МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Кафедра загальної математики

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: **«ГЕОМЕТРИЧНІ ОСНОВИ РОЗВ'ЯЗАННЯ ДЕЯКИХ КЛАСІВ КОМБІНАТОРНИХ ЗАДАЧ»**

Виконала: студентка 2 курсу, групи 8.1119
спеціальності 111 математика
(шифр і назва спеціальності)
освітньої програми математика
(назва освітньої програми)
М. С. Ткачова
(ініціали та прізвище)

Керівник доцент кафедри загальної математики, доцент, к.ф.-м.н. Стєганцева П. Г.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Рецензент доцент кафедри фундаментальної математики, доцент, к.ф.-м.н. Красікова І. В.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Запоріжжя
2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет математичний

Кафедра загальної математики

Рівень вищої освіти магістр

Спеціальність 111 математика
(шифр і назва)

Освітня програма математика

ЗАТВЕРДЖУЮ

Завідувач кафедри загальної математики, к.ф.-м.н., доцент
_____ Зіновєєв І.В.
(підпис)

« ____ » _____ 2020 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТЦІ

Ткачовій Марії Сергіївні
(прізвище, ім'я та по-батькові)

1. Тема роботи (проекту) Геометричні основи розв'язання деяких класів комбінаторних задач

керівник роботи (проекту) Стєганцева Поліна Георгіївна, к.ф.-м.н., доцент
(прізвище, ім'я та по-батькові, науковий ступінь, вчене звання)

затверджені наказом ЗНУ від «20» 05 2020 року № 576- С

2. Строк подання студентом роботи 01.12.2020

3. Вихідні дані до роботи 1. Постановка задачі.
2. Перелік літератури.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Різницеві множини та їх зв'язок з комбінаторними задачами
Аксіоматичні теорії скінчених геометрій, використання геометричних конфігурацій

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
презентація

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 22.05.2020

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Розробка плану роботи.	22.05.2020	
2.	Збір вихідних даних.	15.06.2020	
3.	Обробка методичних та теоретичних	12.08.2020	
	джерел.		
4.	Розробка першого розділу.	03.09.2020	
5.	Розробка другого розділу.	11.10.2020	
6.	Оформлення та нормоконтроль	10.12.2020	
	кваліфікаційної роботи.		
7.	Захист кваліфікаційної роботи.	18.12.2020	

Студент _____ М. С. Ткачова
(підпис) (ініціали та прізвище)

Керівник роботи _____ П. Г. Стєганцева
(підпис) (ініціали та прізвище)

Нормоконтроль пройдено

Нормоконтролер _____ О. Г. Спиця
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Кваліфікаційна робота магістра «Геометричні основи розв’язання деяких класів комбінаторних задач» : 43 с., 16 рис., 2 табл., 9 джерел.

БЛОК-СХЕМА, ЕКВІВАЛЕНТНІСТЬ, КОД ГЕМІНГА, КОНФІГУРАЦІЯ, КРИПТОГРАФІЯ, МАТРИЦІ БЕЗ ПРЯМОКУТНИКІВ, СКІНЧЕННА МНОЖИНА, ТРІЙКИ ШТЕЙНЕРА.

Об’єкт дослідження – класи комбінаторних задач.

Мета роботи: дослідження методів застосування геометричних та комбінаторних конфігурацій до розв'язання задач.

Методи дослідження – аналітичний, оглядовий.

Тематика сучасної комбінаторики різноманітна: нумераційні і екстремальні задачі, проблеми існування, вибору і розташування, геометричні та алгебраїчні інтерпретації.

Основні задачі роботи:

а) вивчити теоретичні аспекти для розкриття теми;

б) побудувати приклади комбінаторних конфігурацій – різницевих множин, блок схем;

в) описати класи геометричних конфігурацій;

г) навести приклади комбінаторних задач та еквівалентних їм геометричних задач.

Робота може зацікавити всіх, хто вивчає комбінаторику, скінченні геометрії, розв’язує олімпіадні задачі.

SUMMARY

Master’s Qualification Thesis «Geometric bases for the determination of classes of combinatorial tasks»: 43 pages, 16 figures, 9 references.

BLOCK DIAGRAM, CONFIGURATION, EQUIVALENCE, FINITE SET, HEMMING CODE, MATRICES WITHOUT RECTANGLES, STEINER TRIPLETS.

The object of research is classes of combinatorial problems.

The aim of the study is to research of methods of solving combinatorial problems on finite and affine planes.

The methods of research are analytical, survey.

Topics of modern combinatorics are diverse: numbering and extreme problems, problems of existence, choice and location, geometric and algebraic interpretations.

The main tasks of the work:

a) to study the theoretical aspects to reveal the topic;

b) build examples of combinatorial configurations–difference sets, block diagrams;

c) describe the classes of geometric configurations;

d) give examples of combinatorial problems and equivalent geometric problems.

The work can be of interest to everyone who studies combinatorics, finishes geometry, solves olympic problems.

ЗМІСТ

ВСТУП

В математиці часто зустрічаються задачі, які можна розв’язувати різними методами. Вибір методу доволі часто не випливає з умови задачі і цей процес є, в деякому сенсі, творчим. Щоб набути відповідні навички, треба зрозуміло якомога більше розв’язувати задач, намагатись розв’язувати одну і ту саму задачу різними методами. Це допоможе розглянути ситуацію з різних сторін, глибше усвідомити деталі. Як наслідок, може виникнути ідея узагальнення задачі, поширення її на інші множини об’єктів.

Центральною задачею комбінаторної теорії можна вважати задачу про розміщення об’єктів у відповідності з окремими правилами та знаходження числа методів, якими це може бути зроблено. Якщо правила виконані, то основною задачею є знаходження числа таких розміщень. Якщо правила не виконуються, то виникає питання про існування таких розміщень та методів їх побудови.

Способи розв’язання комбінаторних задач можна поділити на дві групи: «формальні» і «неформальні». При «формальному» підході для розв’язання потрібно визначити характер комбінаторного об’єкту, вибрати відповідну формулу або комбінаторний принцип, підставити числа і обчислити результат. Результатом є кількість можливих варіантів, самі ж варіанти в цьому випадку не перераховуються.

«Неформальний» спосіб розв’язання полягає в тому, що на першому етапі розв’язання формується спосіб перерахування різних комбінаторних конфігурацій. Іноді цей спосіб елементарний, який не вимагає знання означень і формул, наприклад, безпосередній перебір.

В кваліфікаційній роботі розглядаються геометричні та комбінаторні підходи до розв’язання певного класу задач. У зв’язку з цим розглядаються різницеві множини, блок-схеми, їх зв’язок з булевими матрицями. Наводяться приклади застосування геометричних конфігурацій на скінченній проективній

площині. Показується, як для розв’язання комбінаторних задач використовуються властивості геометричних фігур, і навпаки, як для розв’язання геометричних задач використовуються комбінаторні конфігурації.

1 КОМБІНАТОРНІ ЗАДАЧІ, ПОВ'ЯЗАНІ З ПОНЯТТЯМ РІЗНИЦЕВОЇ МНОЖИНИ

1.1 Поняття різницевої множини

Означення 1.1 Множина D, що складається з k лишків $a_1, \dots, a_k$ за модулем v, називається $(v, k, \lambda)-$ різницевою множиною, якщо для кожного d≠0 $(mod\ v)$ існує точно λ упорядкованих пар $(a_i, a_j), a_i, a_j \in D$, таких, що $a_i - a_j \equiv d\ (mod\ v)$.

Означення 1.2 Множина D, що складається з k різних елементів $a_1, \dots, a_k$ групи G порядку v, називається груповою $(v, k, \lambda)-$ різницевою множиною, якщо виконується одна з умов:

а) для будь-якого d∈ $G, d \neq 1$, існує λ впорядкованих пар (a_i, a_j), $a_i, a_j \in D$ таких, що a_i, a_j^{-1}=d;

б) для будь-якого d∈ $G, d \neq 1$, існує λ впорядкованих пар (a_i, a_j), $a_i, a_j \in D$ таких, що a_i^{-1}, a_j=d.

Теорема 1.1 Множина D з k лишків $a_1, \dots, a_k$ по модулю v, є (v, k, λ)-різницева множина тоді і тільки тоді, коли множина $B_i = \{a_1 + i, \dots, a_k + i\}$ лишків по модулю v, $i = 0, \dots, v-1$, є блоками циклічної (v, k, λ)- блок-схеми B.

Означення 1.3 Блок-схемою називається таке розміщення v різних елементів по b блокам з k різних елементів кожен, що кожен елемент належить рівно r блокам і кожна пара різних елементів з'являється точно в λ блоках. Якщо $r = b$, то схема називається симетричною.

Означення 1.4 Дві блок-схеми B та B' називаються ізоморфними, якщо існує взаємно однозначне відображення α елементів та блоків B на елементи та блоки B', таке, що $x_i -$ елемент, а B_J- блок схема B та виконуються умови:

а) α: $x_i \to x_i' = (x_i)\alpha -$ елемент B′;

б) $\alpha: B_j \to B_j' = (B_j)\alpha -$ блок B′, то $x_i \in B_j$ тоді і тільки тоді, коли $(x_i)\alpha \in (B_j)\alpha$.

Означення 1.5 Автоморфізмом блок-схеми називається перестановка точок, яка переводить кожен блок в блок. Якщо $B' = B$, то відображення α називається автоморфізмом блок схеми B.

Автоморфізм будь-якої блок схеми B утворює групу, якщо α_1 та α_2- два автоморфізми B, то добуток $\alpha_1\alpha_2$ також утворюють автоморфізм і обернене відображення α_1^{-1} та α_2^{-1}- теж буде автоморфізмом.

Приклад 1.1 Розглянемо блок-схему B з лишками 0, 1, …, 12 (mod 13) в якості елементів та блоків B_i, i=0, …, 12 (mod 13):

$$B_0: 0, 1, 3, 9;$$
$$B_1: 1, 2, 4, 10;$$
$$B_2: 2, 3, 5, 11;$$
$$B_3: 3, 4, 6, 12;$$
$$B_4: 4, 5, 7, 0;$$
$$B_5: 5, 6, 8, 1;$$
$$B_6: 6, 7, 9, 2\ ;$$
$$B_7: 7, 8, 10, 3;$$
$$B_8: 8, 9, 11, 4;$$
$$B_9: 9, 10, 12, 5;$$
$$B_{10}: 10, 11, 0, 6;$$
$$B_{11}: 11, 12, 1, 7;$$
$$B_{12}: 12, 0, 2, 8.$$

В даному випадку $\alpha: i \to i + 1, B_i \to B_{i+1}$ є автоморфізмом схеми B, який переставляє елементи та блоки по циклу довжини 13.

