УДК.514.18

Є. О. АДОНЬЄВ, В. М. ВЕРЕЩАГА

ПРИНЦИПИ ГЕОМЕТРИЧНОЇ КОРЕЛЯЦІЇ ПРИ ПОБУДОВІ МОДЕЛЕЙ БАГАТОФАКТОРНИХ СИТУАЦІЙ І ПРОЦЕСІВ

Із застосуванням геометричної формалізації, розробленої на основі точкового БН-числення, доведено необхідність і введено новий математичний термін – «геометрична кореляція». З використанням геометричної кореляції запропоновано алгоритм розв'язання задач багатовимірного евклідового випуклого простору E^n через розв'язання відповідної кількості одно-, двох-, трьохвимірних задач з подальшою суперпозицією отриманих розв'язків. Надано класифікацію принципів геометричної кореляції, наведено приклад алгоритму з використанням одного з принципів побудови моделі багатофакторної ситуації.

Ключові слова: геометрична формалізація, геометрична кореляція, суперпозиція, багатофакторна ситуація.

С применением геометрической формализации, разработанной на основе точечного БН-исчисления, доказана необходимость и введен новый математический термин – «геометрическая корреляция». С применением геометрической корреляции предложен алгоритм решения задач многомерного евклидового выпуклого пространства E^n через решение соответствующего количества одно-, двух-, трехмерных задач с дальнейшей суперпозицией полученных решений. Приведено классификацию принципов геометрической корреляции, приведен пример алгоритма с применением одного из принципов построения модели многофакторной ситуации.

Ключевые слова: геометрическая формализация, геометрическая корреляция, суперпозиция, многофакторная ситуация.

In modeling processes in the field of energy saving, the problem of combining a large number of physically heterogeneous factors often arises. Existing methods of mathematical modeling, as a rule, require the establishment of a correlation between the input values of the future model, and then, based on the correlation results, a model is constructed. It always puts in the model certain limitations on the number of factors that can be included in the model, in the size of the matrices, and so on. In addition, the need to integrate physically diverse factors further complicates modeling with traditional methods. In our opinion, these drawbacks are deprived of compositional methods of geometric modeling, whose geometrical formalization takes place with the help of algebraic methods of the point BN-calculus (Balyuby-Nidische calculus), because of the representation in the analytical form of correlation geometric shapes by creating the corresponding geometric aggregates. In the article, using the geometric formalization developed on the basis of point BN-calculus, the necessity and a new mathematical term - "geometric correlation" - was proved. Using geometric correlation, an algorithm for solving problems of a multidimensional Euclidean convex space E^n through a solution of the corresponding number of one-, two-, and three-dimensional problems with further superposition of the solutions obtained is proposed. A classification of the principles of geometric correlation is given, an example of an algorithm is given with the use of one of the principles for constructing a model of a multifactorial situation.

Keywords: geometric formalization, geometric correlation, superposition, multifactorial situation.

Вступ. У моделюванні ситуацій і процесів, зокрема, у сфері енергоефективних технологій, часто виникає проблема поєднання великої кількості фізично різнорідних факторів, серед яких немає можливості і сенсу визначити головні, що найбільше впливають на перебіг процесу. Традиційні методи математичного моделювання, у царині енергоефективності, нами віднесено до комбінаційних, тобто таких, для яких кореляція між вихідними величинами майбутньої моделі, у алгебраїчній формі встановлюється до створення моделі, а потім за результатами кореляцій, будується модель.

На нашу думку, наявність взаємної залежності між елементами на початковому етапі моделювання, завжди висуває до моделі певні обмеження за кількістю факторів, що можуть бути включені до моделі, за розмірами матриць, тощо. Окрім того, необхідність інтеграції фізично різнорідних факторів додатково ускладнює моделювання традиційними методами, що тягне за собою збільшення похибки у розрахунках та призводить до прийняття помилкових рішень

Вважаємо, що розв'язання проблеми інтеграції у моделі різнорідних факторів та збільшення кількості її вихідних факторів криється у розробці композиційних методів моделювання, геометрична формалізація у яких відбувається алгебраїчними методами точкового БН-числення (Балюби-Найдиша числення), через подання у аналітичному вигляді кореляційних геометричних фігур шляхом створення відповідних геометричних агрегатів [1]. Будь-яка проміжна (змінювана) точка створеної таким чином кореляційної геометричної фігури є сумою відповідних відсотків від усіх опорних (базових) точок. Іншими словами, у композиційному методі геометричного моделювання аналітична модель у точковій формі, для визначення умов, лишається незмінною, а змінюються тільки вихідні точки. За рахунок цього відбувається моделювання. Така особливість композиційного методу є важливою, тому що на практиці, з метою підвищення адекватності моделі, часто виникає необхідність змінювати якісно і кількісно вихідні фактори.

