Авторска справка
за научните приноси

на

Стела Димитрова Железова,
гл. асистент в секция Математически основи на информатиката,
Институт по математика и информатика, БАН

по конкурс за доцент по специалност 01.01.12 информатика
(компютърни методи за изследване на комбинаторни структури)

Пълният списък на научните публикации включва общо 23 заглавия.

За участие в конкурса са представени 14 публикации, като от тях:

- 4 публикации в международни научни периодични списания с импакт-фактор;
- 3 публикации в реферирани научни периодични списания;
- 3 публикации в реферирани сборници на международни конференции;
- 4 публикации в сборници на национални форуми.

Пет от представените публикации са използвани в дисертационния труд за получаване на образователната и научна степен "Доктор". Девет от представените публикации са след дисертационния труд, от тях 2 са в международни научни периодични списания с импакт-фактор и 3 са в реферирани сборници на международни конференции. Приносите на кандидата се отнасят към научната област 01.01.12 – информатика и включват разработване на алгоритми и софтуер за изследване на комбинаторни 2-дизайни, свързаните с тях паралелизми на крайни проективни пространства и приложението на тези комбинаторни структури.

Комбинаторните дизайни и крайните геометрии са интензивно изследвани поради многобройните им приложения в статистическите експерименти, теория на кодирането и криптографията. Комбинаторните структури могат да са в основата на анонимни *(2,q+1)*-прагови схеми за криптографията (Kishimotoa и др., 2002; Stinson, 2004), синхронен достъп до многолентов канал (Colborn и др., 1999) и безусловно сигурни схеми за разпределение (Blundo и др., 2002).

Алгоритми и методи от теория на дизайните успешно могат да се използват за решаване на някои практически проблеми. Първата European Study Group with Industry организирана в България през 2013г. успешно показа как теоретичните знания могат

да са от полза на малки български фирми. В [10] е показано едно такова приложение – кодиране на специфичен вид данни с цел минимизиране на времето за обработка и комуникация. Дадена е лесна и бърза процедура за конвертиране на данните от основен в кодиран вид и обратно.

В криптографията биективните субституционни кутии са основен обект на алгоритмите за симетрично шифриране. Знанията за дизайни и кодове са приложени при решаване на проблема за намиране на ефективна метрика за качествата на субституционните кутии в процеса на генерирането им с генетични алгоритми в [12], на следващото издание на European Study Group with Industry в България.

Един от важните критерии за качествата на субституционна кутия е нейната нелинейност. Тя се определя от спектралните коефициенти в матрицата на спектъра на Walsh-Hadamard. Предложени са различни начини за пресмятане на оценъчната функция, нужна за работата на генетичния алгоритъм, т.е. колко близо до оптимална за тези параметри е получената субституционна кутия. Трудността на проблема тук идва от това, че се разглеждат всички линейни комбинации на съответните координатни булеви функции. С нарастване на размера на субституционната кутия размерът на матрицата на спектъра на Walsh-Hadamard нараства толкова, че ако оценъчната функция не е достатъчно добра и достатъчно бърза, изчисленията не могат да приключат за разумно време. Също така използваните алгоритми трябва да се подбират много внимателно с оглед баланс на заета памет и на бързодействието.

Един комбинаторен дизайн е двойно разрешим, ако притежава поне една двойка взаимно ортогонални резолюции. Специфичните свойства на двойно разрешимите дизайни могат да бъдат използвани в статистически и криптографски приложения и приложения за тестване на софтуер, което обуславя интереса към тяхната класификация. Множества от взаимно ортогонални резолюции могат да се използват например при конструирането на перфектни схеми за разпределение на секрета (Seberry и др. 1996, 1998). Криптографското приложение на резолюциите на дизайн често произлиза от това, че всеки паралелен клас на резолюцията се определя еднозначно, от който и да е негов блок, а блокът от своя страна – от подходящо подмножество на множеството от точките си. По подобен начин паралелен клас на множество от ортогонални резолюции зависи от двойка свои блокове. Ако се разполага с класифицирани резолюции и множества от ортогонални резолюции на дизайни, те лесно могат да се тестват при разработката на дадено приложение и да се избере най-подходящата конфигурация. Затова в [11] е предложена първата класификация на двойно разрешими дизайни с малки параметри и техните множества от ортогонални резолюции.

Инцидентността на точките и *t*-мерните подпространства на *PG(d,q)* дефинира 2-дизайн, т.е. точките на дизайна отговарят на точките на проективното пространство, а блоковете му съответно на неговите *t*-мерни подпространства. Съществува взаимно еднозначно съответствие между паралелен клас от резолюция на този дизайн и *t*-спред и между резолюция на дизайна и *t*-паралелизъм. Обикновено 1-спредовете (1-паралелизмите) се наричат само спредове (паралелизми). Паралелизми се използват при конструирането на кодове с константна размерност (Silberstein и Etzion, 2011).

