УДК 638.322

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

Націоанальний технічний університет України «Київський політехнічний інститут», м. Київ

РЕАЛІЗАЦІЯ ОБЕРНЕНИХ ПІДСТАНОВОК НА ПРОСТОМУ ДВОМОДУЛЬНОМУ КАСКАДІ КОНСТРУКТИВНИХ МОДУЛІВ

Анотація. Визначено умови реалізації на простому двомодульному каскаді підстановок, обернених до підстановок, які також реалізуються на на простому двомодульному каскаді. Визначена залежність структур (типів) конструктивних модулів простого двомодульного каскаду, який реалізує обернену підстановку, від структур (типів) конструктивних модулів простого двомодульного каскаду, який реалізує пряму підстановку. Теоретичні результати проілюстровані на прикладах. Важливість одержаних результатів полягає в забезпеченні теоретичної та практичної бази для реалізації прямих та обернених підстановок довільної розрядності на логічних структурах лінійної складності.

Ключові слова. **функціональні перетворення на комбінаційних пристроях, двомодульний каскад, прямі та обернені підстановки, структури конструктивних модулів каскаду.**

Аннотация: определены условия реализации на простом двомодульном каскаде подстановок, обратных к подстановкам, которые также реализуются на простом двомодульном каскаде. Определена зависимость структур (типов) конструктивных модулей простого двухмодульного каскада, который реализует обратную подстановку от структур (типов) конструктивных модулей, которые реализуют прямую подстановку. Теоретические результаты проиллюстрированы на конкретных примерах. Влажность полученных результатов состоит в обеспечении теоретической и практической базы для реализации прямых и обратных подстановок произвольной разрядности на логических структурах линейной сложности.

Ключевые слова: функциональные преобразования на комбинационных устройствах, прямые и обратные подстановки, структуры конструтивных модулей каскада

Abstract. there are defined conditions of relaization of permutation, which are inverse to ones, realized by two-module cascade. It is defined the dependence of the structure (type) of constructive modules of two-module cascade, realizing the inverse permutation on the structure (type) of constructive modules, realizing the direct one. Theoretical results were illustrated with examples. The importance of results obtained lies in provision of theoretical and practice basis for realization of direct and inverse permutations with arbitrary digit capacity using simple logical structures with linear complexity.

Key words: functional transformations using combinational devices, direct and inverse permutations, structure of constructive modules.

Вступ

Розвиток технології ПЛІС (Programmable Logic Devices – PLD) [1,2] призвів до появи можливості реалізації на мікросхемах доволі складних проектів протягом порівняно короткого часу. Це спонукає до пошуку нових методів реалізації засобів для спеціалізованих обчислень, інженерна розробка яких раніше була економічно недоцільною. Подібні обчислення добре відомі, наприклад, з практичного застосування результатів таких розділів математики, як теорія груп та підстановок [3]. Звичайно підстановки визначаються на множині $\mathbf{A} = \{0,1,...,k-1\}$ із k елементів будь якої природи. Якщо $p(x)$ – підстановка на множині $\mathbf{A}$, то обернена підстановка $p^{-1}(x)$ визначається як $p^{-1}(p(x)) = p(p^{-1}(x)) = x.$ За визначенням пряма і обернена підстановки пов'язані властивостями ізоморфізму. Однак ізоморфним підстановкам можуть відповідати їх програмні чи апаратні реалізації, що суттєво відрізняються за своїми основними характеристиками. Тому велике значення має систематизоване дослідження підстановок і, в першу чергу, їх апаратних реалізацій. Результати таких досліджень потенційно можуть мати і теоретичний інтерес, як операційна база відповідних перетворень.

Зауважимо, що ця робота в змістовному відношенні по суті є продовженням роботи [4] і значною мірою використовує науково-поняттєвий доробок, термінологію і позначення попередньої роботи.

Постановка задачі

Реалізація функціональних перетворень за допомогою комбінаційних пристроїв забезпечує максимальну їх продуктивність, але складність реалізації в загальному випадку зростає по експоненті із ростом кількості входів. Оскільки логічні функції часто мають досить велику кількість аргументів, то їх безпосередня реалізація на ПЛІС не завжди можлива. Тому актуальною є задача пошуку часткових рішень, коли складність реалізації підстановок комбінаційними пристроями буде мати поліноміальний характер. Одним із таких рішень є реалізація підстановок за допомогою простих одновимірних каскадів конструктивних модулів (ОККМ) [3]. Такі каскади є комбінаційними пристроями і мають структуру, показану на рис. 1, де X - вектор вхідних первинних змінних, $\mathrm{F}(x)$ - вектор значень первинної вихідної функції, $r_1..r_n$, $h_1..h_n$ - змінні, що подаються відповідно на правий та лівий боковий вхід відповідного модуля, F_r, F_h - ліва та права бокові функції відповідно.

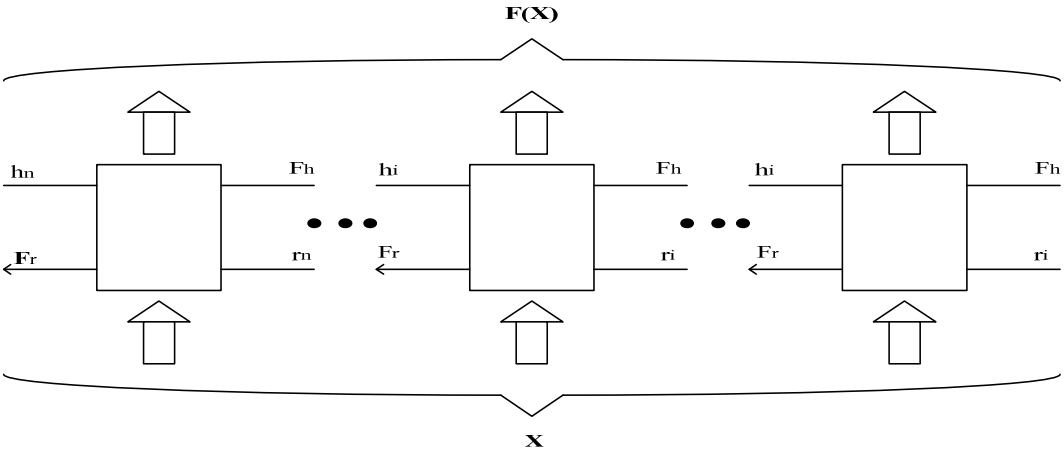

Рисунок 1 – Загальна структура ОККМ

Очевидно, що коли пряма та обернена підстановки реалізуються безпосередньо на ОККМ або, принаймні, на нескладній матричній структурі, то такі підстановки доцільно використовувати в ізоморфних перетвореннях у відповідних алгоритмах для досягнення оптимальних характеристик по певних критеріях. Якщо ж одна із таких підстановок має просту реалізацію, а інша – складну, то вони можуть знайти застосування в криптографічних перетвореннях (односторонні підстановки, односторонні функції). Таким чином, виникає задача визначення, по-перше, можливостей і складності реалізації підстановок, обернених до підстановок, які безпосередньо реалізуються на ОККМ, та, по-друге, структур конструктивних модулів (КМ) для реалізації обернених підстановок на основі відомих структур КМ, які реалізують пряму підстановку [4].

