РЕЦЕНЗИЯ

на представените трудове за участие в конкурс
за академичната длъжност ПРОФЕСОР,
обявен от Висшето строително училище „Любен Каравелов" – София
в ДВ. бр. 54 от 01.07.2014 г.

Област на висше образование: 4. Природни науки, математика и информатика
Професионално направление: 4.5. Математика
Научна специалност: „Алгебра и теория на числата"
Заповед на Ректора за назначаване на научно жури: № 827/03.09.2014

Рецензент: акад. Веселин Стоянов Дренски, д.м.н., професор в ИМИ – БАН
Кандидат: доц. д-р Николай Лазаров Манев от катедра „Механика и математика ", СФ, ВСУ „Любен Каравелов" – София.

1. Общи положения и биографични данни. Конкурсът е обявен в Държавен вестник бр. 54 от 01.07.2014 г. Единственият кандидат доц. д-р Николай Манев е роден през 1952 г. През 1977 г. се дипломира като магистър по математика, специалност „Алгебра" във ФМИ на Софийския университет „Св. Климент Охридски". През 1984 г. защитава кандидатска дисертация по „Алгебра и теория на числата" на тема „Граница на Грийсмър и оптимални кодове". От 1977 до 2012 г. професионална кариера на доц. Николай Манев е свързана с ИМИ – БАН. От 1977 до 1979 г. е математик, от 1979 до 1990 г. е научен сътрудник, а от 1990 до 2012 г. е ст.н.с. II ст. (доцент). Бил е научен секретар и заместник-директор на ИМИ, ръководител на секция „Математически основи на математиката". През отделни периоди е бил на втори трудов договор в Координационния център по информатика и изчислителна техника – БАН, във ФМИ на Великотърновския университет „Св. Св. Кирил и Методи" (включително заместник-декан по учебните въпроси), а от 2012 г. е доцент в катедра „Механика и математика" към СФ на ВСУ "Любен Каравелов" – София.

2. Общо описание на представените материали. Кандидатът е представил за участие в конкурса 32 научни труда (12 в списания, 7 от които с импакт-фактор, 5 в поредици и глави от книги, 2 от които с SJR, 15 в трудове на конференции), всички излезли от печат, и 3 учебника и учебни пособия, от които едно е излязло от печат в издателство „Деметра", а другите две са на интернет-страниците на ФМИ на СУ и на ВСУ. И трите учебника и учебни пособия са достъпни онлайн и на страницата на ИМИ при БАН. Всички публикации са след хабилитацията на кандидата и са по темата на конкурса, поради което ги приемам за рецензиране. Всички научни трудове са на английски език с изключение на два на руски, но списанието се превежда на английски, и един на български. От тях 3 са самостоятелни, 15 са съвместни с един съавтор (6 с Ю. Борисов, по 2 с Е. Колев и Х. Костадинов, по един с Б. Костова, С. Топалова, С. Илиева, Т. Николов и Ф. А. Саллам), 10 са с двама съавтори (4 с Х. Костадинов и Х. Морита, 2 с Е. Атанасов и Д. Георгиев, по един с Ю. Борисов и С. Никова, М. Х. Ли и К- Д. Занг, С. Бумова и Х. Костадинов, С. Ивановска и А. Караиванова), 3 са с трима съавтори (Т. Гуров, С. Ивановска и А. Караиванова, Х. Костадинов, Х. Морита и Н. Иджима, Х. Костадинов, Х. Морита и А. Я. Хан Винк), и един е с четирима съавтори (Х.

