УДК 681.3:519.15

В. Різник
Національний університет “Львівська політехніка”,
кафедра автоматизованих систем управління

КОДИ ПРОСТОРОВИХ СИМЕТРИЧНО-АСИМЕТРИЧНИХ МНОЖИН

Показана можливість застосування нового класу просторових множин, побудованих на багатовимірних симетрично-асиметричних конфігураціях типу ідеальних кільцевих в’язанок (ІКВ) для кодування векторних даних з мінімізованою кількістю вагових розрядів. Досліджено взаємозв’язок теорії симетрично-асиметричних множин і теорії алгебричних структур полів Ґалуа.

Ключові слова: симетрично-асиметрична множина, поле Ґалуа, оптимізація, кодування векторних даних, інформаційна технологія.

It is shown possibility for application a new class of spatial sets using multidimensional symmetrical and non-symmetrical combinatorial configurations "Ideal Ring Bundles" (IRB)s for vector data coding with minimal number of the digit weights. Mutual connection theory of the symmetrical and asymmetrical sets with algebraic structures in Galois fields is developed.

Key words: code, symmetrical and asymmetrical set, Galois field, optimization, vector data coding, information technology.

Вступ

Багато актуальних питань комп’ютерної інженерії та інформаційних технологій пов’язано з умілим використанням математичних моделей та методів оптимізації систем перетворення інформації, що ґрунтуються на властивостях багатовимірних комбінаторних конфігурацій типу ідеальних кільцевих в’язанок (ІКВ) [1] як зручних математичних моделей для проектування інформаційних технологій з розширеними функціональними можливостями перетворення форми інформації у вигляді векторних даних. Досліджувати властивості згаданих моделей доцільно з урахуванням фундаментальних законів світобудови, в основі яких лежить закон просторової симетрії. Особливу увагу варто звернути на симетричні конструкції впорядкованих множин та їхні асиметричні підмножини. Ми пропонуємо розвинути наукову базу теорії просторових симметрично-асиметричних множин у галузі інформаційних технологій на основі використання ідеї сумірності симетричних та асиметричних структур, використавши для більшої наочності їхню геометричну інтерпретацію.

Формулювання проблеми

Серед проблем, пов’язаних з розвитком теорії багатовимірних комбінаторних конфігурацій типу ідеальних кільцевих в’язанок (ІКВ), важливим питанням є синтез багатовимірних кодів з оптимальним розподілом вагових розрядів за критерієм мінімізації кількості розрядів. Згадані проблеми доцільно вирішувати за допомогою методів комбінаторної оптимізації багатовимірних структур з використанням взаємозв’язку теорії ІКВ й алгебричної теорії скінченних полів з проекцією властивостей останніх на просторові симетричні структури та їхні асиметричні підструктури.

Мета дослідження

Метою дослідження є виявлення зв'язку між структурою ІКВ та структурою алгебричних полів Ґалуа із залученням геометричних інтерпретацій симетричних полів Ґалуа та асиметричних структур ІКВ, розроблення алгоритму синтезу векторних кодів з використанням класичної теорії симетричних множин та їхніх асиметричних підмножин у структурі алгебричних полів Ґалуа для розширення можливостей практичного застосування методів кодування та перетворення векторних даних в інформаційних технологіях.

Структура просторових симетрично-асиметричних груп

За наявної різноманітності інтерпретацій «досконалих» комбінаторних конструкцій через циклічні блок-схеми, різницеві множини, скінченні афінні, проективні площини тощо [2] структуру типу ІКВ доцільно порівняти з алгебричними властивостями полів Ґалуа. Наведемо перелік деяких з них [3]:

1) для всякого степеня простого числа p і будь-якого $n \geq 1$ існує єдине з точністю до ізоморфізму скінченне поле $GF(p^n)$, тобто поле зі скінченною кількістю елементів, де GF означає Galois Field;

2) поле $GF(p^n)$ можна зобразити як множину всіх класів лишків за модулем довільного полінома $f(x)$ степеня n незвідного над полем $GF(p)$;