Двомодульний каскад

Структура двомодульного каскаду показана на рис.2. В роботі [4] розглядаються властивості двомодульного каскаду за умови, що каскад в цілому реалізує повну підстановку.

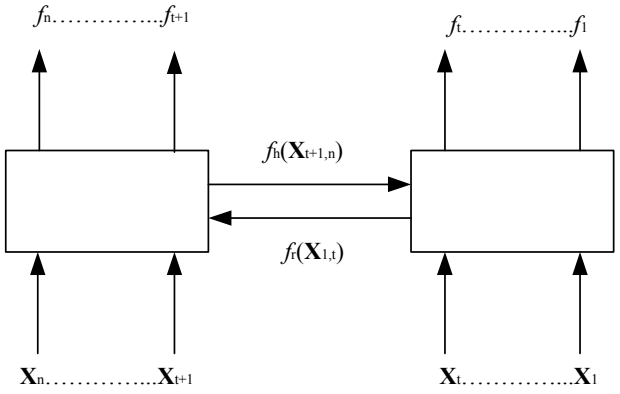

Рисунок 2 – Двомодульний каскад

Позначимо $\mathbf{X}_{1,t}$ кортеж (впорядковану послідовність) аргументів $\langle x_1, x_2, ..x_t \rangle$, що надходять на первинні входи правого модуля ОККМ (молодші розряди аргументу), аналогічно $\mathbf{X}_{t+1,n} \to \langle x_{t+1}, x_{t+2}, ..x_n \rangle$ - кортеж аргументів, що надходять на первинні входи лівого модуля (старші розряди аргументу), $\mathrm{F}_{1,t}$ - кортеж функцій $\langle f_1, f_2, ..f_t \rangle$, що реалізуються на первинних виходах правого модуля ОККМ, аналогічно $\mathbf{F}_{t+1,n} \to \langle f_{t+1}, f_{t+2}, ..f_n \rangle$ - кортеж функцій, що реалізуються на первинних виходах лівого модуля ОККМ, $\mathbf{S}_{1,t}$ – множина кодів значень аргументів із кортежа $\mathbf{X}_{1,t}$, $\mathbf{S}_{t+1,n}$ - множина кодів значень аргументів із $\mathbf{X}_{t+1,n}$.

Значення логічної функції $f\left(\mathbf{X}_{1,t}\right)$ на боковому виході правого модуля поділяє множину $\mathbf{S}_{1,t}$ на дві підмножини $\mathbf{S}_a$ і $\mathbf{S}_b$ так, що для будь-яких значень аргументів $a_1, a_2 \in \mathbf{S}_a \left(a_1 \neq a_2\right)$ значення функції $f_r\left(a_1\right) = f_r\left(a_2\right)$, відповідно $\mathbf{F}_{t+1,n}\left(a_1, \mathbf{X}_{t+1,n}\right) = \mathbf{F}_{t+1,n}\left(a_2, \mathbf{X}_{t+1,n}\right)$, для будь-яких $b_1, b_2 \in \mathbf{S}_b \left(b_1 \neq b_2\right)$ $f_r\left(b_1\right) = f_r\left(b_2\right)$, відповідно $\mathbf{F}_{t+1,n}\left(b_1, \mathbf{X}_{t+1,n}\right) = \mathbf{F}_{t+1,n}\left(b_2, \mathbf{X}_{t+1,n}\right)$, а $\mathbf{F}_{t+1,n}\left(a_1, \mathbf{X}_{t+1,n}\right) \neq \mathbf{F}_{t+1,n}\left(b_1, \mathbf{X}_{t+1,n}\right)$ $\left(f_r\left(a_1\right) \neq f_r\left(b_1\right)\right)$.

Побудуємо наступні множини кодів аргументів із $\mathbf{X} - \mathbf{S}_{ca} = \mathbf{S}_c \times \mathbf{S}_a$, $\mathbf{S}_{da} = \mathbf{S}_d \times \mathbf{S}_a$, $\mathbf{S}_{cb} = \mathbf{S}_c \times \mathbf{S}_b$ та $\mathbf{S}_{db} = \mathbf{S}_d \times \mathbf{S}_b$ як декартові добутки [5] відповідних підмножин. Утворені множини попарно не мають спільних елементів, а їхнє об'єднання дорівнює $\mathbf{S}_{1,n}$ - множині всіх кодів аргументів із $\mathbf{X}$ [4].

Парою підстановки будемо називати впорядковану пару кодів – коду аргументу із $\mathbf{S}_{1,n}$ (або $\mathbf{S}_{t+1,n}$) та коду значень функцій (далі – коду функцій) із кортежу $\mathbf{F}_{1,n}$ (або $\mathbf{F}_{t+1,n}$). Нехай $\mathbf{P}_{ca}^{\wedge}$ - множина пар підстановки з кодами функцій із $\mathbf{F}_{1,t}\left(\mathbf{X}_{1,t}, c\right)$, коли аргументи із $\mathbf{X}_{1,t}$ приймають всі можливі коди із множини $\mathbf{S}_a$, а $\mathbf{T}_{ca}^{\wedge}$ – множина пар підстановки з кодами функцій із $\mathbf{F}_{t+1,n}\left(a, \mathbf{X}_{t+1,n}\right)$, коли аргументи із $\mathbf{X}_{t+1,n}$ приймають всі можливі коди із множини $\mathbf{S}_c$. Аналогічно визначимо множини пар підстановки $\mathbf{P}_{da}^{\wedge}$, $\mathbf{T}_{ad}^{\wedge}$, $\mathbf{P}_{cb}^{\wedge}$, $\mathbf{T}_{bc}^{\wedge}$ та $\mathbf{P}_{db}^{\wedge}$, $\mathbf{T}_{bd}^{\wedge}$. Указані множини пар підстановки однозначно визначають повну підстановку та кортеж функцій $\mathbf{F}\left(\mathbf{X}\right)$, які реалізує двомодульний каскад. Крім того, множини пар підстановок із точністю до інверсії функцій $f_r\left(\mathbf{X}_{1,t}\right)$ та $f_h\left(\mathbf{X}_{t+1,n}\right)$ визначають логічні функції, які реалізуються модулями каскаду.

