

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

доктора фізико-математичних наук, доцента Тилищака Олександра
Андрійовича на дисертаційну роботу Дула Віктора Вікторовича на тему
«Моделі та методи керування конфліктами бінарних векторів у
великорозмірних дискретних системах», представлену на здобуття ступеня
доктора філософії в галузі знань

12 «Інформаційні технології» за спеціальністю

122 «Комп'ютерні науки»

Актуальність теми дисертації.

Сучасний етап розвитку інформаційних технологій характеризується стрімким масштабуванням дискретних структур, ускладненням архітектурних зв'язків між їхніми елементами та підвищенням вимог до обчислювальної стійкості, надійності й кібербезпеки. У реальних дискретних середовищах практично будь-який процес вибору, проектування, планування чи оптимального розподілу обмежених ресурсів супроводжується виникненням відношень несумісності або логічного взаємовиключення. Особливо гостро ця проблема постає у великорозмірних дискретних системах – хмарних обчислювальних платформах, кіберфізичних інфраструктурах, цифрових мережах та високодеталізованих мікроелектронних топологіях, де конфліктні взаємодії набувають системного характеру та безпосередньо впливають на безпеку й живучість об'єктів. Найбільш природним та універсальним математичним інструментом для формалізації станів, ознак, умов та керуючих впливів у таких системах є бінарний вектор. Проте зі збільшенням розмірності системи простір можливих комбінацій зростає за експоненційним законом, що призводить до комбінаторного вибуху та відносить більшість задач пошуку допустимих безконфліктних конфігурацій до класу NP-важких. За таких умов традиційні евристичні схеми локального аналізу виявляються неспроможними забезпечити обчислювальну реалізованість, що висуває на перший план необхідність розробки строгих математичних моделей, компактних матрично-

графових представлень та масштабованих алгоритмів аналізу й усунення конфліктів у режимі реального часу. Міждисциплінарний характер дослідження Дула В.В. виявляється у побудові узгодженої концептуальної парадигми «моделі – інтерпретація – алгоритми», яка поєднує математичну строгість дискретної оптимізації з прикладними вимогами мікроелектроніки, багат шарової поліграфії, транспортної логістики та сучасної криптографії. Особливого теоретичного значення набуває той факт, що автор розглядає структурну конфліктність не як деструктивне обмеження, а як корисний структурний ресурс для побудови самопристосовних інтелектуальних систем підтримки прийняття рішень у великорозмірних середовищах. Усе це безпосередньо вказує на високий рівень актуальності обраного здобувачем наряду досліджень та його суттєве значення для розвитку комп'ютерних наук.

Наукова та структурна характеристика результатів дослідження.

Дисертаційне дослідження Дула В.В. має чітку логічну архітектуру та збалансовану структуру, яка повністю відповідає встановленим вимогам МОН України щодо робіт на здобуття ступеня доктора філософії. Загальний обсяг дисертації становить 147 сторінок, з яких 130 сторінок складає основна текстова частина. Робота містить 20 рисунків, 17 таблиць та список використаних джерел із 105 найменувань.

У першому розділі дисертаційної роботи розглянуто теоретичні засади та сучасний стан досліджень у галузі керування конфліктами бінарних векторів у дискретних системах великої розмірності. Автор обґрунтовує доцільність представлення станів та логічних залежностей у булевому просторі у вигляді систем лінійних нерівностей та графів суміжності. Встановлено, що конфлікт між векторами відображає неможливість їх одночасного включення до допустимої конфігурації без порушення логічних або структурних обмежень.

Другий розділ присвячений розробці методологічних засад і математичних моделей керування конфліктами бінарних векторів. Автор пропонує модель бінарної конфліктності на основі множин виконавців $P = \{p_1, \dots, p_M\}$ та множину подій $E = \{e_1, \dots, e_N\}$, де завдання пошуку максимальної сумісної підсистеми формалізується у вигляді бінарної матриці конфліктів $C = (c_{ij})$. Для незважених моделей обґрунтовано ефективність використання алгоритму Гопкрофта-Карпа зі складністю $O(|F|\sqrt{|P| + |E|})$. У разі зваженої моделі здійснено математично коректне зведення до задачі про максимальний потік у транспортній мережі з використанням алгоритму Дініца. Особливий науковий інтерес викликає запропонована модель безконфліктного стану дискретної системи у просторі з перешкодами. Перешкоди відіграють конструктивну роль: вони забезпечують просторову ізоляцію ресурсів та сегментують лінії конфліктів, що дозволяє суттєво підвищити загальну ємність системи порівняно зі стандартними геометричними обмеженнями. Математично задача зводиться до пошуку максимального паросполучення у двочастковому графі сегментів. Також у розділі розроблено метод оцінки нижньої межі кількості безконфліктних груп на основі властивості дегенеративності графа конфліктів.