3) поліном $f(x)$ степеня $n \geq 1$ з коефіцієнтами із поля $GF(p)$ є незвідним над полем $GF(p)$, якщо його не можна записати у вигляді $f(x) = A(x) \cdot B(x)$, де $A(x)$ і $B(x)$ поліноми над $GF(p)$;

4) у полі $GF(q^s)$ всі його $q^s - 1$ ненульові елементи різні та утворюють циклічну групу за операцією множення ;

5) автоморфізми поля $GF(q^s)$ утворюють циклічну групу порядку s, яка породжується автоморфізмом $\alpha: x \to x^p$ для будь-якого $x \in GF(q^s)$.

Порівнюючи властивості класичних комбінаторних конфігурацій зі структурою ІКВ [1], можна побачити, що ІКВ описується параметрами S_n, n, R, де S_n – сума елементів ідеальної кільцевої в'язанки, n – кількість елементів, R – число кільцевих сум з однаковими числовими значеннями.

Алгоритм синтезу ІКВ полягає в такому:

1) знайти незвідний над полем $GF(p^s)$ поліном;

2) визначити первісний елемент x цього поля з максимально можливим періодом згаданого елемента та обчислити степені $x^0, x^1, \ldots, x^z$, $(z=q^{s-2})$, які повинні "пробігати" усі значення ненульових елементів $GF(p^s)$;

3) за побудованою алгебричною структурою $GF(p^s)$ визначити числові значення елементів ІКВ.

Для дослідження комбінаторних властивостей розширених полів Ґалуа за допомогою ІКВ доцільно використати графічні відображення останніх .

Алгоритм побудови графічних моделей ІКВ полягає в такому:

1) за параметрами ІКВ знайти первісний незвідний над полем Ґалуа поліном відповідного степеня;

2) визначити первісний поліном розширеного поля і обчислити усі ненульові елементи цього поля;

3) побудувати граф, вершинами якого є елементи $x^0, x^1, \ldots, x^z$, $(z= q^{s-2})$;

4) на побудованому графі обрати вершини, яким відповідають однакові значення коефіцієнтів за будь-якого з фіксованих степенів;

5) сполучивши усі сусідні пари вершин ребрами, отримати графічне відображення ІКВ у вигляді многокутника.

Наприклад, для ІКВ з параметрами $S_n = \left(q^{s+1} - 1\right)/(q-1) = 21$, $n = \left(q^{s} - 1\right)/(q-1) = 5$, $R = \left(q^{s-1} - 1\right)/(q-1) = 1$, де $q = 2^2$, $s = 2$, $GF(q^{s+1}) = GF(2^6)$, поле $GF(2^2)$ 0, 1, c, c+1, де $c^2+c+1=0$, можна розглядати як розширення поля $GF(2)$. Первісний елемент x поля $GF(2^6)$ задовольняє рівняння $f(x) = x^3 + cx^2 + cx + c = 0$, де $f(x)$ – незвідний поліном над полем $GF(2^2)$ [2]. Позначивши для зручності обчислень $c + 1 = d$, легко знайти всі елементи цього поля (табл. 1).

Таблиця 1

Елементи поля $GF(2^6)$, утворені незвідним поліномом $f(x) = x^3 + cx^2 + cx + c = 0$

$x = x;$		$x^{11} = 1 + (c+1)x + dx^2$
$x^2 = x^2$		$x^{12} = 1 + cx^2$
$x^3 = c + cx + cx^2$		$x^{13} = c + 1 + cx + dx^2$
$x^4 = d + x + x^2$		$x^{14} = 1 + cx + dx^2$
$x^5 = c + x + dx^2$		$x^{15} = 1 + dx^2$
$x^6 = 1 + d$		$x^{16} = 1 + x^2$
$x^7 = x + dx^2$		$x^{17} = c + dx + cx^2$
$x^8 = 1 + x$		$x^{18} = d + x$
$x^9 = x + x^2$		$x^{19} = dx + x^2;$
$x^{10} = c + cx + dx^2$		$x^{20} = c + cx + x^2;$
		$x^{21} = c.$

На симетричному нуль-графі, вершинами якого є елементи $x^1, x^2, x^3, ..., x^{21}$, легко знайти вершини, яким відповідають нульові значення коефіцієнтів при фіксованому значенні степеня x^i у правій частині рівнянь. Для i = 1 цим вершинам відповідає набір елементів $x^1, x^2, x^7, x^9, x^{19}$, що утворюють асиметричний п'ятикутник (n = 5) у симетричному полі графа з S_n=21 вершинами (рис. 1).

