МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МИКОЛАЇВСЬКИЙ НАЦІОНАЛЬНИЙ АГРАРНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ МЕНЕДЖМЕНТУ
Кафедра економічної кібернетики, комп'ютерних наук та
інформаційних технологій

ДИСКРЕТНА МАТЕМАТИКА

Конспект лекцій
для здобувачів першого (бакалаврського) рівня вищої освіти ОПП
«Комп'ютерні науки» спеціальності F3 (122) «Комп'ютерні науки»
денної форми здобуття вищої освіти

Миколаїв
2025

УДК 519.1

Д48

Друкується за рішенням науково-методичної комісії факультету менеджменту Миколаївського національного університету від 18.09.2025 року протокол № 2

Укладачі:

О. Є. Богатєнкова – асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївський національний аграрний університет

Рецензенти:

В. М. Дармосюк – кандидат фізико-математичних наук, доцент, доцент кафедри фізики та математики Чорноморського національного університету імені Петра Могили

О. В. Бойчук – кандидат фізико-математичних наук, доцент кафедри вищої та прикладної математики Миколаївського національного аграрного університету

ЗМІСТ

ВСТУП

Дискретна математика (також відома як дискретний аналіз або скінченна математика) – це розділ сучасної математики, що досліджує властивості об’єктів, які мають дискретну, тобто перервну й складену з окремих елементів, структуру.

Під спільною назвою «дискретна математика» об’єднують різні напрями, незалежно від часу їх виникнення, за одним ключовим критерієм – їхньою значущістю для теорії та практики роботи з комп’ютерами, алгоритмами й програмним забезпеченням. Вивчаючи цю дисципліну у першому семестрі, студенти формують базову математичну культуру, необхідну для моделювання, формалізації та алгоритмізації прикладних задач у сфері ІТ.

Ці методичні рекомендації створено для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю F3 «Комп’ютерні науки». Матеріал адаптовано відповідно до освітньо-професійної програми та структуровано таким чином, щоб забезпечити поступове формування знань: від базових понять теорії множин до складніших розділів, як математична логіка, комбінаторний аналіз, теорія графів і т. д.

Особливу увагу приділено формуванню зв’язку між абстрактними математичними моделями та реальними комп’ютерними задачами. Завдяки цьому студенти не лише опановують теоретичний матеріал, а й навчаються бачити його роль у побудові алгоритмів, структур даних, логічних схем та інших інструментів, що формують основу сучасних інформаційних технологій.

Запропоновані методичні рекомендації покликані допомогти студентам ефективно опрацьовувати матеріал лекційного курсу, систематизувати основні поняття та навички, а також навчитися застосовувати теоретичні знання для розв’язання прикладних задач.

1. ТЕОРІЯ МНОЖИН

1.1. Множини

Інтуїтивне означення множини

Поняття множини є одним із базових у математиці й належить до аксіоматичних – таких, що не мають точного визначення, подібно до понять «точка» чи «пряма» в геометрії.

Часто приймається формулювання інтуїтивного поняття множини Георга Кантора, основоположника цієї теорії: «*Довільне зібрання певних предметів нашої інтуїції чи інтелекту, які можна відрізнити один від одного і які уявляються як єдине ціле, називається* ***множиною****. Предмети, які входять до складу множини, називаються її* ***елементами***».

Ключова ідея такого підходу полягає в тому, що увага переноситься з окремих предметів на їх зібрання, яке саме може розглядатися як новий об’єкт. При цьому природа елементів не обмежується: множини можуть складатися з чисел, геометричних точок, людей, даних або навіть абстрактних понять. Важливо лише, щоб для будь-якого об’єкта можна було визначити, чи належить він множині, а також розрізнити між собою будь-які її елементи.

Альтернативним інтуїтивним визначенням множини є також твердження математиків, які працювали під псевдонімом Ніколо Бурбаки: «Множина утворюється з елементів, що мають певні властивості, знаходяться у певних відношеннях між собою чи з елементами інших множин» або ж «Логічно кажучи, майже всю сучасну математику можна вивести з єдиного джерела: теорії множин».

Прикладами множин є множина натуральних чисел, множина парних чисел, множина студентів в аудиторії, множина дерев у лісі.

Для позначення конкретних множин використовують великі літери *A, S, X…* Для позначення елементів множин загалом застосовують малі літери *a, s, x…* Для позначення того, що *x* є елементом множини S (тобто *x* належить

S), будемо застосовувати запис $x \in S$, а запис $x \notin S$ значитиме, що елемент x не належить множині S. Символ «$\in$» називається символом належності.

Однозначно визначена множина S, елементами якої є предмети $x_1, x_2, \ldots, x_n$, будемо позначати $S = \{x_1, x_2, \ldots, x_n\}$. Зокрема, $\{x\}$ – **одинична множина**, тобто одноелементна множина, єдиним елементом якої є x. Якщо множина S скінчена, то кількість елементів в множині позначається $|S|$. Наприклад, для $S = \{a, b, c, d\}$ кількість елементів буде $|S| = 4$.

Порядок слідування елементів у множині не має значення. Наприклад, $\{a, b, c, d\}$ та $\{c, a, d, b\}$ – це одна й та сама множина.

Множини, як об'єкти, можуть бути елементами інших множин. Множину, елементами якої є множини, іноді називають **сімейством**. Як правило, визначення множин, які є сімействами, забезпечують індексами, щоби відрізняти їх одне від одної. Запис

$$\boldsymbol{S} = \{S_i\}_{i \in A}$$

позначає, що $\boldsymbol{S}$ є сімейством, елементами якого є множини S_i, причому індекс i «пробігає» множину A.

Сукупність об'єктів, які не є множиною, називається **класом**.

Множина, яка складається з елементів деякої множини S так, що ці елементи можуть входити до складу цієї множини в якій завгодно кількості екземплярів, називається **мультимножиною** множини S і позначається M(S). З точки зору теорії множин, множина і її мультимножина – це один і той самий об'єкт, і вони можуть не розрізнятися між собою. Але часто, особливо коли мова заходить про представлення множини в пам'яті ЕОМ, виникає потреба відрізняти мультимножину від множини.

Способи задання множин

Існує кілька способів задання множин.

1. Вербальний (словесний) спосіб за допомогою опису характеристичних властивостей, які повинні мати елементи множин. Наприклад, S – множина студентів жіночої статі в цій аудиторії.

2. Список (перелік) усіх елементів (у фігурних дужках). Наприклад, S = {1,2,3,4,5}.

3. Предикатний (характеристичний) спосіб за допомогою характеристичного предикату – деякої умови, вираженої у формі логічного твердження або процедури, яка повертає логічне значення, і дозволяє перевіряти, належить чи ні будь-який даний елемент множині. Якщо для даного елемента ця умова виконується, то він належить визначеній множині, у протилежному випадку – не належить. Тобто множина задається у вигляді $\{x : P(x)\}$ або $\{x \mid P(x)\}$, де $P(x)$ – характеристичний предикат. Наприклад:

- S = {x | x – натуральне число};
- S = {x | x – парне число};
- S = {x | x – цифра десяткової системи числення}.

Переліком можна задавати тільки скінченні множини. Нескінчені множини задаються характеристичними предикатами.

Задання множини називається **ненадлишковим**, якщо кожний її елемент входить в дану множину в єдиному екземплярі, і **надлишковим**, якщо хоча б один елемент цієї множини входить до її складу більш ніж в одному екземплярі (випадок мультимножини).

Парадокс Рассела

Введені вище поняття теорії множин з успіхом можуть бути використані в основах аналізу, алгебрі, математичній логіці. Однак при більш строгому розгляді такі інтуїтивні уявлення можуть виявитися незадовільними. Недосконалість інтуїтивних уявлень про множини, їх недостатність ілюструється, наприклад, відомим парадоксом, що його винайшов англійський філософ та математик Бертран Рассел.

Множини або є елементами самих себе, або не є такими. Так, множина абстрактних понять сама є абстрактним поняттям, а множина всіх зірок на небі не є зіркою. Множина звуків також є звуком. Аналогічно, множина всіх множин є множиною.

Розглянемо множину A всіх множин X, що X не є елементом X, тобто

$$A = \{X \mid X \notin X\}.$$

Якщо множина A існує, то ми маємо відповісти на запитання: $A \in A$? Нехай A не є елементом A, то за означенням A також є елементом A. З іншого боку, якщо A є елементом A, то $A \notin A$. Отримали логічне протиріччя, яке відомо як парадокс Рассела.

Цей парадокс відомий у популярній формі як парадокс цирульника. В одному селищі цирульник зобов'язується голити всіх тих мешканців та тільки тих, які не голяться самі. Як бути самому цирульнику: чи має він голити сам себе? Очевидно, що будь-яка відповідь приводить до протиріччя.

Наведемо три способи запобігання цьому парадоксу Рассела.

1. Обмежити характеристичні предикати, які використовуються, виглядом

$$P(x) = x \in S \ \& \ Q(x),$$

де S – відома, свідомо існуюча множина. Зазвичай при цьому використовується позначення $\{x \in S \mid Q(x)\}$. Для A така множина не зазначена, тому A – не є множиною.

2. Теорія типів. Об'єкти мають тип 0, множини елементів типу 0 мають тип 1, множини елементів типу 0 та 1 – тип 2 і т.д. A не має типу, тому не є множиною.

3. Явна заборона приналежності множини самій собі: $X \in X$ – недозволений предикат. Відповідна аксіома має назву аксіома регулярності.

Існування та аналіз парадоксів у теорії множин сприяли розвитку так званого *конструктивізму* – напрямку у математиці, в межах якого розглядаються тільки такі об'єкти, для яких відомі процедури (алгоритми) їх побудови. У конструктивній математиці виключаються ті поняття та методи класичної математики, які не задані алгоритмічно.

Парадоксу Рассела можна запобігти, обмеживши множини, які розглядаються. Наприклад, достатньо заборонити використання в якості множин класи, які містять самі себе. При цьому немає повної впевненості, що

не з’являться інші протиріччя. Повноцінним виходом є аксіоматична побудова теорії множин та доведення побудованої формальної теорії.

Універсум. Підмножини.

У теорії множин використовується поняття порожньої множини. **Порожня множина** – це множина, яка не містить елементів. Позначається вона символом ∅. Введення порожньої множини дає можливість оперувати будь-якою множиною без попереднього застереження, існує вона чи ні. Наприклад, множина S = {x | x – непарне число, що ділиться на 2} буде порожньою.

Означення 1.1. Множина A є **підмножиною** множини B, якщо кожний елемент A є елементом B, тобто якщо $x \in A$, то $x \in B$. Для позначення цього факту водиться знак «⊂» - символ включення (або «⊆»). При цьому множина B буде називатися **надмножиною** множини A.

Якщо необхідно підкреслити, що множина B містить також інші елементи, крім елементів множини A, то використовують символ строгого включення: $A \subset B$. Зв’язок між символами ⊂ та ⊆ задається виразом

$$A \subset B \Leftrightarrow A \subseteq B \ \& \ A \neq B.$$

Зокрема кожна множина є підмножиною самої себе. Якщо A не є підмножиною B, то пишуть $A \not\subset B$. Тобто існує елемент множини A, який не належить B.

Говорять, що множина A є **власною підмножиною** B, якщо $A \subset B$ і $A \neq B$. В такому випадку множина B буде власною надмножиною.

Означення 1.2. **Універсум (універсальна множина) U** – множина з такою властивістю, що всі множини, які розглядаються, є її підмножинами.

У теорії чисел універсум зазвичай співпадає із множиною всіх цілих або натуральних чисел. У математичному аналізі універсум – множина всіх дійсних чисел, або множина всіх точок n-мірного простору. Треба зазначити, що універсум однозначно не визначений, якщо точно не вказана область

визначення (предметна область). Звичайно, будь-яка множина, яка містить **U**, може бути використана як універсум.

За визначенням, кожна з множин є підмножиною універсуму. Порожня множина є підмножиною будь-якої даної множини S, оскільки кожний елемент порожньої множини міститься в S (або не існує елементів порожньої множини, які б не належали S).

Треба бути уважним, щоб розрізняти елементи множини та підмножини цієї множини. Наприклад, коли пишуть $a \in \{a,b,c\}$, це означає, що елемент a є членом множини, що складається з трьох елементів: a, b і c. Коли ж пишуть $\{a\} \subset \{a,b,c\}$, це означає, що множина, що складається з одного елемента a, є підмножиною множини, яка складається з трьох елементів: a, b і c.

Означення 1.3. Дві множини рівні, коли вони складаються з одних і тих самих елементів: $A=B \Leftrightarrow \forall x(x \in A \Leftrightarrow x \in B)$.

Наприклад, {1,2,3} = {3,2,1}.

Лема 1.1. Стверджується наступна рівність: $A \subset B \ \& \ B \subset A \Leftrightarrow A=B$.

Доведення. Необхідність. Розглянемо будь-який елемент $x \in A$. Множина A є підмножиною B, тому $x \in B$. З іншого боку, будь-який елемент $x \in B$ (оскільки $B \subset A$) належить також множині A, тобто $x \in A$. За означенням рівності маємо A=B.

Достатність. Розглянемо будь-який елемент $x \in A$. Оскільки A=B, маємо $x \in B$. Тоді за означенням включення множин $A \subset B$. Розглянемо будь-який елемент $x \in B$. Якщо A=B, то $x \in A$. За означенням включення $B \subset A$.

Лема 1.2. Стверджується наступна рівність (властивість **транзитивності**): $A \subset B \ \& \ B \subset C \Leftrightarrow A \subset C$.

Доведення. Якщо $x \in A$, то $x \in B$. Також якщо $x \in B$, то $x \in C$. Тобто якщо $x \in A$, то $x \in C$. Отримали $A \subset C$.

Лема 1.3. Порожня множина єдина.

Це можна довести виходячи з означення рівності множин.

Ми вже зазначали раніше, що елементами множини можуть бути якісь інші множини.

Означення 1.4. Множину, елементами якої є всі підмножини A, називають множиною підмножин (**булеаном**) множини A і позначають P(A).

Так для триелементної множини $A = \{a,b,c\}$ маємо $P(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$.

У разі кінцевої множини A, що складається з n елементів, її булеан P(A) містить 2^n елементів. Доведення ґрунтується на підсумовуванні всіх коефіцієнтів розкладу бінома Н'ютона або на поданні підмножин n-розрядними двійковими числами, в яких 1 (або 0) відповідає елементам підмножин.

Слід підкреслити відмінності між відношенням належності ($\in$) та відношенням включення ($\subset$). Відношення включення має властивість транзитивності, а відношення належності – ні. Наприклад, множина $A = \{\{1\}, \{2,3\}, \{4\}\}$ у числі своїх елементів містить множину $\{2,3\}$, тоді можна записати $2,3 \in \{2,3\}$ і $\{2,3\} \in A$.

Однак це не означає, що елементи 2 та 3 є в множині A (в наведеному прикладі немає 2 і 3 серед елементів множини A, тобто $2,3 \notin A$).

Операції над множинами

Розглянемо дві множини A та B і введемо кілька операції над ними. Для графічної ілюстрації будемо використовувати так звані діаграми Венна або кола Ейлера. Діаграма Венна являє собою схемне зображення множин у вигляді множин точок: універсум **U** зображується множиною точок деякого прямокутника, а його підмножини – у вигляді кіл або інших простих областей у цьому прямокутнику.

Означення 1.5. **Об'єднання** A і B ($A \cup B$) – множина, що складається з усіх елементів множин A, всіх елементів множини B і не містить ніяких інших елементів (рис 1.1,а), тобто $A \cup B = \{x \mid x \in A \text{ або } x \in B\}$.

Наприклад, $\{1,2,3\} \cup \{2,3,4\} = \{1,2,3,4\}$.

Означення 1.6. **Переріз (перетин)** A і B (A∩B) – множина, що складається з тих і тільки тих елементів, які належать одночасно множині A та множині B (рис 1.1,б), тобто A∩B = {x | x∈A та x∈B}.

Наприклад, {1,2,3}∩{2,3,4} = {2,3}.

Означення 1.7. **Різниця** A і B або **відносне доповнення** B до A (A-B, A\B) – множина, що складається з тих і тільки тих елементів, які належать множині A та не належать множині B (рис 1.1,в), тобто A\B = {x | x∈A та x∉B}.

Наприклад, {1,2,3}\{2,3,4} = {1}.

Означення 1.8. **Симетрична різниця (диз'юнктивна сума)** A і B (A÷B, A⊕B) – множина, що складається з усіх елементів A, які не належать множині B, й усіх елементів B, які не належать множині A (рис 1.1,г), тобто

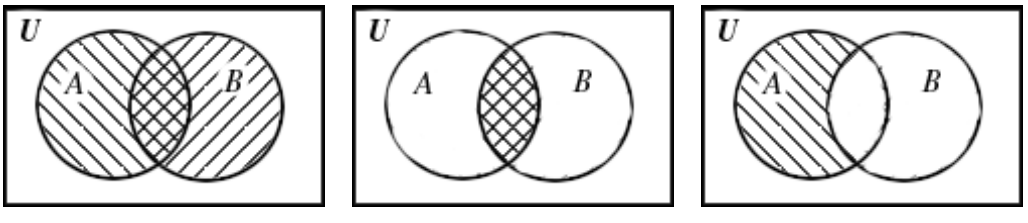
A÷B = {x | (x∈A та x∉B} або (x∉A та x∈B)).

За означенням: A÷B = (A\B)∪(B\A).

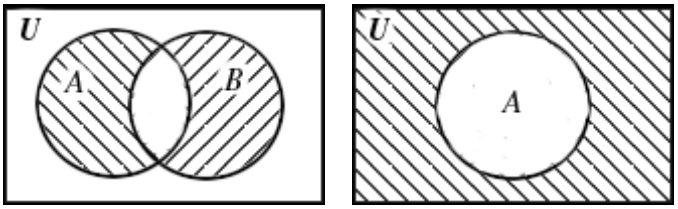
Наприклад, {1,2,3}÷{2,3,4} = {1,4}.

Означення 1.9. **Абсолютне доповнення** або просто **доповнення** A (A', $\overline{A}$) – множина, що містить усі елементи універсуму, за винятком елементів A (рис 1.1,д), тобто A' = {x | x∉A).

За означенням: A' = **U**\A.



а б в



г д

Рис 1.1. Діаграми Венна.

(а – об’єднання, б – перетин, в – різниця, г – симетрична різниця, д – доповнення)

Операції над множинами, як і операції над числами, мають деякі властивості. Останні виражаються сукупністю тотожностей незалежно від конкретного вмісту множин, що входять у них, і є підмножинами деякого універсуму **U**.

Для будь-яких множин A, B та C справедливі наступні властивості:

- *ідемпотентність* (*самопоглинання*)

1а) $A \cup A = A$ 1б) $A \cap A = A$

- *комутативність*

2а) $A \cup B = B \cup A$ 2б) $A \cap B = B \cap A$

- *асоціативність*

3а) $A \cup (B \cup C) = (A \cup B) \cup C$ 3б) $A \cap (B \cap C) = (A \cap B) \cap C$

- *дистрибутивність*

4а) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ 4б) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

- *властивості* $\varnothing$ *та* **U**

5а) $A \cup \varnothing = A$ 5б) $A \cap \varnothing = \varnothing$

6а) $A \cup A' = \mathbf{U}$ 6б) $A \cap A' = \varnothing$

7а) $A \cup \mathbf{U} = \mathbf{U}$ 7б) $A \cap \mathbf{U} = A$

8а) $\varnothing' = \mathbf{U}$ 8б) $\mathbf{U}' = \varnothing$

- *поглинання*

9а) $A \cup (A \cap B) = A$ 9б) $A \cap (A \cup B) = A$

- *закони де Моргана*

10а) $(A \cup B)' = A' \cap B'$ 10б) $(A \cap B)' = A' \cup B'$

- *властивості доповнення, різниці та рівності*

11) $A \cup B = \mathbf{U} \ \& \ A \cap B = \varnothing \Leftrightarrow B = A'$

12) $A'' = A$ (*інволютивність*)

13) $A \setminus B = A \cap B'$

14) $A \div B = (A \cap B') \cup (A' \cap B)$

15) $A \div B = B \div A$

16) $(A \div B) \div C = A \div (B \div C)$

17) $A \div \varnothing = \varnothing \div A = A$

18) $A \subset B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B' = \varnothing$

19) $A = B \Leftrightarrow (A \cap B') \cup (A' \cap B) = \varnothing$

Доведення цих співвідношень можна ґрунтувати на означенні 1.3 та лемі 1.1, або доводити за допомогою побудови діаграм Венна для лівої та правої частин співвідношень.

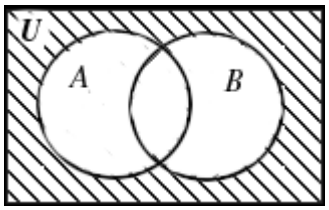
Доведемо, наприклад, співвідношення 3б: $A \cap (B \cap C) = (A \cap B) \cap C$. Нехай $x \in A \cap (B \cap C) \Rightarrow x \in A$, $x \in B$, $x \in C \Rightarrow x \in (A \cap B)$ і $x \in C \Rightarrow x \in (A \cap B) \cap C$ і $A \cap (B \cap C) \subseteq (A \cap B) \cap C$. Одержання оберненого включення виконується аналогічно.

Тепер наведемо доведення для 4а: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. З одного боку, оскільки $(B \cap C) \subseteq B$, то $A \cup (B \cap C) \subseteq A \cup B$. Аналогічно $B \cap C \subseteq C$ і $A \cup (B \cap C) \subseteq A \cup C$. Значить, $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. З іншого боку, якщо $x \in (A \cup B) \cap (A \cup C)$, то $x \in A \cup B$ і $x \in A \cup C$. Якщо $x \in A$, то $x \in A \cup (B \cap C)$. А якщо $x \notin A$, то $x \in B$ і $x \in C$ і тоді $x \in B \cap C$. Отже, $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. Разом з отриманим раніше включенням маємо потрібну рівність.

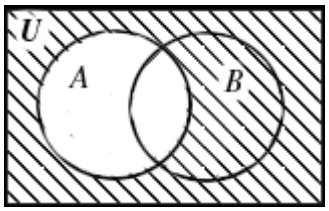
Доведемо співвідношення 1а: $A \cup A = A$.

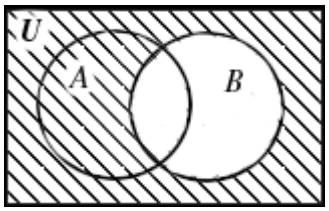
$A \cup A = (A \cup A) \cap \mathbf{U} = (A \cup A) \cap (A \cup A') = A \cup (A \cap A') = A \cup \varnothing = A$.

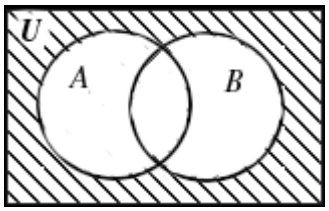
Доведемо співвідношення 10а: $(A \cup B)' = A' \cap B'$ за допомогою діаграм Венна. Спочатку побудуємо діаграму для $(A \cup B)'$ – рис. 1.2, а. Множині A' відповідає рис. 1.2, б. Множині B' – рис. 1.2, в. Множині $A' \cap B'$ відповідають частини, які заштриховані на рис. 1.2 б, в. Ця множина зображена на рис. 1.2, г.



