Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

ВАДНЬОВ ДМИТРО ОЛЕКСАНДРОВИЧ

УДК 519.874:519.852:519.816

МЕТОДИ ФОРМАЛІЗАЦІЇ ПОДАННЯ НЕЧІТКИХ ВЕЛИЧИН НА ОСНОВІ СПЕЦІАЛЬНИХ ПОСЛІДОВНОСТЕЙ ПРОСТИХ ЧИСЕЛ

01.05.04 – системний аналіз і теорія оптимальних рішень

Автореферат
дисертації на здобуття наукового ступеня
кандидата фізико-математичних наук

Київ – 2016

Дисертацією є рукопис

Робота виконана на кафедрі системного аналізу та теорії прийняття рішень факультету кібернетики Київського національного університету імені Тараса Шевченка МОН України

Науковий керівник: доктор фізико-математичнич наук, доцент
Івохін Євген Вікторович,
Київський національний університет імені Тараса Шевченка,
професор кафедри системного аналізу та теорії прийняття рішень
факультету кібернетики

Офіційні опоненти: доктор фізико-математичних наук, професор
Глибовець Микола Миколайович,
Національний університет «Києво-Могилянська академія» МОН
України, завідувач кафедри інформатики факультету інформатики

кандидат фізико-математичних наук, доцент
Антосяк Павло Павлович,
ДВНЗ «Ужгородський національний університет» МОН
України, доцент кафедри системного аналізу та теорії оптимізації
математичного факультету

Захист відбудеться “_10_” _жовтня_ 2016 року о 15.45 годині на засіданні спеціалізованої вченої ради Д 26.001.35 Київського національного університету імені Тараса Шевченка, за адресою: м.Київ, просп. Академіка Глушкова, 2-А, географічний факультет, ауд.310.

З дисертацією можна ознайомитися у Науковій бібліотеці імені М.Максимовича Київського національного університету імені Тараса Шевченка за адресою: 01601, м.Київ, вул.Володимирська, 58.

Автореферат розіслано "06" вересня 2016 р.

Вчений секретар
спеціалізованої вченої ради Д 26.001.35 Зінько П.М.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Класичні методи аналізу, вирішуючи багато завдань аналізу поведінки систем, не забезпечують повною мірою вирішення сучасних завдань дослідження функціонування об'єктів, зокрема в умовах невизначеності. Необхідна модернізація методів, що існують, і розробка нових методів аналізу складних об'єктів, що базуються на сучасних досягненнях математики, теорії систем і т.і.

Математичне моделювання різних реальних явищ містить два принципові етапи, що приводять до необхідності врахування складності та невизначеності систем. Перший з них об‘єктивно обумовлений невідомою точною поведінкою процесів, що моделюються. Це, в свою чергу, веде до неможливості сформулювати точний вигляд моделі фізичного процесу та до незручності використання обраних моделей на практиці, що пояснюється наявністю в них багатьох невизначеностей. Другий етап, пов‘язаний з проблемою адекватності математичного моделювання реальних систем, полягає в суб‘єктивній неспроможності оцінювати події процесів абсолютно точно. Неясність, нечіткість поведінки системи, відсутність достатньої інформації для моделювання процесів не дозволяють коректно описувати моделі в рамках традиційних підходів, що враховують невизначеність.

Для дослідження динаміки систем, які по своїй природі є достатньо складними і недостатньо визначеними, природно використовувати нечіткий підхід, при якому неточність моделі описується в термінах теорії нечітких множин. Існує багато підходів до побудови та математичної обґрунтованості загальної теорії нечітких множин. Треба відмітити, що аксіоматика даної теорії досить повно вивчена, а область застосування нечітких множин постійно розширюється завдяки залученню основних принципів теорії до аналізу складних систем різного призначення (економічних, екологічних, соціальних, політичних та ін.).

Використання теорії нечітких множин дає можливість розв’язувати складні недостатньо формалізовані задачі на основі нових конструктивних підходів. Теоретичні та прикладні передумови проведеного в дисертації дослідження на основі нечітких множин сформовані на основі робіт Заде Л.А., Орловського С.А., Мартинюка А.А., Зайченка Ю.П. та інших.

Дослідженню різних прикладних задач з використанням теорії нечітких множин присвячені роботи Алтунина А.Е., Вострова Н.Н, Кучина Б.Л., Борщевича В.И., Ботнаря В.И., Ягера Р.Р. та інших.

Одним з напрямків досліджень є формування нечітких баз даних на основі побудови табличних представлень, в яких використовуються оцінки особи, що приймає рішення. Створення таких баз даних і методів їх актуалізації дасть можливість проведення оперативної обробки нечіткої проблемної інформації.

Задачі аналітичної обробки сукупності нечітко визначених даних потребують вирішення двох задач: кластеризації даних в відносно однорідні групи та вибору рішення в умовах невизначеності. Розробка програмного забезпечення для обробки інформації, поданої в узагальненому вигляді з врахуванням динаміки інформаційних процесів, дозволить ефективно вирішувати зазначені вище завдання.

Одними з найперспективніших підходів в області математичного моделювання динаміки систем є використання декомпозиції моделей. Багатозв'язність моделей дозволяє за допомогою спеціальних перетворень встановлювати необхідні властивості вихідних систем на основі наявності таких властивостей у окремих підсистем. Дослідницька область нечітких динамічних систем – це нова методика, що зв'язує теоретичні дослідження в області комп'ютерних наук і прикладну математику.

Практичне використання математичних і програмних засобів представлення і обробки нечіткої інформації вимагає створення прикладних автоматизованих систем обробки даних та підтримки прийняття рішень, що є особливо важливим для забезпечення функціонування складних технічних, технологічних і соціальних систем в умовах невизначеності. Існуючі системи мають, як правило, вузький спеціалізований варіант застосування, який не завжди підходить для роботи з недостатньо формалізованими управлінськими ситуаціями. Тому актуальною задачею залишається розробка і впровадження програмних засобів, що застосовують узагальнене подання нечітких величин та розширюють семантику традиційних операторів обробки даних.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота є складовою частиною наукових робіт, що ведуться на кафедрі системного аналізу та теорії прийняття рішень факультету кібернетики та в науково-дослідному підрозділі Київського національного університету імені Тараса Шевченка. Дослідження виконувались в рамках науково-дослідної теми №11БФ015-06 "Проблеми теорії прийняття рішень та системного аналізу стохастичних мереж" (державний номер реєстрації 0111U006680, строк виконання 2011-2015г.г., в рамках програми "Інформатизація суспільства") і науково-дослідної теми «Розробка і впровадження інформаційної та організаційної системи заходів по забезпеченню інноваційної спрямованості науково-дослідних робіт в Київському національному університеті імені Тараса Шевченка», НДР № 08БП 013-01 (за напрямом Підпрограми "Інформаційні технології в науці та навчальному процесі").

Мета і задачі дослідження. Метою роботи є розробка конструктивної методики формалізації нечітких чисел, створення алгоритмів обробки нечітких даних та розробка математичного і програмного забезпечення для дослідження процесів обробки нечіткої інформації, результати якого можуть бути застосовані при розв'язанні актуальних прикладних задач в умовах невизначеності.

Об'єктом дослідження є моделі формалізації процесів, що функціонують в умовах невизначеності; моделі та технології моделювання процесів динаміки нечітких об'єктів і систем; методи та алгоритми обробки нечітких чисел. Предмет дослідження – процеси формалізації нечітко визначених даних та створення методів обробки нечіткої інформації.

Методи дослідження – методи, які базуються на системному підході у дослідженнях процесів формалізації та аналізу процесів у складних системах, що функціонують в умовах невизначеності. Використані у дисертації методи грунтуються на застосуванні теорії чисел, теорії нечітких множин, теорії оптимізації, теорії прийняття рішень і теорії та технології програмування. Для розв'язання практичних задач використано методи шифрування та фільтрації зображень.

Для подання нечітких даних використано спосіб формалізації нечіткості у вигляді нечітких трикутних чисел та метод визначення носія нечітких чисел у формі інтервалу, який задається елементами спеціальної послідовності простих чисел.

Наукова новизна одержаних результатів. У процесі розв'язання поставлених задач отримано нові наукові результати:

- розроблено нові способи формалізації нечітких цілих та раціональних чисел;
- запропоновано оригінальні послідовності простих чисел, досліджено їх властивості та наведено методику їх використання для опису функцій належності нечітких трикутних чисел;
- запропоновано новий метод опису невизначеності у вигляді складених нечітких чисел;
- запропоновано нове розширення синтаксису та семантики мови програмування для реалізації засобів нечіткого моделювання;
- вперше проведено дослідження та підвищення криптостійкості алгоритму шифрування даних з використанням послідовності простих чисел;
- узагальнено спосіб представлення нечітких баз даних, який дав можливість описувати нечіткі дані у вигляді таблиць-представлень з врахуванням суб'єктивного характеру нечіткості;
- розроблено нові конструктивні алгоритми кластеризації нечітко визначених даних, що описуються сукупністю складених нечітких чисел;
- вперше досліджено та отримано умови адекватності динаміки лінійних багатомірних нечітких систем при їх структурному спрощенні;
- запропоновано новий підхід для розв'язання задачі нечіткої фільтрації зображень.

Обґрунтованість та достовірність отриманих результатів підтверджується коректністю постановок задач, строгим доведенням теорем, узгодженістю отриманих аналітичних результатів з даними чисельного експерименту.