Класификационните задачи за конкретни параметри са решавани с помощта на компютър. Конструирането на комбинаторните структури се основава на алгоритми за изчерпващо търсене с връщане и съответно необходимото време нараства експоненциално с нарастването на параметрите. Написването на достатъчно ефективен алгоритъм за дадено множество от параметри не е тривиална задача. Това е причина компютърните методи за изследване на комбинаторни конфигурации да са не по-малко интересни от получените с тях резултати.

Изследванията на комбинаторните структури в представените за конкурса публикации са в следните направления:

- метод за класификация на двойно разрешими дизайни;
- ортогоналност на резолюции на дизайни и на паралелизми на проективни пространства;
- транзитивност на групата от автоморфизми на паралелизъм върху спредовете му;
- транзитивност и цикличност на групата от автоморфизми на паралелизъм върху точките на проективното пространство;
- регулярност на спредове и паралелизми;
- приложения на комбинаторните структури в криптографията.

В [11] в резултат на изследването на двойно разрешими дизайни е разработен метод за тяхната класификация. До тази работа са изследвани основно въпросите по съществуване на двойно разрешими дизайни. Изчерпателен обзор на методите за конструиране на разрешими дизайни и постигнатите резултати е включен в Classification algorithms for codes and designs на Kasski и Östergård, 2006. Според разработения метод подходящият ред за конструиране на двойно разрешими дизайни, от гледна точка на класифицирането им е следният:

- конструиране на неизоморфни резолюции, които притежават ортогонална такава;

- класификация на съответните дизайни (един дизайн може да има няколко неизоморфни резолюции);
- класификация на неизоморфните множества от взаимно ортогонални резолюции на съответния дизайн.

Някои подробности относно реализацията на метода са представени в [4]. Методът е по-ефективен, ако се намери начин за ранно отхвърляне на неподходящите решения в първата му точка. Разработени са две конструкции за тестване на решенията за ортогоналност.

В допълнение на конструктивната част на метода, за повишаване на ефективността му, в [1] е анализирана структурата на резолюциите, които притежават поне една ортогонална резолюция. Установени са теоретични ограничения за структурата на паралелните класове на резолюциите, които притежават поне една ортогонална резолюция за конкретни параметри. За целта са използвани матрици на пресичане на паралелните класове. Такива матрици са използвани от Morales и Velarde (2001, 2005) за конструиране на начална структура на резолюция на разглежданите от тях дизайни и от Kasski, Morales и Östergård (2003) за частична проверка на класификацията на разрешими 2-(14,7,12) дизайни. В [1] такива матрици за първи път са използвани при конструирането на двойно разрешими дизайни.

В [11] е представена първата пълна класификация на двойно разрешими дизайни с малки параметри. При класификацията на множествата от взаимно ортогонални резолюции за кратни дизайни (състоящи се от копия на дизайн без повтарящи се блокове) разработените конструкции и алгоритми се оказаха не достатъчно бързи. За такива параметри с използвания метод се получават твърде много решения за множествата от ортогонални резолюции на дизайна. Възникна въпроса дали от гледна точка на класификацията на тези множества, разрешимите дизайните не трябва да се разделят на различни класове, всеки с евентуално различно приложение. Тези проблеми доведоха до изследването ни в [7]. Там са изведени теоретични зависимости за броя на неизоморфните резолюции, притежаващи ортогонална и за броя на нееквивалентните множества от ортогонални резолюции на кратни дизайни (състоящи се от няколко копия на дизайн без повтарящи се блокове) от броя на нееквивалентните множества от ортогонални латински квадрати.

В резултат на установените зависимости са получени долни граници за броя на множествата от взаимно ортогонални резолюции за дизайни с два блока в паралелен клас. Те зависят от броя на нееквивалентните латински квадрати със страна m, който се знае за много стойности на m. От тях се вижда, че броят на неизоморфните резолюции, притежаващи ортогонална и броят на неизоморфните множества от

взаимно ортогонални резолюции е толкова голям, че класификацията им за такива параметри е невъзможна за разумно време.

За отсяване на изоморфните решения при конструиране на резолюции, притежаващи ортогонална е използван тест за минималност. Тестът и съответният софтуер е разработен от Топалова.

Проверка на коректността на получените резултати е осъществена като за подходящите параметри тестът за ортогоналност е направен и по двете конструкции, направена е различна софтуерна реализация на конструктивната част от метода от съавторите. Там, където е приложимо, софтуерът е използван за получаване на резултатите от изследванията на други автори.