Симетрична блок-схема B з параметрами v, k, λ ((v, k, λ)-блок-схема) називається B -циклічною, якщо B має автоморфізм α, який переставляє

елементи та блоки по циклу довжини v. Розглянемо блок $B_5 = \{5, 6, 8, 1\}$, він має властивість, що $4 \cdot 3 = 12$ різниць різних елементів в цьому блоці, відмінні від 0 і зустрічаються рівно один раз.

$$-1 = 5 - 6 \equiv d(mod\ 13) \quad -4 = 1 - 5 \equiv d(mod\ 13)$$
$$-3 = 5 - 8 \equiv d(mod\ 13) \quad -5 = 1 - 6 \equiv d(mod\ 13)$$
$$4 = 5 - 1 \equiv d(mod\ 13) \quad -7 = 1 - 8 \equiv d(mod\ 13)$$
$$1 = 6 - 5 \equiv d(mod\ 13) \quad 3 = 8 - 5 \equiv d(mod\ 13)$$
$$-2 = 6 - 8 \equiv d(mod\ 13) \quad 2 = 8 - 6 \equiv d(mod\ 13)$$
$$5 = 6 - 1 \equiv d(mod\ 13) \quad 7 = 8 - 1 \equiv d(mod\ 13)$$
$$\pm 1, \pm 3, \pm 4, \pm 5, \pm 7 \equiv d(13)$$

Тому $\{5,6,8,1\}$ є (13,4,1)- різницева множина, де $v = 13, k = 4, \lambda = 1$.

Означення 1.6 Множина $D = \{a_1, \ldots, a_k\}$ з k різних елементів множин $\{0, \ldots, v - 1\}$ називається (v, k, λ)- циклічною різницевою множиною, якщо для кожного $d \neq 0$ знайдеться рівно λ таких впорядкованих пар (a_i , a_j), що $a_i - a_j \bmod v = d$. Зв'язок таких множин з блок-схемами вказує теорема.

Теорема 1.2 Множина $D = \{a_1, \ldots, a_k\} \subset \{0,1, \ldots, v - 1\}$ є циклічною (v, k, λ)- різницевою множиною тоді і тільки тоді, коли множина $B_i = \{a_1 + i\ mod\ v, \ldots, a_k + i\ mod\ v\} \subset \{0,1, \ldots, v - 1\}$, де $i = 0, 1, \ldots, v - 1$, є блоками.

Теорема 1.3 Властивості 1 та 2 групової різницевої множини D еквівалентні. Якщо B є (v, k, λ)- блок-схема, яка допускає групу G порядку v у якості регулярної групи автоморфізму та, якщо $(x)\, a_1, \ldots, (x)a_k$- елементи блоку B_0, то $D = \{a_1, \ldots, a_k\}$ є груповою (v, k, λ)- різницевою множиною. [2]

Множина $D = \{a_1, \ldots, a_k\}$ з k різних елементів множини $\{0, \ldots, v - 1\}$ називається (v, k, λ)-циклічною різницевою множиною, якщо для кожного $d \neq 0$ існує відповідно λ таких упорядкованих пар (a_i, a_j), що $a_i - a_j \equiv d\ (mod\ v)$.

Множина $D= \{a_1, \dots, a_k\} \subset \{0,1, \dots, v-1\}$ є циклічною $(v,\ k,\ \lambda)$-різницевою множиною тоді і тільки тоді коли множина $B_i = \{a_1 + i\ mod\ v, \dots, a_k + i\ mod v\} \subset \{0,1, \dots, v-1\}$, де $i = 0, \dots, v-1$, є блоками.

Теорема 1.4 Нехай D–множина, що складається з k лишків $a_1, \dots, a_k$ по модулю v. Існує (v, k, λ)- різницева множина тоді і тільки тоді, коли множини $B_i = \{a_1 + i, \dots, a_k + i\}$ лишків по модулю $v, i = 0, \dots, v-1,$ є блоками циклічної (v, k, λ)- блок-схеми B.

Теорема 1.5 (Зінгера) В проективній геометрії $PG(2, q), q = p^r$, прямі, взяті в якості блоків, утворюють симметричну блок-схему з параметрами $v = q^2 + q + 1, k = q + 1, \lambda = 1.$ Ця схема циклічна, а точки будь якої прямої визначають циклічну (v, k, λ)- різницеву множину. [3]

Приклад 1.2 Розглянемо (31,6,1)–різницеву множину, побудовану за допомогою теореми Зінгера: {0,1,15,19,21,24}.

Можна, обчислюючи всі 30 попарних різниць по модулю 31, безпосередньо переконатися, що всі вони різні і кожне число від 1 до 30 з'являється серед них рівно один раз. Застосування побудованої різницевої множини до прикладу 1.2 на рисунку 1.1.

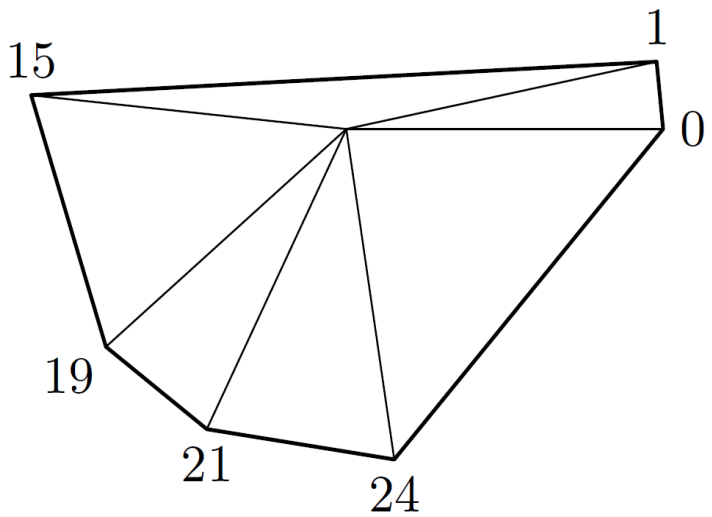

Рисунок 1.1– Шестикутник з вершин правильного 31-кутника без трапецій та рівнобедрених трикутників

Обертаючи цей шестикутник навколо центру даного правильного 31-кутника, отримуємо 31 «вписаних» шестикутників, будь-які два з яких мають тільки одну спільну вершину. Отримаємо 31 множину, кожна з яких збігається з множиною вершин відповідного шестикутника. Ці множини утворюють модель проективної площини 5-го порядку. [1]

Приклад 1.3 У правильному 43-кутнику відмічені 7 вершин. Довести, що існує трапеція або трикутник з вершинами в цих точках. Можна виділити 6 вершин так, що не існує ні трапеції, ні рівнобедреного трикутника з вершинами в цих точках.

Якби якийсь семикутник не містив ні трапеції, ні рівнобедреного трикутника, то існувала б (43, 7, 1)- різницева множина, а її не існує згідно теореми Брука-Райзера. [1]

Теорема стверджує, що якщо (v , b , r , k ,λ) –блок-схема існує з $v = b$ (симетрична конструкція блоку), то:

а) якщо v парне, то k–λ–квадрат;

б) якщо v непарне, то таке рівняння має нетривіальний розв'язок:

$$x^2 - (k-\lambda) y^2 - (-1)^{(v-1)/2} \lambda z^2 = 0.$$

Множина {0, 1, 15, 19, 21, 24} перетворюється в різницеву по модулю 43 множину {0, 1, 27, 31, 33, 36}, якщо збільшити інтервал від 1 до 15, перетворивши його в інтервал від 1 до 27. Безпосередньо можна переконатися, що всі попарні різниці чисел цієї множини по модулю 43 різні. Відповідний даній множині шестикутник на рисунку 1.2.

Приклад 1.4 Дано правильний 26-кутник, чи можна відмітити 8 вершин так, що не існуватиме ні трапеція, ні трикутник з вершинами в цих точках? А чи можна це зробити так, щоб не було ще й прямокутників?

Для перевірки досить для кожної пари не діаметрально протилежних вершин (таких пар $4 \cdot 7 - 4 = 24$) знайти найменшу з двох дуг даного кола з кінцями в цих вершинах, і переконатися, що всі ці дуги попарно різні за

довжиною, за винятком пар діаметрально протилежних дуг. Так як згаданих пар 12, досить обчислити довжини 12 дуг. Якщо дуга з'єднує вершини з номерами i, j, то в якості її довжини можна взяти мінімальне з чисел $|i–j|$, $26–|i–j|$. Так, дійсно можливо отримати 26-кутник без трапецій та рівнобедрених трикутників.