Відома [4] класифікація модулів двомодульного каскаду за умови, що каскад в цілому реалізує повну підстановку. Модулі можна розділити на 6 типів, досліджуючи властивості множин $\mathbf{P}_{da}^{\wedge}$, $\mathbf{T}_{ad}^{\wedge}$, $\mathbf{P}_{cb}^{\wedge}$, $\mathbf{T}_{bc}^{\wedge}$ та $\mathbf{P}_{db}^{\wedge}$, $\mathbf{T}_{bd}^{\wedge}$. Множини $\mathbf{P}^{\wedge}$ та $\mathbf{T}^{\wedge}$ з однаковим комплектом буквених індексів будемо називати спорідненими. Можливі три варіанти розбиття чотирьох множин кодів функцій на дві пари для забезпечення балансності (врівноваженості) [6]. Перший варіант (а) – $\left(\mathbf{P}_{ca}, \mathbf{P}_{cb}\right)$, $\left(\mathbf{P}_{da}, \mathbf{P}_{db}\right)$. Другий варіант (б) – $\left(\mathbf{P}_{ca}, \mathbf{P}_{da}\right)$, $\left(\mathbf{P}_{cb}, \mathbf{P}_{db}\right)$. Третій варіант (в) - $\left(\mathbf{P}_{ca}, \mathbf{P}_{db}\right)$, $\left(\mathbf{P}_{da}, \mathbf{P}_{cb}\right)$. У кожному із цих варіантів виділимо два випадки наявності спільних елементів, що важливо для забезпечення ортогональності [4]. У першому з них серед чотирьох множин $\mathbf{P}_{ca}, \mathbf{P}_{cb}, \mathbf{P}_{da}, \mathbf{P}_{db}$ кодів функцій існують три множини, які попарно мають спільні елементи (тобто, обов'язково існує множина, яка має спільні елементи із двома іншими). Такі типи конструктивних модулів позначаються цифрою 3. В другому випадку серед множин $\mathbf{P}_{ca}, \mathbf{P}_{cb}, \mathbf{P}_{da}, \mathbf{P}_{db}$ попарно спільні елементи можуть мати тільки дві множини (тобто будь-яка із множин може мати спільні елементи лише з однією з інших). Такі типи конструктивних позначаються цифрою 2. В роботі [4] наведені характеристики конструктивних модулів типів 3а, 3б, 3в, 2а, 2б, 2в. також показано, що не кожна пара типів конструктивних модулів є сумісною (тобто реалізує повну підстановку), а тільки : (3а-2а), (3б-2в), (3в-2б), (2а-2а), (2а-2б), (2б-3в), (2б-2в), (2в-2б), (2в-2в). При цьому сумісність має симетричний характер, тобто неважливо, який із модулів буде зліва (старші розряди), а який справа (молодші розряди).

Реалізація обернених підстановок

Розглянемо тепер реалізацію обернених підстановок за допомогою двомодульного ОККМ. Кортеж $\mathbf{G}\left(\mathbf{X}\right)$ реалізує обернену підстановку, якщо $\mathbf{G}\left(\mathbf{F}\left(\mathbf{X}\right)\right) = \mathbf{X}$.Оскільки аргументи множини $\mathbf{X}$ та значення кортежів $\mathbf{G}$ та $\mathbf{F}$ функцій приймають всі значення із множини $\mathbf{S}_{1,n}$, то формування кортежу $\mathbf{G}$ можна однозначно виконати наступним чином. Нехай для будь якого $\mathbf{S} \in \mathbf{S}_{1,n} r = \mathbf{F}\left(s\right)$, тоді $\mathbf{G}(r) = s$.

Згідно з [4], реалізація прямої підстановки на простому двомодульному каскаді характеризується наступними множинами пар підстановки: $\mathbf{M}^{\wedge}_{ca} = \mathbf{T}^{\wedge}_{ac} \times \mathbf{P}^{\wedge}_{ca}$, $\mathbf{M}^{\wedge}_{da} = \mathbf{T}^{\wedge}_{ad} \times \mathbf{P}^{\wedge}_{da}$, $\mathbf{M}^{\wedge}_{cb} = \mathbf{T}^{\wedge}_{bc} \times \mathbf{P}^{\wedge}_{cb}$, $\mathbf{M}^{\wedge}_{db} = \mathbf{T}^{\wedge}_{bd} \times \mathbf{P}^{\wedge}_{db}$. В свою чергу множини пар підстановки $T^{\wedge}$ та $P^{\wedge}$ можна подати наступним чином:

$$\begin{aligned}
&\mathbf{T}^{\wedge}_{ac} = \left(\langle \mathbf{S}_c \rangle, \langle \mathbf{T}_{ac} \rangle\right), \mathbf{T}^{\wedge}_{ad} = \left(\langle \mathbf{S}_d \rangle, \langle \mathbf{T}_{ad} \rangle\right),\\
&\mathbf{T}^{\wedge}_{bc} = \left(\langle \mathbf{S}_c \rangle, \langle \mathbf{T}_{bc} \rangle\right), \mathbf{T}^{\wedge}_{bd} = \left(\langle \mathbf{S}_d \rangle, \langle \mathbf{T}_{bd} \rangle\right),\\
&\mathbf{P}^{\wedge}_{ca} = \left(\langle \mathbf{S}_a \rangle, \langle \mathbf{P}_{ca} \rangle\right), \mathbf{P}^{\wedge}_{da} = \left(\langle \mathbf{S}_a \rangle, \langle \mathbf{P}_{da} \rangle\right),\\
&\mathbf{P}^{\wedge}_{db} = \left(\langle \mathbf{S}_b \rangle, \langle \mathbf{P}_{db} \rangle\right), \mathbf{P}^{\wedge}_{cb} = \left(\langle \mathbf{S}_b \rangle, \langle \mathbf{P}_{cb} \rangle\right),
\end{aligned} \tag{1}$$

де використання кутових дужок вказує на взаємну впорядкованість елементів множин $\mathbf{T}$ і $\mathbf{S}$ та $\mathbf{P}$ і $\mathbf{S}$ у відповідності до $\mathbf{F(X)}$.