Практичне значення одержаних результатів полягає в розробці нового підходу до формалізації невизначеності, досліджено та вирішено ряд практичних задач з нечіткими вхідними даними. Запропоновано методи та підходи, що створено на основі використання спеціальних послідовностей простих чисел. Використовуючи спеціально розроблену методику проведено дослідження процесів функціонування систем великої розмірності. Ці результати можуть бути використані при створенні ефективних програмних систем для аналізу моделювання процесів у багатомірних нечітких об'єктах, для підтримки прийняття рішень при дослідженні процесів і систем, що функціонують в умовах невизначеності.

Наукові та прикладні результати дисертаційної роботи використовуються у навчальному процесі кафедри системного аналізу та теорії прийняття рішень факультету кібернетики при викладанні спеціальних курсів «Сучасні інформаційні технології», «Методи прийняття рішень в умовах нечіткості» та «Методи дослідження нечітких динамічних систем великої розмірності». (спеціальність «системи і методи прийняття рішень») .

Особистий внесок здобувача. Визначення загального напряму досліджень та ідея застосування спеціальних послідовностей простих чисел для формалізації функцій належності нечітких та складених нечітких чисел належать науковому керівнику – Івохіну Є.В. Усі результати, які складають основний зміст дисертації, отримано здобувачем самостійно. В роботах, опублікованих у співавторстві, здобувачу належить:

– розробка методів прийняття рішень за допомогою невизначених нечітких множин [1-3];
– доведення твердження про стійкість розв'язків нечітких лінійних різницевих систем [5];
– викладення та обґрунтування аксіоматики спеціальних послідовностей простих чисел [6];
– реалізація обробки запитів в нечітких базах даних [7].

Апробація результатів дисертації. Результати дослідження доповідалися на 7 наукових міжнародних конференціях і семінарах: Міжнародній науково-практичній конференції, присвяченій 170-річчю КНУ імені Тараса Шевченка та 60-річчю Інституту міжнародних відносин "Моделювання міжнародних відносин" (Київ, 2004); Міжнародній науковій конференції "Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту" (Євпаторія, Україна, вересень, 2013) [8]; Міжнародній науковій конференції "Обчислювальна та прикладна математика" (Київ, Україна, вересень, 2013, жовтень, 2014) [9]; III міжнародній науково-практичній конференції «Обчислювальний інтелект – 2015» (Черкаси, Україна, 2015) [10]; Міжнародній науковій конференції "Dynamic System Modeling and Stability Investigation" (Київ, травень, 2001); XXVII Міжнародній науковій конференції "Problems of Decision Making under Uncertainties" (PDMU-2016)], (Тбілісі-Батумі, Грузія, травень, 2016) [11]; на наукових семінарах факультету кібернетики Київського національного університету імені Тараса Шевченка.

Публікації. Основні наукові твердження, висновки і результати дисертації опубліковані в 11 наукових працях. З них – 7 статей у фахових виданнях з переліку МОН України [1-7], 1 стаття у науковому виданні, що входить у наукометричну базу [6], 4 – тези наукових конференцій [8-11].

Структура дисертації. Дисертаційна робота складається з вступу, чотирьох розділів, висновку, списку використаних джерел з 89 найменувань (на 7 сторінках) і двох додатків (на 6 сторінках). Загальний обсяг роботи становить 122 сторінки. Основний текст становить 104 сторінки. Робота містить 4 рисунки та 1 таблицю.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** до дисертаційної роботи обґрунтовано актуальність теми дослідження, наведено стислий огляд наукових результатів у відповідній галузі, сформульовано мету та задачі дослідження, його наукову новизну.

Перший розділ дисертаційної роботи присвячений огляду літератури, пов'язаної з нечіткими множинами і нечіткими системами. В розділі коротко розглянуто результати досліджень на основі нечітких множин та систем. Наведено аксіоматику нечітких множин, основні поняття і визначення нечітких величин і нечітких чисел, описано узагальнення поняття нечітких множин у вигляді невизначених нечітких множин. Проведено огляд використання нечітких множин та математичних моделей нечітких систем. Відмічено, що перспективним напрямком формалізації нечіткості є використання трикутних нечітких величин, основною ідеєю визначення яких є побудова інтервалів можливих значень невизначеного (невідомого) параметра з застосуванням лінійної функції належності.

Наведемо основні поняття. Нехай $\Re$ – скінченновимірний нормований простір.

Означення 1.1. Нечіткою множиною $\tilde{A}$ універсальної множини $X \subseteq \Re$, називається сукупність пар $\tilde{A} = \{(\mu_{\tilde{A}}(x), x)\}$, де $\mu_{\tilde{A}} : X \to [0,1]$ – відображення множини X в одиничний відрізок [0,1], яке називається функцією належності нечіткої множини $\tilde{A}$.

Означення 1.2. Нечітким відображенням R з X у довільний скінченновимірний простір Y називається нечітка підмножина $\tilde{R}$ в $X \times Y$ з функцією належності:

$$\mu_{\tilde{R}}(x, y) : X \times Y \to [0,1], x \in X, y \in Y. \tag{1}$$

Розглянемо в якості універсальної множини X множину дійсних чисел R^1, тобто $X = R^1$.

Означення 1.3. Нечітким числом називається впорядкована пара функцій $(u(r), v(r))$, $r \in [0,1]$, що задовольняють таким умовам:

1. $u(r)$ обмежена, неперервна зліва, неспадна функція на $[0,1]$;
2. $v(r)$ обмежена, неперервна зліва, незростаюча функція на $[0,1]$; (2)
3. $u(r) \le v(r)$, $r \in [0,1]$.

Означення 1.4. Нечітким трапецеїдальним числом $\tilde{A}$ називається впорядкована четвірка чисел *(a, b, c, d)*, які визначають функцію належності $\mu_{\tilde{A}}(x)$ вигляду:

1. $\mu_{\tilde{A}}(x) = \dfrac{x-a}{b-a}, x \in [a,b]$;
2. $\mu_{\tilde{A}}(x) = 1, x \in [b,c]$; (3)
3. $\mu_{\tilde{A}}(x) = \dfrac{d-x}{d-c}, x \in [c,d]$;
4. $\mu_{\tilde{A}}(x) = 0, x \notin [a,d]$.

Означення 1.5. Нечітким трикутним числом $\tilde{A}$ називається впорядкована трійка чисел *(a, b, c)*, які визначають функцію належності $\mu_{\tilde{A}}(x)$ вигляду:

1. $\mu_{\tilde{A}}(x) = \dfrac{x-a}{b-a}, x \in [a,b]$;
2. $\mu_{\tilde{A}}(x) = \dfrac{c-x}{c-b}, x \in [b,c]$; (4)
3. $\mu_{\tilde{A}}(x) = 0, x \notin [a,c]$.

Відзначимо, що нечітке трикутне число *(a, b, c)* є нечітким числом з функціями $u(r) = \dfrac{cr-a}{b-a},\ r \in [a/c, b/c],\ v(r) = \dfrac{c-rc}{c-b},\ r \in [b/c, 1]$.

Нечітке трикутне число виду *(a, b, b)*, яке називають лівим нечітким трикутним числом, визначається функцією належності вигляду

$$\mu_{\tilde{A}}(x) = 0, x < a;\ \ \mu_{\tilde{A}}(x) = \frac{x-a}{b-a}, x \in [a,b];\ \mu_{\tilde{A}}(x) = 1, x > b, \tag{5}$$

а нечітке трикутне число виду *(b, b, c)*, яке називають правим нечітким трикутним числом, - функцією належності

$$\mu_{\tilde{A}}(x)=1, x<b;\ \mu_{\tilde{A}}(x)=\frac{c-x}{c-b}, x\in[b,c];\ \mu_{\tilde{A}}(x)=0, x>c. \qquad (6)$$

Традиційні задачі математичного моделювання різних фізичних процесів можуть бути узагальнені за рахунок внесення до моделей опису параметрів задачі у формі нечітких множин. Як правило, до моделі вводиться додаткова інформація у вигляді функції належності заданих нечітких множин. Ці функції розглядаються як засіб наближеного відбиття експертом наявного в нього неформалізованого уявлення про реальну величину конкретного параметра.

Формальні модельні представлення з реалізаціями невизначеностей на заданих допустимих множинах легко розповсюджуються на широко вжиті останнім часом нечіткі моделі, методи побудови і функціонування яких базується на принципах теорії нечітких множин і нечіткої логіки.

На цьому шляху можуть бути отримані узагальнення традиційних методів дослідження динаміки систем, теорії управління і оптимізації. У цьому випадку постановки задач відрізняються від класичних лише розширенням множини станів до поняття нечіткої множини, а конкретний вид функцій належності визначається на основі різних додаткових припущень про властивості цих функцій з урахуванням специфіки наявної невизначеності, реальної ситуації на об’єкті й числа ступенів свободи у функціональній залежності.

Слід також зазначити, що при розв’язанні багатьох прикладних задач із застосуванням обчислювальних схем ефективно застосовуються спеціальні послідовності простих чисел, що може бути використано при побудові функцій належності нечітких множин.

