Відгук

офіційного опонента Гороховського Семена Самуїловича
про дисертаційну роботу Гуріна Артема Леонідовича
«Комбінаторні методи розв'язання задач про математичний сейф на графах та матрицях», представлену на здобуття наукового ступеня доктора філософії зі спеціальності 113 – «Прикладна математика»

Актуальність обраної теми.

В дисертаційній роботі досліджуються, розроблюються та обґрунтовуються математичні методи для розв'язання комбінаторних задач. Автор зосереджується на аналізі певних позиційних ігор, які можна представити у вигляді графів та матриць, а саме на дослідженні математичного об'єкту, що отримав назву математичний сейф. Математичний сейф розглядається на орієнтованих і неорієнтованих графах та на матрицях різної розмірності як із замками одного типу, так і з замками різного типу над полями лишків F_k за модулем простого числа K. Розробка та теоретичне обґрунтування комбінаторних методів розв'язання задач про математичний сейф на графах та матрицях є важливим напрямком сучасних досліджень у галузі комбінаторики.

Автором розроблені та обґрунтовані нові методи розв'язання задачі про математичний сейф та запропоновані механізми корегування початкових даних таким чином, щоб задача мала розв'язок. Автор також приділив увагу іншій актуальній проблемі – розробці універсальних ефективних алгоритмів для задач про математичний сейф з урахуванням зростання їхньої розмірності, оскільки існуючі на момент написання дисертації методи розв'язання багато в чому недовершені і не складаються у цілісну методологію, залежачи від конкретних типів графів, початкових умов, тощо.

Структура та основні наукові результати роботи.

Дисертаційна робота складається з анотації, вступу, чотирьох розділів, загальних висновків, списку використаних літературних джерел, який

містить більше 120 найменувань.

У *вступі* наведено огляд літератури, обґрунтована актуальність теми дисертації, вказано основні напрямки досліджень, сформульовано задачі дослідження, визначено методи, які використовуються для досягнення мети роботи.

У *першому розділі* дисертаційної роботи проведено аналіз етапів розвитку теорії позиційних ігор та теорії графів, включаючи розгляд задачі про математичний сейф. В цьому розділі подано короткий огляд поточного стану методів вирішення таких задач і наведено список публікацій вчених, які активно досліджують цю тему. Оглянуті як вітчизняні, так і зарубіжні дослідження, включаючи роботи відомих авторів, таких як Донець Г.П., Кривий С.Л. та інші, в яких представлені методи та алгоритми для розв'язання позиційних ігор.

У другому розділі дисертації розглядаються відомі методи розв'язання задач про математичний сейф на орієнтованих і неорієнтованих графах різної топології таких як «драбинка», «подвійна драбинка», «віяло», «шлях», «ланцюг» та інші. Також у розділі розглядаються методи розв'язання задач про математичний сейф на матрицях різної розмірності у полі лишків (метод Т-матриць, TSS-метод), та у кільці лишків (TSS-метод).

Проведено аналіз алгоритмів TSS-методу, які знаходять базис множин розв'язків систем лінійних однорідних і неоднорідних діофантових порівнянь над полями F_k і кільцями лишків Z_k за модулем простого і складеного числа (mod K).

У *третьому розділі* розроблений новий метод сумарних представлень для задачі про математичний сейф на графах. Описані виняткові випадки, запропоноване корегування початкового стану сейфу. Наведені приклади розв'язку для графів різних топологій над полями F_k.

У цьому розділі запропонований та описаний новий параметричний метод для задач про математичний сейф на графах, сутність якого полягає у

введення певної кількості параметрів, через які знаходяться всі інші змінні задачі про сейф. Наведені приклади розв'язку для графів різних топологій.

У *четвертому розділі* розроблено нові методи для розв'язання задачі про математичний сейф на матрицях: метод формування (виділення) підсистем та метод сумарних представлень. У методі формування (виділення) підсистем з висхідної системи рівнянь виділяють підсистеми двох типів, що дозволяє зменшити обчислювальну складність алгоритму. Завдяки подальшому аналізу, описано задачу з двома типами замків – задача повністю розв'язана методом формування підсистем, знайдено необхідні та достатні умови існування розв'язку, виведено явні формули розв'язку.

Проведено порівняння методів за арифметичною складністю алгоритмів для замків над полем лишків F_k за модулем простого числа.

Розглянуто приклади застосування алгоритмів задачі про математичний сейф на графах у теорії кодування та захисту інформації на базі системи шифрування Віжінера. Це є дуже цінним, оскільки опоненту відомо, що Ґеорґій Панасович Донець скаржився на «бідність» практичних застосувань.

Наукова новизна і ступінь обґрунтованості результатів роботи.

