АВТОРСКА СПРАВКА

за научните приноси на

Светлана Тодорова Топалова

по конкурс за професор по специалност 01.01.12 Информатика (компютърни методи за изследване на комбинаторни дизайни и сродни на тях структури)

1 Общи бележки

Комбинаторните дизайни намират широко приложение в шумозащитното кодиране, статистическите експерименти и криптографията. Много от методите за конструирането и изучаването им са сходни на методи за изследване на шумозащитни кодове, крайни проективни пространства, адамарови матрици, ортогонални латински квадрати и други. Затова теорията на дизайните е актуална и бързо развиваща се област от съвременната комбинаторика.

Задачите за съществуване, изброяване и класификация на дизайни с дадени параметри и техните резолюции могат да се решават много успешно с използването на компютър. Ако се предполага, че съществува дизайн с определени параметри и евентуално със зададени допълнителни свойства, може да се напише програма, която да анализира пространството от възможни решения докато се намери такова, което удовлетворява съответните критерии. Ако съществуват много решения, то програмата трябва да отдели еквивалентните и да класифицира получените дизайни според свойствата им. В голямата част от случаите не е тривиално да се намерят ефективни алгоритми, както за конструиране, така и за анализ на получените решения. Затова компютърните методи за изследване на дизайни представляват също толкова голям интерес, колкото и получените от прилагането им резултати.

За конкурса са представени 25 публикации, които отговарят на тематиката и са след хабилитацията (не са участвали в друг конкурс).

Решение на интересни отворени проблеми обикновено не може да бъде намерено с помощта на софтуер, който работи за много параметри и, съответно, е добре изтестван. Затова в голямата част от случаите, за да бъдат избегнати грешки в програмите, повечето изчисления са дублирани от няколко съавтора, които са ги извършили с различни алгоритми или различни програмни реализации на един и същ алгоритъм. Има и случаи, когато част от резултатите са получени както с компютър, така и теоретично. Винаги е правена проверка за съвместимост с

известните изследвания на други автори.

Публикациите за конкурса могат да бъдат обединени тематично в пет подгрупи, всяка от които е разгледана в някой от следващите раздели. Във всички предложени публикации значителна част от методите е разработена от автора и основната част от необходимия софтуер е писана от автора на C++. В статиите [15] и [22] за намиране на определени подгрупи на групата от автоморфизми на проективното пространство и техните нормализатори използвам и софтуерната система GAP. Програмите на съавторите са на C++, Pascal или Java. Ако в някоя публикация част от резултатите не са получени от автора, а само от съавторите, това е специално описано по-долу.

В повечето случаи изчисленията са правени на персонални компютри. Достъпът до BlueGene през последните две години даде възможност част от резултатите в [18] и [23] да бъдат получени на този мощен паралелен компютър. Тук трябва да отбележим, че класификационните задачи са особено подходящи за имплементиране на паралелни компютри заради доказаната висока степен на скалируемост на алгоритъма за търсене с връщане.

За задачите от раздели 2 и 3, както и в [4], е използван локалният подход за конструиране на дизайни със зададени автоморфизми, при който построяването на дизайните става на два етапа. Първият включва намирането на всички неекивалентни *условни орбитни матрици*. Наричат се условни, защото е възможно някои от тях да не са разширими до дизайни. На втория етап елементите на всяка матрица се заместват с циркуланти така, че получената структура да е дизайн. Това се осъществява с алгоритъм за изчерпващо търсене с връщане и необходимото време нараства експоненциално с нарастването на параметрите. Броят на изоморфните дизайни е огромен и затова от особена важност за бързодействието на софтуера е намирането на критерии за възможно най-ранно отсяване на еквивалентни частични решения. Ако самият тест за еквивалентност на частичните решения не е достатъчно бърз, трябва добре да се прецени дали да бъде прилаган на всички частични решения, или само на част от по-малките от тях. От значение е и от кой елемент на орбитната матрица започва разширяването. Затова решаването на такива задачи става с подход, специфичен за всеки конкретен случай, и често пъти усилията да се намерят дизайните с дадени параметри и автоморфизми могат да останат безплодни.

