Міністерство освіти і науки України
Одеський національний морський університет

КОБОЗЄВА АЛЛА АНАТОЛІЇВНА

СПЕЦІАЛЬНІ РОЗДІЛИ МАТЕМАТИКИ В КІБЕРБЕЗПЕЦІ
частина І

Конспект лекцій

для здобувачів
першого (бакалаврського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Одеса-2025

Розробник: Кобозєва Алла Анатоліївна, доктор технічних наук, професор, завідувач кафедри кібербезпеки та захисту інформації

Конспект лекцій схвалено на засіданні кафедри «Кібербезпека та захист інформації»
(Протокол від «06» жовтня 2025 року №2)

Конспект лекцій схвалено на засіданні НМК ННІ ІТІП
(Протокол від «14» жовтня 2025 року №2)

ЗМІСТ

Тема 1. ПОНЯТТЯ МНОЖИНИ

План

1. Визначення й елементи множини. Скінченні і нескінченні множини.
2. Способи задання множини.
3. Відношення включення. Властивості відношення включення.
4. Основні операції над множинами.
5. Діаграми Вєнна.

1. Визначення й елементи множини. Скінченні і нескінченні множини

Теорія множин як математична дисципліна була створена німецьким математиком Г.Кантором. Множина – основне поняття теорії множин. Згідно з Г.Кантором, *множина* S є будь-яка сукупність певних і таких, що відрізняються між собою, об'єктів нашої інтуїції або інтелекту, яка розглядається як єдине ціле. Ці об'єкти називаються елементами або членами множини S.

Множини, як правило, позначаються великими буквами: A, B, S і т.і., а їх елементи – маленькими: a, b, s і т.і.

Множина називається *скінченною*, якщо вона містить скінченне число елементів, і *нескінченною*, якщо вона містить нескінченне число елементів. Так, множина букв в алфавіті - скінченна, а множина натуральних чисел N - нескінченна.

Для скінченної множини кількість елементів, які містяться в множині, називаються її *потужністю*. Наприклад, потужність множини $X=\{a,b,c,d,e\}$ дорівнює п’ять. Це позначається наступним чином: $|X|=5$. Потужність нескінченної множини дорівнює нескінченності: $|\mathrm{N}|=\infty$.

Якщо деякий елемент a є членом деякої множини A, то будемо писати: $a\in A$. Якщо елемент a не є членом множини A, то будемо писати: $a\notin A$.

Принцип об'ємності: Дві множини A і B рівні в тому і тільки в тому випадку, коли вони складаються з однакових елементів. Позначається: $A=B$.

Таким чином, для того, щоб довести, що $A=B$ треба показати:

1. Якщо $a\in A$, то $a\in B$,
2. Якщо $b\in B$, то $b\in A$.

Приклад. Нехай множина A складається з парних натуральних чисел, а елементами множини B є натуральні числа, які можуть бути представленими у вигляді суми двох непарних натуральних чисел. Довести, що $A=B$.

Доказ:

1. Візьмемо $\forall a\in A$. Це означає, що $a=2n$, де $n\in\mathrm{N}$. Представимо a в еквівалентному вигляді:

$$a=2n=(2n-1)+1. \qquad (1.1)$$

Представлення (1.1) дає вираз для парного натурального числа a в вигляді суми двох натуральних непарних чисел: $(2n-1)$ і 1, а це означає, що $a \in B$.

2. Візьмемо тепер $\forall b \in B$. Для b має місце представлення:

$$b = (2n-1) + (2m-1), \quad n, m \in \mathrm{N}.$$

Перетворимо еквівалентним чином вираз для b:

$$b = (2n-1) + (2m-1) = 2n + 2m - 2 = 2(n+m-1) \qquad (1.2)$$

Представлення числа b в вигляді (1.2) говорить про парність цього числа, а тому $b \in A$. Рівність $A = B$ доведено.

2. Способи визначення множини

Будь-яка множина повністю визначається своїми елементами. Якщо множина скінченна, то її можна задати перерахуванням елементів, що вказуються у фігурних дужках, наприклад, $B = \{1,6,-9,0\}$ (множина B складається із чотирьох елементів: 1, 6, -9, 0. При перерахуванні елементів кожний з них вказується один раз (елементи множини повинні бути різними).