Очевидно, що обернена підстановка буде характеризуватись наступними множинами пар підстановки
$\mathbf{M}^{\wedge 0}_{ca} = \mathbf{T}^{\wedge 0}_{ac} \times \mathbf{P}^{\wedge 0}_{ca}, \mathbf{M}^{\wedge 0}_{da} = \mathbf{T}^{\wedge 0}_{ad} \times \mathbf{P}^{\wedge 0}_{da}, \mathbf{M}^{\wedge 0}_{cb} = \mathbf{T}^{\wedge 0}_{bc} \times \mathbf{P}^{\wedge 0}_{cb}, \mathbf{M}^{\wedge 0}_{db} = \mathbf{T}^{\wedge 0}_{bd} \times \mathbf{P}^{\wedge 0}_{db}$, де коди аргументів та коди значень функцій міняються місцями:

$$\begin{aligned}
&\mathbf{M}^{0}_{ca} = \mathbf{T}^{0}_{ac} \times \mathbf{P}^{0}_{ca} = \left(\langle \mathbf{T}_{ac} \rangle, \langle \mathbf{S}_c \rangle\right) \times \left(\langle \mathbf{P}_{ca} \rangle, \langle \mathbf{S}_a \rangle\right),\\
&\mathbf{M}^{0}_{da} = \mathbf{T}^{0}_{ad} \times \mathbf{P}^{0}_{da} = \left(\langle \mathbf{T}_{ad} \rangle, \langle \mathbf{S}_d \rangle\right) \times \left(\langle \mathbf{P}_{da} \rangle, \langle \mathbf{S}_a \rangle\right),\\
&\mathbf{M}^{0}_{cb} = \mathbf{T}^{0}_{bc} \times \mathbf{P}^{0}_{cb} = \left(\langle \mathbf{T}_{bc} \rangle, \langle \mathbf{S}_c \rangle\right) \times \left(\langle \mathbf{P}_{cb} \rangle, \langle \mathbf{S}_b \rangle\right),\\
&\mathbf{M}^{0}_{ad} = \mathbf{T}^{0}_{bd} \times \mathbf{P}^{0}_{db} = \left(\langle \mathbf{T}_{bd} \rangle, \langle \mathbf{S}_d \rangle\right) \times \left(\langle \mathbf{P}_{db} \rangle, \langle \mathbf{S}_b \rangle\right).
\end{aligned} \tag{2}$$

Вияснимо факт існування наступних спільних декомпозицій кортежів функцій $\mathbf{G}_{t+1,n}(\mathbf{X})$ та $\mathbf{G}_{1,t}(\mathbf{X})$:

$$\mathbf{G}_{t+1,n}(\mathbf{X}) = \mathbf{G}_{t+1,n}\left(\mathbf{X}_{t+1,n}, f'_r\left(\mathbf{X}_{1,t}\right)\right) \tag{3}$$

$$\mathbf{G}_{1,t}(\mathbf{X}) = \mathbf{G}_{1,t}\left(f'_h\left(\mathbf{X}_{t+1,n}\right), \mathbf{X}_{1,t}\right) \tag{4}$$

Розглянемо спільну декомпозицію (3). Коди аргументів в (2) згідно з визначенням – це коди значень функцій в (1). В свою чергу, згідно з [4], множини кодів функцій $\mathbf{P}_{ca}$, $\mathbf{P}_{da}$, $\mathbf{P}_{cb}$ та $\mathbf{P}_{db}$ розбиваються на дві пари таким чином, щоб множини, які належать одній парі не мали спільних елементів і були доповненням одна одній до множини $\mathbf{S}_{1,t}$. Утворимо попарні перетини цих множин, тобто $\mathbf{A}_1 = \mathbf{P}_{ca} \cap \mathbf{P}_{da}$, $\mathbf{A}_2 = \mathbf{P}_{ca} \cap \mathbf{P}_{cb}$, $\mathbf{A}_3 = \mathbf{P}_{ca} \cap \mathbf{P}_{db}$, $\mathbf{A}_4 = \mathbf{P}_{da} \cap \mathbf{P}_{cb}$, $\mathbf{A}_5 = \mathbf{P}_{da} \cap \mathbf{P}_{db}$, $\mathbf{A}_6 = \mathbf{P}_{cb} \cap \mathbf{P}_{db}$. Очевидно, що $\mathbf{A}_i \cap \mathbf{A}_j = \varnothing,\ j = 1,2,...,6, i \neq j$, $\mathbf{A}_1 \cup \mathbf{A}_2 \cup \mathbf{A}_3 \cup \mathbf{A}_4 \cup \mathbf{A}_5 \cup \mathbf{A}_6 = \mathbf{S}_1$. Крім того, дві із шести множин $\mathbf{A}_i$ обов’язково будуть пустими, тобто в загальному випадку непустих множин $\mathbf{A}_i$ не більше 4. Враховуючи, що в ОККМ типу 2 існують пари співпадаючих множин, то в цьому випадку кількість непустих множин $\mathbf{A}_i$ лише 2.

Твердження 1. Нехай $r_1, r_2 \in \mathbf{A}_i (r_1 \neq r_2, \mathbf{A}_i \neq \varnothing)$. Тоді

$$\mathbf{G}_{t+1,n}\left(\mathbf{X}_{t+1,n}, r_1\right) = \mathbf{G}_{t+1,n}\left(\mathbf{X}_{t+1,n}, r_2\right) \tag{5}$$

Згідно з визначенням множин пар підстановки рівність (5) справедлива для будь яких $r_1 \neq r_2$, які містяться в одній із множин $\mathbf{P}$, за умови, що змінні із $\mathbf{X}_{t+1,n}$ є значенням кодів функцій із спорідненої

множини $\mathbf{T}$. Якщо множина $\mathbf{A}_i$ непуста, то це означає, що відповідні множини $\mathbf{P}$ мають спільні елементи, але тоді, згідно з [4], споріднені множини $\mathbf{T}$ не мають спільних елементів і доповняють одна одну до множини $\mathbf{S}_{t+1,n}$. Це означає, що рівність (5) справедлива на всіх значеннях змінних із $\mathbf{X}_{t+1,n}$ для будь яких $r_1, r_2 \in \mathbf{A}_i \left(r_1 \neq r_2\right)$. Твердження доведено. Аналогічно для кортежу $\mathbf{G}_{1,t}(\mathbf{X})$ (4).

