Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»
Кафедра математики факультету інформатики

АЛГЕБРАЇЧНІ СТРУКТУРИ НА СКІНЧЕНИХ МНОЖИНАХ

Курсова робота за спеціальністю «Прикладна математика»

Керівник курсової роботи
канд. фіз.-мат. наук,
старший викладач
Тимошкевич Л. М.
_____
«___» 2023р.
Виконала студентка
3-го року навчання
Бабій А. О.
«____» 2023р.

Київ – 2023

Тема: Алгебраїчні структури на скінчених множинах

Календарний план виконання роботи:

№ п/п	Назва етапу курсової роботи	Термін виконання етапу	Примітки
1	Отримання теми курсової роботи	20.09.2022	
2	Отримання літератури для опрацювання	21.10.2022	
3	Аналіз отриманої літератури	11.02.2023	
4	Дослідження, робота над завданнями	23.03.2023	
5	Опрацювання результатів з керівником	05.05.2023	
6	Оформлення курсової роботи	10.05.2023	
7	Коригування	15.05.2023	
8	Створення презентації	15.05.2023	
9	Захист	23.05.2023	

Зміст

1. Вступ

1.1. Актуальність

Тема є актуальною в сучасній математиці, особливо в теорії комбінаторних структур та теорії кодування. Вона дозволяє досліджувати і вирішувати різноманітні задачі, пов'язані зі скінченими множинами, такі як задачі комбінаторики, криптографії, обчислювальної техніки, теорії графів та інші.

Алгебраїчні структури на скінчених множинах включають такі об'єкти, як алгебри, топології, лінійні простори, бази (розглянуті далі в роботі) і т.д. Вони є основою для розвитку теорії кодування, яка займається створенням та дослідженням кодів, що дозволяють ефективно передавати інформацію через канал з шумом.

Також, алгебраїчні структури на скінчених множинах мають практичне застосування в інформаційних технологіях, зокрема в криптографії та обчислювальній техніці. Наприклад, за допомогою алгебраїчних структур можна розробляти криптосистеми з використанням скінчених полів, які забезпечують ефективне шифрування та розшифрування інформації.

1.2. Мета, завдання дослідження

Метою курсової роботи є дослідження різних алгебраїчних структур на скінчених множинах і вивчення їх властивостей. Також в роботі наявні розбір типових задач для кожної зі структур та порівняння різних алгебраїчних структур на скінчених множинах, визначення відмінностей та збігів між ними.

2. Алгебраїчні структури на скінчених множинах

Дамо означення структурі.

Означення 2.0.1.:

Структурою на множині U_n називається сімейство її підмножин, що замкнене відносно деякого заданого набору операцій.

Множина U_n - це деяка фіксована множина. Структура на множині U_n складається з сімейства її підмножин. Підмножини цієї множини можуть бути замкнені відносно деякого заданого набору операцій.

Поняття ж замкненості відносно деякого набору операцій означає, що якщо застосувати ці операції до будь-якої пари елементів з цієї підмножини, результат буде знову належати до цієї підмножини. Іншими словами, операції, що задані на множині U_n, не виходять за межі цієї множини, коли їх застосовується до її підмножин.

У цій роботі розглянемо декілька типів структур.

2.1. Алгебри

Означення 2.1.1.:

Алгеброю на множині U_n називається сімейство її підмножин, що разом з будь-якими підмножинами A та B також містить їхнє об'єднання, перетин та доповнення.

Означення 2.1.2.:

Базисом алгебри називається найменше за включенням її підсімейство $\{X_1,\ldots, X_k\}$ таке, що будь-який елемент алгебри можна виразити через $X_1,\ldots, X_k$ за допомогою перетину, об'єднання та доповнення.

Означення 2.1.3.:

Ланцюгом алгебр називається така послідовність алгебр, що:

$$\{\emptyset, U_n\} = A_0 \subsetneq A_1 \subsetneq A_2 \ldots \subsetneq A_k = 2^{U_n}$$

між будь-якими двома послідовними (сусідніми) членами не можна вставити ще одну алгебру (тобто, для довільного і не існує алгебри B такої, що $A_i \subsetneq B \subsetneq A_{i+1}$).

Розглянемо декілька завдань, що використовують поняття алгебри.