а







б в г

Рис. 1.2. Діаграми Венна для доведення співвідношення (A∪B)’ = A’∩B’.

(а - (A∪B)’, б - A’, в - B’, г - A’∩B’).

Отримали, що множини (A∪B)’ та A’∩B’ однаково зображуються на діаграмах Венна, тобто (A∪B)’ = A’∩B’.

Доведення інших властивостей залишаємо читачеві на самостійну роботу.

Із властивостей комутативності й асоціативності операції об’єднання випливає, що об’єднання кількох множин можна виконати, послідовно об’єднуючи їх, причому порядок входження множин не впливає на результат. Отже об’єднання сукупності множин можна подати співвідношенням

$$A_1 \cup A_2 \cup ... \cup A_n = \bigcup_{i=1}^{n} A_i .$$

Аналогічно на n множин узагальнюється операція перерізу:

$$A_1 \cap A_2 \cap ... \cap A_n = \bigcap_{i=1}^{n} A_i .$$

Використовуючи узагальнення операцій об’єднання та перерізу на n множин, можна узагальнити також інші співвідношення, наприклад, закон де Моргана, який в узагальненому вигляді має вигляд:

$$\overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i} \text{ і } \overline{\bigcap_{i=1}^{n} A_i} = \bigcup_{i=1}^{n} A_i .$$

Означення 1.10. Сукупність множин A_1, A_2, ..., A_n називається **розбиттям** множини A, якщо:

1. $\bigcup_{i=1}^{n} A_i = A$.

2. $A_i \cap A_j = \varnothing$, $\forall i \neq j$.

Якщо умова 2 не задовольняється, то сукупність множин буде називатися **покриттям**.

1.2. Відношення

Декартовий добуток

Означення 2.1. Нехай A і B – дві множини. Розглянемо множину C = {(a,b) | a∈A, b∈B}. Ця множина називається **декартовим (прямим) добутком множин** A і B і позначається A×B. Якщо множини A і B скінченні і складаються відповідно із m і n елементів, то очевидно, що C складається із mn елементів.

Нехай A = {1,2} і B = {2,3,4}. Тоді A×B = {(1,2), (1,3), (1,4), (2,2), (2,3), (2,4)}.

Елементами декартового добутку є **упорядковані пари**, де перший елемент пари належить першій множині, а другий – другій. Порядок входження пар може бути будь-яким, але розташування елементів у кожній парі визначається порядком множин, що перемножуються. Тому A×B≠B×A, тобто декартовий добуток властивості комутативності не має.

Самостійний інтерес викликає випадок, коли множини A і B рівні між собою. Тоді елементами упорядкованої пари множини A×B будуть об'єкти, які складаються із двох не обов'язково різних елементів множини A. Також важливим залишається порядок елементів у парі. Для наведеної вище множини A, упорядковані пари (1,2) та (2,1) слід вважати різними.

Означення 2.2. Множина $C = \{(a_1,a_2) \mid a_1,a_2 \in A\}$ всіх впорядкованих пар елементів із множини А називається **декартовим квадратом множини А** і позначається A^2.

Поняття упорядкованої пари можна розширити на упорядковані трійки елементів (a_1,a_2,a_3), упорядковані четвірки (a_1,a_2,a_3,a_4) і т.д. Взагалі, упорядкована n-ка елементів із множини А – це n не обов'язково різних між собою елементів із А, заданих в певній послідовності.

Наведене вище означення декартового добутку двох множин і декартового квадрату множини можна звичайним способом узагальнити і на випадок довільної скінченої сукупності множин.

Декартовим добутком $A_1 \times A_2 \times ... \times A_n$ множин $A_1, A_2,...,A_n$ називається сукупність послідовностей (тобто сукупність упорядкованих n-ок елементів) виду $(a_1,a_2,...,a_n)$, де $a_i \in A_i$, i=1,..,n.

Елементи декартового добутку називають іще **кортежами** або **вектором** довжиною n.

Якщо $A_1=A_2=...=A_n=A$, то декартовий добуток $A_1 \times A_2 \times ... \times A_n$ називається **декартовим добутком n-ї степені множини А (A^n)**.

Властивості асоціативності для декартового добутку не виконуються, але виконується властивість дистрибутивності відносно об'єднання, перерізу і відносного доповнення (різниці).

$(A_1 \cup A_2) \times B = (A_1 \times B) \cup (A_2 \times B)$

$(A_1 \cap A_2) \times B = (A_1 \times B) \cap (A_2 \times B)$

$(A_1 \setminus A_2) \times B = (A_1 \times B) \setminus (A_2 \times B)$

Операція декартового добутку відрізняється від операції, введених раніше, тим, що елементи добутку множин суттєво відрізняються від елементів співмножників і є об'єктами іншої природи. Наприклад, якщо R – множина дійсних чисел, то декартовий добуток $R \times R$ – множина всіх точок площини.

Відношення

Означення 2.3. Довільна підмножина множини $A_1 \times A_2 \times ... \times A_n$ називається **відношенням**, заданим або визначеним на множинах $A_1, A_2,...,A_n$. Якщо $A_1=A_2=...=A_n=A$, тобто річ йде про декартовий добуток n-ої степені множини A, то відношення R, яке задано на множинах $A_1=A_2=...=A_n$, називається **n-арним відношенням на множині A**.

Коли $(a_1,a_2,...,a_n) \in R$, то говорять, що елементи a_i (i=1,..,n) знаходяться між собою у відношенні R або відношення R істинне для $a_1,a_2,...,a_n$. Якщо $(a_1,a_2,...,a_n) \notin R$, то вважають, що R хибне для $a_1,a_2,...,a_n$. При n=1 відношення називається **унарним**, при n=2 – **бінарним**, при n=3 – **тернарним**.

Загалом відношення означає який-небудь зв'язок між предметами або поняттями. Приклади бінарних відношень: відношення належності, включення множин, рівності дійсних чисел, нерівності, бути братом, ділитися на яке-небудь натуральне число, входити до складу якого-небудь колективу.

Частіше за все бінарні відношення записуються у вигляді співвідношень aRb, де R – відношення, яке встановлює зв'язок між елементами $a \in A$ та $b \in B$.

Наведемо ще декілька прикладів бінарних відношень.

1. Якщо A – множина дійсних чисел, то $\{(x,y) \mid x \in A, y \in A, x^2+y^2=4\}$ є бінарне відношення на A.

2. Нехай A – множина товарів в магазині, а B – множина дійсних чисел. Тоді $\{(x,y) \mid x \in A, y \in B$, y – ціна x$\}$ – відношення множин A та B.

3. Якщо A – множина людей, то $\{(x,y) \mid x \in A, y \in A$, y є рідним x$\}$ є бінарне відношення на A.

Означення 2.4. **Область визначення** відношення R на A та B є множина всіх $a \in A$ таких, що для деяких $b \in B$ маємо $(a,b) \in R$. Іншими словами, область визначення R є множина всіх перших координат впорядкованих пар із R. **Множина значень** відношення R на A та B є множина всіх $b \in B$ таких, що $(a,b) \in R$ для деяких $a \in A$. Іншими словами,

множина значень R є множина всіх других координат впорядкованих пар із R.

В наведених прикладах вище, у (1) область визначення і множина значень співпадають із множиною $\{t: t\in[-2;2]\}$. В (2) область визначення є множина А, а множина значень є множина всіх дійсних чисел, кожне з яких співпадає із ціною деякого товару в магазині. В (3) область визначення і множина значень є множиною всіх людей, які мають рідних.

Цікавими є такі окремі випадки відношень на А.

1. **Повне (універсальне)** відношення $U=A\times A$, яке справджується для будь-якої пари (a_1,a_2) елементів з А. Наприклад, U – відношення "вчитися в одній групі" у множині А, де А – множина студентів групи КН 1/1.

2. **Тотожне (діагональне)** відношення I, що виконується тільки між елементом і ним самим. Наприклад, рівність на множині дійсних чисел.

3. **Порожнє** відношення, яке не задовольняє жодна пара елементів з А. Наприклад, R – відношення "бути братом" у множині А, де А – множина жінок.

Оскільки відношення, задані на А та В – підмножини $A\times B$, то для них визначені операції об'єднання, перерізу, різниці і доповнення (наступне справедливо для загального випадку відношення):

- $(a,b)\in R_1\cup R_2 \Leftrightarrow (a,b)\in R_1$ або $(a,b)\in R_2$
- $(a,b)\in R_1\cap R_2 \Leftrightarrow (a,b)\in R_1$ і $(a,b)\in R_2$
- $(a,b)\in R_1\setminus R_2 \Leftrightarrow (a,b)\in R_1$ або $(a,b)\notin R_2$
- $(a,b)\in R' \Leftrightarrow (a,b)\notin R$ (заперечення)

Крім того, виділяються специфічні для відношень операції: обернення (симетризація) і композиція.

<u>Означення 2.5.</u> Нехай $R\subseteq A\times B$ є відношення на $A\times B$. Тоді відношення R^{-1} на $B\times A$ визначається наступним чином

$R^{-1} = \{(b,a) \mid (a,b)\in R\}$.

Іншими словами, $(b,a)\in R^{-1}$ тоді і тільки тоді, коли $(a,b)\in R$, або, що рівнозначно, $bR^{-1}a$ тоді і тільки тоді, коли aRb. Відношення R^{-1} називається **оберненим (симетричним) відношенням** до даного відношення R.

Перехід від R до R^{-1} здійснюється взаємною перестановкою координат кожної впорядкованої пари. Наприклад, відношення R - "x дільник y", має обернене до нього R^{-1} – "x кратне y". А відношення R = {(1,2), (3,4), (5,6)} буде мати обернене відношення R^{-1}={(2,1), (4,3), (6,5)}. При переході від R до R^{-1} область визначення стає областю значення і навпаки.

Означення 2.6. Нехай $R\subseteq A\times B$ – відношення на $A\times B$, а $S\subseteq B\times C$ – відношення на $B\times C$. **Композицією** відношень R та S є відношення $T\subseteq A\times C$, визначене наступним чином:

$T = \{(a,c) \mid a\in A, c\in C$ та $\exists b\in B, (a,b)\in R$ та $(b,c)\in S\}$.

Це відношення позначається $T = R°S$.

Наприклад, нехай R = {(1,2), (3,4), (5,6)} та S={(2,3),(2,7),(4,1),(6,9)}, тоді $T_1 = R°S$ = {(1,3), (1,7), (3,1), (5,9)} та $T_2 = S°R$ = {(2,4),(4,2)}. Інший приклад: $R = \{(x,x^2) \mid x\in N\}$ та $S = \{(x,x+2) \mid x\in N\}$, тоді $T_1 = R°S = \{(x,x^2+2) \mid x\in N\}$ та $T_2 = S°R = \{(x,(x+2)^2) \mid x\in N\}$.

Слід зазначити, що операція композиції відношень може бути і невизначеною, якщо в множині B для заданих елементів a із A та c із C не існує відповідного елемента b. Але якщо A=B=C, то ця операція завжди визначена.

Означення 2.7. Нехай R – відношення на множині A. Ступенем відношення R на множині A є його композиція із самим собою. Позначається:

$R^n = R°\ldots$(n разів)$\ldots°R$.

Відповідно, $R^0 = I$, $R^1 = R$, $R^2 = R°R$ і взагалі $R^n = R^{n-1}°R$.

Теорема 2.1. Якщо R, R_1, R_2 – бінарні відношення, задані на множині A, то:

а) $(R_1\cup R_2)°R = R_1°R \cup R_2°R$; $R_1\subseteq R_2 \Rightarrow R_1°R \subseteq R_2°R$.

б) $(R^{-1})^{-1} = R$; $R \subseteq R_1 \Rightarrow R^{-1} \subseteq R_1^{-1}$.

в) $(R_1 \circ R_2)^{-1} = (R_2^{-1}) \circ (R_1^{-1})$.

г) $(R_1 \cap R_2)^{-1} = (R_1^{-1}) \cap (R_2^{-1})$.

д) $(R \circ R_1) \circ R_2 = R \circ (R_1 \circ R_2)$.

Доведення. а) Якщо $(a,b) \in (R_1 \cup R_2) \circ R$, то існує елемент $c \in A$ такий, що $(a,c) \in R_1 \cup R_2$ і $(c,b) \in R$. Значить, $(a,c) \in R_1$ або $(a,c) \in R_2$ і $(c,b) \in R$. Звідси маємо, що $(a,b) \in R_1 \circ R$ або $(a,b) \in R_2 \circ R$, тобто $(a,b) \in R_1 \circ R \cup R_2 \circ R$. Обернене включення доводиться аналогічно.

Друга частина твердження випливає з того, що коли $R_1 \subseteq R_2$, то $R_1 \cup R_2 = R_2$, звідки маємо (в силу вище доведеного), що $(R_1 \cup R_2) \circ R = R_1 \circ R \cup R_2 \circ R = R_2 \circ R$, тобто $R_1 \circ R \subseteq R_2 \circ R$.

б) $(a,b) \in R^{-1} \Leftrightarrow (b,a) \in (R^{-1})^{-1} \Leftrightarrow (b,a) \in R$. Звідки випливає, що $(R^{-1})^{-1} = R$.

Для доведення другої частини зауважимо, що $(a,b) \in R \Leftrightarrow (b,a) \in R^{-1}$, $(a,b) \in R \Rightarrow (a,b) \in R_1 \Rightarrow (b,a) \in R^{-1} \Rightarrow (b,a) \in R_1^{-1}$, тобто $R^{-1} \subseteq R_1^{-1}$.

в) $(a,b) \in (R_1 \circ R_2)^{-1} \Leftrightarrow (b,a) \in (R_1 \circ R_2) \Rightarrow (\exists c \in A \mid (b,c) \in R_1 \text{ і } (c,a) \in R_2)$. Але тоді $(c,b) \in R_1^{-1}$ і $(a,c) \in R_2^{-1} \Rightarrow (a,b) \in (R_2^{-1} \circ R_1^{-1})$, тобто $(R_1 \circ R_2)^{-1} \subseteq (R_2^{-1}) \circ (R_1^{-1})$. Обернене включення доводиться аналогічно.

г) $(a,b) \in (R_1 \cap R_2)^{-1} \Leftrightarrow (b,a) \in R_1 \cap R_2 \Leftrightarrow (b,a) \in R_1$ і $(b,a) \in R_2 \Leftrightarrow (a,b) \in R_1^{-1}$ і $(a,b) \in R_2^{-1}$, тобто $(R_1 \cap R_2)^{-1} = (R_1^{-1}) \cap (R_2^{-1})$.

д) Нехай $(a,d) \in (R \circ R_1) \circ R_2$, тоді існує $c \in A$ такий, що $(a,c) \in R \circ R_1$ і $(c,d) \in R_2$. Отже існує такий b, що $(a,b) \in R$, $(b,c) \in R_1$ і $(c,d) \in R_2$, а це означає, що $(b,d) \in R_1 \circ R_2$ і $(a,d) \in R \circ (R_1 \circ R_2)$, тобто $(R \circ R_1) \circ R_2 \subseteq R \circ (R_1 \circ R_2)$. Обернене включення доводиться аналогічно. ►

Способи задання відношень

Означення 2.8. Розглянемо відношення $R \subseteq A \times B$. Нехай елемент $a_i \in A$. **Перерізом відношення A за елементом a_i** називається множина елементів b з B, для яких пара $(a_i,b) \in R$:

$R(a_i) = \{b \in B \mid (a_i,b) \in R\}$.

Множину всіх перерізів відношення R називають **фактором-множиною** множини B за відношенням R і позначають B/R. Вона повністю визначає відношення R.

Наприклад, нехай A={1,2,3}, B={2,3,4,5,6}. Відношення R = {(1,2), (1,4), (2,3), (3,3), (3,6)}. Очевидно, R(1) = {2,4}, R(2) = {3}, R(3) = {3,6}. Множина {R(1), R(2), R(3)} є фактор-множиною B/R.

Об'єднання перерізів за елементами деякої підмножини C⊆A є перерізом R(C) відношення R за підмножиною C, тобто

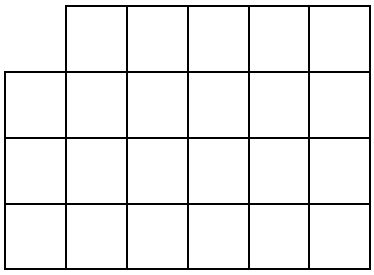
$$R(C) = \bigcup_{a \in C} R(c).$$

Так для C={1,2}, маємо R(C) = {2,3,4} = R(1)∪R(2).

З попереднього зрозуміло, що відношення може бути подане за допомогою фактор-множини. Розглянемо ще два способи подання скінченого бінарного відношення: за допомогою матриці та графа.

Матричний спосіб ґрунтується на поданні відношення R⊆A×B відповідною йому прямокутною таблицею (матрицею), що складається з нулів та одиниць, де рядки – перші координати, а стовпці – другі, причому на перетині i-го рядка і j-го стовпця буде 1, якщо виконується співвідношення $a_i R b_j$, або 0 – якщо воно не виконується.

Для наведеного вище відношення матриця буде мати такий вигляд:



Матриця повного (універсального) відношення – це квадратна матриця, що складається лише з одиниць. Матриця тотожного (діагонального) відношення – це квадратна матриця, яка складається з нулів та одиниць по головній діагоналі. Матриця порожнього відношення – це квадратна матриця, що складається лише з нулів.

Відношення $R \subseteq A \times B$ можна також зображати за допомогою **орієнтованого графа**. Елементи множин A та B зображаються точками на площині (вершини), а впорядковані пари – лінією зі стрілкою (дуги), яка направлена від a до b, якщо aRb.

Для наведеного вище відношення граф буде мати наступний вигляд:

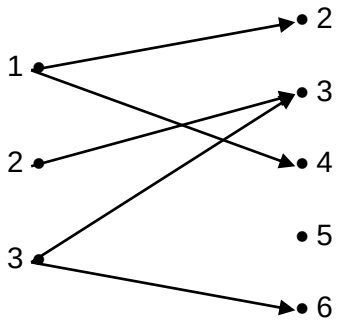


Рис 2.1. Приклад представлення відношення за допомогою графа.

Граф бінарного відношення – це дводольний граф. Відношення в A зображується графом із вершинами, що відповідають елементам цієї множини. Якщо $a_i R a_j$ і $a_j R a_i$, то вершини зв'язуються двома протилежно спрямованими дугами, які умовно можна замінювати однією не спрямованою дугою (ребром). Співвідношенню $a_i A a_i$ відповідає петля.

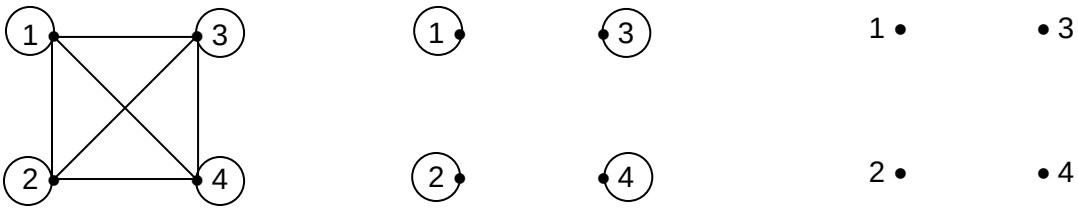


Рис 2.2. Графи універсального (а), тотожного (б) та порожнього (в) відношень.

Нехай A={1,2,3,4}. Тоді граф універсального відношення на A зображено на рис. 2.2,а, граф тотожного відношення на A – на рис. 2.2,б, а граф порожнього відношення на A – на рис 2.2,в.

Матриця оберненого відношення R^{-1} для відношення R – це транспонована матриця відношення R. Граф оберненого відношення R^{-1} утворюється із графа відношення R заміною всіх дуг на протилежні.

Матриця композиції відношень T = R°S утворюється як добуток матриць відношень R та S з подальшою заміною відмінних від нуля елементів одиницями.

Справді, елемент t_{ik} матриці композиції знайдемо як суму добутків відповідних елементів матриць R та S (відповідно до правила множення матриць):

$$t_{ik} = r_{i1}s_{1k} + r_{i2}s_{2k} + \ldots + r_{in}s_{nk} = \sum_{j=1}^{n} r_{ij}s_{jk} .$$

Очевидно, така сума відмінна від нуля тоді й тільки тоді, коли хоча б один доданок відмінний від нуля, тобто дорівнює одиниці:

$$r_{ij}s_{jk} = 1 \Leftrightarrow r_{ij} = 1 \text{ та } s_{jk} = 1 \Leftrightarrow a_i R b_j \text{ та } b_j S c_k \Leftrightarrow a_i R^{\circ} S c_k.$$

Якщо у виразі t_{ik} не один, а кілька одиничних доданків, то кожен з них відповідає одному й тому самому співвідношенню $a_i R^{\circ} S c_k$, через що їх сума має бути замінена одиницею.

Для композиції відношень R = {(1,2), (2,1), (2,2), (3,3), (3,4)} та S={(1,1), (1,2), (2,3), (2,5), (3,2), (3,4), (4,2) (4,3)} матриця утворюється так:

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Нехай $R \subseteq A \times B$ та $S \subseteq B \times C$. Щоб побудувати граф T = R°S, потрібно до графа відношення R добудувати граф відношення S. Граф композиції відношень дістанемо, якщо вилучимо вершини, які відповідають елементам множини B. При вилученні вершини b_j кожний шлях, що проходить через неї від вершин множини A до вершин множини C, замінюється однією дугою з тим самим напрямком.

Для останнього прикладу маємо наступний граф:

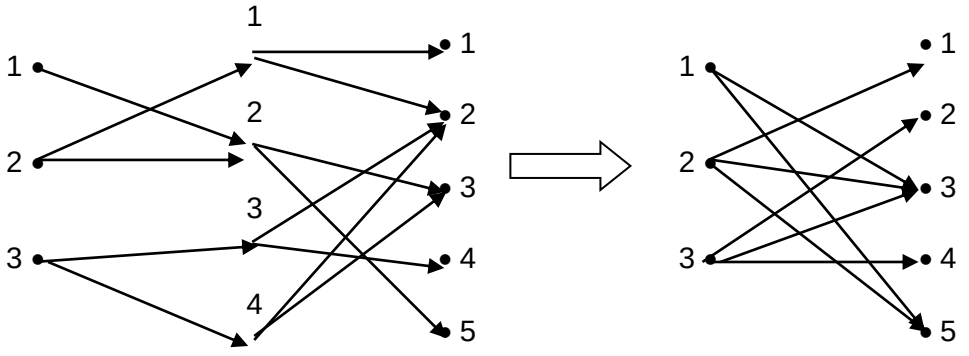


Рис 2.3. Граф композиції відношень.

Властивості відношень

Означення 2.9. Нехай R – бінарне відношення у множині A ($R \subseteq A \times A$). Тоді відношення R є:

- **рефлексивним**, якщо $I \subseteq R$, тобто, іншими словами, воно завжди виконується між елементом і ним самим ($\forall a \in A$, aRa). Як приклад такого відношення можна навести відношення нестрогої нерівності на множині натуральних або дійсних чисел.

Матриця рефлексивного відношення характеризується тим, що всі елементи її головної діагоналі – одиниці. Граф рефлексивного відношення – тим, що петлі є у всіх вершинах.