Із твердження 1 випливає, що коефіцієнти спільних декомпозицій кортежів $\mathbf{G}_{t+1,n}(\mathbf{X})$ та $\mathbf{G}_{1,t}(\mathbf{X})$ принаймні не перевищують кількості не пустих множин $\mathbf{A}_i$. В свою чергу, в ОККМ, які належать до типу 3 (3а, 3б, 3в), кількість непустих множин $\mathbf{A}_i$ дорівнює 3 або 4, а в ОККМ типу 2 (2а, 2б, 2в) – дорівнює 2.

Отже в загальному випадку на простому двомодульному каскаді можуть бути реалізовані підстановки, обернені до підстановок, які реалізуються лише на КМ типу 2.

Розглянемо визначення структур КМ для реалізації обернених підстановок на основі відомих структур КМ, які реалізують пряму підстановку.

Для визначеності будемо розглядати КМ, які використовуються в молодших розрядах двомодульного каскаду, де будь який із них подається наступними множинами пар підстановки $\mathbf{P}^{\wedge}_{ca}$, $\mathbf{P}^{\wedge}_{da}$, $\mathbf{P}^{\wedge}_{db}, \mathbf{P}^{\wedge}_{cb}$. Згідно з попереднім маємо:

$$\mathbf{P}^{\wedge 0}_{ca} = \left(\left\langle P_{ca}\right\rangle, \left\langle S_a\right\rangle\right), \mathbf{P}^{\wedge 0}_{da} = \left(\left\langle P_{da}\right\rangle, \left\langle S_a\right\rangle\right),$$
$$\mathbf{P}^{\wedge 0}_{cb} = \left(\left\langle P_{cb}\right\rangle, \left\langle S_b\right\rangle\right), \mathbf{P}^{\wedge 0}_{db} = \left(\left\langle P_b\right\rangle, \left\langle S_b\right\rangle\right). \quad (6)$$

Враховуючи симетричність при під'єднанні модулів КМ різних типів в двомодульний каскад, одержані результати для КМ в молодших розрядах легко узагальнюються і для КМ в старших розрядах.

Розглянемо КМ типу 2а, який характеризується наступною структурою:

$$\mathbf{P}_{ca} \cap \mathbf{P}_{cb} = \varnothing,\ \mathbf{P}_{ca} \cup \mathbf{P}_{cb} = \mathbf{S}_{1,t};$$
$$\mathbf{P}_{da} \cap \mathbf{P}_{db} = \varnothing,\ \mathbf{P}_{ca} \cup \mathbf{P}_{db} = \mathbf{S}_{1,t};$$
$$\mathbf{P}_{ca} = \mathbf{P}_a \text{ і } \mathbf{P}_{cb} = \mathbf{P}_{db}$$
$$f_r(\mathbf{S}_a) = a,\ \ f_r(\mathbf{S}_b) = b,\ \ a, b \in \{0,1\}, a \neq b$$

Згідно (6)

$$\mathbf{P}^0_{ca} = \mathbf{P}^0_{da} = \mathbf{S}_a,\ \mathbf{S}^0_a = \mathbf{P}^0_{ca} = \mathbf{P}_{da},\ \mathbf{P}^0_{cb} = \mathbf{P}^0_{db} = \mathbf{S}_b,\ \mathbf{S}^0_b = \mathbf{P}_{cb} = \mathbf{P}_{db}.$$

Маємо:

$$\mathbf{P}^0_{ca} \cap \mathbf{P}^0_{cb} = \varnothing,\ \mathbf{P}^0_{ca} \cup \mathbf{P}^0_{cb} = \mathbf{S}_{1,t};$$
$$\mathbf{P}^0_{da} \cap \mathbf{P}^0_{cb} = \varnothing,\ \mathbf{P}^0_{da} \cup \mathbf{P}^0_{db} = \mathbf{S}_{1,t};$$
$$\mathbf{P}^0_{ca} = \mathbf{P}^0_{da} \text{ і } \mathbf{P}^0_{cb} = \mathbf{P}^0_{db};$$
$$f^0_r(\mathbf{S}^0_a) = a,\ \ f^0_r(\mathbf{S}^0_b) = b,\ \ a, b \notin \{0,1\}, a \neq b$$

Отже для реалізації оберненої підстановки КМ типу 2а перетворюються в КМ також типу 2а. КМ для реалізації обернених підстановок будемо в подальшому називати оберненим КМ.

Розглянемо приклад. Нехай n=5, t=3. В табл. 1 та в табл. 2 задано відповідні КМ, а в табл. 3 – підстановка, яка реалізується двомодульним каскадом.

Таблиця 1 – КМ для молодших розрядів

f_r	1	1	1	1	1	0	0	1
$\mathbf{F}_{1,3}$ при f_h=0	4	7	5	6	3	1	0	2
$\mathbf{F}_{1,3}$ при f_h=1	2	4	3	5	7	0	1	6
X	0	1	2	3	4	5	6	7

$$\mathbf{S}_{a(a=0)} = \{5,6\},\ \mathbf{S}_{b(b=0)} = \{0,1,3,4,7\},$$
$$\mathbf{P}_{ca(c=0,a=0)} = \mathbf{P}_{da(d=1,a=0)} = \{1,0\},$$
$$\mathbf{P}_{cb(c=0,b=1)} = \mathbf{P}_{ab(d=1,b=1)} = \{2,3,4,5,6,7\},$$
$$\mathbf{P}^{\wedge}_{ca} = \langle\{5,6\},\{1,0\}\rangle, \mathbf{P}^{\wedge}_{da} = \langle\{5,6\},\{0,1\}\rangle, \mathbf{P}^{\wedge}_{cb} = \langle\{0,1,2,3,4,7\},\{4,7,5,6,3,2\}\rangle,$$
$$\mathbf{P}^{\wedge}_{db} = \langle\{0,1,2,3,4,7\},\{2,4,3,5,7,6\}\rangle$$

Таблиця 2 – КМ для старших розрядів

f_h	1	0	1	1
$\mathbf{F}_{4,5}$ при f_r=0	3	0	1	2
$\mathbf{F}_{4,5}$ при f_r=1	2	0	3	1
X	0	1	2	3

$$\mathbf{S}_{c(c=0)} = \{1\},\ \mathbf{S}_{d(d=1)} = \{0,2,3\},$$
$$\mathbf{T}_{ac(c=0,a=0)} = \mathbf{T}_{bc(d=1,a=0)} = \{0\},$$
$$\mathbf{T}_{ad(c=0,b=1)} = \mathbf{T}_{db(d=1,b=1)} = \{3,1,2\},$$
$$\mathbf{T}^{\wedge}_{ac} = \mathbf{T}^{\wedge}_{bc}\langle\{1\},\{0\}\rangle, \mathbf{T}^{\wedge}_{ad} = \langle\{0,2,3\},\{3,1,2\}\rangle, \mathbf{T}^{\wedge}_{bd} = \langle\{0,2,3\},\{2,3,1\}\rangle,$$

