Р Е Ц Е Н З И Я

от проф. дмн Румен Николов Даскалов,
Технически Университет – Габрово,
катедра „Математика”

на материалите, представени за участие в конкурс
за заемане на академичната длъжност “професор”
в Института по математика и информатика (ИМИ) на БАН

Област на висше образование – 4. Природни науки, математика и информатика,
Професионално направление - 4.6. Информатика и компютърни науки,
Научна специалност - 01.01.12 Информатика (компютърни подходи в изследването на шумозащитни кодове)

В конкурса за професор, обявен в ДВ, бр. 32 от 24. 04. 2012 г. и на страницата на ИМИ-БАН в Интернет за нуждите на секция “Математически основи на информатиката”, като единствен кандидат участва доц. д-р Цонка Стефанова Байчева от ИМИ - БАН.

1. Основание

Тази рецензия е представена на основание заповед № 163 от 23.05.2012 г. на директора на ИМИ-БАН и протокола от първото заседание на научното жури, проведено на 06.07.2012 година.

2. Кратки биографични данни

Доц. д-р Цонка Стефанова Байчева е родена през 1961 г. в гр. Килифарево. Средното си образование завършва в Математическа гимназия, гр. Велико Търново през 1979 г., а висшето си образование в ТУ-София през 1984 година като магистър със специалност „Изчислителна техника”. В периода 1986-1988 г. работи като програмист в ТИИЦ, гр. Велико Търново и от 1988 г. е научен сътрудник в ИМИ-БАН. През 1998 г. защитава дисертация на тема „Радиуси на покритие на класове линейни кодове” и получава образователната и научна степен „доктор” по специалност 01.01.12 Информатика. От 2001 г. е доцент в секция “Математически основи на информатиката” на Института по математика и информатика на БАН.

3. Общо описание на представените научни резултати

Общият брой на публикациите на доц. д-р Цонка Байчева е 63, като част от тях са цитирани 139 пъти. В конкурса доц. Байчева участва с **26** научни публикации, които могат да бъдат класифицирани както следва:

По вид:

- Публикувани статии в научни списания – **19** броя;
- Публикувани доклади на научни конференции – **7** броя;

По значимост

- Статии в научни списания с импакт фактор – **14** броя [1- 14].
- Статии в научни списания без импакт фактор – **5** броя [15- 19].

По място на публикуване:

- Доклади на международни научни конференции в чужбина – **3** броя .
- Доклади на международни научни конференции в България – **2** броя .
- Доклади в научните трудове на университетски конференции – **2** броя .

По езика, на който са написани:

- На английски език - **26** броя ;

По брой на съавторите:

- Самостоятелни – **7** броя ;
- С един съавтор – **12** броя ;
- С двама съавтори – **4** броя ;
- С трима съавтори – **3** броя.

4. Обзор и съдържателен анализ на съдържанието и на научните и научно-приложните постижения в представените материали

Първите шест статии от всичките 14 статии с IF са оценени в конкурса за получаване на академичната длъжност "доцент" и в съответствие с чл. 29, ал.3 от ЗРАСРБ няма да бъдат разглеждани. Останалите 20 представени научни резултати можем да разделим на 5 групи:

В първата група включвам публикациите свързани с радиус на покритие на класове линейни кодове (статии [8], [10], [11] и доклада [22]).

Преди да разгледаме представените публикации ще отбележим, че статиите [8] и [10] са публикувани в авторитетното международно научно списание с висок импакт фактор IEEE Transactions on Information Theory, а [11] в Advances in Mathematics of Communications. Следователно са получили висока оценка от поне двама международни рецензенти, достатъчно известни специалисти в разглежданата област.

Двоичен линеен $[n,k,d]$ код C е k-мерно подпространство на n- мерното векторно пространство F_2^n над двоичното поле F_2 с минимално *разстояние по Хеминг* d. Казваме, че векторът x е R-*покрит* от вектора y, ако $d(x,y) \le R$. *Радиус на покритие* $R(C)$ на кода C е най-малкото цяло число R, такова че всеки вектор x от пространството е R-*покрит* от поне една кодова дума на C.