Третій розділ дисертації присвячений дослідженню конфліктів бінарних векторів у криптографічних системах, зокрема в схемах автентифікованого шифрування з приєднаними даними (AEAD) на прикладі стандарту AES-GCM. Автор формує детальну онтологію криптографічних конфліктів (колізійні, алгебраїчні, протокольні та конфлікти повторного використання параметрів). На основі аналізу поліноміальної функції GHASH над полем $GF(2^{128})$ математично доведено, що порушення унікальності одноразового параметра (нонса) призводить до утворення лінійних систем рівнянь, розв'язання яких за допомогою алгоритму Кантора-Зассенгауза дозволяє повністю відновити таємний ключ автентифікації. Для запобігання таким загрозам запропоновано детерміновані механізми контролю стану на основі

монотонних лічильників та сесійної деривації ключів. Також у розділі розроблено методи структурно-орієнтованої оптимізації арифметичних перетворень у полях Галуа на основі раціонального вибору незвідних поліномів та інтеграції рекурсивного алгоритму Карацуби, який дозволяє знизити обчислювальну складність carry-less множення до $O(m^{1.58})$.

Четвертий розділ містить алгоритмічні рішення та результати експериментальної верифікації розроблених методів оптимального групування попарно диз'юнктних бінарних векторів. Автор пропонує модифікований метод динамічного програмування з використанням побітових операцій, бітових масок і низькорівневих оптимізацій (зокрема асемблерної інструкції процесора CTZ / `__builtin_ctz`), що дозволило розв'язувати задачі для розмірностей до 25×25 на рівні машинного слова. Для більших розмірностей (до 150×150) розроблено модель цілочисельного лінійного програмування, яка була успішно масштабована до розмірності 300×300 за допомогою високоефективних хмарних солверів NEOS-серверу (FICO-Xpress, CPLEX). Для систем екстремальної розмірності ($10^4 \times 10^5$) запропоновано авторський паралельний метод групування, який працює безпосередньо з матричним представленням даних у вигляді множин і уникає ресурсомісткої побудови графа суміжності. Використання технології багатопотокових обчислень OpenMP забезпечило прискорення розрахунків до 7 разів. Практичну цінність розробленого інструментарію підтверджено успішним впровадженням у транспортній логістиці для оптимізації розподілу замовлень між водіями на базі ПП «Західтранссервіс-Ужгород».

Наукова новизна отриманих результатів.

Наукова новизна результатів дисертації Дула В.В. має чітке теоретичне та практичне спрямування, є науково обґрунтованою та структурованою за рівнями внеску в комп'ютерні науки:

Уперше запропоновано:

- інтегрований концептуальний підхід до моделювання конфліктів бінарних векторів у великорозмірних дискретних системах на основі

єдності математичних моделей, прикладних інтерпретацій та обчислювальних алгоритмів. Сформовано нову математичну модель безконфліктного стану дискретної системи в просторі з перешкодами, яка завдяки декомпозиції сіткових структур на незалежні горизонтальні та вертикальні сегменти дає змогу звести просторове планування до пошуку максимального паросполучення у двочастковому графі сегментів ;

- метод пошуку максимальної кліки для розріджених графів конфліктів із обмеженою локальною щільністю ребер. На відміну від класичних алгоритмів, що мають експоненційну складність, запропоновано оригінальний підхід із лінійною обчислювальною складністю $O(n)$, який використовує властивість дегенеративності графа й ітеративне вилучення вершин малої степені. Це забезпечує можливість визначення точної нижньої межі кількості безконфліктних груп для систем надвеликої розмірності у режимі реального часу ;
- математичну модель оптимального групування попарно диз'юнктних бінарних векторів у вигляді задачі цілочисельного лінійного програмування. Модель гарантує мінімізацію кількості безконфліктних груп за умов повної попарної диз'юнктності елементів усередині кожної виділеної групи ;
- модифікований метод динамічного програмування для задач виділення найбільших сумісних підсистем і оптимального групування бінарних векторів, у якому бітове подання даних, побітові операції процесора та бітові маски інтегровано безпосередньо в рекурентну схему обчислень, що забезпечило кардинальне зниження часових і пам'ятних витрат для задач помірної розмірності ;
- паралельний метод групування попарно диз'юнктних бінарних векторів на багатоядерних архітектурах. Метод працює безпосередньо з матричним поданням даних у вигляді множин і використовує потокове розпаралелення на базі технології OpenMP, що дає змогу повністю

уникнути ресурсомісткої процедури побудови графа суміжності для систем екстремальної розмірності.

