БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ПО МАТЕМАТИКА И ИНФОРМАТИКА

А В Т О Р Е Ф Е Р А Т

на

Д И С Е Р Т А Ц И Я

ОПТИМАЛНИ КОДОВЕ ЗА КОНТРОЛ НА ГРЕШКИ И ОПТИЧНИ КОМУНИКАЦИИ

на

Цонка Стефанова Байчева

за придобиване на научната степен
„доктор на науките“
по научна специалност
01.01.12 - информатика

2015 г.

Увод

За рождена дата на теорията на кодирането може да се счита излизането на класическата статия [47] на Шенон през 1948 година. Шумозащитните кодове са били разработени за да откриват и коригират грешките, които се появяват при предаването на дискретна информация по комуникационни канали или при нейното съхраняване на различни носители. Целта на кодирането е да се добави допълнителна информация към данните така, че да има възможност да бъде възстановено оригиналното съобщение, ако са възникнали не повече от предварително очакван брой грешки. На съвременния етап, теорията на кодирането е самостоятелна дисциплина, която използва резултати от различни области на математиката като алгебра, геометрия, комбинаторика, дискретна математика. Това позволява създаването на кодове с добри шумозащитни характеристики.

От гледна точка на практическото приложение на шумозащитните кодове и на кодовете за оптични комуникации е необходимо не само да се покаже съществуването на код с определени характеристики, но и да се конструира самия код. Интерес представлява също пълната класификация на кодове със зададени параметри, както и определянето на техните основни характеристики. Така става възможен избора на най-подходящия за всяка конкретна ситуация код. Особено актуални и интересни са тези резултати в последните години, когато все по-често се правят софтуерни реализации на кодирането и декодирането и това позволява да бъде избран най-точно отговарящия на изискванията на конкретното приложение код.

В огромната част от случаите, използването на чисто математически подходи за решаването на тези задачи не може да доведе до търсения резултат. Една възможност за решаването на такъв тип задачи е използването на компютър, което е свързано с възможностите му да извършва аритметични операции или да съпоставя данни и в зависимост от получения резултат да предприема едно или друго продължение на работата, а също и да съхранява, обработва и предоставя за използуване в най-разнообразен вид огромни обеми от данни. Директната им атака с компютър обаче позволява да се получат решения само за ограничени по обем входни данни, за които е невъзможно те да бъдат получени ръчно. Причината за това е във факта, че експоненциално нарастващата им трудност бързо стопява предимството на компютъра да работи многократно по-бързо от човека и да помни големи количества информация. За по-големи входни данни се налага за всяка отделна задача да се провеждат предварителни математически изследвания, които макар да не решават директно въпроса, силно съкращават възможностите, които трябва да се изследват с компютър. Друга възможност е разработването на все по-бързи и икономични на памет програми, което изисква отличното познаване и умелото използване

на свойствата на изследваните математически обекти и възможностите на компютъра. Така се оформя една все по-успешна хибридна математико-компютърна стратегия, с помощта на която бяха решени някои трудни алгоритмично разрешими задачи в различни области на математиката.

Целта на настоящата работа е изследването и представянето на класове шумозащитни кодове имащи добри характеристики по отношение на откриване и коригиране на грешки, както и на оптични ортогонални кодове и свързаните с тях комбинаторни структури. Да се направят класификации на някои класове от най-широко използваните в практиката кодове и да се определят техни основни характеристики, свързани с възможностите им за контрол на грешки. Да се разработи удобна за използването на тези данни процедура, която да позволи избора на най-подходящ и ефективен за всяко конкретно практическо приложение код. Наред с това, да бъдат решени отворени проблеми от теорията на кодирането.

Работата съдържа, увод, седем глави и приложение.

В първа глава са въведени основните понятия и твърдения от теорията на кодирането, които са използвани по-нататък в изложението. Дадени са горни и долни граници за радиуса на покритие и за стойностите на функцията $t_q[n,k]$.

Множеството от редици с равни дължини (*кодови думи*) от букви на азбуката $L = \{a_1, a_2, \ldots, a_s\}$ се нарича *блоков код* или просто *код* над азбуката L, дължината n на кодовите думи - *блокова дължина*, а броя на ненулевите елементи в кодовата дума - *тегло* на кодовата дума. Когато всички кодови думи на един блоков код имат едно и също тегло, кодът се нарича *константно-тегловен*.

Разстояние по Хеминг между две думи с дължина n над азбуката L се дефинира като броя на позициите, в които тези две думи се различават, а под *разстояние на дума* с дължина n над азбуката L *до код* се разбира най-малкото Хемингово разстояние на думата до кодова дума. *Минимално разстояние на кода* се нарича минималното разстояние между две различни кодови думи.

Радиусът на покритие на код е най-малкото цяло число R такова, че кълбата с радиус R, описани около кодовите думи, покриват цялото n-мерно векторно пространство над $GF(q)$. *Радиусът на сферичната опаковка* е максималната стойност на радиуса e на кълбата, описани около кодовите думи така, че тези кълба да нямат общи точки. Една сравнително проста долна граница за радиуса на покритие R е следната: $R \geq e$. Кодовете, които удовлетворяват тази граница с равенство, се наричат *съвършени*, а тези, за които радиусът на покритие надвишава с 1 радиуса на сферичната опаковка - *квази-съвършени*.

Функцията $t_q[n,k]$ се дефинира като минималния радиус на покритие на линейния код C, когато C се изменя в множеството от всички $[n,k]$ кодове над $GF(q)$ за фиксирани

n, k и q.

Когато искаме да изберем $[n, k, d]$ код за конкретно приложение, най-добрият избор ще бъде код с минимална вероятност за неоткрита грешка $P_{ue}(C, \varepsilon)$ (оптимален код) или с максимална вероятност за коректно декодиране $P_{corr}(C, \varepsilon)$. Ще казваме, че един код C е *t-подходящ* (или само подходящ, когато кодът се използва само за откриване на грешки), ако функцията $P_{ue}(C, \varepsilon)$ е монотонна в целия интервал $[0, \frac{q-1}{q}]$ [37].

Линейният $[n, k]$ код C се нарича *цикличен*, ако за всяка кодова дума $c = (c_0, c_1, \ldots, c_{n-1})$, която принадлежи на C, думата $c' = (c_{n-1}, c_0, \ldots, c_{n-2})$ също принадлежи на този код. Ако разгледаме кодовите думи от C чиито първи j информационни координати са 0 и изтрием тези координати от кодовите думи, ще получим $[n-j, k-j]$ код. Тези кодове наричаме *скъсени циклични* (CRC) кодове. CRC кодовете не са циклични кодове в общия случай, но имат поне същите възможности за контрол на грешки както и цикличния код, от който са получени.

Във втора глава са разгледани параметрите, определящи възможностите за откриване и коригиране на грешки, на линеен код.

Раздел 2.1 представя теоретични резултати, според които минималното разстояние d, радиусът на покритие R, тегловното разпределение на кода $\bar{A}$, на съседните му класове $\bar{\alpha}$ и на лидерите на съседни класове са параметрите определящи поведението на един линеен код при откриване и коригиране на грешки.

Раздел 2.2 е посветен на сложността на задачите за пресмятане на минимално разстояние, радиус на покритие и тегловно разпределение на код. Дефинирани са класовете на сложност P, NP, както и йерархията на задачите решавани за полиномно време. Показано е, че задачите за определяне на параметрите на кодовете, обект на изследване в дисертацията, са NP-трудни.

Методите за пресмятане на тегловно разпределение и на радиус на покритие на линеен код, използвани в дисертацията, са разгледани в раздел 2.3. Описани са и особеностите на програмната им реализация, която е направена на езика C++. Представените в този раздел методи са общи и работят за всякакви линейни кодове. Специфични алгоритми и техните програмни реализации, използвани за решаването на конкретни задачи, са описани в следващите глави, където се разглеждат и решените с тяхна помощ задачи.

В този раздел също са дадени алгоритми за ефективно пресмятане на тегловното разпределение (което включва и определянето на минималното разстояние) на q-ичен линеен код базирани на кода на Grey. За разлика от други алгоритми (виж [29, 42, 46, 49]), разработени за циклични кодове, тези могат да се използват за всеки линеен код без допълнителни изисквания към структурата му освен линейност. Те пресмятат цялото тегловно разпределение на кода, а не само първите няколко тегла, както е в [2]. Описани са и трите основни метода за пресмятане на радиус на покритие на код, използвани в

дисертацията. Те също се базират само на линейността на кодовете и не отчитат други специфични особености на структурата на кода. Описани са особеностите на техните компютърни имплементации и е пресметната сложността им по време и памет. Първият и вторият от тези методи могат да се използват и за пресмятане на тегловното разпределение на лидерите на съседни класове и на теглата на векторите в самите съседни класове.

В края на раздела са коментирани начините за проверка на коректността на получените, с разработените в дисертацията програмни средства, резултати.

В трета глава са определени радиусите на покритие на някои класове линейни кодове.

В раздел 3.1 са пресметнати радиусите на покритие на всички троични негациклични кодове с четни дължини до 26. Направена е класификация на тези кодове като са използвани някои техни алгебрични свойства и специално разработен за това софтуер. За 22 от кодовете са използвани различни математически съображения, за да бъдат определени радиусите им на покритие, а за останалите - компютърни пресмятания. Резултатите са представени в Таблица 3.1.1 в приложението. Пресметнати са и минималните разстояния и тегловните разпределения на тези кодове. Получените резултати водят до затваряне на 7 от отворените случаи за стойностите на функцията $t_3[n,k]$, а за други три са подобрени горните граници.

Твърдение 3.1.1.

1) $t_3[20,6] = 7-8$.

2) $t_3[20,10] = t_3[20,11] = t_3[21,11] = 4$.

3) $t_3[24,12] = t_3[25,13] = 5$.

4) $t_3[21,10] = t_3[22,11] = 5$

5) $t_3[22,10] = 5-6$.

6) $t_3[25,12] = 5-6$.

Резултатите от този раздел са получени самостоятелно, публикувани са в [53] и са представени на International Symposium on Infromation Theory в Соренто, Италия през 2000 г.

В раздел 3.2 е направено систематично изследване на възможните параметри на двоични и троични квази-съвършени кодове с малки размерности. Първо е представен списък от безкрайни фамилии от квази-съвършени кодове, който включва всички известни двоични, троични и четвъртични кодове. След това са дадени известните ни спорадични примери на двоични и троични квази-съвършени кодове. В резултат на нашето изследване (Таблица 3.2.5 от дисертацията) са класифицирани всички двоични квази-съвършени кодове с размерности до 9 и всички троични с размерности до 6. Получени са и частични класификации за кодове с размерности до 14.

Кодовете, получени в Таблица 3.2.5, водят до следните вериги от параметри на квази-съвършени кодове, като тези, които не са получени в настоящата класификация, са дадени в болд.

$[5,2,3]_2 2 \to [6,3,3]_2 2$;
$[8,4,4]_2 2 \to \ldots \to [14,10,3]_2 2$;
$[9,4,4]_2 2 \to \ldots \to [30,25,3]_2 2$;
$[13,7,4]_2 2 \to \ldots \to [\mathbf{18},\mathbf{12},\mathbf{3}]_{\mathbf{2}}\mathbf{2} \to [19,13,3]_2 2 \to [\mathbf{20},\mathbf{14},\mathbf{3}]_{\mathbf{2}}\mathbf{2} \to \ldots \to [\mathbf{62},\mathbf{56},\mathbf{3}]_{\mathbf{2}}\mathbf{2}$;
$[5,2,3]_3 2 \to [12,3,3]_3 2$;
$[8,4,4]_3 2 \to \ldots \to [17,13,3]_3 2 \to [\mathbf{18},\mathbf{14},\mathbf{3}]_{\mathbf{3}}\mathbf{2} \to \ldots \to [\mathbf{40},\mathbf{36},\mathbf{3}]_{\mathbf{3}}\mathbf{2}$;
$[12,7,3]_3 2 \to [\mathbf{13},\mathbf{8},\mathbf{3}]_{\mathbf{3}}\mathbf{2} \to \ldots \to [\mathbf{121},\mathbf{116},\mathbf{3}]_{\mathbf{3}}\mathbf{2}$.

