ВІДГУК

офіційного опонента – доктора фізико-математичних наук,
професора Кривого Сергія Лук'яновича
на дисертаційну роботу **Гуріна Артема Леонідовича**
на тему «**Комбінаторні методи розв'язання задач**
про математичний сейф на графах та матрицях»
представлену на здобуття наукового ступеня **доктора філософії**
з галузі знань **11 – «Математика та статистика»**
за спеціальністю **113 – «Прикладна математика»**

1. Актуальність обраної теми дисертації.

Дисертаційна робота Гуріна А.Л. присвячена методам розв'язання дискретних задач, пов'язаних моделлю математичного сейфа, які мають потенційне застосування у теорії ігор, теорії кодування, захисті інформації та інших наукових галузях. Ці методи можна класифікувати як позиційні ігри на графах та матрицях.

У роботі розглянуті сучасні методи розв'язання задач про математичний сейф: TSS-метод та метод Т-матриць, а також прпонуютьс нові методи: метод формування підсистем, параметричний метод, метод сумарних представлень, Проведено порівняння методів за арифметичною складністю алгоритмів для моделі математичного сейфа над полем лишків за модулем простого числа. Запропоновано застосування запропонованих методів до розв'язання задач криптології. Розглянуті умови існування розв'язків при певних обмеженнях виродженості та обмежень на початкові умови задачі. В дисертаційній роботі описано спосіб корекції вхідних даних, після якої задача про математичний сейф завжди буде мати розв'язок. Це підтверджує практичну цінність дисертаційного дослідження.

Отже, дисертаційна робота є актуальною та вирішує практичні питання в теорії комбінаторних позиційних ігор.

2. Ступінь обгрунтовнаості наукових положень, висновків дисертації.

Дисертаційна робота Гуріна А.Л. має цілісну концептуально повну будову, яка включає комплексне дослідження методів розв'язку задачі про математичний сейф на матрицях та графах. Крім того наведені приклади та розглянуті умови існування розв'язків для деяких випадків виродження та обмежень на початкові умови задачі, запропоновано практичне застосування у сфері шифрування повідомлень в інформаційних системах. Наукові положення дисертації, висновки та методичні рекомендації викладені у зрозумілій формі та відповідають цілям і завданням дослідження.

Оскільки здобувачем опрацьовано велику кількість вітчизняних та зарубіжних матеріалів, що відповідають темі дипломної роботи, усі відомості та висновки в роботі мають відповідне теоретичне, методологічне та емпіричне обґрунтування. Структура дисертаційної роботи логічна і послідовна, і її тема розкрита досупно і у повному обсязі.

3. Наукова новизна і теоретична та практична значущість результатів роботи.

Розв'язання задачі про математичний сейф в дисертаційній роботі розглядається над полями лишків за модулем простого числа.

Найбільш вагомими результатами дисертаційної роботи А.Л. Гуріна є такі:

- вперше сформульовано та доведено необхідні та достатні умови при яких початкові стани засувів сейфа гарантують існування розв'язку задачі про математичний сейф на графах;
- вперше остаточно описаний та обґрунтований метод сумарних представлень розв'язання задачі про математичний сейф на графах;
- вперше розроблений та представлений такий оригінальний метод розв'язання задачі про математичний сейф на графах, як параметричний метод;
- вперше розроблений та представлений метод формування підсистем розв'язання задачі про математичний сейф на матрицях, який дозволяє за скінчену кількість кроків отримати розв'язок задачі з одним та двома типами засувів;
- вперше запропоновано метод сумарних представлень для розв'язання задачі про математичний сейф на матрицях, який зводиться до розв'язання системи лінійних порівнянь;
- вперше системно проаналізовано арифметичну складність алгоритмів існуючих методів розв'язання задачі про математичний сейф на матрицях.

4. Повнота викладення наукових положень та висновків в опублікованих працях.

Основні положення та результати дисертаційного дослідження опубліковано у семи статтях: 5 статей опубліковано у виданнях України, англомовні версії яких включені до наукометричної бази SCOPUS, дві – у фахових виданнях України. Здобувач має три тези доповідей на наукових конференціях. Аналіз внеску автора в публікаціях показує, що він є вагомим.

5. Оцінка змісту дисертації.

Дисертаційна робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних літературних джерел, який містить 125 найменування. Загальний обсяг дисертаційних досліджень викладено на 161 сторінках друкованого тексту, де обсяг основного тексту – 137 сторінок. Дисертація включає 17 рисунків, 1 таблицю та 1 додаток на 4 сторінках.

У вступі належним чином обґрунтована актуальність вибраної теми дисертації. Надано загальний огляд роботи, яка містить важливість цього дослідження у контексті наукових програм, а також його практичне значення. Сформульовано мету та задачі дослідження, а також визначено методи, які використовуються для досягнення цих цілей. Виділено наукову новизну даної роботи.

Крім того, наведено кількісну оцінку публікацій та особистого внеску автора (здобувача) у цих публікаціях.

В першому розділі роботи розглянуто етапи розвитку теорії позиційних ігор та теорії графів, включаючи задачу про математичний сейф. Здійснено коротку оглядову характеристику сучасного стану методів розв'язання таких задач та наведено список публікацій відомих авторів, що їх досліджують. Аналізовані роботи як вітчизняних, так і закордонних вчених, в яких представлені відомі методи та алгоритми для розв'язання задач позиційних ігор. Оглянуті всі аспекти класифікації і методології розв'язання нової задачі про математичний сейф, що активно досліджується останніми двадцятьма роками. На підставі проведеного огляду зроблено висновки та визначено напрямки подальших досліджень.