Удосконалено:

- методи аналізу та запобігання конфліктам у криптографічних схемах автентифікованого шифрування з приєднаними даними (на прикладі режиму AES-GCM) шляхом формалізації умов унікальності бінарних векторів (нонсів) ;
- методи структурно-орієнтованої оптимізації арифметичних перетворень у двійкових скінченних полях Галуа $GF(2^m)$ для криптографічних хеш-функцій на основі раціонального вибору незвідних поліномів та поєднання рекурсивного алгоритму Карацуби з апаратними інструкціями PCLMULQDQ.

Набули подальшого розвитку:

- концептуальні засади організації безконфліктних розбиттів та виділення найбільших сумісних підсистем у зважених моделях через їх редукцію до задачі знаходження максимального потоку та мінімального розрізу в орієнтованих мережах.

Ступінь обґрунтованості та достовірності наукових положень і висновків.

Дисертаційне дослідження Дула В.В. характеризується високим рівнем наукової обґрунтованості та достовірності висновків. Автор демонструє впевнене володіння апаратом дискретної математики, булевої алгебри, теорії графів, комбінаторної оптимізації та теорії алгоритмів. Формальні постановки задач і математичні моделі сформульовано коректно, з дотриманням математичної строгості. Достовірність розроблених методів підтверджується строгими математичними доведеннями, а також репрезентативним обсягом числових експериментів, проведених на реальних та випадково згенерованих великих масивах даних. Експериментальні дослідження виконувалися з використанням програмного забезпечення (солвер Gurobi) та академічних хмарних ресурсів NEOS Server. Отримані результати порівняльного аналізу

швидкодії різних алгоритмів узгоджуються з теоретичними оцінками обчислювальної складності.

Повнота оприлюднення результатів дослідження.

Результати дисертаційного дослідження опубліковані у 12 наукових працях, зокрема: 5 статей у фахових періодичних наукових виданнях України категорії «Б»; 7 праць у матеріалах міжнародних наукових конференцій, з яких 1 праця індексується в наукометричній базі Scopus.

Кількість, рівень і тематичне охоплення публікацій повністю відповідають вимогам до дисертацій на здобуття ступеня доктора філософії; основні наукові результати оприлюднено вичерпно.

Відомості про дотримання академічної доброчесності.

Ознайомлення з текстом дисертації та публікаціями Дула В.В. не виявило порушень академічної доброчесності. Запозичені ідеї, методи й результати супроводжуються коректними посиланнями; внесок здобувача у спільних публікаціях визначено явно і він є визначальним. Ознак плагіату, фабрикації або фальсифікації даних не встановлено.

Мова та стиль викладення результатів.

Текст дисертації написано якісною науковою українською мовою, термінологія та математична нотація використовуються коректно, а кожна формальна конструкція супроводжується змістовним поясненням. Таблиці та ілюстрації є інформативними та містять потрібні пояснення. Оформлення роботи відповідає вимогам наказу МОН України № 40 від 12.01.2017 р.

Практичне значення отриманих результатів.

Практичне значення отриманих результатів полягає у створенні комплексної концепції керування конфліктами для онлайн-аналітики та ресурсного планування. Теоретичні та прикладні результати дисертаційної роботи Дула В.В. безпосередньо впроваджено у виробничу діяльність транспортного підприємства ПП «Західтранссервіс-Ужгород» (що дозволило оптимізувати розподіл замовлень між водіями, скоротити простой та мінімізувати задіяні ресурси). Також результати досліджень інтегровано в

навчальний процес ДВНЗ «Ужгородський національний університет» та Закарпатського угорського університету імені Ференца Ракоці II, що підтверджено відповідними актами впровадження.

