Р Е Ц Е Н З И Я

по конкурс за професор с единствен кандидат
доц. д-р Николай Лазаров Манев
Научна област: **4. Природни науки, математика и информатика**
Професионално направление: **4.5. Математика (Алгебра и теория на числата)**
За нуждите на: ВСУ "Л. Каравелов"
Обявен в "Държавен вестник" бр. 54/01.07.2014 г.

1. Данни за конкурса

Конкурсът е обявен в бр. 54/01.11.2011 г. на "Държавен вестник". Документи е подал единствен кандидат: доц. д-р Николай Лазаров Манев. Не забелязах допуснати нарушения по процедурата на конкурса.

2. Данни за кандидата

Николай Манев е роден на 26. юни 1952 г. във Велико Търново. През 1977 г. завършва Факултета по математика и механика на СУ "Кл. Охридски". През 1977 г. започва работа като научен сътрудник в ИМИ – БАН, където е последователно научен сътрудник III, II и I степен. През 1941 г. Николай Манев защитава кандидатска дисертация на тема "Граница на Грийсмър и оптимални кодове". През 1990 г. е избран за старши научерн сътрудник II ст. (доцент) по Алгебра и теория на числата. В периода 1992-1995 г. доц. Манев е научен секретар на ИМИ, а от 1997 до 2000 г. е и заместник-директор на ИМИ. Николай Манев е ръководител на катедра "Математически основи на информатиката" в периода 2007-2012 г. През май 2012 г. Николай Манев постъпва на работа във ВСУ "Л. Каравелов".

3. Описание на научните трудове

Кандидатът е представил за участие в конкурса 32 научни статии и три учебни помагала. От статиите дванадесет са публикувани в реферирани списания (осем от тях са с импакт фактор), пет са глави в различни сборници статии и петнадесет са в сборници с доклади от конференции и симпозиуми. Трите учебни помагала са лекции по теория на числата, лекции по кодиране и криптография и сборник от задачи по механика със MATLAB. Статиите са отпечатани в следните издания:

- IEIEC Trans. Fundamentals - 3; (Oxford Univ. Press, IF 0.24)
- Applied Mathematics and Computation - 2; (Elsevier, IF 1.6)
- Пробелмы Передачи Информации - 2; (IF Math Net Ru 0.506)
- Comptes Rendus de l'Academie Bulgare des Sciences - 1;
- Discrete Applied Mathematics - 1; (IF 0.838)
- Serdica Math. Journal - 2;
- Serdica Journal of Computing - 1;
- Proceedings of the Int. Workshop on Optimal codes and related topics - 2;
- Proceedings of the Workshop on ACCT - 6;
- сборник с доклади: Математика и математическо образование - 4;
- Proceedings of the IEEE Symposium in Discrete Mathematics - 1;
- доклади на конференцията "20 години математика във ВТУ - 1;
- Proceedings of MIPRO 2012, Croatia - 1.

Четири от тези списания – IEIEC Trans. Fundamentals, Applied Mathematics and Computation, Discrete Applied Mathematics и Проблемы Передачи Информации имат импакт фактор. Бих желал да отбележа, че при цялата условност на импакт-фактора на изданията, където са публикувани работите по дисертационния труд, той все пак е индикатор за това, че тематиката е актуална и резултатите на кандидата са значими и добре приети от научната колегия. Всички работи са написани след представянето на дисертационния труд за присъждане на степента "кандидат на науките" и след хабилитацията на кандидата.

Научните изследвания на кандидата са посветени на различни математически проблеми, възникващи при защитата на данни; това са задачи от теория на кодирането, криптографията и други свързани с тях области. Кандидатът е класифицирал работите, представени за участие в конкурса в няколко направления.

Оптимални кодове.

В работите, представени за участие в конкурса, кандидатът е представил само една работа по оптимални кодове [I-1]. В нея се доказва несъществуването на

двоичен $[25, 8, 10]$-код което решава въпроса за намирането на точната стойност на $n_2(8, 10)$. Към момента на написването на тази работа, 8 беше най-малката размерност, за която основната задача на теория на кодирането не беше решена за всички минимални разстояния d. Статията решава един от десетината открити случая към този момент. Останалите случаи бяха решени през следващите десетина години.

Двоични образи на линейни кодове.

Един начин за конструиране на двоични кодове е изобразяването на линейни кодове над $GF(2^m)$ в двоични чрез подходящо съответствие, изпращащо елементите на $GF(2^m)$ в m-орки от елементи на $GF(2)$. Въпросът, който изниква е пресмятането на спектъра на получения двоичен код от спектъра на първоначалния код над $GF(2^m)$. На тази задача са посветени работи [I-2] и [III-3]. В първата работа е определен спектърът на образа на двоичния код на разширения код на Рид-Соломн над $GF(2^m)$ с параметри $[2^m, 5]$ за определен клас от базиси на $GF(2^m)$. Втората работа е посветена отново на кодове на Рид-Соломон с параметри $[2^m, K]$, но при изображението към всяка m-орка се добавя проверка по четност. Доказано е, че за $K \leq 3$ спектърът на образа не зависи от спектъра на базиса на $GF(2^m)$. Това разпределение е пресметнато и за $K = 4$ и нечетно m.