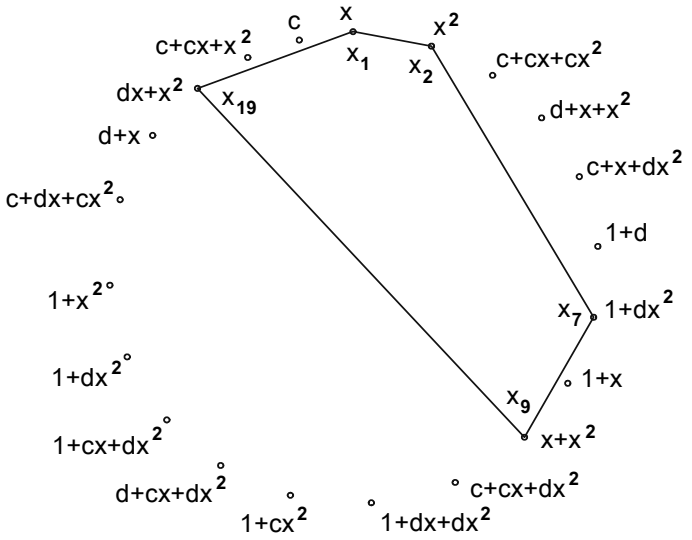

Рис. 1. Графічне відображення ІКВ (1,3,10,2,5) з параметрами S_n = 21, n = 5, R = 1 в $GF(2^6)$

Розглянемо відображення ІКВ з параметрами $n=4, R=1, S_n=13$. У цьому випадку первісний елемент x поля $GF(3^2)$ задовольняє рівняння $f(x)=x^3-x-1$, де $f(x)$ – незвідний поліном над полем $GF(3^2)$, $p=3$, $s=2$. Елементи цього поля зведені в табл. 2.

Таблиця 2

Елементи поля $GF(3^2)$, утворені за незвідним поліномом $f(x)=x^3-x-1$

$x^1=x$	$x^8=2x^2+2$
$x^2=x^2$	$x^9=x+2$
$x^3=x+1$	$x^{10}=x^2+2x$
$x^4=x^2+x$	$x^{11}=2x^2+x+1$
$x^5=x^2+x+1$	$x^{12}=x^2+2$
$x^6=x^2+2x+1$	$x^{13}=1$
$x^7=2x^2+2x+1$	

На симетричному нуль-графі (рис. 2) вершинам x^1, x^3, x^9, x^{13} відповідають однакові нульові коефіцієнти при степенях x^2, а вписаний в цей граф асиметричний чотирикутник відображає ІКВ з параметрами S_n=13, n=4, R=1 в полі $GF(3^2)$.

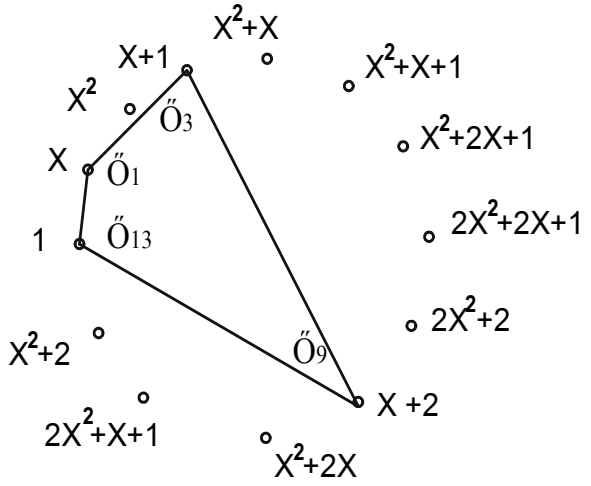

Рис. 2. Графічне відображення ІКВ з параметрами S_n=13, n = 4, R = 1, утворене поліномом $f(x)=x^3-x-1$