Недоліки та зауваження по роботі:

1. У підрозділі 2.1 (математична модель 2.1–2.3) розглядається задача виділення найбільшої сумісної підсистеми для незваженого випадку з критерієм максимізації сумарної кількості елементів $|P'| + |E'|$ при тім обмеженні на не порожність множин P', E' не накладено. Варто зауважити, що за умов високої щільності матриці конфліктів дана формалізація допускає ризик отримання тривіального (виродженого) розв'язку. Оскільки для порожньої множини подій ($E' = \emptyset$) умови відсутності конфліктів виконуються тривіально для будь-якого виконавця, математичний оптимум може звестися до вибору $P' = P$ та $E' = \emptyset$ із значенням цільової функції $|P'| + |E'| = |P|$. У практичних системах прийняття рішень такий розв'язок позбавлений прикладного змісту, адже система не призначає жодної події. Для усунення цієї математичної аномалії доцільно було б доповнити модель обмеженнями на мінімально допустимий обсяг кожної з підмножин ($|P'| \geq P_{min}$, ($|E'| \geq E_{min}$) або максимізувати не сумарну кількість елементів $|P'| + |E'|$ а добуток кількостей $|P'| \cdot |E'|$ що автоматично охопить непридатність вироджених розв'язків і виглядає природнішим для практики.

2. У підрозділі 3.2 детально проаналізовано загрози колізій нонсу в схемах автентифікованого шифрування (AES-GCM) та запропоновано детерміновану структуру нонсу на основі префіксів та монотонних лічильників. Змістовно оцінюючи вагомість алгебраїчного аналізу в $GF(2^{128})$, варто зауважити, що в умовах високонавантажених розподілених мікросервісних систем синхронізація лічильників між вузлами без створення централізованого «вузького місця» (bottleneck) є складною інженерною задачею. У роботі недостатньо розкрито практичні рекомендації щодо забезпечення незмінності стану лічильників при асинхронній горизонтальній масштабованості серверних вузлів.

3. У четвертому розділі для запропонованого паралельного методу наведено порівняння лише за часом виконання. Оскільки послідовно-жадібне групування не гарантує оптимальності, бажано кількісно показати, наскільки кількість груп, отримана цим методом, відхиляється від оптимуму (відомого з ЦПП-моделі) або від нижньої межі (клікового числа).

4. На ст. 34 у фразі «Ребро існує, якщо відповідні вектори X_a та X_b є несумісними, тобто $X_a \cap X_b \neq \emptyset$ » остання формула не має змісту. Читається, очевидно, правильно, якщо у формулі $X_a \cap X_b \neq \emptyset$, замість бінарних векторів X_a та X_b взяти множини індексів одиниць у відповідних векторах, або замість перетину символ логічного множення (побітове "і"), тоді замість порожньої множини — нульовий вектор.

5. У тексті дисертації та додатках трапляються інші поодинокі редакційні й технічні помилки, які не мають відчутного впливу на сприймання матеріалу дисертації, про які автору було повідомлено в особистому листуванні.

Висловлені зауваження та рекомендації мають здебільшого уточнюючий та дискусійний характер, вони не впливають на загальну високу оцінку дисертаційної роботи, не ставлять під сумнів її наукову новизну, обґрунтованість і практичну цінність.

Загальні висновки по дисертації.

Дисертаційна робота Дула Віктора Вікторовича «Моделі та методи керування конфліктами бінарних векторів у великорозмірних дискретних системах» є завершеним самостійним науковим дослідженням, виконаним на високому науковому рівні. Робота виконана на належному науковому рівні, її результати є новими, достовірними та практично значущими.

Робота не порушує принципів академічної доброчесності та 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 12.01.2022 р. (зі змінами), та

наказу Міністерства освіти і науки України від 12.01.2017 № 40 «Про затвердження Вимог до оформлення дисертації» (зі змінами).

Автор дисертаційної роботи Дуло Віктор Вікторович заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 – «Комп'ютерні науки» у галузі знань 12 – «Інформаційні технології».

Офіційний опонент –

професор кафедри математики та інформатики

Закарпатського угорського університету

імені Ференца Ракоці II

доктор фіз.-мат. наук, доцент



Олександр ТИЛИЩАК

Підпис Тилищака О.А. засвідчую

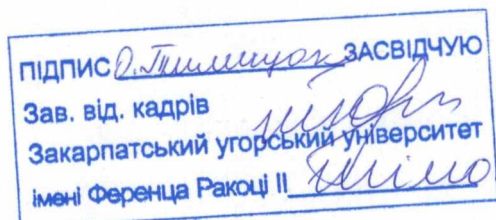
Вчений секретар

Закарпатського угорського університету

імені Ференца Ракоці II



Михайло ФІЛЕП



Юрчишин Т.В.