Костадинов, Х. Морита, Н. Иджима и А. Я. Хан Винк). Разпределението на публикациите е както следва: в списания: 4 в „IEICE Trans. Fundamentals“, по 2 – в „Проблемы передачи информации“ и „Applied Mathematics and Computation“, по 1 – в „Доклади на БАН”, „Discrete Applied Mathematics“, „Serdica Math. J.“ и „Serdica J. Comp.“; в поредици и глави от книги: 3 в Springer, включително 1 в LNCS, по 1 в IOS Press и в American Institute of Physics Conference Proceedings; в трудове на конференции: 10 в трудове на специализирани международни конференции по теория на информацията и кодиране (5 в България, 3 в Русия, по 1 в Хърватия и Нова Зеландия), 4 в Трудовете на Пролетната конференция на СМБ, включително с доклад по покана, 1 в трудовете на Великотърновския университет. Смятам, че големият брой съвместни публикации е положително качество. То повишава „коефициента на полезно действие” на научните изследвания и говори за способността на кандидата да работи в колектив. Част от съвместните публикации са с ученици на кандидата, като някои от работите са написани след защитата на дипломната работа или дисертацията, което показва, че той продължава да работи с бившите си ученици. Приемам, че съвместните научни трудове, представени за участие в конкурса, са написани при равноправно участие на съавторите (дори когато имената на авторите не са наредени по азбучен ред, както е в случая на статиите в списания с номера 5, 7, 11, 12 и в трудове на конференции с номера 8, 10, 12). Учебниците и учебните пособия са самостоятелни и на български език.

3. Обща характеристика на научно-изследователската и научно-приложната дейност на кандидата. Основните научни и научно-приложни интереси на доц. Манев са в прилагането на математически (предимно алгебрични и комбинаторни) методи в теория на информацията (теорията на кодирането, коригиращо грешки, и в криптографията и близките до нея области стеганография и дигитални водни знаци, имащи за цел защитата на съобщенията и информацията от атаки и от други злонамерени действия), както и практически приложения. По-точно, той работи в област, която е гранична за няколко математически и информатични дисциплини – теория на кодирането, коригиращо грешки, комбинаторика, алгебра (линейна алгебра над крайни полета), теория на числата, криптография, стеганография и информатика (съществена част от резултатите са получени с използването на компютър). Доц. Манев е автор на 9 научни труда, включени в кандидатската (днес докторска) дисертация и на 9 труда от конкурса за ст.н.с. II ст. (доцент). Повечето от останалите научни публикации са написани след хабилитацията. Това са 16 статии в списания, 5 в поредици и глави от книги, 33 в трудове на конференции, 7 резюмета в материали на конференции. Освен това, доц. Манев има 10 авторски свидетелства, регистрирани през периода 1985-1989 г. (6 в България и 4 в Русия) за разработване на устройства, свързани с практическа работа с крайни полета и с директни приложения на теория на кодирането. Традиционно, в България изследванията по теория на кодирането и криптографията се отнасят към научните специалности „Алгебра и теория на числата“ или „Информатика“. Тъй като в изследванията на кандидата преобладават теоретични методи, считам, че е естествено участието му в конкурс по „Алгебра и теория на числата“.

В последните десетилетия теория на кодирането е активно и успешно разработвана област на българската математика и информатика. Много често при предаването на информация полученото съобщение се различава от изпратеното поради наличието на смущения (или „шум”) по канала. Това явление се наблюдава в много различни области и се проявява по най-различни начини, например при обичайното предаване на