Радиусът на покритие е един от основните параметри на линеен код. Той е мярка за разстоянието между кода и най-отдалечените вектори в пространството. Ако радиусът на покритие е строго по-малък от минималното разстояние на кода, то такъв код е максимален и към него не могат да се добавят нови думи без да се намали минималното му разстояние.

В книгата си „Covering codes“, North-Holland mathematical Library (1997), G. Kohen, I, Honkala, S. Lytsin и A. Lobstein представят таблица (Таблица 7.1, стр. 193-200) с горни и долни граници за функцията $t_2[n,k]$ - минималният радиус на

покритие на линеен двоичен $[n,k]$ код. В статията [8], *от материалите за участие в конкурса*, е предложен метод за конструиране на кодове с даден радиус на покритие и фиксирано разстояние на ортогоналния код. Методът е приложен за кодове с радиус на покритие равен на долната граница за $t_2[n,k]$ от таблица 7.1 и като са използвани особености на пораждащите матрици са решени първите шест отворени случаи от тази таблица. Доказано е, че долните граници не могат да се достигнат и по този начин са установени следните точни стойности – $t_2[17,6]=5$, $t_2[17,8]=4$, $t_2[18,7]=5$, $t_2[19,7]=5$, $t_2[20,8]=5$, $t_2[21,7]=6$.
(***Редактор на статията е бил S. Lytsin.***)

В статията на R. Graham, N.J.A. Sloane „On the covering radius of codes", IEEE Trans. Inf. Theory, (1985) са определени стойностите на функцията $t_2[n,k]$ за кодове с размерности до 5. Представени са и горни граници за функциите $t_2[n,6]$ и $t_2[n,7]$. Статията [11] е съвместна с Илия Буюклиев. В нея са определени минималните радиуси на покритие на всички двоични линейни кодове с размерност 6, като основният резултат е, че $t_2[n,6]=\left\lfloor \frac{n-8}{2} \right\rfloor$ при $n \geq 18$. В основата на получените резултати е разработеният от авторите евристичен алгоритъм, който бързо определя долна граница на радиуса на покритие на линеен код. Изведена е и горна граница за функцията $t_2[n,k]$ за кодове с размерности 8 и 9. Направена е класификация и са конструирани всички двоични линейни кодове с дължини до 15 и размерности до 6, имащи минимален радиус на покритие. Използвайки получената класификация е представена конструкция на кодове с произволна дължина и минимален радиус на покритие, имащи размерност до 5. Показано е, че съществува единствен [19, 6, 7] код с минимален радиус на покритие 5. Като е използван този резултат, а също така, че [14, 6, 5] кода с минимален радиус на покритие 3 е единствен, и че двата кода са нормализирани и всичките им координати са приемливи е дадена конструкция на кодове с минимален радиус на покритие и размерност по-голяма от 6. (***Редактор на тази статия е бил отново S. Lytsin.***)

Квазисъвършени кодове (КС кодове) са кодовете, на които радиусът на сферичната опаковка и радиусът на покритие се различават с единица. Те са обобщение на съвършените кодове, които имат равни такива радиуси. Съвършените кодове могат да коригират всички грешки, които откриват, но както знаем те са много малко на брой. КС кодове са широко изследвани, но до появата на статията [10] известните примери на такива кодове са съдържали само по един код за съответните дължина и размерност. В [10] е даден отговор на въпроса: при фиксирани дължина и размерност има ли нееквивалентни КС кодове? Отговорът е положителен и е получен след като са класифицирани всички двоични КС кодове с размерности до 9 и троични КС кодове с размерности до 6. Получени са и частични резултати за двоични КС кодове с размерности до 14 и за троични КС кодове с размерности до 13. Предложена е модификация на един от методите за намиране радиуса на покритие на линеен код, в която се разглеждат само тези кодове, които имат предварително зададен