1. Знайдіть всі алгебри на U_1, U_2, U_3.
   Алгебри на U_1: {∅, {1}}
   Алгебри на U_2: {∅, {1, 2}},
   {∅, {1}, {2}, {1, 2}}
   Алгебри на U_3: {∅, {1, 2, 3}},
   {∅, {1}, {2, 3}, {1, 2, 3}}
   {∅, {2}, {1, 3}, {1, 2, 3}}
   {∅, {3}, {1, 2}, {1, 2, 3}}
   {∅, {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}, {1, 2, 3}}

2. Установіть взаємно однозначну відповідність між алгебрами на U_n та розбиттями множини U_n.
   - Розбиттям множини U_n називається невпорядкований набір $\{X_1,\ldots, X_k\}$ з підмножин U_n, для якого $U_n = X_1 \cup X_2 \cup \ldots \cup X_k$ та $X_i \cap X_j = \emptyset$ при будь-яких $i \neq j$.

$U_n = \{X_{i_1} \cup X_{i_2} \cup \ldots \cup X_{i_e} | \{i_1, \ldots i_e\} \in 2^{U_n}\}$
$X = X_{i_1} \cup \ldots \cup X_{i_e}$, $X' = X_{j_1} \cup \ldots \cup X_{j_m}$
Тоді $X \cup X' = X_{r_1} \cup \ldots \cup X_{r_s}$, де $\{r_1, \ldots r_s\} = \{i_{1,\ldots} i_e\} \cup \{j_1, \cdots j_m\}$
$2^{U_n} \setminus X = X_{\gamma_1} \cup \ldots \cup X_{\gamma_{k-e}}$
$\{\gamma_1, \cdots \gamma_{k-e}\} = U_n \setminus \{i_{1,\ldots} i_e\}$

У алгебрі розглянемо всі мінімальні елементи за включенням, окрім $X_1, \dots, X_k$

$U_n \subseteq 2^{U_n}, A, B \in 2^{U_n}$

Випадок 1: $A < B,\ A \subsetneq B$

$X_i \cap X_j = \emptyset,$ якщо $i \neq j$

Від супротивного:

$X_i \cap X_j \in U_n$

$X_i \cap X_j \subsetneq X_i$

Випадок 2: $A \leq B,\ A \subseteq B$

$X_1 \cup X_2 \cup \dots \cup X_k = U_n$

Від супротивного:

$X_1 \cup X_2 \cup \dots \cup X_k = \{m_1, m_{2,\dots} m_l\} \neq U_n$

$U_n \setminus (X_1 \cup X_2 \cup \dots \cup X_k) = X' \in U_n$

$\emptyset \neq X_{k+1} \subseteq X', X_{k+1} \in U_n$, мінімум за включенням

3. Доведіть, що кількість елементів у будь-якій довільній алгебрі завжди є степенем двійки 2^k.

   Для доведення того, що кількість елементів у будь-якій алгебрі завжди є степенем двійки 2k, розглянемо довільну алгебру з n елементами. Зафіксуємо цю кількість елементів та розглянемо можливість розбиття на пари.

Якщо n є парним числом, тоді можна розбити всі елементи на попарні пари, тобто n можна представити у вигляді n=2k, де k - додатнє ціле число. Таким чином, кожній парі елементів відповідає один із двох можливих підмножин: перше множина з двома елементами або друга множина з двома елементами. Таким чином, кількість можливих підмножин дорівнює 2^k.

Якщо ж n є непарним числом, то можна виділити один елемент і розбити всі інші елементи на попарні пари. Таким чином, кількість можливих підмножин дорівнює $2^{(k-1)}$, оскільки на одну з пар припадає окремий елемент. Загальна кількість підмножин буде дорівнювати $2^{(k-1)} \cdot 2 = 2^k$.

Отже, у будь-якій алгебрі кількість елементів завжди можна представити у вигляді 2^k, де k - додатнє ціле число.

4. Доведіть, що розміри різних базисів однієї алгебри можуть різнитися.
   Для цього завдання розглянемо алгебру на 2^{U_4} та два базиси: {1, 2}, {1, 3} та {1}, {2}, {3}.
   (1) Базис {1, 2}, {1, 3}

$\{1\} = \{1,2\} \cap \{1,3\}$

$\{1,2\} \setminus \{1\} = \{2\}, \{1,3\} \setminus \{1\} = \{3\}$

$U_4 \setminus (\{1,2\} \cup \{1,3\}) = \{4\}$

Тобто, можемо отримати: $\{\emptyset, \{1,2\}, \{3,4\}, \{1,2,3,4\}\}$

(2) Базис $\{1\}$, $\{2\}$, $\{3\}$

$\{4\} = U_4 \setminus (\{1\} \cup \{2\} \cup \{3\})$

Тобто: $\{\{1\}, \{2,3,4\}, \{1,2,3,4\}, \emptyset\}$

5. Доведіть, що всі ланцюги алгебр мають однакову довжину

Для будь-якої алгебри над A, можна розглянути її ланцюг алгебр, що починається з підалгебри, що складається з одного елемента. Підалгебра, що складається з одного елемента, є тривіальною алгеброю, в якій операції додавання та множення є тотожностями.