- **антирефлексивним (іррефлексивним)**, якщо $R \cap I = \varnothing$, тобто якщо співвідношення $a_i R a_j$ виконується, то $a_i \neq a_j$. Це, наприклад, відношення строгої нерівності на множинах натуральних або дійсних чисел, відношення “бути старшим” у множині людей.

Матриця антирефлексивного відношення характеризується тим, що всі елементи її головної діагоналі – нулі. Граф антирефлексивного відношення не має жодної петлі.

- **симетричним**, якщо $R = R^{-1}$, тобто при виконанні співвідношення $a_i R a_j$ виконується співвідношення $a_j R a_i$. Як приклад такого відношення можна навести відстань між двома точками на площині, відношення “бути братом” на множині людей.

Симетричність відношення спричиняє також симетричність матриці. Також для такого відношення вершини графа можуть бути пов’язані тільки парами протилежно спрямованих дуг (тобто ребрами).

- **асиметричним**, якщо $R \cap R^{-1} = \varnothing$, тобто із двох співвідношень $a_i R a_j$ та $a_j R a_i$ щонайменше одне не виконується. Як приклад такого відношення можна навести відношення “бути батьком” у множині людей, відношення строго включення в множині всіх підмножин деякого універсуму. Очевидно, якщо відношення асиметричне, то воно й антирефлексивне.

Матриця асиметричного відношення характеризується тим, що всі елементи її головної діагоналі – нулі й немає жодної пари одиниць на місцях, симетричних відносно головної діагоналі. У графа такого відношення петлі відсутні, а вершини можуть бути пов’язані тільки однією спрямованою дугою.

- **антисиметричним**, якщо $R \cap R^{-1} \subseteq I$, тобто обидва співвідношення $a_i R a_j$ та $a_j R a_i$ одночасно виконуються тоді й тільки тоді, коли $a_j = a_i$. Як приклад можна навести нестрогу нерівність.

Матриця антисиметричного відношення має ті самі властивості, що й асиметричного, за винятком вимоги рівності нулю елементів головної діагоналі. У графі такого відношення можуть бути петлі, але зв’язок між вершинами, якщо він є, також відбувається тільки однією спрямованою дугою.

- **транзитивним**, якщо $R \circ R \subseteq R$, тобто з виконання співвідношень $a_i R a_j$ та $a_j R a_k$ випливає виконання співвідношення $a_i R a_k$. Як приклад можна навести відношення “бути дільником” на множині цілих чисел, “бути старшим” на множині людей.

Матриця транзитивного відношення характеризується тим, що коли $r_{ij}=1$ й $r_{jk}=1$, то $r_{ik}=1$, причому наявність одиничних елементів на головній діагоналі не порушує транзитивність матриці. Граф транзитивного відношення характеризується тим, що коли через деяку сукупність вершин графа проходить шлях, то існують дуги, які з’єднують будь-яку пару вершин з цією сукупністю в напрямку шляху. Як правило, на графі транзитивного відношення зображують тільки цей шлях, а зумовлені транзитивністю дуги

опускають. Такий граф називають **графом редукції** (або **кістяковим графом**).

Означення 2.10. Нехай R – бінарне відношення на множині A. **Рефлексивним замкненням** R є найменше рефлексивне відношення на A, що містить R як підмножину. **Симетричне замкнення** R є найменше симетричне відношення на A, що містить R як підмножину. **Транзитивне замкнення** R є найменше транзитивне відношення на A, яке містить R як підмножину.

Теорема 2.2. Нехай R – бінарне відношення на множині A і I – тотожне відношення на A. Тоді:

а) $R \cup I$ є рефлексивним замкненням R.

б) $R \cup R^{-1}$ є симетричним замкненням R.

в) якщо A – кінцева множина, що містить n елементів, то відношення $R \cup R^2 \cup R^3 \cup \ldots \cup R^n$ є транзитивним замкненням R.

Доведення. Доведення тверджень (а) та (б) залишаємо на самостійну роботу. Позначимо транзитивне замкнення R через R^T. Для доведення твердження (в) спочатку покажемо, що $R \cup R^2 \cup R^3 \cup \ldots \cup R^n \subseteq R^T$. Проведемо індукцію по n. Для n=1 маємо $R \subseteq R^T$, що безумовно істинно. Нехай $R \cup R^2 \cup R^3 \cup \ldots \cup R^k \subseteq R^T$. Необхідно показати, що $R \cup R^2 \cup R^3 \cup \ldots \cup R^k \cup R^{k+1} \subseteq R^T$ або, що теж саме, $R^{k+1} \subseteq R^T$. Нехай $(a,c) \in R^{k+1}$. Тоді існує b таке, що $(a,b) \in R^k$ і $(b,c) \in R$. Але, згідно індуктивному припущенню, (a,b) і $(b,c) \in R^T$. Оскільки R^T транзитивне, $(a,c) \in R^T$. Тому $R \cup R^2 \cup R^3 \cup \ldots \cup R^{k+1} \subseteq R^T$. Для того, щоб показати, що $R^T \subseteq R \cup R^2 \cup R^3 \cup \ldots \cup R^n$, просто покажемо, що $R \cup R^2 \cup R^3 \cup \ldots \cup R^n$ транзитивне. Нехай $(a,b) \in R^j$ і $(b,c) \in R^k$. Тоді $(a,c) \in R^{j+k}$. Якщо a=c, твердження доведено. Інакше існують $b_2, b_3, b_4, \ldots, b_{j+k-1} \in A$ такі, що (a,b_2), (b_2,b_3), $(b_3,b_4),\ldots,(b_{j+k-2},b_{j+k-1})$, $(b_{j+k-1},c) \in R$. Позначимо a через b_1, а c через b_{j+k}. Якщо деякі із b_i рівні, наприклад, $b_p=b_q$, із вказаної вище послідовності впорядкованих пар, які знаходяться у відношення R, можна видалити (b_p,b_{p+1}), $(b_{p+1}, b_{p+2}),\ldots,(b_{q-1},b_q)$ і після цього отримати послідовність $a, b_2,$

$b_3,\ldots,b_{p-1},b_q,\ldots,b_{j+k-1},c$, в якій кожний попередній елемент знаходиться у R-відношенні до наступного. Так можна продовжувати до тих пір, поки всі елементи не стануть відмінними, але при цьому кожний з них буде знаходитись у R-відношенні до наступного. Оскільки у множині A існує тільки n різних елементів, отримаємо, що $(a,c)\in R^n$ і $R\cup R^2\cup R^3\cup\ldots\cup R^n$ транзитивне.

2. МАТЕМАТИЧНА ЛОГІКА

2.1. Алгебра висловлень

Термін «логіка» походить від грецького λόγος, що означає слово, думка, поняття, міркування. У процесі осмислення взаємозв'язку між мовою та мисленням давньогрецькі філософи поступово сформували логіку як науку про закони, форми та способи правильного міркування. Її мета – визначити, які способи мислення приводять до істинних висновків і як вибудовувати міркування, щоб уникати помилок.

Поняття висловлення. Логічні операції (зв'язки). Складені висловлення

Просте (елементарне) висловлення – це просте твердження, тобто розповідне речення, щодо змісту якого доречно ставити запитання про його правильність або неправильність. Прості висловлення, у яких виражено правильну думку, називають істинними, а ті, що виражають неправильну, – хибними.

Приклад. Чи є наведений вираз простим висловленням? Якщо вираз є висловленням, то вказати, яким саме – істинним чи хибним.

(а) Число 48 є парним.

(б) У цьому абзаці сім слів.

(в) Нехай нам щастить!

(г) Париж – столиця Нідерландів.

(д) Існує нескінченно багато натуральних чисел.

(е) Чи можна поділити 17 на 5 без остачі?

(є) Не розмовляйте під час лекції.

(ж) Сьогодні йде дощ.

(з) Перевірте правильність розв'язку.

(и) Рівність $5 + 7 = 12$ істинна.

(і) Рівність $10 < 4$ істинна.

(ї) Це висловлення є істинним.

У наведених прикладах висловленнями є лише ті речення, зміст яких можна однозначно оцінити як істинний або хибний факт. Істинними є твердження: (а); (д); (и). Хибними є висловлення: (б); (г); (і). Речення (ж) може бути істинним або хибним залежно від обставин, але все ж є висловленням.

Речення, які є наказами, побажаннями або запитаннями ((в), (є), (з)), не відносять до висловлень, оскільки вони не мають істиннісного значення. Вислів (ї) становить логічний парадокс, у якому неможливо встановити істинність без суперечності, тому він також не є висловленням у логічному сенсі.

Зазвичай конкретні елементарні висловлення позначають малими латинськими літерами: a, b, c, … (інколи з індексами), а значення висловлень істинно та хибно – відповідно символами 1 та 0 (або **I** та **X**, а в англомовній літературі – відповідно **T** і **F**).

Крім того, розглядатимемо **змінні висловлення**, які позначатимемо латинськими літерами x, y, z, … (інколи з індексами) і називатимемо також **пропозиційними** змінними. Після підстановки замість пропозиційної змінної певного елементарного висловлення ця змінна набуде відповідного значення (1 або 0).

Окремі елементарні висловлення можна з'єднувати між собою за допомогою певних зв'язок (сполучників), утворюючи складені висловлення.

У математичній логіці використання мовних зв'язок трактується як виконання над висловленнями певних логічних операцій, що мають такі назви: кон'юнкція, диз'юнкція, заперечення, імплікація та еквівалентність. У табл. 2.1 наведено різні назви та позначення, що використовують для цих операцій.

Таблиця 2.1

Назва	Позначення
Кон'юнкція (логічне множення, логічне *і*)	$\wedge$ & $\cdot$
Диз'юнкція (логічне додавання, логічне *або*)	$\vee$
Заперечення (логічне *ні*)	$\neg$ ′ ¯
Імплікація (логічне *якщо*, *…то…*)	$\rightarrow \supset \Rightarrow$
Еквівалентність (рівнозначність)	$\sim \leftrightarrow \equiv$

Зазвичай використовуватимемо перші із наведених назв і по значень. Табл. 2.2 містить означення цих операцій.

Таблиця. 2.2

$x\ y$	$x \wedge y$	$x \vee y$	$\neg x$	$x \rightarrow y$	$x \sim y$
0 0	**0**	**0**	**1**	**1**	**1**
0 1	**0**	**1**	**1**	**1**	**0**
1 0	**0**	**1**	**0**	**0**	**0**
1 1	**1**	**1**	**0**	**1**	**1**

Отже, з елементарних висловлень і пропозиційних змінних за допомогою означених операцій і дужок утворюються складені висловлення, яким відповідають формули або вирази. Зауважимо, що символам логічних операцій відповідають у звичайній мові такі мовні зв'язки, або сполучники:

∧ – і; та; а; але; хоч; разом із; незважаючи на; …

∨ – або; чи; хоч (принаймні) одне з; …

¬ – не; неправильно, що; …

→ – якщо (коли) … , то (тоді)…; … імплікує …; із … випливає …; у разі … має місце …; …

~ – … тоді й тільки тоді, коли …; … якщо й тільки якщо …; … еквівалентне …; … рівносильне … тощо.

Застосовуючи пропозиційні змінні та символи логічних операцій, будь-яке складене висловлення можна формалізувати, тобто перетворити на формулу, яка виражатиме (задаватиме) його логічну структуру.

Приклади.

1. Висловлення *Якщо число 30 кратне 2 і 5, то число 30 кратне 10* має таку логічну структуру: (a ∧ b) → c. Тут пропозиційній змінній *a* відповідає

елементарне висловлення *Число 30 кратне 2*, змінній b – висловлення *Число 24 кратне 5*, а змінній c – висловлення *Число 30 кратне 10*.

2. Нехай задано елементарні висловлення:

a) 10 – парне число; b) 10 – додатне число;

c) 10 – просте число; d) Число 10 кратне 4.

Сформулювати словами складене висловлення, визначити його істинність чи хибність для таких формул:

(а) $(b \to \neg a) \vee c$; (б) $(\neg a \wedge \neg c) \to d$.

Формула (а) задає складене висловлення *Якщо 10 – додатне число, то 10 – не парне число, або 10 – просте число*. Що є хибним, адже йому відповідає логічний вираз $\mathbf{0 \vee 0}$, який має значення **0**.

Формулі (б) відповідатиме складене висловлення *Якщо 10 – не парне число і 10 – не просте (складене) число, то число 10 кратне 4*, що є істинним, адже $\mathbf{0 \to 0}$ є істинним логічним виразом.

У математичній мові імплікацію $p \to q$ трактують так: твердження p є достатньою умовою для q, а твердження q – необхідною умовою для твердження p. Вираз $p \to q$ інтерпретують ще як q тоді, коли p або p тільки тоді, коли q. В імплікації $p \to q$ операнд p називають **антецедентом**, або засновком, а q – **консеквентом**, або висновком.

Приклад.

Записати словами у вигляді твердження задане висловлення різними способами, використовуючи вирази: *необхідна умова; достатня умова; тоді, коли; тільки тоді, коли*.

(а) (24 кратне 6) → (24 кратне 3).

Для пункту (а) такими твердженнями будуть:

– висловлення 24 кратне 3 є необхідною умовою для висловлення 24 кратне 6;

– висловлення 24 кратне 6 є достатньою умовою для висловлення 24 кратне 3;

– 24 кратне 3 тоді, коли 24 кратне 6;

– 24 кратне 6 тільки тоді, коли 24 кратне 3.

2.2. Числення висловлень

Формули алгебри висловлень. Таблиця істинності. Тавтології

Алфавіт найбільш поширеної формальної мови алгебри висловлень складається з трьох груп символів:

1) символи елементарних висловлень і пропозиційних змін них: a, b, c, … та x, y, z, … (інколи з індексами);

2) символи операцій: ∧, ∨, ¬, →, ~ ;

3) допоміжні символи – круглі дужки: (і).

Із символів цього алфавіту будують пропозиційні формули або просто формули алгебри висловлень за індуктивним правилом:

1) усі пропозиційні змінні та елементарні висловлення є формулами;

2) якщо A та B – формули, то вирази (A ∧ B), (A ∨ B), (¬ A), (A → B), (A ~ B) також є формулами (для всіх цих виразів фор мули A та B є підформулами);

3) інших формул, крім тих, що побудовані за правилами 1) та 2), немає.

Формули алгебри висловлень позначатимемо великими латинськими літерами.

Приклад.

Визначити, чи є послідовність символів формулою алгебри висловлень.

(a) (((x → y) ∧ z) ~ ((¬ x) → (y ∨ z))).

Для цього за допомогою індексів спочатку занумеруємо по рядок виконання операцій у першій послідовності символів (у багатьох випадках ця процедура виконується неоднозначно).

Матимемо такий вираз: (((x $\to_1$ y) $\wedge_2$ z) $\sim_6$ ((¬ 3x) $\to$5 (y $\vee_4$ z))) (зручно відповідний номер записувати над операцією).

Подамо його у вигляді

($F_1 \sim_6 F_2$), де F_1 = ((x $\to_1$ y) $\wedge_2$ z) і F_2 = ((¬ 3x) $\to_5$ (y $\vee_4$ z)).

У свою чергу, формула F1 має вигляд (F11 ∧2 F12) і розкладається на підформули F_{11} = (x $\rightarrow_1$ y) і F_{12} = z, а формула F_2 має вигляд (F_{21} $\rightarrow_5$ F_{22}) і розкладається на підформули F_{21} = (¬ 3x) і F_{22} = (y $\vee_4$ z).

Вираз F_{12} є формулою згідно з п. 1) в означенні пропозиційної формули. А кожна з решти підформул F_{11}, F_{21} та F_{22} утворюється відповідно до п. 2) цього означення:

$$F_{11} = (F_{111} \rightarrow_1 F_{112}),$$

де F_{111} = x і F_{112} = y,

$$F_{21} = (\neg_3 F_{211}),$$

де F_{211} = x і, нарешті,

$$F_{22} = (F_{221} \vee_4 F_{222}),$$

де F_{221} = y та F_{222} = z.

Отже, ми продемонстрували, що ця формула побудована із пропозиційних змінних

$$F_{12} = z,\ F_{111} = x,\ F_{112} = y,\ F_{211} = x,\ F_{221} = y,\ F_{222} = z$$

за викладеними вище правилами. При спробі аналогічно розкласти другу послідовність символів на певному кроці отримаємо вираз (F1 ~ F2, який не має закриваючої дужки. Отже, ця послідовність не є пропозиційною формулою.

Нехай $\mathbf{p_1, p_2, \ldots, p_n}$ – це всі пропозиційні змінні, що входять до формули A; позначатимемо цей факт $\mathbf{A(p_1, p_2, \ldots, p_n)}$. Формулі $\mathbf{A(p_1, p_2, \ldots, p_n)}$ поставимо у відповідність функцію $\mathbf{f\ (p_1, p_2, \ldots, p_n)}$, що означена на множині впорядкованих наборів $\mathbf{(p_1, p_2, \ldots, p_n)}$, де кожне $\mathbf{p_i}$ набуває значення у множині $\mathbf{B = \{0, 1\}}$, і значенням функції **f** є **0** або **1**. Значення функції f на наборі значень $a_1, a_2, \ldots, a_n$ її змінних $p_1, p_2, \ldots, p_n$ дорівнює значенню формули $A(p_1, p_2, \ldots, p_n)$ при підстановці до неї замість пропозиційних змінних $p_1, p_2, \ldots, p_n$ значень $a_1, a_2, \ldots, a_n$, відповідно. Зауважимо, що **кількість елементів в області визначення функції f** дорівнює $\mathbf{2^n}$.

Функцію f називають **функцією істинності** для формули A або відповідного складеного висловлення. Для функції істинності f можна

побудувати таблицю істинності (табл. 2.3). Традиційно набори значень змінних розташовують у цій таблиці в лексикографічному порядку.

Таблиця 2.3

$p_1\, p_2 \ldots p_{n-1}\, p_n$	$f(p_1, p_2, \ldots, p_{n-1}, p_n)$
0 0 ... 0 0	f**(0, 0, ..., 0, 0)**
0 0 ... 0 1	f**(0, 0, ..., 0, 1)**
0 0 ... 1 0	f**(0, 0, ..., 1, 0)**
0 0 ... 1 1	f**(0, 0, ..., 1, 1)**
.....	.....
1 1 ... 1 0	f**(1, 1, ..., 1, 0)**
1 1 ... 1 1	f**(1, 1, ..., 1, 1)**

Приклад.

Побудувати таблицю істинності для формули:

$$(((a \to_4 (\neg_1 b)) \to_7 (b \wedge_6 ((\neg_2 c) \to_5 a))) \sim_8 (\neg_3 a))$$

У першому рядку кожного стовпця останньої таблиці записано вираз (підформулу) і номер відповідної операції.

Наприклад, запис (a→(1)) (4) означає, що результатом операції із номером 4 є імплікація значення пропозиційної змінної *a* та результату операції з номером 1, а запис ((4)→(6)) (7) означає, що результатом операції з номером 7 є імплікація значення операції із номером 4 і результату операції із номером 6 тощо.

a b c	$(\neg b)$ (1)	$(\neg c)$ (2)	$(\neg a)$ (3)	$(a \to (1))$ (4)	$((2) \to a)$ (5)	$(b \wedge (5))$ (6)	$((4) \to (6))$ (7)	$((7) \sim (3))$ (8)
0 0 0	1	1	1	1	0	0	0	0
0 0 1	1	0	1	1	1	0	0	0
0 1 0	0	1	1	1	0	0	0	0
0 1 1	0	0	1	1	1	1	1	1
1 0 0	1	1	0	1	1	0	0	1
1 0 1	1	0	0	1	1	0	0	1
1 1 0	0	1	0	0	1	1	1	0
1 1 1	0	0	0	0	1	1	1	0

Формулу алгебри висловлень **$A(p_1, p_2, \ldots, p_n)$** називають **тавтологією**, коли їй відповідає функція істинності, що тотожно дорівнює 1. Те, що формула A є тавтологією, позначають як $\vDash A$.

Тавтології ще називають **тотожно істинними формулами**, або **законами алгебри висловлень**.

Наведемо приклади деяких важливих тавтологій:

$(p \vee (\neg p))$ – закон виключення третього;

$(\neg (p \wedge (\neg p)))$ – закон виключення суперечності;

$(p \to p)$ – закон тотожності.

Переконатись у тому, що ці формули є тавтологіями, можна за допомогою відповідних таблиць істинності.

Іноді перевірку того, що певна формула є тавтологією, виконують за допомогою **способу відшукання контрприкладу** (або методу від супротивного). Пояснимо його на прикладі.

Приклад.

Перевірити, чи є тавтологією формула

$$A = (((a \to \neg b) \wedge (b \to (a \wedge c))) \wedge (\neg c \to \neg a)) \to (a \vee \neg c).$$

Припустимо, що формула A не є тавтологією. Тоді принаймні на одному наборі значень формула A набуває значення **0**. Спробуємо відшукати цей набір. Оскільки останньою (головною) операцією формули A є імплікація, то її консеквент має дорівнювати нулю, а антецедент – одиниці. Консеквент $(a \vee \neg c)$ дорівнює нулю, коли $a = \mathbf{0}$ та $c = \mathbf{1}$. Звідси $(a \to \neg b) = \mathbf{1}$ та $(\neg c \to \neg a) = \mathbf{1}$. Залишилось з'ясувати, чи може за цих умов вираз $(b \to (a \wedge c))$ дорівнювати одиниці. Відповідь позитивна (для $b = \mathbf{0}$). Отже, ми знайшли набір **(0, 0, 1)**, на якому формула A на буває значення 0, тобто відшукали контрприклад, який свідчить, що формула A не є тавтологією.

Якщо формула $A \to B$ є тавтологією, то кажуть, що формула A **сильніша ніж** B, а формула B **слабша ніж** A.

Формула алгебри висловлень $A(p_1, p_2, \ldots, p_n)$, яка набуває значення 0 на всіх наборах $(a_1, a_2, \ldots, a_n)$ значень своїх пропозиційних змінних, називається

суперечністю, або **тотожно хибною формулою**. Формулу, що не є ні тавтологією, ні суперечністю, називають **нейтральною**. Множину всіх формул алгебри висловлень розбивають на тавтології, суперечності та нейтральні формули. Формулу, яка не є суперечністю, називають **виконуваною**, інакше – **невиконуваною**.

Порядок виконання операцій у формулі визначається за допомогою дужок. Задля зменшення їх кількості випускають зовнішні дужки й запроваджують такий порядок (пріоритет) виконання операцій у разі відсутності дужок: ¬, ∧, ∨, →, ~ (за спаданням). Часто у формулах алгебри висловлень випускають знак кон'юнкції ∧ і замість a ∧ b записують ab.

Для визначення порядку виконання операцій у формулі пріоритету операцій не достатньо. Потрібно ще вказувати для однакових операцій, групуються вони зліва направо чи справа наліво. Наприклад, операції ∧ та ∨ групуються зліва направо, а операція → – справа наліво. Тому для формули a ∧ b ∧ c дужки роз ставляємо таким чином: ((a ∧ b) ∧ c), для формули a → b → a дужки розставляємо так: (a → (b → a)). Зазначимо, що для операцій ∧ та ∨ порядок групування не є суттєвим, але для операції → він є важливим. Тому для формули a → b → a при групуванні дужок справа наліво отримаємо формулу (a → (b → a)), яка не еквівалентна попередній формулі (a → (b → a)).