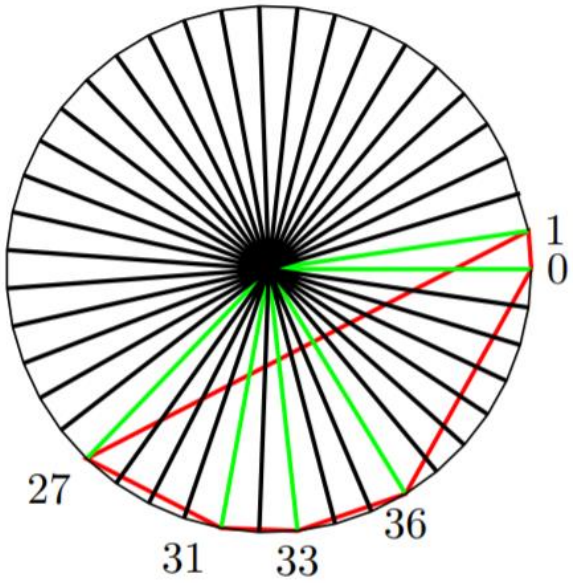

Рисунок 1.2 – Шестикутник з вершин правильного 43-кутника без трапецій і рівнобедрених трикутників

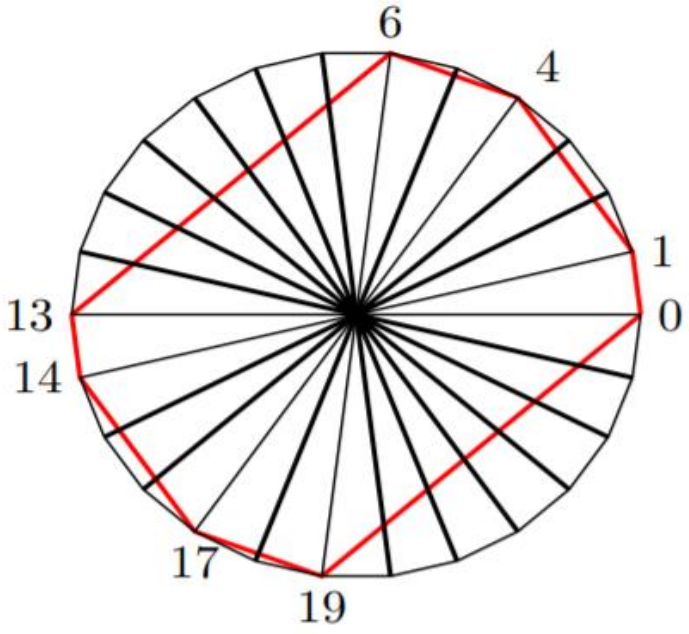

Рисунок 1.3 – Восьмикутник з вершин правильного 26-кутника без трапецій та рівнобедрених трикутників

На друге питання відповідь негативна. Розглянемо всі $7 \cdot 8/2 = 28$ прямих, що проходять через пари вибраних вершин. З них дві паралельні один одному, так як сторони та діагоналі правильного n-кутника утворюють n класів попарно паралельних прямих. Вони утворюють рівнобічну трапецію або прямокутник (при непарному n завжди виходила б трапеція). Цей приклад-окремий випадок наступного твердження.

У правильному n-кутнику при $n = 2$ $(q^2 + q + 1)$, де $q = p^m$–степінь простого числа, можна відмітити $2(q + 1)$ вершин так, що не існуватиме ні трапеція, ні рівнобедрений трикутник з вершинами в цих точках.

Наведемо ще один приклад різницевої множини, яку не можна отримати з теореми Зінгера, але можна побудувати іншими методами. Множина $\{2, 4, 5{,}27, 31, 36\}$ є різницевою по модулю 42. Можна, обчислюючи всі 30 попарних різниць по цьому модулю, безпосередньо переконатися, що всі вони різні.

1.2 Еквівалентність формулювань деяких геометричних та комбінаторних задач

Задача 1.1 У правильному 1981-кутнику відмічені 64 вершини. Довести, що існує трапеція з вершинами у відмічених точках.

Необхідно розглянути всі можливі прямі, що продовжують сторони та діагоналі правильного n −кутника, де $n -$ непарне. Вони розбиваються на n множин («напрямків») таким чином, що всі прямі одного напрямку паралельні, а прямі різних напрямків паралельними не будуть. Нехай в $n -$ кутнику виділені k вершин. Якщо $k(k-1)/2 > n,$ то згідно з принципом Діріхле існують дві паралельні прямі, що перетинають $n -$ кутник у виділених чотирьох вершинах. Вони утворюють рівнобічну трапецію, яка є симетричною відносно діаметру описаного навколо n-кутника кола, перпендикулярному її основам. Дана трапеція не може бути прямокутником, тому що її діагоналі не

є діаметрами кола, що є неможливим у правильному непарному кутнику. Ми розглянули задачу у геометричному формулюванні, розглянемо дану задачу у комбінаторному формулюванні, та перевіримо еквівалентність їх формулювань.

Нехай серед чисел від 0 до 1980 вибрано 64 числа. Тоді сума по модулю 1981 будь-яких двох різних вибраних чисел дорівнює сумі по модулю 1981 деякої іншої пари вибраних чисел (така пара обов'язково існує).

Розв'язання. Розглянемо $а + в$, де $а, в$ – будь-які з заданих чисел. Зрозуміло, що ця сума (по модулю 1981) приймає значення 0 (990+991) до 1980 (0+1980). Очевидно, що $(а + к) + (в - к)$ (по модулю 1981) $= а + в$ (по модулю 1981). Тобто утворюється 1980 класів пар чисел, суми яких по модулю 1981 однакові. Тепер виберемо з даних чисел 64 числа і розглянемо попарні суми цих чисел. Кількість можливих пар дорівнює числу комбінацій з 64 по 2, тобто $C_{64}^2 = \frac{64 \cdot 63}{2} = 2016$. Оскільки це число більше за 1981, то принаймні дві пари дають по модулю 1981 однакові суми.

Доведемо еквівалентність даних формулювань. Занумеруємо вершини 1981-кутника з геометричного формулювання задачі числами від 0 до 1980 по кругу. Символ $(а, в)$ будемо використовувати для позначення сторони або діагоналі многокутника, яка проходить через вершини а та в. Тоді паралельними будуть, наприклад, сторона (0,1980) та діагональ (1979,1), сторона (3,4) та діагональ (2,7). З іншого боку суми чисел в цих парах однакові (по модулю 1981) це і доводить еквівалентність геометричного та комбінаторного формулювань задачі.

1.3 Зв'язок різницевої множини з булевими матрицями без прямокутників

Означення 1.7 Булеві матриці, тобто матриці з нулів та одиниць, без одиничних прямокутників розміру (a, b) називають (a, b) −рідкісними, а кількість одиниць в них, їх вагою.

Теорема 1.6 *Я*кщо в $(n \times n)$- матриці із нулів та одиниць немає двох рядків та двох стовпців, на перехресті котрих стоять одиниці (тобто немає підматриць 2 x 2, заповнених одиницями), то число одиниць в матриці не більше $n(\sqrt{n - 3/4} + 1/2)$. Рівносильне формулювання: якщо в квадратній таблиці розміру $n \times n$, $n > 2$ міститься більше $n\left(1 + \sqrt{4n - 3}\right)/2$ нулів, то в ній знайдеться прямокутник (чотири клітини, розташовані на перехресті двох рядків та двох стовпців), складений із нулів.

Циклічною називається квадратна матриця, кожен рядок якої виходить циклічним зрушенням попереднього рядка на одну позицію. Тобто циклічна $(n \times n)$ матриця має вигляд:

$$\begin{pmatrix} a_0 & a_1 & \dots & a_j & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{j+1} & \dots & a_{n-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_1 & a_1 & \dots & a_{j-1} & \dots & a_0 \end{pmatrix}.$$

Для побудови циклічної матриці без прямокутників розглянемо будь-яку множину $S = \{s_1, \dots, s_k\} \subset \mathbb{Z}_n$, в котрій всі різниці $s_i - s_j$ (по $mod\ n$), де $i \neq j$, різні. Для всіх $i = 1, \dots, k$ покладемо $a_{si} = 1$, а решта a_j покладемо рівними нулю. Відповідна циклічна матриця складається з k циклічних одиничних діагоналей, що проходять через $s_i - e$ позиції першого рядка. Величини $s_i - s_j$ є відстанями між цими діагоналями. Одиниці, які стоять на однакових позиціях в деяких двох рядках, відносяться до різних циклічних діагоналей. Отже, якби по дві одиниці в деяких двох рядках були розташовані

на одних і тих же позиціях, то для кожного з рядків ці одиниці ставилися б у різних (впорядкованих) парах циклічних діагоналей, але це суперечить побудові: відстані між діагоналями не повторюються. Тому побудована матриця не містить прямокутників. В якості такої множини S можна взяти $(q^2 + q + 1, q + 1, 1)$ – різницеву множину Зінгера. Число одиниць в цій матриці знаходимо так само як і в отриманій в теоремі 1.6 верхній оцінці числа одиниць: $n\,(1 + \sqrt{4n - 3})\,/\,2 = nk$, де $n = q^2 + q + 1, k = q + 1$.

Розглянемо $(n \times n)$–матрицю без прямокутників, що містить приблизно $n^{3/2}$одиниць. Цей приклад застосовується в теорії складності булевих функцій. Через E_0 позначимо одиничну матрицю розміру $p \times p$, а через E_i– матрицю, що отримується з E_0 циклічним зрушенням рядків на i позицій вниз. Матриця H_p має вигляд:

$$H_p = \begin{pmatrix} E_0 & E_0 & \dots & E_0 & \dots & E_0 \\ E_0 & E_1 & \dots & E_j & \dots & E_{p-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ E_0 & E_i & \dots & E_{ij} & \dots & E_{i(p-1)} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ E_0 & E_{p-1} & \dots & E_{(p-1)j} & \dots & E_{(p-1)^2} \end{pmatrix}.$$

Перевіримо, що матриця H_p не містить прямокутників. Скористаємося розбиттям зазначеної матриці на горизонтальні і вертикальні смуги ширини p, перенумерувавши їх від 0 до $p - 1$. Зауважимо, що на перетині $i -$ ї горизонтальної смуги та $j -$ ї вертикальної смуги знаходиться матриця E_{ij}. Припустимо, що деякі два рядки і деякі два стовпці матриці Hp в перетині утворюють «одиничний» прямокутник. Нехай ці рядки розташовані в i_1-й та i_2-й горизонтальних смугах, а стовпці–в j_1-й та j_2-й вертикальних смугах. Очевидно, $i_1 \neq i_2$ і $j_1 \neq j_2$, так як в будь-якому рядку і кожному стовпці матриці E_k міститься рівно по одній одиниці.

Задача 1.2 Побудувати (13x13)- матрицю з нулів та одиниць, з 52 одиницями, без прямокутників.

Розглянемо різницеву множину $\{0, 1, 3, 9\} \subset Z_{13}$ та побудуємо циклічну матрицю:

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Замість одиниць даної матриці поставимо крапки, а на місці нулів залишимо порожнє місце, результат ми бачимо на рисунку 1.4. Дана матриця має вагу 52.