съобщения (по радиото или по телефона, с телеграми, SMSи или от една част на компютъра до друга). Възниква естествената и важна задача за разработване на ефективни методи за възстановяване на първоначалното съобщение. Един математически подход, който е в основата на теорията на кодирането, е фиксирането на множество от думи с дадена дължина (наречено „код") от азбука с краен брой символи и разглеждането на съобщението като редица от думи от кода. След това се въвежда подходящо „разстояние" между думите, което отчита броя и вида на грешките при предаването на думата. Задачата се свежда до намирането на тази дума от кода, която е „най-близко" до получената дума. При това се прави естественото ограничение, че „силата" на шума трябва да е относително „малка", за да не отдалечава твърде много полученото съобщение от изпратеното. С цел максимално въвличане на математически методи обикновено за азбука се използва крайно поле, а за отделни класове от кодове се предполага наличието на допълнителни алгебрични, геометрични или комбинаторни свойства (например се иска кодът да е линейно пространство). Изследванията на доц. Манев са свързани с редица основни задачи от теория на кодирането: намирането на минималната дължина на код с дадени мощност и коригиращи възможности и над фиксирано крайно поле, както и описанието на такива кодове с дадени параметри; анализирането, на базата на конкретни данни от практиката, на типичните грешки при използването на различни начини на комуникация и намирането на най-подходящите за съответните случаи кодове; решаването на математически и практически задачи, свързани с ефективното декодиране на съобщенията. Впоследствие в своите изследвания, сам или със съавтори, доц. Манев развива тематика, която се различава съществено от традиционната тематика у нас, с което внася свежа струя в областта на изследване на българския колектив. На практика при дигиталните комуникационни системи е необходимо превръщането на дигиталния сигнал в аналогов, който се изпраща по канала, а след получаването му се превръща отново в дигитален. Това става с т.н. устройство модулатор/демодулатор. Вместо стандартните методи за работа, се предлага използването на кодове над пръстена $\boldsymbol{Z}_n$ от остатъци по модул n, при което се отчитат само най-вероятните грешки, но значително се намалява сложността на пресмятанията. Оказва се, че кодовете над $\boldsymbol{Z}_n$ са подходящи и за записване и коригиране на грешки при флаш памети, които имат редица специфики. Например, в клетките на флаш паметта могат да се записват няколко стойности, а устройството не позволява изтриването само на една отделна клетка, което е твърде времеемко.

Теорията на криптосистемите с публичен ключ е създадена съвсем неотдавна. Първите публикации са от 1976 г., а в края на миналия век става известно, че първите засекретени разработки са от 1973 г. Това е изключително важна област от приложенията на алгебрата и теорията на числата в най-различни сфери на човешката дейност, включително в банковото дело, при плащанията по Интернет и много други. При обичайното „симетрично" зашифроване на съобщението един и същи ключ се използва както за шифроване, така и за дешифриране. При криптосистеми с публичен ключ системата за шифриране е достъпна публично, но дешифрирането е бързо и евтино само ако е известен ключът за дешифриране. Неавторизираните опити за разшифроване на съобщението са свързани с решаването на задачи с голяма сложност. Типичен пример е използването на протокола RSA, при който се налага разлагането на големи числа на прости множители, което засега е задача, която не е решима в реално време. Системи с публичен ключ се използват и за идентификация на потребителите. В изследванията на

доц. Манев се прави анализ на съществуващи криптографски схеми с прилагане на кодове, поправящи грешки, посочват се слабости на схемите и се предлагат нови мерки за защита. Идеята на стеганографията и дигиталния воден знак е да се вмъкне информацията в изображение или звук така, че да остане незабелязана за околните. Целта на стеганографията е съобщенията да се предават незабележимо, а дигиталният воден знак е за защита срещу фалшифициране и пиратство, включително за доказване на авторски права. В трудовете се предлага използването на кодове, коригиращи грешки, за влагане на скрита информация в изображения, при което се постига по-голяма устойчивост и капацитет на влаганата информация. Накрая, част от изследванията на доц. Манев са свързани с високо-производителни и паралелни пресмятания в теория на числата и алгебрата. Те косвено са свързани с криптографията, където много от методите се базират на алгебрични и теоретико-числови пресмятания. Ще отбележим и работите по редици над крайни пръстени, които са подходящи за използване в методите Монте Карло.

4. Оценка на педагогическата подготовка и дейност на кандидата. В продължение на много години с доц. Манев сме преподавали във ФМИ на СУ. Прави приятно впечатление добрата организация на неговите лекции и упражнения и тяхното много добро представяне пред аудиторията. Освен това имам непосредствени наблюдения от ръководството му на докторанти и дипломанти. Личните ми впечатления от преподавателската му дейност са отлични. Считам, че кандидатът има много успешна преподавателска работа. Водил е упражнения и е чел лекции по всички основни алгебрични дисциплини, по теория на числата и по теория на кодирането в СУ и ВТУ, курсове в магистърската програма на ИМИ, както и курсове по теория на кодирането и криптография в Англия, Япония и Южна Корея. В последните години чете лекции по основните математически дисциплини във ВСУ. Автор и съавтор е на учебници, ръководства и учебни пособия, качествата на тези, представени за конкурса, ще коментирам в следващия раздел. Има петима успешно защитили докторанти (включително една докторантка от чужбина един носител на наградата „Джон Атанасов“ за млад учен) и на няколко дипломанти.