Спосіб перерахування елементів не підійде для того, щоб визначити нескінченну множину. У цьому випадку необхідно задати ***визначальну властивість*** множини: $P(x)$. Загальний вид задання множини з використанням визначальної властивості наступний: $X = \{x \mid P(x)\}$ - множина X складається з таких елементів x, які задовольняють властивості $P(x)$. Необхідно відзначити, що спосіб задання множини за допомогою визначальної властивості може бути використаний не тільки для нескінченних, але й для скінченних множин.

Приклад. Нехай множина B задана наступним чином:

$$B = \{b \mid b = 2n,\ n \in \mathrm{N}\}.$$

Властивість, якій задовольняють елементи цієї множини, говорить про те, що множина є нескінченною і складається з парних натуральних чисел.

3. Відношення включення. Властивості відношення включення

Визначення. Якщо кожний елемент множини A є елементом множини B, то кажуть, що A ***включено в*** B (чи A є ***підмножиною*** B; чи B включає A) і позначають: $A \subseteq B$ чи $B \supseteq A$. Якщо $A \subseteq B$ і при цьому $A \neq B$, то будемо казати, що A ***строго включено*** в B, і позначати: $A \subset B$ $(B \supset A)$.

Приклад.

$$\mathrm{N} \subset \mathrm{Z} \subset Q \subset R,$$

де N - множина натуральних чисел, Z - множина цілих чисел, Q - множина раціональних чисел, R - множина дійсних чисел.

Властивості відношення включення:

1. $\forall X: \quad X \subseteq X$;
2. $\forall X, Y, Z: \quad$ *якщо* $X \subseteq Y$ *і* $Y \subseteq Z$, *то* $X \subseteq Z$;
3. Якщо $X \subseteq Y$ *і* $Y \subseteq X$, *то* $X = Y$.

Із властивості 3 випливає ще один можливий спосіб доказу рівності двох множин: щоб показати, що $X = Y$, надо показати, що $X \subseteq Y$ *і* $Y \subseteq X$.

Для відношення строго включення має місце тільки властивість, аналогічна властивості 2:

$$\forall X, Y, Z: \quad \text{якщо } X \subset Y \text{ і } Y \subset Z, \text{ то } X \subset Z.$$

Необхідно чітко розрізняти відношення приналежності й включення. Так властивості 1 і 2 відношення включення не мають місця для відношення приналежності.

Приклад. $1 \in \mathrm{Z}, \quad \mathrm{Z} \in \{\mathrm{Z}\}$, але $1 \notin \{\mathrm{Z}\}$, оскільки єдиний елемент множини $\{\mathrm{Z}\}$ - це вся множина Z.

Серед усіх множин виділяється своєю унікальністю порожня множина $\varnothing$ - це множина, яка не містить жодного елемента. Порожня множина є підмножиною будь-якої множини: $\forall X: \quad \varnothing \subseteq X$. Дійсно, якщо припустити, що $\varnothing \not\subset X$, то це буде означати, що найдеться хоча б один елемент у множині $\varnothing$, який не належить множині X, але це не так, оскільки в $\varnothing$ взагалі не міститься елементи.

Будь-яка множина $A \neq \varnothing$ має, принаймні, дві різні підмножини: A і $\varnothing$. Більше того, якщо $|A| = n$, то кількість його різних підмножин дорівнює 2^n.

Приклад. Побудувати всі пімножини для множини $A = \{a, b, c, d\}$. Перерахуємо всі підмножини: A, $\varnothing$, $\{a\}$, $\{b\}$, $\{c\}$, $\{d\}$, $\{a, b\}$, $\{a, c\}$, $\{a, d\}, \{b, c\}$, $\{b, d\}$, $\{c, d\}$, $\{a, b, c\}$, $\{a, b, d\}$, $\{a, c, d\}$, $\{b, c, d\}$. Оскільки $|A| = 4$, то, як і очікувалося, їхня кількість визначається $16 = 2^4$.

4. Основні операції над множинами

Визначення. ***Об'єднанням*** множин A і B (позначається $A \cup B$) називається множина, що складається із усіх тих елементів, які належать хоча б одній з множин A, B:

$$A \cup B = \{x \mid x \in A \quad чи \quad x \in B\}.$$

Для будь-яких множин A і B множина $A \cup B$ визначається однозначно.

Приклад. Нехай $A = \{b,c,k\}$, $B = \{k,f,g\}$. Тоді $A \cup B = \{b,c,k,f,g\}$.