радиус на покритие. Получените в това изследване резултати показват, че за всяка размерност има само по няколко възможни дължини, за които могат да съществуват КС кодове. В някои от случаите са намерени хиляди кодове. Налага се изводът, че задачата за класифициране на всички възможни параметри на КС кодове е многократно по-тежка от тази за съвършените кодове. До появата на [10] са били известни само няколко примера на КС кодове с минимално разстояние по-голямо от 5. В [10] се дават нови примери на такива кодове и се поставя въпроса: има ли КС кодове с минимално разстояние по-голямо от 8. (***Редактор на тази статия е бил T.Etzion.***)

В доклада [22] са изследвани троичните проективни кодове с размерности $k = 4$ и $k = 5$. С програмата Q-EXTENSION са класифицирани всички проективни троични кодове в първата размерност. В следващата размерност $k = 5$ са класифицирани само кодовете с дължина до 15. Определени са и точните стойности на функцията $t_3[n,4]$ за $13 \le n \le 21$.

Във втората група включвам публикациите, посветени на поведението на шумозащитни кодове при откриване и коригиране на грешки (статии [7], [16], [17], [18] и доклад [25])

В тази група са разгледани няколко „добри" конкретни кодове от гледна точка на това, дали са подходящи за контрол на грешки. Един код се нарича *t-подходящ*, ако вероятността му за неоткрита грешка е монотонна функция в интервала $\varepsilon \in \left[0, \frac{q-1}{q}\right]$. Оказва се, че проверката дали един код е подходящ за контрол на грешки е доста трудна задача и намирането на такива кодове предизвиква значителен интерес сред изследователите.

В съвместната със С. Додунеков и R. Koetter статия [7] е изследван квадратично-остатъчния $[13,7,5]_3$ код. Показано е, че той има радиус на покритие 3 и че е подходящ за откриване и коригиране на грешки. Представени са два ефективни алгоритъма за декодирането му, като първият свежда декодирането до използване на стандартен BCH декодер, а вторият е по-ефективен и използва таблица с 12 елемента в GF(27).

В статията [16] са разгледани кодовете на Reed-Solomon RS(10;9) и Glynn Gl(10;9) над GF(9). Тези кодове са нееквивалентни [10, 5, 6] MDS кодове, които се разширяват до [12, 6, 9] такива и всички разширени кодове са почти MDS. Въпреки, че двата кода се различават геометрично, тегловите разпределения на лидерите на съседни класове напълно съвпадат. От това, че радиусите им на покритие са равни на 4, следва че имат еднакви вероятности за неоткрита грешка след коригиране на до 4 грешки.

Интересен въпрос за линейни кодове е следния въпрос: Дали основните параметри (*дължина, размерност, минимално разстояние и радиус на покритие)* на един код определят еднозначно поведението му при отриване и коригиране на грешки? В методичната статия [17] са изследвани двоични линейни кодове с параметри [15, 3, 7], [15, 3, 8] и [16, 3, 8] с цел демонстриране как различните

параметри на един линеен код влияят върху поведението му при контрол на грешки. Показано е, че спектърът на лидерите на съседни класове на един линеен код не определя еднозначно спектъра на лидерите на съседните класове на ортогоналния му код. Следователно, за тези спектри не могат да се изведат тъждества от типа на тъждествата на MacWilliams.

В [18] и [25] са пресметнати тегловите разпределения, разпределенията на лидерите на съседните им класове и тегловите разпределения на самите съседни класове на двоични циклични кодове, на двоични MDS кодове, на двоични CRC кодове и на троични циклични и негациклични кодове. Базирайки се на резултати на Додунекова и Додунеков и използвайки системата Maple е определено кои от тях не са *t*-подходящи. Резултатите, получени в [18] и [25], позволяват да определи дали даден код е *t*-подходящ в някой подинтервал на интервала $\left[0, \frac{q-1}{q}\right]$. Общите теоретични части на [18] и [25] почти съвпадат.