5. Основни научни и научно-приложни приноси. Ще се спра накратко на основните резултати, съдържащи се в представените работи на кандидата, както и на оценката ми за тях. Ще следвам разпределението на статиите от справката за научните приноси.

Работа [I-1] е свързана със една от основните задачи на теория на кодирането – намирането на минималната дължина $n(k,d)$ на двоичен линеен код с дадени размерност k и минимално разстояние d. Намира се числото $n(k,d)$ за първия открит към момента на написването на статията случай и се доказва, че $n(8,10)=26$. Като страничен резултат от самостоятелен интерес се дава пълно описание на кодовете с параметри [16,7,6] и [15,7,5].

Съществуват редица важни кодове над крайни полета с повече от два елемента. Но при практическото им използване се налага преминаване към бинарни символи. В статии [I-2, III-3] се разглеждат цикличните кодове на Рид-Соломон с дължина 2^m и размерност 5 над поле с 2^m елемента. Елементите на полето се записват като наредени m-торки от двоични символи (или $(m+1)$-орки с добавяне на проверка за четност) и се определят параметрите на получените двоични кодове в зависимост от избрания базис на полето с 2^m елемента. Към този цикъл от работи кандидатът е отнесъл и статии [III-1, III-2]. В

първата статия се предлага програмно тестване за това кои кодове на Рид-Соломон са най-подходящи за шумозащита на даден канал. Системата е приложена за анализ на данните от грешките при радиокомуникации между военни поделения на територията на България. Във втората статия се разглеждат двоични циклични кодове с дължина 63 и 65 и с минимално разстояние, по-голямо от това на важните BCH-кодове. С компютърно търсене са намерени т.н. двойки кодове, които играят роля при изправянето на грешки.

Някои алгоритми за декодиране на съобщенията с коригиране на грешките се базират на минималните думи в кода. Това са думи, които са с минимален носител, т.е. в кода няма нетривиална дума, която се получава чрез заместване на някои от единиците с нули. Минималните думи се появяват и при конструкции на схеми за разпределение на тайната. Такива схеми се използват за съхраняване на особено важна информация, като кодове за дешифриране, кодове за изстрелване на ракети при военните, номерирани банкови сметки (при които името на собственика на сметката е засекретено) и др. Идеята е информацията да се раздели на части и всеки от участниците в системата да получи и пази секретна само своята част. Статии [I-3, I-4, I-6, III-5, III-7] са посветени на изучаването на минималните и близки до тях думи с методи на алгебрата, крайните проективни геометрии и компютърно търсене. Работа [I-6] обобщава по-ранните работи [I-3, I-4]. Описват се всички минимални думи или такива от даден тип за някои циклични кодове (включително на някои BCH-кодове) и за някои кодове на Рид-Малер, както и някои типове от неминимални думи за кодове на Рид-Малер.

В работи [II-1, III-4] се анализират схеми за идентификация с публичен ключ, при които се използват методи на шумозащитното кодиране. Работа [III-6] е доклад по покана на Пролетната конференция на СМБ, която прави обзор на резултатите за използване на теория на кодирането в криптографията и спомага за популяризирането на тематиката. Работа [II-2] предлага използването на кодове, коригиращи грешки, за влагане на скрита информация в изображения. Резултатите в тези четири статии коментирах по-горе в третия раздел на рецензията.