Визначення. ***Перерізом*** множин A і B (позначається $A \cap B$) називається множина, що складається із усіх тих і тільки тих елементів, які належать і множині A, і множині B:

$$A \cap B = \{x \mid x \in A \quad і \quad x \in B\}.$$

Для будь-яких множин A і B множина $A \cap B$ визначається однозначно.

Дві множини A і B називаються *непересічними*, якщо $A \cap B = \varnothing$, і *пересічними,* якщо $A \cap B \neq \varnothing$. Так, множини $A = \{b,c,k\}$ і $B = \{k,f,g\}$ є пересічними, оскільки $A \cap B = \{k\} \neq \varnothing$, а множини $A = \{b,c\}$ і $B = \{k,f,g\}$ - непересічними, оскільки не мають однакових елементів.

Для будь-яких множин A і B має місце співвідношення:

$$\varnothing \subseteq (A \cap B) \subseteq A \subseteq (A \cup B).$$

Визначення. ***Абсолютним доповненням*** множини A називається множина (позначається $\overline{A}$), що складається з елементів, що не належать множині A:

$$\overline{A} = \{x \mid x \notin A\}.$$

Визначення. ***Відносним доповненням*** множини A до множини X називається множина (позначається $X - A$ чи $X \setminus A$), що складається з елементів X, які не належать A, тобто

$$X - A = X \cap \overline{A} = \{x \in X \mid x \notin A\}. \qquad (1.3)$$

Визначення. ***Симетричною різницею*** множин A і B (позначається $A + B$) називається множина

$$A + B = (A - B) \cup (B - A). \qquad (1.4)$$

Властивості симетричної різниці:

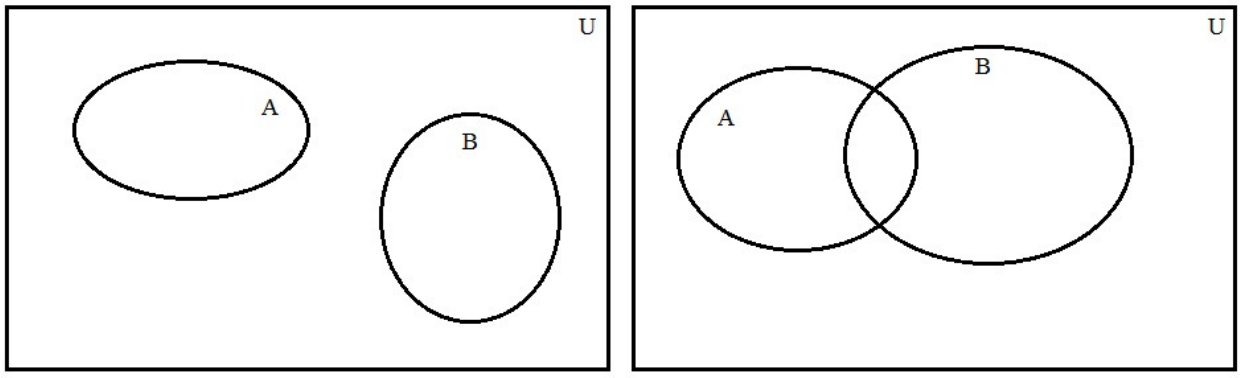
1. $A + B = B + A$;
2. $(A + B) + C = A + (B + C)$;
3. $A + A = \varnothing$; $\varnothing + A = A$.

Якщо всі множини, що розглядаються в ході якогось міркування, є підмножинами деякої множини U, то множина U називається *універсальною* (для цього міркування).

5.Діаграми Вєнна

Діаграми Вєнна - це геометричне представлення множин і операцій над ними. Діаграми Вєнна використовуються для ілюстрації дій над множинами, наведення прикладів результатів операцій над множинами тощо, але **не можуть використовуватися для доказу тверджень**, які є загальними для множин. У діаграмі універсальна множина U представляється прямокутником. Усі розглянуті множини, що є підмножинами U, представляються у вигляді частин побудованого прямокутника, обмежених замкненими кривими. Точки, що лежать усередині різних областей діаграми, розглядаються як елементи відповідних множин. Маючи побудовану діаграму, можна заштрихувати (зафарбувати) певні області для позначення утворених множин.