Таблиця 3 – Пряма підстановка

F(X)=	22	24	23	25	27	30	31	26	04	07	05	06	03	01	00	02
X=	00	01	02	03	04	05	06	07	10	11	12	13	14	15	16	17
F(X)=	32	34	33	35	37	10	11	36	12	14	13	15	17	20	21	16
X=	20	21	22	23	24	25	26	27	30	31	32	33	34	35	36	37

Розглянемо формування КМ для оберненої підстановки. Обернений КМ для молодших розрядів.

$$\mathbf{P}^{0}_{ca} = \mathbf{P}^{0}_{da} = \mathbf{S}_a = \{5,6\},$$
$$\mathbf{S}^{0}_{a} = \mathbf{P}_{ca} = \mathbf{P}_{da} = \{1,0\},$$
$$\mathbf{P}^{0}_{cb} = \mathbf{P}^{0}_{ab} = \mathbf{S}_b = \{0,1,2,3,4,7\},$$
$$\mathbf{S}^{0}_{b} = \mathbf{P}_{cb} = \mathbf{P}_{cb} = \{2,3,4,5,6,7\},$$
$$\mathbf{P}^{\wedge 0}_{ca} = \langle\{1,0\},\{5,6\}\rangle, \mathbf{P}^{\wedge 0}_{da} = \langle\{0,1\},\{5,6\}\rangle, \mathbf{P}^{\wedge 0}_{cb} = \langle\{4,7,5,6,3,2\},\{0,1,2,3,4,7\}\rangle.$$

Звідси випливає наступна структура (табл. 4).

Таблиця 4 – Структура оберненого КМ для молодших розрядів

f^{0}_{r}	0	0	1	1	1	1	1	1
$\mathbf{G}_{1,3}$ при $f^{0}_{h} = 0$	6	5	7	4	0	2	3	1
$\mathbf{G}_{1,3}$ при $f^{0}_{h} = 1$	5	6	0	2	1	3	7	4
X	0	1	2	3	4	5	6	7

Обернений КМ для старших розрядів:

$$\mathbf{S}^{0}_{c(c=0)} = \{0\}, \mathbf{S}^{0}_{d(d=1)} = \{1,2,3\},$$
$$\mathbf{T}^{0}_{ac(c=0,b=1)} = \mathbf{T}^{0}_{bc(d=1,a=1)} = \{1\},$$

$$\mathbf{T}^0_{ad(c=0,b=1)} = \mathbf{T}^0_{bd(d=1,b=1)} = \{0,2,3\},$$

$$\mathbf{T}^{\wedge 0}_{ac} = \mathbf{T}^{\wedge 0}_{bc} = \langle\{0\},\{1\}\rangle, \mathbf{T}^{\wedge 0}_{ad} = \langle\{3,1,2\},\{0,2,3\}\rangle, \mathbf{T}^{\wedge 0}_{bd} = \langle\{2,3,1\},\{0,2,3\}\rangle.$$

Звідси випливає наступна структура (табл. 5)

Таблиця 5 – Структура оберненого КМ для старших розрядів

f^0_h	0	1	1	1
$G_{4,5}$ при $f^0_r = 0$	1	2	3	0
$G_{4,5}$ при $f^0_r = 1$	1	3	0	2
X	0	1	2	3

Таблиця 6 – Обернена підстановка

G(**X**) =	16	15	17	14	10	12	13	11	25	26	30	32	31	33	37	34
X =	00	01	02	03	04	05	06	07	10	11	12	13	14	15	16	17
G(**X**) =	35	36	00	02	01	03	07	04	05	06	20	22	21	23	27	24
X =	20	21	22	23	24	25	26	27	30	31	32	33	34	35	36	37

Аналогічно попередньому, шляхом простого перейменування кодів функцій та кодів аргументів в множинах пар підстановок, КМ, обернений до КМ типу 2б може мати тип 2б або 2в. , а КМ, обернений до КМ типу 2в може мати тип 2в або 2б. Конкретний тип оберненого КМ, в цьому випадку, залежить від типу другого КМ двомодульного каскаду, який реалізує пряму підстановку. Так, для типів (2а-2б) прямої підстановки, обернена підстановка відповідає типам (2а-2б), для типів (2б-2в) – типи (2в-2б), для типів (2в-2в) – типи (2в-2в).

Розглянемо окремі випадки для КМ типу 3. Згідно з попереднім, для КМ типу 3 існують 3 або 4 непусті множини $\mathbf{A}_i (i = 1,2,...,6)$. Розглянемо, при яких умовах можливе об'єднання множин $\mathbf{A}_i$, $\mathbf{A}_j$, ($i \neq j$) в один клас по спільній декомпозиції виду (3). Нехай $r_1 \in \mathbf{A}_i, r_2 \in \mathbf{A}_j$, ($r_1 \neq r_2, i \neq j$). Тоді таке об'єднання не можливе, якщо

$$\mathbf{G}_{t+1,n}(\mathbf{X}_{t+1,n}, r_1) \neq \mathbf{G}_{t+1,n}(\mathbf{X}_{t+1,n}, r_2). \quad (7)$$

Вказана нерівність має місце при існуванні принаймні одного такого значення $t \in \mathbf{S}_{t+1,n}$, де $\mathbf{G}_{t+1,n}(t, r_1) \neq \mathbf{G}_{t+1,n}(t, r_2)$. Для цього серед елементів множин пар підстановки $\mathbf{T}^{\wedge}$, споріднених до відповідних множин $\mathbf{P}^{\wedge}$ (тобто тих, де множини кодів функцій **P** використовувались при створенні $\mathbf{A}_i$ та $\mathbf{A}_j$) повинна бути принаймні одна пара, де коди функцій одинакові, а коди аргументів – різні. Очевидно, що ця умова виконується для будь яких множин $\mathbf{T}^{\wedge}$, які мають спільні елементи множин кодів функцій та різні множини кодів аргументів. Якщо дві множини $\mathbf{T}^{\wedge}$ мають одинакові множини кодів аргументів та мають спільні елементи множин кодів функцій, то для невиконання (7) необхідне повне спів падання пар підстановок для спільних кодів функцій. З КМ типу 3 сумісні КМ лише типу 2, де множини кодів функцій співпадають. При цьому лише для КМ типу 2а можливе спів падання множин кодів функцій при спів паданні множин кодів аргументів. Звідси випливає, що коли в КМ типу 2а виконується умова:

$$\mathbf{T}^{\wedge}_{ac} = \mathbf{T}^{\wedge}_{bc} \text{ або } \mathbf{T}^{\wedge}_{ad} = \mathbf{T}^{\wedge}_{bd}, \quad (8)$$

то з будь яким КМ типу 3а утворюється підстановка, обернена до якої також реалізується на простому двомодульному каскаді. Зауважимо, що при виконанні обох умов (8), функції КМ не будуть залежати від значень молодших розрядів

Розглянемо наступний приклад. Нехай КМ в старших розрядах як і раніше задається табл. 2. Відзначимо, що $\mathbf{T}^{\wedge}_{ac} = \mathbf{T}^{\wedge}_{bc} = \langle\{1\},\{0\}\rangle$.