У **другому розділі** дисертаційної роботи розглянуто спеціальні послідовності простих чисел, їх властивості, введено операції на даних послідовностях. Запропоновано алгоритм для наближення довільного раціонального числа за допомогою елементів введених послідовностей простих чисел. Розглянуто множину невід’ємних раціональних чисел, які представляються у вигляді частки двох елементів з розглянутих послідовностей. Для цієї множини отримано нижню і верхню спряжені множини, доведено твердження для оцінок інтервалів розміщення найближчих до заданого цілого простих чисел. Викладено методику подання цілих та раціональних нечітких чисел. Розроблено спосіб формалізації процесу динаміки функцій належності станів нечіткої дискретної системи. Запропоновано модифікацію базової схеми алгоритму Меркла-Хелмана шифрування повідомлень на основі нечіткого підходу, що сприяє підвищенню криптостійскості алгоритму. На основі формування нечітких представлень і формалізації нечітких операцій вибору за кількісними атрибутами узагальнено поняття нечітких баз даних для обробки слабоформалізованої інформації. Сформульовано розширення синтаксису та семантики мови С для реалізації програмних засобів нечіткого моделювання. Отримані результати дозволили обгрунтувати методику застосування трикутних нечітких чисел у вигляді інтервалів, межі яких вибираються з елементів спеціальних послідовностей простих чисел.

Підрозділ 2.1 присвячений опису властивостей послідовностей простих чисел відносно числа a та їх використанню у схемах моделювання різних характеристик в задачах з нечіткими даними.

Означення 2.1. Послідовності невід'ємних простих чисел $P_j(a)\ge 0$, $j\in Z$, що належать інтервалу $[a,\infty)$ при $j\ge 0$ або інтервалу $[0,a)$ при $j<0$ для заданого, необов'язково простого, цілого числа $a\ge 0$, називатимемо послідовностями простих чисел відносно числа a.

Неважко перевірити, що справедливі співвідношення, які характеризують властивості послідовності простих чисел:

1) $P_0(0)=0$, $P_0(1)=1$, $P_1(0)=1$;

2) $P_0(a)=a$, якщо число $a\ge 0$ - просте, інакше - $P_0(a)$ не існує;

3) $P_j(a)\le P_k(a)$, якщо $j\le k$, $P_j(a)<P_k(a)$ при $j<k$, $j\in Z$, $k\in Z$;

4) $P_j(a)=P_j(a+1)=\ldots=P_j(a+l)$ для усіх $1\le l<P_{j+1}(a)-P_j(a)$, $j=0,1,2,\ldots$, $a\ge 0$;

5) $P_j(a)=P_1(P_{j-1}(a))=P_1(P_1(P_{j-2}(a)))=P_2(P_{j-2}(a))=\ldots=P_{j-1}(P_1(a))$, якщо число $a\ge 0$ - просте, $j\in Z$;

6) $P_j(a)\ge a$ для усіх $j=0,1,2,\ldots$, якщо число $a\ge 0$ - просте, $P_j(a)>a$ для усіх $j=1,2,\ldots$, якщо $a\ge 0$ - непросте;

7) $P_j(a)<a$ для усіх $j=-1,-2,\ldots,j_0$, де номер $j_0<0$ визначається як найменший індекс простого числа з послідовності, для якого $0\le P_{j_0}(a)<a$.

Для послідовностей $P_j(a),\ j=0,1,2,\ldots$, простих чисел відносно довільного $a\ge 0$ введемо операцію зсуву на $m, m\in Z$, $j+m\ge j_0$, простих чисел у вигляді

$$P_j(a)\oplus m=P_{j+m}(a)=P_m(P_j(a)), \tag{7}$$

яка за визначенням не виводить за нижню межу заданої послідовності ($j+m\ge j_0$), і операцію n-кратної композиції ($n\in Z$) частки двох чисел $P_j(a)$ і $P_k(a)$, $j,k\in Z$, $j\le k$, у вигляді

$$\left.P_j(a)\middle/P_k(a)\right.\circ n=\left.P_j(a)\oplus n\middle/P_k(a)\oplus n\right.=\left.P_{j+n}(a)\middle/P_{k+n}(a)\right.=\left.P_n(P_j(a))\middle/P_n(P_k(a))\right.. \tag{8}$$

Припустимо, що розглядається довільне раціональне число r. Будемо вважати, що число r невід'ємне, $r\ge 0$. Справедливі такі твердження.

Лема 2.1. Довільне раціональне число $r=p/q$, $p\in Z$, $q\in N$, може бути подане у вигляді

$$r=\prod_{i=1}^{s_p}P_{k_i}(a_{k_i})\Big/\prod_{j=1}^{s_q}P_{n_j}(a_{n_j}), \tag{9}$$

де s_p, s_q - кількість множників у представленнях $|p|$ і q у вигляді відповідних добутків елементарних дільників, $a_{k_i}\ge 0$, $a_{n_j}\ge 0$ - деякі цілі числа, $k_i,n_j\in Z$, $i=\overline{1,s_p}$, $j=\overline{1,s_q}$.

Лема 2.2. Для довільного раціонального числа r і заданого $n\in N$ існують цілі числа $a\ge 0$, $b\ge 0$ і прості числа з номерами $i^*\in Z$ та $j^*\in Z$ з послідовностей простих чисел відносно a і b відповідно, такі, що для всіх $i,j\in N$, $i\le n$, $j\le n$, справедлива нерівність

$$\left|P_{i^*}(a)/P_{j^*}(b)-r\right|\le\left|P_i(a)/P_j(b)-r\right|. \tag{10}$$

Лема 2.3. Для довільних двох простих чисел $P_k(a)$, $P_n(a)$, $k\le n$, $k,n\in Z$, з послідовності простих чисел відносно числа a і довільного числа $T\ge 0$ справедливе співвідношення:

$$(P_k(a)+T)/(P_n(a)+T)\ge P_k(a)/P_n(a). \tag{11}$$

Розглянемо множину невід'ємних раціональних чисел $r(k,n)$, $k,n\in Z$, $0\le r(k,n)\le 1$, які подаються у вигляді частки двох простих чисел з послідовності відносно числа $a\ge 0$:

$$r(k,n)=P_k(a)/P_n(a),\ k\le n,\ k,n\in Z. \tag{12}$$

Без обмеження загальності покладемо $a = 0$. При цьому, раціональні числа $r(k,n)$ будуть подаватися у вигляді

$$r(k,n) = P_k(0)/P_n(0),\ k \le n\ ,\ k,n \in N \cup \{0\}. \tag{13}$$

З урахуванням операції зсуву на m простих чисел у послідовності $P_j(0)$, $j \in Z$, отримуємо співвідношення

$$r(k+m,n+m) = r(k,n) \circ m,\ m \in N \cup \{0\}. \tag{14}$$

Означення 2.2. Множину раціональних чисел $r_T(k,n)$, $T \ge 0$, $k \le n$, $k,n \in N \cup \{0\}$, що мають вигляд

$$r_T(k,n) = (P_k(0)+T)/(P_n(0)+T),\ k \le n\ ,\ k,n \in N \cup \{0\}, \tag{15}$$

назвемо T - послідовністю для множини чисел $r(k,n)$ і заданого $T \ge 0$.

Означення 2.3. Для заданої множини чисел $r(k,n)$, $k \le n$, $k,n \in N \cup \{0\}$, множину чисел

$$r_*(k+m,n+m) = \frac{P_k(0) \oplus m_*}{P_n(0) \oplus m},\ k \le n\ ,\ m \in Z\ ,\ k,n \in N \cup \{0\}, \tag{16}$$

де m_*: $0 \le m_* \le m$ при $m \in N \cup \{0\}$, і $m_* \le m$ при $m < 0$ - найбільше ціле число таке, що $P_k(0) \oplus m \big/ P_n(0) \oplus m \ge P_k(0) \oplus m_* \big/ P_n(0) \oplus m$, будемо називати нижньою спряженою множиною, а множину чисел

$$r^*(k+m,n+m) = \frac{P_k(0) \oplus m^*}{P_n(0) \oplus m},\ k \le n\ ,\ m \in Z\ ,\ k,n \in N \cup \{0\}, \tag{17}$$

де m^*: $m^* \ge m$ при $m \in N \cup \{0\}$ і $m \le m^* \le 0$ при $m < 0$ - найменше ціле число таке, що $P_k(0) \oplus m \big/ P_n(0) \oplus m \le P_k(0) \oplus m^* \big/ P_n(0) \oplus m$, - верхньою спряженою множиною.

Лема 2.4. Справедливі співвідношення

$$r(k,n) \le r_T(k,n), \tag{18}$$

$$r_*(k+m,n+m) \le r(k+m,n+m), \tag{19}$$

$$r(k+m,n+m) \le r^*(k+m,n+m), \tag{20}$$

$$r_*(k+m,n+m) \le r_T(k+m,n+m), \tag{21}$$

для довільних $T \ge 0$, $k,n \in N \cup \{0\}$, $k \le n$, $m \in Z$.

Розглянемо далі дві неспадні числові послідовності:

1) $$g(n) = \max\{g(n-1), r(n)\},\quad n \in N,\ g(0) = 0, \tag{22}$$

де $r(n)$, $n \in N$, - відстань між двома найближчими до числа $n \in N$ простими числами $q_s(n), q_{s+1}(n)$, $s \in N$, такими, що $n \ge q_s(n)$, $n < q_{s+1}(n)$, тобто $r(n) = q_{s+1}(n) - q_s(n)$;

2) $$p(n) = \max\{p(n-1), l(n)\},\quad n \in N,\ p(0) = 0, \tag{23}$$

де $l(n) = P_1(n) - P_{-1}(n)$, $n \in N$, $P_{-1}(n), P_1(n)$ - попереднє і наступне прості числа відносно числа $n \in N$.