Конструирането на резолюции, двойно разрешими дизайни, спредове и паралелизми и оптични ортогонални кодове в задачите от раздели 4, 5 и 6 също се базира на алгоритми за изчерпващо търсене с връщане и основните проблеми при тях

са подобни на описаните по-горе. В повечето случаи решенията се генерират в лексикографски ред и тестът за еквивалентност е всъщност тест за минималност на частичното решение (т.е. проверка дали то не е еквивалентно на лексикографски по-малко решение).

Голяма част от получените класификационните резултати са достъпни в интернет, което ги прави удобни за ползване от всички, които се интересуват.

2 Дизайни, които съдържат поддизайни

Към тази група спадат публикации [1], [2], [7] и [11]. Броят на изоморфните на даден дизайн е обратно пропорционален на реда на групата от автоморфизмите му. В някои случаи, в които е известен броят на всички дизайни с дадени параметри и допълнителни свойства, изброяване с точност до изоморфизъм и класификация според реда на групата от автоморфизми са възможни като се построят и изследват само дизайните с нетривиални автоморфизми, а те са много по-малко от тези с тривиалния автоморфизъм.

Един такъв случай са Щайнеровите системи от тройки от ред 19 и 21, които съдържат три Щайнерови подсистеми от тройки от ред 7. Такива системи нарича-ме Уилсонови, защото са разглеждани за пръв път от Wilson (през 1974 година), който с помощта на известни резултати за латински квадрати определя общия им брой и извежда долни граници за броя на техните класове на изоморфизъм.

Щайнеровите системи от тройки от ред n ($STS(n)$) са сред най-изучаваните и най-широко използвани дизайни. През миналия век бяха класифицирани всички $STS(n)$ за $n < 19$, а през 2004 Kaski и Östergård публикуваха пълната класификация на $STS(19)$. В момента $STS(21)$ са системите от най-малък ред, които все още не са класифицирани. Те представляват особен интерес и защото още не е известно дали сред тях има двойно-разрешими.

В [11] е направена класификация на $STS(19)$ с подсистеми от ред 7 и на Уилсонови $STS(21)$. Резултатите са получени по няколко различни начина, в частност Kaski и Östergård използват за целта модификация на алгоритъма, с който класифицират всички $STS(19)$, а ние със Златарски построяваме Уилсоновите $STS(19)$ и $STS(21)$ с всички възможни автоморфизми от прост ред, като Златарски използва особеностите на конкретната задача (по-точно това, че автоморфизмите са от ред 2 или 3), а аз локалния подход. Броят на неизоморфните Уилсонови системи с тривиалния автоморфизъм се определя по общия брой Уилсонови сис-

теми (заедно с изоморфните) и класификацията на системите с нетривиални автоморфизми. Освен това със софтуер на автора са класифицирани резолюциите на всички конструирани $STS(21)$ и е установено, че сред тях няма двойно-разрешими. В [11] не са дадени подробности за начина на конструиране на дизайните във всеки от 13-тте разгледани случая на зададени автоморфизми. Представа за подхода ни може да бъде получена от [1] и [2].

Двойните на даден дизайн са друг случай, в който е известен общият брой (заедно с изоморфните). Долни граници за броя на двойните на някои видове геометрични дизайни са изведени от Jungnickel (и съавтори) в края на 80-те години на миналия век. В [7] дефинираме понятието *уникално разложим* двоен дизайн, извеждаме долна граница за броя на неизоморфните двойни на уникално-разложим дизайн и показваме как точният им брой може да бъде определен, ако сме класифицирали двойните дизайни с нетривиални автоморфизми. В частност, доказваме уникалната разложимост на двойните на дизайна от точките и правите на проективната равнина от ред 4 и намираме техния брой, като първо построяваме такива дизайни с всичките възможни зададени автоморфизми. Този брой е на порядъци по-голям от известните долни граници, но е близък до изведената от нас долна граница за броя на неизоморфните двойни на уникално-разложим дизайн.