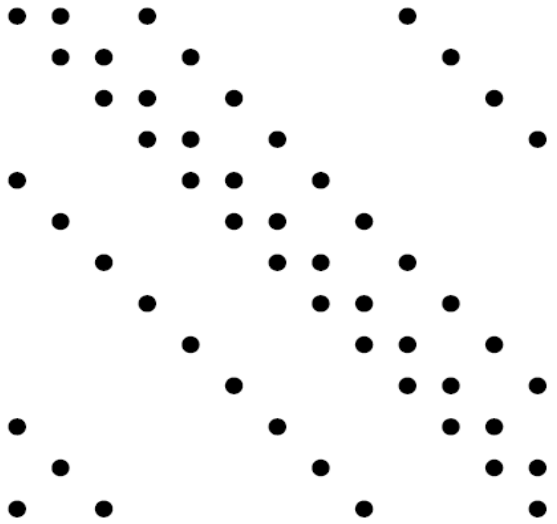

Рисунок 1.4 – Матриця з нулів та одиниць без прямокутників

2 КОМБІНАТОРНІ ЗАДАЧІ, ПОВ'ЯЗАНІ ЗІ СКІНЧЕННОЮ МНОЖИНОЮ

2.1 Скінченні геометрії та блок схеми

Означення 2.1 Множина називається скінченною проективною площиною, якщо виконуються наступні аксіоми:

а) для будь-яких двох різних точок існує рівно одна пряма, яка проходить через ці точки;

б) будь-які дві прямі мають рівно одну спільну точку;

в) існують чотири точки, з яких будь-які три не лежать на одній прямій.

Задача 2.1 Дано 10 множин з 4 елементів кожна, причому об'єднання будь-яких двох множин містить рівно 7 елементів. Скільки елементів може бути в об'єднанні всіх цих множин, необхідно вказати всі можливі значення.

Будемо проводити міркування для більш загального випадку, а саме, коли в кожній множині k елементів, а число множин дорівнює n. Число елементів в об'єднанні всіх n множин позначимо m. З умови випливає, що будь-які дві множини мають рівно один спільний елемент. Ці множини назвемо «прямими», а їх об'єднання–«площиною». Тоді отримана скінченна геометрія задовольняє двом аксіомам:

а) будь-які дві різні «прямі» мають не більше однієї спільної «точки»;

б) через кожну точку проходить хоча б одна пряма.

Очевидно, що якщо всі n прямі мають спільну точку, то загальне число точок на них $m = 1 + n\,(k - 1)$. Оскільки $k = 4$, одна з можливих відповідей в задачі: $m = 1 + 10 \cdot 3 = 31$.

А що буде, якщо не всі прямі мають спільну точку? Тоді кожен пучок прямих (тобто множина всіх прямих, що проходять через одну точку) містить не більше ніж k прямих. Дійсно, є хоча б одна пряма l, яка не входить в нього. Всі прямі пучка перетинають l, причому в різних точках (адже їх спільна точка

не лежить на l), тому число прямих в пучку не більше k, а загальне число точок на прямих цього пучка максимум $1 + k\,(k - 1)$. Якщо в пучку k прямих, то він буде мати $1 + k\,(k - 1)$ точок. Доведемо для числа прямих нерівність $n \leq 1 + k\,(k - 1)$. Дійсно, крім прямої l є не більше $k\,(k - 1)$ прямих, так як кожна пряма перетинає l в одній з k її точок, а через кожну таку точку проходить не більше $k - 1$ прямих, крім самої l. Якщо в кожному пучку менше k прямих, тоді так само доводиться, що $n \leq 1 + k\,(k - 2)$. Так як в нашому випадку $n = 10 > 1 + 4 \cdot 2$, знайдеться пучок, в якому k прямих. Але тоді, як було вже доведено, $m \geq 1 + k\,(k - 1)$. Покажемо, що тоді $m = 1 + k\,(k - 1)$.

Якщо $m > 1 + k\,(k - 1)$, то знайдеться точка A, що не лежить на прямих цього пучка. Розглянемо пряму, що проходить через неї. Вона не збігається з прямими пучка (в силу вибору точки A) і перетинається з кожною з них, причому ці точки різні і не збігаються з A. Тоді на прямій $k + 1$ точка, а це суперечить умові. Наведемо приклад «площини» з 13 точками і 10 прямими.

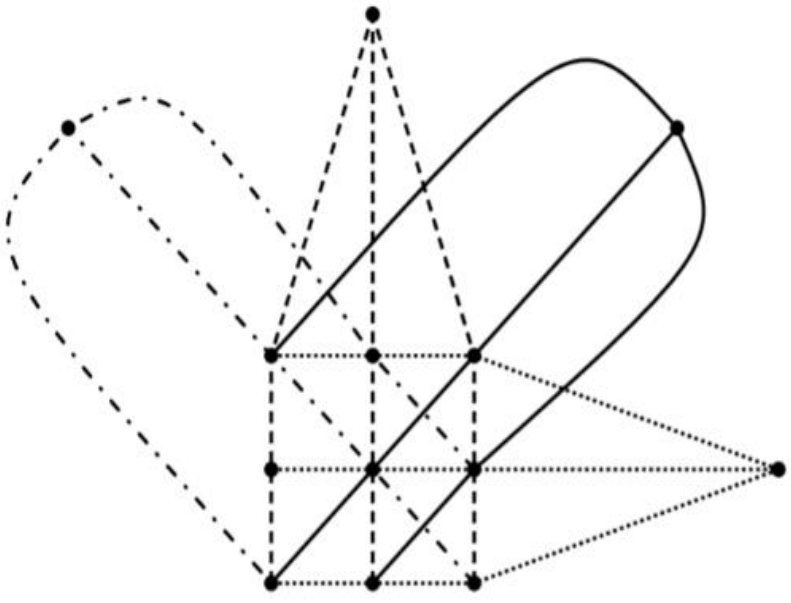

Рисунок 2.1 – Площина з 13 точками та 10 прямими

У цьому прикладі однотипні прямі мають спільну точку, так як утворюють пучки. Прямі різного типу теж попарно перетинаються, що менш очевидно, але легко перевіряється. Насправді навіть можна намалювати ще 3 прямі так, щоб будь-які дві з 13 прямих попарно перетиналися.

Рівність $n = 1 + k\,(k - 1)$ можлива тільки в разі, коли в кожному пучку рівно k прямих. Доведемо, що тоді через будь-яку пару точок A, B проходить пряма, причому єдина. Розглянемо пучок з k прямих, що проходять через B. Всі вони перетинають пряму l, причому в різних точках. Так як точок на прямій теж k, одна з прямих цього пучка проходить через точку A прямої l, що і потрібно було довести.

Описана площина складається з $1 + k\,(k - 1)$ точок, містить стільки ж прямих, кожна з яких містить k точок, в кожному пучку k прямих і виконані дві аксіоми: через будь-які дві точки проходить єдина пряма і будь-які дві прямі мають спільну точку. Це аксіоми проективної геометрії, а описана площина є скінченною проективною площиною. Однак незрозуміло, чи при будь-якому k можливо таке сімейство скінченних множин. Якщо $q = k - 1$ є степінь простого числа, то це можливо. Вище це було фактично доведено у випадку $q = 3$. Якби в умові завдання було $n > 1 + k\,(k - 1)$ множин, то тривіальна відповідь $1 + (k - 1) \cdot n$ була би єдиною, фактично це ми і довели.

У разі $k = 4$ і $10 \leq n \leq 13$ окрім тривіальної відповіді $1 + 3 \cdot n$ є ще відповідь 13, що теж було вище доведено. Наведений приклад для 10 прямих доповнюється до 13 прямих з дотриманням умов завдання і без збільшення числа точок. Отже 13 або 31 елементів може бути в об'єднанні всіх цих множин [1].

Наведена задача є частинним випадком більш загального твердження, яке формулюється у вигляді наступної теореми.

Теорема 2.1 Нехай $q \geq 2$ – ціле число. Площина $PG(2, q)$ називається скінченою проективною площиною порядку q, якщо рівносильні наступні шість умов:

а) деяка пряма містить $q + 1$ точку;

б) деяка точка лежить рівно на $q + 1$ прямій;

в) кожна пряма містить $q + 1$ точку;

г) кожна точка лежить рівно на $q + 1$ прямій;

д) площина містить рівно $q^2 + q + 1$ точок;

е) на площині існує рівно $q^2 + q + 1$ прямих.

Теорема 2.2 Скінченна проективна площина порядку q утворює симетричну блок-схему з $v = q^2 + q + 1$ елементами, $b = v$ блоками по $k = q + 1$ елементів в кожному $\lambda = 1$, а симетрична блок-схема $(q^2 + q + 1, q + 1, 1)$ утворює площину $PG(2, q)$.

Теорема 2.3 Скінченна проективна площина порядку q утворює симетричну блок-схему з $v = q^2 + q + 1$ елементами, $b = v$ блоками по $k = q + 1$ елементів в кожному та $\lambda = 1$. Та навпаки, симетрична $(q^2 + q + 1, q + 1, 1)$–блок-схема утворює площину $PG(2, q)$.

Система Штейнера- різновид блок схеми, а саме t −схеми з $\lambda = 1$ і $t \geq 2$. Система Штейнера з параметрами t, k, n, позначається як $S(t, k, n)$ − це n-елементна множина S з набором k − елементних підмножин множини S − блоками.

Головна властивість цієї системи говорить, що кожна t елементарна підмножина S знаходиться рівно в одному блоці. Це класичне означення системи Штейнера, в якому необхідною умовою є, $k = t + 1$. Схема $S(2,3, n)$ − називається системою трійок Штейнера, а його блоки трійками.

Число трійок, що проходять через точку, так само $(n - 1) / 2$, а тому загальна кількість трійок дорівнює $n \cdot (n - 1) / 6$. Це показує, що n повинно мати вигляд $6k + 1$ або $6k + 3$ для деякого k.