Лема 2.5. Для всіх значень $n \in N$, $n \ge 7$, таких, що число $2n+1$ не є простим, справедлива нерівність

$$2p(n) > p(2n). \tag{24}$$

Лема 2.6. Для всіх значень $n \in N$, $n \ge 4$, таких, що число $2n+3$ є простим, справедлива нерівність

$$P_1(2n+3) < 2n+3+2p(n). \tag{25}$$

Теорема 2.1. Нехай для довільного значення $n \in N$ величина $p(n) = \overline{p}$. Тоді справедливі нерівності

$$2n - 2\overline{p} + 1 \le P_{-1}(2n), \tag{26}$$

$$2n - 2\overline{p} + 3 \le P_{-1}(2n+1). \tag{27}$$

Теорема 2.2. Нехай для довільного значення $n \in N$ величина $p(n) = \overline{p}$. Тоді справедливі нерівності

$$P_1(2n) \le 2n + 2\overline{p} - 3, \tag{28}$$

$$P_1(2n+1) \le 2n + 2\overline{p} - 1. \tag{29}$$

Пропонуються способи подання цілих та раціональних чисел на основі застосування спеціальних множин простих чисел.

Схема формалізації нечітких цілих чисел.

Означення 2.4. Нечітким цілим числом $\tilde{n}$ будемо називати впорядковану трійку чисел *(k, n, l)*, $k \le n \le l$, $k, n, l \in Z$, де

$$k = \begin{cases} P_{-1}(n), n \ge 0, \\ -P_1(-n), n < 0, \end{cases} \quad l = \begin{cases} P_1(n), n \ge 0, \\ -P_{-1}(-n), n < 0, \end{cases} \tag{30}$$

а $P_1(\cdot), P_{-1}(\cdot)$ - попереднє і наступне прості числа відносно n, $n \ge 0$, и $-n$, $n < 0$.

Такий підхід дозволяє для кожного значення $n \in Z$ визначити нечітке ціле число $\tilde{n}$ = *(k, n, l)*, не вказуючи діапазон подання нечіткого числа $[k, l]$: можна покласти k та l у вигляді (2.32) і використати лінійну функцію належності

$$\mu_{\tilde{n}}(x) = \frac{x-k}{n-k}, x \in [k, n]; \quad \mu_{\tilde{n}}(x) = \frac{l-x}{l-n}, x \in [n, l]; \quad \mu_{\tilde{n}}(x) = 0, x \notin [k, l]. \tag{31}$$

Запропоноване означення нечіткого цілого числа спрощує виконання традиційних арифметичних операцій додавання, віднімання, множення і ділення над нечіткими цілими числами. Для двох нечітких цілих $\tilde{n}$ та $\tilde{m}$, заданих у вигляді нечітких трикутних чисел $\langle k_n, n, l_n \rangle$ і $\langle k_m, m, l_m \rangle$ відповідно, маємо

1. $\tilde{n} + \tilde{m} = \langle k_+, n+m, l_+ \rangle$, (32)

де $k_+ = \begin{cases} P_{-1}(n+m), n+m \ge 0, \\ -P_1(-n-m), n+m < 0, \end{cases} \quad l_+ = \begin{cases} P_1(n+m), n+m \ge 0, \\ -P_{-1}(-n-m), n+m < 0, \end{cases}$

2. $\tilde{n} - \tilde{m} = \langle k_-, n-m, l_- \rangle$, (33)

де $k_- = \begin{cases} P_{-1}(n-m), n-m \ge 0, \\ -P_1(-n+m), n-m < 0, \end{cases} \quad l_- = \begin{cases} P_1(n-m), n-m \ge 0, \\ -P_{-1}(-n+m), n-m < 0, \end{cases}$

3. $\tilde{n} * \tilde{m} = \langle k_*, n*m, l_* \rangle$, (34)

де $k_* = \begin{cases} P_{-1}(n*m), n*m \ge 0, \\ -P_1(-n*m), n*m < 0, \end{cases} \quad l_* = \begin{cases} P_1(n*m), n*m \ge 0, \\ -P_{-1}(-n*m), n*m < 0, \end{cases}$

4. $\tilde{n} / \tilde{m} = \langle k_{div}, n/m, l_{div} \rangle$, $m \ne 0$, (35)

де $k_{div} = \begin{cases} P_{-1}(n/m), n/m \ge 0, \\ -P_1(-n/m), n/m < 0, \end{cases} \quad l_{div} = \begin{cases} P_1(n/m), n/m \ge 0, \\ -P_{-1}(-n/m), n/m < 0, \end{cases}$

5. $\tilde{n}$ % $\tilde{m} = \langle k_{\mathrm{mod}}, n\%m, l_{\mathrm{mod}} \rangle$, $n \ge 0$, $m > 0$, (36)

де $k_{\mathrm{mod}} = \begin{cases} P_{-1}(n\%m), n\%m \ge 0, \\ -P_1(-n\%m), n\%m < 0, \end{cases}$ $l_{\mathrm{mod}} = \begin{cases} P_1(n\%m), n\%m \ge 0, \\ -P_{-1}(-n\%m), n\%m < 0, \end{cases}$

і при цьому результати не залежать від початкових інтервалів $[k_n, l_n]$ і $[k_m, l_m]$ подання нечітких цілих чисел $\tilde{n}$ та $\tilde{m}$.

Схема формалізації нечітких раціональних чисел.

Використаємо послідовності простих чисел для комп'ютерного моделювання нечітких раціональних чисел, базуючись на поданні довільних раціональних чисел у форматі IEEE 754.

Припустимо, що для подання раціональних чисел використовуються n-байтні двійкові подання. Це означає, що будь-яке раціональне число $x \in R$ може бути подане у двійковому вигляді

$$x = \left[\underset{1\,bit}{s} \mid \underset{p\,bit}{characteristic} \mid \underset{q\,bit}{mantissa} \right], \tag{37}$$

де $s = \begin{cases} 0, x \ge 0 \\ 1, x < 0 \end{cases}$ - знак числа x, $characteristic = k + BIAS$, k - порядок числа x за основою 2 (степінь, до якої необхідно піднести число 2, щоб виконувалась умова $m = |x| * 2^k \in [1,2)$), $BIAS > 0$ - деяка константа, величина якої обчислюється за формулою $BIAS = 2^{p-1} - 1$, $mantissa = m - 1$ - мантиса числа x без уявної одиниці, p та q - відповідно кількості розрядів для представлення характеристики та мантиси числа x, $(p + q + 1)/8 = n$.

У представленні (37) характеристика та мантиса визначаються полями двійкових цифр, які є записами цілих чисел. Використовуючи поняття нечіткого цілого числа, отримуємо схему для визначення діапазону представлення нечіткого трикутного раціонального числа.

Схема формалізації процесу динаміки функцій належності.

Запропоноване у (12) подання множини раціональних чисел $r(k,n)$, $k \le n$, $k \in Z$, $n \in Z$, та введені операції на послідовностях простих чисел у вигляді (7), (8) зручно використовувати при формалізації та дослідженні динаміки величин міри належності нечітких множин.

Динаміку процесів зміни станів системи опишемо у вигляді нечіткої дискретної моделі:

$$\mu_{s+1}(x) = A_s \circ \mu_s(x),\ s = 0,1,2,.... \tag{38}$$

де $A_s, s = 0,1,2,...$– неперервні оператори, що визначають динаміку змін значень функцій належності, $\mu_s(x) = (\mu_s(x_1),...,\mu_s(x_n))^T$, $\mu_{s+1}(x) = (\mu_{s+1}(x_1),...,\mu_{s+1}(x_n))^T$ – вектор-функції належності нечітких множин $\tilde{X}(t)$ у моменти часу t_s, t_{s+1} відповідно, "o" - операція композиції.

За лемою 2.2 для довільного раціонального числа r існують номери k та n елементів з послідовностей простих чисел такі, що величина $r(k,n) = P_k(a)/P_n(a)$ наближає число r з будь-якою точністю. Таким чином, за допомогою частки значень $P_k(a)/P_n(a)$ з відповідними номерами k та n, $k \in Z$, $n \in Z$, елементів послідовності простих чисел відносно a визначимо величину міри належності елементів $x_1,...,x_n$ до нечіткої множини $\tilde{X}_s$, $s = 0,1,2,...$ у вигляді:

$$\mu_s(x_i) = P^s_{k_i}(a)/P^s_{n_i}(a),\ k_i \in Z,\ n_i \in Z,\ k_i \le n_i,\ i = \overline{1,n},\ s = 0,1,2,.... \tag{39}$$

Використовуючи операцію кратної композиції частки простих чисел (7), запропоновано схему модифікації величин міри належності. Дійсно, якщо модель динаміки має вигляд (38), то, розглядаючи в якості A_s, $s = 0,1,2,...$, векторні $A_s = (a^s_i)_{i=\overline{1,n}}$ або скалярні $A_s = (a^s_0)$, $s = 0,1,2,...$ цілочислові величини, що визначають збільшення ($a^s_i > 0$, $i = \overline{0,n}$), зменшення ($a^s_i < 0$, $i = \overline{0,n}$) або незмінність ($a^s_i = 0$, $i = \overline{0,n}$) рівнів належності станів системи, динамічний процес можна формалізувати у вигляді $\mu_{s+1}(x_i)=\mu_s(x_i)\circ a_i^s = P_{k_i}^s(a)/P_{n_i}^s(a)\circ a_i^s$, $k_i+a_i^s \ge j_0^i$, $i=\overline{1,n}$, $s=0,1,2,\ldots$, у випадку векторного представлення коефіцієнтів $A_s=\{a_i^s\}_{i=\overline{1,n}}$, $s=0,1,2,\ldots$, та $\mu_{s+1}(x_i)=$ $=\mu_s(x_i)\circ a_0^s = P_{k_i}^s(a)/P_{n_i}^s(a)\circ a_0^s$, $k_i+a_0^s \ge j_0^i$, $i=\overline{1,n}$, $s=0,1,2,\ldots$, у випадку скалярного подання $A_s=\{a_0^s\}$, $s=0,1,2,\ldots$, а величини j_0^i, $i=\overline{1,n}$, - найменші відповідні значення індексів у послідовностях простих чисел, для яких справедлива властивість 7).