Для будь-якого i, який задає позицію елемента в ланцюзі алгебр, можна розглянути всі можливі підалгебри, що містяться в підмножині $\{a_1, a_2, ..., a_i\}$ множини A, де a_1, a_2, ..., a_i – елементи ланцюга алгебр. Оскільки множина A є скінченною, то кількість всіх підмножин $\{a_1, a_2, ..., a_i\}$ також є скінченною. Оскільки кожна з цих підалгебр є

алгеброю, то її розмірність $\{a_1, a_2, ..., a_i\}$ не може перевищувати n.

Таким чином, кожен елемент в ланцюзі алгебр може бути представлений підмножиною множини A розмірності не більше, ніж n. Крім того, довжина ланцюга алгебр дорівнює кількості елементів у ланцюгу, тобто на одиницю більше, ніж кількість підалгебр, що ми розглядаємо в ланцюзі.

Отже для будь-якої множини A з n елементами всі ланцюги алгебр мають однакову довжину n+1.

2.2. Лінійні простори

Означення 2.2.1.:

Лінійним простором на множині U_n називається сімейство її підмножин, яке разом з будь-якими підмножинами A і B також містить їхню симетричну різницю.

Будь-яка алгебра є лінійним простором. Цей факт легко довести, враховуючи означення 2.1.1. та 2.2.1. Варто перевірити, чи можливо виразити симетричну різницю, використовуючи операції характерні для алгебр – перетин, об'єднання та різниця.

$$A\Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) U (B \setminus A)$$

Введемо означення векторного простору та наведемо приклад.

Означення 2.2.1.*:

Нехай V – це множина, на якій задана внутрішня бінарна алгебраїчна операція додавання і зовнішня бінарна алгебраїчна операція множення елементів множини V на елементи поля P. Якщо $\bar{a}, \bar{b} \in V$, то їх сума позначається через $\bar{a} + \bar{b}$, а добуток скаляра $\alpha \in P$ на $\bar{a}$ позначається $\alpha \cdot \bar{a}$. Якщо наступні умови виконуються для всіх елементів $\bar{a}, \bar{b}, \bar{c}$ множини V і довільних елементів $\alpha_1, \alpha_2 \in P$, то множина V називається векторним (лінійним) простором над полем P. Умови:

1) $\bar{a} + (\bar{b} + \bar{c}) = (\bar{a} + \bar{b}) + \bar{c}$

2) $\bar{a} + \bar{b} = \bar{b} + \bar{a}$

3) існує нуль − вектор $\bar{0} \in v$, такий, що $\bar{a} + \bar{0} = \bar{a}$

4) для $\forall \bar{a} \in V$ існує такий $(-\bar{a}) \in V$, що $\bar{a} + (-\bar{a}) = \bar{0}$

5) $\alpha_1(\alpha_2\bar{a}) = (\alpha_1\alpha_2)\bar{a}$

6) $\alpha_1(\bar{a} + \bar{b}) = \alpha_1\bar{a} + \alpha_1\bar{b}$

7) $(\alpha_1 + \alpha_2)\bar{a} = \alpha_1\bar{a} + \alpha_2\bar{a}$

8) $1\bar{a} = \bar{a}$

Приклад до 2.2.1.*:

Розглянемо булеан 2^n множини натуральних чисел, який можна ототожнити з множиною нескінчених послідовностей нулів та одиниць. Будемо розглядати їх, як послідовності елементів поля F_2. Побітове додавання послідовностей Δ та очевидне множення на скаляри $0, 1 \in F_2$ задають структуру векторного простору на 2^n. Якщо не переходити до послідовностей – характеристичних функцій, то додавання підмножин $A, B \subsetneq N$ визначається як симетрична різниця $A \Delta B \subsetneq N$, і множення на скаляр визначається таким чином: $0A = \emptyset$, $1M = M$.

Означення 2.2.2.:

Базисом лінійного простору називається найменше за включенням його підсімейство $\{X_1, \ldots, X_k\}$ таке, що будь-

який елемент лінійного простору можна виразити через $X_1,\ldots, X_k$ за допомогою симетричної різниці.