Публикациите от тази група са цитирани общо 19 пъти, както в работи върху нови конструкции на дизайни с поддизайни, така и в изследвания върху двойната разрешимост на $STS(21)$ и върху класификацията на дизайни с дадени автоморфизми.

3 Адамарови дизайни и адамарови матрици

Към тази група спадат публикации [3], [6], [8], [9] и [13]. Взаимната ортогоналност на редовете на адамаровите матрици обуславя разнообразните приложения както на адамаровите матрици, така и на съответните адамарови дизайни. Адамаровите матрици от редове до 28 са класифицирани напълно, а за тези от по-голям ред са известни частични класификации.

В [3] и [13] с помощта на локалния подход са конструирани адамарови дизайни (съответно с 43 и 63 точки) с дадени автоморфизми. Освен дизайните са класифицирани и съответните им адамарови матрици. За да се провери дали са еквивалетни две адамарови матрици от ред 44 са използвани съответни бинарни матрици с два пъти повече (88) редове и стълбове, докато за тези от ред 64 това е твърде бавно

и затова са разглеждани подходящи инварианти.

От адамаровите матрици от ред 44 се получават екстремални самодуални кодове с дължина 88, а тези от ред 64 са свързани посредством конструкция на Rahilly с афинни 2-$(64, 16, 5)$ дизайни, сред които са няколкото известни контрапримери на хипотезата на Hamada (През 1973 г. Hamada прави предположение, че дизайнът, получен от точките и подпространствата от дадена размерност на $AG(n, p^m)$ (p просто) има минимален p-ранг, а всички останали дизайни със същите параметри имат по-голям p-ранг). В [13] не са намерени нови контрапримери.

Класификация на двойните на адамарови дизайни може да бъде използвана, както за изследвания за уникална разложимост в контекста на [7], така и за евентуално подобряване (за конкретни параметри) на съществуващите оценки за броя на адамаровите матрици, които съдържат четири адамарови подматрици (долни граници за броя им са изведени от Lam, Lam и Tochev през 2001). В [6] и [8] са конструирани и класифицирани квазидвойни (с параметри като на двойните) на адамарови 2-$(15, 7, 3)$ дизайни с дадени автоморфизми и сред тях са намерени двойните дизайни. В [9] с модификация на локалния подход са конструирани двойните на адамарови 2-$(19, 9, 4)$ дизайни с автоморфизми от ред 3. Следващи изследвания показват, че двойните на геометричния 2-$(15, 7, 3)$ дизайн са уникално разложими.

Публикациите от тази група са цитирани общо 14 пъти в изследвания за адамарови мартици, самодуални кодове, дизайни с дадени автоморфизми, както и във връзка с хипотезата на Hamada.

4 Двойно-разрешими дизайни и ортогонални резолюции

Към тази група спадат публикации [4], [5], [10], [14], [21] и [25]. Един дизайн е *двойно разрешим*, ако притежава поне една двойка взаимно ортогонални резолюции. Съществува връзка между ортогонални резолюции, Киркманови квадрати и квадрати на Рум. Специфичните свойства на двойно разрешимите дизайни могат да бъдат използвани в статистически и криптографски приложения, което обуславя и интереса към тяхната класификация. Някои подробности относно възможностите за използване в криптографията са дадени в [14].

Върху двойната разрешимост се работи активно през последните десетилетия. Резултатите са добре обобщени в статиите на Abel, Lamken и Wang (2008) и на Lamken (2009). Те се отнасят до разрешаване на проблема за съществуване

на двойно разрешими дизайни с определени параметри и установяване на долна граница за броя на взаимно ортогоналните резолюции. Преди [21] класификационни резултати бяха известни само за квадратите на Рум (Квадрат на Рум със страна n е еквивалентен на две ортогонални резолюции на 2-$(n+1, 2, 1)$ дизайн), чиито брой с точност до нееквивалентност е определен за $n \leq 9$.