Приклад. Представити множину $A + B$ за допомогою діаграми Вєнна. У виразі використовуються дві множини A і B, які на діаграмі Вєнна можуть розташовуватися так, як показано на рис.1(а), де множини не перетинаються, або так, як показано на рис.1(б), що відповідає пересічним множинам A і B.



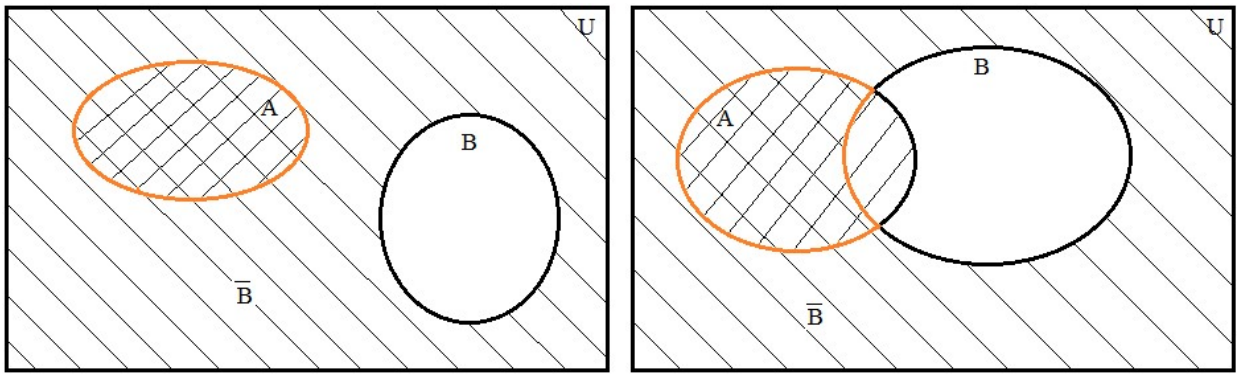
а б

Рисунок 1.

Зі співвідношень (1.4) і (1.3) випливає:

$$A + B = (A - B) \cup (B - A) = \left(A \cap \overline{B}\right) \cup \left(B \cap \overline{A}\right).$$

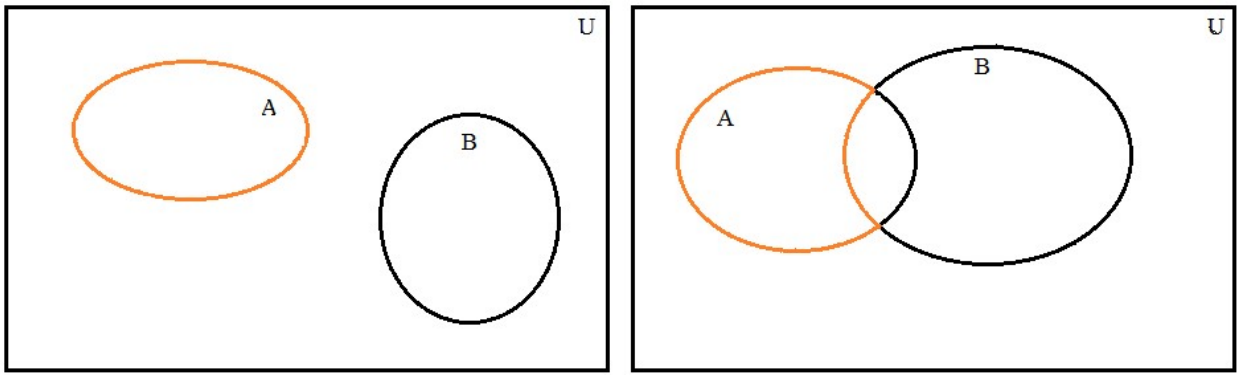
Виділимо на діаграмах (рис.1) множину $A \cap \overline{B}$. Для цього фігуру, що відповідає множині A, заштрихуємо лініями, що складають гострий кут з додатним напрямком осі абсцис, а область, що відповідає $\overline{B}$, лініями, що складають тупий кут з додатним напрямком осі абсцис (рис.2). Частина, що містить штрихування обох типів, є спільною для множин A і $\overline{B}$, тобто відповідає множині $A \cap \overline{B}$ (на рис.2 виділена червоним).



а б

Рисунок 2.

Заберемо з діаграми (рис.2) використане штрихування (рис.3).