На рис. 2 можна бачити ІКВ у вигляді чотирикутника (n = 4), сусідні вершини якого рознесені асиметрично на відстані, що утворюють послідовність (1,2,6,4) у симетричному полі графа з S_n =13 вершинами.

Для незвідного полінома $f(x)=x^3-x-2$ таблиця елементів поля $GF(3^2)$ набуває такого вигляду (табл. 3).

Кільцевий граф для цього випадку зображено на рис. 3.

На рис.3 можна бачити ІКВ у вигляді асиметричного чотирикутника (n=4), сусідні вершини якого рознесені на відстані, що утворюють послідовність (1,2,6,4) в симетричному полі $GF(3^2)$.

Таблиця 3

Елементи поля $GF(3^2)$, утворені за незвідним поліномом $f(x) = x^3 - x - 2$

$x = x$ $x^2 = x^2$ $x^3 = x + 2$ $x^4 = x^2 + 2x$ $x^5 = 2x^2 + x + 2$ $x^6 = x^2 + x + 1$ $x^7 = x^2 + 2x + 2$	$x^8 = 2x^2 + 2$ $x^9 = x + 1$ $x^{10} = x^2 + x$ $x^{11} = x^2 + x + 2$ $x^{12} = x^2 + 2$ $x^{13} = 2$

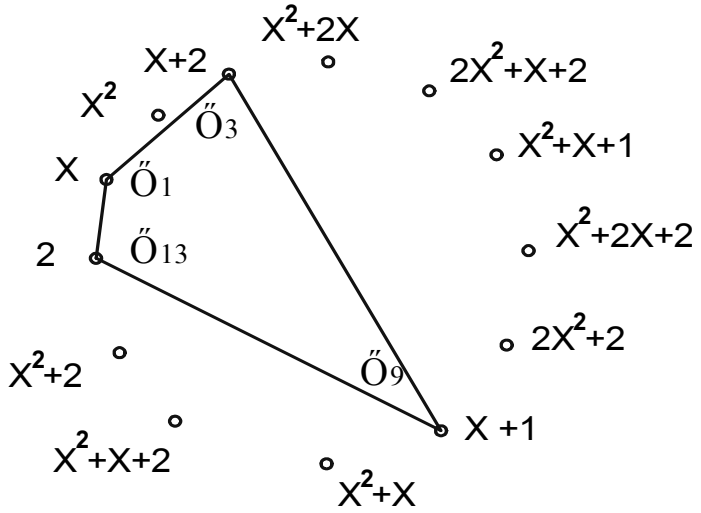

Рис. 3. Графічне відображення ІКВ з параметрами S_n=13, n=4, R=1, утворене незвідним поліномом $f(x) = x^3 - x - 2$

Для незвідного полінома $f(x) = x^3 - x^2 - 2x - 2$ рівняння для $x, x^2, ..., x^{13}$ набувають такого вигляду (табл. 4).

Таблиця 4

Елементи поля $GF(3^2)$, утворені за незвідним поліномом $f(x) = x^3 - x^2 - 2x - 2$

$x = x$ $x^2 = x^2$ $x^3 = x^2 + 2x + 2$ $x^4 = x + 2$ $x^5 = x^2 + 2x$ $x^6 = 2x + 2$ $x^7 = 2x^2 + 2x$	$x^8 = x^2 + x + 1$ $x^9 = 2x^2 + 2$ $x^{10} = 2x^2 + 1$ $x^{11} = 2x^2 + 2x + 1$ $x^{12} = x^2 + 2x + 1$ $x^{13} = 2$

Вибравши на графі (рис. 4) вершини x^i $(i = 1,...,n)$, значенням яких відповідають однакові нульові коефіцієнти при фіксованому x^2, легко встановити, що цими вершинами будуть x, x^4, x^6, x^{13}.