2.2 Блок-схема або конфігурація, симетричні блок-схема і конфігурація. Приклади

Приклад 2.1 При $q = 2$, симетрична блок-схема (7, 3, 1), де $b = v = 7, r = k = 3$, λ=1 матиме вигляд:

$$B_0: 0, 1, 3;$$
$$B_1: 1, 2, 4;$$
$$B_2: 2, 3, 5;$$
$$B_3: 3, 4, 6;$$
$$B_4: 4, 5, 0;$$
$$B_5: 5, 6, 1;$$
$$B_6: 6, 0, 2\ ;$$

$$\{\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 0\}, \{5, 6, 1\}, \{6, 0, 2\ \}\}.$$

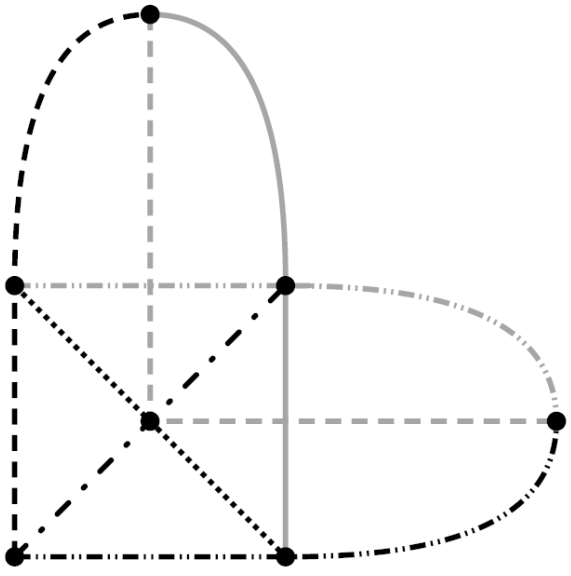

Рисунок 2.2 – Проективна площина $PG(2, 2)$ – Площина Фано

Приклад 2.2 При $q = 3$, симетрична блок-схема (9, 12, 3, 1), де $b = 12, v = 9, r = 4, k = 3, \lambda = 1$ матиме вигляд:

B_1: 1, 2, 3;

B_2: 4, 5, 6;

B_3: 7, 8, 9;

B_4: 1, 4, 7;

B_5: 2, 5, 8;

B_7: 1, 5, 9;

B_8: 2, 6, 7;

B_9: 3, 4, 8;

B_{10}: 1, 6, 8;

B_{11}: 2, 4, 9;

B_{12}: 3, 5, 7;

{{1, 2, 3},{4, 5, 6},{7, 8, 9},{1, 4, 7},{2, 5, 8},{3, 6, 9},{1, 5, 9}, {2, 6, 7}, {3, 4, 8},{1, 6, 8}, {2, 4, 9},{3, 5, 7}}.

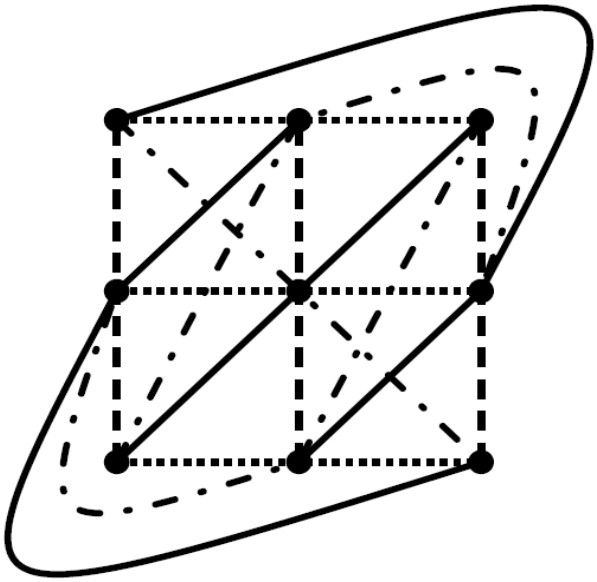

Рисунок 2.3 – Афінна площина $AG(2,3)$

Приклад 2.3 При $q = 4$, симетрична блок-схема (15, 7, 3), де $b = v = 15, r = k = 7, \lambda = 3$ матиме вигляд:

B_0: 0, 1, 2, 3, 4, 5, 6;

B_1: 0, 1, 2, 7, 8, 9, 10;

B_2: 0, 1, 2, 11, 12, 13, 14;

B_3: 0, 3, 4, 7, 8, 11, 12;

B_4: 0, 3, 4, 9, 10, 13, 14;

B_5: 0, 5, 6, 7, 8, 13, 14;

B_6: 0, 5, 6, 9, 10, 11, 12 ;

B_7: 1, 3, 5, 7, 9, 11, 13;

B_8: 1, 3, 6, 7, 10, 12, 14;

B_9: 1, 4, 5, 8, 10, 11, 14;

B_{10}: 1, 4, 6, 8, 9, 12, 14;

B_{11}: 2, 3, 5, 8, 10, 12, 13;

B_{12}: 2, 3, 6, 8, 9, 11, 14;

B_{13}: 2,4,5,7,9,12,14;

B_{12}: 2, 4, 6, 7,10, 11, 13.

У випадку блок-схеми Адамара, кількість точок на кожній прямій дорівнює $\lambda = 3$. Це тривимірний проективний простір, який складається з 15 точок, 35 прямих та 15 гіперплощин.

Площина $PG(3,2)$ – це найменший проективний простір, який можна розглядати як розглядати як розширення площини Фано. Він володіє наступними властивостями:

а) кожна точна належить 7 прямим та 7 площинам;

б) кожна пряма міститься в 3 площинах і містить 3 точки;

в) кожна площина містить 7 точок і 7 прямих;

г) кожна площина ізоморфна площині Фано;

д) будь-яка пара різних площин не перетинається по прямій;

е) пряма і площина, що не містять пряму, мають одну спільну точку.

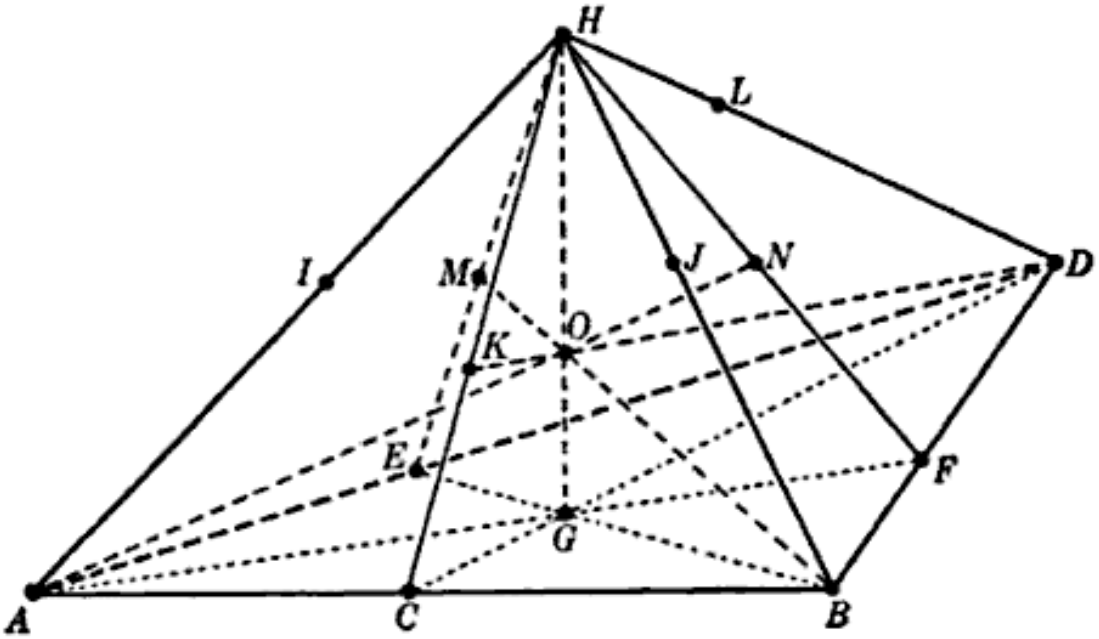

Рисунок 2.4 – Блок-схема Адамара $PG(3,2)$

Означення 2.2 Конфігурація на площині – це скінченна система точок і прямих, розташованих таким чином, що кожна точка належить фіксованій кількості ліній, а кожна лінія містить фіксовану кількість точок.

Конфігурація на площині позначається символом (p_γ ℓ_π), де p – число точок, ℓ – число прямих, γ – число прямих, що проходять через кожну точку, а π – число точок на кожній прямій. З описання конфігурації випливає, що для її існування необхідними умовами є наступні:

а) $p\gamma = l\pi$, оскільки цей добуток дорівнює числу інциденцій точка–пряма;

б) $p \geq \gamma(\pi - 1) + 1$.

Проективно двоїстою конфігурацією для (p_γ l_π) є конфігурація (l_π p_γ), в якій ролі «точок» і «прямих» міняються місцями. Тому конфігурації можна розглядати взаємодвоїстими парами, за винятком випадків, коли двоїста конфігурація ізоморфна вихідній [1]. Ці виключення називаються самодвоїстими конфігураціями і в цих випадках $p = \ell$. Самодвоїстність означає, що можна знайти відповідність точок першої конфігурації прямим з

іншої конфігурації і прямим першої конфігурації точкам другої таким чином, що всі інцидентності зберігаються .

Означення 2.3 У деяких конфігураціях $p = \ell$, а тому і $\gamma = \pi$. Вони називаються симетричними або збалансованими конфігураціями і зазвичай позначення спрощується. Наприклад, $(9_3 9_3)$–конфігурація Паппа – скорочується до (9_3). У загальному випадку симетрична конфігурація типу (n_3) складається з абстрактного набору з n точок разом з набором з n трійок точок – ліній так, що кожна точка належить 3 лініям, а кожна лінія містить 3 точки.

Зауваження 2.1 Конфігурації з однаковими позначеннями не зобов'язані бути ізоморфними.

Твердження 2.1 Число неізоморфних конфігурацій типу (n_3), починаючи з n = 7, є елементами послідовності:

1, 1, 3, 10, 31, 229, 2036, 21399, 245342, ...

Ці числа підраховані як абстрактні структури інцидентності, вони показують кількість конфігурацій данного типу.