Изследването на t-паралелизми на проективни пространства е направено от гледна точка на връзката им с комбинаторните дизайни и техните резолюции. Тъй като се изследват във връзка с конкретни групи от автоморфизми, методът и алгоритмите за класификацията им са различни от разработения метод за класификация на двойно разрешими дизайни.

За различните параметри спецификата на конкретната група от автоморфизми налага различен подход. Ако групата е силова, достатъчно е да изберем която и да е от съответния ред. Ако не е – разглеждаме съответната силова група от ред, кратен на търсения, намираме нейните подгрупи и класовете им на спрегнатост и разглеждаме действието на всеки представител на клас върху t-подпространствата на проективното пространство.

Конструирането на t-паралелизми с дадени автоморфизми ни позволява да не построяваме всички спредове (цялата резолюция), а само по един представител от орбита. В зависимост от конкретната група от автоморфизми, един t-спред може да се състои от t-подпространства от различни орбити или може да съдържа цели орбити от непресичащи се t-подпространства. Конкретната конструкция на t-спред и съответно на t-паралелизъм зависи изцяло от особеностите на търсената група от автоморфизми, затова решаването на такива задачи става със специфичен за конкретните параметри подход.

Обикновено броят на изоморфните решения е голям, в много случаи те не могат да се получат за разумно време. Затова съществена част от задачата за класификация на конкретните комбинаторни обекти е задачата за отделяне на еквивалентните решения. За тази цел при конструиране на t-паралелизмите използваме нормализатора на подгрупата, с която ги построяваме.

Най-често софтуерът за решаване на конкретни класификационни задачи, поради спецификата на проективните пространства, работи само за няколко близки множества от параметри. За да се избегнат грешки в програмите, за разглежданите параметри на проективни пространства, изчисленията са правени от съавторите по различни алгоритми. Софтуерът за определяне типа на спредовете е разработен от автора, затова е направена проверка за съвместимост с известните изследвания на други автори. В *PG(3,4)* е известно, че спредовете са три типа – регулярен, субрегулярен и нерегулярен. Броят на различните спредове от всеки тип е получен чрез тестване на множеството от всички изоморфни спредове и съвпада с дадения от Prince (Covering sets of spreads in *PG(3,q),* 2001).

Необходимият софтуер е написан на C++. За намиране на използваните подгрупи на групите от автоморфизми на разглежданите проективни пространства и техните нормализатори е използвана софтуерната система GAP, а в [14] за намиране на пълната група от автоморфизми на съответния дизайн е използван модула "Isomorphism and automorphism group" на програмата Q-Extension на проф.Илия Буюклиев.

Съществуват множество конструкции на *t*-спредове и *t*-паралелизми (например Denniston, Johnson, Penttila и Williams), а също така са проведени и много изследвания на вида на групите от автоморфизмите им. Обобщение на получените в тази област резултати може да бъде намерено в книгата *Combinatorics of Spreads and Parallelisms* на Johnson (2010). В $PG(2^n - 1,q)$ е известна конструкция на *t*-паралелизми на Beutelspacher, а в *PG(3,q)* – на двойка ортогонални паралелизми на Fuji-Hara. Преди [2], [3], [6], [8], [9] и [13] паралелизми със зададени автоморфизми са класифицирани с помощта на компютър в *PG(3,3)* и *PG(3,5)* (Prince, 1997, 1998) и в *PG(5,2)* (Stinson и Vanstone, Sarmiento).

В [2] са конструирани всички паралелизми на PG(3,4) с автоморфизми от ред 7. Преди тази работа *q=4* беше най-малкия ред на проективно пространство, за който нямаше класификация на паралелизми.

Един *t*-паралелизъм е транзитивен, ако притежава група автоморфизми, действаща транзитивно върху *t*-спредовете му. Една основна причина за интензивното изследване на *t*-спредове и *t*-паралелизми е връзката им с транслационните равнини. Получени паралелизми изследваме за ортогоналност, защото от множествата от взаимно ортогонални паралелизми на *PG(3,q)* може да се получи проективна равнина от ред *q(q+1)*.