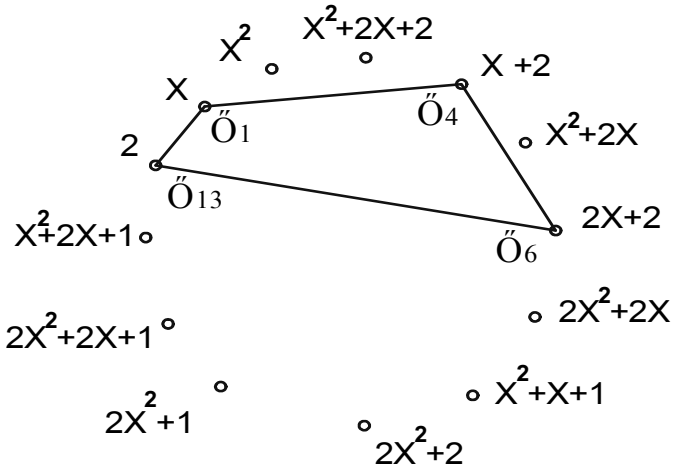

Рис. 4. Графічне відображення ІКВ з параметрами S_n =13, n = 4, R = 1, утворене незвідним поліномом $f(x) = x^3 - x^2 - 2x - 2$

На рис.4 можна бачити ІКВ у вигляді асиметричного чотирикутника (n=4), сусідні вершини якого рознесені між собою на відстані, що утворюють послідовність (1,3,2,7) в симетричному полі $GF(3^2)$.

Багатовимірні векторні ІКВ-коди

Встановимо зв'язок багатовимірних векторних ІКВ-кодів зі стандартними комбінаторними структурами [2], обравши для прикладу формування векторних кодових комбінацій на основі тривимірних ідеальних кільцевих в'язанок (3D-ІКВ). Для побудови тривимірних систем кодування представимо її модель у вигляді послідовності впорядкованих цілочислових 3-кортежів ((k_{11}, k_{21}, k_{31}), (k_{12}, k_{22}, k_{32}), ... , (k_{1i}, k_{2i}, k_{3i}), ... , (k_{1n}, k_{2n}, k_{3n})), яка замкнена на саму себе у вигляді кільцевої схеми. У загальному випадку числа k_{11}, k_{21}, k_{31}, k_{12}, k_{22}, k_{32}, ... , k_{1i}, k_{2i}, k_{3i}, ... , k_{1n}, k_{2n}, k_{3n} такої моделі можуть набувати будь-яких значень. Однак, коли йдеться про оптимальну систему кодування повідомлень у вигляді комбінацій тривимірних векторів, необхідно дотримуватися таких вимог:

1) впорядковані числа у всіх послідовностях (3-кортежах) не повинні повторюватися;
2) усі 3D вектор-суми поруч розміщених 3-кортежів не повинні повторюватися;
3) множина усіх 3-кортежів разом з множиною усіх сум послідовно розміщених 3-кортежів повинні заповнити координати вузлів тривимірної циклічної матриці.

Під 3D вектор-сумою розуміють результат арифметичного додавання чисел, обраних від кожного з n 3-кортежів з однойменними порядковими номерами, причому додавання здійснюють за відповідними модулями, значення яких визначаються розмірами циклічної матриці за кількістю вузлів на кожній її координаті .

Нехай (k_{11}, k_{21}, k_{31}) = (0,1,0); (k_{12}, k_{22}, k_{32}) = (0,2,3); (k_{13}, k_{23}, k_{33}) = (1,1,2);
(k_{14}, k_{24}, k_{34}) = (0,2,2); (k_{15}, k_{25}, k_{35}) = (1,0,3); (k_{16}, k_{26}, k_{36}) = (1,1,1).