Потрібно відмітити конструктивність даного підходу для формалізації та обробки величин мір належності нечітких множин, що знайшло застосування при вирішенні ряду прикладних задач.

У *підрозділі 2.2* розглянуто алгоритм шифрування на основі задачі про рюкзак Меркла-Хелмана та його вдосконалення на основі застосування різних додаткових схем та процедур, що підвищують захищеність алгоритму.

Запропоновано модифікацію базової схеми алгоритму за допомогою нечіткого підходу та послідовностей невід'ємних простих чисел $P_j(a)\ge 0$, $j\in Z$ відносно числа a.

Числа, що входять до відкритого ключа $K=\{r_1,\ldots,r_n\}$, є довільними цілими числами. Традиційне поняття нечіткості в даному випадку може інтерпретуватися як рівень складності кодування кожного числа $r_j \in K, j=\overline{1,n}$.

Для визначення величини складності доповнимо відкритий ключ двома довільними значеннями k та l, $k\le l$, $k=0,1,2,\ldots$, $l=1,2,3,\ldots$, за якими з послідовності простих чисел визначаються величини $s=P_k(a)$, $q=P_l(a)$ для деякого числа $a\ge 0$. За таких умов отримуємо, що $0\le s/q\le 1$. Ця величина може служити показником складності кодування, а за допомогою значень s та q змінюються ваги відкритого ключа K та величини N та T за наступною схемою:

- для чисел T та N, які є взаємно простими числами, обчислюються числа $P_s(T)$ та $P_q(N)$ відповідно, де $s=P_k(a)$, $q=P_l(a)$;
- для цілих чисел $r_j\in K, j=\overline{1,n}$, які входять до ключа K, обчислюються величини $u_j=P_s(r_j)-r_j$ та $v_j=P_q(r_j)$, $j=\overline{1,n}$, $s=P_k(a)$, $q=P_l(a)$;
- формується вектор пар елементів $\overline{K}=\{(u_1,v_1),\ldots,(u_n,v_n)\}$, який буде новим значенням відкритого ключа *K*. Величини $P_s(T)$, $P_q(N)$ та вектор $\overline{K}$ пересилаються отримувачу разом з зашифрованим за допомогою елементів v_j, $j=\overline{1,n}$, повідомленням.

Зрозуміло, що дана схема допускає різні модифікації. В якості основних можна розглядати:

- схему з кодуванням лише чисел N та T,
- паралельне кодування чисел N , T та чисел ключа K,
- послідовне кодування чисел N та T у числа $P_s(T)$ та $P_q(N)$, відповідно, з подальшим перетворенням елементів ключа $K=\{r_1,\ldots,r_n\}$ за традиційною процедурою $r_j * P_s(T) \bmod P_q(N)$, $j=\overline{1,n}$, $s=P_k(a)$, $q=P_l(a)$ і кодуванням отриманих значень вектором пар елементів $\overline{K}=\{(u_1,v_1),\ldots,(u_n,v_n)\}$.

У *підрозділі 2.3* запропоновано узагальнення поняття нечітких баз даних. для довільної чіткої бази даних може бути побудоване нечітке представлення (нечітка БД), в якому інформація про характеристики (поля) об'єктів проблемної області подаються парою стовбців: у першому – конкретні значення атрибута з таблиці чіткої бази даних, у другому – значення відповідності даних першого стовпця деякому правилу (нечіткому поняттю). Ця процедура має назву фазифікації чітко визначених даних.

Результат процесу фазифікації чіткого відношення $R = \{< d_1, d_2, ..., d_n >\}$, де d_s - елементи з доменів D_s, $s = \overline{1,n}$, за i-им атрибутом, $i = \overline{1,n}$, можна виразити у вигляді нової реляційної таблиці (R-таблиці). Це нове нечітке відношення

$$\overline{R} = \{< d_1, d_2, ..., (d_i, \mu_{\tilde{A}_i}(d_i)), ..., d_n >\}, \quad (40)$$

що формується як множина кортежів з $n+1$ елемента, в яких величини $\mu_{\tilde{A}_i}(d_i)$ задають міру належності значень елементів d_i, $i = \overline{1,n}$, деякій нечіткій множині $\tilde{A}_i = \{(d, \mu_{\tilde{A}_i}(d)), d \in D_i\}$. Таким чином, операція фазифікації даних кожного з доменів D_s, $s = \overline{1,n}$, за атрибутами p_i, $i = \overline{1,n}$, реалізується за допомогою операції розширення R-таблиць у вигляді складеної нечіткої множини

$\overline{R} = \{< (d_1, \mu_{\tilde{A}_1^1}(d_1) | ... | \mu_{\tilde{A}_1^{p_1}}(d_1)), ..., (d_i, \mu_{\tilde{A}_i^1}(d_i) | ... | \mu_{\tilde{A}_i^{p_i}}(d_i)), ..., (d_n, \mu_{\tilde{A}_n^1}(d_n) | ... | \mu_{\tilde{A}_n^{p_n}}(d_n)) >\}$.

У *підрозділі 2.4* запропоновано розширення синтаксису та семантики мови С для реалізації засобів нечіткого моделювання. Опис нечітких числових даних та запис дій для реалізації м'яких обчислень та нечіткого моделювання потребує розширення синтаксису та семантики мов С/С++.

Використовуючи наведені вище підходи для подання нечітких цілих та раціональних значень, опис типів для позначення нечітких чисел розширимо новими типами, що утворюються на основі використання лексем для стандартних скалярних типів, перед якими записується ключове слово *fuzzy* (наприклад, *fuzzy int*). При цьому, довільна змінна з префіксом *fuzzy* передбачає подання значення у вигляді нечіткого трикутного числа з носієм, який задається у формі інтервалу, побудованому на основі найближчих простих чисел (у цілочисловому випадку – для самого числа, а у випадку раціональних чисел – для мантиси числа) і з урахування граничних значень відповідних діапазонів.

Для запису дій з нечіткими змінними мають застосовуватися арифметичні операції та операції порівняння, умовний оператор *if*, оператор-перемикач *switch*, оператори циклу *for* та *while*. Пропонується семантика розширення у вигляді наступних правил:

1. Виконання арифметичних операцій відбувається за правилами (32)-(36).
2. Виконання операцій порівняння і визначення результатів обчислення умовних виразів з нечіткими числами в операторах *if* , *switch, while* може бути описане на основі нечітких відношень, заданих для двох нечітких трикутних чисел. Нечіткий результат порівняння двох заданих нечітких чисел визначається у вигляді меншої величини у розумінні нечіткого відношення переваги "<". Для визначення «меншого» застосовується нечітке відношення переваги, введене Орловським. В рамках даного підходу вважається, що нечітке відношення переваги $g(a,b)$ для довільних нечітких елементів $a \in \tilde{A}, b \in \tilde{B}$ за умови $\mu_g(a,b) = \min\{\mu_{\tilde{A}}(a), \mu_{\tilde{B}}(b), \mu_{\tilde{A}\times\tilde{B}}(a,b)\} > 0$ визначає співвідношення у вигляді $a < b$ із ступенем $g(a,b) = \mu_g(a,b)$.

Третій розділ дисертаційної роботи присвячено визначенню та застосуванню складених нечітких чисел трикутного вигляду. В розділі визначено поняття складених нечітких чисел, досліджено їх властивості, сформульовано поняття відстані між довільними складеними нечіткими числами на основі побудови множин рівня спеціального вигляду, розроблено схему для порівняння відстаней, вирішено задачу кластеризації за умов подання даних у формі складених нечітких чисел, запропоновано математично обгрунтований декомпозиційний підхід для дослідження поведінки нечітких багатомірних систем, що функціонують в умовах невизначеності.

Розглянуто моделі та властивості розв'язків нечітких різницевих систем, стани яких описуються за допомогою складених нечітких чисел. Запропоновано підхід, що базується на декомпозиції нечітких систем на підсистеми. Сформульовано і доведено твердження про адекватність поведінки розв'язків вихідної системи та отриманих нечітких підсистем.

У *підрозділі 3.1* наведено аксіоматику складених нечітких чисел.

Нехай задано сукупність нечітких чисел $\tilde{A}_1, \ldots, \tilde{A}_m$, визначених в універсальних множинах $X_1, \ldots, X_m$, де $X_i \subseteq R^1, i = \overline{1,m}$. Тоді можна говорити, що задано множину нечітких чисел. Будемо вважати, що кожне з них має трикутний вигляд, тобто $\tilde{A}_i = \{(a_i, b_i, c_i)\}$, $a_i \le b_i \le c_i$, $i = \overline{1,m}$, з лінійними функціями належності $\mu_{\tilde{A}}(x)$ вигляду (1.22).