Означення 2.2.3.:

Ланцюгом лінійних просторів називається така послідовність лінійних просторів, що:

$$\{\emptyset, U_n\} = L_0 \subsetneq L_1 \subsetneq L_2 \ldots \subsetneq L_k = 2^{U_n}$$

між будь-якими двома послідовними (сусідніми) членами не можна вставити ще один лінійний простір (тобто, для довільного і не існує лінійного простору M такого, що $L_i \subsetneq M \subsetneq L_{i+1}$).

Розглянемо декілька завдань, в яких використовуватимемо поняття лінійного простору.

1. Доведіть, що будь-який лінійний простір містить $\emptyset$.

Припустимо, що у лінійному просторі L на деякій скінченій множині не міститься порожня множина, тобто кожен елемент $l \in L$ має хоча б один компонент з U_n ненульовим.

Тоді розглянемо множину всіх векторів $l \in L$ з одним ненульовим компонентом, що належить до множини U_n.

Така множина міститиме скінчену кількість векторів, але не міститиме порожньої множини, бо будь-який вектор $l \in L$ з хоча б одним ненульовим компонентом належатиме до цієї множини.

Але тоді ця множина буде лінійним підпростором L, бо вона замкнена відносно операцій додавання та множення на скаляр, і вона містить ненульовий вектор. А це суперечить тому, що L містить лише скінченну кількість векторів, оскільки лінійний підпростір, який містить ненульовий вектор, має нескінченну кількість векторів. Отже, припущення є хибним, і лінійний простір L на скінченій множині U_n містить порожню множину.

2. Знайдіть всі лінійні простори на U_1, U_2.

   Лінійні простори на U_1: $\{\emptyset\}$, $\{\emptyset, \{1\}\}$

   Лінійні простори на U_2: $\{\emptyset\}$, $\{\emptyset, \{1\}\}$, $\{\emptyset, \{2\}\}$, $\{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$

3. Доведіть, що всі ланцюги лінійних просторів мають однакову довжину.

Для будь-якого i, який задає позицію елемента в ланцюзі лінійних просторів, можна розглянути всі можливі підпростори, що містяться в підмножині $\{a_1, a_2, ..., a_i\}$ множини A, де $a_1, a_2, ..., a_i$ – елементи ланцюга лінійних просторів. Оскільки множина A є скінченною, то кількість всіх підмножин $\{a_1, a_2, ..., a_i\}$ також є скінченною. Оскільки кожний з цих підпросторів є лінійним простором, то його розмірність $\{a_1, a_2, ..., a_i\}$ не може перевищувати n.

Таким чином, кожен елемент в ланцюзі лінійних просторів може бути представлений підмножиною множини A розмірності не більше, ніж n. Крім того, довжина ланцюга лінійних просторів дорівнює кількості елементів у ланцюгу, тобто на одиницю більше, ніж кількість підпросторів, що ми розглядаємо в ланцюзі. Отже для будь-якої множини A з n елементами всі ланцюги лінійних просторів мають однакову довжину n+1.

2.3. Топології

Означення 2.3.1.:

Топологією на множині U_n називається сімейство її пімножин, що містить U_n, ∅ і разом з довільними підмножинами A і B також їхні перетин та об'єднання.

Будь-яка алгебра є топологією. Цей факт також випливає з означень 2.1.1. та 2.3.1.

Означення 2.3.2.:

Базисом топології називається найменше за включенням її підсімейство $\{X_1,\ldots, X_k\}$ таке, що будь-який елемент топології можна виразити через $X_1,\ldots, X_k$ за допомогою їхнього перетину та об'єднання.

Означення 2.3.3.:

Ланцюгом топологій називається така послідовність топологій, що:

$$\{\emptyset, U_n\} = T_0 \subsetneq T_1 \subsetneq T_2 \ldots \subsetneq T_k = 2^{U_n}$$

між будь-якими двома послідовними (сусідніми) членами не можна вставити ще одну топологію (тобто, для довільного і не існує топології S такої, що $T_i \subsetneq S \subsetneq T_{i+1}$).

Розглянемо кілька завдань, що побудовані на понятті топології.