Таким чином, розробка та дослідження композиційного методу геометричного моделювання є актуальними через його можливості поєднувати у моделі різнорідні фактори, змінювати (замінювати) кількісно і якісно фактори без зміни аналітичної точкової форми моделі. Зважаючи на це, розробка принципів геометричної кореляції у композиційному геометричному моделюванні, є також актуальною задачею.

Аналіз останніх досліджень. Створення композиційного методу геометричного моделювання (КМГМ) стало можливим тільки на основі методів точкового БН-числення [1]. Розробниками КМГМ є автори цієї статті [5–8], у яких було зроблено перші спроби щодо створення та аналізу Б-поверхонь (Балюби поверхонь), розробки композиційного методу геометричного моделювання, обґрунтування необхідності його розробки та його переваги над існуючими способами моделювання процесів, стосовно особливостей і властивостей Б-поверхонь та означено перспективи застосування КМГМ. Із сказаного випливає, що поява нового методу моделювання відкриває нові можливості для створення багатофакторних моделей.

Формування мети дослідження. Обґрунтувати необхідність введення нового поняття – «геометричної кореляції», розробити алгоритм розв'язання задачі

багатовимірного простору через її поділення на відповідну кількість задач просторів меншої розмірності. Надати визначення та класифікацію принципів геометричної кореляції у побудові моделей для багатофакторних ситуацій і процесів.

Геометрична кореляція у композиційному методі геометричного моделювання. Зазвичай, під геометричною формалізацією розуміють графічно-вербальне (синтетичне) відображення ситуації або процесу, комп'ютерна реалізація яких потребує значних зусиль, для їхнього аналітичного відображення. При цьому, встановлення кореляцій між вихідними елементами, показниками, тощо відбувається на етапі формування аналітичної моделі, а початкова геометрична схема використовується лише для пояснення аналітичних операцій, і ніяк не впливає на моделювання процесу. Такий процес моделювання нами названо «традиційним». І навпаки, геометрична формалізація з використанням алгебри точкового БН-числення, здійснює кореляцію між вихідними елементами, показниками, тощо на початку моделювання у процесі створення геометричної схеми з подальшим її аналітичним відображенням у точковій формі, що створюється з використанням алгебри точкового БН-числення. При цьому, зміна вихідної геометричної схеми обов'язково призведе до зміни аналітичного запису у точковій формі. Такий процес назвемо «формалізованим геометричним моделюванням» [1], а кореляцію – «геометричною кореляцією».

Із сказаного, на нашу думку, випливає, що у традиційному методі моделювання алгебраїчна складова передує геометричній, яка існує, у більшості випадків, для пояснень алгебраїчних операцій і, ні у якому разі, не впливає на аналітику розрахунків. І навпаки, у формалізованому геометричному моделюванні ніяким чином не можна створити аналітичний запис у точковій формі, доки не буде прийнято геометричної схеми, під яку будуть створюватись точкові агрегати [1]. При цьому, зміна геометричної схеми призводить до відповідних змін у відповідній точковій формі, що відображає аналітику процесу.

Таким чином, у формалізованому геометричному моделюванні кореляційні процеси відбуваються на етапі створення геометричної схеми, а аналітика точкових агрегатів дозволяє виконувати перетворення вихідних геометричних форм. А це і підтверджує, що у формалізованому геометричному моделюванні геометрія передує алгебрі.

Як відомо [2], кореляція –встановлення залежності між величинами, що не має чіткого аналітичного характеру. На відміну від кореляції у традиційних алгебраїчних методах моделювання, вводимо поняття «геометричної кореляції» для формалізованого геометричного моделювання (геометричної формалізації). Під геометричною формалізацією будемо розуміти аналітичне подання геометричних фігур методами алгебри точкового БН-числення. Геометрична формалізація з використанням алгебри точкового БН-числення, тобто – формалізоване геометричне моделювання (ФГМ) покладено у основу композиційного методу геометричного моделювання (КМГМ). Покажемо декілька варіантів застосування ФГМ у КМГМ на геометричній формалізації одного фактору – «Вікно» (фрагмент), параметри для якого наведені у табл. 1.