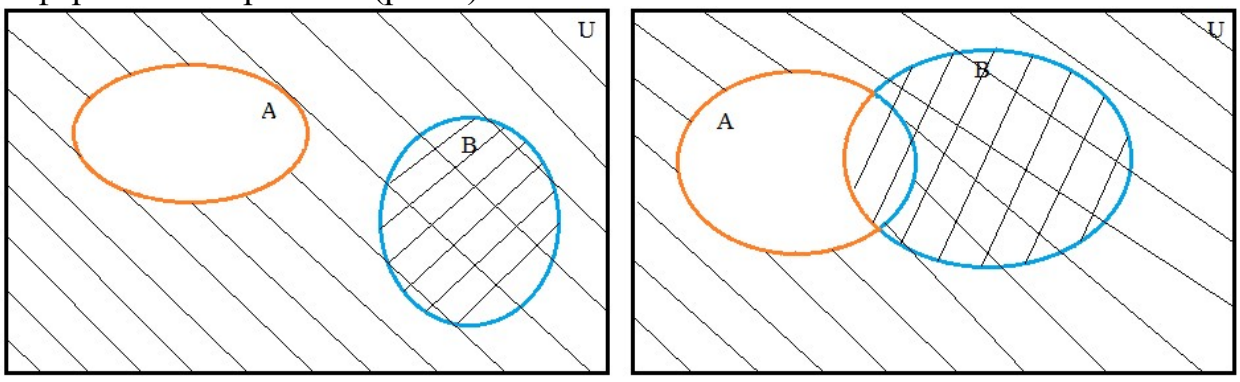


а б

Рисунок 3.

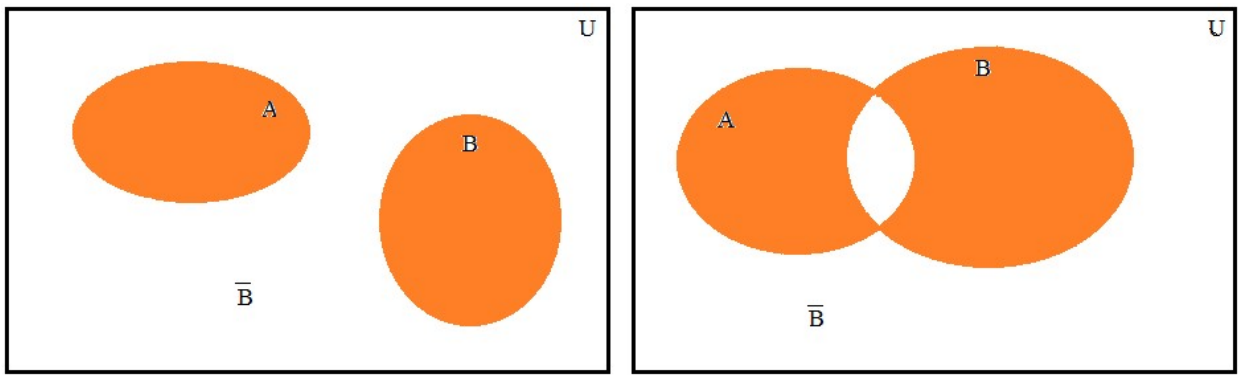
Виділимо на діаграмах (рис.3) множину $B \cap \overline{A}$. Для цього фігуру, що відповідає множині B, заштрихуємо лініями, що складають гострий кут з додатним напрямком осі абсцис, а область, що відповідає $\overline{A}$, лініями, що складають тупий кут з додатним напрямком осі абсцис (рис.4). Частина, що містить штрихування обох типів, є спільною для множин B і $\overline{A}$, тобто відповідає множині $B \cap \overline{A}$ (на рис.4 виділена синім).

Тоді множині $A + B$ на діаграмі Вєнна буде відповідати фігура, зафарбована червоним (рис.5)



а б

Рисунок 4.



а б

Рисунок 5.

Питання

1. Що називається множиною? Навести приклади множин.
2. Яка множина називається скінченною? Навести приклади скінченних множин.
3. Яка множина називається нескінченною? Навести приклади нескінченних множин.
4. Що таке потужність множини? Як визначається потужність нескінченної множини?
5. Які дві множини називаються рівними?
6. Як доводиться рівність множин?
7. Що таке підмножина множини? Скільки підмножин має довільна множина? Навести прикладі.
8. Що таке порожня множина? Чому порожню множину можна розглядати як підмножину будь-якої множини?
9. Яка множина називається перерізом множин A і B? Навести приклади.
10. Яка множина називається об'єднанням множин A і B? Навести приклади.
11. Що таке універсальна множина?
12. Як визначається доповнення множини? Навести приклади.
13. Що таке симетрична різниця множин? Властивості симетричної різниці.
14. Як діаграми Вєнна використовуються в теорії множин?