До нашата работа, единствените известни примери на квази-съвършени кодове с минимално разстояние по-голямо 5 бяха двоичните кодове с повторение, $[22,12,6]_2 3$ съкратеният код на Golay, $[7,1,7]_3 4$ и $[8,1,8]_2 4$ кодовете, класифицирани в [17]. Ние даваме примери на още такива кодове и по този начин отговаряме на отворения проблем поставен в статията на Etzion и Mounits [20], където се предлага да се намерят нови или да се докаже несъществуването на квази-съвършени кодове с $d > 5$. Най-интересни са $[24,12,7]_2 4$ и $[25,12,8]_2 4$ кодовете, които са първите примери на квази-съвършени кодове с $R = 4$ извън $[24,12,8]_2 4$ разширения код на Golay, $[7,1,7]_3 4$ и $[8,1,8]_2 4$ кодовете с повторение.

Получените резултати показват, че за всяка размерност има само няколко възможни дължини, за които съществуват квази-съвършени кодове. За някои параметри са намерени стотици и дори хиляди квази-съвършени кодове, което показва, че условието радиусът на покритие да превишава с едно радиуса на сферичната опаковка не е толкова рестриктивна характеристика на кода. Изследването поставя и два отворени въпроса свързани със съществуването на други квази-съвършени кодове с минимално разстояние по-голямо от 8, освен двоичните кодове с повторение, и за горна граница за минималното разстояние на квази-съвършен код.

Резултатите от този раздел са съвместни с Илия Буюклиев, Стефан Додунеков и Veerle Fack и са публикувани в [65]. Представени са на International Workshop on Optimal Codes and Related Topics във Бялата Лагуна, България, през 2007 година и на лекция на семинара на групата CAAGT от университета в Гент, Белгия.

Следващите три раздела на тази глава са посветени на определяне на стойности на функцията $t_2[n,k]$.

В раздел 3.3 е използвана класификация на кодове със зададени параметри, за да се докаже несъществуването им. Първо са определени възможните стойности на дуалното

разстояние на кодовете, които ще се класифицират. След това е използвано компютърно търсене за кодове с фиксирани дължина, размерност, радиус на покритие и минимално разстояние на дуалния код. Това е направено за кодове с параметри отговарящи на първите 6 отворени случая за стойности на $t_2[n,k]$ и радиус на покритие равен на долната граница за тези стойности. Оказа се, че кодове с търсените параметри не съществуват и тъй като горната и долната граница за $t_2[n,k]$ в тези случаи се различават само с 1 бяха определени стойностите на $t_2[17,6]=5$, $t_2[17,8]=4$, $t_2[18,7]=5$, $t_2[19,7]=5$, $t_2[20,8]=5$ и $t_2[21,7]=6$. Като следствие бяха определени и 4 нови стойности на функцията $l(m,R)$ - минималната дължина на код с размерност m и радиус на покритие R.

Следствие 3.3.9.

$l(9,3)=18$, $l(11,4)=19$, $21 \leq l(12,4) \leq 23$ *и* $22 \leq l(14,5) \leq 24$.

Паказано е също така, че съществува единствен $[14,6]$ код с минимален радиус на покритие 3.

Резултатите от този раздел са получени съвместно с Веселин Ваврек и са публикувани в [56]. Представени са на EuroWorkshop on Optimal Codes and Related Topics в Слънчев бряг, България през 2001 г.

В раздел 3.4 са определени минималните радиуси на покритие на всички двоични линейни кодове с размерност 6.

Теорема 3.4.1.

$$t_2[n,6]=\left\lfloor \frac{n-8}{2} \right\rfloor, \ \textit{за } n \geq 18.$$

Стойностите на функцията за дължини по-малки от 18 бяха известни от Таблица 7.1 [11]. Класифицирани са също всички двоични кодове с размерност до 6 и дължина до 15 имащи минимален радиус на покритие. На основата на тази класификация е предложена конструкция позволяваща да се определи пораждаща матрица за всеки код с размерност до 6 и минимален радиус на покритие. Показани са и примери за конструиране на кодове с минимален радиус на покритие и размерности по-големи от 6.

Резултатите в този раздел са съвместни с Илия Буюклиев и са публикувани в [68]. Представени са на International Workshop on Algebraic and Combinatorial Coding Theory в Пампорово, България през 2008 и на семинар на групата CAAGT в университета в Гент, Белгия през същата година.

В раздел 3.5 са изследвани троичните линейни кодове с размерност 4. Направена е класификация на всички троични линейни кодове с размерност 4 и на базата на тази класификация са определени следните неизвестни стойности на функцията $t_3[n,4]$:

$t_3[13,4]=t_3[14,4]=6$, $t_3[15,4]=7$, $t_3[16,4]=t_3[17,4]=8$, $t_3[18,4]=t_3[19,4]=9$, $t_3[20,4]=10$, $t_3[21,4]=t_3[22,4]=11$, $t_3[23,4]=12$ и $t_3[25,4]=13$.

Уточнени са още следните 9 стойности на $t_3[n,k]$:
1 - $t_3[16,8] \leq t_3[8,4] + t[8,4] = 4 \Rightarrow t_3[16,8] = 4$,
2 - $t[18,8] \leq t[14,7] + t[4,1] = 5 \Rightarrow t_3[18,8] = 5$,
3 - $t_3[24,11] \leq t_3[20,10] + t_3[4,1] = 6 \Rightarrow t_3[24,11] = 6$,
4 - $t_3[28,14] \leq t_3[24,12] + t_3[4,2] = 6 \Rightarrow t_3[28,14] = 6$,
5 - $t_3[31,16] \leq t_3[20,10] + t[11,6] = 6 \Rightarrow t_3[31,16] = 6$,
6 - $t_3[33,20] \leq t_3[20,10] + t_3[13,10] = 5 \Rightarrow t_3[33,20] = 5$,
7 - $t_3[34,17] \leq t_3[20,10] + t_3[14,7] = 7 \Rightarrow t_3[34,17] = 7$,
8 - $t_3[36,18] \leq t_3[34,17] + t_3[2,1] = 7 \Rightarrow t_3[36,18] = 7$,
9 - $t_3[40,20] \leq t_3[20,10] + t_3[20,10] = 8 \Rightarrow t_3[40,20] = 8$.

Резултатите в този раздел са съвместни с Илия Буюклиев и са публикувани в [57]. Представени са на International Workshop on Algebraic and Combinatorial Coding Theory в Кранево, България през 2004.

В четвърта глава е изследвано поведението на шумозащитни кодове при откриване и коригиране на грешки.

В раздел 4.1 са пресметнати тегловните разпределения на кодовите думи, на съседните класове и на лидерите на съседни класове на двоичните циклични кодове с дължини до 33, на троичните циклични и негациклични кодове с дължини до 20 и на някои двоични линейни кодове с дължини до 33, имащи максимално минимално разстояние. С програма, написана на Maple, е проверена монотонността на функцията $P_{ue}(C,\varepsilon)$ за краен брой точки от интервала $\varepsilon \in [0, \frac{q-1}{q}]$, като по този начин са определени кодовете, които не са подходящи за контрол на грешки. Резултатите са представени в Таблици 4.1.1 - 4.1.4 в приложението на дисертацията.

Резултатите в този раздел са получени самостоятелно и са публикувани в [63]. Част от резултатите са представени на International Workshop on Algebraic and Combinatorial Coding Theory в Банско, България [51].

Цикличните кодове са важен клас на линейните кодове. Те са интересни от теоретична гледна точка заради богатата си алгебрична структура. Изследванията на тази структура са довели до разработването на методи за конструиране на такива кодове с голямо минимално разстояние каквито са БЧХ кодовете и квадратично-остатъчните кодове, както и на ефективни методи за декодиране какъвто е Meggit декодера. В раздел 4.2 е предложен метод за пресмятане на тегловното разпределение на съседните класове на циклични кодове като е използвана алгебричната им структура. Като илюстрация на метода са пресметнати тегловните разпределения на лидерите на съседни класове на всички троични циклични кодове с дължини до 14.

Резултатите в този раздел са получени съвместно с Евгения Великова и са публи-

кувани в [60].

В раздел 4.3 е разгледан троичният квадратично-остатъчен $[13, 7, 5]$ код и е пресметнато, че радиусът му на покритие е 3, т.е. кодът е квази-съвършен. Показано е, че кодът е *подходящ* за откриване и коригиране на грешки.

Алгебричен декодиращ алгоритъм за троичния $[13, 7, 5]$ квадратично-остатъчен код е представен в [31]. Като използваме допълнителна информация за структурата на кода, ние предлагаме два нови декодиращи алгоритъма за този код, които са с по-малка сложност в сравнение с представения в [31] алгоритъм. Първото предложение се основава на факта, че кодът C е БЧХ код. Вторият подход използва друго важно свойство на C. Корени на полинома $g(x)$ са α и α^{-1} едновременно, т.е. C е реверсивен. Ще отбележим, че вторият предложен алгоритъм за декодиране е особено ефективен, защото намирането на позициите на грешките и декодирането използват таблица само с 12 елемента от GF(27).

Резултатите в този раздел са получени съвместно със Стефан Додунеков и Ralf Kötter и са публикувани в [54]. Представени са на International Workshop on Algebraic and Combinatorial Coding Theory в Псков, Русия

На базата на богата гама от прости примери, в раздел 4.4 са демонстрирани интересни факти, които са полезни при решаването на практически проблеми в съвременните комуникации. Показано е, че кодове с еднакви основни параметри като дължина, размерност, минимално разстояние и радиус на покритие могат да имат различно поведение при контрол на грешки.

В края на раздела е представен един интересен пример, който дава решение на изследователския проблем 5.1, поставен в книгата на MacWilliams и Sloane [39] (Глава 5, стр. 132). Проблемът е следния.

Нека C да е линеен код. Нека α_i да е броят на лидерите на съседни класове на C с тегло i и α'_i да е съответният брой за дуалния му код $C^{\perp}$. До каква степен числата $\{\alpha_i\}$ определят $\{\alpha'_i\}$?

Оказа се, че тегловното разпределение на лидерите на съседни класове на кода не определя това на дуалния му код. В таблица 4.4.5 са представени тегловните разпределения на лидерите на съседни класове на дуалните на $[15, 3, 7]$ кодовете. Това са $[15, 12]$ кодове. Вижда се, че $[15, 3, 7]$ кодовете с номера 1,2 и 16 имат еднакви спектри на лидерите на съседните им класове, но техните дуални - не. По-точно дуалните кодове на кодовете с номера 1 и 2 имат еднакви спектри, но код номер 16 има различен. Това е вярно също и за кодовете с номера 3,6,7,9,11 и 12,13,15.

Таблица 4.4.5. Тегловни разпределения на лидерите на съседни класове на $[15, 12]$ кодовете

№	α_0	α_1	α_2	№	α_0	α_1	α_2	№	α_0	α_1	α_2	№	α_0	α_1	α_2
1	1	6	1	6	1	7		11	1	7		16	1	5	2
2	1	6	1	7	1	7		12	1	6	1	17	1	4	3
3	1	6	1	8	1	6	1	13	1	7					
4	1	6	1	9	1	7		14	1	7					
5	1	6	1	10	1	6	1	15	1	7					

Резултатите в този раздел са съвместни с Илия Буюклиев, Стефан Доддунеков и Wolfgang Williems и са публикувани в [59]. Представени са на Internationa Congress MASSEE в Боровец през 2003 г.

В пета глава се разглежда поведението при откриване и коригиране на грешки на CRC кодове.

В раздел 5.1 е направен обзор на поведението при откриване на грешки на стандартизирани CRC кодове. Представени са известните методи за пресмятане на тегловните разпределения на CRC кодовете. Сравнени са стандартизирани CRC кодове и е показано, че някои от тях са лош избор за почти всички дължини. Такъв пример е DARK, който е оптимален за дължина 8, но за дължини по-големи от 10 има вероятност за неоткрита грешка значително по-голяма от оптималната. Дори за дължините, за които е стандартизиран този код, той има поведение много по-лошо от други CRC кодове.

Резултатите от този раздел са съвместни с Faiza Sallam и са публикувани в [61, 62, 64]. Представени са на семинара "Математика, Информатика и Компютърни Науки"във Велико Търново, България, 2006 г. и на International Workshop on Algebraic and Combinatorial Coding Theory в Звенигород, Русия, 2006 г.

В раздел 5.2 са разгледани полиноми от 8-ма степен над GF(2), които са подходящи за пораждащи полиноми на CRC кодове. Техните минимални разстояния, вероятността за неоткрита грешка и свойството да са *подходящи* са сравнени с кода използван в ATM стандарта. Пресметнати са радиусите им на покритие и тегловното разпределение на лидерите на съседните им класове. Намерени са два по-добри от ATM стандарта кодове за дължина 40, на която стандартизирания код се използва.