Застосуємо для фактору «Вікно» монофакторний принцип побудови моделі [3], який передбачає окремий аналіз по кожному з 50-х параметрів (табл. 1, в таблиці показані 33 з усіх 50-ти параметрів), виходячи з цього, кожну з типо-моделей вікон, будемо розглядати як окрему точку 50-вимірного простору. У наших дослідженнях було розглянуто 20 моделей вікон різних виробників з різними параметрами (характеристиками), які у даній статті не наведено через великий об'єм інформації.

Таким чином, у якості вихідних даних наших досліджень маємо 20 типо-моделей вікон, кожне з яких характеризується 50-ма параметрами, тобто одна тисяча значень. На такій кількості показників можна побудувати десятки або навіть сотні моделей. Звідси випливає, що перш ніж будувати модель, необхідно визначити її мету, тобто яке питання, відносно вікна, ми хочемо дослідити, з використанням створеної моделі. Мета створення не може бути однозначною, тому що однозначні розв'язки можна дістати, використовуючи дані таблиці 1. Після формування мети моделі, що створюється, необхідно визначити параметри, які у найбільшій мірі відповідають поставленій меті. Оскільки мета не є однозначною, то таких параметрів буде два і більше. Окремо, по кожному з визначених параметрів, що відповідають меті моделі, розташуємо їхні показники у порядку зростання або зменшення для усіх двадцяти моделей вікон. Таке розташування параметрів спростить обрання дев'яти опорних точок, що будуть характеризувати Б-поверхню відгуку. Фіксуємо номера точок, що увійшли до складу опорних. На області визначення $0\le u\le 1$; $0\le v\le 1$ будуємо відсік Б-поверхні відгуку, який складається з чотирьох чарунок (рис. 1)

У середині кіл (рис. 1) позначено номера точок, у яких визначається параметр. У точці (0.5, 0.5) позначено два номера 8 та 9, у точці (0, 1) позначено чотири номера 17, 18, 19, 20 – це означає, що в усіх цих точках параметр є однаковим. Обираючи три найменших значення параметру, три – у середині ряду та три найбільших значення, визначаємо дев'ять опорних точок для побудови відсіку Б-поверхні.

На тих же самих точках, не змінюючи їхнього розташування, побудуємо Б-поверхні ще для двох параметрів. На першій, другій та третій Б-поверхнях визначаємо значення параметрів, що задовольняють вимогам моделі і тим самим знаходимо область визначення.

Нехай, для прикладу, область визначення знаходиться у межах $0.4\le u\le 0.7$; $0.5\le v\le 0.75$. Для цих значень параметрів будуємо одну з Б-поверхонь $1=f(2, 3)$; $2=\varphi(1, 3)$; $3=\psi(1, 2)$ (рис. 2).

На одній з цих поверхонь і знаходимо розв'язок задачі за визначеними вимогами.

Далі розглянемо інший, більш узагальнюючий, принцип застосування Б-поверхонь для моделювання процесів, який враховує у моделі усі параметри, що характеризують будь-який фактор.

Таблиця 1 – Фактор «ВІКНО», класифікація параметрів

№	Параметри		од. вим.
1. Економічні			
1	1.1.	Вартість вікна,	грн
2	1.2.	Вартість монтажу,	грн
3	1.3.	Загальна вартість,	грн
4	1.4.	Відповідність вимогам програми «теплих кредитів»	Так/Ні
5	1.5.	Економія на опаленні за сезон (теплова енергія)	Гкал
6	1.6.	Економія на кондиціюванні за сезон (електроенергія)	кВт·год
7	1.7.	Загальна економія енергії за рік	кВт·год
8	1.8.	Загальні втрати енергії за рік	кВт·год
9	1.9.	Експлуатаційні витрати за рік	грн
2. Екологічні			
10	2.1.	Зменшення викидів CO_2 за рік	кг
11	2.2.	Матеріал профілю (металопластик, дерево, алюміній)	назва
3. Фізичні			
12	3.1.	Тип вікна (кількість створок)	шт
13	3.2.	Ширина вікна	м
14	3.3.	Висота вікна	м
15	3.4.	Ширина профільної системи	мм
16	3.5.	Ширина склопакету	мм
17	3.6.	Кількість камер склопакету	шт
18	3.7.	Товщина скла (якщо різні – вказати кожне)	мм
19	3.8.	Ширина камери склопакету	мм
20	3.9.	Наповнювач склопакету (повітря, аргон)	назва
21	3.10.	Опір теплопередачі вікна R_0	$м^2 \cdot К/Вт$
22	3.11.	Коефіцієнт теплопередачі вікна U_w	$Вт/(м^2 \cdot К)$
23	3.12.	Коефіцієнт теплопередачі склопакету U_g	$Вт/(м^2 \cdot К)$
24	3.13.	Сонячний фактор вікна g	%
25	3.14.	Світлопропускання вікна	%
26	3.15.	Клас шумоізоляції	№, дБ
27	3.16.	Клас енергоефективності вікна (А … Е)	літера
4. Технологічні			
28	4.1.	Супутні матеріали	назва
29	4.2.	Технологічне обладнання	назва
30	4.3.	Додаткові технологічні роботи	назва
31	4.4.	Інші технологічні параметри	назва
5. Художньо-естетичні			
32	5.1.	Колір	назва
33	5.2.	Фактурність	назва