Нехай КМ для молодших розрядів задається наступною табл.7.

Таблиця 7

f_r	0	1	0	0	0	0	1	0	
$\mathbf{F}_{1,3}$ при $f_h = 0$	4	7	5	6	1	3	0	2	
$\mathbf{F}_{1,3}$ при $f_h = 1$	2	7	3	5	4	0	1	6	
X	0	1	2	3	4	5	6	7	

Для даного КМ маємо:

$$\mathbf{S}_{a(a=0)} = \{0,2,3,4,5,7\},\ \mathbf{S}_{b(b=1)} = \{1,6\},$$

$$\mathbf{P}_{ca(c=0,a=0)} = \{4,5,6,1,3,2\},\ \mathbf{P}_{da(d=1,a=0)} = \{2,3,5,4,0,6\},$$

$$\mathbf{P}_{cb(c=0,b=0)} = \{7,0\},\ \mathbf{P}_{db(d=1,b=1)} = \{7,1\},$$

$$\mathbf{P}^{\wedge}_{ca} = \langle\{0,2,3,4,5,7\},\{4,5,6,1,3,2\}\rangle, \mathbf{P}^{\wedge}_{da} = \langle\{0,2,3,4,5,7\},\{2,3,4,0,6\}\rangle,$$

$$\mathbf{P}^{\wedge}_{cb} = \langle\{1,6\},\{7,0\}\rangle, \mathbf{P}^{\wedge}_{db} = \langle\{1,6\},\{7,1\}\rangle,$$

$$\mathbf{A}_1 = \mathbf{P}_{ca} \cap \mathbf{P}_{da} = \{2,3,4,5,6\},\ \mathbf{A}_2 = \mathbf{P}_{ca} \cap \mathbf{P}_{cb} = \varnothing,$$

$$\mathbf{A}_3 = \mathbf{P}_{ca} \cap \mathbf{P}_{db} = \{1\},\ \mathbf{A}_4 = \mathbf{P}_{da} \cap \mathbf{P}_{cb} = \{0\},$$

$$\mathbf{A}_5 = \mathbf{P}_{da} \cap \mathbf{P}_{db} = \varnothing,\ \mathbf{A}_6 = \mathbf{P}_{cb} \cap \mathbf{P}_{db} = \{7\},$$

$$\mathbf{M}^{\wedge}_{ca} = \mathbf{T}^{\wedge}_{ac} \times \mathbf{P}^{\wedge}_{ca},\ \mathbf{M}^{\wedge}_{da} = \mathbf{T}^{\wedge}_{ad} \times \mathbf{P}^{\wedge}_{da}, \mathbf{M}^{\wedge}_{cb} = \mathbf{T}^{\wedge}_{bc} \times \mathbf{P}^{\wedge}_{cb},\ \mathbf{M}^{\wedge}_{db} = \mathbf{T}^{\wedge}_{bd} \times \mathbf{P}^{\wedge}_{db},$$

$$\mathbf{T}^{\wedge}_{ac} = \mathbf{T}^{\wedge}_{bc}\langle\{1\},\{0\}\rangle,\ \mathbf{T}^{\wedge}_{ac} = \langle\{0,2,3\},\{3,1,2\}\rangle,\ \mathbf{T}^{\wedge}_{bd} = \mathbf{T}^{\wedge}_{bc}\langle\{0,2,3\},\{3,2,1\}\rangle.$$

Враховуючи (7), сформуємо множини $\mathbf{M}^{\wedge}$:

$$\mathbf{M}^{\wedge}_{ca} = \mathbf{T}^{\wedge}_{ac} \times \mathbf{P}^{\wedge}_{ca} = \langle\{1\},\{0\}\rangle \times \langle\{0,2,3,4,5,7\},\{4,5,6,1,3,2\}\rangle,$$

$$\mathbf{M}^{\wedge}_{da} = \mathbf{T}^{\wedge}_{ad} \times \mathbf{P}^{\wedge}_{da} = \langle\{0,2,3\},\{3,1,2\}\rangle \times \langle\{0,2,3,4,5,7\},\{4,3,5,4,0,6\}\rangle,$$

$$\mathbf{M}^{\wedge}_{cb} = \mathbf{T}^{\wedge}_{bc} \times \mathbf{P}^{\wedge}_{cb} = \langle\{1\},\{0\}\rangle \times \langle\{1,6\},\{7,0\}\rangle,$$

$$\mathbf{M}^{\wedge}_{db} = \mathbf{T}^{\wedge}_{bd} \times \mathbf{P}^{\wedge}_{db} = \langle\{0,2,3\},\{2,3,1\}\rangle \times \langle\{1,6\},\{7,1\}\rangle.$$

Таблиця 8 – Пряма підстановка

F(X)	32	27	33	35	34	30	21	36	04	07	05	06	01	03	00	02
X	00	01	02	03	04	05	06	07	10	11	12	13	14	15	16	17
F(X)	12	37	13	15	14	10	31	16	22	17	23	25	24	20	11	26
X	20	21	22	23	24	25	26	27	30	31	32	33	34	35	36	37

Для формування оберненої підстановки використовуємо обернений КМ для старших розрядів, заданий в табл. 5.