Структура формули. Розстановка дужок у формулі вказує не лише на порядок виконання операцій, а фактично задає її структуру. Тут важливими є поняття головної операції у формулі та її аргументів.

Приклад.

Проаналізувати структуру формули

$$(a \to (b \to (((\neg b) \wedge a) \to (c \vee (a \wedge (\neg c)))))).$$

Головною буде перша імплікація (позначаємо головну операцію зірочкою *). Маємо такий запис:

$$(a \to^{*} (b \to (((\neg b) \wedge a) \to (c \vee (a \wedge (\neg c)))))).$$

Далі аналізуємо підформули.

Підформули a та (b → (((¬ b) ∧ a) → (c ∨ (a ∧ (¬ c))))) задають перший і другий аргументи цієї операції.

Для другої підформули головною буде перша імплікація, тобто

(b →* (((¬ b) ∧ a) → (c ∨ (a ∧ (¬ c))))).

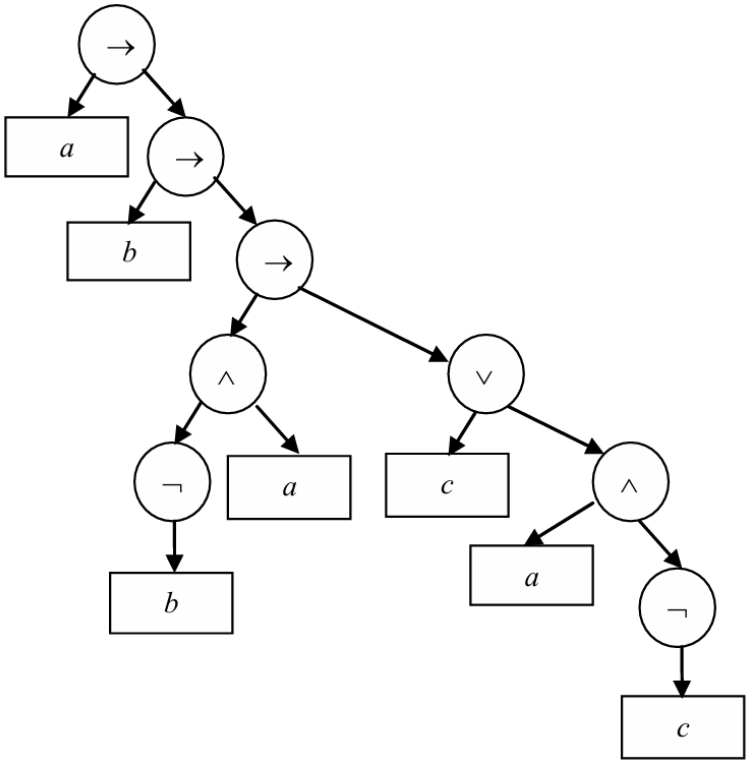
Далі, у підформулі (((¬ b) ∧ a) → (c ∨ (a ∧ (¬ c)))) головною є імплікація, тому отримуємо (((¬b) ∧ a) →* (c ∨ (a ∧ (¬c)))).

Аргументами є підформули ((¬ b) ∧ a) та (c ∨ (a ∧ (¬ c))).

Подаємо першу підформулу у вигляді

((¬ b) ∧* a), а другу – (c ∨* (a ∧ (¬ c))).

Продовжуючи таким чином, підійдемо до найпростіших підформул a, b, c. Структуру формули часто подають **деревом синтаксичного аналізу формули**. У ньому дужки не вказують. Для проаналізованої формули дерево синтаксичного аналізу має вигляд:



Наведене дерево дає наочне уявлення про порядок виконання операцій, оскільки спочатку виконуються операції, записані внизу дерева, а потім ті, які йдуть вище.

Проблема розв'язності в алгебрі висловлень – це задача знаходження алгоритму, за допомогою якого для будь-якої формули А алгебри висловлень можна визначити, є А тотожно істинною (тавтологією), чи ні.

Для алгебри висловлень цю проблему можна, зокрема, роз в'язати такими двома способами:

1) побудувати таблицю істинності для формули А й перевіри ти, чи складається стовпчик значень А лише з одиниць;

2) застосувати спосіб відшукання контрприкладу.

Аналогічно можна сформулювати й розв'язати проблему розв'язності для визначення того, чи є певна формула алгебри висловлень суперечністю або виконуваною.

Рівносильні формули алгебри висловлень.

Формули А та В алгебри висловлень називають **рівносильними**, якщо їм відповідає та сама функція істинності, тобто вони набувають однакових значень на всіх наборах значень їхніх пропозиційних змінних.

Рівносильність формул А та В позначають за допомогою позначення ≡ (= або ↔): записують А ≡ В.

Рівносильні формули ще часто називають **еквівалентними**.

Рівносильність формул можна перевірити складанням таблиць істинності відповідних функцій і порівнюванням цих таблиць.

Рівносильним перетворенням формули А називають дію або процедуру, у результаті якої дістаємо формулу В, рівносильну формулі А.

Неважко довести (побудовою відповідних таблиць істинності) **основні тотожності (рівносильності, закони) алгебри висловлень.**

1. (a ∨ b) ∨ c ≡ a ∨ (b ∨ c), (a ∧ b) ∧ c ≡ a ∧ (b ∧ c) – **асоціативність**;

2. a ∨ b ≡ b ∨ a, a ∧ b ≡ b ∧ a – **комутативність**;

3. a ∧ (b ∨ c) ≡ (a ∧ b) ∨ (a ∧ c), a ∨ (b ∧ c) ≡ (a ∨ b) ∧ (a ∨ c) – **дистрибутивність**;

4. a ∨ a ≡ a, a ∧ a ≡ a – **ідемпотентність**;

5. $\neg (a \vee b) \equiv \neg a \wedge \neg b$, $\neg (a \wedge b) \equiv \neg a \vee \neg b$ – **закони де Моргана**;

6. $\neg \neg a \equiv a$ – **закон подвійного заперечення**;

7. $a \vee 0 \equiv a$, $a \wedge 1 \equiv a$; $a \vee 1 \equiv 1$, $a \wedge 0 \equiv 0$ – **властивості елементів 0 та 1**;

8. $a \vee \neg a \equiv 1$, $a \wedge \neg a \equiv 0$ – **властивості заперечення**;

9. $a \vee (a \wedge b) \equiv a$; $a \wedge (a \vee b) \equiv a$ – **правила поглинання**.

Кожну із наведених рівносильностей неважко довести, побудувавши відповідні таблиці істинності для її правої і лівої частин і порівнявши ці таблиці.

Важливим висновком із цих рівносильностей є те, що операції $\rightarrow$ та $\sim$ є надлишковими в алгебрі висловлень. Кожну під формулу, що містить такі операції, можна замінити на рівно сильну їй (згідно з наведеними рівносильностями), що міститиме лише операції кон'юнкції, диз'юнкції та заперечення.

Нормальні форми логічних функцій. Досконала диз'юнктивна нормальна форма (ДДНФ). Досконала кон'юнктивна нормальна форма (ДКНФ).

Вище описано спосіб побудови таблиці істинності для заданої пропозиційної формули, тобто побудови таблиці логічної функції, яку задає ця формула.

Не менш важливою є обернена задача: для функції, заданої таблицею, графіком, словесно тощо, визначити (побудувати) формулу, що цю функцію задає. У багатьох розділах математики побудувати таку формулу для довільної функції не вдається. Замість формули, яка абсолютно точно визначає вихідну функцію, використовують методи побудови різних формул, що відтворюють цю функцію наближено (або апроксимують її) з певною точністю.

В алгебрі логіки існує кілька процедур, що дають змогу для заданої логічної функції побудувати формули, які задають цю функцію й використовують певний набір логічних операцій.

Будемо вважати, що основною формою задання логічної функції є її таблиця істинності. Якщо функція задана якимось іншим способом (словесно, графіком, якоюсь формулою з іншим набором операцій тощо), то спочатку визначаємо за заданням відповідну таблицю істинності.

Досконала диз'юнктивна нормальна форма (ДДНФ).

Уведемо такі позначення: для логічної змінної x вважатимемо, що $x_0 = \neg x$ та $x_1 = x$. Неважко переконатись, що для логічної змінної $a \in B$ виконується $x_a = 1$, якщо $a = x$ (тобто якщо значення змінних a та x збігаються), а $x_a = 0$, якщо $a \neq x$.

Розглянемо довільну логічну функцію $f(x, y, z)$ від трьох змінних. Нехай $(a_1, b_1, c_1), (a_2, b_2, c_2), \ldots, (a_k, b_k, c_k)$ – це всі набори значень змінних, для яких функція f істинна (тобто дорівнює 1). Тоді формула, що задає цю функцію, має вигляд:

$$x^{a_1} y^{b_1} z^{c_1} \vee x^{a_2} y^{b_2} z^{c_2} \vee \ldots \vee x^{a_k} y^{b_k} z^{c_k} \qquad (1.1)$$

Справді, якщо до цієї формули підставити замість x, y та z один із наборів (a_i, b_i, c_i) (тобто покласти $x = a_i$, $y = b_i$ *і* $z = c_i$), то рівно один із логічних доданків формули (1.1), а саме доданок $x^{a_i} y^{b_i} z^{c_i}$ дорівнюватиме 1, $i = 1, 2, \ldots, k$. Отже, значенням усієї формули (1.1) на цьому наборі (a_i, b_i, c_i) буде 1. Якщо ж до (1.1) підставити будь-який інший набір значень змінних (тобто набір, що не увійшов до вищезазначеного списку з k елементів), то всі доданки формули (1.1) дорівнюватимуть 0, отже, і значенням усієї формули на такому наборі буде 0.

Таким чином, обґрунтовано, що значення формули (1.1) збігається зі значенням заданої функції $f(x, y, z)$ на будь-якому на борі (a, b, c) значень її змінних, тобто (1.1) задає (реалізує) функцію $f(x, y, z)$.

Формулу (1.1) називають **досконалою диз'юнктивною нормальною формою** (ДДНФ) логічної функції *f(x, y, z)*.

Операції, що входять до складу ДДНФ – це кон'юнкція, диз'юнкція та заперечення.

Приклад.

1. Побудувати ДДНФ логічної функції, таблицю істинності якої отримано вище.

Ця функція набуває значення 1 на наборах (0,1,1), (1,0,0) і (1,0,1), тому її ДДНФ – це

$$x^0y^1z^1 \vee x^1y^0z^0 \vee x^1y^0z^1 \text{ або } (\neg x\ y\ z) \vee (x\ \neg y\ \neg z) \vee (x\neg\ y\ z).$$

2. Побудувати ДДНФ логічної функції *f(x, y, z)* від трьох змін них, яка набуває такого самого значення, як і більшість її змін них (функція голосування).

Функція голосування є істинною на наборах (0,1,1), (1,0,1), (1,1,0) та (1,1,1), тому її ДДНФ – $(\neg x\ y\ z) \vee (x\ \neg y\ z) \vee (x\ y\neg\ z) \vee (x\ y\ z)$.

Алгоритм побудови ДДНФ для логічних функцій від двох, чотирьох, п'яти та більшої кількості змінних аналогічний.

Досконала кон'юнктивна нормальна форма (ДКНФ).

За допомогою тих самих операцій кон'юнкції, диз'юнкції і заперечення можна побудувати іншу формулу, що реалізує певну логічну функцію.

Нехай $(a_1, b_1, c_1), (a_2, b_2, c_2), \ldots, (a_k, b_k, c_k)$ – це всі набори значень змінних, для яких логічна функція f(x, y, z) хибна (набуває значення 0). Тоді формула

$$(x^{\neg a_1} \vee y^{\neg b_1} \vee z^{\neg c_1}) \wedge (x^{\neg a_2} \vee y^{\neg b_2} \vee z^{\neg c_2}) \vee \ldots \vee (x^{\neg a} y^{\neg b_k} z^{\neg c_k}) \quad (1.2)$$

реалізує функцію *f*.

Аналогічно вищенаведеним міркуванням можна обґрунтувати, що для будь-якого набору (a_i, b_i, c_i), $i = 1, 2, \ldots, k$ значенням формули (1.2) буде 0, а для будь-якого іншого набору, що не увійшов до цього списку, (1.2) дорівнюватиме 1. Пропонуємо переконатись у цьому самостійно.

Формулу (1.2) називають **досконалою кон'юнктивною нормальною формою (ДКНФ)** відповідної логічної функції *f(x, y, z)*.

Приклад.

Побудувати ДКНФ для логічної функції *f(x, y, z)* із прикладу вище.

Ця функція набуває значення 0 на наборах (0,0,0), (0,0,1), (0,1,0), (1,1,0) і (1,1,1), тому її ДКНФ має вигляд

$$(x^{\neg 0} \vee y^{\neg 0} \vee z^{\neg 0}) \wedge (x^{\neg 0} \vee y^{\neg 0} \vee z^{\neg 1}) \wedge (x^{\neg 0} \vee y^{\neg 1} \vee z^{\neg 0}) \wedge$$
$$\wedge (x^{\neg 1} \vee y^{\neg 1} \vee z^{\neg 0}) \wedge (x^{\neg 1} \vee y^{\neg 1} \vee z^{\neg 1}) \text{ або}$$
$$(x \vee y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge (\neg x \vee \neg y \vee z) \wedge (\neg x \vee \neg y \vee \neg z).$$

2.3. Логіка предикатів

Логіка предикатів. Квантори

Алгебра висловлень, яку вже було розглянуто, справді є важливою частиною математичної логіки, проте її можливостей недостатньо, щоб повноцінно описувати й аналізувати навіть відносно прості міркування з науки чи практики.

Це зумовлено, зокрема, тим, що в логіці висловлень будь-яке просте висловлення трактується як неподільна одиниця без внутрішньої структури, яка має лише одну характеристику – бути істинним або хибним.

Щоб створити систему правил, яка дозволяє робити логічні міркування й отримувати змістовні, нетривіальні висновки з урахуванням структури складених висловлень і змісту простих, була розроблена формальна теорія, що отримала назву **числення предикатів**.

Теорія предикатів починається з уважного аналізу простих висловлень і спирається на таке їх трактування: просте висловлення повідомляє про те, що певний об’єкт (або кілька об’єктів) має конкретну властивість або перебуває у певному відношенні з іншим об’єктом.

Для прикладу, у висловленні «3 – просте число» об’єктом є число 3, а вислів «просте число» описує його властивість.

У класичній латинській граматиці така частина речення називається **предикатом**, звідси й походження відповідного терміну в математичній логіці. У логіці предикатів головну роль відіграє саме ця частина – присудок, що задає властивість або відношення. Його фіксують, а значення об'єкта змінюють, щоб у кожному випадку отримувати осмислені речення, тобто висловлення.

Такий підхід дає змогу тлумачити вислів *«x – просте число»* не як окреме елементарне висловлення, а як **висловлювальну форму** – певний шаблон, який перетворюється на конкретне висловлення лише після того, як замість змінної *x* підставляють об'єкт із заданої множини *M*. Іншими словами, ця форма задає структуру висловлення, а його істинність чи хибність визначається вже після вибору конкретного значення для *x*.

n-місним предикатом $P(x_1, x_2, \ldots, x_n)$ на якійсь множині M називають довільну функцію, яка впорядкованому набору елементів $(a_1, a_2, \ldots, a_n)$ множини M ставить у відповідність логічне значення **1** або **0**.

Множину M називають предметною областю, або універсальною множиною, а $x_1, x_2, \ldots, x_n$ – предметними змінними предикату P.

Множина наборів $(a_1, a_2, \ldots, a_n)$ таких, що $P(a_1, a_2, \ldots, a_n) = \mathbf{1}$, називається **областю істинності (або характеристичною множиною)** предиката P.

Якщо $P(a_1, a_2, \ldots, a_n) = \mathbf{1}$, то згідно із логічною інтерпретацією казатимемо, що предикат P є **істинним** на $(a_1, a_2, \ldots, a_n)$. В іншому разі казатимемо, що предикат P є **хибним**.

Вираз $P(x_1, x_2, \ldots, x_n)$, що перетворюється на висловлення після заміни всіх його змінних $x_1, x_2, \ldots, x_n$ на елементи певної предметної області M, називають **пропозиційною (висловлювальною) формою**.

Приклад.

Нехай предметною областю є множина N натуральних чисел, тоді вирази *x* – просте число, *x* ділить *y*, $x + y = z$, $x < 5$ тощо є пропозиційними формами.

Пропозиційна форма є одним зі способів задання предиката.

Для $n = 1$ предикат $P(x)$ називається **одномісним**, або унарним, для $n = 2$ $P(x, y)$ – **двомісним**, або **бінарним**, для $n = 3$ $P(x, y, z)$ – **тримісним**, або **тернарним предикатом**.

Якщо в n-арному предикаті P(x1, x2, …, xn) зафіксувати значення деяких m змінних (тобто надати їм певних значень із множини M), то отримаємо (n – m)-місний предикат на множині M. Тому можна вважати висловлення нульмісними предикатами, які утворено з багатомісних предикатів підстановкою замість усіх їх параметрів певних значень із предметної області. Отже, висловлення можна розглядати як окремий випадок предиката.

Як з елементарних висловлень за допомогою логічних операцій можна утворювати складені висловлення, так і, використовуючи прості (елементарні) предикати й логічні зв'язки (операції), можна будувати складені предикати, або **предикатні формули**.

Зазвичай основні логічні операції ∧, ∨, ¬, →, ~ означають для предикатів, що задані на тій самій предметній області M і залежать від тих самих змінних.

Нехай $P(x_1, x_2, \ldots, x_n)$ і $Q(x_1, x_2, \ldots, x_n)$ – n-місні предикати на множині M.

Кон'юнкцією $P(x_1, x_2, \ldots, x_n) \wedge Q(x_1, x_2, \ldots, x_n)$ називають предикат $R(x_1, x_2, \ldots, x_n)$, що набуває значення 1 на тих і тільки тих наборах значень змінних, на яких обидва предикати $P(x_1, x_2, \ldots, x_n)$ і $Q(x_1, x_2, \ldots, x_n)$ дорівнюють 1.

Зауважимо, що на інших наборах значень змінних предикат набуває значення 0.

Диз'юнкцією $P(x_1, x_2, \ldots, x_n) \vee Q(x_1, x_2, \ldots, x_n)$ називають пре дикат $T(x_1, x_2, \ldots, x_n)$, що набуває значення 1 на тих і тільки тих наборах значень змінних, на яких принаймні один із предикатів $P(x_1, x_2, \ldots, x_n)$ або $Q(x_1, x_2, \ldots, x_n)$ дорівнює 1.

Відповідно на ін ших наборах значень змінних предикат набуває значення 0.

Запереченням ¬ $P(x_1, x_2, \ldots, x_n)$ предиката $P(x_1, x_2, \ldots, x_n)$ на зивають предикат $S(x_1, x_2, \ldots, x_n)$, що дорівнює 1 на тих і лише тих наборах значень термів, на яких предикат $P(x_1, x_2, \ldots, x_n)$ до рівнює 0.

Аналогічно вводять також інші логічні операції: →, ~ тощо. Знаючи, як виконуються окремі операції предикатів, можна утворювати вирази або формули, операндами яких є предикати.

У логіці предикатів додають дві спеціальні операції – **квантори**. Завдяки їм можна точніше описувати властивості об'єктів та узагальнювати висловлення. Ці операції значно розширюють можливості логічного аналізу, роблять теорію предикатів гнучкішою й змістовнішою. Саме через важливу роль кванторів логіку предикатів інколи називають ***теорією квантифікації***.

Найпопулярнішими й найуживанішими виразами в математиці є фрази або формулювання типу для всіх та існує. Поняття, що відповідає словам для всіх, лежить в основі означення квантора загальності.

Нехай $P(x)$ – предикат на множині М. Тоді **квантор загальності** (із параметром x) – це операція, що ставить у відповідність $P(x)$ висловлення для всіх x із М $P(x)$ істинне; для позначення цієї операції використовують знак ∀, записують $\forall x P(x)$ (читають для всіх х Р від х).

Іншу операцію називають **квантором існування** та позначають її знаком ∃. Якщо $Q(x)$ – деякий предикат на множині М, то висловлення існує в множині М елемент х такий, що $Q(x)$ істинне записують у вигляді $\exists x Q(x)$ і читають існує такий x, що Q від х або є такий x, що Q від x.

Походження обраних позначень пояснюється тим, що символ ∀ – це перевернута велика перша літера німецького слова alle або англійського слова all, що перекладають як усі. А символ ∃ відповідає першій літері слів existieren (нім.) або exist (англ.) – існувати.

Вираз $\forall x$ читають також як усі x; для кожного x; для довільного x; для будь-якого x; а вираз $\exists\ x$ – як деякий x; для деякого x; знайдеться такий x тощо.

Зазначимо, що, крім уведених символічних позначень кванторів, використовують також інші позначення. Наприклад, замість $\forall\ x$ іноді пишуть $\forall(x)$, (x) або $\wedge x$, а замість $\exists x$ – відповідно $\exists(x)$, $(\mathrm{E}x)$ або $\vee x$.

Приклад.

Розглянемо два бінарні предикати на множині натуральних чисел N: предикат *x менше y* та предикат *x ділить y*. Перший із них записуватиме у традиційній формі $x < y$, а другий – y вигляді $x \mid y$. Тоді неважко переконатись, що висловлення:

$\forall\ x\ \exists\ y\ (x < y)$ та $\forall\ x\ \exists$ y $(x \mid y)$ є істинними,

$\exists\ y\ \forall\ x\ (\mathrm{x} < \mathrm{y})$ та $\exists\ y\ \forall\ x\ (x \mid y)$ є хибними.

Істинними будуть, наприклад, висловлення

$$\forall\ x\ (0 < x^2 - x + 1),$$

$$\exists\ x\ ((x \mid 1) \wedge (\neg\ (1 < \mathrm{x}))),$$

$$\forall\ x\ ((x < 1) \rightarrow (x < 2)),$$

$$\forall\ x\ (((2 \mid x) \wedge (3 \mid x)) \rightarrow (6 \mid x)),$$

а хибними –

$$\forall\ x\ (2 \mid x),\ \exists\ x\ (x^2 < 0),\ \forall\ x\ ((3 \mid x) \rightarrow (6 \mid x)).$$

Важливу роль у логіці предикатів відіграє поняття області дії квантора у заданій формулі, під якою розумітимемо той вираз (підформулу), до якого належить квантор. Область дії квантора позначають за допомогою дужок. Ліва дужка, що відповідає початку області дії, записується безпосередньо після кванторної змінної даного квантора, а відповідна до неї права дужка означає закінчення області дії цього квантора. Там, де це не викликає невизначеності, дужки можна опускати й замість $\forall x(P(x))$ або $\exists x(P(x))$ писати відповідно $\forall xP(x)$ або $\exists xP(x)$. Це означає, що операції квантифікації мають більший пріоритет, ніж логічні операції.

Зауважимо, що така ситуація не виняткова й доволі часто зустрічається в інших розділах математики. Наприклад, у виразах

$$\int_a^b f(x)dx, \lim_{x\to c} x^n \quad \text{та} \quad \sum_{j=k}^{n} f(j)$$

параметри a, b, c, k і n – це змінні, замість яких можна підставляти певні значення, а параметри x та j – зв'язані змінні, підстановка замість яких будь-яких значень не має жодного сенсу.

