

РЕЦЕНЗИЯ

на дисертационния труд за придобиване
на образователна и научна степен „Доктор“

Тема: „Дискретни трансформации и приложението им в теория на кодирането и комбинаториката“

Автор: Паскал Николаев Пиперков,

Секция „Математически основи на информатиката“ (МОИ), Институт по
Математика и информатика, Българска академия на науките

Научен ръководител: проф. д.м.н Илия Георгиев Буюклиев

Научна област: 4. Природни науки, математика и информатика

Професионално направление: 4.5. Математика

Научна област: Алгебра и теория на числата

Рецензент: проф. дмн Николай Иванов Янков – ШУ „Епископ К. Преславски“

Със заповед № 159/27.06.2022 г. на Директора на Института по математика и информатика (ИМИ) при БАН съм назначен за член на Научното жури по процедурата и на първото заседание на това жури съм избран за изготвянето на настоящата рецензия. Предоставени са ми всички материали в съответствие с изискванията на нормативните документи, които са редовни и съответстват на ЗРАСРБ. Нямам информация за нарушения по процедурата, не ми е известно в дисертацията да има плагиатство.

1. Данни за дисертанта

Дисертантът Паскал Пиперков завършва през 1997 г. специалността „математика“ в СУ „Св. Климент Охридски“. От декември 2017 г. е зачислен като задочен докторант по Математика с научна област „Алгебра и теория на числата“ към секция МОИ. В приложената автобиография, както и другите материали към настоящата процедура, за съжаление, не открих данни за участията на дисертанта в научни проекти, което считам за важно понеже законодателят е предвидил че степента доктор е „образователна и научна“.

2. Данни за докторантурата

Докторантът е зачислен в редовна форма на обучение от 01.01.2018 г. с период на обучение 3 г., а по-късно със заповед №226 от 12.02.2018 г. докторантурата е трансформирана в задочна. С решение на НС на ИМИ (Протокол № 5/07.01.2022 г.) докторантът е отчислен с право на защита. Предварителното обсъждане на дисертацията се състоя на 10.06.2022 г. на разширено заседание на секция МОИ, на което присъствах.

Със заповед на директора на ИМИ е определено научно жури и датата на защитата. Считаю, че процедурата е редовна и няма нарушения.

3. Данни за дисертацията и автореферата

Представения за рецензия дисертационен труд се състои от: увод (5 стр.), основен текст (76 стр.) в 4 глави, разделени на секции. В дисертацията е включен списък с приносите, литература от 71 заглавия, списъци с публикациите и изнесените докладите по дисертацията. Трудът отговаря на изискванията на Закона за развитие на академичния състав в РБ (ЗРАСБ) и правилника за приложение на ЗРАСРБ (ППЗРАСРБ), както и на Правилника за условията и реда за придобиване на научни степени и за заемане на академични длъжности в БАН (ПБАН). Авторефератът в обем от 31 стр. отразява адекватно основните идеи и съществените крайни резултати, които са описани в дисертационния труд.

4. Актуалност на разработвания проблем

Като е известно от работата на Берлекамп, МакЕлис и ван Тилборг от 1978 проблемът за намирането на тегловното разпределение на линеен код е NP-пълнен. Що се отнася до радиуса на покритие: през 1984 Айлийн Маклафлин доказва, че намирането на радиус на покритие на линеен код е NP-труден проблем. Затова работата по опростяването на алгоритмите, а още повече за тяхното ускоряване е актуална. Следователно актуалността и научните приноси на дисертацията за развитието на тематиката са безспорни. Важността на разработките на дисертанта се потвърждават и от реализираните три цитирания на статията в журнала *Cryptography and Communications*, включена в дисертацията.

5. Степен на познаване на състоянието на проблема

Дисертантът познава много добре състоянието на проблема. Списъкът от 71 литературни източника хронологично започва с работи на Силвестър от 1867 и Адамар от 1893, като 20 от публикациите са от 2000 г. досега. Образователната част в ОНС „доктор” изисква дисертанта да покаже, че е навлязъл в съответната научна област. В тази връзка, считам Паскал Пиперков е навлязъл успешно в алгебричната теория на кодирането - съвременна област на математиката, а дисертацията дава ясна представа за историята и съвременното състояние на разглежданите проблеми и на методите за тяхното изследване.