В [21] е представена пълна класификация на двойно разрешими дизайни с малки параметри. Получените резултати са подредени в таблици, от които лесно се виждат най-малките отворени случаи. Разработен е метод, при който за дадени параметри се конструират първо резолюциите, които са ортогонални на поне една друга резолюция, после съответните им двойно разрешими дизайни и накрая множествата от взаимно ортогонални резолюции. Резолюциите с дадените параметри и свойства построяваме в лексикографски ред (по-точно построяваме съответния еквидистантен код) чрез търсене с връщане. На частичните решения прилагаме тест за минималност (за отсяване на еквивалентните) и тест за съществуване на ортогонална резолюция. Последният е от голямо значение за бързодействието на софтуера, затова е обърнато специално внимание на използвания алгоритъм. Разработени са два алгоритъма за този тест, които са подробно описани и сравнени в [10].

Някои от проблемите, възникнали при конструирането на ортогоналните резолюции доведоха до допълнителни изследвания в [25] за случая на кратни дизайни. Там е изведена зависимост на броя n_m на множествата от m взаимно ортогонални резолюции на m-кратен разрешим дизайн от броя на глобално нееквивалентните множества от $q-1$ (q - брой блокове в паралелен клас) ортогонални латински квадрата от ред m. Това позволява да бъдат пресметнати някои долни граници за n_m.

Въпросът за съществуване на двойно разрешим 2-$(v, 3, 1)$ дизайн, т.е. двойно разрешима $STS(v)$, е решен с изключение на 12 стойности на v, най-малката сред които е 21 (Abel, Lamken и Wang, 2008). Известни са редица класификации на $STS(21)$ със зададени допълнителни свойства, но двойно разрешима $STS(21)$ все още не е намерена. В [4] са конструирани и изследвани $STS(21)$ с автоморфизми от ред 3 с 3 фиксирани точки и 7 фиксирани блока и техните резолюции. В [5] е изследвана структурата на хипотетична двойно разрешима $STS(21)$. Установени са ограничения, според които случаят е разделен на няколко подслучая. С помощта на компютър е разгледан частен случай на един от тях и не е намерена двойно разрешима $STS(21)$.

Публикациите от тази група са цитирани общо 6 пъти.

5 Спредове и паралелизми в $PG(n, q)$

Към тази група спадат публикации [12], [15], [19], [22] и [24]. Инцидентността на точките и t-мерните подпространства на $PG(n, q)$ дефинира 2-дизайн. Съществува взаимно еднозначно съответствие между паралелен клас от резолюция на този дизайн и t-спред и между резолюция на дизайна и t-паралелизъм. Вместо 1-спред (1-паралелизъм) се използва спред (паралелизъм).

Интересът към спредовете в $PG(n, q)$ възниква заради връзката им с крайни афинни траслационни равнини. Приложения на спредовете и паралелизмите в теорията на кодирането са описани в статиите на Silberstein и Etzion (2011) за кодове с константна размерност и на Mavron, McDonough и Tonchev (2008) за контрапримери на хипотезата на Хамада.

Известни са редица конструкции на спредове и паралелизми и множество изследвания върху вида на групите от автоморфизмите им. Повече информация може да бъде намерена в книгата *Combinatorics of Spreads and Parallelisms* на Johnson (2010). Преди резултатите от този раздел с точност до еквивалентност бяха класифицирани всички максимални частични спредове в $PG(3, 2)$, $PG(4, 2)$, $PG(3, 3)$ и $PG(3, 4)$, а за други параметри бяха известни частични класификации. С помощта на компютър бяха конструирани паралелизми със зададени автоморфизми в $PG(3, 3)$ (Prince, 1997), $PG(3, 5)$ (Prince, 1998) и $PG(5, 2)$ (Stinson и Vanstone, 1986; Sarmiento, 2000).