• За вероятност за грешка на канала $\varepsilon \in [0, 0.022266]$, най-добър е кодът C_2 породен от полинома $g_2(x) = x^8 + x^5 + x^3 + x^2 + x + 1$.

• За вероятност за грешка на канала $\varepsilon \in [0.022266, 0.5]$, най-добър е кодът C_1 породен от полинома $g_1(x) = x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$.

При стойности на вероятността за неоткрита грешка между 0.019331 и 0.2, поведението на C_1 е с до 18% по-добро от това на ATM кода, като максимумът се достига при $\varepsilon = 0.048$. Поведението на кодът C_2 е с до 5% по-добро от това на ATM кода и има същото минимално разстояние $d = 4$ и радиус на покритие $R = 3$ като него. C_1 има с

едно по-малко минимално разстояние $d = 3$ от тях и затова има значително по лошото поведение (до -25% за $\varepsilon = 0.01$) в сравнение с ATM кода за по-слабо зашумени канали.

Протоколът, с който работи ATM стандарта, включва режим на работа само за откриване на грешки, когато каналът е зашумен и за откриване и коригиране на единична грешка (минималното му разстояние е 4), когато не е. ATM кодът има радиус на покритие 3 и такъв или с едно по-малък имат всички останали изследвани кодове. Сравнение беше направено и по отношение на поведението спрямо вероятността за коректно предаване на всички изследвани кодове на дължина 40. За няколко кода беше получена най-ниска стойност на тази вероятност. Кодът C_1 е измежду тях, но разликите в стойностите на тази функция за всички изследвани кодове са твърде незначителни и затова можем да приемем, че на тази дължина, всички кодове имат еднакво поведение по отношение на вероятността за коректно предаване.

Резултатите от този раздел са съвместни със Стефан Додунеков и Петър Казаков и са публикувани в [50].

CRC кодовете с пораждащ полином от 16 степен над GF(2), които могат да се използват за откриване на грешки в комуникационни системи, са изследвани в раздел 5.3. Направена е пълна класификация на всички такива кодове. Както и в изследването на кодовете от предишния раздел, са пресметнати минималните им разстояния, вероятността за неоткрита грешка и свойството да са *подходящи* за дължини от 18 до 1024. Направени са сравнения и са определени оптималните по отношение на вероятността за неоткрита грешка и минимално разстояние кодове за всяка от тези дължини и за седем фиксирани стойности на вероятността за грешка на канала $\varepsilon = 10^{-5}$, $\varepsilon = 10^{-4}$, $\varepsilon = 10^{-3}$, $\varepsilon = 10^{-2.5}$, $\varepsilon = 10^{-2}$, $\varepsilon = 10^{-1.5}$ и $\varepsilon = 10^{-1}$. Резултатите от изследването за вероятност за грешка на канала $\varepsilon = 10^{-3}$ са представени в таблица 5.3.1 в приложението на дисертацията.

Най-добрите полиноми за $\varepsilon = 10^{-5}$ съвпадат с тези от таблица 5.3.1 само с 5 изключения. Тези изключения са следните:

- за $n = 879 - 883$ най-добри са кодовете с пораждащ полином 10595;
- за $n = 720$ най-добър е кодът с пораждащ полином 1E667;
- за $n = 705$ и $n = 706$ най-добри са кодовете с пораждащ полином 1FC9F;
- за $n = 680$ и $n = 681$ най-добри са кодовете с пораждащ полином 19E91;
- за $n = 361$ и $n = 595$ най-добри са кодовете с пораждащ полином 1941F.

Резултатите от сравнението на най-добрите кодове със стандартизираните такива показва, че с много малки изключения, стандартизираните кодове имат поведение полошо от оптималното. Поведението на IEEE WG77.1 е близо да оптималното, с разлика до 5% от него, за дължини между $n = 181$ и $n = 255$. За дължини извън този интервал, поведението му е значително по-лошо. Кодовете, породени от стандартизирания полином

IEC TC57 на дължини от 94 до 128, имат стойности на вероятността за неоткрита грешка близка до оптималните (разлики от 1% до 5%) и достигат оптималната стойност на $P_{ue}(C, \varepsilon)$ на дължина $n = 19$. Поведението на останалите стандартизирани полиноми е незадоволително за всички изследвани дължини от $n = 18$ до $n = 1024$.

За слабо зашумени двоични симетрични канали, които много по-често генерират вектор-грешки с малко тегло отколкото с голямо, е удобно да се използват кодове с максимално минимално разстояние. Оказва се, че най-добрите кодове, посочени в таблица 5.3.1 и в допълнението към нея за $\varepsilon = 10^{-5}$, са най-добри и в това отношение, защото имат максималното възможно минимално разстояние измежду двоичните кодове с техните дължини и размерности. Има само едно изключение за кодът на дължина $n = 152$.

Резултатите от този раздел са съвместни със Стефан Додунеков и Петър Казаков и са публикувани в [52]. Предварителни резултати са представени на International Workshop on Algebraic and Combinatorial Coding Theory в Псков, Русия през 1998 г. и на семинар в университета в Улм, Германия.

В раздел 5.4 са продължени изследванията върху поведението на CRC кодове от предишните два раздела. В този раздел е направена пълна класификация на всички полиноми над GF(2) до 10-та степен, които могат да бъдат пораждащи полиноми на CRC кодове. Пресметнати са всички необходими данни за оценката на поведението за откриване и коригиране на грешки на тези кодове. Данните са на разположение на всички, за които биха представлявали интерес, на `http://www.moi.math.bas.bg/~tsonka`. Предложена е бърза и лесна процедура за избор на оптимален за конкретно приложение код. Стъпките на процедурата са следните.

1. Първото ограничение, което всяко приложение налага, е броят на проверочните символи, които трябва да бъдат добавени към данните, за да се осъществи контрола на грешките. Този брой определя степента p на полиномите, които трябва да бъдат разглеждани.

2. Измежду всички полиноми с фиксирана степен p избираме само тези от ред поголям или равен на максималната дължина n, на която кодът ще бъде използван. Ако редовете на всички полиноми са по-малки от n, избираме тези с максимален ред.

3. От множеството полиноми, формирано на предишната стъпка, разглеждаме само тези, чието минимално разстояние е максимално. Ако има твърде много такива полиноми, избираме само тези, които имат най-малък брой кодови думи с минимално тегло.

4. Пресмятаме и сравняваме стойностите на $P_{ue}(C, \varepsilon)$ за избраните кодове за конкретната вероятност за грешка на канала ε, при която ще работи кода, и избираме този с най-малка стойност на $P_{ue}(C, \varepsilon)$. В допълнение, ако кодът ще бъде използван и за коригиране на грешки, сравняваме и вероятностите им за коректно предаване P_{corr} и избираме този с най-голяма стойност на тази вероятност.

Разгледани са също и кодове с дължини по-големи от реда на полинома n_c, тъй като в практиката се използват и такива кодове. Тези кодове са повторение на кода с дължина n_c. Изведена е формула за пресмятане на броя на кодовите им думи с минимално тегло, което за кодовете с повторение е 2.

Твърдение 5.4.4. *Нека $n = qn_c + r,\ 0 \leq r \leq n_c$. Броят на кодовите думи с тегло две се определя от равенството*

$$A_2 = \frac{q(n - n_c + r)}{2}.$$

Този брой е важен при оценката на вероятността за неоткрита грешка на кода.

Резултатите в този раздел са самостоятелни и са публикувани в [66].

В шеста глава са изследвани някои характеристики на шумозащитни кодове свързани с техните възможности за контрол на грешки.

Известно е, че за един линеен $[n, k, d]$ код C всички грешки с тегло $t \leq (d-1)/2$ са коригируеми по единствен начин. Съществуват обаче грешки с тегло по-голямо от t, които са също коригируеми по единствен начин. Това са случите когато съседните класове с тегла по-големи от t имат единствен лидер. Така възникват няколко важни въпроса. Кои са грешките, които са коригируеми по единствен начин? Колко са те за предварително зададено тегло? Какво е най-голямото тегло на грешка, която може да се коригира по единствен начин?

В [28] е въведен параметърът *Нютонов радиус на покритие* за двоичен линеен код като най-голямото тегло на коригируем по единствен начин вектор-грешка. Граници и точни стойности за Нютоновия радиус на някои класове линейни кодове са дадени в [23], [27] и [36]. По-късно тези граници са обобщени за линейни кодове над произволна азбука в [24].

В раздел 6.1 ние пресмятаме Нютоновите радиуси на покритие на всички двоични циклични кодове с дължини до 31, на двоични кодове с максимално минимално разстояние с дължини до 33 и на всички троични циклични и негациклични кодове с дължини до 22.

Предимство на това изследване е, че не само определяме точните стойности на Нютоновия радиус на покритие на разглежданите кодове, но посочваме и броя на единствените лидери за всички тегла на съседни класове между $t+1$ и $\nu(C)$. Пълните резултати от изследването могат да се намерят на http://www.math.bas.bg/∼tsonka/nutable.pdf.

Резултатите в този раздел са получени самостоятелно, представени са на International Workshop on Algebraic and Combinatorial Coding Theory в Царское село, Русия и са публикувани в сборника с доклади на конференцията [55].

Линейни кодове с неравномерна защита на символите са разгледани в раздел 6.2.

Концепцията за неравномерна защита на информационните символи в кодовата дума е въведена от Masnick и Wolf [41]. Те разглеждат неравномерна защита на един бит от кодовата дума и описват някои свойства, намират граници и дават примери на систематични кодове с неравномерна защита на символите. В работите [5, 6, 7, 18, 19, 26, 35, 38, 40, 41] са представени подходи за конструиране на пораждащите или проверочните матрици на кодове с неравномерна защита на символите.

В нашата работа, предлагаме алгоритъм за определяне на възможностите за неравномерна защита на символите на линеен код. С този алгоритъм са определени възможностите за неравномерна защита на всички троични циклични и негациклични кодове с дължини до 26, които имат минимално разстояние поне 3.

Резултатите в този раздел са съвместни с Ирина Ганчева и са публикувани в [58]. Представени са на International congress MASSEE в Боровец, България през 2003 г.

В раздел 6.3 е доказано, че всички двоични кодове с дължини 16, 17 и 18, или ко-размерност 10 са нормализирани.

В [33] е получен резултат за това кога двоичните линейни кодове с дължина 16 и ко-размерност 10 са нормализирани.

Теорема 6.3.7. *Всички двоични линейни кодове с дължина 16 са нормализирани евентуално с изключение на* $[16, 6, 5$ *или* $6]4$ *кодовете имащи като подкодове всички кодове от типа* $[15, 5, 5$ *или* $6]6$.

Теорема 6.3.8. *Всички кодове с ко-размерност 10 са нормализирани с евентуално изключение на кодовете*
(i) $[16, 6, 5$ *или* $6]4$
(ii) $[17 + j, 7 + j, 6]4$, $j = 0, 1, 2$
(iii) $[17 + j, 7 + j, 5]4$, $0 \leq j \leq 5$,
в които за всяка координата скъсения код има радиус на покритие 6.

Ние разширяваме този резултат за кодове с дължини 17 и 18.

Теорема 6.3.9. *(i) Всички двоични линейни кодове с дължина 17 са нормализирани евентуално с изключение на* $[17, 6, 5$ *или* $6]5$ *кодовете имащи като подкодове всички кодове от типа* $[16, 5, 5$ *или* $6]7$.

(ii) Всички двоични линейни кодове с дължина 18 са нормализирани евентуално с изключение на $[18, 6, d \geq 5]5$ *кодовете имащи като подкодове всички кодове от типа* $[17, 5, d \geq 5]7$ *и* $[18, 7, 5$ *или* $6]5$ *кодовете имащи като подкодове всички кодове от типа* $[17, 6, 5$ *или* $6]7$.

За да завършим доказателството, че кодовете от теореми 6.3.7, 6.3.8 и 6.3.9 са нормализирани, ние конструираме всички такива кодове и проверяваме дали са нормализирани. Броят на кодовете, които трябва да се тестват, за дължини 17 и 18 нараства много бързо. За да направим възможна класификацията, доказваме следния резултат.