В третата група включвам публикациите свързани със скъсени циклични кодове (CRC codes) (статии [9], [19] и доклади [23], [24])

За осигуряване на коректното предаване на информация в комуникационните системи в края на информационните последователности се добавят допълнителни битове. Много често за това се използват CRC кодове. В приложенията обикновено се избира стандартизиран CRC, като се счита че той ще е достатъчно добър. В голяма част от случаите това не е така. Някои от стандартизираните 16-битови CRC кодове имат поведение при контрол на грешки, което е по-лошо от това на други 16-битови CRC кодове. Една от причините за това е, че в началните години са били използвани основно хардуерни разработки с пораждащи полиноми, които имат по-малко ненулеви коефициенти. В статията [19] и доклада [23] чрез изследване на някои от най-често използваните стандартизирани кодове е показано, че подходът да се избира стандартизиран код или такъв с неразложим пораждащ полином или пораждащ полином, който в разлагането си има множител $(x+1)$ не винаги е удачен.

В много изследвания се предлагат най-добрите полиноми за фиксирани дължини и вероятности за грешка на канала, но не се дава достатъчно информация, която да позволява на тези, които разработват комуникационни системи сами да правят сравнение между полиномите и да изберат най-подходящия за тяхната разработка. За да се попълни тази празнота и предостави нужната информация за сравняване поведението при контрол на грешки на CRC кодове с до 10 проверочни символа (в практиката се използват до 64), в [9] и [24] са изследвани полиномите, които са подходящите да бъдат използвани като пораждащи полиноми на CRC кодове. Първо е съставен списък на всички такива полиноми, като от него са изключени реципрочните, тъй като пораждат еквивалентни кодове и е определен реда на тези полиноми. След това се пресмятат всички необходими данни, които позволяват сравняване поведението им при откриване и коригиране на грешки за линейно време. За избягване сравняването на всички полиноми от зададена степен, се предлага процедура от 4

стъпки, която дава възможност да се сравняват само няколко от най-добрите кодове.

В някои от комуникационните протоколи кодирането със CRC кодове се прилага към съобщения с дължина, многократно надвишаваща реда на пораждащия полином. Затова трябва да се използва повторение на оригиналния код. Кодиращите и декодиращите процедури за тези кодове са същите както и при CRC кодовете, но тяхното минимално разстояние е 2. В [9] е изведена формула за пресмятане на кодовите думи с тегло 2 в такива кодове и този резултат се оказва достатъчно полезен при оценката на вероятността им за неоткрита грешка.

В четвъртата група включвам характеристики на шумозащитни кодове, свързани с техните възможности за контрол на грешки (статии [13], [15] и доклади [20], [21])

Един (n, M, d) код е множество от M двоични думи с дължина n и минимално разстояние по-голямо или равно на d. За фиксирани стойности на n и d, с $A(n,d)$ се означава максималното цяло число M, за което съществува (n, M, d) код. Известно е, че $A(8,3) = 20$, а в [20] е доказано, че нееквивалентните $(8,20,3)$ кодовете са пет на брой.

Свойството на един код да е нормализиран е въведено в цитираната вече статия на Graham и Sloane от 1985 година. Това свойство трябва да притежават кодовете, за да могат да участват в конструкцията смесена директна сума (*amalgamated direct sum* (ADS)), представена в същата работа. Целта на тази конструкция е да се получат кодове с колкото е възможно по-малък радиус на покритие. В [13] са обобщени резултатите за известните параметри, за които двоичните кодове са нормализирани, доказано е, че всички двоични кодове с дължини 16, 17 и 18 и ко-размерност 10 са нормализирани и е направена класификация на тези кодове. Дадени са и примери как получените класификационни резултати могат да се използват за конструиране на кодове с минимален радиус на покритие.

Възможностите за коригиране на грешки на голяма част от блоковите кодове, които се срещат в различни публикации, се описват в контекста на коректното приемане на цялото съобщение. Съществуват, обаче, много приложения, при които някои от позициите на съобщението имат по-голяма тежест от други. Линейни кодове, които защитават някои от позициите на съобщението срещу по-голям брой грешки отколкото други негови позиции се наричат линейни кодове с неравномерна защита от грешки (linear unequal error protection (LUEP)). В [15] са разглеждани кодове с неравномерна защита на един от информационните символи.