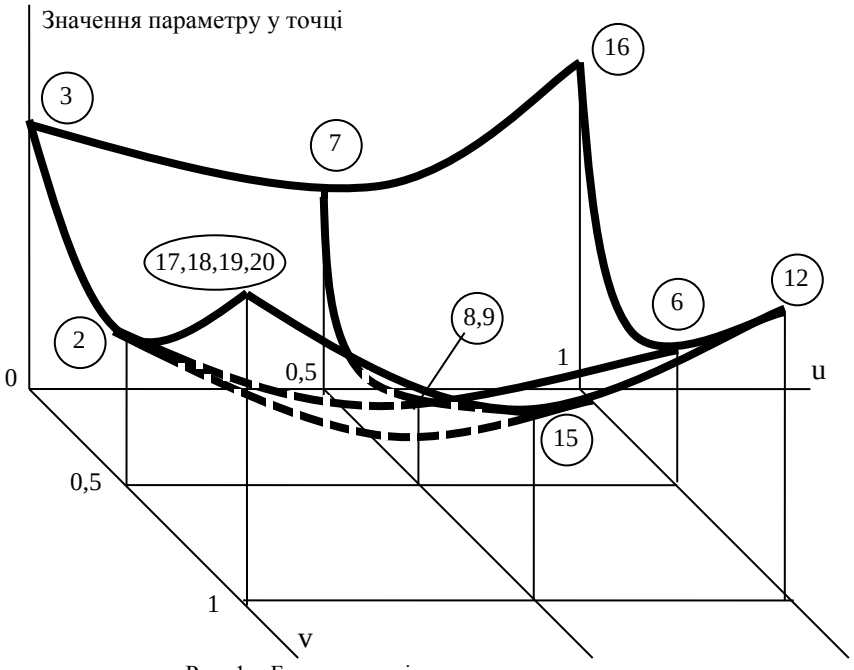

Рис. 1 – Б-поверхня відгуку по одному параметру

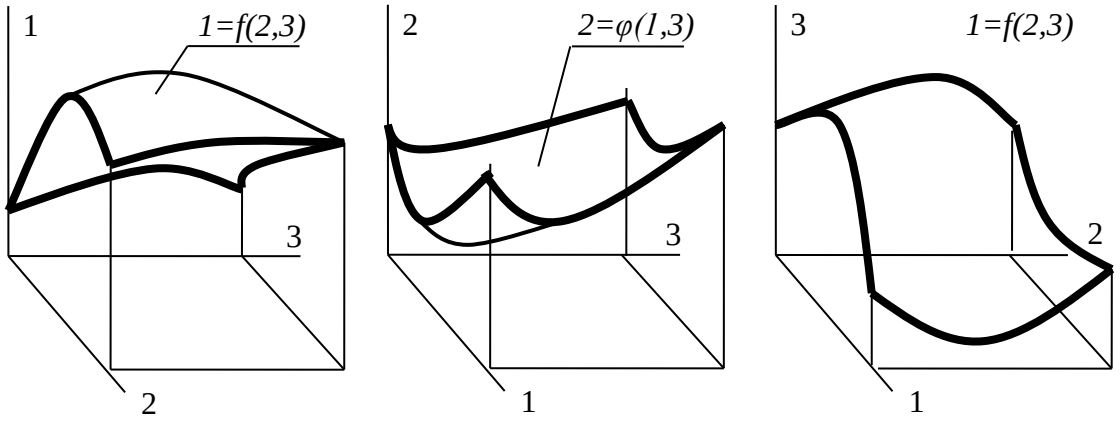

Рис. 2 – Приклади побудови Б-поверхні за трьома параметрами: а) $f(2,3)$; б) $\varphi(1,3)$ в) $\psi(1,2)$

У відповідності до поставленої мети створення моделі, визначаємо опорний параметр, на базі якого будемо обирати номери дев'яти вузлових точок для створення Б-поверхні відгуку, що аналогічна рис. 1. На визначених дев'яти вузлових точках будуємо решту – сорок дев'ять, як для нашого прикладу, Б-поверхонь.