Твърдение 6.3.11. *Нека B да е $[n,k,d]R$ код и нека да го разширим до $[n+1,k+1,d' \leq d]$ код B_1. Тогава $R(B_1) \leq R(B)$.*

Като се използва класификацията на изследваните от нас нормализирани кодове, можем да получим нови кодове с малък или минимален радиус на покритие, като приложим конструкцията смесена директна сума към тях. Например известно е от [11, Таблица 7.1], че $t_2[19,7] = t_2[20,7] = 5$ и $t_2[22,11] = t_2[23,11] = 4$. Смесената директна сума на класифицираните в тази работа нормализирани $[17,6]5$ и $[20,10]4$ кодове с четни норми (10 и 8 съответно) и нормализирания $[3,2]1$ код с норма 2 дава $[19,7]5$ и $[22,11]4$ кодове.

Резултатите в този раздел са получени самостоятелно, публикувани са в [69], представени са на International Workshop Optimal Codes and Related Topics във Варна, България и са публикувани в сборника с доклади на конференцията.

В седма глава са получени първите класификационни резултати за оптични ортогонални кодове с параметри, които са най-често използвани в практиката. Това са първите класификационни резултати за такива кодове, които представляват интерес както от изследователска гледна точка, така и заради практическото им приложение. Наличието на класификационните резултати позволява конструираните кодове да се използват директно за различни практически приложения, като основа на нови безкрайни фамилии от кодове, както и да се докаже несъществуването на кодове с определени параметри. Заради връзката им с други комбинаторни структури, получените резултати за ООС водят до получаване на нови резултати и за тези структури.

Да означим с Z_v пръстена от целите числа по модул v.

Дефиниция 7.1.1. *$(v,k,\lambda_a,\lambda_c)$ оптичен ортогонален код (OOC) е колекция $\mathcal{C} = \{C_1,\ldots,C_s\}$ от k-елементи подмножества (кодови думи) на Z_v, такива че всеки две различни транслации на кодова дума имат най-много λ_a общи елементи, а всеки две транслации на две различни кодови думи имат най-много λ_c общи елемента:*

$$|C_i \cap (C_i + t)| \leq \lambda_a, \quad 1 \leq i \leq s, \quad 1 \leq t \leq v-1 \tag{1}$$

$$|C_i \cap (C_j + t)| \leq \lambda_c, \quad 1 \leq i < j \leq s, \quad 0 \leq t \leq v-1. \tag{2}$$

Условието (1) се нарича *автокорелационно свойство*, а условието (2) - *кроскорелационно свойство*. *Размер* на кодът $\mathcal{C}$ наричаме броя s на кодовите му думи. Когато $\lambda_a = \lambda_c$, кодът се означава с (v,k,λ). *Оптимални* оптични ортогонални кодове са тези, които имат най-големия възможен брой кодови думи за фиксирани параметри.

Класификации на оптимални оптични ортогонални кодове с тегла 4 и 5, автокорелация 2 и крос-корелация 1 са направени в раздел 7.1.

Разнообразни конструкции на безкрайни фамилии от оптимални $(v,4,2,1)$ оптични

ортогонални кодове и някои резултати за несъществуване са представени в [8] и [43]. Все още обаче има много стойности на v, за които не е известно дали съществуват оптични ортогонални кодове. В нашата работа ние отговаряме на този въпрос за всички нерешени случаи за $v < 182$ и класифицираме с точност до изоморфизъм оптималните $(v, 4, 2, 1)$ оптични ортогонални кодове с $v < 76$, $v \neq 71$. Доказателствата в [8] показват, че за някои безкрайни фамилии е трудно теоретично да се покаже съществуването на оптични ортогонални кодове с малки параметри и в този случай компютърното търсене е по-ефективно (виж например [8], Теорема 4.6, Теорема 6.3). За конструирането на други безкрайни фамилии пък са нужни оптични ортогонални кодове с малки параметри и с допълнителни свойства и в този случай класификационните резултати могат също да са полезни. Например в забележката след Теорема 4.7 в [8] е показано, че полученият в теоремата резултат би могъл да бъде значително разширен, ако съществува $(88, 4, 2, 1)$ OOC, който има една кодова дума, чиито разлики са точно ненулевите елементи на подгрупата от ред 8 на Z_{88}. В нашата работа ние намираме такъв код. В този смисъл, получените от нас резултати за съществуване и направените класификации на оптични ортогонални кодове с малки дължини могат да допринесат за бъдещите изследвания на кодове с по-големи дължини.

Оптимални $(v, 5, 2, 1)$ оптични ортогонални кодове са разгледани в работата на Buratti, Pasotti и Wu [9]. В нея те показват, че за $(v, 5, 2, 1)$ оптични ортогонални кодове

$$s \leq \lceil v/12 \rceil \text{ ако } v \equiv 11 \ (mod\ 132) \text{ или } v \equiv 154 \ (mod\ 924) \tag{3}$$

$$s \leq \lfloor v/12 \rfloor \text{ в останалите случаи.} \tag{4}$$

Освен това, те предлагат конструкции на $(v, 5, 2, 1)$ оптични ортогонални кодове, достигащи тази граница, с кодови думи от типа $\{0, x, -x, y, -y\}$, няколко рекурсивни конструкции на такива кодове, както и отговарят на въпроса за съществуването им за $v \leq 62$. В нашето изследване решаваме задачата за съществуването на $(v, 5, 2, 1)$ оптични ортогонални кодове, достигащи границата от [9], за всички нерешени случаи за $v \leq 155$ и класифицираме тези с $v \leq 114$. За целта използваме алгоритъма за класификация на оптималните $(v, 4, 2, 1)$ оптични ортогонални кодове, като разработваме негова версия за пресмятане на паралелен компютър. Алгоритъмът е от типа търсене с връщане и може успешно да се имплементира на паралелен компютър с ускоряване близко до оптималното [34]. Така част от резултатите ни са получени като е използван българския суперкомпютър BlueGene.

Преди настоящата работа не бяха известни примери на достигащи границата от [9] $(v, 5, 2, 1)$ оптични ортогонални кодове за

- v се дели на 12 и $s > 1$

- $v \equiv 154$ (mod 924)
- 76 стойности на v за $63 \leq v \leq 155$, за които не е установено несъществуване.

В нашата работа

- Намерени са примери на достигащи границата от [9] оптични ортогонални кодове с v, което се дели на 12 за дължини 108, 120, 132 и 144.
- Установено е, че не съществува достигащ границата от [9] $(154, 5, 2, 1)$ оптичен ортогонален код. Проблемът за съществуването на достигащи границата от [9] оптични ортогонални кодове с $v \equiv 154$ (mod 924) остава отворен.
- Установено е несъществуването на достигащи границата от [9] оптични ортогонални кодове с $63 \leq v \leq 155$ за $v = 63$, 72, 84, 86, 96, 122 и 154. В останалите случаи са представени примери на достигащи границата от [9] оптични ортогонални кодове. Направена е и класификация за $v \leq 114$.

Получените в тази работа резултати за малки стойности на v могат да бъдат използвани и в рекурсивни конструкции. Ако рекурсивните конструкции от теореми 9.5, 9.6, 9.7, 9.8 и 9.9 от [9] се приложат към резултатите от директните конструкции от [9], следва че съществуват достигащи границата от [9] $(v, 5, 2, 1)$ оптични ортогонални кодове за 222 стойности на $v \leq 1000$, за 883 стойности на $v \leq 5000$ и за 1641 стойности на $v \leq 10000$. Ако се приложат същите рекурсивни конструкции към резултатите от [9] и към получените от нас резултати, следва че съществуват достигащи границата от [9] $(v, 5, 2, 1)$ оптични ортогонални кодове за 305 стойности на $v \leq 1000$, за 1067 стойности на $v \leq 5000$ и за 1964 стойности на $v \leq 10000$.

Един от най-интересните класове на константно-тегловните кодове е този на циклично-пермутационните константно-тегловни кодове. *Циклично - пермутационните кодове* са въведени от Gilbert [25] през 1963 година за използване при CDMA комуникациите. Това са двоични блокови кодове с дължина n, такива че всяка кодова дума има n различни циклични завъртания и нито една кодова дума не може да бъде получена като циклично завъртане на някоя друга кодова дума. *Циклично-пермутационните константно-тегловни* кодове са едновременно константно-тегловни и циклично-пермутационни. Тези кодове са изследвани в [4, 44, 45] и се използват за конструирането на последователности за комуникационни канали без обратна връзка, използвани едновременно от много потребители.

Оптични ортогонални кодове с определени параметри се наричат също циклично-пермутационни константно-тегловни (cyclically permutable constant weight, CPCW) кодове. В раздел 7.2 са класифицирани оптималните циклично-пермутационни константно-тегловни кодове с тегло на кодовите думи 3 и дължини до 61.

Да означим с Z_v пръстена на целите числа по модул v, а с $\oplus$ и $\odot$ събирането и умножението в него.

Двоичният (v, k, λ) циклично-пермутационен константно-тегловен (CPCW) код $\mathcal{C}$ е колекция от $\{0, 1\}$ последователности с дължина v и тегло по Хеминг k такъв, че:

$$\sum_{i=0}^{v-1} x(i)x(i \oplus j) \leq \lambda,\ 1 \leq j \leq v-1 \tag{5}$$

$$\sum_{i=0}^{v-1} x(i)y(i \oplus j) \leq \lambda,\ 0 \leq j \leq v-1 \tag{6}$$

за всички двойки различни последователности $x, y \in \mathcal{C}$. Същата дефиниция е валидна и за (v, k, λ) оптичен ортогонален код.

В [1] и [10] е показано, че циклично-пермутационни константно-тегловни кодове съществуват, тогава и само тогава когато $v \not\equiv 14$ или 20 $(mod\ 24)$. До нашата работа не бяха известни класификационни резултати за циклично-пермутационни константно-тегловни кодове, но имаше такива за Щайнерови системи от тройки от ред v с $v \leq 57$ [15]. По-точно за $v = 19, 21, 25, 27, 31, 33, 37, 39, 43, 45, 49, 51, 55,$ и 57. Измежду тях, дизайните с $v = 19, 25, 31, 37, 43, 49$ и 55 са еквивалентни на $(v, 3, 1)$ циклично-пермутационни константно-тегловни кодове, докато дизайните с $v = 121, 27, 33, 39, 45, 51$ и 57 имат по една къса орбита.

Ние класифицираме с точност до мултипликативна еквивалентност оптималните $(v, 3, 1)$ циклично-пермутационни константно-тегловни кодове с $v \leq 61$. По този начин към известните вече класификации на циклични $STS(v)$ добавяме и такава за $v = 61$ като същевременно повтаряме и резултатите за циклични $STS(v)$ за $v \leq 57$.

Връзката между съвършените оптични ортогонални кодове и цикличните разностни фамилии позволи получаването на класификационни резултати за циклични разностни фамилии с малки параметри, като се използва подход подобен на този от раздел 7.1. Резултатите са представени в раздел 7.3.

Класификацията на цикличните разностни множества представлява интерес както от изследователска гледна точка, така и заради приложението им при конструирането на други видове комбинаторни структури. Известни са техни приложения при еднофакторизация на пълни графи и при циклично разрешими циклични Щайнерови системи от тройки [21], както и за конструирането на регулярни LDPC кодове [22]. В [30] е представена ефективна конструкция на нови оптимални системи със съвършена сигурност на базата циклични разностни множества. Оптимални последователности за прескачане на честоти могат също да бъдат конструирани от $(v, k, 1)$ циклични разностни множества.

$(v, k, 1)$ циклично разностно множество може да бъде получено от всеки опти-

мален съвършен $(v, k, 1)$ циклично-пермутационен константно-тегловен код (оптимален съвършен $(v, k, 1)$ оптичен ортогонален код) и от всеки оптимален двоичен цикличен константно-тегловен код с тегло k и минимално разстояние $2(k-1)$. Има еднозначно съответствие между $(v, k, 1)$ цикличните разностни множества и цикличните 2-$(v, k, 1)$ дизайни.

До нашата работа бяха известни класификации за $k = 3$ и $v \leq 57$ [15], $k = 4$ и $v \leq 64$ [13], $k = 5$ и $v \leq 65$ [13], $k = 6$ и $v = 91$ [14], [32] и $k = 7$ и $v = 91$ [3]. Ние разширяваме тези резултати като към тях добавяме и класификациите за $k \leq 7$ на $(61, 3, 1)$, $(73, 4, 1)$, $(76, 4, 1)$, $(81, 5, 1)$ и $(85, 5, 1)$ цикличните разностни множества, както и правим първите класификации за $k \geq 7$.

Резултатите в тази глава са съвместни със Светлана Топалова и са публикувани в [70, 71, 72, 73, 74].