Розглянемо універсальну множину X у вигляді декартового добутку $X = \mathop{\times}\limits_{i=1}^{m} X_i$. Сформуємо вектор

$$\tilde{A}^m = \{(x^1, \mu_{\tilde{A}_1}(x^1)), (x^2, \mu_{\tilde{A}_2}(x^2)), \ldots, (x^m, \mu_{\tilde{A}_m}(x^m))\}, \quad x^i \in X_i, \ i = \overline{1,m}. \tag{41}$$

Означення 3.1. Вектор $\tilde{A}^m$ назвемо складеним нечітким числом в універсальній множині $\mathop{\times}\limits_{i=1}^{m} X_i$.

Означення 3.3. Множину $L^m(\alpha) = \{x^1 \in X_1, x^2 \in X_2, \ldots, x^m \in X_m : \mu_{\tilde{A}_1}(x^1) \ge \alpha, \mu_{\tilde{A}_2}(x^2) \ge \alpha, \ldots,$ $\mu_{\tilde{A}_m}(x^m) \ge \alpha\}$ назвемо множиною рівня $\alpha \in (0,1]$ складеного нечіткого числа $\tilde{A}^m$.

Скінченний набір складених нечітких чисел $\tilde{A}^m$ у множині $X = \mathop{\times}\limits_{i=1}^{m} X_i$ позначимо $K(\tilde{A}^m)$, $|K(\tilde{A}^m)| = k$.

Означення 3.6. Нечітка множина точок за Уонгом

$$\tilde{D}(\tilde{A}^m) = \{(d, \gamma) : d = \left\| L^m_{\tilde{A}}(\gamma) \right\|, \ \gamma = \min_{i=\overline{1,m}} \mu_{\tilde{A}_i}(x^i) \in (0,1]\}, \tag{42}$$

де $\|\cdot\|$ - евклідова норма простору R^m, визначає метрику на множині $K(\tilde{A}^m)$.

Таким чином, кожне складене нечітке число $\tilde{A}^m$ «вимірюється» за допомогою нечіткої величини $\tilde{D}(\tilde{A}^m)$, а для знаходження нечіткої відстані $\rho(\tilde{U}^m, \tilde{V}^m)$ між довільними складеними нечіткими числами $\tilde{U}^m, \tilde{V}^m$ можна використати нечітку величину

$$\rho(\tilde{U}^m, \tilde{V}^m) = \{(d, \gamma) : d = \left\| L^m_{\tilde{U}}(\gamma) - L^m_{\tilde{V}}(\gamma) \right\|, \gamma = \min_{Z \in \{U,V\}, i=\overline{1,m}} \mu^Z_{\tilde{A}_i}(x^i)\}, \tag{43}$$

У підрозділі 3.2 визначено спосіб порівняння відстаней між двома довільними парами складених нечітких чисел за допомогою нечіткого відношення переваги, яке формулюється на основі порівняння відстаней нечітких множин до деякої наперед заданої чіткої множини і знаходженні компромісного значення в процесі вибору найменшої з них.

Нехай $\tilde{\rho}_1 = \rho(\tilde{U}_1^m, \tilde{V}_1^m)$, $\tilde{\rho}_2 = \rho(\tilde{U}_2^m, \tilde{V}_2^m)$ - нечіткі відстані між складеними нечіткими числами $\tilde{U}_1^m, \tilde{V}_1^m$ та $\tilde{U}_2^m, \tilde{V}_2^m$ відповідно. За допомогою нечіткого відношення переваги можна порівнювати відстані $\tilde{\rho}_1$ та $\tilde{\rho}_2$: вираз $g(\tilde{\rho}_1, \tilde{\rho}_2)$ визначає ступінь того, наскільки $\tilde{\rho}_1$ «менше», ніж $\tilde{\rho}_2$. Це також надає можливість визначити "найближчий" до заданого складеного нечіткого числа $\tilde{Z}^0$ елемент $\tilde{Z}^*$, де $\tilde{Z}^*$ - складене нечітке число, значення функцій належності якого для кожного $x^i \in X_i$, $i = \overline{1,m}$, визначаються з співвідношення $\mu^{Z^*}_{\tilde{A}_i}(x_i) = \min_{x \in X_i}(1 - \mu_T(x_i, x)) = 1 - \max_{x \in X_i} \mu_T(x_i, x)$,

$i=\overline{1,m}$, де через T позначено нечітке відношення строгої переваги, що відповідає $g(a,b)$, $a,b\in X_i$, $i=\overline{1,m}$:

$$\mu_T(a,b)=\begin{cases}0, & якщо\ \mu_g(a,b)<\mu_g(b,a)\\ \mu_g(a,b)-\mu_g(b,a), & у\ протилежному\ випадку\end{cases}.$$

Підрозділ 3.3 присвячено розгляду задачі кластеризації даних, поданих у вигляді сукупності складених нечітких чисел $\{\tilde{A}^{m(j)}, j=\overline{1,p}\}$ з $K(\tilde{A}^m)$. На основі введеного поняття відстані між складеними нечіткими числами та способу їх порівняння наведено алгоритми нечіткого пікового та різницевого групування даних, поданих у вигляді сукупності складених нечітких чисел $\{\tilde{A}^{m(j)}, j=\overline{1,p}\}$ з $K(\tilde{A}^m)$.

Вважається, що цю сукупність можна згрупувати в k кластерів. На початку процесу задається величина $\gamma\in(0,1]$, яка буде визначати рівень нечіткості даних, що розглядаються. Припустимо, що складені нечіткі числа $\tilde{A}^{m(j)}$, $j=\overline{1,q}$, $q\le p$, мають непорожні множини рівня $L^m(\gamma)$, що розглядаються як звичайні вектори $S(\tilde{A}^{m(j)})= =\{x^{1(j)},x^{2(j)},\dots,x^{m(j)}\}$, $j=\overline{1,q}$.

Визначено особливості та уточнення кожного з методів кластеризації в залежності від умов застосування та його структурно-концептуальної реалізації.. Результати дослідження та застосування методів кластеризації на сукупності двомірних складених нечітких чисел дозволили зробити ряд висновків щодо оптимізації окремих схем алгоритмів.

У *підрозділі 3.4* досліджено математичні аспекти процесу моделювання динаміки нечітких систем великої розмірності.

Розглянемо нечітку динамічну систему S, множина станів якої описується сукупністю складених нечітких чисел $\tilde{A}_S=\{(x,\mu_S(x)),x\in X\}$, де $X=R^1$ - універсальна множина. Припустимо, що в системі виділено дві підсистеми S_1,S_2, стани яких також мають бути представлені у вигляді складених нечітких чисел $\tilde{A}_{S_1}=\{(x^1,\mu_{S_1}(x^1)),x^1\in X_1\}$ та $\tilde{A}_{S_2}=\{(x^2,\mu_{S_2}(x^2)),x^2\in X_2\}$ універсальних множин $X_1\in R^1, X_2\in R^1$ відповідно, $X_1\cup X_2=X$.

Для визначення функцій належності $\mu_{S_1}(x^1):X_1\to[0,1]$ та $\mu_{S_2}(x^2):X_2\to[0,1]$ нечітких множин $\tilde{A}_{S_1}$ та $\tilde{A}_{S_2}$ використаємо підхід з теорії корисності. Ототожнюючи $\mu_{S_1}(x^1)$ та $\mu_{S_2}(x^2)$ з корисністю підсистем S_1,S_2, представимо величини міри належності $\mu_S(x)$ у вигляді

$$\begin{aligned}\mu_S(x^1)&=[\mu_{S_1}(x^1)]^\alpha, x^1\in X_1,\\ \mu_S(x^2)&=[\mu_{S_2}(x^2)]^\beta\ x^2\in X_2,\end{aligned}\quad \alpha,\beta\ge 0. \tag{44}$$

Розглянемо універсальний простір $X_1\cup X_2=X$ розмірності $m=m_1+m_2$, який містить значення станів нечіткої системи S, складеної з підсистем S_1,S_2. Визначено правило побудови значень функції належності $\mu(x)$ для кожного $x=(x^1,x^2)\in X$ на основі величин функцій належності станів підсистем S_1,S_2, заданих за допомогою співвідношень (44).

Запропоновані процедури декомпозиції та агрегування дозволяють вирішити задачу дослідження динаміки багатомірних нечітких систем наступного вигляду

$$\tilde{X}_{k+1}=R_k\circ\tilde{X}_k \tag{45}$$

де $\tilde{X}_k=\tilde{X}(t_k)$ - складні нечіткі числа, що використовуються для опису станів системи, $\tilde{X}_0=\tilde{X}(t_0)$ - складне нечітке число, що визначає початковий стан системи, $R_k=R(t_k)$ - оператори переходу, що визначають динаміку системи, $t_k=k$, $k=0,1,\dots$, - моменти часу, $\circ$ - операція композиції.