Треба зауважити, що від обрання опорної Б-поверхні багато у чому залежить адекватність побудованої моделі до процесу. Для будь-якої з дев'яти вузлових точок знайдемо суму усіх п'ятдесяти значень параметрів, не зважаючи на одиниці виміру. Отримане число приймемо за одиницю. Із пропорції визначимо коефіцієнти $\overline{K_i}(i=\overline{1,50})$ які забезпечують перехід від абсолютних значень параметрів до відносних. Обернені до коефіцієнти $K_i = \frac{1}{\overline{K_i}}$ зрівноважують вплив на суперпозицію усіх параметрів, не зважаючи на їхні абсолютні величини.

Назвемо – коефіцієнти відсоткові; K_i – коефіцієнти вагові. Таке зрівноваження координат точки, за допомогою вагових коефіцієнтів K_i, дозволяє не загубити вплив кожної з них при побудові суперпозиції з п'ятдесяти Б-поверхонь, що відображають зміну кожної з координат. Якщо параметри (Б-поверхні) позначити через m_i, то суперпозицію з усіх координат, в цілому, для фактору "Вікно", у загальному вигляді, можна записати:

$$M_{вікно} = \sum_{i=1}^{50} m_i k_i \ . \qquad (1)$$

У наведеному прикладі було показано, як задачу п'ятидесятивимірного простору було розкладено на п'ятдесят одновимірних задач з подальшою їхньою суперпозицією. При цьому, типи показників – економічні, екологічні, фізичні, технологічні, художньо-естетичні було об'єднано у одній моделі. Інколи доцільно будувати моделі окремо за кожним з означених типів показників окремо, наприклад, за економічними з усіх факторів, що входять до досліджуваної ситуації або процесу, тощо.

Надамо класифікацію принципів створення моделей, про які йшла мова вище.

1. Принцип монопараметричний-монофакторний. Передбачає виконання геометричної кореляції за одним параметром серед усіх типо-моделей фактору "Вікно" (або будь-якого іншого).

2. Принцип монопараметричний-поліфакторний. Передбачає виконання геометричної кореляції за одним параметром, за усіма типо-моделями серед багатьох факторів.

3. Принцип поліпараметричний-монофакторний. Передбачає виконання геометричної кореляції за усіма параметрами (координатами) серед усіх типо-моделей у межах одного фактору.

4. Принцип поліпараметричний-поліфакторний. Передбачає виконання геометричної кореляції за усіма параметрами, за усіма типо-моделями серед багатьох факторів.

Безумовно, окрім згаданих принципів геометричної кореляції для побудови моделі можуть бути застосовані їхні комбінації.

Наведемо, для прикладу, алгоритм побудови моделі з використанням поліпараметричного-монофакторного принципу геометричної кореляції.

1. Формулюємо мету створення моделі.

2. Визначаємо основні параметри, відносно яких буде побудована модель.

3. За показниками будь-якого з визначених основних параметрів, призначаємо номери точок (типо-моделей) у порядку зростання (зменшення) значень параметру, що розглядається серед усіх типо-моделей у межах одного фактору.

4. Для основного параметру, будь-якої його окремої точки, яка являє собою типо-модель, а її параметри є координатами точки, визначаємо відсоткові – $\overline{K_i}$, та вагові – K_i коефіцієнти.

5. Одним із способів, які було задано вище, або якимось іншим, будуємо, у відповідності до (1), Б-поверхню, яка і є поліпараметричною-монофакторною моделлю багатофакторної ситуації.

6. Відповідний аналіз отриманої Б-поверхні надає шуканий розв'язок задачі для однієї тисячі (як для нашого прикладу) вихідних елементів.

В усіх, наведених у цій статті, прикладах було застосовано Б-поверхні, що побудовані на дев'яти дійсних точках евклідового простору E^3. Хоча вихідні точки фактору "Вікно" є точками евклідового простору E^{50}. Таким чином, з використанням композиційного методу геометричного моделювання, задачу п'ятидесятивимірного простору було зведено до великої кількості одно-, дво- та тривимірних задач.