Класификационните резултати за различни класове кодове получени в настоящата работа са систематизирани и представени в таблици в приложенията към нея. Таблиците са отделени от основния текст, за да не се затруднява четенето му от една страна, и за да могат лесно да се правят справки за интересуващите читателя конкретни параметри, от друга.

Апробация на резултатите

В дисертацията са включени резултати получени в периода 1998 г. – 2013 г. Резултатите, представени в публикации [51, 53, 55, 63, 66, 67] и [69], са получени самостоятелно. Останалите резултати са получени в съавторство, както следва:

Додунеков, Kötter	[54]
Буюклиев	[57, 68]
Буюклиев, Додунеков, Williams	[59]
Великова	[60]
Буюклиев, Додунеков, Fack	[65]
Ваврек	[56]
Додунеков, Казаков	[50, 52]
Sallam	[61, 64, 62]
Ганчева	[58]
Топалова	[70, 71, 72, 73, 74]

Публикувани са в следните научни списания:

IEEE Trans. on Information Theory	[53], [54], [56], [65]
Advances in Mathematics of Communications	[68], [69]
Computer Communications	[50]
IEE Proc. Communications	[52]
IEEE Trans. on Communications	[66]
Journal of Combinatorial Designs	[70]
Applical Algebra in Eng., Communic. and Computing	[74]
Mathematics of Distances and Applications	[73]
Annuarie de L'Université de Sofia 'St. Kl. Ohridski'	[60]
Mathematica Balkanica	[58], [59], [64]
Serdica, Journal of Computing	[63]

Включените в дисертацията резултати са докладвани на:

Международна конференция *Algebraic and Combinatorial Coding Theory*, 1998 г., 2002 г., 2006 г., Русия и 2000 г., 2004 г., 2008 г., 2012 г., България;

Международна конференция *Optimal codes and Related Topics*, 1998 г., 2001 г., 2007 г., 2009 г., 2011 г., България;

IEEE International Symposium of Information Theory, 2000 г., Италия;

Конгрес на Математическата асоциация на Югоизточна Европа *MASSEE*, 2003 г., България, 2006 г., Кипър, 2009 г., Македония;

Юбилейна конференция на ВТУ *Mathematics, Informatics and Computer Sciences*, 2006 г., България;

Workshop on Combinatorial search, 2005 г., Унгария

NATO Advsnced Recearch Workshop *Enchancing cryptographic primitives with techniques from error correcting codes*, 2008 г., България;

Международна конференция *Applications of Computer Algebra*, 2006 и 2012 г., България;

Международна конференция *Mathematics in Industry*, 2010 г., България;

Международна конференция *Mathematics of Distances and Applications*, 2012 г., България;

Международна конференция *Mathematics Days in Sofia*, 2014 г., България.

Отделни резултати от дисертацията са докладвани пред:

Националния семинар по теория на кодирането;

Семинар на Великотърновски университет „Св. св. Кирил и Методий“ и секция МОИ;

Семинар в Технически университет в Улм, 2000 г., Германия;

Семинар в Института по математика на Унгарската Академия на науките 2004 г., 2005 г., 2008 г. Унгария;

Семинар в университета в Гент, 2006 г., 2008 г., 2010г., Белгия.

Авторска справка

По мнение на автора основните приноси на дисертанционния труд са:

- Определени са
  - Радиусите на покритие всички троични негациклични кодове с четни дължини до 26.
  - $t_2[17,6]=5, t_2[17,8]=4, t_2[18,7]=5, t_2[19,7]=5, t_2[20,8]=5$ и $t_2[21,7]=6$.
  - $t_3[20,10] = t_3[20,11] = t_3[21,11] = 4$, $t_3[24,12] = t_3[25,13] = 5$, $t_3[21,10] = t_3[22,11] = 5, t_3[16,8] = 4, t_3[18,8] = 5, t_3[24,11] = 6, t_3[28,14] = 6, t_3[31,16] = 6$, $t_3[33,20] = 5$, $t_3[34,17] = 7$, $t_3[36,18] = 7$, $t_3[40,20] = 8$.
  - Минималните радиуси на покритие на всички двоични линейни кодове с размерност 6.
  - Двоичните циклични кодове с дължини до 33, троичните циклични и негациклични кодове с дължини до 20 и някои двоични кодове с дължини до 33 и максимално минимално разстояние, които не са подходящи за контрол на грешки.
  - Нютоновите радиуси на покритие на всички двоични циклични кодове с дължини до 31, на двоични кодове с максимално минимално разстояние с дължини до 33 и на всички троични циклични и негацикличини кодове с дължини до 22.
  - Възможностите за неравномерна защита на символите на всички троични циклични и негациклични кодове с дължини до 26, които имат минимално разстояние поне 3.
- Класифицирани са
  - Двоичните квази-съвършени кодове с размерности до 9 и троичните квази-съвършени кодове с размерности до 6. Получени са частични класификации за двоични и троични квази-съвършени кодове с размерности до 14.
  - Всички двоични кодове с минимален радиус на покрите с размерност до 6 и дължина до 15.
  - Всички троични кодове с размерност до 4.
  - Скъсените цикличини кодове с до 10 и с 16 проверочни символа.
  - Оптималните $(v,4,2,1)$ оптични ортогонални кодове с $v \leq 75$, $v \neq 71$.
  - Оптималните $(v,5,2,1)$ оптични ортогонални кодове с $v \leq 114$.

  - $(v, k, 1)$ циклично-пермутационните константно-тегловни кодове с $v \leq 61$.
  - $(61, 3, 1)$, $(73, 4, 1)$, $(76, 4, 1)$, $(81, 5, 1)$ и $(85, 5, 1)$ цикличните разностни множества.

- Предложена е конструкция за определяне на пораждаща матрица на произволен двоичен код с размерност до 6 и минимален радиус на покритие.

- Доказано е, че всички двоични кодове с дължини 16, 17 и 18, или ко-размерност 10 са нормализирани.

- Предложена е ефективна процедура за избор на най-подходящия за съответното приложение скъсен цикличен код, която използва резултатите от класификацията на скъсените циклични кодове с до 10 и с 16 проверочни символа.

- Решен е поставен от Etzion и Mounits отворен въпрос като са намерени нови примери на квази-съвършени кодове с минимално разстояние по-голямо от 5.

- Решен е отворен проблем 5.1 (глава 5, стр. 132) поставен в книгата на MacWilliams and Sloane „The theory of Error-Correcting Codes“.

- Определени са оптималните по отношение на вероятността за неоткрита грешка и минимално разстояние скъсени циклични кодове с до 10 и с 16 проверочни символа. Някои от тях са намерили различни практически приложения в:

  - комуникационни системи за управление на жп транспорт и градски релсов транспорт в Италия (Ansaldo STS S.p.A.), Германия (Thales Rail Signalling Solutions GesmbH), Индия (Safety Critical Railway project);

  - телекомуникационни системи в Русия, Турция (UEKAE-TUBITAK);

  - затворени безжични системи разработвани в ТУ Берлин;

  - US патент 8341510 B2, 2012;

  - US патент 8327251 B2, 2012.

Л И Т Е Р А Т У Р А

[1] R. J. R. Abel and M. Buratti, Some progress on (v, 4, 1) difference families and optical orthogonal codes, *J. Combin. Theory* Ser. A, vol. 106 (2004) 59–75.

[2] A. M. Barg and I. I. Dummer, On computing the weight spectrum of cyclic codes, *IEEE Trans. Inform. Theory*, vol. 38 (1992) 1382–1386.

[3] V. N. Bhat-Nayak, V. D. Kane, W. L. Kocay, R. G. Stanton, Settling some BIBD conjectures, *Ars Combin.*, vol. 16 (1983) 229–234.

[4] S. Bitan and T. Etzion, Constructions for optimal constant weight cyclically permutable codes and difference families, *IEEE Trans. Inform. Theory*, vol. 41 (1995) 77–87.

[5] I. M. Boyarinov, On unequal error protection codes, *Proc. Fifth Conf. on Theory of Transmission and Coding of Inform.*, Moskow-Gorki, U.S.S.R., pt. II (1972) 22–24.

[6] I. M. Boyarinov and G. L. Katsman, On linear unequal error protection codes, *Proc. Seventh Nat. Symp. on Problems of Redundacy in Information System*, Leningrad, U.S.S.R., pt. I (1977) 66–70.

[7] I. M. Boyarinov and G. L. Katsman, Linear unequal error protection codes, *Voprosi Kibernetiki*, no. 34 (1977) 60–91.

[8] M. Buratti, K. Momihara, A. Pasotti, New results on optimal $(v, 4, 2, 1)$ optical orthogonal codes, *Designs, Codes and Cryptography*, vol. 58 (2011) 89—109.

[9] M. Buratti, A. Pasotti, D. Wu, On optimal $(v, 5, 2, 1)$ optical orthogonal codes, *Designs, Codes and Cryptography*, vol. 68, issue 1-3 (2013) 349–371.

[10] F. R. K. Chung , J. A. Salehi , V. K. Wei, Optical orthogonal codes: design, analysis and applications, *IEEE Trans. Inform. Theory*, vol. 35 (1989) 595–604.

[11] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North- Holland, Elsevier Science B.V. (1997).

[12] G. D. Cohen, S. N. Litsyn, A. C. Lobstein and H. F. Mattson, Jr., Covering radius 1985-1994, *AAECC* (Springer), vol. 8 (1997) 173–239.

[13] M. J. Colbourn, R. A. Mathon, On cyclic Steiner 2-designs, *Ann. Discrete Math.*, vol. 7 (1980) 215–253.

[14] C. J. Colbourn, On cyclic Steiner systems S(2,6,91), *Abstracts Amer. Math. Soc.*, vol. 2 (1981).

[15] C. J. Colbourn and A. Rosa, *Triple systems*, Oxford University Press, Oxford (1999).

[16] C. J. Colbourn , J. H. Dinitz , D. R. Stinson , Applications of combinatorial designs to communications, cryptography, and networking, *Surveys in combinatorics*, J. D. Lamb, D. A. Preece (eds.), Cambridge University Press, London (1999) 37–100.

[17] A. A. Davydov, G. Faina, S. Marcugini, and F. Pambianco, Locally optimal (non-shortening) linear covering codes and minimal saturating sets in projective spaces, *IEEE Trans. Inf. Theory*, vol. 51, No. 12 (2005) 4378–4387.

[18] L. A. Dunning and W. E. Robbins, Optimal encodings of linear block codes for unequal error protection, *Inform. Contr.*, vol. 37 (1978) 150–177.

[19] V. N. Dynkin and V. A. Togonidze, Cyclic codes with unequal protection of symbols, *Probl. Peredach. Inform.*, vol. 12, no. 1 (1976) 24–28.

[20] T. Etzion and B. Mounits, Quasi-perfect codes with small distance, *IEEE Trans. Inf. Theory*, vol. 51, No 11 (2005) 3938–3946.

[21] R. Fuji-Hara, Y. Miao and S. Shinohara, Complete Sets of Disjoint Difference Families and their Applications, *Journal of Statistical Planning and Inference*, vol. 106, 1 August (2002) 87–103.

[22] M. Fujisawa, S. Sakata, A class of quasi-cyclic regular LDPC codes from cyclic difference families with girth 8, *Proceedings International Symposium on Information Theory*, 4-9 Sept. (2005) 2290–2294.

[23] E. Gabidulin and T. Kløve, On the Newton radius, *Reports in Informatics* (Dept. Informatics, Univ. Bergen, Bergen, Norway), no. 130, Feb. (1997).

[24] E. Gabidulin and T. Kløve, On the Newton and covering radii of linear codes, *IEEE Trans. on Inform. Theory*, vol. 45, No. 7 (1999) 2534–2536.

[25] E. N. Gilbert, Cyclically permutable error-correcting codes, *IEEE Trans. Inform. Theory*, vol. 9 (1963) 175–180.

[26] W. J. van Gils, Two topics on linear unequal error protection codes: Bounds on their length and cyclic code classes, *IEEE Trans. Inform. Theory*, vol. 29, no. 6, Nov. (1983) 866–876.

[27] T. Helleseth and T. Kløve, The Newton radius of codes, *IEEE Trans. on Inform. Theory*, vol. 43, No. 6 (1997) 1820–1831.

[28] T. Helleseth, T. Kløve and V. Levenshtein, The Newton radius of equidistant codes, *Proc. IEEE Intern. Symp. on Inform. Theory and its Applications*, Victoria, B.C., Canada, Sept. 17-30 (1996) 721–722.