Основната задача е да се намери LUEP код с фиксирана размерност и отделящ вектор такъв, че дължината му да е минимална. Тогава скоростта му ще е максимална. За целта се използва компютърно търсене за пресмятане на отделящите вектори на троични циклични и нега-циклични кодове с дължини до 26 и минимално разстояние поне 3.

Известно е, че за един линеен $[n,k,d]$ код всички грешки с тегло $t \le \frac{d-1}{2}$ са поправими по единствен начин. Съществуват, обаче, грешки с тегло по-голямо от t, които са също могат да се коригират по единствен начин. Това са случите когато съседните класове с тегла по-големи от t имат единствен лидер. Естествени са следните въпроси: кои са грешките, които могат да се коригират по единствен начин; колко са те при предварително зададено тегло; какво е най-голямото тегло на грешка, която може да се коригира по единствен начин? В [21] е даден отговор на тези въпроси за двоичните циклични кодове с дължина до 31, двоичните кодове с максимално минимално разстояние с дължини до 33 и всички троични циклични и нега-циклични кодове с дължини до 22, като не само са опредени точните стойности на теглата на поправимите по единствен начин грешки, но е посочен и броя на единствените лидери в съседните класове.

В петата група включвам публикациите свързани с оптимални оптични ортогонални кодове и свързаните с тях комбинаторни структури (статии [12], [14] и доклад [26])

Въведените в статията на Chung F.R.K., Salehi J.A., Wei V.K., „Optical orthogonal codes: design, analysis and applications", IEEE Trans. Inform. Theory 35, (1989), 595-604 оптични ортогонални кодове (OOC) са фамилии от двоични последователности с определени авто-корелационни и крос-корелационни свойства. Те осигуряват много високи скорости на комуникация през оптични CDMA комуникационни мрежи. Използването на тези кодове позволява на голям брой потребители да предават данни асинхронно с необходимата скорост и надеждност. OOC имат приложения също в мобилните радиосистеми, комуникациите с разпръснат спектър и прескачане на честота, радари и други. Оптичните ортогонални кодове са свързани и с много други комбинаторни структури. В [12], [14] и [26] са направени пълни класификации на OOC и на свързаните с тях комбинаторни обекти. В [12] и [26] са класифицирани до изоморфизъм оптималните (v, 4, 1) OOC (двоичните (v, 4, 1) CPCW кодове) с $v \le 76$, цикличните $2-(73, 4, 1)$ и $2-(76, 4, 1)$ дизайни и (73, 4, 1) цикличните разностни фамилии. В основата на алгоритъма за класификация е известната техника за търсене с връщане с тест за минималност на частичните решения, представена в книгата на Kaski и Osterg˚ard "Classification algorithms for codes and designs". За ефективното осъществяване на теста за минималност всички възможни блокове са подредени според въведена лексикографска наредба и действието на автоморфизмите на цикличната група от ред v.

В статията си „Optimal (n, 4, 2)- OOC of small order", Discrete Math. 279 (2004), 163-72, Chu W. и Colbourn C.J представят таблица на оптималните (v, 4, 2) OOC с $v \le 44$, като конструират по един код за всяко v с помощта на алгоритъм, основан на задачата за максимална клика в граф. С подход, подобен на този от [12] и [26] в [14] Байчева и Топалова правят пълна класификация на (v, 4, 2, 1) кодовете с $v \le 75$ и $v \ne 71$. Някои от резултатите в [12], [14] са получени с помощта на паралелни програми, изпълнени на българския суперкомпютър BlueGene/P.

5. Отражение на научните публикации на кандидата в научната общност (известни цитирания)

Представен е списък със 139 известни цитирания на всички публикации на кандидатката. От този списък се вижда, че цитиранията на научните публикации от списъка за участие в конкурса са 119. Голяма част от тях са от чуждестранни автори в международни специализирани научни списания. От тези цитирания 97 са на първите 6 статии от списъка. Останалите статии и доклади са цитирани 22 пъти.