Тема 2. ВЛАСТИВОСТІ ОПЕРАЦІЙ НАД МНОЖИНАМИ

План

1. Поняття обмеженості множини. Точні верхня й нижня границі обмеженої множини.
2. Асоціативні, комутативні й дистрибутивні закони теорії множин.
3. Закони ідемпотентності, поглинання, закони де Моргана.

1. Поняття обмеженості множини. Точні верхня й нижня границі обмеженої множини

Визначення 1. Множина X називається обмеженою знизу, якщо існує така стала M, що для $\forall x \in X$ виконується: $M \le x$. В цьому випадку M називається нижньою межею множини X.

Визначення 2. Множина X називається обмеженою зверху, якщо існує така стала T, що для $\forall x \in X$ виконується: $T \ge x$. В цьому випадку T називається верхньою межею множини X.

Приклад 1. $X = [3,9]$ - сегмент. $M = 0$ - нижня межа X, оскільки всі елементи $x \in X$ будуть більші за 0. Крім того нижньою межею також можуть бути числа: $M = 3$, $M = -7$, $M = -4.5$. Взагалі будь-яке число, менше або рівне 3, є нижньою межею X, множина X - обмежена знизу. Будь-яке число, яке більше або дорівнює 9, буде верхньою межею X, тому X - множина, яка обмежена зверху.

З розглянутого прикладу зрозуміло: якщо деяка множина обмежене знизу (або зверху), вона має нескінченно багато нижніх (або верхніх) меж.

Приклад 2. Множина натуральних чисел N обмежена знизу, тому що всі натуральні числа більші, наприклад, 0, тобто 0 - це одна з нижніх меж, але N - не обмежена зверху.

Визначення 3. Множина X називається обмеженою, якщо вона обмежена знизу й зверху, тобто існує така стала $P \ge 0$, що для $\forall x \in X$ виконується: $|x| \le P$.

Таким чином, $X = [3,9]$ - обмежена множина, а N - необмежена множина.

Визначення 4. Число A називається точною нижньою межею, або інфімумом множини X і позначається $A = \inf X$, якщо виконуються наступні умови:

1. A - нижня межа X;
2. Для $\forall \varepsilon > 0$ $A + \varepsilon$ вже не буде нижньою межею для X, тобто знайдеться такий елемент $\bar{x} \in X$, що $\bar{x} < A + \varepsilon$.

Таким чином, точна нижня межа - це найбільша з усіх нижніх меж множини, вона визначається однозначно. Так для попередніх прикладів, коли $X = [3,9]$, то $\inf X = 3$, а $\inf N = 1$.

Визначення 5. Число B називається точною верхньою межею, або супремумом множини X і позначається $B = \sup X$, якщо виконуються наступні умови:

1. B - верхня межа X;
2. Для $\forall \varepsilon > 0$ $B - \varepsilon$ вже не буде верхньою межею для X, тобто знайдеться такий елемент $\bar{x} \in X$, що $\bar{x} > B - \varepsilon$.

Таким чином, точна верхня межа - це найменша з усіх верхніх меж множини, вона визначається однозначно. Так для попередніх прикладів, коли $X = [3,9]$, то $\sup X = 9$, а $\sup N$ не існує.

Якщо множина обмежена зверху (знизу), у неї обов'язково існує точна верхня (нижня) межа.

2. Асоціативні, комутативні й дистрибутивні закони теорії множин

Для будь-яких підмножин A, B, C універсальної множини U мають місце наступні властивості ($\bar{A}$ тут розуміється як $U - A$):

1. $A \cup (B \cup C) = (A \cup B) \cup C$	1-а. $A \cap (B \cap C) = (A \cap B) \cap C$
2. $A \cup B = B \cup A$	2-а. $A \cap B = B \cap A$
3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	3-а. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4. $A \cup \varnothing = A$	4-а. $A \cap U = A$
5. $A \cup \bar{A} = U$	5-а. $A \cap \bar{A} = \varnothing$

Закони 1 і 1-а називаються *асоціативними* законами для об'єднання й перерізу.

