Алгебрични и комбинаторно-геометрични задачи в теория на кодирането

КП-06-Русия/33 от 17.12.2020г.

Научни резултати

Работен пакет 1. Изследвани са кодове с две разстояния – d и n (n е дължината на кода). Класифицирани са всички такива адитивни кодове, както и кодовете, които са ортогонални масиви със сила поне 2. Получени са и са изследвани границите на линейното програмиране за случая на разстояния d и n. Получени са и нови граници в различни съотношения, свързващи параметрите n (дължина на кода), d (минимално разстояние) и q (размер на азбуката), като резултати за двоичния случай са обобщени за произволно q>2. Резултатите от тази дейност са публикувани в работа, която е съвместна между членове на колективите по проекта от българска и руска страна (П. Бойваленков и В. Зиновиев).

Изследвани са оптимални сферични кодове, които са сферични 7-дизайни с 4 разстояния. Хипотезата, че сферични 7-дизайни с 4-разстояния съществуват само в известните досега случаи, е доказана за всички размерности, по-малки от 1000.

Получени са и са изследвани универсални граници за специален случай на енергия (задача на Фейеш Тот) на кодове с относително малка (спрямо размерността) мощност. В редица от случаите на кодове с две разстояния е показано, че горните и долните граници дефинират малък интервал от възможни енергии и следователно известни кодове с две разстояния, свързани със силни регулярни графи (като например кодовете на Сиделников и кодовете на Кердок), са асимптотично оптимални. Получените граници могат да се разгледат и като мярка на отдалеченост на добри кодове от универсалната оптималност в смисъла на Кон-Кумар.

Работен пакет 2. Разработен е софтуер за конструиране на дизайни на Менон, който работи успешно, но за параметри по-малки от очакваните.

Конструирани са $(v,k,2,1)$ оптични ортогонални кодове (ООК) с максималния възможен брой кодови думи за $k=6$ и дължини $v<126$, както и за $k=7$ и $v<104$. Резултатите показват, че известните до момента горни граници за броя на кодовите думи на $(v,k,2,1)$ ООК с $k>5$, се достигат от много малък брой ООК.

Конструирани са и са класифицирани и изследвани паралелизми с различни параметри. Проективните пространства с размерност три PG(3,q) са обект на интензивно изследване, повечето известни конструкции на паралелизми са за PG(3,q). От особен интерес са транзитивните паралелизми с един недостиг. Съществува безкраен клас от такива паралелизми в PG(3,q), представен от Johnson. Конструирани са паралелизми на PG(3,5), инвариантни относно група от автоморфизми от ред 25. С точност до спрегнатост има

две подгрупи от ред 25 на групата от автоморфизми на проективното пространство. При изследване на свойствата на получените паралелизми са намерени 12 транзитивни с един недостиг, два от тях от известния клас на Johnson.

Конструирани са и са изследвани паралелизми в проективното пространство от най-малък ред с размерност пет. До тези изследвания, в PG(5,2) бяха класифицирани транзитивните върху точките паралелизми (Stinson и Vanstone, 1986 и Sarmiento, 2000) и цикличните паралелизми (Железова). Доказано е, че с точност до спрегнатост има една циклична подгрупа от ред 21, която може да бъде група от автоморфизми на паралелизъм. Разглежданата група фиксира до десет спреда в паралелизъм, като частичният паралелизъм с десет фиксирани спреда е единствен. Построени са и са изследвани свойствата на всички паралелизми, които се получават при разширяването на този частичен паралелизъм. Класификационни резултати са достъпни на страниците на авторите в интернет за евентуални приложения.

Работен пакет 3. Разработен е алгоритъм за еквивалентност на кодове, базиран на характеристичен вектор на пораждаща матрица. В основата му се използва факта, че два линейни кода са еквивалентни, ако характеристичните им вектори са в една орбита относно групата от автоморфизми на нормализираната матрица от кодови думи на симплексния код.

Разрабботен е алгоритъм за намиране радиус на покритие на линейни кодове. За недвоични кодове е използвана бързата дискретна трансформация на Виленкин-Крестенсон. Разработеният алгоритъм е q-1 (q е размерът на азбуката) пъти по-бърз от известните досега алгоритми в това направление и много удобен за изследване на кодове, при които дължината на кодовата дума е много по-голяма от размерността.

Изследвани са кодове, свързани с линейни двоични кодове, достигащи границата на Грей-Ранкин. Такива кодове се асоциират с двойнотегловни, самоортогонални кодове и с много други комбинаторни структури с интересни свойства. В изследването се изучава връзката между шест безкрайни фамилии самоортогонални кодове с две и три тегла. На базата на получените резултати е разработен метод за конструиране и е направена класификация за кодове с определени свойства.

Продължи разработването на библиотека от функции за паралелни пресмятания с приложения в теория на кодирането и криптографията. От особено значение за алгоритми е ефективността на компилаторите при оптимизация и паралелизация. Направен е сравнителен анализ на характеристиките и ефективността на най-разпространените компилатори на C/C++ при използване на разширените процесорни инструкции.

Доказан е резултат, касаещ различността на сумите на Клостерман над крайни полета с характеристика 3. Във връзка с тази тематика е получен резултат за несъизмеримостта на ъглите на сумите на Клостерман над крайни полета с константата пи.

Работен пакет 4. Изследвани са спорадичните (3 mod 5)-арки в PG(3,5) с мощности, съответно, 128, 143, 168, конструирани с помощта на компютър от Курц, Ланджев и Русева. Изследвани са безкрайни класове от нелифтвани (t mod q) в геометрии с

произволна размерност над произволни полета с нечетна характеристика. Получена е геометрична конструкция на трите нелифтвани (3 mod 5) арки в PG(3,5) с мощности 128, 143 и 168. Оказва се че първата е свързана с една от пълните 20-шапки на Абатанджело, Корчмарош и Ларато, докато другите две са свързани с двете квадрики в PG(3,5). Конструкцията, използваща квадрики, се обобщава в геометрии от прозволна размерност, над произволно поле с нечетна характеристика. Тези изследвания водят до преформулиране на основната хипотеза за (t mod q) арки. Сега тя гласи, че всички (t mod q)-арки в геометриите с достатъчно голяма размерност над полета с нечетна характеристика са или лифтвани или плучени от квадрики с обобщена от нас конструкция.

Изследвана е задачата за намиране на максималната мощност на арка в проективна равнина на Йелмслев над малки верижни пръстени с индекс на нилпотентност 2. Подобрени са таблиците на най-добрите арки в проективни равнини на Йелмслев над малки верижни пръстени. Доказани са и нови граници за максималната мощност на (k,n)-арка по отношение на стандартната метрика и хомогенната метрика на Хайзе. Тези резултати автоматично водят до конструирането на нови добри кодове над верижните пръстени над малки полета.

Изследвана е задачата за намиране на максимална антиверига в решетката на подмодулите над произволен (несвободен) верижен пръстен. Доказани са теореми от тип Шпернер за решетката на подмодулите на несвободни модули над крайни верижни пръстени. Тези изследвания могат да се разглеждат като продължение на резултатите на Р. Стенли и Ю. Уонг за решетката на подгрупите на подмодулите на свободен модул над краен верижен пръстен. Доказано е, че решетката от подмодулите на модули от тип 21^n над верижни пръстени с индекс на нилпотентност 2 е от Шпернеров тип само за четни стойности на n. За нечетни n максимална антиверига се състои от елементи с различни рангове. Доказано е, че и в двата случая максималната верига е единствена. Подобни резултати са доказани и за решетката от подмодулите на несвободен модул от тип $m1^n$ с произволен индекс на нилпотентност.