Навішувати квантори можна й на багатомісні предикати. Наприклад, застосовуючи квантори ∀ і ∃ до змінних x та y двомісно го предиката $A(x, y)$, отримаємо чотири різні одномісні предикати:

$$\forall x\, A(x, y),\ \exists x\, A(x, y),\ \forall y\, A(x, y) \text{ і } \exists y\, A(x, y).$$

У перших двох змінна x є зв'язаною, а змінна y – вільною, а у двох останніх – навпаки.

Вираз $\forall x\ A(x, y)$ (читають як *для всіх x A від x та y*) є одномісним предикатом $B(y)$. Він є істинним для тих і тільки тих $b \in M$, для яких одномісний предикат $A(x, b)$ є істинним для всіх x із M.

Навішування одного квантора завжди зменшує кількість вільних змінних і арність предиката на одиницю. Застосування кванторів до всіх змінних предиката перетворює його на висловлення (іноді таку предикатну формулу називають **замкненою**).

3. СИСТЕМИ ЧИСЛЕННЯ

3.1. Системи числення

Система числення (далі – СЧ) – це спосіб представлення будь-яких чисел за допомогою певного набору знаків (цифр) і визначені правила дій над ними.

У процесі розвитку, історично першою СЧ людства, швидше за все, була одинична система. Одинична (унарна) система числення – це система, будь-яке число якої утворюється шляхом повторення одного знаку, що символізує одиницю. У цій СЧ для позначення числа предметів рисували ці предмети, повторюючи їх зображення потрібну кількість разів.

З часом виникли інші, більш економні (для запису та збереження чисел у пам'яті ПК) системи числення. Записати довільне число обмеженою кількістю цифр дозволяє позиційна система числення. Значення чисел, записаних у позиційній СЧ, залежить не тільки від символів, з яких складається запис числа, а й від їх розташування.

Наприклад, числа 754 і 457 (у 10-й позиційній СЧ) є різними, на відміну від унарної системи числення, в якій важливим є не місце розташування зарубок (вузликів тощо), а тільки їх кількість. Ця властивість називається *позиційністю*, а система числення, що володіє нею, називається **позиційною системою числення**.

В інформатиці, запис чисел у деякій СЧ називається його **кодом**. Існують також **непозиційні** СЧ та **змішані**.

Позиційні системи числення

Позиційна системи числення – це система у якій величина, яку позначає цифра, залежить від її позиції у числі.

Позиційна СЧ складається з обмеженої кількості цифр, проте позиція кожної цифри у числі забезпечує значимість (вагу) цієї цифри. Позиція цифри на мові математики називається *розрядом*. Тобто значення цифри «мінливе» і залежить від її позиції в числі.

Наприклад, у 10-й СЧ, в числі 33 дві трійки мають різне значення: права трійка означає цифру 3 (кількість одиниць), а ліва – число 30 (кількість десятків).

Для позиційних систем числення характерні наочність зображення чисел і відносна простота виконання арифметичних операцій. Саме позиційні системи числення стали основою сучасної математики. Слід зауважити, що позиційні СЧ, в свою чергу, поділяють на **однорідні** (вага їх розрядів змінюється згідно із степеневим законом) і **неоднорідні**. Далі, розглядатимемо тільки однорідні СЧ.

Існує велика кількість позиційних систем числення, які відрізняються одна від одної **алфавітом – множиною використовуваних цифр**.

Основа позиційної системи числення – це розмір алфавіту, тобто кількість різних знаків або символів (цифр), що використовуються для зображення чисел у даній системі.

Вибір алфавіту тієї чи іншої СЧ, швидше за все, визначався потребами реального життя, науки чи зручностями обробки. Історично ж вибір СЧ визначався звичками або традиціями конкретного народу. Ми користуємось десятковою СЧ з цілком зрозумілих причин – у нас на руках десять пальців. Ми звикли до неї, і ніколи свідомо не підкреслюємо значення основи. Але можна побудувати систему числення, взявши за основу будь-яке інше натуральне число.

Примітка. Для зручності у СЧ з основою не більше 10, використовують арабські (десяткові) цифри, якщо ж основа більша за 10, то роль цифр часто відіграють латинські літери розташовані в лексикографічному (алфавітному) порядку як, наприклад, у 16-вій системі числення.

Таблиця 2.4. Алфавіт позиційних систем числення

Основа *q*	**Система числення**	**Знаки**
2	Двійкова	0, 1
3	Трійкова	0, 1, 2
5	П’ятіркова	0, 1, 2, 3, 4
8	Вісімкова	0, 1, 2, 3, 4, 5, 6, 7
10	Десяткова	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
16	Шістнадцяткова	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F
і т.д.		

Наприклад, числа трійкової СЧ будуть наступними: 0, 1, 2, 10, 11, 12, 20, 21, 22…

Для зазначення основи системи, до якої належить число, вводять індексне позначення: 75_{10} , 1011_2 , $2A7_{16}$, 54_8.

У позиційній СЧ число можна представити через його цифри за допомогою многочлена відносно основи q :

$$A_q = a_k q^k + a_{k-1} q^{k-1} + \ldots + a_0 q^0 + a_{-1} q^{-1} + \ldots + a_{-m} q^{-m} = \sum_{i=-m}^{k} a_i q^i$$

де q – основа СЧ, q^i – вага позиції, a^i – цифри в позиціях числа, *0..k* – номери розрядів цілої частини числа, *-1…-m* – номери розрядів дробової частини числа.

Тобто число є послідовністю цифр: $a_k a_{k-1} \ldots a_0 a_{-1} \ldots a_{-m}$.

Вищенаведений поліном називається **розгорнутою формою запису числа**. Доданки в цьому виразі є добутками значущих цифр числа і степенів основи системи числення, що залежить від позиції цифри в числі – розряду. Розряд числа зростає справа наліво, від молодших розрядів до старших (для цілого числа молодший розряд є нульовим). За кількістю розрядів визначають довжину числа.

Приклади запису чисел:

- двійкова СЧ, q=2; $a_i \in \{0,1\}$,
  $A_2 = 101_2 = 1*2^2 + 0*2^1 + 1*2^0$
- вісімкова СЧ, q=8; $a_i \in \{0,1...7\}$,
  $A_8 = 175_8 = 1*10_8^2 + 7*10_8^1 + 5*10_8^0 = 1*8_{10}^2 + 7*8_{10}^1 + 5*8_{10}^0$,
  тобто $10_8 = 8_{10}$
- десяткова СЧ, q=10; $a_i \in \{0,1...9\}$,
  $A_{10} = 531{,}26_{10} = 5*10^2 + 3*10^1 + 1*10^0 + 2*10^{-1} + 6*10^{-2} =$
  $= 500 + 30 + 1 + 0{,}20 + 0{,}06$

Непозиційні системи числення

Не всякі числові системи використовують позиційний спосіб запису.

Непозиційні системи числення – це СЧ у яких величина, яку позначає цифра, не залежить від її позиції у числі. При цьому система може накладати обмеження на позиції цифр, наприклад, щоб вони були розташовані по спаданню, чи згруповані за значенням.

У непозиційній системі кожен знак у записі числа, незалежно від місця його розташування, означає одне й те саме число. Найвідомішою непозиційною СЧ є римська (виникла у древньої цивілізації – етрусків, біля 500 р. до н. е., а згодом перейнята римлянами), в якій використовують сім знаків:

I	V	X	L	C	D	M
один	п'ять	десять	п'ятдесят	сто	п'ятсот	тисяча

Наприклад: III – 3, MDC – 1600.

Форма римських цифр походить від використання для лічби пальців і долонь та від словесної назви чисел (Centum – сто, Demimille – половина тисячі, Mille – тисяча). У римській СЧ вага цифри у числі, у будь-якій позиції є незмінною. До прикладу, цифра X у будь-якій позиції числа дорівнює просто десяти (у числі XIX – всі X означають десять).

Недоліком римської СЧ є і те, що цифри даної системи розкидані по осі чисел (зображення чисел є занадто громіздким), відсутність нуля та чітких правил виконання арифметичних дій над числами (не кажучи вже, про більш складні функції). У зв’язку з цим, римська СЧ використовується вкрай рідко.

Десяткова система числення

У цій системі використовуються спеціальні графічні знаки – арабські цифри, які можна записати в наступному порядку: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, а основою є число 10. Десятковою вона називається тому, що в цій СЧ десять одиниць одного розряду становлять одну одиницю наступного, старшого розряду.

Одним з важливих досягнень індійської науки було також введення особливого позначення для пропуску розрядів – нуля (який означав відсутність числа). Араби ж першими засвоїли дану СЧ й поширили Європою. У розгорнутій формі ціле десяткове число матиме вигляд:

$$257_{10} = 200+50+7=2\cdot 10^2+5\cdot 10^1 + 7\cdot 10^0$$

У даному прикладі 10 є основою системи числення, а показник степеня – це розряд (місце розташування символів у числі). У цілому десятковому числі цифра, що перебуває в крайній праворуч позиції (розряді), означає кількість одиниць, цифра, зміщена на одну позицію вліво, – кількість десятків, ще лівіше – сотень, потім тисяч і т.д. Відповідно маємо розряд одиниць, розряд десятків і т.д.

Саме десяткові цифри отримали широкого вжитку; на них базується метрична система одиниць, нумерація тощо.

Перші обчислювальні машини працювали на десятковій системі числення. Механічний калькулятор Б. Паскаля мав колесо з десятьма поділками, а пізніші електромеханічні й електронні пристрої реалізовували десяткову систему за допомогою десяти тригерів (мікросхеми з двома стійкими станами). Однак потреба у великій кількості елементів зробила такий підхід занадто дорогим, що й спричинило пошук простіших та дешевших систем.

Двійкова, вісімкова та шістнадцяткова системи числення

В основу пошуків інженери і математики поклали двійкову природу елементів обчислювальної техніки. Тому, апаратну частину ЕОМ було спроектовано на основі двопозиційних елементів (найпростішим є діод), які можуть перебувати лише в одному з двох стійких станів: 0 чи 1. Тож нові

обчислювальні машини почали рахувати за допомогою нулів і одиничок. Знаки 0 і 1 є цифрами двійкової СЧ, яка і в наш час використовується в ПК.

В інформатиці двійкова цифра має назву біт.

З появою персональних комп'ютерів двійкова система числення повноправно увійшла в життя суспільства. Ми використовуємо її щодня, працюючи за комп'ютером чи дивлячись цифрове телебачення, знімаючи фото чи відео, здійснюючи дзвінок чи прослуховуючи музику тощо. Двійкова система числення є одним з найважливіших винаходів людства.

Вісімкова СЧ набула популярності завдяки бурхливому розвитку інформатики та програмування. Це позиційна цілочисельна СЧ з основою 8. Для представлення чисел у ній використовуються цифри від 0 до 7. Вісімкова система часто використовується в галузях, пов'язаних з цифровими пристроями та характеризується легким перетворенням вісімкових чисел у двійкові і навпаки, шляхом заміни вісімкових чисел на тріади (триплети) двійкових.

У наш час майже повністю витіснена шістнадцятковою, завдяки швидким темпам збільшення розрядності процесорів, росту об'ємів носіїв інформації та розробки відповідного програмного забезпечення.

Шістнадцяткова СЧ – це позиційна система числення, кожне число в якій записується за допомогою 16-ти символів. Цю систему часто називають також Hex (від англ. hexadecimal — шістнадцятковий). Для запису чисел в цій системі окрім 10 арабських цифр (від 0 до 9) використовують 6 літер латинської абетки: A, B, C, D, E, F. Наприклад, запис шістнадцяткового числа $3E8_{16}$ у вигляді полінома має вигляд:

$$3E8_{16}=3*16^2 + 14*16^1 + 8*16^0 = 768 + 224 + 8 = 1000_{10}$$

Шістнадцяткова СЧ широко вживана в інформатиці, оскільки значення кожного байту можна записати у вигляді двох цифр шістнадцяткової системи. Таким чином, значення послідовних байтів можна представити у вигляді списку двозначних чисел.

Таблиця 3.1. Відповідність двійкових, вісімкових, десяткових та шістнадцяткових чисел

2-ва	*8-ва*	*2-ві тріади*	*10-ва*	*16-ва*	*2-ві тетради*
0	0	000	0	0	0000
1	1	001	1	1	0001
10	2	010	2	2	0010
11	3	011	3	3	0011
100	4	100	4	4	0100
101	5	101	5	5	0101
110	6	110	6	6	0110
111	7	111	7	7	0111
1000	10	001 000	8	8	1000
1001	11	001 001	9	9	1001
1010	12	001 010	10	A	1010
1011	13	001 011	11	B	1011
1100	14	001 100	12	C	1100
1101	15	001 101	13	D	1101
1110	16	001 110	14	E	1110
1111	17	001 111	15	F	1111
10000	20	010 000	16	10	0001 0000
…	…	…	…	…	…
100000	40	100 000	32	20	0010 0000
…	…	…	…	…	…
1000000	100	001 000 000	64	40	0100 0000
…	…	…	…	…	…
10000000	200	010 000 000	128	80	1000 0000
…	…	…	…	…	…
100000000	400	100 000 000	256	100	0001 0000 0000
…	…	…	…	…	…
1000000000	1000	001 000 000 000	512	200	0010 0000 0000
…	…	…	…	…	…
10000000000	2000	010 000 000 000	1024	400	0100 0000 0000
…	…	…	…	…	…
100000000000	4000	100 000 000 000	2048	800	1000 0000 0000
…	…	…	…	…	…
1000000000000	10000	001 000 000 000 000	4096	1000	0001 0000 0000 0000

3.2. Арифметичні дії у різних системах числення

Наука, що вивчає дії над цілими числами, вчить розв'язувати задачі, які зводяться додавання, віднімання, множення та ділення цих чисел називається *арифметикою*. Кожна СЧ має свої правила арифметики (таблицю додавання та множення).

Арифметичні дії у різних системах числення здійснюються за таким самим принципом, як у десятковій, тобто по розрядах. Арифметичні дії над десятковими числами проводяться за допомогою досить простих операцій, в основі яких лежать таблиці множення й додавання, а також правило переносу: якщо в результаті додавання двох цифр виходить число, яке більше або рівне за основу СЧ (у нашому випадку 10), то воно записується за допомогою декількох цифр, що перебувають на сусідніх позиціях.

Арифметичні операції у 2-й, 8-й, 16-й СЧ виконують ідентично 10-й системі, з врахуванням арифметики відповідної СЧ.

Таблиця 3.2. Додавання та множення двійкових цифр

+	0	1
0	0	1
1	1	10

*	0	1
0	0	0
1	0	1

Таблиця 3.3. Додавання та множення вісімкових цифр

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	10
2	2	3	4	5	6	7	10	11
3	3	4	5	6	7	10	11	12
4	4	5	6	7	10	11	12	13
5	5	6	7	10	11	12	13	14
6	6	7	10	11	12	13	14	15
7	7	10	11	12	13	14	15	16

*	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	10	12	14	16
3	0	3	6	11	14	17	22	25
4	0	4	10	14	20	24	30	34
5	0	5	12	17	24	31	36	43
6	0	6	13	22	30	36	44	52
7	0	7	16	25	34	43	52	61

Таблиця 3.4. Додавання та множення десяткових цифр

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	10
2	2	3	4	5	6	7	8	9	10	11
3	3	4	5	6	7	8	9	10	11	12
4	4	5	6	7	8	9	10	11	12	13
5	5	6	7	8	9	10	11	12	13	14
6	6	7	8	9	10	11	12	13	14	15
7	7	8	9	10	11	12	13	14	15	16
8	8	9	10	11	12	13	14	15	16	17
9	9	10	11	12	13	14	15	16	17	18

*	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	10	12	14	16	18
3	0	3	6	9	12	15	18	21	24	27
4	0	4	8	12	16	20	24	28	32	36
5	0	5	10	15	20	25	30	35	40	45
6	0	6	12	18	24	30	36	42	48	54
7	0	7	14	21	28	35	42	49	56	63
8	0	8	16	24	32	40	48	56	64	72
9	0	9	18	27	36	45	54	63	72	81

Таблиця 3.5. Додавання та множення шістнадцяткових цифр

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10
2	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11
3	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12
4	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13
5	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14
6	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15
7	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16
8	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17
9	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18
A	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19
B	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A
C	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B
D	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C
E	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D
F	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E

*	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	10	12	14	16	18	1A	1C	1E
3	0	3	6	9	C	F	12	15	18	1B	1E	21	24	27	2A	2D
4	0	4	8	C	10	14	18	1C	20	24	28	2C	30	34	38	3C
5	0	5	A	F	14	19	1E	23	28	2D	32	37	3C	41	46	4B
6	0	6	C	12	18	1E	24	2A	30	36	3C	42	48	4E	54	5A
7	0	7	E	15	1C	23	2A	31	38	3F	46	4D	54	5B	62	69
8	0	8	10	18	20	28	30	38	40	48	50	58	60	68	70	78
9	0	9	12	1B	24	2D	36	3F	48	51	5A	63	6C	75	7E	87
A	0	A	14	1E	28	32	3C	46	50	5A	64	6E	78	82	8C	96
B	0	B	16	21	2C	37	42	4D	58	63	6E	79	84	8F	9A	A5
C	0	C	18	24	30	3C	48	54	60	6C	78	84	90	9C	A8	B4
D	0	D	1A	27	34	41	4E	5B	68	75	82	8F	9C	A9	B6	C3
E	0	E	1C	2A	38	46	54	62	70	7E	8C	9A	A8	B6	C4	D2
F	0	F	1E	2D	3C	4B	5A	69	78	87	96	A5	B4	C3	D2	E1

Правила виконання основних арифметичних операцій

Додавання та віднімання двійкових, вісімкових та шістнадцяткових чисел виконується аналогічно десятковим, з врахуванням наведених вище таблиць додавання, відповідно. Додаючи два багатозначних числа, застосовуємо правило додавання в стовпчик. При цьому все зводиться до додавання цифр, для яких необхідним є знання таблиці додавання у відповідній СЧ. При відніманні від меншого числа більшого, виконується позичання зі старшого розряду.

В основі множення та ділення лежить таблиця множення одноцифрових чисел. Взагалі кажучи, за таким принципом арифметичні дії можна виконувати у будь-якій позиційній системі числення.

Перетворення чисел із однієї системи числення в іншу

Існує два основних способи перетворення (переведення) числа з однієї СЧ в іншу: табличний і розрахунковий. Табличний спосіб прямого перетворення базується на співставленні таблиць відповідності чисел різних СЧ. Цей спосіб занадто громіздкий, а в комп'ютерній техніці вимагає значного об'єму пам'яті для зберігання таблиць. Розрахунковий спосіб перетворення чисел з однієї СЧ в іншу передбачає виконання певних арифметичних обчислень. Існує велика кількість способів перетворення чисел з однієї позиційної СЧ в іншу. Розглянемо найбільш популярні.

Перетворення 10-вого числа у недесяткову СЧ

А) Метод ділення (для цілої частини) та метод множення (для дробової частини)

Для перетворення чисел із позиційної системи числення з основою p в позиційну систему числення з основою q з використанням арифметики старої системи числення з основою p потрібно:

- для перетворення цілої частини: послідовно число, записане в системі з основою p ділити на основу нової системи числення q, виділяючи остачі. Ділення виконується, до тих пір, поки остання частка не стане меншою за дільник. Отримані остачі від ділення, взяті у зворотному порядку, будуть значеннями розрядів числа в новій СЧ. Остання частка дає старшу цифру числа;

- для перетворення дробової частини: послідовно дробову частину множити на основу нової системи числення, виділяючи цілі частини добутку. Отримані цілі частини добутків будуть цифрами дробу у новій системі числення. Цей процес продовжують до того часу, поки не буде знайдено число із заданою точністю (кінцевому дробу в іншій СЧ може відповідати нескінченний (іноді періодичний) дріб; у цьому випадку кількість знаків у поданні дробу в новій СЧ береться в залежності від потрібної точності).

Примітка. Цим правилом зручно користуватися у разі перетворення з десяткової системи числення у будь-яку іншу, оскільки десяткова

арифметика є для нас звична. У разі ж, якщо потрібно перетворити двійкове число у десяткову СЧ, нам необхідно ділити це число на основу нової СЧ, тобто на 1010_2 та ще й з використанням двійкової арифметики. Такі операції виконувати складно, тому для подібних перетворень використовують інші методи, які розглянуто нижче.

Приклад.

Перетворимо число $25{,}25_{10}$ з десяткової СЧ у 2-ву:

Ціла частина (три методи):

1. 25:2=12+**1** – молодший розряд
   12:2=6+**0** (перша цифра)
   6:2=3+**0**
   3:2=**1**+**1**

2.

25_{10}	2_{10}
12	**1**
6	**0**
3	**0**
1	**1**
0	**1**

3.

25	2			
24	12	2		
1	12	6	2	
	0	6	3	2
		0	2	**1**
			1	

Примітка. Тобто, число записуємо у зворотному порядку – 11001 !

Дробова частина:

0,25*2=**0**,50

0,50*2=**1**,00

Відповідь: $25{,}25_{10}=11001{,}01_2$

Перетворимо число $25{,}25_{10}$ з десяткової СЧ у 8-ву.

Ціла частина: 25:8=**3**+**1**

Дробова частина: 0,25*8=**2**,00

Відповідь: $25{,}25_{10}=31{,}2_8$

Перетворимо число $25{,}25_{10}$ з десяткової СЧ у 16-ву.

Ціла частина: 25:16=**1**+**9**

Дробова частина: 0,25*16=**4**,00

Відповідь: $25{,}25_{10}=19{,}4_{16}$

Примітка. У випадку, коли результат ділення на 16 дає десяткові числа від 10 до 15, їх слід замітити відповідними знаками 16-вої СЧ, тобто латинськими буквами A…F.

Приклад.

Перетворимо число 175_{10} з десяткової СЧ у 16-ву. 175:16=10+15

Відповідь: $175_{10}=AF_{16}$

Б) Метод віднімання (на прикладі переведення 10-го числа у 2-ве)

Даний метод застосовуємо для цілих чисел. З десяткового числа віднімається найбільша можлива степінь двійки, у відповідний розряд двійкового числа записується одиниця. Якщо різниця менше наступного степеня двійки, то далі записується нуль, а якщо більше – записується одиниця і знову проводиться віднімання, і так до того часу, поки вихідне число не зменшиться до нуля.

$25_{10}=2^4+9=2^4+2^3+1=2^4+2^3+2^0=11001_2$

$175_{10}=2^7+47=2^7+2^5+15=2^7+2^5+2^3+7=2^7+2^5+2^3+2^2+3=2^7+2^5+2^3+2^2+2^1+2^0=$
$=10101111_2$

Перетворення чисел із недесяткової СЧ у 10-ву

Спосіб 1. Для перетворення чисел із будь-якої системи числення в десяткову необхідно це число представити у вигляді полінома і розкрити всі члени полінома в десятковій системі числення. Іншими словами, слід перейти до розгорнутої форми запису числа в десятковій формі та обчислити отриманий вираз за правилами десяткової арифметики.