[29] T. Helleseth, T. Kløve and J. Mykkeltveit, The weight distribution of irreducible cyclic codes, *Discrete Mathematics*, vol. 18 (1977) 179–211.

[30] M. Huber, Perfect Secrecy Systems Immune to Spoofing Attacks, *International Journal of Information Security*, vol. 11, Issue 4 (2012) 281–289.

[31] J. F. Humphreys, Algebraic decoding of the ternary $[13, 7, 5]$ quadratic- residue code, *IEEE Trans. Inform. Theory*, vol. 38, No. 3 (1992) 1122– 1125.

[32] Z. Janko, V. D. Tonchev, Cyclic 2-(91, 6, 1) designs with multiplier automorphisms, *Discrete Mathematics*, vol. 97 (1991) 265–268.

[33] H. Janwa and H. F. Mattson, Jr., Some upper bounds on the covering radii of linear codes over F_q and their applications, *Designs, Codes and Cryptography*, vol. 18 (1999) 163–181.

[34] R. M. Karp and Y. Zhang, Randomized parallel algorithms for backtrack search and branch-and-bound computation, *Journal Assoc. Comput. Mach. (USA)* vol. 40, (3) (1993) 765-789.

[35] C. C. Kilgus and W. C. Gore, A class of cyclic unequal-error-protection codes, *IEEE Trans. Inform. Theory*, vol. 18, Sept. (1972) 687–690.

[36] T. Kløve, Relations between the covering and Newton radii of binary codes, *Discrete Mathematics*, vol. 238 (2001) 81–88.

[37] T.Kløve, V. Korzhik. *Error Detecting Codes*, Kluwer Academic Publishers, Boston (1995).

[38] M. C. Lin and S. Lin. Cyclic unequal error protection codes constructed from cyclic codes of composite length, *IEEE Trans. Inform. Theory*, vol. 34, no. 4, July (1988) 867–871.

[39] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting codes*, North-Holland Publishing Company, Amsterdam, London, New York, Tokyo, Ninth impression (1996).

[40] D. Mandelbaum, Unequal-error-protection codes derived from difference sets, *IEEE Trans. Inform. Theory*, vol. 18, Sept. (1972) 686–687.

[41] B. Masnik and J. Wolf, On linear unequal error protection codes, *IEEE Trans. Inform. Theory*, vol. 13, Oct. (1967) 600–607.

[42] R. J. McEliece and H. Rumsey, Euler products, cyclotomy, and coding, *J. Number Theory*, vol. 4 (1972) 302–311.

[43] K. Momihara, M. Buratti, Bounds and Constructions of Optimal (n, 4, 2, 1) Optical Orthogonal Codes, *IEEE Trans. on Inform. Theory*, vol. 55 (2009) 514–523.

[44] O. Moreno, Z. Zhang, P. V. Kumar and V. A. Zinoviev, New constructions of optimal cyclically permutable constant weight codes, *IEEE Trans. on Inform. Theory*, vol. 41 (1995) 448–455.

[45] Q. A. Nguyen, L. Györfy and J. L. Massey, Construction of binary constant-weight cyclic codes and cyclically permutable codes, *IEEE Trans. on Inform. Theory*, vol. 38 (1992) 940–949.

[46] R. Segal and R. Ward, Weight distributiona of some irreducible cyclic codes, *Mathematics of Computation*, vol. 46 (1986) 341–354.

[47] C. E. Shannon, A mathematical theory of communication, *Bell Syst. Tech. J.*, vol. 27 (1948) 379–423 and 623–656.

[48] F. I. Solov'eva, Designs and Perfect Codes, General Theory of Information Transfer and Combinatorics *Lecture Notes in Computer Science*, vol. 4123 (2006) 1104–1105.

[49] R. Ward, Weight enumerators of more irreducible cyclic binary codes, *IEEE Trans. Infom. Theory*, vol. 39 (1993) 1701–1709.

Публикации по дисертацията

[50] T. Baicheva, S. Dodunekov and P. Kazakov, On the cyclic redundancy-check codes with 8-bit redundancy, *Computer Communications*, vol. 21 (1998) 1030–1033.

[51] T. Baicheva, Binary and ternary linear codes which are good and proper for error correction, *Proc of the International Workshop on Algebraic and Combinatorial Coding Theory*, Bansko, Bulgaria (2000) 55–60.

[52] T. Baicheva, S. Dodunekov and P. Kazakov, On the Undetected Error Probability Performance of Cyclic Redundancy-Check Codes of 16-bit Redundancy, *IEE Proc. Communications*, vol. 147, No. 5 (2000) 253 –256.
T. Baicheva, S. Dodunekov and P. Kazakov, On the cyclic redundancy-check codes with 16-bit redundancy, *Proc. of the International Workshop on Algebraic and Combinatorial Coding Theory*, Pskov, Russia (1998) 17–21.

[53] T. Baicheva, On the covering radius of ternary negacyclic codes with length up to 26, *IEEE Trans. on Inform. Theory*, vol. 47, No. 1 (2001) 413–416.
T. Baicheva, On the covering radius of ternary negacyclic codes with length up to 26, *Proc of IEEE Intern. Symposium of Inform. Theory*, Sorento, Italy (2000) p. 392.

[54] T. Baicheva, S. Dodunekov and R. Kötter, On the Performance of the Ternary [13,7,5] Quadratic-Residue Codes, *IEEE Trans. Inform. Theory*, vol. 48, No. 2 (2002) 562–564.
T. Baicheva, S. Dodunekov and R. Kötter, On the Performance of the Ternary [13,7,5] Quadratic-Residue Codes, *Proc of the International Workshop on Algebraic and Combinatorial Coding Theory*, Pskov, Russia (1998) 93–97.

[55] T. Baicheva, The Newton radius of some binary and ternary cyclic codes, *Proc of the International Workshop on Algebraic and Combinatorial Coding Theory*, Tsarskoe Selo, Russia (2002) 18–21.

[56] T. Baicheva and V. Varek, On the least covering radius of binary linear codes with small lengths, *IEEE Trans. On Inform. Theory*, vol. 49, No. 3 (2003) 738–740.
T. Baicheva and V. Varek, On the least covering radius of binary linear codes with small lengths, *Proc. of the EuroWorkshop on Optimal Codes and related topics*, Sunny Beach, Bulgaria (2001) 13–18.

[57] T. Baicheva and I. Boyukliev, On the ternary projective codes with dimensions 4 and 5, *Proc of the International Workshop on Algebraic and Combinatorial Coding Theory*, Kranevo, Bulgaria (2004) 34–39.

[58] T. Baicheva and I. Gancheva, Computer search for ternary cyclic and negacyclic LUEP codes of lengths up to 26, *Mathematica Balkanica*, New Series vol. 18 (2004) 79–80.

[59] T. Baicheva, I. Boyukliev, S. Dodunekov and W. Willems, Teaching linear codes, *Mathematica Balkanica*, New Series vol. 19 (2005) 3–16.

[60] E. Velikova and T. Baicheva, On the computation of the weight distribution of the cosets of cyclic codes, *Annuarie de L'Université de Sofia 'St. Kl. Ohridski'*, vol. 97 (2005) 109–114.

[61] T. Baicheva and F. Sallam, On the error detection performance of some CRC codes, *Proc. of the workshop 'Mathematics, Informatics and Computer Sciences'*, Veliko Tarnovo, Bulgaria (2006) 107–110.

[62] T. Baicheva and F. Sallam, Error control performance of CRC codes with up to 8 bit redundancy, *Proc. of the International Workshop on Algebraic and Combinatorial Coding Theory*, Zvenigorod, Russia (2006) 11–14.

[63] T. Baicheva, On the error correcting performance of some binary and ternary linear codes, *Serdica, Journal of Computing*, vol. 1 (2007) 157–170.

[64] T. Baicheva and F. Salam, CRC codes for error control, *Mathematica Balkanica*, New series vol. 21, Fasc. 3-4 (2007) 377–388.

[65] T. Baicheva, I. Bouyukliev, S. Dodunekov, and V. Fack, Binary and Ternary Quasi-perfect Codes with Small Dimensions, *IEEE Trans. on Inform. Theory*, vol. 54, issue 9 (2008) 4335–4339.
T. Baicheva, I. Bouyukliev, Stefan Dodunekov and V. Fack, Binary and ternary quasi-perfect codes with small dimensions, *Proc. of the International Workshop Optimal Codes and Related Topics*, White Lagoon, Bulgaria (2007) 13–18.

[66] T. Baicheva, Determination of the best CRC codes with up to 10-bit redundancy, *IEEE Trans on Communic.*, vol. 56, issue 8 (2008) 1214 –1220.

[67] T. Baicheva, Linear codes of good error control performance, *Enchancing cryptographic primitives with techniques from error correcting codes*, IOS Press (2009) 250–259.

[68] T. Baicheva and I. Bouyukliev, On the least covering radius of the binary linear codes of dimension 6, *Advances in Mathematics of Communications*, vol. 4, No 3 (2010) 399–403.
T. Baicheva and I. Bouyukliev, On the least covering radius of the binary linear codes of dimension 6, *Proc. of the International Workshop on Algebraic and Combinatorial Coding Theory*, Pamporovo, Bulgaria (2008) 7–12.

[69] T. Baicheva, All binary linear codes of lengths up to 18 or redundancy up to 10 are normal, *Advances in Mathematics of Communications*, vol. 5, No 4 (2011) 681–686.
T. Baicheva, Normality of some binary linear codes, *Proc. of the International Workshop Optimal Codes and Related Topics*, Varna, Bulgaria (2009) 5–10.

[70] T. Baicheva and S. Topalova, Optimal (v,4,2,1) optical orthogonal codes with small parameters, *Journal of Combinatorial Designs*, vol. 20 (2) (2012) 142–160.

[71] T. Baicheva and S. Topalova, Optimal optical orthogonal codes of weight 5 and small lengths, *International Conference on Applications of Computer Algebra*, Sofia, Bulgaria (2012).

[72] T. Baicheva and S. Topalova, Optimal $(v, 3, 1)$ binary cyclically permutable constant weight codes with small v, *Proc. of the International Workshop on Algebraic and Combinatorial Coding Theory*, Pomorie, Bulgaria (2012) 33–38.

[73] T. Baicheva and S. Topalova, Classification results for (v, k, 1) cyclic difference families with small parameters, *Mathematics of Distances and Applications*, M. Deza, M. Petitjean, K. Markov (eds.), ITHEA, Sofia (2012) 24–30.

[74] T. Baicheva and S. Topalova, Optimal (v, 5, 2, 1) optical orthogonal codes of small v, *Applical Algebra in Engeneering Communication and Computing*, vol. 24, numbers 3-4 (2013) 165–177.

Списък на цитирания

[50] T. Baicheva, S. Dodunekov and P. Kazakov, On the cyclic redundancy-check codes with 8-bit redundancy, *Computer Communications*, vol. 21 (1998) 1030–1033.

1. R. Dodunekova, *On the binomial moments of linear codes and undetected error probability*, Preprint 2002:49, Chalmers University of Technology, 14 p.

2. R. Dodunekova, The duals of MMD codes are proper for error detection. *IEEE Trans. Inform. Theory*, vol.49, No.8, 2003, pp. 2034-2038.

3. R. Dodunekova, The extended binomial moments of a linear code and the undetected error probability, *Problems of Information Transmission*, v.39, No.3, 2003, pp.255-265.

4. Q. Zhou and X. Wang, Performance analysis on extended-shortened codes. *Journal of Chongqing university of posts and telecommunications (natural sciences)*, V.16, No.3, 2004, pp.115-117.

5. Q. Zhou and X. Wang, Performance analysis and study on linear extended shortened codes, *Management&control technology*, V.23, No.9, 2004, pp.64-66.

6. P. Koopman and T. Chakravarty, Cyclic Redundancy Check (CRC) Polynomial Selection for Embedded Networks, *Proc. of the International Conference on Dependable Systems and Networks*, DSN-2004, pp.145-154.

7. F. Worm, P. Ienne and P. Thiran, Soft self-synchronizing codes for self-calibrating communication, *IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD*, 2004, pp.440-447.

8. Q. Zhou, X. Wang and H. Ge, Performance analysis and study on linear extended shortened codes, *Xibei Gongye Daxue Xuebao/Journal of Northwestern Polytechnical University*, 22(5), 2004, pp.640-643.

9. E. Nikolova, *Подходящи кодове за откриване на грешки*, Дисертация за присъждане на научната степен 'Доктор', 2005.

10. R. Dodunekova, O. Rabaste and J.L.V. Páez, Error detection with a class of irreducible binary cyclic codes and their dual codes, *IEEE Trans. on Inform. Theory*, vol. 51, No. 4, pp. 1206-1209, 2005.