Така можливість КМГМ пояснюється тим, що у основу його розробки покладено точкове числення Балюби-Найдиша, алгебра якого і передбачає таку можливість.

Для підвищення точності відображення вихідних факторів необхідно використовувати Б-поверхні, що побудовані на кількості точок більшій, ніж дев'ять, наприклад, 12, 16, 20, 25, тощо. Однак, збільшення їхньої кількості призводить до ускладнення та збільшення розрахунків навіть для E^3.

Висновок. Надано пояснення щодо геометричної формалізації, яку розроблено на основі алгебри точкового БН-числення, вказано на її відмінність від формалізації методами традиційної математики. На підставі застосування геометричної формалізації виникла необхідність введення нового поняття – геометричної кореляції.

Було показано спосіб розв'язання задачі п'ятидесятивимірного простору шляхом розв'язання п'ятдесяти одновимірних задач з подальшою суперпозицією отриманих розв'язків.

Надано визначення та класифікацію принципів геометричної кореляції у побудові моделей для багатофакторних ситуацій і процесів.

Запропоновано алгоритм побудови багатофакторної моделі, що відповідає поліпараметрично-монофакторному принципу геометричної кореляції.

Список літератури:

1. *Балюба, И. Г.* Точечное исчисление [Текст]: уч. пос. / *И. Г. Балюба, В. М. Найдыш; под ред. В. М. Верещаги*. – Мелитополь: Изд-во МГПУ им. Б. Хмельницкого, 2015. – 234 с.
2. *Нечволод, Л. І.* Сучасний словник іншомовних слів [Текст] / *Л. І. Нечволод*. – Харків: Торсинг плюс, 2007. – 768 с.
3. *Верещага, В. М.* Монофакторний принцип побудови моделі багатофакторних задач терморегенерації будівель [Текст] / *В. М. Верещага, Є. О. Адоньєв* // Сучасні проблеми моделювання. – 2016. – Вип. 7. – С. 24–31.
4. *Конопацький, Є. В.* Геометричне моделювання алгебраїчних кривих та їх використання при конструюванні поверхонь у точковому численні Балюби-Найдиша [Текст]: дис. … канд. техн. наук / *Є. В. Конопацький*. – Мелітополь, ТДАТУ, 2012. – 163 с.
5. *Кучеренко, В. В.* Формалізовані геометричні моделі нерегулярної поверхні для гіперкількісної дискретної скінченої множини точок [Текст]: дис. … канд. техн. наук / *В. В. Кучеренко*. – Мелітополь, ТДАТУ, 2013. – 232 с.
6. *Адоньєв, Є. О.* Алгоритм формування моделей багатофакторних процесів композиційного методу [Текст]: VI-ї Всеукр. наук.-практ. конф. / *Є. О. Адоньєв, В. М. Верещага, А. В. Найдиш* // Прикладна геометрія, дизайн, об'єкти інтелектуальної власності та інноваційна діяльність студентів та молодих вчених. – К.: НТУУ «КПІ», 2017. – Вип. 6. – С. 12–18.
7. *Адоньєв, Є. О.* Композиційний метод утворення поверхонь: суть, особливості та перспективи використання у моделюванні багатофакторних процесів [Текст]: XII Міжнар. наук.-практ. конф. / *Є. О. Адоньєв, В. М. Верещага, А. В. Найдиш* // Обухівські читання. – К., 2017. – С. 94–99.
8. *Адоньєв, Є. О.* Визначення та аналіз параболічної поверхні Балюби (БПП) [Текст] / *Є. О. Адоньєв, В. О. Верещага* // Системні технології. – 2017. – Вип. 1 (108). – С. 3–11.
9. *Бумага, А. І.* Точкове рівняння дуги параболи другого порядку [Текст]: IX Крымская междунар. научн.-практ. конф. / *А. І. Бумага* // Геометрическое и компьютеное моделирование: энергосбережение, экология, дизайн. – К.: КНУБА, 2012. – Вип. 90. – С. 49–52.
10. *Підгорний, О. Л.* Актуальні проблеми геометричного моделювання в задачах енергозбереження у будівництві [Текст] / *О. Л. Підгорний, В. О. Плоский, О. В. Сергейчук* // Вентиляція, освітлення та теплогазапостачання. – 2010. – Вип. 14. – С. 25–31.