Результати, які отримані в роботі Гуріна А.Л., є суттєвими для розвитку методів розв'язання задач про математичний сейф на графах та матрицях. Гурін А.Л. досконало систематизував теоретичну постановку задачі про математичний сейф та довів основний закон математичних сейфів, головну увагу приділив питанням методології розв'язання задачі про сейф як на графах, так і матрицях у полі лишків за модулем простого числа. Розробив нові методи розв'язання задачі, такі як метод формування підсистем, метод сумарних представлень, параметричний метод. У роботі автор описав виняткові випадки задачі про математичний сейф, коли розв'язку немає, для таких випадків запропонував корегування початкового стану математичного сейфу при якому буде існувати розв'язок. Провів порівняння методів за арифметичною складністю алгоритмів для замків над полем лишків F_k. Навів

приклад практичного застосування задачі про математичний сейф в теорії захисту інформації.

Дослідження, проведені автором в даній дисертаційній роботі, спрямовані на постановку та розв'язання нових наукових задач в теорії комбінаторних позиційних ігор.

Теоретичні результати роботи можуть бути застосовані у подальших дослідженнях з комбінаторики та теорії позиційних ігор.

Усі результати, що представлені в дисертаційному досліджені є істотно новими, математично строго обґрунтованими.

Апробація та повнота викладу основних положень дисертації.

Наукові досягнення, отримані у дисертаційній роботі, були представлені в 10 наукових публікаціях. З них 5 статей опубліковані в наукових виданнях, які включені до бази даних SCOPUS. Всі наукові статті опубліковані у виданнях які входять до переліку фахових видань за спеціальністю 113 Прикладна математика.

Дисертація відповідає встановленим вимогам щодо кількості публікацій за темою дисертації у фахових виданнях, а також щодо об'єму та оформлення дисертаційних робіт.

Практичне та теоретичне значення одержаних результатів.

Отримані результати дослідження в дисертації мають як теоретичне, так і практичне значення. Вони дозволяють використовувати комбінаторні методи для вирішення різноманітних завдань для задач про математичний сейф на графах та матрицях. Ці методи можуть бути застосовані для створення моделей та пошуку рішень у практичних завданнях шифрування в теорії захисту інформації.

У роботі Гурін А.Л. майстерно систематизував теоретичну постановку задачі про математичний сейф, довів ряд тверджень, які дозволяють отримати розв'язання задачі в явному вигляді, навів вичерпні приклади застосування запропонованих методів, які дозволяють стверджувати поліноміальну часову складність розроблених методів, приділив значну увагу питанням

методології розв'язання задачі про сейф, як на графах так і на матрицях, проаналізував арифметичну складність алгоритмів та навів практичні приклади застосування задачі в теорії кодування.

Зауваження, що висуваються до роботи та побажання:

1. В анотації не дуже вдало згадуються вчені, які зробили внесок в розвиток теорії комбінаторних позиційних ігор, не вказаний професор Перепелиця Віталій Опанасович, вказано Павлов А.А., потрібно - Павлов О.А., не згадується доктор фіз.-мат. наук О. П. Ігнатенко.

2. В роботі відсутній перелік скорочень, що ускладнює її прочитання.

3. Дисертація містить неточності та друкарські помилки на сторінках 30, 34, 38, 41, 91, 111, 134, а також стилістичні огріхи на кшталт «розв'язок» замість «розв'язання», забуваючи, що розв'язання це процес, а розв'язок це результат (стор. 2, 3, 5, 16, 19, 26, 34, 42 та ще в багатьох місцях).

4. Бажано б було обґрунтувати, чому нові методи не були запропоновані для розв'язання задач про математичні сейфи над кільцями лишків Z_k за модулем складеного числа (mod K).

5. Бажано також розробити програмне забезпечення за запропонованими та існуючими методами та на його основі провести аналіз швидкодії алгоритмів.

6. Калька «двійна» замість «подвійна» (стор. 130).

7. Зазначимо перевантаженість підрозділу 4.4. Практичне застосування моделі задачі про математичний сейф на графах загальними відомостями.

Висновок.

Наведені зауваження не знижують загального враження від високого науково-технічного рівня наукового дослідження, не мають принципового характеру та не впливають на позитивну оцінку проведених досліджень.

Дисертація є самостійною завершеною науково-дослідницькою працею. Враховуючи актуальність обраної теми, ступінь обґрунтованості та достовірності наукових результатів дисертаційна робота відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України №44 від 12 січня 2022 року, а її автор заслуговує присудження ступеня доктора філософії за спеціальністю 113 «Прикладна математика».

Завідувач кафедри інформатики
Національного університету
"Києво-Могилянська академія"
кандидат фізико-математичних наук,
старший науковий працівник С.С. Гороховський

18.10.2023

Підпис С. С. Гороховського завіряю,