Декодиране на циклични кодове.

В работи [III-1] и [III-2] са разгледани някои въпроси, възникващи при декодирането на циклични кодове.

Минимални думи в линейни кодове.

Една дума в линеен код се нарича минимална, ако носителят ѝ е минимален по включване. Минималните думи в ортогоналния код задават авторизираните коалиции в схема за разпределяне на данни, реализирана чрез линеен код. Работи [I-3], [I-4], [I-6], [III-5] и [III-7] са посветени на определянето на минималните думи в опредлени класове кодове. В работи [I-3], [I-6] и [III-5] се разглеждат циклични кодове с дължина $n = 2^m - 1$ и пораждащи полиноми $m_1(x)m_3(x)$, $m_1(x)m_5(x)$ и $m_1(x)m_{2^s+1}$. В [III-7] се определя мощността на множеството от минмални думи за всички двоични циклични кодове с дължина 31. В [I-4] се изследват минимални думи в кодове на Рид-Малер.

Кодове, поправящи грешки и криптография.

В тази група се включват четири работи: [II-1], [II-2], [III-4] и [III-6]. Общото в тях е, че изследваните криптосистеми с публичен ключ се основават на линейни кодове. В [II-1] е анализирана криптосистемата на Босерт-Мар-Хайлиг и са

посочени редица слабости, които могат да доведат до компрометирането ѝ. Предложени са мерки за отстраняването на тези слабости.

В работа [III-4] е направен подробен анализ на схемата на Стърн за идентификация. Тя се основава на трудността на общата задача за декодиране с линейни кодове, за която е известно, че е NP-пълна.

Статия [III-6] е обзор, представящ някои приложения на теория на кодирането в криптографията. В работа [II-2] е описана възможност за използване на идеи от теория на кодирането в стеганографията и създаването на цифров воден знак.

Кодове над $\mathbb{Z}_m$ и схеми за модулация.

В това направление попада най-голямата група от работи: [I-5], [I-7], [I-10], [I-12], [I-13], [III-10], [III-11] и [III-12]. В тях се изследват специални кодове над $\mathbb{Z}_m$ и приложението им към различни схеми за модулация. В работа [I-5] се конструират кодове, поправящи единична грешка от тип $(\pm 1, \pm e, \ldots, \pm e^{k-1})$. По-нататък те се обобщават до кодове, поправящи единична грешка от тип $(\pm e_1, \pm e_2, \ldots, \pm e_s)$, където $e_i \in \mathbb{Z}_A$. За много от конструираните кодове е получен точния вид на проверочната матрица. В работи [I-11] и [I-12] се конструират кодове, поправящи две $\{\pm 1\}$-грешки и се изяснява прилагането им към QAM-схеми за модулация. Работа [I-10] е описание на възможностите, които предлагат изчислителните грид-технологии за симулация на цифрови комуникационни системи. В останалите три работи, [III-10], [III-11] и [III-12] се съдържат междинни резултати от изследванията втова направление, които са докладвани на различни международни конференции.

Изследване на редици над различни структури.

В работа [III-8] се разглеждат двоични взаимнодопълнителни редици, въведени от М. Голей във връзка със проблем на инфрачервената спектрометрия. В статията е описан нов алгоритъм за намиране на двойки взаимнодопълнителни редици. Една двойка редица се нарича ядро, ако тя не може да бъде построена от двойка по-къси редици по определени правила. Дължините на известните ядра са 2, 10 и 26. Използвайки новия алгоритъм, в статията е пресметнато, че за $n \leq 100$ възможните дължини на ядра са 34, 50, 58,68, 74 и 82.

В [I-9] се изследват два вида линейни рекурентни редици над пръстени от остатъци $\mathbb{Z}_M$ строго балансирани редици (т.е. такива, при които всеки елемент се появява a пъти в рамките на един период) и редици пораждащи пермутации (такива, за които тази константа е 1). Доказани сеа необходими и достатъчни условия за една редица от втори ред да е от един от тези два типа. Обсъждат се и възможни приложения на тези редици.

В работи [II-3] и [II-4] са описани експериментите за числено интегриране на многомерни интеграли с помощта на един генератор на линейни рекурентни редици, използващ линейни рекурентни редици от втори ред, които са изследвани в [I-9].

Паралелни изчисления в теория на числата и алгебрата.

В тази група попадат три статии [II-5], [III-9] и [III-13]. В тях са описани някои резултати, получени при разработване на високопроизводителни алгоритми за решаване на задачи от теория на числата.

Кодове за флаш-памети.

Оказва се, че спецификите на флаш паметите създават необходимост от специални кодове. В работи [III-14] и [III-15] се разглеждат конструкции на линейни кодове над $\mathbb{Z}_m$, които се оказват особено добре пригодени за използване във флаш-памети. В [III-14] е предложена конструкция на код, поправящ единична асиметрична грешка. Друга конструкция на код, поправящ единична грешка от тип $(\pm 1, 2)$ е описана в [III-15].