У цьому випадку система для кодування 3D векторів за допомогою шести (n=6) кодових комбінацій набуває такого вигляду: ((0,1,0), (0,2,3), (1,1,2), (0,2,2), (1,0,3), (1,1,1)):

Якщо по кожній з координат 3D решітки значеннями модулів обрати відповідно числа 2, 3, 5, можна отримати такі комбінації у вигляді сум послідовних 3-кортежів:

(0, 0, 0) ≡ (0,1,0) + (0,2,3) + (1,1,2) + (0,2,2) +(1,0,3),
(0, 0, 1) ≡ (0,2,2) + (1,0,3) + (1,1,1),
(0, 0, 2) ≡ (1,1,2) + (0,2,2) + (1,0,3),
(0, 0, 3) ≡ (0,1,0) + (0,2,3),
(0, 0, 4) ≡ (0,2,2) + (1,0,3) + (1,1,1) + (0,1,0) + (0,2,3),
(0, 1, 0) ≡ (0,1,0),
(0, 1, 1) ≡ (0,2,2) + (1,0,3) + (1,1,1) + (0,1,0),
(0, 1, 2) ≡ (1,0,3) + (1,1,1) + (0,1,0) + (0,2,3),

(0, 1, 3) ≡ (1,1,1) + (0,1,0) + (0,2,3) + (1,1,2) + (0,2,2),
(0, 1, 4) ≡ (0,1,3) + (1,1,1),
(0, 2, 0) ≡ (0,2,3) + (1,1,2) + (0,2,2) + (1,0,3),
(0, 2, 1) ≡ (1,1,1) + (0,1,0) + (0,2,3) + (1,1,2),
(0, 2, 2) ≡ (0, 2, 2), і т.д.
…….…….

Легко побачити, що множина отриманих 3-кортежів вичерпує значення координат тривимірної решітки, де одна з координат набирає значень цілих чисел у діапазоні від 0 до 1, друга – від 0 до 2, третя – від 0 до 4. Отже, впорядкована кільцева послідовність 3-кортежів ((0,1,0), (0,2,3), (1,1,2), (0,2,2), (1,0,3), (1,1,1)) – це приклад побудови системи для кодування множини векторів на тривимірній решітці з розмірами 2×3×5, яка має вигляд 3D тора, з використанням лише шести (n =6) кодових розрядів.

Назвемо кільцевою вектор-сумою суму будь-якої кількості (від 1 до n-1) послідовно впорядкованих t-вимірних векторів кільцевої n-послідовності. Кільцева n-послідовність упорядкованих t-вимірних векторів, на якій множина кільцевих вектор-сум вичерпує множину значень усіх координат t-вимірної решітки фіксовану кількість разів, називається t- вимірною ідеальною кільцевою в'язанкою (tD- ІКВ), а утворена цією послідовністю система циклічно впорядкованих векторів – досконалим t- вимірним кодом.

Результати теоретичних та експериментальних досліджень свідчать про те, що існує численна кількість багатовимірних ІКВ. Цей факт відкриває можливості для проектування новітніх інформаційних систем та перспективних комп'ютерних технологій на основі використання багатовимірного векторного коду.

Перспективи розроблення високопродуктивних систем кодування векторних даних

Прикладом використання багатовимірних досконалих циклічних співвідношень в інформаційних та комунікаційних системах є так званий «монолітний код» [1]. Під монолітним розуміють код, комбінації якого побудовані на послідовностях однорідних інформаційних символів («одиниць» або «нулів»), тому поява між ними хоча б одного «нуля» серед «одиниць», або, навпаки, вказує на появу помилки, не потребуючи додаткових контрольних перевірок, що забезпечує високу швидкодію щодо виявлення і виправлення помилок. Забезпечення максимальної потужності коду досягається завдяки відповідному розподілу векторних вагових розрядів. За таких умов монолітний код вичерпує множину способів формування комбінацій, що зводить до мінімуму його інформаційну надлишковість. Дослідження, пов'язані з проблемою проектування багатовимірних систем кодування та перетворення форми сигналів у векторний монолітний код, дають можливість розробляти інформаційні технології та апаратно-програмні засоби з розширеними функціональними можливостями, що ґрунтуються на одно- та багатовимірних ІКВ, проектування ефективних систем перетворення форми інформації, розроблення спеціалізованих процесорів на багатовимірній комп'ютерній арифметиці.