Приклади:

$31,2_8=(3*10^1+1*10^0+2*10^{-1})_8=(3*8^1+1*8^0+2*8^{-1})_{10}=(24+1+0,25)_{10}=25,25_{10}$
$AF_{16}=(A*10^1+F*10^0)_{16}=(10*16^1+15*16^0)_{10}=(160+15)_{10}=175_{10}$

Спосіб 2. Для перетворення числа у 10-ву СЧ за його розгорнутою формою запису існує зручний спосіб, який має назву *обчислювальна схема Горнера*. Основна ідея даного методу полягає у перетворенні розгорнутого запису числа у еквівалентну форму з допомогою вкладених дужок.

$175_8=(1*8^2+7*8^1+5*8^0)_{10}=(1*8+7)*8+5$
$7575_{16}=(7*16^3+5*16^2+7*16^1+5*16^0)_{10}=((7*16+5)*16+7)*16+5$

Спосіб 3. Для перетворення цілих чисел у 10-ву СЧ, слід послідовно множити початкове число X10 на основу нової СЧ q та, додавати отримане значення до цифри наступного розряду і т.д. у результативній СЧ.

Аналогічна процедура виконується для дробових чисел починаючи з молодшої цифри, з заміною множення діленням.

Приклад. Перевести двійкове число 11001_2 у десяткову СЧ.

1*2=2+**1**
3*2=6+**0**
6*2=12+**0**
12*2=24+**1**
Відповідь: $11001_2=25_{10}$

Перетворення чисел із 2-вої у 8-ву та 16-ву СЧ і навпаки

Існує простий зв'язок між двійковою і вісімковою та між двійковою і шістнадцяткою СЧ, оскільки це є системи з кратною основою. Якщо основи СЧ кратні одна одній, тобто зв'язані залежністю $q=p^m$, то кожна цифра системи з основою q може бути представлена m цифрами в системі з основою p. При перетворенні числа з однієї системи в іншу, одній вісімковій цифрі відповідає трирозрядний двійковий код (двійкова тріада), а шістнадцятковій цифрі відповідає чотирирозрядний двійковий код (двійкова тетрада) (див. Таблицю 3.1). Цей зв'язок базується на тому, що:

- $8=2^3$, а кількість різних трирозрядних комбінацій із цифр 0 і 1 рівна 8: від 000 до 111;
- $16=2^4$, а кількість різних чотирирозрядних комбінацій із цифр 0 і 1 дорівнює 16: від 0000 до 1111.

Тому перетворення чисел із 8-ї у 2-ву, із 16-вої у 2-ву і навпаки проводиться шляхом формального перекодування, яке сформулюємо у наступних правилах.

Правило 1. Перетворення 2-вого числа у 16-ву СЧ. Двійкове число розбиваємо на тетради (по 4 цифри), починаючи з молодших розрядів. Якщо кількість цифр вихідного двійкового числа не кратна 4, то воно доповнюється зліва незначущими нулями до досягнення кратності 4. Далі, кожна тетрада замінюється відповідною 16-вою цифрою згідно таблиці.

Правило 2. Перетворення 16-вого числа у 2-ву СЧ. Кожна 16-ва цифра вихідного числа заміняється двійковою тетрадою у відповідності до таблиці.

Якщо у таблиці двійкове число містить менше 4 цифр, то воно доповнюється зліва незначущими нулями до тетради. Незначущі нулі у результуючому числі відкидаються. Аналогічні правила можна сформулювати і для перетворення 2-вого числа у 8-ву СЧ та навпаки, врахувавши те, що вісімковій цифрі відповідає двійкова тріада, а не тетрада.

4. КОМБІНАТОРИКА ТА ШИФРУВАННЯ

4.1. Комбінаторика

Предмет комбінаторного аналізу не так легко описати. В деякому сенсі слово “комбінаторика” можна сприймати як синонім терміну “дискретна математика”, тобто дослідження скінчених математичних структур. На нижчому рівні з терміном “комбінаторики” пов’язують просто набір відомих формул, які слугують обчисленню так званих комбінаторних чисел, про які мова піде в першій лекції цього розділу. Може здатися, що ці формули корисні тільки для розв’язання олімпіадних задач і не мають практичного сенсу. Але це далеко не так. Обчислення на дискретних скінчених математичних структурах, які часто називають **комбінаторними обчисленнями**, вимагають комбінаторного аналізу для встановлення властивостей та виявлення оцінки застосування алгоритмів, які використовуються.

Комбінаторні задачі

В багатьох практичних випадках виникає необхідність підрахунку кількості можливих комбінацій об’єктів, які задовольняють певним властивостям. Такі задачі називаються **комбінаторними**. Багатоманітність комбінаторних задач неможливо описати, але серед них є цілий ряд таких, які зустрічаються особливо часто та для яких відомі способи підрахунку.

Для формулювання та розв’язку комбінаторних задач використовуються різні моделі комбінаторних конфігурацій. Розглянемо наступні дві найбільш популярні.

1. Задано n предметів. Їх потрібно розмістити по m ящикам так, щоби виконувались задані обмеження. Скількома способами це можна зробити?

2. Розглянемо множину функцій F: $X \to Y$, де $|X|=n$, $|Y|=m$. Можемо враховувати, що $X=\{1,\ldots,n\}$, $Y=\{1,\ldots,m\}$, $F=\langle F(1),\ldots,F(n)\rangle$, $1 \le F(i) \le m$. Скільки існує функцій F, які задовольняють заданим обмеженням?

Правила суми та добутку

Правило суми. Якщо об'єкт x можна вибрати n_1 способами, а інший об'єкт y – n_2 способами, то можна вибрати або x, або y n_1+n_2 способами.

Наприклад, студент має вибрати тему реферату зі списку, розміщеного на трьох аркушах. Аркуші містять відповідно 20, 15 і 17 тем. З якої кількості можливих тем студент робить свій вибір? За правилом суми кількість тем для вибору становить 20 + 15 + 17 = 52.

У ящику знаходиться 20 кульок: 5 білих, 6 чорних, 7 синіх та 2 червоних. Скількома способами можна взяти з ящику одну кольорову кульку? Тут передбачається, що кольорова кулька – це або синя, або червона кулька, тому потрібно застосовувати правило суми. Кольорову кульку можна вибрати 7+2 = 9 способами.

Правило добутку. Якщо об'єкт x можна вибрати n_1 способами та після кожного такого вибору об'єкт y можна вибрати n_2 способами, то пару об'єктів (x,y) у зазначеному порядку можна вибрати $n_1 \times n_2$ способами.

Це правило можна узагальнити на довільну кількість елементів. Нехай є n об'єктів. Якщо об'єкт x_1 можна вибрати n_1 способами, після чого об'єкт x_2 можна вибрати n_2 способами, і для будь-якого j, $2 \le j \le m-1$, після вибору об'єктів $x_1,\ldots,x_j$ об'єкт x_{j+1} можна вибрати n_{j+1} способами, то вибір упорядкованої послідовності m об'єктів $(x_1, x_2,\ldots,x_m)$ може бути здійснений $n_1 \times n_2 \times \ldots \times n_m$ способами.

Наприклад, припустимо, що певний шифр містить дві літери українського алфавіту, за якими йдуть три цифри. Тоді існує 33 способи вибору кожної літери та 10 способів вибору кожної цифри. Таким чином, загальна кількість можливих шифрів складатиме:

$33 \times 33 \times 10 \times 10 \times 10 = 1089000$.

Скільки може бути різних комбінацій випадання граней коли підкидують дві гральні кісті (гральна кість – це кубик, на гранях якого нанесені числа 1, 2, 3, 4, 5, 6)? На першій кісті може випасти 1, 2, 3, 4, 5 або 6,

тобто всього буде 6 варіантів. Так само й на другій кісті. Отримуємо 6×6 = 36 способів.

З міста А у місто В йде 5 доріг, а з міста В у місто С – 3 дороги. Скількома способами можна проїхати з міста А до міста С? Щоби проїхати з А до С, треба проїхати з А до В та з В до С, тому застосуємо правило добутку: 5×3 = 15.

Розміщення, сполучення та перестановки

Розглянемо основні комбінаторні об'єкти – розміщення, сполучення та перестановки, - попередньо означивши важливе поняття вибірки.

Означення. Нехай задано скінчену не порожню множину $A=\{a_1,\ldots,a_n\}$ і виконано r таких кроків.

Крок 1. Із множини А вибирають якийсь елемент a_{i1}.

Крок 2. Із множини А чи з $A\setminus\{a_{i1}\}$ вибирають якийсь елемент a_{i2}.

.....

Крок r. Якщо $a_{i1},a_{i2},\ldots,a_{ir-1}$ – елементи, які вибрані на перших r-1 кроках ($r\geq 3$), то на цьому кроці вибирають якийсь елемент a_{ir} із множини А чи $A\setminus\bigcup_{k=1}^{r-1}\{a_{ik}\}$. Тоді елементи $a_{i1},a_{i2},\ldots,a_{ir}$ утворюють **вибірку обсягом** r, або **r-вибірку**, з множини А.

Вибірку називають **впорядкованою**, якщо задано порядок її елементів, а якщо порядок не задано, то – **невпорядкованою**.

Наприклад, з цифр 1, 2, 3, 4, 5 складаємо трьохзначні числа 123, 431, 524,... і т.д. Це впорядковані трьохзначні вибірки, тому що 123 та 132 – різні числа. Інший приклад: з 20 учнів класу будемо обирати двох чергових. Будь-яка пара чергових є невпорядкована двохелементна вибірка, тому що порядок їх вибору не важливий.

Означення. Впорядковані r-вибірки з n-елементної множини називають **розміщенням з n елементів по r**, а невпорядковані – **сполученнями з n елементів по r**. Розміщення з n елементів по n називається **перестановкою**.

Використовують також поняття r-розміщення, r-сполучення та n-перестановки.

Розглянемо два способи вибору елементів. Згідно з першим способом вибору на кожному кроці вибирають елемент з усієї множини A. Отже, один й той самий елемент із множини A може зустрітись у вибірці декілька разів. Такі вибірки називають **вибірками з повтореннями**.

У разі застосування другого способу вибраний елемент вилучають із множини A. Це означає, що на кожному j-му кроці ($1 \le j \le k$) вибирають елемент із множини $A \setminus \bigcup_{k=1}^{j-1} \{a_{ik}\}$ і вибірка не містить однакових елементів. Такі вибірки називають **вибірками без повторень**.

Наприклад, задано множину A = {a,b,c}, тобто n=3. Наведемо розміщення без повторень із трьох елементів по два, тобто r=2:

(a,b), (a,c), (b,c), (b,a), (c,a), (c,b);

розміщення з повтореннями з трьох елементів по два:

(a,b), (a,c), (b,c), (b,a), (c,a), (c,b), (a,a), (b,b), (c,c);

сполучення без повторень із трьох елементів по два:

(a,b), (a,c), (b,c);

сполучення з повтореннями з трьох елементів по два:

(a,b), (a,c), (b,c), (a,a), (b,b), (c,c);

Розміщення

Кількість усіх розміщень без повторень з n елементів по r позначають як A_n^r або A(n,r), де r і n – невід'ємні цілі числа, причому r≤n.

Твердження 1. Справджується рівність $A_n^r = n(n-1)...(n-r+1) = \frac{n!}{(n-r)!}$.

Знайдемо, наприклад, число розміщень з 7 по 3. Тут n=7, n-r+1 = 5. Значить $A_7^3 = 7 \times 6 \times 5 = 210$. Відмітимо, що верхній індекс показує яку кількість співмножників потрібно взяти у добутку.

Рекурентна формула має вигляд:

$$A_n^r = A_{n-1}^r + rA_{n-1}^{r-1},$$

де $A_k^0 = 1$ (не має комбінаторного значення); $A_k^1 = k, \forall k$; $A_k^s = 0$ при k<s.

Наприклад, на п’яти картках написані числа 1, 2, 3, 4, 5. Скільки різних трьохзначних чисел можна з них скласти? Трьохзначні числа представляють собою трьохелементі вибірки з п’яти цифр, причому, вибірки впорядковані, оскільки порядок цифр в числі є важливим. Відповідно цих чисел буде стільки, скільки існує з п’яти елементів по 3: A_5^3 =5×4×3=60.

Кількість різних розміщень із повтореннями з n елементів по r позначають як $\tilde{A}_n^r$ або $\tilde{A}(n,r)$, де r і n – невід’ємні цілі числа.

Твердження 2. Справджується рівність $\tilde{A}_n^r = n^r$.

Наприклад, скільки чотирьохлітерних “слів” можна скласти з літер “М” та “А”? Складемо декілька таких “слів”: МММА, МАМА, МААА ... Ми бачимо, що склад вибірки змінюється, порядок елементів у виборці є суттєвим. Значить, це – розміщення з повторенням з 2-х літер “М” та “А” по 4 літери: $\tilde{A}_2^4 = 2^4 = 16$.

Інший приклад: вздовж дороги стоять 6 світлофорів. Скільки може бути різних комбінацій їх сигналів, якщо кожний світлофор має 3 стани: “червоний”, “жовтий”, “зелений”? Випишемо декілька комбінацій: ЧЧЧЖЗЗ, ЗЗЗЗЗЗ, ЧЖЗЧЖЗ,... Ми бачимо, що склад вибірки змінюється і порядок елементів є суттєвим (якщо, наприклад, у вибірці ЧЖЗЧЖЗ замінити місцями Ч та Ж, то ситуація на дорозі стане іншою). Тому застосовуємо формулу розміщень з повтореннями з 3 по 6: $\tilde{A}_3^6 = 3^6 = 729$.

Перестановки

Кількість різних перестановок позначають як P_n. Формулу для P_n одержують із формули для A_n^n =n!

Наприклад, потрібно знайти кількість способів складання 7 книжок у стопку. Кожна стопка буде відрізнятись від іншої порядком слідування

книжок. Тому це буде перестановка з семи елементів $P_7 = 7! = 7\times6\times5\times4\times3\times2\times1 = 5040$.

Розглянемо тепер задачу про перестановки n елементів за умови, що не всі елементи різні (перестановки з повтореннями). Точніше, нехай є n елементів k різних типів, а число n_j (j=1,…,k) – кількість елементів j-го типу. Очевидно, що $n_1+\ldots+n_k = n$. Перестановки з n елементів за такої умови називають перестановками з повтореннями. Кількість таких перестановок позначають як $P_n(n_1,\ldots,n_k)$. Щоб знайти явний вираз для $P_n(n_1,\ldots,n_k)$, візьмемо окрему перестановку та замінимо в ній усі однакові елементи різними. Тоді кількість різних перестановок, котрі можна отримати з узятої однієї перестановки, дорівнює $n_1! \times n_2! \times\ldots\times n_k!$. Якщо зробити це для кожної перестановки, то одержимо n! перестановок. Отже:

$$P_n(n_1,\ldots, n_k) = \frac{n!}{n_1!\times\ldots\times n_k!}.$$

Наприклад, знайдемо кількість слів, які можна утворити, переставляючи літери слова СОНЦЕ. Оскільки кожна літера тут не повторюється, то можна утворити $P_5 = 5! = 120$ слів. Тепер знайдемо теж саме для слова МАТЕМАТИКА. У цьому слові є повторні входження літер, тому скористаємося формулою для перестановок із повтореннями:

$$P_{10}(2,3,2,1,1,1) = \frac{10!}{2!\times3!\times2!\times1!\times1!\times1!} = 151\,200.$$

Скількома способами можна розставити білі фігури (2 ладі, 2 коня, 2 слона, ферзя та короля) на першій лінії шахової дошки? Перша лінія шахової дошки являє собою 8 клітин, на яких і потрібно розташувати ці 8 фігур. Різні варіанти будуть відрізнятися тільки порядком фігур, тому, це буде перестановка з повторенням $P_8(2,2,2,1,1) = 5040$.

Сполучення

Кількість усіх сполучень без повторень з n елементів по r позначають як C_n^r або C(n,r), де r і n – невід'ємні цілі числа, причому r≤n. Щоб знайти C_n^r, задамося питанням, скільки r-розміщень можна утворити з кожного r-

сполучення. Очевидно, що r!. Тому шукане число, буде в r! разів меншим, ніж число r-розміщень з n елементів.

Твердження 3. Справджується рівність

$$C_n^r = \frac{A_n^r}{r!} = \frac{n(n-1)...(n-r+1)}{r!} = \frac{n!}{r!(n-r)!}.$$

Наприклад, потрібно скласти всі сполучення з трьох літер A, B, C по дві літери. Це будуть AB, AC, BC. Перевіримо це за формулою: $C_3^2 = \frac{3 \cdot 2}{1 \cdot 2} = 3$.

З 20 учнів потрібно обрати двох чергових. Скількома способами це можна зробити? Потрібно обрати двох людей з 20. Ясно, що від порядку вибору нічого не залежить, тобто Іваненко-Петренко та Петренко-Іваненко – це одна й та сама пара чергових. Відповідно, це буде сполучення з 20 по 2:

$$C_{20}^2 = \frac{20 \cdot 19}{1 \cdot 2} = 190.$$

Скількома способами можна групу з 15 студентів розбити на дві групи так, щоби в одній групі було 4, а в іншій – 11 людей? Щоб це зробити, достатньо вибрати 4 людини з 15, а решта самі утворять іншу групу. А обрати 4 людини з 15 можна C_{15}^4 способами.

Цю задачу можна розв'язати інакше: з 15 студентів обрати 11, а решта 4 утворять другу групу. Це можна зробити C_{15}^{11} способами.

Отримуємо ту ж саму відповідь і виникає підозра, що $C_{15}^{11} = C_{15}^4$. Це дійсно так. Сполучення мають властивість:

$$C_n^r = C_n^{n-r}.$$

В цьому легко переконатись:

$$C_n^{n-r} = \frac{n!}{(n-r)!(n-n+r)!} = \frac{n!}{(n-r)!r!} = C_n^{n-r}.$$

Твердження 4. Справджується рівність $C_n^r = C_{n-1}^r + C_{n-1}^{r-1}$.

Кількість усіх сполучень із повтореннями з n елементів по r позначають як $\tilde{C}_n^r$ або $\tilde{C}(n,r)$, де r і n – невід'ємні цілі числа.

Твердження 5. Справджується рівність $\widetilde{C}_n^r = \frac{(n+r-1)!}{r!(n-1)!} = C_{n+r-1}^r$.

Розглянемо наступний приклад. У хлібному відділі магазину є буханки білого та чорного хлібу. Скількома способами можна купити 6 буханок хлібу? Позначаючи буханки білого та чорного хлібу літерами Б та Ч, складемо декілька вибірок: БББЧЧЧ, БЧБЧБЧ, БББББЧ... Склад змінюється від вибірки до вибірки, значить це вже не перестановки; порядок елементів несуттєвий – це сполучення з повторенням з 2 по 6: $\widetilde{C}_2^6 = C_{2+6-1}^6 = C_7^6 = 7$. Зробимо перевірку та випишемо всі варіанти покупок: БББББББ, ББББББЧ, БББББЧЧ, БББЧЧЧ, ББЧЧЧЧ, БЧЧЧЧЧ, ЧЧЧЧЧЧ. Їх дійсно 7.

Схема визначення виду комбінації

Приведемо у систему отримані формули всіх шести видів комбінацій з повтореннями та без. Представимо алгоритм визначення виду комбінації наступною схемою.

Розглянемо декілька прикладів. На колі розташовано 20 точок. Скільки існує вписаних трикутників з вершинами в цих точках? Для знаходження розв’язку пронумеруємо точки числами від 1 до 20. Тоді кожний вписаний

трикутник буде представляти собою трійку чисел. Випишемо декілька вибірок: (1, 5, 19), (15, 2, 9), (14, 13, 7),... Числа у вибірках не можуть повторюватися, тому що всі вершини трикутника різні. Склад змінюється від вибірки до вибірки, порядок не суттєвий, тому що (1, 5, 19) та (19, 5, 1) – один й той самий трикутник. За схемою отримємо, що це сполучення без повторень з 20 по 3.

$$C_{20}^{3} = \frac{20 \cdot 19 \cdot 18}{2 \cdot 3} = 1140.$$

В деякій казковій країні не було двох мешканців з однковим набором зубів (або в них різна кількість зубів, або зубів не має в різних містах). Потрібно оцінити найбільшу чисельність населення цієї країни, якщо максимальна кількість зубів в людини – 32. Для розв'язку закодуємо кожного мешканця набором з 32 нулей та одиниць. Одиниця відповідає наявності зуба в даному місті, нуль – його відсутності. Випишемо декілька комбінацій: 11111...11, 1010...11, 0000...00,... Елементи не повторюються, склад змінюється, порядок суттєвий. Це – розміщення з повтореннями з 2 по 32.

$$A_{2}^{32} = 2^{32} = 4\ 294\ 967\ 296.$$

4.2. Біном Ньютона та поліномна формула

$x + a$, $a + b$, $x + y$ – кожний двочлен, в алгебрі називається біномом.

$(a \pm b)^2 = a^2 \pm 2ab + b^2$

$(a \pm b)^3 = a^3 \pm 3a^2b + 3ab^2 \pm b^3$

$(a+b)^0$	=	1	0
$(a+b)^1$	=	$a+b$	1
$(a+b)^2$	=	$a^2+2ab+b^2$	2
$(a+b)^3$	=	$a^3+3a^2b+3ab^2+b^3$	3
$(a+b)^4$	=	$a^4+4a^3b+6a^2b^2+4ab^3+b^4$	4
$(a+b)^5$	=	$\dots$	5
$(a+b)^6$	=	$\dots$	6

						1						
					1		1					
				1		2		1				
			1		3		3		1			
		1		4		6		4		1		
	1		5		10		10		5		1	
1		6		15		20		15		6		1

Для будь-яких $\boldsymbol{n \in N}$ і $\boldsymbol{a \in R, b \in R}$ має місце рівність

$$\boldsymbol{(a+b)^n = C_n^0 a^n + C_n^1 a^{n-1} b + C_n^2 a^{n-2} b^2 + \cdots + C_n^{n-1} a b^{n-1} + C_n^n b^n.} \quad (1)$$

Ця формула відома в математичній літературі як біном Ньютонаі дозволяє, користуючись формулою для обчислення числа комбінацій з n елементів по k елементів, обчислювати коефіцієнти в розкладі n-гостепеня двочлена.

Приклад. Знайти розклад $(x+a)^6$. Розв'язання.

$$(x+a)^6\ x^6 + C_6^1 x^5 a + C_6^2 x^4 a^2 + C_6^3 x^3 a^3 + C_6^4 x^2 a^4 + C_6^5 x^1 a^5 + a^6 = \cdots$$

$$1 \qquad 6 \qquad 15 \qquad \underline{\mathbf{20}} \qquad 15 \qquad 6 \qquad 1$$

Властивості розкладу бінома Ньютона

$$(a+b)^n = C_n^0 a^n + C_n^1 a^{n-1} b + C_n^2 a^{n-2} b^2 + \cdots + C_n^{n-1} a b^{n-1} + C_n^n b^n$$

1. Кількість доданків у розкладі (1) дорівнює n + 1.

2. У кожному доданку сума степенів при a та b дорівнює n. Показники степені букви a спадають від n до 0, показники степені букви b зростають від 0 до n.