6. Обща характеристика на дейността на кандидата

Доц. д-р Цонка Стефанова Байчева е чела лекции и водила упражнения във ВТУ"Св.св. Кирил и Методий" по шест учебни дисциплини; в ТУ-Варна – по четири дисциплини; в Бургаски свободен университет – по три дисциплини и във Варненски свободен университет, УНК Смолян – по една учебна дисциплина.

Изнесла е три лекции при посещение в университета в Гент, Белгия и четири лекции при посещения в Института по математика на Унгарската академия на науките.

Била е научен ръководител на двама докторанти, от които единият е защитил успешно дисертационен труд в Норвегия през 2007 година.

Участвала е в разработването на шест научноизследователски проекти с националния фонд „НИ" (N 35/1991-1994, N 197/1994, ММ-502/1995, I-519/1995, ММ-901/1999, ММ-1405/2004); съвместен проект на БАН и фондът за научни изследвания на Фландрия (2006-2011); проекти на ЕБР с Русия и с Унгария, както и в проекти, финансирани от външни за България източници като: DFG, Улм, Германия, 1999; DAAD, Охрид, Македония, 2009; „Finite structures", Marie Curie Host Fellowship for the Transfer of Knowledge, 2004, 2005 и NATO Advanced Research Workshop „Enhancing cryptographic primitives with techniques from error correcting codes", 2008.

Била е член на организационните комитети на международните научни конференции – Алгебрична и комбинаторна теория на кодирането, Поморие, 2012; Оптимални кодове, Варна, 2009; Конференцията на НАТО по криптография, В. Търново, 2008; Научна конференция на ВТУ, 2006 и есенните национални семинари по теория на кодирането, 2002-2011. Съорганизатор е на съвместния семинар по „Математически основи на информатиката" между секция „Математически основи на информатиката" на ИМИ-БАН и факултет „Математика и информатика" на ВТУ"Св.св.Кирил и Методий".

Доц. д-р Цонка Байчева е член на Съюза на математиците в България от 1990 г. и на American Mathematical Society от 2006 година.

7. Приноси (научни, научно-приложни, приложни)

Приносите можем да класифицираме като научни и научно-приложни.

8. Оценка на личния принос на кандидата

Самостоятелните публикации са седем**.** Приемам, че приносът на доц. д-р Цонка Стефанова Байчева в съвместните публикации е равностоен с този на съавторите.

9. Критични бележки

Според **чл. 29, ал. 3 от ЗРАСРБ** представените от кандидатите за заемане на академичната длъжност „професор" публикации в специализирани научни издания не трябва да повтарят представените за придобиване на образователната и научна степен "доктор", на научната степен "доктор на науките" и за заемане на академичната длъжност "доцент". Правилникът за условията и реда за придобиване на научни степени и за заемане на академични длъжности в ИМИ-БАН позволява включване на такива публикации, но в този случай има противоречие със ЗРАСРБ и тъй като този правилник на ИМИ-БАН има най-нисък ранг, то в такъв случай трябва да се прилага ЗРАСРБ.

Поради горната причина не е било необходимо включването на първите шест статии с импакт фактор в списъка за участие в конкурса. Останалите 14 статии (осем в престижни научни списания с импакт фактор) и 6 доклада са достатъчни и напълно удовлетворяват изискванията на гореспоменатия правилник на ИМИ. Приемам, че тези статии са включени само за пълнота на разглежданите изследвания.

10. Заключение

За мен няма никакво съмнение, че представените научни резултати напълно отговарят на изискванията на ЗРАСРБ и на правилника за условията и реда за придобиване на научни степени и за заемане на академични длъжности в Института по математика и информатика на БАН. Поради това убедено предлагам на научния съвет на Института по математика и информатика на БАН доц. д-р Цонка Стефанова Байчева **да бъде избрана** за „ професор" на ИМИ в област на висше образование - 4. Природни науки, математика и информатика,
професионално направление - 4.6 Информатика и компютърни науки,
научна специалност - 01.01.12 Информатика (компютърни подходи в изследването на шумозащитни кодове)

05. 09. 2012 г. Подпис:

/проф. дмн Р. Даскалов/