Нехай система (45) складається з двох підсистем. Тоді вона буде мати вигляд

$$\begin{aligned}\tilde{X}^{(1)}_{k+1} &= \mathrm{R}^{(1)}_k \mathrm{o} \tilde{X}^{(1)}_k + F^{(1)}_k \mathrm{o} \tilde{X}^{(2)}_k,\\ \tilde{X}^{(2)}_{k+1} &= \mathrm{R}^{(2)}_k \mathrm{o} \tilde{X}^{(2)}_k + F^{(2)}_k \mathrm{o} \tilde{X}^{(1)}_k,\end{aligned} \tag{46}$$

де $R^{(1)}_k, R^{(2)}_k$ – нечіткі відображення з X_i в X_i, $i=1,2$, відповідно, що визначають переходи станів підсистем, $k=0,1,2,...$, а $F^{(1)}_k, F^{(2)}_k$, $k=0,1,2,...$, - визначають взаємний вплив підсистем.

Нехай нечіткі відображення $R^{(1)}_k, R^{(2)}_k$, $k=0,1,2,...$, задаються однорідними операторами, а дію операторів $F^{(1)}_k(\cdot), F^{(2)}_k(\cdot)$ можна записати у вигляді $F^{(1)}_k \mathrm{o} \tilde{X}^{(2)}_k = f^{(1)}_k(\tilde{X}^{(2)}_k)$, $F^{(2)}_k \mathrm{o} \tilde{X}^{(1)}_k = = f^{(2)}_k(\tilde{X}^{(1)}_k)$, $k=0,1,2,...$, відповідно, де $f^{(i)}_k(\cdot)$, $k=0,1,2,...$, $i=1,2$, - неперервні оператори.

Припустимо, що ізольовані підсистеми

$$\begin{aligned}\tilde{\tilde{X}}^{(1)}_{k+1} &= R^{(1)}_k \mathrm{o} \tilde{\tilde{X}}^{(1)}_k,\\ \tilde{\tilde{X}}^{(2)}_{k+1} &= R^{(2)}_k \mathrm{o} \tilde{\tilde{X}}^{(2)}_k,\end{aligned} \tag{47}$$

з початковими значеннями $\tilde{\tilde{X}}^{(1)}_0 = \{(x^1, \mu^{(1)}_0(x^1)) : x^1 \in X_1\}$, $\tilde{\tilde{X}}^{(2)}_0 = \{(x^2, \mu^{(2)}_0(x^2)) : x^2 \in X_2\}$ мають розв'язки, які мають вигляд $\tilde{\tilde{X}}^{(1)}_k = \{(x^1, \bar{\mu}^{(1)}_k(x^1)) : x^1 \in X_1\}$ та $\tilde{\tilde{X}}^{(2)}_k = \{(x^2, \bar{\mu}^{(2)}_k(x^2)) : x^2 \in X_2\}$,

Розглянемо динаміку системи (46) з початковими даними $\tilde{X}^{(1)}_0 = \tilde{\tilde{X}}^{(1)}_0$, $\tilde{X}^{(2)}_0 = \tilde{\tilde{X}}^{(2)}_0$.

Теорема 3.1. Припустимо, що у системі (46) оператори $R^{(1)}_k, R^{(2)}_k$, $k=0,1,2,...$, є стискаючими і для $\forall k=0,1,2,...$,

$$\rho(\tilde{\tilde{X}}^{(i)}_{k+1}, f^{(i)}_k(\tilde{X}^{(3-i)}_k)) \le g^{(i)}(\rho(\tilde{\tilde{X}}^{(i)}_k, \tilde{X}^{(i)}_k)), \tag{48}$$

де $g^{(i)}(w^{(i)}_k)$, $i=1,2$, $k=0,1,2,...$, – неперервні додатні функції на області визначення.

Позначимо через $r^{(i)}_k(w^{(i)}_0)$, $k=0,1,2,...$, $i=1,2$, – максимальні розв'язки скалярних різницевих рівнянь:

$$w^{(i)}_{k+1} = \lambda^{(i)}_k w^{(i)}_k + g^{(i)}(w^{(i)}_k), w^{(i)}_0 \ge 0, 0 < \lambda^{(i)}_k \le 1, k=0,1,2,...,i=1,2. \tag{49}$$

Тоді для кожного $i=1,2$, $k=0,1,2,...$, маємо

$$\begin{aligned}\rho(\tilde{\tilde{X}}^{(i)}_{k+1}, f^{(i)}_k(\tilde{X}^{(3-i)}_k)) &\le r^{(i)}_k(w^{(i)}_0),\\ \rho(\tilde{\tilde{X}}^{(i)}_1, f^{(i)}_0(\tilde{X}^{(3-i)}_0)) &\le w^{(i)}_0.\end{aligned} \tag{50}$$

Запропоновані у дослідженні методики та алгоритми використано при розв'язанні прикладних задач локальної фільтрації зображень. Опису застосування нечіткого підходу для цих задач присвячений **четвертий розділ**. Задача фільтрації зображень полягає у поліпшенні якості вихідного зображення. Розглянуто лінійні та нелінійні фільтри, різні схеми обробки граничних областей. Досліджено властивості вагових функцій і нормуючих коефіцієнтів процедури побудови відгуку фільтру. За умов, що збільшення розмірів апертури істотно збільшує об'єм обчислень, тоді як якість обробки поліпшується несуттєво, запропоновано модифікацію методики на основі алгоритмів лінійної фільтрації сукупності проекцій зображення у вигляді піраміди. Для покращення результатів фільтрації проекцій пропонується застосувати нечітке подання розмірів апертури за допомогою інтервального подання нечітких трикутних цілих чисел, наведеного у попередніх розділах. Отримане при цьому підвищення обчислювальної складності компенсується покращенням якості отриманих відгуків реальних зображень. Отримано чисельні результати, що підтверджують ефективність та конструктивність запропонованої методики.

ВИСНОВКИ

Дисертаційна робота присвячена розробці конструктивних методів формалізації подання нечітких чисел, розробленню методів структурування нечітких величин, розробці математичного та програмного забезпечення для дослідження процесів обробки нечіткої інформації, результати якого можуть бути застосовані при розв'язанні актуальних прикладних задач аналізу та синтезу в умовах невизначеності.

Основними результатами дисертаційної роботи є:

- розроблено нові способи формалізації нечітких цілих та раціональних чисел;
- запропоновано оригінальні послідовності простих чисел, досліджено їх властивості та наведено методику їх використання для опису функцій належності нечітких трикутних чисел;
- запропоновано новий метод опису невизначеності у вигляді складених нечітких чисел;
- запропоновано нове розширення синтаксису та семантики мови програмування для реалізації засобів нечіткого моделювання;
- вперше проведено дослідження та підвищення криптостійкості алгоритму шифрування даних з використанням послідовностей простих чисел;
- узагальнено спосіб представлення нечітких баз даних, який дав можливість описувати нечіткі дані у вигляді таблиць-представлень із врахуванням суб'єктивного характеру нечіткості;
- розроблено нові конструктивні алгоритми кластеризації нечітко визначених даних, що описуються сукупністю складених нечітких чисел;
- вперше досліджено та отримано умови адекватності динаміки нечітких багатомірних лінійних систем при їх структурному спрощенні;
- на основі застосування нечітких цілих чисел вперше розв'язано задачу нечіткої локальної фільтрації, що дозволило покращити якість відгуків при обробці реальних зображень.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях:

1. Вадньов Д.О. Про підхід до прийняття рішень на основі застосування невизначених множин / Д.О.Вадньов, Є.В. Івохін // Вісник Київського університету. Серія: Фіз.–мат. науки. – 2000. – Вип.3. – С. 201–206.
2. Вадньов Д.О. Застосування методу максимізуючих множин для одного випадку задачі прийняття рішень / Д.О.Вадньов, Є.В. Івохін // Вісник Київського університету. Серія: Фіз.-мат. науки. – 2000. – Вип.4. – С.150–154.
3. Вадньов Д.О. Про деякі задачі спостереження в динаміці дискретних невизначених нечітких систем / Д.О.Вадньов, С.О.Волчков, Є.В. Івохін // Вісник Київського університету. Серія: Фіз.-мат. науки. – 2001. – Вип.3. – С. 131 – 136.
4. Вадньов Д.О. Використання задачі про рюкзак в якості алгоритму для шифрування даних / Д.О. Вадньов //Вісник КНУ імені Тараса Шевченка. Серія: Кібернетика. – 2014. – №14. – С.5-9.

5. Івохін Є.В. Дослідження стійкості лінійних різницевих систем великої розмірності / Є.В. Івохін, Д.О.Вадньов // Журнал обчислювальної та прикл. математики. – 2009. – № 2.– С.28–34.
6. Ивохин Е.В. О некоторых свойствах и оценках для последовательностей простых чисел / Е.В.Ивохин, Д.А.Ваднев// Проблемы управления и информатики. – 2015. – №6. – С.105-118.
7. Івохін Є.В. Про реалізацію кількісних запитів в нечітких базах даних / Є.В. Івохін, Д.О. Вадньов // Вісник Київського національного університету імені Тараса Шевченка. Серія: фіз.-мат. науки. – 2015.– Вип.3. – С. 76 – 79.