Розглянемо побудову оберненого КМ для молодших розрядів. Маємо:

$$\mathbf{M}^{\wedge 0}_{ca} = \mathbf{T}^{\wedge 0}_{ac} \times \mathbf{P}^{\wedge 0}_{ca} = \langle\{0\},\{1\}\rangle \times \langle\{4,5,6,1,3,2\},\{0,2,3,4,5,7\}\rangle,$$

$$\mathbf{M}^{\wedge 0}_{da} = \mathbf{T}^{\wedge 0}_{ad} \times \mathbf{P}^{\wedge 0}_{da} = \langle\{3,1,2\},\{0,2,3\}\rangle \times \langle\{2,3,5,4,0,6\},\{0,2,3,4,5,7\}\rangle,$$

$$\mathbf{M}^{\wedge 0}_{cb} = \mathbf{T}^{\wedge 0}_{bc} \times \mathbf{P}^{\wedge 0}_{cb} = \langle\{0\},\{1\}\rangle \times \langle\{7,0\},\{1,6\}\rangle,$$

$$\mathbf{M}^{\wedge 0}_{db} = \mathbf{T}^{\wedge 0}_{bd} \times \mathbf{P}^{\wedge 0}_{d} = \langle\{2,3,1\},\{0,2,3\}\rangle \times \langle\{7,1\},\{1,6\}\rangle,$$

Сформуємо множини **A**:

$$\mathbf{A}_1 = \mathbf{P}_{ca} \cap \mathbf{P}_{da} = \{2,3,4,5,6\},\ \mathbf{A}_2 = \mathbf{P}_{ca} \cap \mathbf{P}_{cb} = \varnothing,$$
$$\mathbf{A}_3 = \mathbf{P}_{ca} \cap \mathbf{P}_{db} = \{1\},\ \mathbf{A}_4 = \mathbf{P}_{da} \cap \mathbf{P}_{cb} = \{0\},$$
$$\mathbf{A}_5 = \mathbf{P}_{da} \cap \mathbf{P}_{db} = \varnothing,\ \mathbf{A}_6 = \mathbf{P}_{cb} \cap \mathbf{P}_{db} = \{7\}.$$

Оскільки елементи множини $\mathbf{A}_1$ є кодами аргументів для множин $\mathbf{M}_{ca}^{\wedge 0}$ та $\mathbf{M}_{da}^{\wedge 0}$ і елементи множини $\mathbf{A}_4$ є кодами аргументів для множин $\mathbf{M}_{da}^{\wedge 0}$ та $\mathbf{M}_{cb}^{\wedge 0}$, а $\mathbf{T}_{ac}^{\wedge 0} = \mathbf{T}_{bc}^{\wedge 0}$, то елементи множин $\mathbf{A}_1$ та $\mathbf{A}_4$ входять в один і той же клас еквівалентності по декомпозиції (3). Дійсно, легко бачити, що для будь якого елемента *r* цих множин функція $\mathbf{G}_{4,5}(\mathbf{X}_{4,5}, r)$ визначається рядком при $f_r^0 = 0$ або рядком при $f_r^0 = 1$ в табл.5 . Звідси випливає наступна структура оберненого КМ для молодших розрядів.

Таблиця 9 – Обернений КМ типу 3а для молодших розрядів.

f_r^0	0	1	0	0	0	0	0	1
$\mathbf{G}_{1,3}$ при $f_h^0 = 0$	6	4	7	5	0	2	3	1
$\mathbf{G}_{1,3}$ при $f_h^0 = 1$	5	6	0	2	4	3	7	1
$\boldsymbol{X}$	0	1	2	3	4	5	6	7

В результаті буде реалізована підстановка, яка задана в табл. 10. Легко бачити, що ця підстановка є оберненою до підстановки, яка задана в табл. 8

Зауважимо, що всі отримані результати мають місце, якщо доведення проводить базуючись на множинах **T** , а не **P** .

Таблиця 10 – Обернена підстановка

16	14	17	15	10	12	13	11	25	36	20	22	24	23	27	31
00	01	02	03	04	05	06	07	10	11	12	13	14	15	16	17
35	06	30	32	34	33	37	01	05	26	00	02	04	03	07	21
20	21	22	23	24	25	26	27	30	31	32	33	34	35	36	37

Висновки

Таким чином встановлено:

1) Якщо підстановки реалізуються простим двомодульним каскадом з використанням КМ лише типу 2 (2а, 2б, 2в), то обернена підстановка також реалізується на простому двох модульному каскаді.

2) При використанні КМ типів 3б та 3в обернена підстановка не може бути реалізована на простому каскаді (з одним боковим виходом).

3) При використанні КМ типу 3а реалізація оберненої підстановки на простому двох модульному каскаді можлива за умови, що в КМ типу 2а при фіксованому значенні на боковому виході (0 або 1) функції КМ на первинних виходах не залежать від значення на боковому вході.

4) Для КМ типу 2а або 3а обернений КМ має відповідно тип 2а або 3а. Для КМ типу 2б обернений КМ має тип 2б, якщо пряма підстановка реалізована парою 2а-2б і тип 2в, якщо пряма підстановка реалізована парою 2в-2б. Для КМ типу 2в обернений КМ має тип 2б, якщо пряма підстановка реалізована парою 2в-2б і тип 2в, якщо пряма підстановка реалізована парою 2в-2в.

Можливим напрямком подальших досліджень є поширення одержаних результатів для більш складних КМ та реалізації прямих та обернених підстановок на багатомодульних каскадах.

Література

1) Опанасенко В.Н., Сахарин В.Г. ПЛИС типа FPGA фирмы Xilinx: возможности, проектирование и применение// Электронные системы и компоненты. – 2003, № 4, с.7-11

2) Кузелин М.О., Кнышев Д.А., Зотов В.Ю. Современные семейства ПЛИС фирмы Xilinx. – М: «Горячая линия-Телеком», 2004, 440 с.

3) Тарасенко В.П., Тесленко О.К., Яновська О.Ю. Проблеми апаратної реалізації підстановок. Наукові записки УНДІЗ, №2, 2007, с 52-58

4) В.П. Тарасенко, О.К. Тесленко, О.Ю. Яновська. Реалізація повних підстановок на простому двомодульному каскаді конструктивних модулів. Інформаційні технології та комп'ютерна інженерія.№1(11), 2008, с.88-97

5) Кантор Г. Труды по теории множеств.- Москва. Наука, 1985.

6) Логачев О.А., Сальников А.А, Ященко В.В. Булевы функции в теории кодирования и криптологии. – Москва. Издательство МЦНМО, 2004.

Стаття надійшла: 22.11.2013.

Відомості про авторів

Тарасенко Володимир Петрович, д.т.н., проф. Завідуючий кафедрою системного програмування і спеціалізованих комп’ютерних систем НТУУ «КПІ».

Тесленко Олександр Кирилович, к.т.н., ст.н.с. Доцент кафедри системного програмування і спеціалізованих комп’ютерних систем НТУУ «КПІ».

Яновська Олена Юріївна, Асистент кафедри звукотехніки і регістрації інформації НТУУ «КПІ».