Закони 2 і 2-а називаються *комутативними* законами; 3 і 3-а - *дистрибутивними* законами для об'єднання й перерізу.

Доведемо для прикладу твердження 3, скориставшись для цього способом доказу, що випливає із принципу об'ємності (лекція 1). Для цього:

1. Візьмемо $\forall x \in A \cup (B \cap C)$ і покажемо, що цей елемент $x \in (A \cup B) \cap (A \cup C)$. Дійсно: якщо $x \in A \cup (B \cap C)$, то $x \in A$ чи $x \in (B \cap C)$. Якщо $x \in A$, то $x \in A \cup B$ і $x \in A \cup C$, але тоді $x \in (A \cup B) \cap (A \cup C)$. Якщо ж $x \in (B \cap C)$, то $x \in B$ і $x \in C$, а тоді $x \in A \cup B$ і $x \in A \cup C$, а тому $x \in (A \cup B) \cap (A \cup C)$.
2. Візьмемо тепер $\forall x \in (A \cup B) \cap (A \cup C)$ і покажемо, що $x \in A \cup (B \cap C)$. Дійсно, якщо $x \in (A \cup B) \cap (A \cup C)$, то $x \in A \cup B$ і $x \in A \cup C$, тому, $x \in A$ чи $x \in B$ і $x \in C$, тобто $x \in A \cup (B \cap C)$.

Згідно із законом 1 об'єднання множин A, B, C можна записувати без дужок: $A \cup B \cup C$. Отриманий висновок можна узагальнити: усі множини, що отримуються за допомогою операції об'єднання із заданих множин $A_1, A_2, ..., A_n$, узятих у фіксованому порядку, рівні одна одній. Будемо позначати таку множину: $A_1 \cup A_2 \cup ... \cup A_n = \bigcup_{i=1}^{n} A_i$.

Аналогічне твердження має місце й для перерізу: $A_1 \cap A_2 \cap ... \cap A_n = \bigcap_{i=1}^{n} A_i$.

Загальні асоціативні закони дозволяють установити загальні комутативні закони: якщо $k_1, k_2, ..., k_n$ - це числа 1,2,…,*n*, які беруться в довільному порядку, то:

$$A_1 \cup A_2 \cup ... \cup A_n = A_{k_1} \cup A_{k_2} \cup ... \cup A_{k_n},$$

$$A_1 \cap A_2 \cap ... \cap A_n = A_{k_1} \cap A_{k_2} \cap ... \cap A_{k_n}.$$

Аналогічно можна сформулювати загальні дистрибутивні закони:

$$A \cup (B_1 \cap B_2 \cap ... \cap B_n) = (A \cup B_1) \cap (A \cup B_2) \cap ... \cap (A \cup B_n)$$

$$A \cap (B_1 \cup B_2 \cup ... \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup ... \cup (A \cap B_n).$$

3. Закони ідемпотентності, поглинання, закони де Моргана

Для будь-яких підмножин A, B універсальної множини U мають місце наступні властивості ($\overline{A}$ тут розуміється як $U - A$):

1. Якщо для $\forall A$ виконується рівність: $A \cup B = A$, то $B = \varnothing$.

1-а. Якщо для $\forall A$ виконується рівність: $A \cap B = A$, то $B = U$.

2. Якщо $A \cup B = U$ і $A \cap B = \varnothing$, то $B = \overline{A}$.

3. $\overline{\overline{A}} = A$.

4. $\overline{U} = \varnothing$.

4-а. $\overline{\varnothing} = U$.

5. $A \cup A = A$

5-а. $A \cap A = A$.

6. $A \cup U = U$

6-а. $A \cap \varnothing = \varnothing$.

7. $A \cup (A \cap B) = A$

7-а. $A \cap (A \cup B) = A$.

8. $\overline{A \cup B} = \overline{A} \cap \overline{B}$

8-а. $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Закони 5 і 5-а називаються законами *ідемпотентності*, 7 і 7-а - закони *поглинання*, 8 і 8-а - закони *де Моргана*.

Закон 2 стверджує, що будь-яка множина має єдине доповнення.