Примери на транзитивни паралелизми са представени в *PG(3,q)* (Denniston, Penttila и Williams) и в *PG(5,2)* (Stinson и Vanstone). В книгата на Johnson е доказано,

че транзитивни *t*-паралелизми не могат да съществуват за $t > 1$. В [3] са класифицирани 2-паралелизмите с автоморфизми от ред 31 и сред тях са получени първите примери на транзитивни *t*-паралелизми за $t > 1$. След резултата в [3] Johnson и Montinaro в тяхната статия The transitive t-parallelisms of a finite projective space (2012) поправиха тази грешка. Също там несъществуването на транзитивни паралелизми в *PG(3,4)* е посочено като отворен проблем. За да получим паралелизъм в това проективно пространство са нужни 21 спреда, следователно, за да е транзитивен, той трябва да притежава автоморфизъм от ред най-малко 21, т.е. и автоморфизъм от ред 7. Отговор на въпроса за съществуване на транзитивни паралелизми в *PG(3,4)* даваме в [9]. Там показваме, че транзитивни паралелизми в *PG(3,4)* няма – всички конструирани паралелизми притежават пълна група от автоморфизми само от ред 7. Софтуерът за определяне на реда на пълната група от автоморфизмите е на Топалова. Конструираните паралелизми са класифицирани според типа на техните спредове, като сред тях има еднородни (състоящи се само от спредове от един и същи тип), но не и регулярни паралелизми. В [5] теоретично е показано несъществуването на транзитивни 2-паралелизми в PG(5,3).

В *PG(3,5)* са класифицирани транзитивните паралелизми от Prince (1998), като между тях са показани 2 регулярни паралелизма. Всички познати до момента регулярни паралелизми са от класа на Penttila и Williams *за PG(3,q), $q \equiv 2 \pmod 3$*. Съществуването на други регулярни паралелизми е отворен въпрос. Това мотивира изследването ни в [8]. Там са конструирани паралелизмите с автоморфизъм от ред 13, но сред тях няма регулярни.

Един паралелизъм е транзитивен върху точките, ако притежава група от автоморфизми, действаща транзитивно върху тях. Един паралелизъм е частичен – с дефицит *m*, ако спредовете му са с *m* по-малко от $1+q+q^2$. Частичен паралелизъм с дефицит 1 се разширява по единствен начин до паралелизъм. Транзитивните частични паралелизми с дефицит 1 в *PG(3,q)* са изследвани от Johnson (2001), който е конструирал един безкраен клас такива частични паралелизми за $q=p^r$, p – нечетно. Преди изследването, направено в [13], примери на транзитивни частични паралелизми с дефицит 1 в *PG(3,4)* не бяха известни. Ако съществуват транзитивни върху точките или транзитивни частични паралелизми с дефицит 1 в *PG(3,4)*, то те трябва да притежават автоморфизми от ред 5. Затова в [6] и [13] са конструирани всички паралелизми с такива автоморфизми. Класифицирани са според вида на спредовете им и пълната им група от автоморфизми.

За тези параметри спрегнатите групи от ред 5 са 3 на брой. При голяма част от паралелизмите съответната група фиксира точно един спред. От тях най-интересни са тези с регулярен фиксиран спред, защото е доказано, че транзитивните частични

паралелизми с дефицит 1 теоретично са между тях. Установено е, че за 4 от тях, пълната им група от автоморфизми е от ред 960 и действа транзитивно върху спредовете, т.е. представени са първите 4 примера на транзитивни частични паралелизми с дефицит 1 в *PG(3,4)*.

Транзитивните частични паралелизми с недостиг, получени в [13] отговарят на теоретичните изследвания на Biliotti, Jha, Johnson (2005) и Diaz, Johnson, Montinaro (2008). Те са с пълна група от автоморфизми с нормална подгрупа от ред $q^2=16$ и спредът, който допълва частичния паралелизъм е регулярен и неизоморфен на спредовете на транзитивния частичен паралелизъм с дефицит 1.

Две от групите от ред 5 не фиксират точки от проективното пространство, следователно, ако има транзитивни върху точките паралелизми, те ще са между построените с тези групи. Направеното изследване показа, че от тях няма транзитивни върху точките паралелизми. Този резултат проверихме като опитахме да построим паралелизмите с автоморфизми от ред 17 за същото проективно пространство и установихме, че такива не са възможни, поради спецификата на групата.

Един паралелизъм е цикличен върху точките, ако е инвариантен относно цикъла на Singer. Такива паралелизми са класифицирани в *PG(5,2)* с помощта на компютър от Sarmiento (2000, 2002), в *PG(7,2)* от Hisida и Jimbo (1998), показана е конструкция в *PG(9,2)* от Braun (2006). Циклични върху точките паралелизми в *PG(3,7)* са разглеждани в [14]. Особеното при този случай е, че поради дължините на орбитите на правите под действие на групата се наложи конструиране на спред от прави от една и съща орбита по специална конструкция – без да се взема цялата орбита. В резултат установихме, че в това проективно пространство не съществуват циклични върху точките паралелизми.

Получените класификационни резултати са достъпни в интернет, за да са удобни за използване от интересуващите се.

23.03.2015г. Подпис:

гр.София Стела Железова