Дослідження геометричних властивостей просторових симетрично-асиметричних груп передбачають розширення сфери застосування оптимізованих векторних монолітних кодів в тих галузях науки і техніки, де впроваджуються загальносистемні принципи, що ґрунтуються на теорії комбінаторних конфігурацій: математиці (векторна алгебра, теорія груп), обчислювальній техніці, криптографії, інформаційно-вимірювальній техніці, комп'ютерних технологіях, радіофізиці, системах зв'язку.

Висновки

Результати дослідження комбінаторних властивостей ІКВ за участі геометричних інтерпретацій симетричної структури алгебричних полів Ґалуа та асиметричних структур ІКВ розкривають зв'язок теорії ІКВ з класичною теорією симетричних груп та їхніх асиметричних конфігурацій у симетричній структурі алгебричних полів Ґалуа, що свідчить про геометричну

природу одно- та багатовимірних ІКВ, розкриває фундаментальне значення просторових симетрично-асиметричних структурних співвідношень в теорії оптимального кодування векторних даних і створює можливості для проектування новітніх пристроїв та систем на векторних інформаційних технологіях з поліпшеними технічними характеристиками.

1. Різник В.В. Синтез оптимальних комбінаторних систем. – Львів: Вища школа, 1989. – 168 с. 2. Холл М. Комбинаторика. – М.: Мир, 1970. 3. Свердлик М.Б. Оптимальные дискретные сигналы. – М., 1975.

УДК 621.314

U. Dzelendzyak[1], **V. Samotyy**[1,2], **I. Dzelendzyak**[3]
[1.] Lviv Polytechnic National University
The Department of computerized automatics' systems
[2.] Cracow University of Technology
The Department of Automation and Information Technology
[3.] Lviv Polytechnic National University
The Department of Marketing and Logistic

SOME DEPENDENCE OF FIBONACCI'S NUMBERS AND GOLDEN CHOPPING

Для золотого січення і для поліномів з нескінченним числом членів створено нові аналітичні залежності. Показано аналітично, як можливо визначити нескінченний поліном, в якому аргумент є золоте січення з використанням ряду Тейлора. Вирази для розрахунку цих поліномів, в якому коефіцієнти є числа послідовності Фібоначчі, додаються.

Ключові слова: алгоритм Фібоначчі, золоте січення, степеневий ряд, різниця, дільник.

New analytical dependences were established for golden chopping and for polynomials with infinite number of members. It is shown how we can determine analytically infinite polynomial in which the argument is the golden chopping using a Taylor's series. The expressions for calculating these polynomials in which the coefficients are numbers in the Fibonacci's series are displayed.

Key words: Fibonacci's algorithm, golden chopping, power series, difference, divider.

Introduction

In 1202 Italian mathematician Leonardo of Pisa also known as Fibonacci (which means son of Bonacci) wrote a book "Liber abacci" ("Book about abacus") [1]. With this book Europeans first learned of Hindu ("Arabic") numerals, as well as the Fibonacci's sequence.

The Fibonacci's sequence is expressed as as $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$, $F_7 = 13$, $F_8 = 21$, $F_9 = 34$, ... , $F_{77} = 5527939700884757$, $F_{78} = 8944394323791464$, ... We deal with a game-theoretic framework [2] involving a finite number of infinite populations, members of which have a finite number of available strategies. The payoff of each individual depends on her own action and distributions of actions of individuals in all populations. Fischer's concept, which is presented in [3], is an attempt to use Fibonacci's numbers for constructing the method of market behavior forecast taking into consideration the aspects of price and time. The wide range of Fibonacci's numbers application, especially in statistics, sports, non-Euclidean geometry, RSA codes, coloring of geographical maps, etc. are presented