_1	x_5	0	1	0	1	0	1	0	1
0	0	0	0		0	1	1	0	1	0	0	1
0	0	0	1		1	0	0	1	0	1	1	0
0	0	1	0		0	0	0	1	0	1	1	0
0	0	1	1		0	1	1	0	1	0	0	1
0	1	0	0		1	0	0	1	0	1	1	0
0	1	0	1		0	0	1	0	1	0	0	1
0	1	1	0		0	1	0	0	1	0	0	1
0	1	1	1		0	0	0	1	0	1	1	0
1	0	0	0		1	0	0	0	0	1	1	0
1	0	0	1		0	1	0	0	1	0	0	1
1	0	1	0		0	0	1	0	1	0	0	1
1	0	1	1		1	0	0	1	0	1	1	0
1	1	0	0		0	1	1	0	1	0	0	1
1	1	0	1		1	0	0	1	0	1	1	0
1	1	1	0		1	0	0	1	0	1	1	0
1	1	1	1		0	0	1	0	1	0	0	1

За допомогою третього програмного інструменту (Min) досліджувались можливості більш ефективної мінімізації логічних функцій в класі ДНФ, при умові попереднього перекодування наборів значень аргументів за допомогою розглянутих ОККМ. Дослідження показали можливість розширення класу логічних функцій, які допускають ефективну мінімізацію.

Наприклад, для функції від 7 змінних, заданою табл. 2 повна, мінімальна та найкоротша ДНФ співпадають, кількість букв – 392, кількість термів – 56. За допомогою розробленого програмного інструментарію Min була виявлена підстановка П(9,3,м,0), при використанні якої результуюча мінімальна ДНФ мала 68 букву, а найкоротша ДНФ – 14 термів.

Підстановка реалізується на ОККМ(9,3,м) при r_0=0. Загальні витрати на реалізацію функції із табл. 2 – 5*7+81 = 116 букв або 7*3+16 = 37 термів.

Отже в результаті використання підстановки маємо виграш в 286 букв або 19 термів.

Мінімізація в класі ДНФ важлива при використанні ПЛІС CPLD.

При використанні ПЛІС FPGA для мінімізації витрат значення має наявність нетривіальних декомпозицій булевих функцій.

За допомогою програмного інструментарію Decomp шляхом повного перебору всіх варіантів розподільної декомпозиції функції із табл. 2 визначено мінімальний коефіцієнт декомпозиції 6 при відділенні змінних x_1,x_2,x_3,x_4.

В разі використання підстановки П(9,9,с,0) мінімальний коефіцієнт декомпозиції – 3 при відділенні змінних x_3,x_4,x_5,x_6.

Висновки

Проведені аналітичні та експериментальні дослідження показали наступне. Існує 30 функціонально різних найпростіших однонаправлених регулярних ОККМ довільної розрядності, які при обох значеннях змінної налагоджування реалізують повні підстановки.

Для кожного із 30 ОККМ існує функціонально тотожний каскад, але побудований із інших (спряжених) модулів, що дає додаткові можливості схемної оптимізації апаратних структур на їх основі.

На найпростіших однонаправлених регулярних ОККМ можна реалізувати 48 різних повних підстановок довільної розрядності n>2.

При n=2 таких підстановок 12. Із 48 підстановок 8 – тривіальні, 40 – не тривіальні. Цикли всіх 48 підстановок мають кількість елементів, яка є степенем 2.

По циклічних властивостях не тривіальні підстановки можна розділити на наступні чотири групи. До першої з них відносяться підстановки з фіксованою (не залежно від n) кількістю циклів та експоненціальною залежністю по кількості елементів в циклі.

До другої групи належать підстановки з фіксованою (не більше 2) кількістю елементів в циклах та експоненціальною залежністю від n по кількості циклів. До цієї групи належать також всі тривіальні підстановки.

До третьої групи належать підстановки з однаковою кількістю елементів у всіх циклах, яка монотонно зростає з ростом n.

До четвертої групи належать підстановки, в яких цикли характеризуються деяким набором значень кількості елементів, а з ростом n спостерігається зростання як кількості циклів, так і кількості елементів у циклах.

Одержані результати мають широкі перспективи практичного застосування. Прикладом може бути розширення класу булевих функцій, які допускають просту реалізацію.

На основі одержаних експериментальних даних можна прогнозувати значний виграш в апаратних витратах з ростом кількості змінних. Вказаний виграш досягається за рахунок збільшення затримки

сигналів, тому найбільш ефективне практичне застосування – при оптимізації проектів по витратах.

Подальші дослідження стосуються як сфер практичного застосування отриманих результатів, так і їх розвиток для простих ОККМ при m = k-1, де k – розрядність LUT ПЛІС FPGA.

Література

1. Тарасенко В.П. Проблеми апаратної реалізації підстановок / 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 / В.П. Тарасенко, О.К. Тесленко, О.Ю. Яновська // Інформаційні технології та комп'ютерна інженерія. –.2008. – №1 (11).

3. Тарасенко В.П. Реалізація повних підстановок за допомогою багатомодульного каскаду найпростіших конструктивних модулів / В.П. Тарасенко, О.К. Тесленко, О.Ю. Яновська // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2008. – Вип. 2 (17).

Надійшла до редакції 2.02.2010

Рецензент: д-р техн. наук О.В. Потій, Харківський національний університет радіоелектроніки, Харків.

СВОЙСТВА ПОЛНЫХ ПОДСТАНОВОК, КОТОРЫЕ РЕАЛИЗУЮТСЯ С ПОМОЩЬЮ ПРОСТЕЙШЕГО ОДНОНАПРАВЛЕННОГО РЕГУЛЯРНОГО КАСКАДА КОНСТРУКТИВНЫХ МОДУЛЕЙ

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

Приводятся результаты исследования реализации подстановок на множестве $\{0,1,\ldots,2^n-1\}$ с помощью регулярной логической сети линейной структуры – одномерного каскада конструктивных (ОККМ). Показано существование 30 функционально различных ОККМ, с помощью которых реализуются 48 подстановок при любых n>2. Исследованы циклические свойства указанных подстановок. Рассмотрены и экспериментально подтверждены перспективы применения полученных результатов.

Ключевые слова: подстановки, логическая сеть, регулярная структура, количественные характеристики, циклические свойства, примеры применения.

PROPERTIES OF COMPLETE PERMUTATIONS, WHICH ARE REALIZED BY MEANS OF THE SIMPLEST REGULAR CASCADE OF CONSTRUCTIVE MODULES

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

There are represented researches results of realization of permutaiotns at a set $\{0,1,\ldots,2^n-1\}$ by means of regular logical linear network, which is one-dimetional cascade of constructive modules (OCCM). It is shown an existence of 30 functionally different OCCMs, realizing 48 permutations in case of any n>2. There are researched cyclic properties of mentioned permutations. There are considered and experimentally proven directions of obtained results application.

Key words: permutations, logical network, regular structure, quantitive characteristics, cyclic properties, application examples.

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

Тесленко Олександр Кирилович – канд. техн. наук, доц. кафедри спеціалізованих комп'ютерних систем, Національний технічний університет України «КПІ», Київ, Україна, e-mail: teslenko@scs.ntu-kpi.kiev.ua.

Яновська Олена Юріївна – аспірант кафедри спеціалізованих комп'ютерних систем, Національний технічний університет України «КПІ», Київ, Україна, e-mail: yanovskaya@voliacable.com.