В статии [I-5, I-7, I-10, I-11, I-12, III-10, III-11, III-12] се предлага използването на кодове над пръстена $\boldsymbol{Z}_n$ при схеми за модулация. Три от статиите, [III-10, III-11, III-12] включват резултати от междинни етапи на изследванията, доразвити впоследствие в журналните статии [I-5, I-7, I-11, I-12]. В [I-5] се разглеждат кодове, които коригират една грешка от специален вид, в [I-7] се оценява вероятността за грешка при канали с Гаусов шум, в [I-11] се дава алгоритъм за меко декодиране, а в [I-12] се предлагат нови класове от такива кодове. Като резултат от изследванията значително се намалява сложността на пресмятанията. Накрая, работа [I-10] дава описание на софтуерна схема за тестване и експерименти с разработените схеми. Тя показва възможностите на използването на грид-технологии за симулации на дигитални комуникационни системи и води до намаляване на времето за експерименти.

В работа [III-8] се дава нов алгоритъм за търсене на допълващи се редици на Голей, който се прилага за търсене на редици с дължина ≤ 100. Такива редици от нули и единици (или от ± 1) са въведени за нуждите на спектрометрията, а впоследствие намират приложение в ултразвуковите и акустичните измервания, безжичния интернет, комуникациите и др. За съжаление, може би поради ограничения в обема на статията, не са приведени резултатите от търсенето. В [I-9] кандидатът разглежда линейни рекурентни редици над краен пръстен, които задават пермутации на елементите на пръстена. Такива редици могат да се използват в методите Монте-Карло. Дава се пълно

описание на такива редици от втори ред над пръстена от остатъци по модул n. Резултатът се прилага в статии [II-3, II-4] за създаване на нови генератори за псевдослучайни числа, които се използват за числено пресмятане на многомерни интеграли и за симулация и числено решаване на интегрални уравнения, описващи движението на електрони в полупроводник.
Статии [II-5, III-9, III-13] са посветени на високо-производителни и паралелни пресмятания в теория на числата и алгебрата. В [III-9] се разглеждат тройки прости числа (p,q,$2pq$+1) и се изследва тяхното разпределение, като особено внимание се обръща на случаите, когато p и q са близнаци (q=p+2) или братовчеди (q=p+4). Пресмятането на константите се свежда до пресмятане с голяма точност на дзета-функцията на Риман и на L-функцията на Дирихле. В другите две статии се описват усилията за създаване на софтуерен пакет за различни алгоритми в теорията на числата и в частност за разлагане на прости множители на големи числа с използване на алгебрични криви. Както вече отбелязахме, такива алгоритми имат отношение към криптографията.
В двете статии [III-14, III-15] се създават нови кодове над пръстена от остатъци по модул m за коригиране на специфични грешки за работа с флаш памети. Сложността на декодиране на кодовете е линейна функция на дължината, което ги прави удобни за практически цели.
Последната работа [I-8] е посветена на описанието на квадратните матрици, които могат да се диагонализират чрез спрягане с т.н. жакетови матрици. (Името „жакетова“ идва от аналогията с дрехата, която може да се носи и обърната наопаки.) Диагонализацията чрез жакетови матрици намира разнообразни приложения за създаването на бързодействащи алгоритми на линейната алгебра, в безжичните комуникации и др.
В заключение на коментариите си по научните приноси на кандидата ще отбележа, че кандидатът е запознат много добре основните задачи в областта и с литературата по разглежданите въпроси и използва богат арсенал от методи от различни области на математиката и информатиката, както и компютърни методи и пресмятания. Достоверността на аргументите в доказателствата не буди съмнение. Не съм забелязал и съществени неточности.

Лекциите по теория на числата, достъпни онлайн на страниците на ФМИ на СУ и на ИМИ – БАН, първоначално са били предназначени за бакалаври във ФМИ, но впоследствие са разширени с елементи на приложения в криптографията. Те могат да се използват и от студенти и докторанти и от други университети. Освен стандартния материал по елементарна теория на числата, те включват материал за разпределение на простите числа, нелинейни диофантови уравнения, теоретико-числови преобразования (дискретното преобразование на Фурие), както и алгоритмични аспекти на теория на числата.
Учебникът по кодиране и криптография, издаден първоначално в книжен формат, впоследствие е допълнен и достъпен онлайн на страницата на ИМИ – БАН. Той съдържа увод в теорията на информацията, основи на теория на кодирането, включително алгоритми за декодиране и увод в криптографията. В електронния вариант има и елементи на стеганографията.
Учебното пособие MATLAB в механиката и съпротивление на материалите е предназначен за курса по MATLAB за студентите във ВСУ и е в процес на разширение. Той се базира на курса по съпротивление на материалите, а учебните примери са от