В [12] са конструирани всички нееквивалентни спредове в $PG(5, 2)$. За целта са използвани специфични особености на групата от автоморфизми на $PG(5, 2)$. Представена е класификация спрямо реда на стабилизаторите на спредовете и спрямо инварианти, които отчитат както броя на 3-мерните подпространства, съдържащи $i (i \leq 5)$ прави от спреда, така и ранга на свързания чрез конструкцията на Rahilly 2-$(64, 16, 5)$ дизайн.

Резултатите в [12] се оказаха съвместими с направената от Shaw и още непубликувана тогава класификация на *книжните спредове (book spreads)* в $PG(5, 2)$ със *страници*, които са 3-мерни подпространства. Shaw ги класифицира само с геометрични съображения, без помощта на компютър. Те са много малка част (9) от всички спредове (131044), но са едни от най-интересните, защото имат богати групи от автоморфизми, само те покриват изцяло поне пет 3-мерни подпространства и сред тях са и двата спреда, които водят до 2-$(64, 16, 5)$ дизайни с минимален ранг. Геометричната структура на книжните спредове е причина да очакваме интересни резултати и за други проективни пространства. Това мотивира разработ-

ването на софтуер за конструиране на книжни спредове в $PG(7,2)$, чиито страници са 5-мерни подпространства, съдържащи книжни спредове (на $PG(5,2)$). В частност с този софтуер се получават и деветте книжни спреда на $PG(5,2)$, както и информация за техните свойства. Тази компютърна проверка на класификацията на Shaw е описана в [24], а резултатите за $PG(7,2)$ са анонсирани в [19].

Обект на [15] са 2-спредове и 2-паралелизми в $PG(5,2)$. Получаваме, че 2-спредът е единствен с точност до еквивалентност. Оказа се, че теоретично доказателство на този факт е публикувано от Shaw през 1999 в статията му *Configurations of planes in PG(5,2)*. Уникалността на 2-спреда е използвана в [15] за частична проверка на софтуера за конструиране на 2-паралелизмите. Основният резултат в [15] е класификацията на 2-паралелизмите с автоморфизми от ред 31. Сред тях са първите примери на транзитивни t-паралелизми за $t > 1$. В книгата *Combinatorics of Spreads and Parallelisms* на Johnson (2010) е доказано, че транзитивни t-паралелизми не могат да съществуват за $t > 1$. Нашият резултат допринесе за своевременното оправяне на тази грешка от Johnson и Montinaro в статията им *The transitive t-parallelisms of a finite projective space* (2012).

Тук искам да отбележа, че използваният метод за конструиране на паралелизми със зададени автоморфизми е съвсем различен от този за дизайни с дадени автоморфизми. При t-паралелизмите първо намираме подгрупа на групата от автоморфизми на проективното пространство от съответния ред и орбитите на t-мерните подпространства спрямо нея. За елементите на всеки спред на t-паралелизма проверяваме условия, свързани с тези орбити, а за отсяване на изоморфните решения използваме нормализатора на подгрупата, с която строим t-паралелизми.

В [22] са конструирани паралелизмите в $PG(3,4)$ с автоморфизми от ред 7. Те са класифицирани според реда на групите от автоморфизмите им и според вида на спредовете, които съдържат (в $PG(3,4)$ има три спреда - регуларен, субрегуларен и арегуларен). Изследванията за вида на спредовете са със софтуер на Железова. Сред конструираните паралелизми няма регуларни. Резултатите показват, че в $PG(3,4)$ не съществуват транзитивни паралелизми.

Публикациите от тази група са цитирани общо 10 пъти.

6 Оптимални оптични ортогонални кодове и циклични дизайни

Към тази група спадат публикации [16], [17], [18], [20] и [23]. Оптичните ортогонални кодове (OOK) дават възможност за бързо и надеждно асинхронно предаване на данни от голям брой потребители през оптични CDMA комуникационни мрежи. Освен това имат приложения в мобилни радиосистеми, комуникации с разпръснат спектър и прескачане на честота, радари и сонари и др. Затова те са интензивно изследвани от 80-тте години насам.