Другий розділ присвячено розгляду існуючих та актуальних методів розв'язання задач про математичний сейф на графах та матрицях – TSS-методу, методу Т-матриць. Загальною ідеєю є формулювання задачі про математичний сейф за допомогою графів і подальше зведення її до систем лінійних рівнянь у класах лишків (*residues*) за скінченним модулем (*mod K*).

Далі у дисертації пропонуються методи та алгоритми ефективнішого розв'язання задач, враховуючи топологію графу, що описує математичний сейф. Цей підхід продемонстровано на топологічно складних типах графів, таких як графи типу "віяло".

Досліджено клас задач, де математичні сейфи описуються за допомогою матриць. Слід зазначити, що матричний і графовий сейфи відрізняються між собою матрицями систем лінійних порівнянь, до яких вони зводяться.

У висновках підкреслено обмеження існуючих методів і підкреслено необхідність подальшого розвитку більш досконалих комбінаторних методів і алгоритмів для розв'язання задач про математичний сейф в цілому.

У **третьому розділі** дисертації розглядається подальший розвиток методології розв'язання задач про математичний сейф на графах. Виявлено, що наявні методи, навіть для графів складної структури, мають обмежену доступність розв'язку та частковий характер. Тому стає очевидною необхідність розвитку більш ефективних та універсальних методів. Цей розвиток призвів до появи методу сумарних представлень. Основна ідея цього методу полягає в тому, що певний тип графів допускає обмежену кількість елементів рівняння, які дорівнюють сумі всіх змінних цього рівняння. Деякі графи дозволяють виразити змінні системи через цей параметр. Після того, як ці параметри знайдені, можна отримати рівняння щодо цього параметра і, відповідно, значення всіх змінних.

Досліджено виняткові випадки, коли рівняння мають кратні корені. У такому випадку, необхідно коригувати початковий стан сейфа, щоб усі коефіцієнти були кратними. Потім задача може бути розв'язана за допомогою загальних правил методу.

У четвертому розділі дисертації представлені нові та оригінальні методи для розв'язання задач про математичний сейф на матрицях

Спершу описується метод формування (виділення) підсистем, який полягає у виділенні підсистем з висхідної системи рівнянь. Метод детально описаний, наведені необхідні та достатні умови розв'язку, а також алгоритм його виконання, за цим методом розглядається задача з двома типами замків. Проаналізовано випадки виродження та обмежень, і показано, що висока ефективність цього методу не погіршується через ці випадки завдяки способу коригування вхідних даних. Знайдено необхідні та достатні умови існування розв'язку та виведено явні формули розв'язку.

Далі у розділі, описується метод сумарних представлень на матрицях, який використовує представлення суми всіх змінних через обмежену кількість змінних системи рівнянь. Цей метод дозволяє більш ефективно розв'язувати задачі, оскільки спрощує зв'язки між змінними і сприяє більш ефективному розв'язку задачі.

В розділі, проаналізовано арифметичну складність алгоритмів існуючих методів розв'язання задачі про математичний сейф на матрицях у полях лишків за модулем простого числа. Розглянуто приклади застосування алгоритмів задачі про математичний сейф на графах у теорії кодування на базі системи шифрування Віжінера.

Всі результати дисертації обґрунтовані.

6. Недоліки дисертації щодо її змісту і оформлення.

Зазначаючи високий рівень роботи дисертаційного дослідження, слід зазначити, що Гуріну А.Л. не вдалося уникнути деяких помилок і неточностей:

– не наведено способів узагальнення запропонованих методів розв'язання задач про математичний сейф над кільцями лишків за скінченним модулем, як перспективного напрямку подальшого розвитку;

– оцінки часової складності алгоритмів можна дати не тільки в арифметичній, а і в бітовій моделі складності (яка дає точнішу оцінку складності), а вони в роботі відсутні;

– в роботі присутня велика кількість стилістичних помилок та недосконалі приклади використання термінів українською мовою: на сторінці 38 приведено позначення поля F_k^p , яке далі позначається як поле F_p^k, на сторінці 67 не закінчена фраза про існування розв'язку порівняння, початок якої (якщо $a=0$...., то має розв'язок) є хибним, на сторінці 75 замість «кінцеві поля» потрібно вжити термін «скінченні поля», на сторінці 129 замість фрази «рішення системи», варто було би вжити «розв'язок системи» та багато інших фраз.

Наведені зауваження **суттєво не впливають** на загальну позитивну оцінку дисертаційної роботи здобувача.

7. Висновок про відповідність дисертації вимогам.

Дисертація Гуріна Артема Леонідовича є цілісною завершеною науковою працею, яка містить нові науково обґрунтовані результати, тема дисертації є актуальною. Автор продемонстрував відповідну кваліфікацію та володіння методами розв'язання задач про математичний сейф на графах та матрицях. Стиль викладу матеріалу послідовний, чіткий і зрозумілий.

На основі проведеного аналізу вважаю, що дисертаційна робота Гуріна Артем Леонідовича «Комбінаторні методи розв'язання задач про математичний сейф на графах та матрицях», яку подано на здобуття доктора філософії з прикладної математики, за обсягом наукових досліджень, їх актуальністю, теоретичного та практичного значення, новизною та науковим рівнем 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 Гурін Артем Леонідович **заслуговує присудження** ступеня доктора філософії за спеціальністю 113 «Прикладна математика».

.

Офіційний опонент
професор кафедри інтелектуальних
програмних систем
Київського національного університету
імені Тараса Шевченка
доктор фізико-математичних наук,
професор С.Л. Кривий

Підпис С.Л. Кривого завіряю,
Проректор з науково-педагогічної роботи
Київського національного університету
імені Тараса Шевченка