Прикладами таких конфігурацій є:

а) площина Фано. Це єдина (7_3) конфігурація, вона є скінченною проективною площиною, яка має найменшу можливу кількість точок та прямих – всього 7 точок і 7 прямих, причому кожна пряма проходить через три точки і через кожну точку проходить три прямі. Вона є системою трійок Штейнера $S(2,3,7)$, в цьому випадку блоками будуть 7 прямих, кожна ж яких містить три точки (рисунок 2.5);

б) єдина (8_3) конфігурація – конфігурація Мебіуса – Кантора. Ця конфігурація складається з двох чотирикутників, одночасно описаних і вписаних відносно один одного. Всі окрім однієї лінії конфігурації можна зобразити прямими, всі одночасно – не можливо;

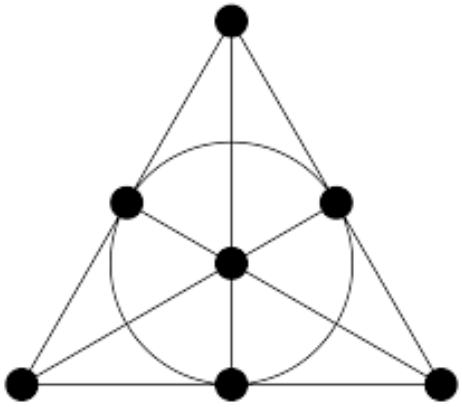

Рисунок 2.5– Конфігурація Фано

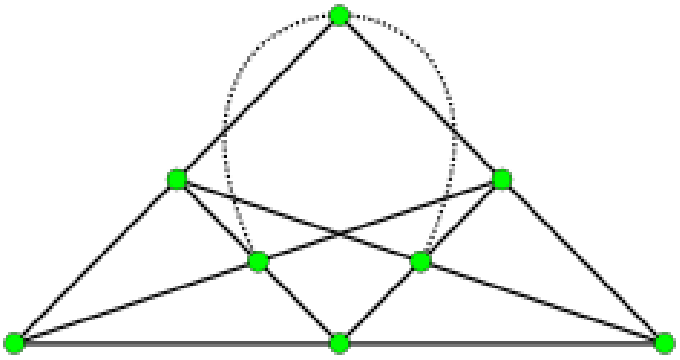

Рисунок 2.6 – Конфігурація Мебіуса–Кантора

в) існує 3 конфігурації типу (9_3) – конфігурація Паппа та дві менш відомі конфігурації. В геометрії конфігурацією Паппа називається конфігурація дев'яти точок і дев'яти прямих на евклідовій площині, по три точки на кожній прямій і через кожну точку проходять три прямі;

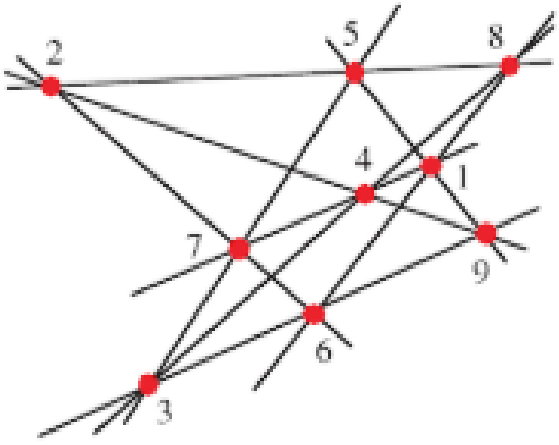

Рисунок 2.7 – Конфігурація Паппа

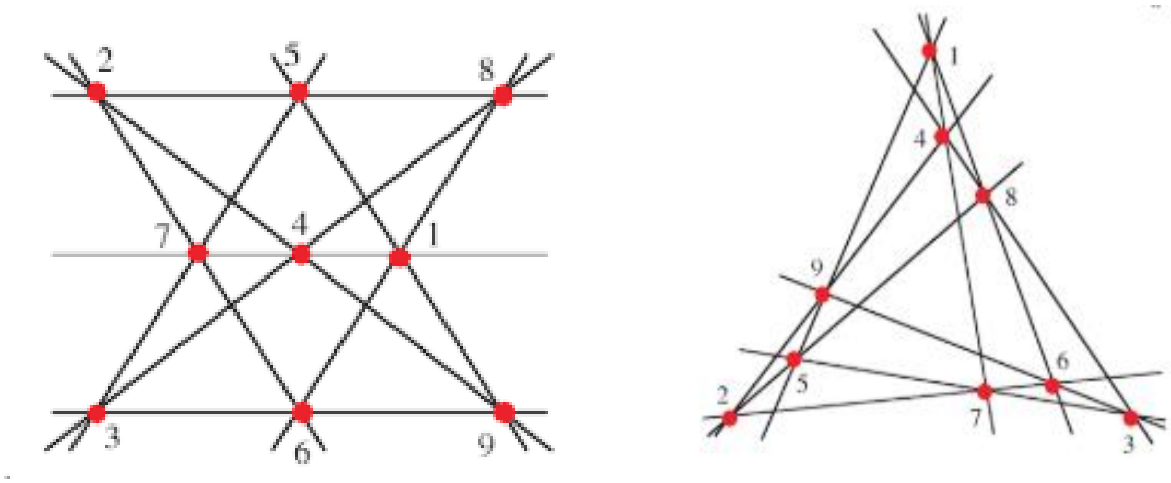

Рисунок 2.8 – Інші конфігурації типу (9_3)

г) (10_3) конфігурація Дезарга – це конфігурація з 10 рівноправних точок і 10 рівноправних прямих. Як проективна конфігурація, конфігурація Дезарга має позначення (10_3), що означає, що кожна з її 10 точок інцидентна трьом прямим, а кожна з 10 прямих інцидентна трьом точкам.

Існує ще вісім інших (10_3) конфігурацій, що не ізоморфні конфігурації Дезарга.

Конфігурація називається симетричною якщо існує пряма, що проходить через один з вузлів, в осьовій симетрії відносно якої конфігурація відображається на себе.

Для знаходження кількості симетричних відносно осі конфігурацій будемо використовувати формулу:

$$R(n) = \frac{(n-1)!+(n-1)^2}{2n}.$$

Розглянемо конфігурації п'ятого порядку. Не важко переконатися, що конфігурацій, які нас цікавлять, всього чотири (рисунок 2.9).

$$R(5) = \frac{4! + 4^2}{10} = 4 .$$

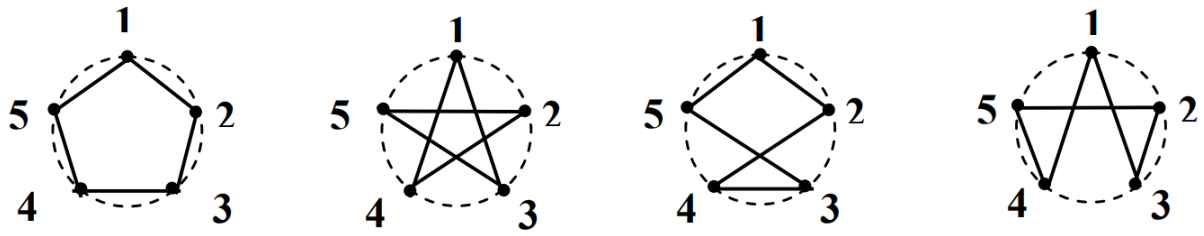

Рисунок 2.9 – Конфігурації п’ятого порядку

Дійсно, всі вони мають осьову симетрію і вісь симетрії проходить через точку 1.[8]

2.3 Задачі, пов’язані з конфігурацією Фано, зв’язок з криптографією

Площина $PG(3,2)$ виникає при розв’язанні деяких комбінаторних задач. Задача Кіркмана «про школярок»– комбінаторна задача, яка довгий час була однією з головних проблем комбінаторики.[9]

П'ятнадцять молодих дівчат в школі прогулюються по три в ряд сім днів (щодня), потрібно розподілити їх на кожну прогулянку так, щоб ніякі дві дівчини не йшли в тому ж ряду.

Переформулюємо задачу, якщо існує n школярок, необхідно створити групи розміром k, так щоб набори з t дівчат, ніколи не зустрічались, двічі в одній групі. Таке формулювання є схемою n, k, t.

Якщо дівчат пронумеровати від 0 до 14, наступний розподіл буде одним з розв’язків.

Таблиця 2.1 – Розв’язання задачі Кіркмана методом перебору

Понеділок	Вівторок	Середа	Четвер	П’ятниця	Субота	Неділя
0, 1, 4	1, 2, 5	4, 5, 8	2, 4, 10	4, 6, 12	10, 12, 3	0, 5, 10
2, 3, 6	3, 4, 7	6, 7, 10	3, 5, 11	5, 7, 13	11, 13, 4	1, 6, 11
7, 8, 11	8, 9, 12	11, 12, 0	6, 8, 14	8, 10, 1	14, 1, 7	2, 7, 12
9, 10, 13	10, 11, 14	13, 14, 2	7, 9, 0	9, 11, 2	0, 2, 8	3, 8, 13
12, 14, 5	13, 0, 6	1, 3, 9	12, 13, 1	14, 0, 3	5, 6, 9	4, 9, 14

Розв’язок цієї задачі є прикладом системи трійок Штейнера. Ця система розбиває блоки системи трійок на паралельні класи, які є розбиттям точок на блоки, що не перетинаються.

Якщо дівчат, занумерувати двійковими числами від 0001 до 1111, наступний розподіл є розв’язком, таким, що для будь-яких трьох дівчат, які утворюють групу, диз’юнкції двох чисел утворюють третє число.

Таблиця 2.2 – Розв’язання задачі Кіркмана у двійковій системі

Понеділок	Вівторок	Середа	Четвер	П’ятниця	Субота	Неділя
0001, 0100, 0101	0001, 0110, 0111	0001, 1000, 1001	0001, 1010, 1011	0001, 1100, 1101	0001, 1110, 1111	0001, 0010, 0011
0010, 1000, 1010	0010, 1001, 1011	0010, 1100, 1110	0010, 1101, 1111	0010, 0100, 0110	0010, 0101, 0111	0100, 1000, 1100
0011, 1101, 1110	0011, 1100, 1111	0011, 0101, 0110	0011, 0100, 0111	0011, 1001, 1010	0011, 1000, 1011	0101, 1010, 1111
0110, 1001, 1111	0100, 1010, 1110	0100, 1011, 1111	0101, 1001, 1100	0101, 1011, 1110	0100, 1001, 1101	0110, 1011, 1101

Продовження таблиці 2.2

Понеділок	Вівторок	Середа	Четвер	П’ятниця	Субота	Неділя
0111, 1011, 1100	0101, 1000, 1101	0111, 1010, 1101	0110, 1000, 1110	0111, 1000, 111	0110, 1010, 1100	0111, 1001, 1110

Це розв’язання має геометричну інтерпретацію, пов'язану з PG (3,2). Візьмемо тетраедр і перенумеруємо його вершини як 0001 0010, 0100 і 1000. Перенумеруємо шість центрів ребер як виключну диз’юнкцію кінців ребра. Присвоїмо чотирьом центрам граней мітки, рівні диз’юнкції трьох вершин, а центру тіла дамо мітку 1111. Тоді 35 трійок і диз’юнкція розв’язку відповідають 35 прямим PG (3,2).