3. (k + 1)-й член розкладу ($0 \le k \le n$) має вигляд:

$\boldsymbol{T_{k+1} = C_n^k a^{n-k} b^k}$ – загальний член розкладу

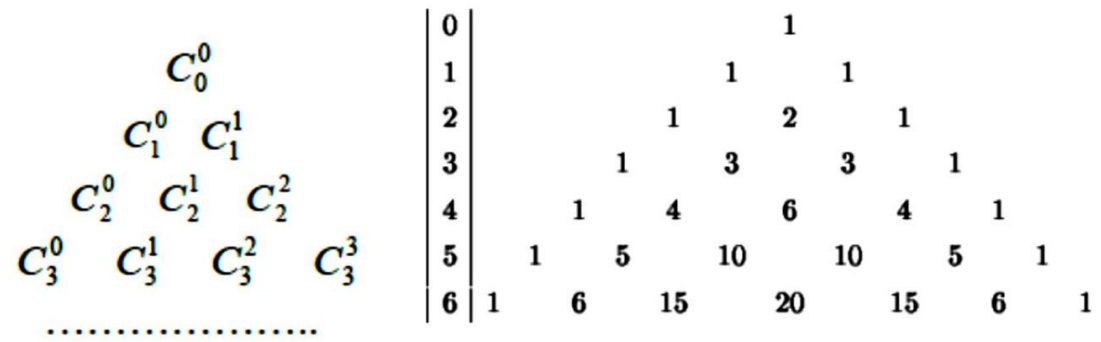
Біномні коефіцієнти та їх властивості

$\boldsymbol{C_n^0,\ C_n^1, C_n^2, \ldots, C_n^k, \ldots, C_n^{n-1}, C_n^n}$ – біноміальні коефіцієнти

1. Біномні коефіцієнти членів розкладу, рівновіддалених від його кінців, рівні між собою:

$$C_n^0 = C_n^n, \quad C_n^1 = C_n^{n-1}, \ldots, \quad C_n^m = C_n^{n-m}.$$

2. Якщо показник степені n – парне число, то середній член розкладу має найбільший біноміальний коефіцієнт; якщо n – непарне число, то біноміальні коефіцієнти двох середніх членів рівні між собою та також є найбільшими (див. трикутник Паскаля).



3. Перший біномний коефіцієнт дорівнює 1, другий – *n*, коефіцієнт (k + 1)-го члену розкладу дорівнює коефіцієнту k-го члена, помноженого на

$$C_n^k = C_n^{k-1} \cdot \frac{n-k+1}{k}$$ – рекурентна формула.

4. Сума всіх біноміальних коефіцієнтів дорівнює 2^n:

$$C_n^0 + C_n^1 + C_n^2 + \cdots + C_n^n = 2^n,$$

$$\sum_{k=0}^{n} C_n^k = 2^n.$$

5. Сума біноміальних коефіцієнтів, що стоять на парних місцях розкладу, дорівнює сумі біноміальних коефіцієнтів членів, що стоять на непарних місцях:

$$C_n^1 + C_n^3 + \cdots = C_n^0 + C_n^2 + \cdots = 2^{n-1}.$$

Приклад 1.

Знайдіть середній член розкладу бінома $\left(2x + \frac{y}{2}\right)^8$

$$T_5 = C_8^4 (2x)^4 \left(\frac{y}{2}\right)^4 = \ldots = 70x^4y^4$$

Приклад 2.

Довести, що сума всіх коефіцієнтів розкладу бінома $(2a - b)^n$ при будь-якому натуральному *n* дорівнює 1.

В розкладі (1) покладемо: a = b = 1, отримаємо $(2 - 1)n = 1$.

4.3. Основи криптографії: класичні методи

Шифрування – це кодування даних з метою захисту від несанкціонованого доступу. Процес кодування називається шифруванням, а

процес декодування – **розшифруванням**. Само кодоване повідомлення називається **шифрованим**, а застосований метод називається **шифром**.

Основна вимога до шифру полягає в тому, щоб розшифрування (і, можливо, шифрування) були можливе тільки при наявності санкцій, тобто деякої додаткової інформації (або пристрою), яка називається **ключем шифру**. Процес декодування шифровки без ключа називається **дешифруванням**.

Галузь знань про шифри, методи їх побудови та розкриття називається криптографією. Властивість шифру протистояти розкриттю називається криптостійкістю або надійністю і звичайно визначається складністю алгоритму дешифровки.

У практичній криптографії криптостійкість шифру оцінюється з економічних міркувань. Якщо розкриття шифру коштує (в грошовому еквіваленті, включаючи необхідні комп'ютерні ресурси, спеціальні пристрої тощо) більше, за саму зашифровану інформацію, то шифр вважається достатньо надійним.

Симетричні криптосистеми

Симетричні криптосистеми (**симетричне шифрування**) – спосіб шифрування, в якому для шифрування та дешифрування використовуються один й той самий криптографічний ключ.

Ключ шифрування має зберігатись у секреті обома сторонами та має бути обраним до початку обміну повідомленнями.

Одним з прикладів симетричного шифрування є алгоритм **гамування**. Він заснований на випадкових числах. Нехай маємо датчик псевдо-випадкових чисел, який працює за деяким визначеним алгоритмом. Часто використовують наступний алгоритм:

$$T_{i+1} = (a \cdot T_i + b) \bmod c,$$

де T_i – попереднє псевдо-випадкове число, T_{i+1} – наступне псевдо-випадкове число, а коефіцієнти a, b, c сталі та добре відомі. Зазвичай $c = 2^n$,

де n – розрядність процесору, a mod 4 = 1, b – непарне. В цьому випадку послідовність псевдо-випадкових чисел має **період** c.

Процес шифрування визначається наступним чином. Шифроване повідомлення представляється у вигляді послідовності слів S_0, S_1,…, кожне довжини n, які додаються за модулем 2 зі словами послідовності T_0, T_1, …, тобто

$$C_i = S_i \oplus T_i.$$

Послідовність T_0, T_1, … називається **гамою шифру**.

Процес розшифрування заключається в тому, щоби ще раз скласти шифровану послідовність з тією самою гамою шифру:

$$S_i = C_i \oplus T_i.$$

Ключем шифру є початкове значення T_0, яке є секретним та має бути відоме тільки відправнику та адресату шифрованого повідомлення. Якщо період послідовності псевдо-випадкових чисел достатньо великий, щоби гама шифру була довша повідомлення, то дешифрувати повідомлення можна тільки підбором ключа. При збільшенні n експоненційно збільшується криптостійкість шифру.

Описаний метод має суттєвий недолік. Якщо відома хоча б частина висхідного повідомлення, то все повідомлення може бути легко дешифроване. Дійсно, нехай відоме одне висхідне слово S_i. Тоді:

$$T_i = C_i \oplus S_i,$$

і далі вся права частина гами шифру визначається за вказаною формулою датчика псевдо-випадкових чисел.

Більшість симетричних шифрів використовують складну комбінацію великої кількості підстановок та перестановок. Багато таких шифрів виконуються у декілька (до 100) проходів, використовуючи на кожному проході **ключ проходу**. Множина «ключів проходів» для всіх проходів називається **розкладом ключів**. За звичай, він утворюється з ключа шляхом виконання над ним певних операцій, в тому числі перестановок та підстановок.

Найважливішими параметрами всіх алгоритмів симетричного шифрування є:

- стійкість;
- довжина ключа;
- кількість раундів;
- довжина блоку, якій обробляється;
- складність апаратно/програмної реалізації;
- складність перетворень.

До переваг симетричної системи можна віднести:

- порівняно високу швидкість (приблизно на 3 порядки вищу ніж у асиметричних систем);
- простота реалізації (за рахунок більш простих операцій);
- менша необхідна довжина ключа для відповідної стійкості;

Але є також суттєві недоліки, які практично призводять до того, що дана система майже не використовується на даний час.

- складність керування ключами у великій мережі. Це означає квадратичне збільшення кількості ключів, які необхідно генерувати, зберігати, передавати та знищувати у мережі. Для мережі з 10 абонентів потрібно 45 ключів, для 100 – вже 4950, для 1000 – 499500;
- складність обміну ключами. Для застосування симетричної системи необхідно вирішити проблему надійної передачі ключів до кожного абонента, тому що необхідний секретний канал для передачі кожного ключа обом сторонам.

Асиметричні криптосистеми

Криптографічна система з відкритим ключем (або асиметрична криптосистема, асиметричне шифрування) – це система шифрування, при якій відкритий ключ передається по відкритому (тобто не захищеному) каналу зв'язку та використовується для шифрування повідомлень. Для

розшифрування повідомлень використовується секретний (або приватний) ключ.

Наявність двох ключів – відкритого та закритого – й робить цю систему асиметричною. Відкритий ключ розсилається всім, хто бажає відправляти повідомлення адресату, а приватний ключ зберігається адресатом і не повинен відправлятись будь-кому. Навіть якщо знати відкритий ключ та все відправлене розшифроване повідомлення, неможливо знайти приватний ключ.

Підхід у системі з відкритим ключем базується на існуванні односторонніх функцій – функцій f(x), для яких по відомому x легко знайти значення функції f(x), але для відомого значення функції f(x) неможливо (або занадто важко) знайти значення аргументу x, тобто обчислити обернену функцію.

Розглянемо один з найвідоміших та найбільш поширених алгоритмів – RSA. Цей алгоритм, зокрема, використовується для передачі даних захищеними каналами зв'язку мережі Інтернет – HTTPS, SSH. Інший відомий алгоритм, який був першим з алгоритмів асиметричного шифрування – алгоритм Діффі-Хелмана (DH).

Алгоритм RSA базується на властивостях простих та взаємно простих чисел, а саме задача множення та розкладання складених чисел на прості співмножники. Ця задача є обчислювально одно направленою. Тобто для заданих простих співмножників знайти складене число дуже легко – необхідно просто перемножити ці співмножники, а для заданого складного числа знайти його прості співмножники – набагато складніше. У реальних системах, коли використовуються складені числа розмірності в 100 знаків та більше, час, необхідний для розв'язання задачі розкладання числа на прості співмножники, вимірюється роками.

У системі RSA кожен ключ складається з пари цілих чисел. Відкритий та закритий ключі утворюють узгоджену пару, тобто є взаємно оберненими з точки зору задачі шифрування.

Наведемо алгоритм RSA генерації закритого та відкритого ключів.

1. Обрати два випадкових простих числа p та q заданого розміру (наприклад 1024 біт).

2. Обчислити n = pq, яке називається **модулем**.

3. Обчислити $\varphi(n) = (p-1)(q-1)$.

4. Обрати ціле число e ($1 \leq e \leq \varphi(n)$), взаємно просте з $\varphi(n)$. Зазвичай у якості e беруть прості числа, які містять невелику кількість одиничних бітів у двійковому записі (наприклад 17, 257, 65537).

Число e називається **відкритою експонентою**. Занадто малі значення e потенційно можуть послабити криптостійкість шифру.

5. Обчислити число d, яке є мультиплікативно оберненим до числа e за модулем $\varphi(n)$, тобто число, яке задовольняє умові:

$$de = 1 \bmod (\varphi(n))$$

Число d називається **секретною експонентою**.

Пара P = (e, n) публікується в якості відкритого ключа RSA. Пара S = (d, n) відіграє роль закритого (приватного) ключа RSA.

Повідомлення мають бути менші за число n. Якщо повідомлення більше за n, то його б'ють на частини.

Процес обміну повідомленнями від сторони B стороні A полягає у таких кроках:

- сторона A генерує за вказаним алгоритмом пару ключів - P = (e, n) та S = (d, n) - і відправляє відкритим каналом стороні B свій відкритий ключ;
- сторона B шифрує повідомлення M за допомогою ключа P = (e, n):

$$C = M^e \bmod n$$

та відправляє його стороні A;

- сторона A приймає зашифроване повідомлення C та розшифровує його своїм закритим ключем S = (d, n):

$$M' = C^d \bmod n.$$

Теорема 4.1. (без доведення). Шифрування з відкритим ключем є коректним, тобто M = M’.

До переваг можна віднести:

- не потрібно передавати закритий ключ будь-якими каналами зв'язку;
- на противагу симетричній криптосистемі, секретний ключ зберігається тільки у одній стороні;
- у симетричній криптосистемі варто змінювати ключ після кожного сеансу передачі даних; у асиметричній ключі можна тримати незміненими достатньо довгий час;
- у більшості мереж кількість ключів при асиметричному шифруванні набагато менша, ніж при симетричному.

Недоліки:

- хоча повідомлення шифруються надійно, але самі сторони «засвічуються» самим фактом передачі (на чому може буде побудована атака);
- асиметричні алгоритми використовують набагато довші ключі ніж симетричні;
- у чистому вигляді асиметричні системи вимагають значних обчислювальних ресурсів, тому на практиці вони частіше використовуються разом з іншими алгоритмами.

Наведемо декілька слів відносно криптостійкості асиметричного шифрування. Одна з можливих атак на таку систему полягає в наступному. Припустимо, що сторони A та B обмінюються повідомленнями, як це було описано вище. Якщо третя сторона C захоче втрутитись у цей процес, то вона може прослуховувати канал зв'язку між A та B і підставляти свої повідомлення замість оригінальних. Так, спочатку, коли A відправляє B свій відкритий ключ P_A, сторона C може перехопити цей ключ та надіслати до B власний ключ P_C. Тоді B буде кодувати повідомлення за допомогою неправильного ключа P_C. Перехопивши ці повідомлення, C зможе їх розкодувати своїм приватним ключем, а замість оригінального повідомлення

направити до А якесь інше некоректне повідомлення, закодоване вже ключем P_A. Описаний тип атаки має назву «men-in-the-middle».

Цифровий підпис

Також асиметрична система з відкритим ключем використовується у системах цифрових підписів. Цей процес ґрунтується на властивості комутативності операцій шифрування та розшифрування:

$$M = (M^e)^d \bmod n = M^{ed} \bmod n = M^{de} \bmod n = (M^d)^e \bmod n = M.$$

Нехай сторона А відправляє стороні В повідомлення М. Для того, щоб підтвердити, що повідомлення дійсно відправлено від А, ця сторона супроводжує його підписом $C = M^d \bmod n$, таким чином надсилаючи до В пару (М, С). Сторона В, отримав це повідомлення з підписом, кодує повідомлення М відкритим ключем P_A: $C' = M^e \bmod n$. Якщо $C = C'$, то повідомлення М дійсно прийшло від сторони А неушкодженим. Інакше, повідомлення було пошкоджено або замінено третьою стороною.

Використання теорії множин до аналізу текстів та підбору здвигу в шифрі Цезарі (одноалфавітної заміни)

У математиці під множиною розуміють сукупність, зібрання деяких предметів, об’єктів, які об’єднуються між собою характеристичною ознакою. Математичний зміст терміну «множина» відрізняють від повсякденного, де його зв’язують з великою кількістю об’єктів. У математиці розглядаються множини, які складаються з декількох елементів або їх немає. Об’єкти будь-якої природи (літери, числа, книги), з яких складається множина називається елементами.

Приклад. Які літери використовуються в записі слова «м а т е м а т и к а»? Яка їх потужність (кількість елементів)?

М={ м, а, т, е, и, к}.

Зауваження:

1) у множині кожен елемент зустрічається лише один раз.

2) порядок запису елементів множин немає значення.

літери	м	а	т	е	и	к
потужн.	2	3	2	1	1	1

Такий спосіб можна використовувати для аналізу шифрів.

Шифри одноалфавітної заміни є найпростішими серед інших шифрів заміни. Принцип їхньої дії побудований на тому, що кожній букві відкритого тексту ставиться у відповідність інша, але детермінована (незмінна) буква деякого алфавіту (алфавіту заміни). Через те, що кожній букві відкритого тексту відповідає єдина буква алфавіту заміни, всьому відкритому алфавіту відповідає єдиний незмінний алфавіт заміни, тому шифри цього класу називають шифрами одноалфавітної заміни.

Розглянемо шифр одноалфавітної заміни на прикладі так званого **шифру Цезаря**. Щоб розібрати і прочитати його тексти, потрібно всякий раз читати четверту букву замість першої відповідно до алфавіту, наприклад Д замість А, у цьому разі алфавіт представлявся як кільце – наступним за символом Я вважався символ А. Ми розглянемо узагальнений шифр Цезаря, у якому будемо зсовувати символи початкового алфавіту на довільну кількість позицій. Знак пробілу між словами не враховується.

Алфавіт для шифрування

АБВГДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ

Алф.	А	Б	В	Г	Д	Е	Є	Ж	З	И
Зам.	Е	Є	Ж	З	И	І	Ї	Й	К	Л

І	Ї	Й	К	Л	М	Н	О	П	Р	С
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц

Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
Ч	Ш	Щ	Ь	Ю	Я	А	Б	В	Г	Д

Зашифруємо текст шифром Цезаря з ключем К=5:

Відкритий текст:

МНОЖИНА – ОДНЕ З ОСНОВНИХ ПОНЯТЬ СУЧАСНОЇ МАТЕМАТИКИ. СТРОГО ВОНО НЕ ВИЗНАЧАЄТЬСЯ, АЛЕ МОЖЕ БУТИ ДАНО ІНТУЇТИВНЕ ВИЗНАЧЕННЯ МНОЖИНИ ЯК СУКУПНОСТІ ПЕВНИХ І РІЗНИХ ОБ'ЄКТІВ ДОВІЛЬНОЇ ПРИРОДИ, ЯКА РОЗГЛЯДАЄТЬСЯ ЯК ОДНЕ ЦІЛЕ. ОБ'ЄКТИ, ЯКІ СКЛАДАЮТЬ МНОЖИНУ, НАЗИВАЮТЬСЯ ЇЇ ЕЛЕМЕНТАМИ. НАПРИКЛАД, МОЖНА ГОВОРИТИ ПРО МНОЖИНУ УСІХ КНИГ У ПЕВНІЙ БІБЛІОТЕЦІ, МНОЖИНУ ЛІТЕР УКРАЇНСЬКОГО АЛФАВІТУ АБО ПРО МНОЖИНУ ВСІХ КОРЕНІВ ПЕВНОГО РІВНЯННЯ.

Усього літер у тексті – 360.

Шифротекст:

СТУЙЛТЕУИТІКУЦТУЖТЛЬФУТДЧВЦШЯЕЦТУНСЕЧІСЕЧЛПЛЦЧХУЗУЖУТУТІЖЛКТ
ЕЯЕЇЧВЦДЕРІСУЙІЄШЧЛИЕТУМТЧШНЧЛЖТІЖЛКТЕЯІТТДСТУЙЛТЛДПЦШПШФТУ
ЦЧМФІЖТЛЬМХМКТЛЬУЄЇПЧМЖИУЖМРВТУНФХЛХУИЛДПЕХУКЗРДИЕЇЧВЦДДПУ
ИТІЮМРІУЄЇПЧЛДПМЦПРЕИЕГЧВСТУЙЛТШТЕКЛЖЕГЧВЦДННІРІСІТЧЕСЛТЕФХЛП
РЕИСУЙТЕЗУЖУХЛЧЛФХУСТУЙЛТШШЦМЬПТЛЗЖФІЖТМОЄМЄРМУЧІЮМСТУЙЛТ
ШРМЧІХШПХЕНТЦВПУЗУЕРЩЕЖМЧШЕЄУФХУСТУЙЛТШЖЦМЬПУХІТМЖФІЖТУЗ
УХМЖТДТТД

Побудуємо діаграму розподілу частот символів відкритого і шифротексту:

Відкритий текст:

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М
23	6	17	6	8	18	4	8	6	25	18	6	1	14	10	12

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
43	37	9	13	13	19	12	1	5	2	3	0	0	7	2	12

Шифротекст:

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М
0	0	7	2	12	23	6	17	6	8	18	4	8	6	25	18

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
6	1	14	10	12	43	37	9	13	13	19	12	1	5	2	3

З двох приведених діаграм розподілу частот, ми бачимо, що рядок чисел для відкритого тексту складається з чисел:

23, 6, 17, 6, 8, 18, 4, 8, 6, 25, 18, 6, 1, 14, 10, 12 , 43, 37, 9, 13, 13, 19, 12, 1, 5, 2, 3, 0, 0, 7, 2, 12,

а рядок чисел для шифротексту складається з чисел:

0, 0, 7, 2, 12, 23, 6, 17, 6, 8, 18, 4, 8, 6, 25, 18, 6, 1, 14, 10, 12 , 43, 37, 9, 13, 13, 19, 12, 1, 5, 2, 3.

Іншими словами, починаючи з шостого символу, числовий рядок для шифротексту ідентичний початку рядка для відкритого тексту, перші п’ять членів рядка повторюють останні п’ять членів рядка. Побудувавши діаграму, побачимо це в більш наглядній формі:

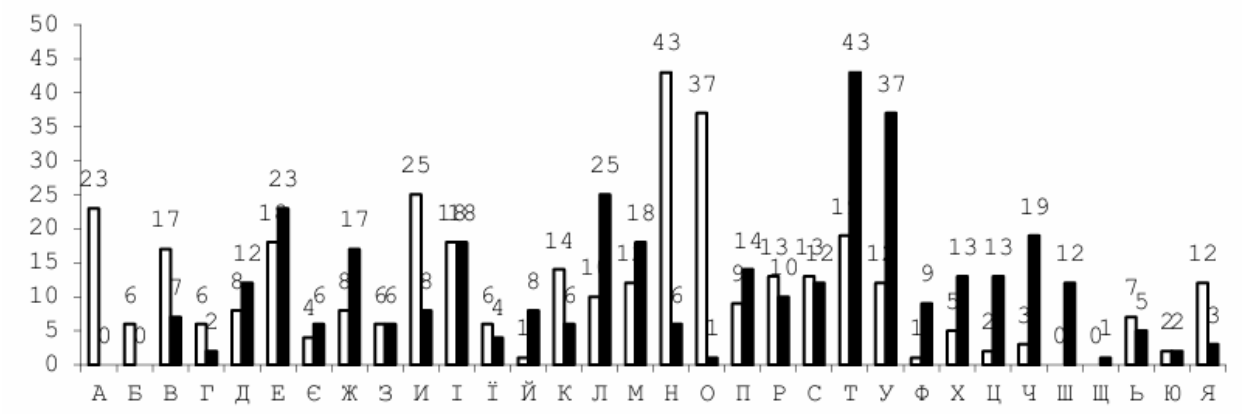


Рис. 4.1. Діаграма розподілу частот відкритого і шифрованого текстів, де – відкритий текст; – шифротекст

Причому порівнювати можна як окремі елементи (О–У (37)), так і групи символів (И, І – Л, М). Перейдемо до аналізу шифру Цезаря тільки на основі шифротексту.

Для цього ми повинні:

− побудувати діаграми розподілу частот для відкритого і шифрованого текстів у процентному відношенні, оскільки довжина відкритого і шифрованого текстів може відрізнятися;

− розташувати частоти у порядку зростання;

− знайти можливі значення ключа як різницю між відповідними значеннями частот.

Приклад.

Таблиця 4.1. Ранжовані частоти використання букв української мови

О	0,0942	р	0,0448	я	0,0248	ж	0,0093
А	0,0807	с	0,0424	з	0,0232	ю	0,0093
Н	0,0681	л	0,0369	б	0,0177	ц	0,0083
И	0,0626	к	0,0354	ь	0,0177	ш	0,0076
І	0,0575	д	0,0338	г	0,0155	ї	0,0065
В	0,0535	у	0,0336	ч	0,0141	є	0,0061
Т	0,0535	м	0,0303	й	0,0138	щ	0,0056
Е	0,0495	п	0,0290	х	0,0119	ф	0,0028

Рисунок 4.2. Гістограма частот використання букв алфавіту української мови

5. ТЕОРІЯ ГРАФІВ

5.1. Графи

Теорія графів – розділ дискретного аналізу, який має широке застосування в багатьох наукових дисциплінах завдяки тому, що поняття і інструментарії цієї теорії виявися дуже зручним для дослідження та інтерпретації різноманітних проблем у великої кількості наук: кібернетиці, технічній і економічній, теорії автоматів, теорії управління, теорії інформації тощо.