1. Знайдіть всі топології на U_1, U_2, U_3.
   Топології на U_1: {∅, {1}}
   Топології на U_2: {∅, {1, 2}},
   {∅, {1}, {1, 2}}
   {∅, {2}, {1, 2}}
   {∅, {1}, {2}, {1, 2}}
   Топології на U_3: {∅, {1, 2, 3}},
   {∅, {1}, {1, 2, 3}}, {∅, {2}, {1, 2, 3}}, {∅, {3}, {1, 2, 3}}
   {∅, {1}, {2, 3}, {1, 2, 3}}, {∅, {2}, {1, 3}, {1, 2, 3}}, {∅, {3}, {1, 2}, {1, 2, 3}},
   {∅, {2, 3}, {1, 2, 3}}, {∅, {1, 3}, {1, 2, 3}}, {∅, {1, 2}, {1, 2, 3}},
   {∅, {1}, {1, 2}, {1, 2, 3}}, {∅, {2}, {2, 1}, {1, 2, 3}}, {∅, {3}, {3, 1}, {1, 2, 3}},
   {∅, {1}, {1, 3}, {1, 2, 3}}, {∅, {2}, {2, 3}, {1, 2, 3}}, {∅, {3}, {3, 2}, {1, 2, 3}},
   {∅, {1}, {2}, {1, 2}, {1, 2, 3}}, {∅, {2}, {3}, {2, 3}, {1, 2, 3}}, {∅, {3}, {1}, {3, 1}, {1, 2, 3}},
   {∅, {1}, {2}, {1, 2}, {2, 3}, {1, 2, 3}}, {∅, {2}, {3}, {2, 3}, {3, 1}, {1, 2, 3}}, {∅, {3}, {1}, {3, 1}, {3, 2}, {1, 2, 3}},

$\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

Всього – 29 топологій, 9 з точністю до ізоморфізму.

2. Чи існує топологія, кількість елементів якої не є степенем двійки?
   Припустимо, що такої топології не існує. Але у прикладі 1., для топологій на U_2, наприклад, маємо дві топології, що містять по 3 елементи – число 3 не є степенем двійки.
   Отже, існують топології, кількість елементів якої не є степенем двійки.

3. Чи будь-яка топологія є лінійним простором?
   Використаємо означення топології та лінійного простору, щоби довести або ж спростувати цей факт.
   Варто розглянути концепт симетричної різниці та перевірити, чи можна її виразити через операції перетину та об'єднання.
   Єдиний можливий спосіб вираження симетричної різниці через перетин та об'єднання також містить операцію різниці: $A\Delta B = (A \cup B) \setminus (A \cap B)$, отже, прямого вираження не існує.
   Тобто, не будь-яка топологія є лінійним простором.

Цікавим фактом є те, що формули для кількості топологій на скінченій множині, по суті, поки що нема. У книжках

наводиться розрахунок до n=18 елементів. У таблиці нижче наведено для 10.

Кількість топологій на множині з *n* точок

H	Різних топологій	Різних T_0-топологій	Нееквівалентним топологій	Нееквівалентних T_0-топологій
0	1	1	1	1
1	1	1	1	1
2	4	3	3	2
3	29	19	9	5
4	355	219	33	16
5	6942	4231	139	63
6	209527	130023	718	318
7	9535241	6129859	4535	2045
8	642779354	431723379	35979	16999
9	63260289423	44511042511	363083	183231
10	8977053873043	6611065248783	4717687	2567284
OEIC	A000798	A001035	A001930	A000112

4. Знайдіть найменшу та найбільшу довжину ланцюгів топологій.

Найменша: $D_T^+ = 2n + 2$

Найбільша: $D_B(n) = 2^n + 1$

3. Висновки

Отже, у цій роботі було розглянуто три алгебраїчні структури на скінчених множинах, супровідні теоретичні факти та типові завдання. Було розглянуто їхні деякі відмінності та збіжності.

Продовженням дослідження такої роботи може бути також застосування алгебраїчних структур на скінчених множинах до різних областей, таких як криптографія, комбінаторика, теорія графів та інші. Робота може поповнитися детальним оглядом основних результатів, що стосуються цих областей, та їх застосування.

4. Список літератури

[1] May, J.P. (2003). "Notes and reading materials on finite topological spaces" (PDF). Notes for REU. http://www.math.uchicago.edu/~may/MISC/FiniteSpaces.pdf

[2] Stong, Robert E. (1966). "Finite topological spaces" (PDF). Transactions of the American Mathematical Society. 123: 325–340. doi:10.1090/s0002-9947-1966-0195042-2. MR 0195042. https://www.maths.ed.ac.uk/~v1ranick/papers/stong2.pdf

[3] Moussa Benoumhani, The Number of Topologies on a Finite Set, Journal of Integer Sequences, Vol. 9 (2006), Article 06.2.6. https://cs.uwaterloo.ca/journals/JIS/VOL9/Benoumhani/benoumhani11.pdf