Bibliography (transliterated):

1. Balyuba, I. G., Naydysh, V. M.; Vereshchaga, V. M. (Ed.) (2015). Tochechnoe ischislenie. Melitopol': Izd-vo MGPU im. B. Hmel'nickogo, 234.
2. Nechvolod, L. I. (2007). Suchasnyi slovnyk inshomovnykh sliv. Kharkiv: Torsynh plius, 768.
3. Vereshchaha, V. M., Adoniev, Ye. O. (2016). Monofaktornyi pryntsyp pobudovy modeli bahatofaktornykh zadach termorenovatsii budivel. Suchasni problemy modeliuvannia, 7, 24–31.
4. Konopatskyi, Ye. V. (2012). Heometrychne modeliuvannia alhebraichnykh kryvykh ta yikh vykorystannia pry konstruiuvanni poverkhon u tochkovomu chyslenni Baliuby-Naidysha. Melitopol, TDATU, 163.
5. Kucherenko, V. V. (2013). Formalizovani heometrychni modeli nerehuliarnoi poverkhni dlia hiperkilkisnoi dyskretnoi skinchenoi mnozhyny tochok. Melitopol, TDATU, 232.
6. Adoniev, Ye. O., Vereshchaha, V. M., Naidysh, A. V. (2017). Alhorytm formuvannia modelei bahatofaktornykh protsesiv kompozytsiinoho metodu. Prykladna heometriia, dyzain, obiekty intelektualnoi vlasnosti ta innovatsiina diialnist studentiv ta molodykh vchenykh. Kyiv: NTUU «KPI», 6, 12–18.
7. Adoniev, Ye. O., Vereshchaha, V. M., Naidysh, A. V. (2017). Kompozytsiinyi metod utvorennia poverkhon: sut, osoblyvosti ta perspektyvy vykorystannia u modeliuvanni bahatofaktornykh protsesiv. Obukhivski chytannia. Kyiv, 94–99.
8. Adoniev, Ye. O., Vereshchaha, V. O. (2017). Vyznachennia ta analiz parabolichnoi poverkhni Baliuby (BPP). Systemni tekhnolohii, 1 (108), 3–11.
9. Bumaha, A. I. Tochkove rivniannia duhy paraboly druhoho poriadku. Geometricheskoe i komp'yutenoe modelirovanie: ehnergosberezhenie, ehkologiya, dizayn. Kyiv: KNUBA, 90, 49–52.
10. Pidhornyi, O. L., Ploskyi, V. O., Serheichuk, O. V. (2010). Aktualni problemy heometrychnoho modeliuvannia v zadachakh enerhozberezhennia u budivnytstvi. Ventyliatsiia, osvitlennia ta teplohazapostachannia, 14, 25–31.

Надійшла (received) 24.05.2017

Бібліографічні описи / Библиографические описания / Bibliographic descriptions

Принципи геометричної кореляції при побудові моделей багатофакторних ситуацій і процесів/ Адоньєв Є. О., Верещага В. М. / Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків : НТУ «ХПІ», 2017. – No 19(1241). – С.48–53. – Бібліогр.: 10 назв. – ISSN 2079-5459.

Принципы геометрической корреляции при построении моделей многофакторных ситуаций и процессов/ Адоньев Е. А., Верещага В. М. / Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків : НТУ «ХПІ», 2017. – No 19(1241). – С.48–53. – Бібліогр.: 10 назв. – ISSN 2079-5459.

Principles of geometric correlation in the construction of models of multifactorial situations and processes/ Adoniev Y., Vereshchaga V. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2017. – № 19 (1241).– P.48–53. – Bibliogr.:10. – ISSN 2079-5459

Відомості про авторів / Сведения об авторах / About the Authors

Верещага Віктор Михайлович – доктор технічних наук, професор кафедри прикладної математики та інформаційних технологій Мелітопольського державного педагогічного університету ім. Богдана Хмельницького; вул. Гетьманська, 20, м. Мелітополь, Україна, 72300; e-mail: vervik49@gmail.com.

Адоньев Евгений Александрович – кандидат технических наук, доцент, декан Экономико-гуманитарного факультета Запорожского национального университета в г. Мелитополе; ул. Героев Украины, 160А, г. Мелитополь, Украина, 72316, e-mail: evgen.adoniev@gmail.com.