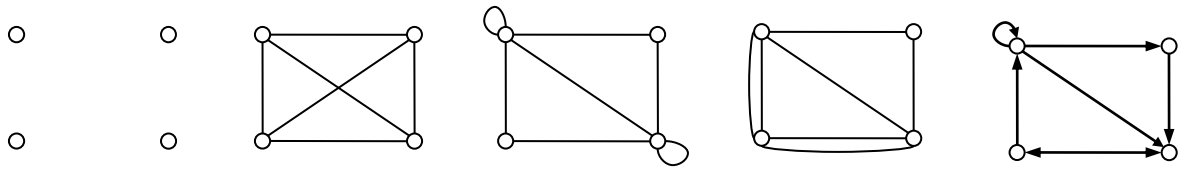
За допомогою інструментарію теорії графів розв'язується велика кількість економіко-математичних задач, зокрема наведена у вступі задача „про призначення", задача календарного планування, мережевого планування тощо. Взагалі теорія має велике значення у всіх галузях науки, які стосуються аналізу і управління економікою.

Основні поняття теорії графів.

З поняттям графа зазвичай пов'язують його графічне представлення, при якому він зображується як множина точок, деякі з яких з'єднані лініями. Але граф відрізняється від геометричних конфігурацій (скажімо, фігур, які також складаються з точок та ліній) тим, що в графі несуттєві відстані між точками, форма з'єднувальних ліній та кути між ними. Важливо лиш те, чи з'єднана дана пара точок лінією, чи ні. Тому граф іноді називають **топологічним об'єктом**, тобто об'єктом, властивості якого не змінюються при розтягуванні, стисненні та викривленні. За цією ж причиною (важливим є тільки наявність або відсутність з'єднань) граф – об'єкт дискретний і може бути заданий двома дискретними множинами: множиною точок, які будемо називати **вершинами**, та множиною ліній, які з'єднують деякі вершини. Лінії будемо називати **ребрами**.

Графом G = (V,E) називається об'єкт, який заданий парою множин (V, E), де V – множина **вершин**, $E \subseteq V \times V$ – множина **ребер**. Граф називається скінченним, якщо множини його вершин і ребер є скінченними. Множину вершин графа G позначають V(G), а множину ребер – E(G).

Кількість вершин графа n(G) = |V(G)|, а кількість ребер m(G) = |E(G)|. Кількість вершин n(G) графа називають його **порядком**.



а б в г д

Рисунок 5.1.

Якщо для деякого ребра e = (v,w) ∈ E(G), то кажуть:

- вершини v та w **суміжні**;
- вершини v та w **інцидентні** ребру e;
- ребро e **інцидентне** вершинам v і w.

Означення 21.2. Множина вершин, які суміжні з вершиною v, називається **множиною суміжності** вершини v і позначається $\Gamma^+(v)$:

$$\Gamma^+(v) = \{w \in V \mid (w,v) \in E\},\ \Gamma^*(v) = \Gamma^+(v) + v.$$

Зазвичай $\Gamma^+(v)$ позначається просто $\Gamma(v)$. Очевидно, $w \in \Gamma(v)$ тоді й тільки тоді, коли $v \in \Gamma(w)$.

Якщо $A \subset V$ – множина вершин, то $\Gamma(A)$ – множина всіх вершин, суміжних з вершинами з A:

$$\Gamma(A) = \{w \in V \mid \exists v \in A,\ w \in \Gamma(v)\} = \bigcup_{v \in A} \Gamma(v).$$

Множина ребер E може бути порожньою (рис. 5.1, а). Такий граф називається **нуль-графом** і позначається ∅. Якщо ж множина вершин V – порожня, то порожньою є також множина E. Такий граф називається **порожнім**. Лінії, що зображують ребра графа, можуть перетинатися, але точки перетину не є вершинами (рис. 5.1, б). Ребро може з'єднувати деяку вершину саму з собою (рис. 5.1, в), таке ребро називається **петлею**. Цей випадок відповідає наявності в множині E пар вигляду (v, v). Різні ребра можуть бути інцидентними одній і тій самій парі вершин (тобто одну й ту саму пару вершин з'єднує більше ніж одне ребро), такі ребра називаються **кратними** (рис. 5.1, г).

Граф називається **простим**, якщо кожну пару вершин з'єднує не більше, ніж одне ребро. Граф називається **мультиграфом**, якщо він має кратні ребра. Граф називається **псевдографом**, якщо він має петлі та кратні ребра.

Розглядають також орієнтовані графи (до цього були розглянуті неорієнтовані графи).

Орієнтованим графом (орграфом) називається граф D = (V, E), де V – множина вершин, $E \subseteq V \times V$ – множина орієнтованих ребер, або **дуг**.

При зображенні орієнтованих графів напрямки ребер позначаються стрілками (рис. 5.1, д). Орієнтований граф може мати кратні ребра, петлі, а також петлі, що з'єднують одні й ті самі вершини, але у зворотних напрямках.

Кожному неорієнтованому графу можна поставити у відповідність орієнтований граф з тією самою множиною вершин, в якій кожне ребро замінено двома орієнтованими ребрами, що є інцидентними тим самим вершинам і мають зворотні напрямки.

5.2. Основні алгоритми на графах

Алгоритми пошуку найкоротших шляхів

При розв'язанні широкого кола прикладних задач нерідко виникає необхідність знайти маршрут, що зв'язує задані вершини в графі G. Наведемо алгоритм розв'язання такої задачі. В ньому задача зводиться до пошуку маршруту у зв'язаному графі G = (V, E), який з'єднує задані вершини $v, u \in V$, де $v \neq u$.

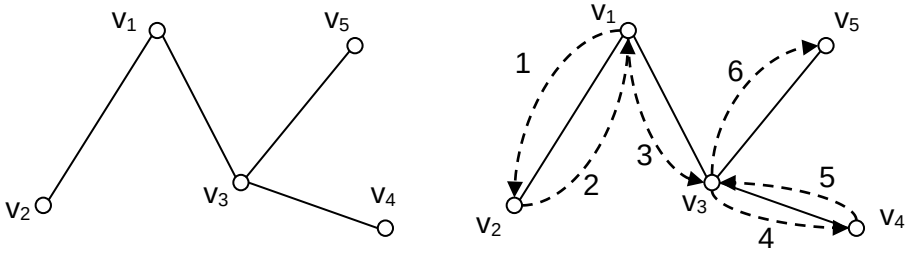
Алгоритм Террі знаходження маршруту

У зв'язаному графі зажди можна знайти такий маршрут, що зв'язує дві задані вершини v та u, якщо, виходячи з вершини v і здійснюючи послідовний перехід від кожної досягнутої вершини до суміжної з нею, керуватися такими правилами:

1) йдучи по довільному ребру, кожний раз відмічати напрямок, в якому воно було пройдене;
2) виходячи з деякої вершини v_1, завжди рухатися тільки по тому ребру, яке не було пройдене або було пройдене у зворотному напрямку;
3) для кожної вершини v_1, відмінної від v, відмічати те ребро, яке першим заходить у v_1, якщо вершина v_1, зустрічається вперше;
4) виходячи з деякої вершини v_1, відмінної від v, по першому ребру, яке заходить у v_1, рухатися лише тоді, коли немає інших можливостей.

Обґрунтування алгоритму. Припустимо, що, керуючись цим алгоритмом, зупинимося в деякій вершині w (не досягши вершини u), а всі ребра, інцидентні w, вже пройдено в напрямку з w (тоді внаслідок правила 2 вже не можна вийти з w). Покажемо, що в цьому випадку: а) вершина w збігається з v; б) всі вершини графа G пройдено.

Наведемо приклад використання алгоритму Террі. Необхідно знайти у графі G (рис. 27.1, а) маршрут, який з'єднує вершини v_1 та v_5.



а б

Рисунок 5.2.

Пошук вершини v_5 у G будемо здійснювати так, неначе нічого невідомо про цей граф (це можна порівняти з тим, що G – це лабіринт, v_1 та v_5 – вхід та вихід лабіиринту. На рис. 5.2, б показаний один із можливих варіантів руху по графу G згідно з алгоритмом Террі. Пронумерованими штриховими дугами зображено схему руху по графу G. Знаками помічено перші ребра, які заходять у вершини. Ця схема руху відповідає маршруту (v_1, v_2, v_1, v_3, v_4, v_3,

v_5). Зазначимо, що після того, як із вершини v_1 зайшли у вершину v_3 (дуга 3), внаслідок правила 4 не можна повернутися у v_1, оскільки існують інші можливості, а (v_1, v_3) є першим ребром, що заходить у v_3. Далі, після того, як із вершини v_4 зайшли у вершину v_3 (дуга 5), внаслідок правила 2 не можна рухатися до вершини v_1, і, таким чином, залишається єдина можливість – рухатися до вершини v_5.

Пошук відстані між вершинами графа

Розглянемо деякі властивості мінімальних (шляхів) маршрутів.

Назвемо образом вершини x в орієнтованому графі G множину кінців дуг, початком яких є вершина x (позначається D(x)), а множину початків дуг, кінцем яких є вершина x, назвемо прообразом вершини x (позначається $D^{-1}(x)$).

Зрозуміло, що $D(x) \cup D^{-1}(x) = Г(x)$, де Г(x) – множина суміжності вершини x.

Нехай G = (V, E) – орієнтований граф з n вершинами (n≥2), а v, u - задані вершини з V, де v≠u. Опишемо алгоритм пошуку відстані та відповідного їй мінімального шляху з v до u в орієнтованому графі G. Цей алгоритм також має назву хвильового.

Алгоритм (хвильовий)

1. Позначаємо вершину v індексом 0, а вершини, що належать образу вершини v, - індексом 1. Множину вершин з індексом k позначаємо $F_k(v)$. Вважаємо k=1.
2. Якщо $F_k(v) = \varnothing$ або виконується $k = n - 1$ і $u \notin F_k(v)$, то вершина u є незв'язаною з v і робота алгоритму на цьому завершується. В іншому випадку перейти до пункту 3.
3. Якщо $u \notin F_k(v)$, то переходимо до пункту 4. В іншому випадку існує шлях із v до u завдовжки k, причому цей шлях є мінімальним. Послідовність вершин v, u_1, u_2,…, u_{k-1}, u, де

$u_{k-1} \in F_{k-1}(v) \cap D^{-1}(u)$,

$u_{k-2} \in F_{k-2}(v) \cap D^{-1}(u_{k-1})$,

……..

$u_1 \in F_1(v) \cap D^{-1}(u_2)$,

і є шуканим мінімальним шляхом з v у w. На цьому робота алгоритму завершується.

4. Позначаємо індексом k+1 всі непозначені вершини, які належать образу множини вершин з індексом k. Множину вершин з індексом k+1 позначаємо $F_{k+1}(v)$. Збільшуємо індекс k на 1 і переходимо до пункту 2.

Назва алгоритму – хвильовий – пов’язана з тим, що визначення індексів k вершин графа G відбувається як розповсюдження з початкової вершини v певної хвилі, яка спрямовується за напрямком дуг. Коли хвиля дійде до кінцевої вершини u, це буде означати, що алгоритм закінчив свою роботу. Значення індексу, „принесеного хвилею”, у вершині u буде відповідати довжині знайденого маршруту. А для того, щоб визначити цей маршрут (послідовність вершин), потрібно з кінцевої вершини u повертатися в зворотному до розповсюдження хвилі напрямку і відзначати послідовно одну довільну вершину зі значеннями індексу k-1, k-2, …, 1, 0. Зрозуміло, що вершина з індексом 0, - це початкова вершина v.

Вершини u_1, u_2,…, u_{k-1}, взагалі, можуть бути визначені неоднозначно. Ця неоднозначність відповідає випадкам, коли існує кілька різних мінімальних шляхів з v до u в орграфі G.

Наприклад, визначимо мінімальний шлях з v_1 до v_6 в орієнтованому графі G, заданому матрицею суміжності (відповідний граф представлено на рис. 5.3):

	1	2	3	4	5	6
1						
2						
3						

4						
5						
6						

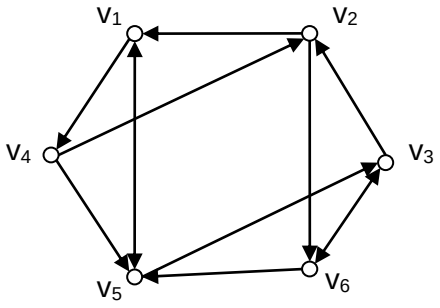


Рис. 5.3

Діючи згідно з хвильовим алгоритмом, послідовно знаходимо $F_1(v_1) = \{v_4, v_5\}$; $F_2(v_1) = = D(F_1(v_1)) \setminus \{v_1, v_4, v_5\} = \{v_2, v_3\}$; $F_3(v_1) = D(F_2(v_1)) \setminus \{v_1, v_2, v_3, v_4, v_5\} = \{v_6\}$. Таким чином, $v_6 \in F_3(v_1)$, а отже, за пунктом 3 існує шлях з v_1 до v_6 завдовжки 3, і цей шлях є мінімальним.

Знайдемо тепер мінімальний шлях із v_1 до v_6. Визначимо множину

$F_2(v_1) \cap D^{-1}(v_6) = \{v_2, v_3\} \cap \{v_2, v_3\} = \{v_2, v_3\}$.

Виберемо будь-яку вершину зі знайденої множини, наприклад, v_3. Визначимо далі множину

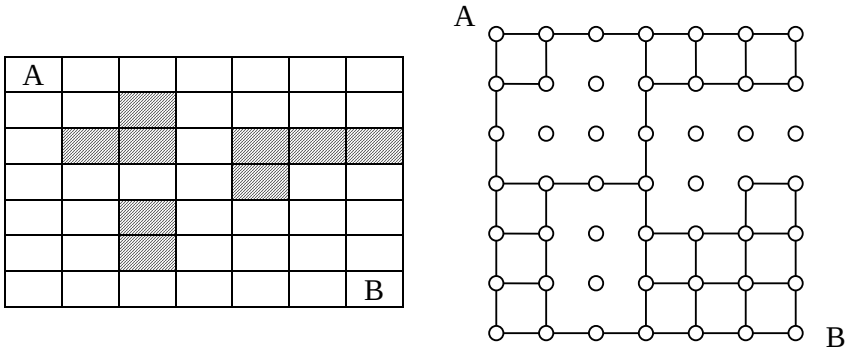
$F_1(v_1) \cap D^{-1}(v_3) = \{v_4, v_5\} \cap \{v_4, v_5, v_6\} = \{v_4, v_5\}$.

Виберемо будь-яку вершину зі знайденої множини, наприклад, v_5. Тоді (v_1, v_5, v_3, v_6) – шуканий мінімальний шлях з v_1 до v_6 в орієнтованому графі G, а відстань між v_1 та v_6 дорівнює 3.

Очевидно, хвильовий алгоритм може застосовуватися не тільки для орієнтованих, а й для неорієнтованих графів. В останньому випадку, пересування з однієї вершини до іншої можливі в обидві сторони.

Хвильовий алгоритм широко застосовується у розробці комп'ютерних ігор – коли необхідно визначити оптимальний маршрут пересування гравця або певного «юніта» з однієї точки віртуальної місцевості (карти) до іншої. Наведемо приклад такої задачі. Нехай потрібно знайти найкоротший

маршрут з точки A до точки B на карті, яка зображена на рис. 5.4, а. На ній заштриховані комірки відповідають певним перепонам на шляху, тобто в цих частинах місцевості «юніт» не зможе пройти. Також будемо вважати, що «юніт» може пересуватись тільки по вертикалі та горизонталі. Відповідний цієї карті граф представлено на рис. 5.4, б.



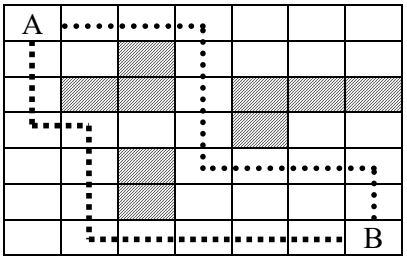
а б

Рисунок 5.4.

Після роботи хвильового алгоритму отримаємо наступні індекси вершин - комірок карти (рис. 5.5, а). На рис. 5.5, б зображено два зі знайдених маршрутів з вершини A у вершину B. Як можна побачити, довжина знайденого маршруту дорівнює 12.

0	1	2	3	4	5	6
1	2		4	5	6	7
2			5			
3	4	5	6		10	11
4	5		7	8	9	10
5	6		8	9	10	11
6	7	8	9	10	11	12

а



б

Рисунок 5.5

Можна зробити процес пошуку найкоротшого маршруту за допомогою хвильового алгоритму більш економнішим, а відтак, й більш швидким. Для цього будемо розповсюджувати хвилю не тільки з початкової вершини A (перша хвиля), а й з кінцевої вершини B (друга хвиля). Для того, щоб відрізняти індекси першої хвилі від другої, індекси останньої будемо

позначати зі штрихом. Робота модифікованого алгоритму закінчується коли обидві хвилі зустрінуться (рис. 5.6).

0	1	2	3	4	5	6
1	2		4	5	6	
2			5			
3	4	5	6/6’		4’	3’
4	5		5’	4’	3’	2’
5	6/6’		4’	3’	2’	1’
6/6’	5’	4’	3’	2’	1’	0’

Рисунок 5.6.

Комірки, де дві хвилі зустрічаються, позначені подвійними лініями. З порівняння рис. 5.5 та 5.6 видно, що знайдені найкоротші маршрути співпадають. І хоча в цьому прикладі економія склала всього лиш одну комірку (яка не була відмічена), можна зрозуміти, що на більш складних, тобто насичених «перепонами» картах, робота модифікованого хвильового алгоритму буде більш ефективнішою за простий хвильовий алгоритм.

СПИСОК РЕКОМЕНДОВАНИХ ТА ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Білак Ю. Ю., Данько-Товтин Л. Я. Системи числення: методичні рекомендації з базової теми дисципліни «Інформатика». Ужгород : ДВНЗ «УжНУ», 2015. 24 с.
2. Борисенко О. А. Дискретна математика: підручник. Суми : Університетська книга, 2023. 255 с.
3. Висоцька В. А., Литвин В. В., Лозинська О. В. Дискретна математика. Практикум : навчальний посібник. Львів: Новий Світ - 2000, 2024. 575 с.
4. Гавриленко О. В., Клименко О. М., Рибачук Л. В. Дискретна математика: навчальний посібник. Київ : КПІ, 2020. 76 с. URL: https://ela.kpi.ua/handle/123456789/38770.
5. Дискретна математика (частина 1): навчальний посібник / уклад. В. М. Пивоварчик, О. М. Яковлєва, О. М. Болдарєва. Одеса: ПНПУ імені К. Д. Ушинського, 2022. 145 с.
6. Дискретна математика : конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти ОПП «Комп'ютерні науки» спеціальності 122 «Комп'ютерні науки» денної форми здобуття вищої освіти / уклад. О. В. Шебаніна, С. І. Тищенко, В. О. Крайній, О. Ю. Пархоменко, І. І. Хилько. Миколаїв: МНАУ, 2023. 162 с. URL: https://dspace.mnau.edu.ua/jspui/handle/123456789/14555
7. Дискретна математика : конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти ОПП «Комп'ютерні науки» спец. 122 «Комп'ютерні науки» денної форми здобуття вищої освіти / уклад. О. Ю. Пархоменко. Миколаїв: МНАУ, 2025. 60 с. https://dspace.mnau.edu.ua/jspui/handle/123456789/22002
8. Дискретна математика : метод. реком. для виконання практ. та індивід. завдань для здобувачів першого (бакалаврського) рівня вищої освіти ОПП «Комп'ютерні науки» спеціальності 122 «Комп'ютерні науки» денної

форми здобуття вищої освіти / уклад. О. Ю. Пархоменко. Миколаїв: МНАУ, 2025. 53 с. https://dspace.mnau.edu.ua/jspui/handle/123456789/22001

9. Дискретна математика : навчальний посібник / уклад. С. І. Балога. Ужгород : АУТДОР-ШАРК, 2021. 124 с. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/42936.

10. Дискретна математика. Збірник індивідуальних завдань: навчальний посібник / уклад. І. Спекторський, О. Стусь, В. Статкевич. Київ : КПІ ім. Ігоря Сікорського, 2022. 88 с. URL: https://ela.kpi.ua/handle/123456789/50767.

11. Ємець О. О., Парфьонова Т. О. Дискретна математика: навчальний посібник для самостійного вивчення навчальної дисципліни студентами денної форми навчання спеціальності 122 Комп'ютерні науки освітня програма «Комп'ютерні науки» ступеня бакалавра. Полтава: ПУЕТ, 2023. 282 с. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi73/0053713.pdf.

12. Кулаковська І. В. Дискретна математика. Частина 1. Множини, відношення та математичні основи крипто графії. Методичні вказівки для виконання лабораторних робіт з дисципліни «Дискретна математика» студентами спеціальностей 121 «Інженерія програмного забезпечення», 122 «Комп'ютерні науки», 124 «Системний аналіз» : методичні вказівки / І. В. Кулаковська. Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2021. 100 с.

13. Ліхоузова Т. А. Дискретна математика. Практикум : навчальний посібник. Київ: КПІ ім. І. Сікорського, 2020. 62 с. URL: https://ela.kpi.ua/handle/123456789/33702

14. Новотарський М. А. Дискретна математика : навчальний посібник. Київ: КПІ, 2020. 278 с.

15. Пивоварчик В. М., Яковлєва О. М., Болдарєва О. М. Дискретна математика (частина 1): навчальний посібник. Одеса, 2022. 145 с. URL: http://dspace.pdpu.edu.ua/jspui/handle/123456789/14760.

16. Порубльов І. М. Дискретна математика: навчальний посібник. Черкаси: ФОП Гордієнко Є. І., 2018. 220 с.

17. Харченко В. М. Практикум з дискретної математики. Ніжин : НДУ ім. М. Гоголя, 2022. 148 с.

18. Сергієнко А. М., Молчанова А. А., Романкевич В. О. Комп'ютерна дискретна математика : навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2022. 189 с. URL: https://ela.kpi.ua/handle/123456789/52232.

19. Темнікова О. Л. Дискретна математика. Частина 1: конспект лекцій. Київ : КПІ ім. І. Сікорського, 2021. 154 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/990893b6-f853-408a-8476-d3dd7c89d2a1/content.

20. Трохимчук Р. М., Нікітченко М. С. Дискретна математика у прикладах і задачах : навч. посібник. Київ : Київський університет, 2017. 248 с.

Навчальне видання

ДИСКРЕТНА МАТЕМАТИКА

Конспект лекцій

Укладачі: **Богатєнкова** Олександра Євгенівна

Формат 60х84 1/16. Ум. друк. арк. 10,06
Тираж 50 прим. Зам. № __

Надруковано у видавничому відділі
Миколаївського національного аграрного університету
54020, м. Миколаїв, вул. Георгія Гонгадзе, 9

Свідоцтво суб'єкта видавничої справи ДК № 4490 від 20.02.2013 р.