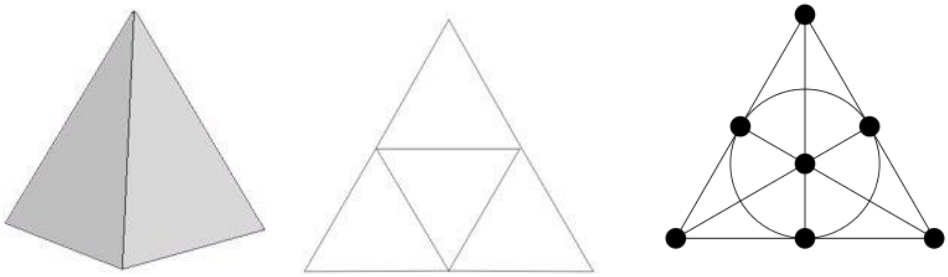

Рисунок 2.10– Розв’язок задачі Кіркмана як 3-вимірний простір Фано

Два неізоморфних розв’язки цієї задачі можуть бути вкладені як структури в 3-вимірний простір Фано. Зокрема, розшарування PG (3,2) є розкладанням точок на прямі, що не перетинаються, і відповідає розподілу дівчат (точок) на неперетинні рядки (прямі) для одного дня для задачі Кіркмана. Є 56 різних розшарувань по 5 прямих в кожному. Упакування PG (3,2)–це розбиття 35 прямих на 7 неперетинних шарів по 5 прямих в кожному шарі і це відповідає розв’язку для всіх семи днів. Є 240 упакувань PG (3,2), які розпадаються на два класи суміжності по 120 упаковок під дією PGL (4,2) (групи коллініацій простору). Дана задача привела нас до ще однієї частини комбінаторних задач, а саме теорії кодування.

Криптографія – наука про математичні методи забезпечення конфіденційності, тобто неможливості прочитання інформації сторонніми.

Оскільки основним завданням криптографії є захист інформації, то необхідно розглянути певні вимоги до шифрів. Шифр повинен забезпечувати достатню стійкість до злому. Незважаючи на те, що одиночне шифрування повідомлення може бути в принципі незламним, часто буває необхідно переслати сотні повідомлень, зашифрованих в одній і тій же системі.

Шифр повинен бути простий у використанні. Часто користувачі уникають користуватися складними і громіздкими шифросистемами або користуються ними з помилками.

Розглянемо найпростіший приклад коду, що виправляє одну помилку. Припустимо, нам потрібно передати двійкове слово (x_1, x_2, x_3, x_4). Додамо до нього перевірочні символи $x_5 = x_1 + x_3 + x_4$, $x_6 = x_1 + x_2 + x_4$, $x_7 = x_1 + x_2 + x_3$, знак " + " позначає додавання по модулю два; символи x_1, x_2, x_3, x_4 називаються інформаційними. Процедура обчислення по інформаційним символам перевірочних символів та складання з них кодового слова (закодованого повідомлення) називається кодуванням (так само називається і саме відображення вихідного повідомлення в кодове слово).

Мовою матриць в розглянутому прикладі кодування зводиться до множення деякої матриці М на транспонований вектор $(x_1, x_2, x_3, x_4)^{\mathrm{T}}$, тобто вектор, розташований в стовпець:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix}.$$

Передаємо закодоване повідомлення $c = (x_1, \dots x_7)$ та отримуємо зашумлене повідомлення $r = c + e$, де $\mathrm{e} = (e_1, \dots, e_7)$ – вектор похибок. В

нашому випадку він має вагу (суму координат) 1, так як за припущенням помилка може трапитись (якщо трапиться) тільки в одній позиції. Наприклад, можливо $e = e_3 = (0, 0, 1, 0, 0, 0, 0)$.

Тоді $r = c + e = (c_1, c_2, c_3 + 1, c_4, c_5, c_6, c_7) = (c_1, c_2, \bar{c_3}, c_5, c_6, c_7)$, де $\bar{0} = 1, \bar{1} = 0$. Число 3 буде в розглянутому випадку позицією помилки. Для визначення позиції помилки (а значить, і виявлення самої помилки) можна обчислити перевірочні суми:

$$S_1 = r_1 + r_3 + r_4 + r_5,$$
$$S_2 = r_1 + r_2 + r_4 + r_6,$$
$$S_3 = r_1 + r_2 + r_3 + r_7.$$

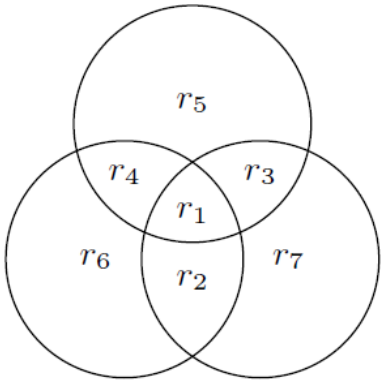

Рисунок 2.11 – Код Гемінга з блоковою довжиною 7

Побудований код є окремим випадком кодів Гемінга. Наочно перевірочні суми зображені на рисунку 2.10. Кожна сума міститься в своєму колі. Розглянемо деякі його властивості більш детально.

Його потужність (кількість кодових слів) дорівнює 2^4= 16, сума будь-яких двох кодових слів по модулю два знову є кодовим словом, відстань коду дорівнює трьом (відстань $d\ (a, b)$ між кодовими словами a, b дорівнює числу позицій, в яких вони відрізняються, а відстань коду за визначенням дорівнює мінімальному відстані між різними кодовими словами).

Так як код має кодове слово ваги нуль (нульове слово), а кодова відстань дорівнює трьом, кодових слів ваги 1 або 2 в ньому немає. Для кожного кодового слова розглянемо кулю радіусу 1 с центром в ньому. Ця куля містить, окрім центру, ще 7 довічних наборів (вершин семивимірного довічного куба), які утворюються, якщо в центральному наборі замінити рівно один з семи його символів на протилежний. Ці кулі з центрами в кодових словах не перетинаються, тому в сукупності містять $2^4 \cdot 8 = 2^7$ різних вершин куба, тобто всі ці вершини. Такі точні покриття багатовимірного куба неперетинними кулями називаються досконалими, а відповідні їм коди– досконалими кодами. Виходячи тільки з властивості досконалості зазначеного коду, можна однозначно визначити число кодових вершин на третьому шарі семивимірного кубу.

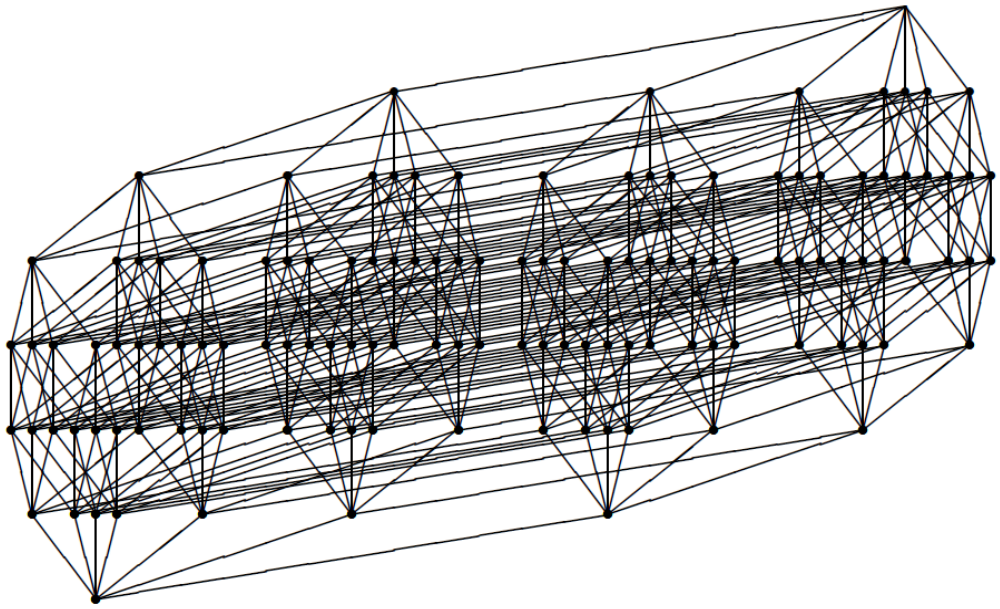

Рисунок 2.12 – Схематичне зображення семивимірного кубу

Для цього розглянемо одиничні сфери з центрами в кодових словах ваги три (сфера-це поверхня кулі). Зауважимо, що їх перетиин з другим шаром кубу мають потужність 3 ,так як існують тільки три набори ваги два, що лежать на даній сфері: дійсно, серед координат центру сфери тільки три одиниці, які можна замінювати на нулі.

Тому число кодових слів ваги три не більше $C_7^2 : 3 = 7$. А так як вершини другого шару покриваються тільки кулями з центрами в третьому шарі, а кулі з центрами в четвертому і більш високих шарах до другого шару не дістають, якщо код досконалий, то число кодових слів ваги три дорівнює рівно 7. Обчислимо, скільки вершин четвертого шару покривається сімома розглянутими кулями. Кожна куля покриває 4 вершини, ці перетини куль з площиною попарно не перетинаються, тому загальне число покритих вершин 4-го шару дорівнює $7 \cdot 4 = 28$.

Непокриті вершини третього шару можна покрити тільки кулями з центрами в четвертому шарі, а кожен такий шар покриває в третьому шарі рівно 4 вершини. Отже, для покриття решти вершин третього шару необхідно не менше 28/4 = 7 куль з центрами в четвертому шарі, а непокритих вершин там рівно 7, таким чином, їх потрібно використовувати в якості кодових вершин і центрів куль. Тому кодових вершин ваги 4 рівно 7.