OOK са фамилии от двоични последователности с определени авто- и крос-корелационни свойства. Те могат да бъдат разглеждани и като циклични частични дизайни, за които са в сила някои допълнителни изисквания. За циклични комбинаторни структури се дефинира мултипликативна еквивалентност. Авторите, които са класифицирали циклични дизайни с дадени параметри, правят първо класификация с точност до мултипликативна еквивалентност.

Известни са редица работи по решаване на въпроса за съществуването на оптимални OOK с дадени параметри, като са използвани преди всичко методи и резултати от теорията на разностните множества. Подробен обзор на направените изследвания съдържа статията на Buratti, Momihara и Pasotti (2011). Тази статия ни мотивира да започнем работа по класификация на OOK, защото за някои от представените в нея рекурсивни конструкции е отбелязано, че биха довели до подобър резултат, ако влизащите в тях OOK с малки параметри са с определени свойства, но не е ясно дали има такива. Публикациите от настоящия раздел представят първите класификации на OOK с дадени параметри.

За построяването на всички OOK с точност до мултипликативна еквивалентност предварително намираме елементите на масив, който съдържа всички възможни (удовлетворяващи авто-корелационното свойство) кодови думи. Те са подредени по начин, отчитащ както въведен от нас лексикографски ред, така и действието на автоморфизмите на цикличната група от ред v. Такава подредба позволява бърз тест за минималност на частичните решения. Кодовите думи на OOK, който конструираме, избираме от този масив, като следим за валидността на крос-корелационните изисквания. При добавяне на кодова дума проверяваме дали някой от автоморфизмите на Z_v изобразява текущото частично решение в лексикографски по-малко (което вече е било построено) и ако е така, не я добавяме, а преминаваме към разглеждане на следващата възможност. В [16] и [17] е направена и проверка за изоморфизъм на получените OOK и дизайни, защото е възможно

две мултипликативно еквивалентни решения да са изоморфни, но такива не са намерени. При проверката за изоморфизъм използваме обобщени множители, дефинирани от Muzychuk в статията му *A solution of the isomorphism problem for circulant graphs* (2004).

В [17] и [23] са класифицирани съответно оптимални $(v, 4, 2, 1)$ ООК с $v \leq 75$ и оптимални $(v, 5, 2, 1)$ ООК с $v \leq 114$. Даден е и по един оптимален ООК за някои стойности на v извън обсега на класификацията. В [23] е разработен и паралелен вариант на генериращия алгоритъм и част от резултатите са получени на паралелния компютър BlueGene.

ООК с еднакви авто- и крос-корелационен параметър (означават се (v, k, λ, λ) ООК или (v, k, λ) ООК) могат да се разглеждат и като двоични циклично-пермутационни (v, k, λ) константно тегловни кодове. Съвършените $(v, k, 1)$ ООК съответстват на 2-$(v, k, 1)$ циклични дизайни и на $(v, k, 1)$ циклични разностни фамилии.

Обект на [16] и [18] са съответно класифицациите на оптимални $(v, 4, 1)$ ООК с $v \leq 76$ и оптимални $(v, 3, 1)$ ООК с $v \leq 61$. Преди това бяха известни класификационни резултати за 2-$(v, 4, 1)$ циклични дизайни с $v \leq 64$ и за 2-$(v, 3, 1)$ циклични дизайни с $v \leq 57$. В [16] са построени с точност до изоморфизъм всички циклични 2-$(73, 4, 1)$ и 2-$(76, 4, 1)$ дизайни, а в [18] мултипликативно нееквивалентните циклични 2-$(61, 3, 1)$ дизайни. На тези дизайни съответстват и циклични разностни фамилии.

В [20] са събрани класификационни резултати за $(v, k, 1)$ циклични разностни фамилии с $k \leq 11$ и малки v, които получаваме с помощта на същия алгоритъм.

Публикациите от тази група са цитирани общо 4 пъти.

София

28. 06. 2013 г.

Подпис:

/Светлана Топалова/