Верещага Виктор Михайлович – доктор технических наук, профессор кафедры прикладной математики и информационных технологий Мелитопольського государственного педагогического университета им. Богдана Хмельницкого; ул. Гетьманская, 20, г. Мелитополь, Украина, 72300; , e-mail: vervik49@gmail.com.

Adoniev Yevhen – PhD, associate professor, dean of the Economics and Humanities Faculty of the Zaporizhzhya National University in Melitopol. Heroiv Ukrainy str., 160A, Melitopol, Ukraine, 72316; e-mail: evgen.adoniev@gmail.com.

Vereshchaga Viktor – Doctor of Technical Sciences, Professor of the Department of Applied Mathematics and Information Technologies of the Melitopol State Pedagogical University named after Bohdan Khmelnytsky; Getmansky str., 20, Melitopol, Ukraine, 72300;, e-mail: vervik49@gmail.com.

УДК 004.056.55

Р. С. ГАНЗЯ

ВДОСКОНАЛЕННЯ МЕТОДУ НОРМУВАННЯ В КІЛЬЦІ Р-АДИЧНИХ ЧИСЕЛ

Аналізуються методи обчислення норми елемента в кільці р-адичних чисел. Пропонується використання альтернативного методу обчислення результанта через детермінант матриці Сильвестра, що може бути застосований для розрахунку норми елемента. Наводиться наша модифікація такого метода обчислення норми через зменшену матрицю Сильвестра. В роботі показано розрахунок теоретичної складності виконання методів, а також представлено порівняння теоретичних та практичних значень обчислення норми. Результати досліджень можуть бути використані при обчислені порядку еліптичних кривих в певних системних рішеннях.

Ключові слова: порядок еліптичної кривої, обчислення норми, матриця Сильвестра, результант.

Анализируются методы вычисления нормы элемента в кольце р-адических чисел. Предлагается использование альтернативного метода вычисления результанты через детерминант матрицы Сильвестра, который может быть применен для расчета нормы элемента. Приводится наша модификация такого метода вычисления нормы через уменьшенную матрицу Сильвестра. В работе показано расчет теоретической сложности выполнения методов, а также представлено сравнение теоретических и практических значений вычисления нормы. Результаты исследований могут быть использованы при вычислении порядка эллиптических кривых в определенных системных решениях.

Ключевые слова: порядок эллиптической кривой, вычисление нормы, матрица Сильвестра, результант.

In this paper, we show the main stages of the procedure of elliptic curves order computation, which are defined over binary field. The main attention is paid to the analysis of computational complexity (time complexity) of known methods for norm computation and research the phase of normalization in the generation elliptic curves.

The paper proposes the use of an alternative method of calculation resultants through determinants Sylvester's matrix, that can be used to compute the norm of the element. However, this improvement is due to computation determinant internal structure Sylvester's matrix and basic operations. This reduces the overall complexity of the norm computation for almost 30%. We provide an assessment of theoretical complexity of this method and compare with other methods of norm computation Using practical implementation of explore methods we note the similarity of theoretical and practical evaluations of norm computation.

The research results can be used for counting order of the elliptical curves in specific system solutions. The advantage of methods based on resultants is with using other module: is the possibility of parallelizing computations of determinant (while the analytical method cannot be parallelizing) and a lot more speed in that case. In fact, our modification of the method of norm computation is optimal in terms of computational complexity for the case when you need to switch between bases for norm computation.

Keywords: order of the elliptic curve, norm computation, Sylvester's matrix, resultant.

Вступ. В Україні та в світі дуже швидко прогресують інформаційні технології. В еру активного розвитку технологій кожен день з'являються нові інформаційні сервіси та послуги, що облегшують кінцевим користувачам існування в "інформаційному світі" та додають нові можливості. При цьому питання захисту інформації стає все актуальнішим. Для забезпечення безпеки інформаційних ресурсів в каналах зв'язку в України на рівні держави прийняті стандарти, що містять криптографічні алгоритми для виконання даних задач. Такі стандарти є або власні національні (ДСТУ 4145-2002, ДСТУ 7664-2014, ДСТУ 7624-2014), або гармонізовані міжнародні (ДСТУ ISO/IEC 14888, ДСТУ ISO/IEC 9796 та інші).

При використанні алгоритмів зі стандартів, розробники систем в більшості випадкові використовують рекомендовані у стандартах значення та показники. Наприклад, для національного стандарту електронного цифрового підпису (далі – ЕЦП) визначені наступні загальносистемні параметри: поле, на якому визначена еліптична крива (далі – ЕК); коефіцієнти