11. A. Youssef, *Reseau de communication a haut niveau d'integrite*, PhD Thesis No. 2292, 2005, INPT, France.

12. F. Worm, *Robust checkers for self-calibrating designs*, PhD Thesis No. 3647, 2006, Lausanne, EPFL.

13. T. C. Maxino, *The effectiveness of checksums for embedded networks*, MS Thesis, Carnegie Melon University, Pttsburg, USA, May, 2006.

14. Z. Zhi, J. B. Tan, H. D. Huang and F. F. Chen, Algorithms for high-speed generating CRC error detection coding in separated ultra-precision measurement, *Journal of Physics: Conference Series*, 48, pp. 228-232, 2006.

15. Файза А. Р. Салам Муджахед, *Предизвикателства към сигурността в информационна система, базирана на УЕВ технологиите*, Дисертация за присъждане на научната степен 'Доктор', ИМИ-БАН, 2007.

16. T. Klove, *Codes for error detection*, Series on Coding Theory and Cryptology, vol 2., World Scientific, 2007.

17. T. Mattes, F. Schille1, A. Mörwald, J. Pfahler and T. Honold, Safety proof of Combinations of CRC for Industrial Communication, *Journal of Applied Computer Science*, Vol. 16. No 1, 2008, pp. 15-32.

18. F. Schiller, T. Mattes, Analysis of nested CRC with additional net data by means of stochastic automata for safety-critical communication, *Proc. of IEEE International Workshop on Factory Communication Systems*, Dresden, 21-23 May 2008, Article number 4638714, Pages 295-304.

19. H. D. Wacker and J. Börcsök, Binomial and monotonic behavior of the probability of undetected error and the 2-r-bound, *Journal WSEAS Transactions on Communications*, Vol. 7 Issue 3, March 2008, pp. 188-197.

20. T. Maxino and P. Koopman, The effectiveness of checksums for embedded control networks, *IEEE Trans. on Dependable and Secure computing*, vol. 6, No. 1, pp. 59-72, 2009.

21. O. Egwali Annie and V. V. N. Akwukwuma, Performance Evaluation of AN-VE: An Error Detection and Correction Code, *African Journal of Computing & ICT*, vol. 6, No 1, pp. 117-126, 2013.

22. X. Ji, G. Wang, F. Liu, RS-485 Bus Design of a Missile Simulation Training System, *Telkomnika*, Vol. 11, No. 2, 2013, pp. 291-296.

[51] T. Baicheva, Binary and ternary linear codes which are good and proper for error correction, *Proc of the International Workshop on Algebraic and Combinatorial Coding Theory*, Bansko, Bulgaria (2000) 55–60.

1. E. Nikolova, *Подходящи кодове за откриване на грешки*, Дисертация за присъждане на научната степен 'Доктор', 2005.

2. R. Dodunekova, S. Dodunekov and E. Nikolova, A survey on proper codes, *Discrete Applied Mathematics*, Volume 156, Issue 9, 1 May 2008, pp. 1499-1509.

[52] T. Baicheva, S. Dodunekov and P. Kazakov, On the Undetected Error Probability Performance of Cyclic Redundancy-Check Codes of 16-bit Redundancy, *IEE Proc. Communications*, vol. 147, No. 5 (2000) 253 –256.

1. D. Sheinwall, J. Satran, P. Thaler, V. Cavanna, Internet Protocol Small Computer System Interface (iSCSI) Cyclic Redundancy Check (CRC) Checksum Considerations. RFC-3385, Sept. 2002, *The Internet Society.*

2. F. Zhai, I.J. Fair, Efficient cyclic redundancy checks for turbo-coding, *Proc. Wireless and optical communications*, WOC 2002, Banff, Canada, pp. 356-196.

3. R. Dodunekova, On the binomial moments of linear codes and undetected error probability, Preprint 2002:49, Chalmers University of Technology, 14 p.

4. R. Dodunekova, The duals of MMD codes are proper for error detection, *IEEE Trans. Inform. Theory*, vol.49, No.8, 2003, pp. 2034-2038.

5. R. Dodunekova, The extended binomial moments of a linear code and the undetected error probability, *Problems of Information Transmission*, v.39, No.3, 2003, pp.255-265.

6. A. Youssef, A. de Bonneval, Y. Couzet, Dependability of Communications in Critical Real-Time Control Systems, *8-th CaberNet Radicals Workshop*, Ajaccio, Corsica, 5-8 October, 2003.

7. A. Youssef, *Systeme de commande de voldufutur: nouvelle architecture de communication*, Thesis, LAAS-CNRS, Groupe TSF 7, Toulouse, France,2003.

8. F. Zhai and I.J. Fair, Techniques for early stopping and error detection in turbo decoding, *IEEE Transactions on Communications*, 51 (10), 2003, pp.2034-2038.

9. V. A. Khitrovskyy, Schematic and technological aspects of frequency synthesizer design for advanced radars, *Proc of Int. Crimean Conference Microwave & Tele- communication Technology*, Sevastopol, Ukraine, 2003, pp. 11-14.

10. P. Koopman, T. Chakravarty, Cyclic Redundancy Check (CRC) Popynomial Selection for Embedded Networks, *Proc. The International Conference on Dependable Systems and Networks*, DSN-2004.

11. M.M. Carvalho and J.J. Garcia-Luna-Aceves, Modeling single-hop wireless networks under Rician fading channels, *2004 IEEE Wireless Communications and Networking Conference*, WCNC 2004, 1, pp.219-224.

12. E. Nikolova, *Подходящи кодове за откриване на грешки*, Дисертация за присъждане на научната степен 'Доктор', 2005.

13. A. Youssef, *Reseau de communication a haut niveau d'integrite*, PhD Thesis No. 2292, 2005, INPT, France.

14. R. Dodunekova, O. Rabaste and J.L.V. Páez, Error detection with a class of irreducible binary cyclic codes and their dual codes, *IEEE Trans. on Inform. Theory*, vol. 51, No. 4, pp. 1206-1209, 2005.

15. J. Zhao, F. Zarkeshvari and A.H. Banihashemi, On implementation of min-sum algorithm and its modifications for decoding low-density Parity-check (LDPC) codes, *IEEE Trans. on Communications*, vol. 53, Issue 4, April 2005, pp. 549 - 554. ISSN: 0090-6778

16. T.C. Maxino, *The effectiveness of checksums for embedded networks*, MS Thesis, Carnegie Melon University, Pttsburg, USA, May, 2006.

17. S. Huettinger, Low-complexity short-length error detecting codes, *Proc. of the International Workshop on Algebraic and Combinatorial Coding Theory*, Zvenigorod, Russia, pp. 118-121, 2006.

18. M.M. de Carvahlo, *Analytical modeling of medium access control protocols in wireless networks*, PhD Thesis, Univ.of California Santa Cruz, March 2006.

19. C. Nguyen and G. R. Redinbo, Detecting computer-induced errors in remote-sensing JPEG compression algorithms, *IEEE Transactions on Image Processing*, Vol. 15, Issue 7, July 2006, pp. 1728-1739. ISSN: 1057-7149

20. J. Börcsök, J. Hölzel and H. D. Wacker, Probability of Undetected Error with Redundant Data Transmission on a Binary Symmetric Channel without Memory, *Proceedings of the*

6th WSEAS International Conference on Applied Computer Science, Tenerife, Canary Islands, Spain, December 16-18, 2006, pp. 103-106.

21. Файза А. Р. Салам Муджахед, *Предизвикателства към сигурността в информационна система, базирана на УЕВ технологиите*, Дисертация за присъждане на научната степен 'Доктор', ИМИ-БАН, 2007.

22. J. Börcsök, Some Inequalities Concerning Binomial Coefficients and the Weight Distribution of Proper Linear Codes, *7th WSEAS International Conference on Applied Computer Science*, Venice, Italy, November 21-23, 2007, pp. 43-48.

23. T. Klove, *Codes for error detection*, Series on Coding Theory and Cryptology, vol 2., World Scientific, 2007.

24. Ph. Golden, H. Dedieu, K. Jacobsen, *Implementation and Applications of DSL Technology*, CRC Press, 2007.

25. H. D. Wacker and J. Börcsök, Some inequalities concerning binomial coefficients and the weight distribution of proper linear codes, *Proceedings of the 7th Conference on 7th WSEAS International Conference on Applied Computer Science - Volume 7*, Venice, Italy pp. 43-48, 2007.

26. H. D. Wacker and J. Börcsök, The probability of undetected error of some communication channels, *Risk, Reliability and Societal Safety* Aven & Vinnem (eds.), Taylor & Francis Group, London, 2007.

27. N. Kaabouch, A. Dhirde, S. Faruque, Improvement of the orthogonal code convolution capabilities using FPGA implementation, *IEEE International Conference on Electro/Information Technology*, Chicago, IL, 17-20 May 2007, pp. 337 - 341.

28. A. Wang and N. Kaabouch, FPGA based design of a novel enhanced error detection and correction technique, *IEEE International Conference on Electro/Information Technology*, Ames, IA, 18-20 May 2008, pp. 25 - 29.

29. H. D. Wacker and J. Börcsök, Binomial and monotonic behaviour of the probability of undetected eror and the 2^{-r}-bound, *WSEAS Transactions on Communications*, vol. 7, March 2008, pp. 188-197.

30. H. D. Wacker and J. Börcsök, The Dual Distance of a CRC and Bounds on the Probability of Undetected Error, the Weight Distribution, and the Covering Radius, *WSEAS Transactions on Communications*, vol. 7, April 2008, pp. 188-197.

31. F. Schiller and T. Mattes, Analysis of nested CRC with additional net data by means of stochastic automata for safety-critical communication, *IEEE International Workshop on Factory Communication Systems*, 21-23 May, 2008, pp. 295 - 304

32. T. Maxino and P. Koopman, The effectiveness of checksums for embedded control networks, *IEEE Trans. on Dependable and Secure computing*, vol. 6, No. 1, pp. 59-72, 2009.

33. Damien O'Rourke, *Practical packet combining for use with cooperative and non-cooperative ARQ schemes in wireless sensor networks*, PhD thesis, Dublin City University, 2009.

34. P. K. Pendli, M. Schwarz, H. D. Wacker and J. Börcsök, Bluetooth for Safety Systems, *ISSC 2011*, Trinity College Dublin, June 23-24, 2011.

35. T. Zheng, W. Shaoping and A. El Kamel, Bluetooth communication reliability of mobile vehicles, *Proc. of International Conference on Fluid Power and Mechatronics*, Beijing, China, pp. 873-877, 2011.

36. P. K. Pendli, M. Schwarz, H. D. Wacker and J. Boercsoek, Bluetooth for Safety Systems, *22nd IET Irish Signals and Systems Conference*, Dublin, Ireland, 23-24 June2011.

37. Damien O'Rourke and Conor Brennanb, Practical packet combining for use with cooperative and non-cooperative ARQ schemes in resource-constrained wireless sensor networks, *Ad Hoc Networks*, Volume 10, Issue 3, pp. 339–355, 2012.

38. H. D. Wacker, P. Pendli and J. Börcsök, Data transmission via erasure type channels protected by linear codes, *J. Phys.: Conf. Ser.* 364 012058, 2012.

39. M. Shinagawa, K. Kondou, M. Noda, *CRC generator polynomial select method, CRC coding method and CRC coding circuit*, US Patent 8341510 B2, December 25, 2012.

40. M. Shinagawa, M. Noda, H. Yamagishi, K. Kondou, *Transmission apparatus and method, reception apparatus and method, and program*, US Patent 8327251 B2, December 4, 2012.

41. You-Gang Cha, Cha-Keon Cheong, Analysis of CRC-p code performance and determination of optimal CRC code for VHF band maritime ad-hock wireless communication, *The Journal of Korea Information and Communications Society*, Vol. 37A, No. 6, pp. 438-449, 2012.

42. O. Egwali Annie and V. V. N. Akwukwuma, Performance Evaluation of AN-VE: An Error Detection and Correction Code, *African Journal of Computing & ICT*, vol. 6, No 1, pp. 117-126, 2013.

43. M. Gholase, L.P.Thakare and A.Y. Deshmuk, Enhancement of Error Detection and Correction Capability Using Orthogonal Code Convolution, *International Journal of Computational Engineering Research*, Vol, 03, Issue, 4, pp. 66-71, 2013.