6. Научни и научно-приложни приноси в дисертацията

В глава 2 е разработен нов алгоритъм за пресмятането на тегловно разпределение на код над просто поле. Това е постигнато чрез използването на характеристичен вектор и характеристично разпределение, както и съкратено характеристично разпределение, което се явява обобщение на спектъра на Уолш. Освен новите теоретични разработки, в дисертацията е изчислена сложността на предложения нов алгоритъм и са представени

експериментални резултати. От данните в дисертацията може да се направи извод, че при по-големи дължини $n > 300$ е постигнато ускорение от $x5$ до $x500$ в сравнение със старите известни алгоритми. Ако се направи съпоставка на предложения нов алгоритъм със съответния алгоритъм в системата за компютърна алгебра „MAGMA“ ускорението, което е постигнато е между 2 и 20 пъти, което считам за отлично постижение, т.к. в системата MAGMA винаги са имплементирани най-бързите и най-нови алгоритми известни към момента.

В глава 3 е представен нов метод за пресмятане на тегловно разпределение на линеен код над крайно съставно поле, като за целта се използват трансформация на следите и самодуален базис и така се получава трансформация на Уолш-Адамар при характеристика 2 или трансформация на Виленкин-Крестенсон при $p > 2$. Това води до намаляване на сложността на предложения бърфлай алгоритъм. Отново тук има подобрене, когато дължината на кода е голяма или имаме по-голямо поле, т.е. при по-трудните случаи.

В глава 4 са разработени методи за определянето на радиус на покритие над крайно поле, като тук са разгледани и двата различни случая: когато имаме просто и съответно съставно поле. При просто поле се използва връзката между преобразованието на Виленкин-Крестенсон и радиусът на покритие, като за целта се използва проверочна матрица на кода. Предложният метод може да се използва и за намиране на тегловно разпределение на лидерите на съседните класове на линеен код над просто поле с нечетна характеристика. За съставно поле, този метод е преформулиран чрез използването на трансформацията на следите, което позволява да се използва съкратеното характеристично разпределение за намирането на радиус на покритие, при което имат роля и алгоритмите от предходните две глави. Методите в тази глава се явяват доказани обобщения на метода на Карповски, който е използван само за двоични кодове, а в дисертацията имаме обобщение до по-сложните случаи.

Рецензираният дисертационен труд има добре завършен вид, като основните твърдения и факти, които са използвани са надлежно доказани теоретично. Получените алгоритми са описани с псевдокод, илюстрирани с диаграми, в значителна част са доказани теоретично, а освен това са реализирани на практика и показват подобрения в сравнение с преди известните приложения.

Признавам посочените в дисертацията научни и научно-приложни приноси.

7. Публикации и участия в научни форуми

В списъка с публикации по дисертацията има 4 статии, всички с по един или повече съавтори, като всички статии са в издания, които са рецензирани. От изданията едно: Cryptography and Communications Discrete Structures, Boolean Functions and Sequences има импакт-фактор (JCR-2021, IF=1.376) и се намира във втори квартал за

направление приложна математика. От другите публикации две са в тематични сборници: “Recent Topics in Differential Geometry and its Related Fields” и “New Horizons in Differential Geometry and its Related Fields” на издателство World Scientific Publishing Company, Сингапур. Последната четвърта публикация е от сборника на международната конференция OCRT 2017 г.

Считам, че участието на дисертанта във всички публикации е равностойно на останалите съавтори. Броят на статиите покрива изискванията на Закона за развитие на академичния състав в Република България, правилника за неговото приложение, както и правилниците на БАН и ИМИ.

В текста на дисертацията е приложен списък от 13 доклада (от които 6 самостоятелни), в който самия докторат е оповестил резултати от настоящата дисертация на различни национални и международни форуми. Според мен, тази апробация на резултатите от дисертационния труд надвишава минималните изисквания и показва готовността на Паскал Пиперков за самостоятелни научни изследвания и тяхното представяне на специализирани научни форуми.

8. Заключение

Дисертацията напълно отговаря на изискванията установени от ЗРАСБ, както и на правилниците на БАН и на ИМИ, затова с убеденост предлагам на уважаемото научно жури да гласува **ДА СЕ ПРИДОБИЕ** образователната и научна степен „доктор” от Паскал Николаев Пиперков в професионално направление 4.5. „Математика“ в научната област „Алгебра и теория на числата“.

Член на журито

/проф. дмн Николай Янков/

25.07.2022 г.

Шумен