варианти на курсови работи.
Материалът в учебника и учебните пособия е подбран внимателно, а изложението е с грижа за читателя и на разбираем за студентите език. Бих препоръчал след известна дообработка, текстовете да бъдат издадени и в книжен формат.

Кандидатът е представил списък с 137 цитата на негови трудове, повечето от които са в монографии и статии на изтъкнати чуждестранни специалисти. От тези цитати 42 са на статии, написани след хабилитацията, като са дадени цитати и на 10 от представените в конкурса 32 статии. Приятно е да се отбележи, че част от първите статии на доц. Манев продължават да се цитират и днес.

Документацията по конкурса е пълна и е в съответствие с изискванията на Правилника за развитието на академичния състав във ВСУ „Любен Каравелов“. Тя е добре оформена и спомага за даване на обективна оценка на постиженията на кандидата. Авторската справка правилно отразява основните приноси на трудовете, представени за участие в конкурса. Представена е справка за количествените показатели на критериите за заемане на академичната длъжност „професор”, от която се вижда, че кандидатът има 3041 точки, от които 2460 са по показателите по научно-изследователската и научно-приложната дейност. Това е значително над препоръчителните 600 точки, от които поне 80% (т.е. 480) да са от научно-изследователска и научно-приложна дейност.

6. Значимост на приносите за науката и практиката. Получените резултати в научно-изследователските статии на кандидата са интересни и съдържателни. Те съдържат нови факти за обекти, които се появяват по естествен начин в редица области на математиката и нейните приложения. Резултатите и методите за тяхното получаване са използвани и могат и занапред да се използват успешно в други изследвания от този род. Учебните пособия показват педагогическа зрялост на автора им и несъмнено са полезни за студентите и преподавателите. Кандидатът е сред уважаваните членове на българската математическа колегия.

7. Критични бележки и препоръки. Нямам особени критични бележки към документацията и към научната, научно-приложната и преподавателската дейност на кандидата.

8. Лични впечатления и становище на рецензента. Познавам кандидата от студентските му години и имам най-добри впечатления от неговите качества като човек, колега, преподавател, учен и администратор. Особено приятно впечатление прави това, че продължава да работи с млади хора, които са негови бивши ученици, всеотдайността му в преподавателската дейност и в подготовката на методически пособия за предметите, които преподава. По стечение на обстоятелствата съм имал достъп до някои от рецензиите на статии, публикувани от кандидата (например в Serdica Math. J.), и добрите ми впечатления се подсилват и от положителното мнение на рецензентите.

ЗАКЛЮЧЕНИЕ

В представените научни трудове доц. д-р Николай Лазаров Манев е получил интересни резултати в областта на приложенията на алгебрата и близки до нея области в теория на информацията. Въпреки, че резултатите носят предимно теоретичен характер, повечето

от тях са мотивирани и ориентирани към практиката. Те вече са използвани или могат да бъдат използвани при подобен род изследвания от други автори. Част от тях имат и конкретни приложения в комуникационните и информационните технологии и по-специално в теорията на сигурността при предаването на информация. Съществена част от резултатите са публикувани в авторитетни издания и докладвани на авторитетни научни форуми. Като имам предвид и наличните данни за качеството на преподавателската дейност на кандидата, това ми дава основания да предложа доц. д-р Николай Лазаров Манев да заеме академичната длъжност „професор" в професионалното направление 4.5. Математика по специалността „Алгебра и теория на числата".

София, 31 октомври 2014 г. Рецензент:

(акад. д.м.н. В. Дренски)