44. H. D. Wacker, P. Pendli and J. Boercsoek, Data transmission via erasure type channels protected by linear codes, *Journal of Physics: Conference Series*, vol. 364, Issue 1, 2013.

45. H. D. Wacker, P. Pendli and J. Boercsoek, Error control capability of orthogonal code convolution by means of FPGA application, *International Journal of Engineering Sciences Paradigms and Researches*, Vol. 05, Issue 01, pp. 27-30, 2013.

46. Y. Zhang, X. Li, Apparatus for appending cyclic redundancy check in communication system, US Patent US 8464140 B2, June 11, 2013.

47. J. H. Collet, A brief overview of the challenges of the multicore roadmap, *Proc. of International Conference MIXDES*, Lublin, Poland, 2014.

48. J. Noh, H. Song and C. Lee, An Error Pattern Estimation Scheme for Iterative Receiver in MIMO Systems, *IEEE Communications Letters* Vol. 18, Issue 4, pp. 552-555, 2014.

49. V. K. Shendre and R. Nawkhare, Enhancement of Error Control Capability of Orthogonal Code Convolution for Digital Communication, *IJCAT International Journal of Computing and Technology*, Volume 1, Issue 3, April 2014, pp. 5-9.

50. Umberto Mattei, *Extended physical layer modeling for smart metering utility network simulators*, Master Thesis, KTH, Communication Theory, Sweden, 2014.

51. S. Jirapure, Implementation of 16 bit orthogonal code convolution with enhanced error control technique using VHDL, *Int. Journal of Pure and Applied Research in Eng. and Techn.*, vol. 2 (9), pp. 78-85, 2014.

52. A. Kant, Enchance orthogonal code convolution capabilities for efficient digital communication, *Int. Journal For Technological Research In Engineering*, vol. 2, issue 4, pp. 2347-4718, 2014.

[53] T. Baicheva, On the covering radius of ternary negacyclic codes with length up to 26, *IEEE Trans. on Inform. Theory*, vol. 47, No. 1 (2001) 413–416.

1. G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland, Elsevier Science B.V., 1997, Updated July 12, 2010 list with bibliography at http://www.infres.enst.fr/ lobstein/bib-a-jour.pdf.

2. E. Velikova, The weight distribution of the cosets leaders of ternary cyclic codes with generator polynomial of small degree, *Annuarie de L'Université de Sofia 'St. Kl. Ohridski'*, vol. 97, pp. 109-114, 2005.

3. E. Velikova and A. Bojilov, On the Weight Distribution of the Coset Leaders of Constacyclic Codes, *Serdica J. Computing*, vol. 2, No. 2, pp. 105-110, 2008.

4. A. A. Davydov, M. Giulietti, S. Marcugini and F. Pambianco, Linear nonbinary covering codes and saturating sets in projective spaces, *Advances in Mathematics of Communications*, vol. 5, issue 2, 2011, pp. 119-147.

[54] T. Baicheva, S. Dodunekov and R. Kötter, On the Performance of the Ternary [13,7,5] Quadratic-Residue Codes, *IEEE Trans. Inform. Theory*, vol. 48, No. 2 (2002) 562–564.

1. E. Nikolova, *Подходящи кодове за откриване на грешки*, Дисертация за присъждане на научната степен 'Доктор', 2005.

2. R. Dodunekova, O. Rabaste and J.L.V. Páez, Error detection with a class of irreducible binary cyclic codes and their dual codes, *IEEE Trans. on Inform. Theory*, vol. 51, No. 4, pp. 1206-1209, 2005.

3. T. Klove, *Codes for error detection*, Series on Coding Theory and Cryptology, vol 2., World Scientific, 2007.

4. H. P. Lee, H. Y. Chen and H.C. Chang, A Method for Decoding the (24, 15, 5) Cyclic Code, *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Kaohsiung, 26-28 Nov. 2007, pp. 391-394. ISBN: 978-0-7695-2994-1

5. D. Kisku, P. Gupta and J. Sing, Feature Level Fusion of Face and Palmprint Biometrics, *Proc of Joint IAPR International Workshop SSPR&SPR*, Cesme, Izmir, Turkey, August 18-20, 2010.

6. M. Effros, G. D. Forney Jr., F. R. Kschischang, M. Médard, A. Singer, A. Vardy, The Scientific Legacy of Ralf Koetter, *IEEE Trans. Inform. Theory*, Vol. 57, N0. 2, FEBRUARY 2011, pp. 589-592.

7. K Xenoulis, List Permutation Invariant Linear Codes: Theory and Applications, *IEEE Trans. Inform. Theory*, Vol. 60, Issue 9, Sept. 2014, pp. 5263-5282.

[56] T. Baicheva and V. Varek, On the least covering radius of binary linear codes with small lengths, *IEEE Trans. On Inform. Theory*, vol. 49, No. 3 (2003) 738–740.

1. G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland, Elsevier Science B.V., 1997., Updated July 12, 2010 list with bibliography at http://www.infres.enst.fr/ lobstein/bib-a-jour.pdf.

2. И. Буюклиев, *Алгоритмични подходи за изследване на линейни кодове*, Дисертация за присъждане на научната степен 'Доктор на математическите науки', 2007.

3. Li Ping, Zhu Shi-xin, Yu Hai-feng, Covering radius of codes over ring $F_2 + uF_2$, *Journal of University of Science and Techology of China*, 38(2), 2008.

[59] T. Baicheva, I. Boyukliev, S. Dodunekov and W. Willems, Teaching linear codes, *Mathematica Balkanica*, New Series vol. 19 (2005) 3–16.

1. A. Faldum, On the trustworthiness of error-correcting codes, *IEEE Trans. Inform. Theory*, vol. 53, No. 12, 2007, pp. 4777 - 4784.

2. R. Jurrius and R Pellikaan, Extended and Generalized Weight Enumerators, *Proceedings of the International Workshop on Coding and Cryptography*, WCC 2009, Ullensvang, May 10-15, Selmer Center, Bergen, pp. 76-91, 2009.

3. R. Jurrius and R Pellikaan, The extended coset leader weight enumerator, *Proceedings 30th Symposium on Information Theory on the Benelux*, May 28-29, pp. 217-224, 2009.

4. R. Jurrius and R Pellikaan, The coset leader and list weight enumerator, *Contemporary Mathematics*, vol. 632, pp. 229-250, 2015

[65] T. Baicheva, I. Bouyukliev, S. Dodunekov, and V. Fack, Binary and Ternary Quasi-perfect Codes with Small Dimensions, *IEEE Trans. on Inform. Theory*, vol. 54, issue 9 (2008) 4335–4339.

1. G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, Covering Codes, North-Holland, *Elsevier Science B.V.*, 1997., Updated July 12, 2010 list with bibliography at http://www.infres.enst.fr/ lobstein/bib-a-jour.pdf.

2. Foto N. Afrati, Anish Das Sarma, David Menestrina, Aditya Parameswaran, Jeffrey D. Ullman, Fuzzy Joins Using MapReduce, *Technical Report. Stanford InfoLab*, July 2011.

3. F. N. Afrati, A.D. Sarma, D. Menestrina, A. Parameswaran, J. D. Ullman, Fuzzy Joins Using MapReduce, *IEEE 28th International Conference on Data Engineering*, Washington, DC, 1-5 April 2012, pp. 498-509.

4. L. H. Aslanyan and H. E. Danoyan, Complexity of Elias algorithm based on codes with covering radius 3, *Proc. of the Yerevan State University*, No. 1, pp. 44-50, 2013.

5. L. H. Aslanyan and H. E. Danoyan, Complexity of Elias algorithm for hash functions based on Hamming and extended Hamming codes, *Reports of National Academy of Sciences of Armenia*, vol. 113, No. 2, 2013.

[66] T. Baicheva, Determination of the best CRC codes with up to 10-bit redundancy, *IEEE Trans on Communic.*, vol. 56, issue 8 (2008) 1214–1220.

1. T. Zhu, Z. Zhong, J. Zhang, A quick coding method based on dynamic table look-up for arbitrary bit length polynomial division in embedded system, *7th International Conference on Networked Computing and Advanced Information Management*, Gyeongju, 21-23 June, 2011, pp. 15-19.

2. E. Üstünel, I. Hökelek, O. Ileri, H. Arslan, Joint optimum message length and generator polynomial selection in Cyclic Redundancy Check (CRC) coding, *2011 IEEE 19th Signal Processing and Communications Applications Conference*, Antalya, 20-22 April 2011, pp. 222-225.

3. E. Üstünel, I. Hökelek and O. Ileri, A cross-layer goodput enhancement considering CRC coding and ARQ dinamics, *IEEE Symposium on Computer Communications*, Cappadocia, Turkey, pp. 23-28, 2012.

4. H. Patel and D. Jain, Design & check cyclic redundancy code using VERILOG HDL, *Int. Journal for Scientific Research & Development*, vol.1, issue 5, pp. 1096-1098, 2013.

5. H. Patel, D. Patel, M. Chaudhary and M. Zala, An Automated CRC engine, *International Journal for Innovative Research in Science & Technology*, Vol. 1, Issue 1, pp. 73-77, June 2014.

6. Li Chia Choo, Zander Lei, CRC codes for short control frames in IEEE 802.11ah, *The 80-th IEEE Vehicular Technology Conference*, Vancouver, Canada, 14-17 September, 2014, pp. 1-5.

7. C. Bai, M. S. Leeson, M. D. Higgins, Performance of SW-ARQ in bacterial quorum communications, *Nano Communication Networks*, vol. 6, Issue 1, pp. 3–14, March 2015.

8. M. El-Khamy, J. Lee, I. Kang, Detection Analysis of CRC-Assisted Decoding, *IEEE Commun. Letters*, vol. 19, issue 3, pp. 483-486, 2015.

9. D. A. Nugroho, S. Rizal, Dong-Seong Kim, Reconstruct unrecoverable data in real-time networks using Bézier curve, *IET Communications*, Available online: 05 January 2015, pp. 596-602

[68] T. Baicheva and I. Bouyukliev, On the least covering radius of the binary linear codes of dimension 6, *Advances in Mathematics of Communications*, vol. 4, No 3 (2010) 399–403.

1. G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland, Elsevier Science B.V., 1997, Updated November 29, 2011 list with bibliography at http://www.infres.enst.fr/ lobstein/bib-a-jour.pdf.

[69] T. Baicheva, All binary linear codes of lengths up to 18 or redundancy up to 10 are normal, *Advances in Mathematics of Communications*, vol. 5, No 4 (2011) 681–686.

1. G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland, Elsevier Science B.V., 1997, Updated November 29, 2011 list with bibliography at http://www.infres.enst.fr/ lobstein/bib-a-jour.pdf.

[70] T. Baicheva and S. Topalova, Optimal (v,4,2,1) optical orthogonal codes with small parameters, *Journal of Combinatorial Designs*, vol. 20 (2) (2012) 142–160.

1. X. Wang and Y. Chang, Further results on optimal (v, 4, 2, 1)-OOCs, *Discrete Mathematics*, volume 312, issue 2, pp. 331 - 340, 2012.

2. M. Buratti, A. Pasotti and D. Wu, On optimal (v, 5, 2, 1) optical orthogonal codes, *Design Codes and Cryptography*, vol. 68, Issue 1-3, pp. 349-371, 2013.

3. H. Zhao, D. Wu and R. Qin, Further results on balanced $(n, 3, 4, \lambda_a, 1)$-OOCs, *Discrete Mathematics*, Vol. 337, 28 December 2014, pp. 87–96.

[71] T. Baicheva and S. Topalova, Optimal optical orthogonal codes of weight 5 and small lengths, *International Conference on Applications of Computer Algebra*, Sofia, Bulgaria (2012).

1. S. M. Ibraheem, M. M. A. Elrazzak, S. M. S. Eldin, W. Saad and A.E. Aboelazm, A class of structured quasi-cyclic LDPC codes based on planar difference families, *International Conference on Advanced Technologies for Communications*, Ho Chi Minh City, 16-18 Oct. 2013, pp. 614-619.

[74] T. Baicheva and S. Topalova, Optimal (v, 5, 2, 1) optical orthogonal codes of small v, *Applical Algebra in Engeneering Communication and Computing*, vol. 24, numbers 3-4 (2013) 165–177.

1. H. Zhao, D. Wu and R. Qin, Further results on balanced $(n, 3, 4, \lambda_a, 1)$-OOCs, *Discrete Mathematics*, Vol. 337, 28 December 2014, pp. 87–96.