Відповідні кулі покривають в п'ятому шарі $7 \cdot 3 = 21$ вершину (кулі попарно не перетинаються, так як їх центри-кодові слова), тобто всі його вершини. Кодових слів на шостому шарі бути не може, так як куля з центром в цьому шарі містить вершини п'ятого шару, а вони вже покриті. Залишається єдина вершина сьомого шару–одинична вершина, яка повинна входити в код, щоб її сфера покрила шостий шар. Таким чином, припускаючи існування досконалого коду з відстанню три в семивимірному кубі, можна точно встановити його ваговий спектр, а саме число його слів заданої ваги**.**

Він складається з чисел $a_0 = 1, a_1 = 0, a_2 = 0, a_3 = 7, a_4 = 7, a_5 = 0, a_6 = 0, a_7 = 1$.

Розглянемо кодові слова вагою 3. Кожне з них визначає трьохелементну підмножину в множині $\{1,2,3,4,5,6,7\}$, яка складається з номерів з позицій одиниць в цьому слові. Можна зробити висновок, що будь-які з цих множин мають не більше одного спільного елементу, в іншому випадку відстань між кодовими словами дорівнювала двом. Тому система з 7 трійок утворює систему Штейнера, тобто кожна пара елементів, а в нашому випадку їх рівно

$C_7^2 = 21$, належить рівно одній трійці, тому що сім трійок містять 21 пару. Спільний елемент у будь-яких двох трійок рівно один, так як в іншому випадку, решта трійок, які перетинаються з цими двома і не більше ніж по одному елементу, повинні мати один спільний для всіх елемент- той, який не належить двом першим трійкам. Зазначимо той факт, що інших спільних елементів у них бути не може, отже, таких трійок не більше трьох, а всього трійок не більше п’яти, тоді як повинно бути сім.

Тому система трійок ізоморфна конфігурації 7 прямих в проективній площині на 7 точках. Дана конфігурація називається площиною Фано. Відстань між будь-якими двома кодовими словами з третього шару дорівнює 4. Можна зробити висновок, що максимальне число вершин третього шару семимірного куба, попарні відстані між якими не менше трьох або чотирьох, дорівнює семи. Таким чином, максимальна потужність коду вагою три зі словами довжини 7 дорівнює сім.

2.4 Побудова скінченної площини

Нехай $q = p^n$–степінь простого числа. Нехай також існує скінченне поле $GF\ (q)$, тобто поле з q елементів. Просте поле $GF(p)$ визначаємо як множину чисел $\{0, 1, \ldots, p\ -\ 1\}$, операції додавання та множення в якому виконуються по модулю p, тобто для знаходження суми або добутку необхідно знайти звичайну суму або добуток і замінити їх на залишок від ділення на p. Ці операції задовольняють тим же законам, що і операції додавання і множення раціональних чисел, а саме:

а) комутативність:

$$a + b\ mod p\ =\ b + a\ mod\ p, ab\ mod\ p\ =\ ba\ mod\ p;$$

б) асоціативність:

$$(a + b) + c = a + (b + c)\ mod\ p, (ab)c = a(bc)\ mod\ p;$$

в) дистрибутивність :

$$a(b + c) = ab + ac.$$

Що задовольняють тотожностям $a + 0 = a, a \cdot 1 = a$, а також мають однозначно визначені обернені операції: віднімання $a - b\ mod\ p$, ділення $a/b\ mod\ p$, які задовольняють тотожностям $(a - b) + b = a\ mod\ p, (a/b)b = a\ mod\ p$.

Якщо $n > 1$ поле $GF(p)$ можна визначити як множину многочленів степеня меншого за n з коефіцієнтами з простого поля $GF(p)$. Додавання і віднімання многочленів визначається стандартним чином, тобто коефіцієнти додаються або віднімаються по модулю p, а множення виконується за модулем даного незвідного многочлена $f(x)$ степеня n з коефіцієнтами з поля $GF(p)$, тобто результат звичайного множення многочленів замінюється на залишок від ділення на $f(x)$. Многочлен називається незвідним над полем $GF\ (p)$, якщо його не можна розкласти в добуток многочленів меншого степеня над тим же полем. Ділення многочленів із залишком визначається так само, як і ділення чисел із залишком, тільки замість умови, що залишок від ділення повинен бути менше дільника, використовується умова, що степінь залишку повинен бути менше степеня дільника, тобто многочлена $f\ (x)$.

Приклад 2.4 Побудуємо скінчене поле з 9 елементів. У ньому фактично можна обійтися без використання многочленів над полем з 3 елементів, так як конструкція дуже схожа на побудову поля комплексних чисел. Розглянемо множину $F_9 = \{\gamma_0, \dots, \gamma_8\}$ з елементів виду (a, b), де $a, b = 0, \pm 1$. Визначимо на ньому операцію додавання за формулою $(a, b) + (c, d) = (a + c, b + d)$, де $1 + 1 = -1, (-1) + (-1) = 1$, а все інше, як в звичайному додаванні. Операцію множення над числами $0, \pm 1$ беремо звичайну, а операцію множення

над парами (a, b), (c, d) визначаємо як $(ac - bd, ad + bc)$. Елемент (0,0) відіграє в цьому полі роль нуля, а елемент (1, 0) — роль одиниці. Елементи виду (a, 0) утворюють підполе в цьому полі, що складається з трьох елементів (0, 0), (1, 0),(−1, 0), їх можна позначати як 0, 1, −1. Виконання операцій в цьому підполі зводиться до виконання зазначених вище операцій на множині $\{0, 1, -1\}$. Елемент (0,1) при піднесенні до квадрату дорівнює (−1, 0), тобто −1. Для будь-якого (a, b) можна визначити операцію обчислення оберненого елемента щодо додавання (її можна назвати операцією зміни знаку): $-(a, b) = (-a, -b)$, де $-0 = 0$. Тому (a, b) $+ (-(a, b)) = (0, 0) = 0$. Після цього визначається операція віднімання: (a, b) $- (c, d) = (a, b) + (-c, -d)$, яка є оберненою операцією до операції додавання. Для $(a, b) \neq (0, 0)$ можна ще визначити операцію обчислення оберненого елемента щодо множення: $(a, b)^{-1} = (-a, b)$, якщо $ab \neq 0$, а в інших випадках $(a, 0)^{-1} = (a, 0)$, $(0, b)^{-1} = (0, -b)$. Звідси $(a, b)^{-1} \cdot (a, b) = (1,0)$.

Теорема 2.4 Для будь-якого q, що є степенем простого числа, існує скінченна проективна площина порядку q.

Доведення. Розглянемо тривимірний векторний простір $GF(q)^3$, тобто множину трійок (x_1, x_2, x_3), $x_i \in GF(q), i = 1,2,3$. Назвемо дві ненульові трійки еквівалентними, якщо одна з них коллінеарна другій, тобто $x_i = ay_i$, $i = 1,2,3, a \in GF(q)\backslash\{0\}$.

Клас еквівалентності трійок назвемо точкою проективної площини. В кожному класі еквівалентності рівно q – 1 ненульових трійок, тому число цих класів (число точок побудованої проективної площини) дорівнює $(q^3 - 1)/(q - 1) = q + 1$ класів колінеарних трійок, тобто кожному такому двовимірному півпростору можна співставити q + 1 точку, кожна з яких будується на проективній площині і назвати цю множину прямою проективної площини.

Будь-які два двовимірні півпростори (a,x)=0, (b, x) = 0 перетинаються по одновимірному простору, ненульові трійки якого визначають точку C побудованої проективної площини–єдину точку перетину відповідних прямих

а та b. Число різних двовимірних підпросторів дорівнює $(q^3 - 1)/(q-1)=q^2 + q + 1$, так як півпростори (a, x) = 0, (b, x) = 0 збігаються тоді і тільки тоді, коли трійки a и b еквівалентні, отже число прямих на побудованій проективній площині дорівнює $q^2 + q + 1$. Через будь-які дві точки A,C даної площини проходить єдина пряма a, а саме та, яка відповідає двовимірному простору (a, x) = 0, натягнутому на трійки з класів еквівалентності A, B. Теорема доведена.

ВИСНОВКИ

Проблеми комбінаторики привертали увагу видатних математиків багато століть, і дотепер цей розділ математики інтенсивно розвивається і знаходить численні застосування.

В кваліфікаційній роботі для окремих класів задач встановлено еквівалентність їх комбінаторних та геометричних формулювань, розглянуто геометричні та комбінаторні підходи до розв’язання певного класу задач. Показано, що теоретичною базою для реалізації цих підходів є поняття різницевих множин та блок-схем. Побудовані приклади різницевих множин та блок-схем.

В кваліфікаційній роботі було розглянуто одну з головних проблем комбінаторики, яка впродовж довгого часу була не вирішеною. Це задача Кіркмана. В роботі наведено 3 з 7 існуючих варіантів розв’язання цієї задачі, серед яких комбінаторний та геометричний методи.

В роботі наведено приклади застосування геометричних конфігурацій на скінченній проективній площині. Однією з таких конфігурацій є площини Фано. Описано використання площини Фано для складання і дешифровки шифрів, що свідчить про зв’язок цього поняття з криптографією та теорією інформації.

Робота буде корисною всім, хто цікавиться комбінаторикою, теорією скінченних геометрій, їх застосуваннями.

ПЕРЕЛІК ПОСИЛАНЬ

1. Вишенський В. А., Перестюк М. О. Комбінаторика : перші кроки: Кам’янець-Подільський : Аксіома, 2010. 320 с.

2. Базилевич Л. Є. Дискретна математика у прикладах і задачах : теорія множин, математична логіка, комбінаторика, теорія графів. Львів : Мир, 2013. 486 с.

3. Павлова Л. В., Дітчук Р. Л. Елементи комбінаторики і стохастики : навч.- метод. посіб. Тернопіль : Підручники і посібники, 2005. 159 с.

4. Вербіцький О. В. Вступ до криптології. Львів : Науково-технічна література, 1998. 248 с.

5. Яковлев И. В. Комбинаторика для олимпиадников. Москва : МЦНМО, 2016. 80 с.

6. Толпунов В. Л. Комбинаторика : практикум по решению задач. Москва : МПГУ, 2016. 88 с.

7. Бродський Я. С. Статистика, ймовірність, комбінаторика : навч.-метод. посіб. Тернопіль : БОГДАН, 2013. 256 с.

8. Agibalov G. P., Pankratova I. A. Asymmetric cryptosystems on Boolean functions. Berlin : Heidelberg, 2018. P. 23.

9. Клепко В. Ю. Поняття множини : навч. посіб. 2-ге вид., перероб та доп. Київ : ЦУЛ, 2009. 154 с.