Комбинаторика.

Работа [I-8] е единствената статия по комбинаторика. Тя е посветена на т.нар. jacket матрици - квадратни матрици, обобщаващи матриците на Адамар. В статията се доказват някои свойства на тези матрици. Доказват се и необходими и достатъчни условия за това една матрица да е диагонализуема чрез трансформация, зададена с jacket-матрица. Доказани са и редица интересни странични резултати като например необходимо и достатъчно условие една матрица на Вандермонд да е jacket-диагонализуема.

Учебни помагала.

Кандидатът е представил и три учебни помагала: лекции по теория на числата, лекции по кодиране и криптография и сборник със задачи по механика за MATLAB.

Помагалото по теория на числата е в обем от 107 страници и включва както стандартен увод в теория на числата, така и няколко приложни глави, посветени на някои теми по криптография и дискретно преобразуване на Фурие.

Помагалото по кодиране и криптография е в обем от 112 страници и фокусирано върху циклични кодове и асиметрични криптосистеми.

4. Научни приноси

По мое мнение по-важните приноси на кандидата се свеждат до следното:

(1) Доказано е несъществуването на двоичен $[25, 8, 10]$-код.

(2) Пресметнати са спектрите на двоичните образи на някои кодове на Рид-Соломон над $GF(2^m)$.

(3) Определени са множествата от минимални думи за различни класове двоични кодове.

(4) Конструирани са кодове, поправящи единична грешка от тип $(\pm e_1, \pm e_2, \ldots, \pm e_s)$, където $e_i \in \mathbb{Z}_A$, както и кодове, поправящи две $\{\pm 1\}$-грешки и се изследва прилагането им към QAM-схеми за модулация.

(5) Предложени са конструкции на линейни кодове над $\mathbb{Z}_m$, пригодени за използване във флаш-памети.

(6) Създаден е нов алгоритъм за намиране на двойки взаимнодопълнителни редици на Голей.

(7) Доказани са се и необходими и достатъчни условия за това една матрица да е диагонализуема чрез трансформация, зададена с jacket-матрица.

5. Преподавателска дейност

Кандидатът има богата преподавателска дейност, обхващаща период от над 35 години. Тя включва изнасяне на лекции по Линейна алгебра, Висша алгебра, Алгебра и теория на числата, Компютърна алгебра, Криптография, Теория на кодирането и др. в Софийския Университет "Св. Кл. Охридски", Великотърновския Университет И ВСУ "Л. Каравелов" .

Доц. Николай Манев има (поне) петима докторанти (между тях са Емил Колев, Юри Борисов, Христо Костадинов) и девет дипломанти.

6. Проектна дейност, участия в конференции, лични впечатления и др.

Доц. Николай Манев участва активно в различни проекти за научни изслердвания. През годините той е ръководител на три прокта с Фонд "Научни изследвания", координатор е на един проект по TEMPUS и е ръководител на един проект с Европейската Комисия HPCF-CT-1999-00164. Доц. Манев е председател на 11 и член на 18 организационни и програмни комитета на научни конференции, провеждани у нас и в чужбина. Сред тях следва да се отбележи ролята му в утвърждаването на изключително успешната конференция по Алгебрична и комбинаторна теория на кодирането, която се провежда от 1988 г. и има вече 14 издания.

Административна дейност също е изключително богата: той е научен секретар на Института по математика и информатика в периода януари 1992 - юни 1995 година; заместник-директор на ИМИ от 1997 до 2000 г; заместник декан по учебната част на ФМИ на ВТУ в периода 1990 - 1997 г., както и ръководител на секция "Математически основи на информатиката" в периода 2000 – 2007 г.

Познавам лично кандидата от повече от 30 години. Присъствал съм многократно на негови доклади, изнасяни на наши и международни конференции. Впечатленията ми са, че той е сериозен изследовател със задълбочени познания в широки области на теория на кодирането и криптографията. За мен е извън всяко съмнение, че той удовлетворява изискванията за заемане на длъжността "професор" във ВСУ.

7. Заключение

Считам, че в своята научно-изследователска работа доц. Николай Манев е получил важни научни резултати, които съответстват на съвременните постижения и представляват значителен и оригинален принос в науката. С работите си кандидатът показва задълбочени теоретични знания в областта на теорията на кодирането, както и способност да ръководи научни изследвания. Преподавателската му дейност е изключително интензивна и е провеждана на високо ниво. Заедно с това той взима активно участие в живота на математическата общност. Гореизложеното ми дава основание убедено да препоръчам на Уважаемото Жури, както и на уважаемите членове на Академичния сывет на ВСУ, да присъдят на доц. Николай Лазаров Манев научното звание "Професор" на ВСУ "Л. Каравелов" в професионално направление: Математика (алгебра и теория на числата).

София, 31.10.2014 г.

Рецензент:

(проф. д.м.н. Иван Ланджев)