Матеріали та тези доповідей на наукових конференціях:

8. Івохін Є.В. Дослідження стійкості нечітких лінійних різницевих систем великої розмірності / Є.В.Івохін, Д.О.Вадньов // Матер. ІІІ міжнар. конф. [«Інтелектуальні системи прийняття рішень та прикладні аспекти інформаційних технологій» (ISDMIT)], (Євпаторія, вересень 2013р.). – Євпаторія, 2013. – С.446-447.
9. Івохін Є.В. Використання спеціальних множин простих чисел для шифрування методом рюкзака / Є.В.Івохін, Д.О.Вадньов // Матер. VI міжнар. наук. конф. [«Обчислювальна та прикладна математика»], (Київ, 5-6 вересня 2013р.). – Київ, 2013. – С.126.
10. Івохін Є.В. Про один спосіб подання нечітких дійсних чисел у формі триплету / Є.В.Івохін, Д.О.Вадньов // Матер. ІІ міжн. наук.-техн. конф. ["Обчислювальний інтелект" (ОІ-2013)], (Черкаси, 14-18 травня 2013р.). – Черкаси, 2013. – С.75-76.
11. Vadnyov D. About the properties and application of the special prime numbers sequences / D.Vadnyov, E.Ivohin // Abstr. XXVII Intern. Conf. ["Problems of Decision Making under Uncertainties" (PDMU-2016)], (Tbilisi-Batumi, May 23 – 27, 2016). – Київ, 2016. – С.165.

АНОТАЦІЯ

Вадньов Д.О. Методи формалізації подання нечітких величин на основі спеціальних послідовностей простих чисел. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата фізико-математичних наук із спеціальності 01.05.04 – системний аналіз і теорія оптимальних рішень. – Київський національний університет імені Тараса Шевченка МОН України, Київ, 2016.

Дисертаційна робота присвячена розробці конструктивної методики формалізації нечітких чисел, розробці математичного та програмного забезпечення для дослідження процесів обробки нечітких даних і його застосуванню для розв'язання прикладних задач в умовах невизначеності.

Наведено аксіоматику нечітких множин, основні поняття та визначення нечітких величин і чисел. Проведено огляд використання нечітких множин та математичні моделі нечітких систем.

Вивчено спеціальні послідовності простих чисел, їх властивості, введено операції на даних послідовностях. Розроблено алгоритм для наближення довільного раціонального числа на основі елементів введених послідовностей простих чисел. Викладено методику подання цілих та раціональних нечітких чисел. Формалізовано процес динаміки функцій належності станів нечіткої дискретної системи. За допомогою нечіткого підходу модифіковано базову схему алгоритму шифрування Меркла-Хелмана. Узагальнено поняття нечітких баз даних для обробки слабоформалізованої інформації. Сформульовано розширення синтаксису та семантики мови С.

Запропоновано поняття складених нечітких чисел трикутного вигляду, досліджено їх властивості. Розв’язано задачі кластеризації даних у формі складених нечітких чисел, розроблено декомпозиційний підхід для дослідження динаміки нечітких багатомірних систем, що функціонують в умовах невизначеності.

Запропоновані в роботі методики та алгоритми використано для розв’язанні прикладних задач локальної фільтрації зображень. Отримано числові результати, що підтверджують ефективність та конструктивність запропонованої методики.

Ключові слова: нечіткі множини, нечіткі трикутні числа, прості числа, кластеризація, нечіткі бази даних, декомпозиція нечітких багатовимірних систем, нечітка лінійна фільтрація.

АННОТАЦИЯ

Ваднев Д.А. Методы формализации представления нечетких величин на основе специальных последовательностей простых чисел. – Рукопись.

Диссертация на соискание ученой степени кандидата физико-математических наук по специальности 01.05.04 – системный анализ и теория оптимальных решений. – Киевский национальный университет имени Тараса Шевченко МОН Украины, Киев, 2016.

Диссертационная работа посвящена разработке конструктивной методики формализации нечетких чисел, созданию новых алгоритмов обработки нечетких данных, разработке математического и программного обеспечения для исследования процессов обработки нечеткой информации и его использованию для решения актуальных прикладных задач в условиях неопределенности.

В первом разделе проведен обзор результатов исследований на основе нечетких множеств и систем. Приведена аксиоматика нечетких множеств, основные понятия и определения нечетких величин и нечетких чисел. Проведен обзор использования нечетких множеств и математические модели нечетких систем. Отмечено, что перспективным направлением формализации нечеткости является использование треугольных нечетких величин путем построения интервалов возможных значе-ний неопределенного параметра с использованием линейной функции принадлежности.

Во втором разделе работы рассмотрены и детально изучены специальные последовательности простых чисел, их свойства, введены операции на заданных последовательностях. Предложен алгоритм для приближения произвольного рационального числа с помощью элементов введенных последовательностей простых чисел. Рассмотрено множество неотрицательных рациональных чисел, которые представляются в виде отношения двух элементов из предложенных последовательностей. Доказаны утверждения для оценок интервалов размещения ближайших к заданному целому простых чисел. Изложена методика представления нечетких целых и действительных чисел. Разработан способ формализации процесса динамики функций принадлежности состояний нечеткой дискретной системы. На основе нечеткого подхода предложена модификация базовой схемы алгоритма шифрования Меркла-Хеллмана, что позволило повысить криптоустойчивость алгоритма. Обобщено понятие нечетких баз данных для обработки слабо-формализованной информации. Предложено расширение синтаксиса и семантики

языка С для реализации программных средств нечеткого моделирования. Полученные результаты позволили обосновать методику задания треугольных нечетких чисел в виде интервалов, границы которых выбираются из элементов специальных последовательностей простых чисел.

В третьем разделе введено понятие составных нечетких чисел треугольного вида, обобщающих применение нечетких чисел. Исследованы их свойства, сформулировано понятие расстояния между произвольными составными нечеткими числами на основе построения множеств уровня специального вида, разработана схема для сравнения расстояний. Решена задача кластеризации при условии представления данных в форме составных нечетких чисел, предложен математически обоснованный декомпозиционный подход для исследования поведения нечетких многомерных систем, функционирующих в условиях неопределенности.

Рассмотрены модели, свойства решений и непрерывность решений нечетких разностных систем, состояния которых описываются с помощью составных нечетких чисел. Предложен подход, базирующийся на декомпозиции систем на подсистемы. Доказано утверждение об адекватности поведения решений исходной системы и полученных нечетких подсистем.

Предложенные в исследовании методики и алгоритмы использованы для решения прикладных задач локальной фильтрации изображений для улучшения качества их исходного состояния. Описание результатов приведено в четвертом разделе. Рассмотрены линейные и нелинейные фильтры, различные схемы обработки пограничных областей. Предложена модификация методики линейной фильтрации совокупности проекций изображения, представленных в виде пирамиды. Для улучшения результатов фильтрации проекций предложено использовать нечеткое представление размеров апертуры на основе интервального представления нечетких треугольных целых чисел. Получены результаты, подтверждающие эффективность и конструктивность предложенной методики.

Ключевые слова: нечеткие множества, нечеткие треугольные числа, простые числа, кластеризация, нечеткие базы данных, декомпозиция нечетких многомерных систем, нечеткая линейная фильтрация.

ANNOTATION

Vadnyov D.O. Formalization methods of fuzzy values representations based on specific sequences of prime numbers. – Manuscript.

Candidate’s thesis in Physics and Mathematics, speciality 01.05.04 – System Analysis and Optimal Decision Theory. – Taras Shevchenko National University of Kyiv, Ministry of Education and Science of Ukraine, 2016.

The thesis is devoted to constructive methods of fuzzy numbers formalization development, processing fuzzy data new algorithms development, research of software and approaches for solving current interest tasks for processing fuzzy information with uncertain conditions.

First chapter contains review of fuzzy sets and systems based research results. This chapter also contains axioms, basic concepts and definitions of fuzzy sets and numbers, uncertain fuzzy sets as generalization of fuzzy sets. A review of fuzzy sets and fuzzy models of systems usage is held.

Second chapter contains analysis of special sequences of prime numbers and their properties and definitions of operations on defined sequences. An algorithm to approximate an arbitrary rational number with usage of elements from given prime number sequence is proposed. Set of non-negative rational numbers represented as two elements from given sequences ratio is reviewed. Representation method for fuzzy integers and real numbers revealed. A method of formalization of the process of fuzzy discrete system states membership functions dynamics is developed. A fuzzy approach based modification of Merkle-Hellman's messages encryption algorithm is offered. Concept of fuzzy databases for processing weakly formalized information is generalized on the basis of fuzzy concepts formation and formalization of fuzzy select operations for quantitative terms. C language semantics and syntax extension to implement fuzzy modeling is proposed. The obtained results are allowed to prove the technique of using triangular fuzzy numbers as intervals, the boundaries of which are selected from the elements of specific prime numbers sequences.

Third chapter contains the concept of composite fuzzy numbers of triangular form, generalizing the use of fuzzy numbers. Their properties were investigated. Data clustering problem were solved for input data defined as composite fuzzy numbers. Mathematically founded decomposition approach to research behavior of fuzzy multidimensional systems operating under conditions of uncertainty was set out.

Models, solution properties and solution's continuity for fuzzy difference systems with states described by a composite fuzzy numbers were investigated. Approach based on decomposition of systems to subsystem was proposed. Statement of original system and obtained fuzzy subsystems behavior adequacy was proven. Proposed methods and algorithms used for solving image local filtration task to improve input image quality. Results can be found in the fourth chapter. Linear, non-linear filters and different border processing methods were reviewed. Weight functions properties and normalizing factors of filter feedback build method were researched. Proposed resolution pyramid linear filtering method modification to decrease computation time. To improve filtering results proposed to use aperture size as interval based triangular integer fuzzy numbers. Obtained results prove method's efficiency and constructivity.

Key words: fuzzy sets, fuzzy triangular numbers, prime numbers, data clustering, fuzzy databases, decomposition of fuzzy multidimensional systems, fuzzy linear filtering.