Доведемо для прикладу закон 8. Для цього:

1. Візьмемо довільний елемент $x \in \overline{A \cup B}$ і покажемо, що $x \in \overline{A} \cap \overline{B}$. Дійсно, якщо $x \in \overline{A \cup B}$, то $x \notin A \cup B$, тому, $x \notin A$ і $x \notin B$, а значить $x \in \overline{A}$ і $x \in \overline{B}$, тобто $x \in \overline{A} \cap \overline{B}$.

2. Візьмемо довільний елемент $x \in \overline{A} \cap \overline{B}$ і покажемо, що $x \in \overline{A \cup B}$. Дійсно, якщо $x \in \overline{A} \cap \overline{B}$, то $x \in \overline{A}$ и $x \in \overline{B}$, тому, $x \notin A$ і $x \notin B$, а значить x не може належати $A \cup B$, тобто $x \in \overline{A \cup B}$.

Наступні твердження про довільні множини A, B попарно еквівалентні:

(I) $A \subseteq B$;

(II) $A \bigcap B = A$;

(III) $A \bigcup B = B$.

Питання

1. Які закони об'єднання й перерізу множин називаються комутативними, загальними комутативними?
2. Які закони об'єднання й перерізу множин називаються асоціативними, загальними асоціативними?
3. Які закони об'єднання й перерізу множин називаються дистрибутивними, загальними дистрибутивними?
4. Сформулювати й довести закони де-Моргана.
5. Довести закони поглинання.

Тема 3. БІНАРНІ ВІДНОШЕННЯ

План

4. Бінарне відношення. Область визначення, область значення бінарного відношення. Поняття впорядкованої пари.
5. Декартовий добуток множин. Властивості декартового добутку множин.
6. Матриця бінарного відношення, заданого на скінченній множині.
4. Властивості бінарних відношень

1. Бінарне відношення. Область визначення, область значення бінарного відношення. Поняття впорядкованої пари.

Терміном «відношення» у математиці часто користуються для того, щоб позначити який-небудь зв'язок між предметами, зокрема, елементами множини.

Найчастіше використовуваними є бінарні відношення. Бінарні (двомісні) відношення використовуються для визначення якихось взаємозв'язків, якими характеризуються пари елементів у множині A (на множині людей можуть бути задані, наприклад, наступні бінарні відношення: жити в одному будинку, бути старше, бути матір'ю). Задати відношення, визначене на скінченній множині, можна простим перерахуванням пар елементів, що знаходяться у заданому відношенні.

У загальному випадку при встановленні бінарного відношення для об'єктів важливо, у якому вони беруться порядку. Для ілюстрації розглянемо наступний приклад. Нехай множина членів однієї родини $A = \{M, O, S, D, B\}$, де елементи визначаються наступним чином:

M - мати (35 років);
O - батько (41 рік);
S - син (11 років);
D - донька (7 років);
B - бабуся (60 років).

Між членами родини розглянемо відношення «бути старше». Будемо позначати відношення ρ. Якщо два члени родини перебувають у такому відношенні один до іншого, як, наприклад, O і M (оскільки батько старше матері), то будемо писати $O\rho M$. Зауважимо, що M і O у розглянутому відношенні не знаходяться, тому що не вірно те, що мати старше батька. А тому у розглянутому бінарному відношенні важливий порядок об'єктів: який з них узятий першим, а який другим. Для розглянутої множини отримаємо, що, крім $O\rho M$, мають місце: $O\rho S$, $O\rho D$, $M\rho S$, $M\rho D$, $S\rho D$, $B\rho M$, $B\rho O$, $B\rho S$, $B\rho D$, однак, якщо об'єкти в парах поміняти місцями, то в зазначеному відношенні вони вже перебувати не будуть.

Звичайно бінарне відношення розглядає пари об'єктів, узятих у певному порядку: так звані *впорядковані пари*.

Впорядкованою парою елементів a і b, що позначається як $<a,b>$, називається об'єкт, що має дві властивості:

1. $<a,b>$ однозначно визначається елементами a і b;
2. Якщо існує впорядкована пара $<u,v>$ така, що

$$<a,b>=<u,v>,$$

то $a=u$, $b=v$.

Таким чином, ***бінарне відношення – це множина впорядкованих пар***. Якщо ρ - це деяке відношення, то запис $<u,v>\in\rho$ означає, що $u\ \rho\ v$.

Таким чином, задати відношення «бути старше» на множині $A=\{M,O,S,D,B\}$ з попереднього прикладу можна наступним чином:

$$\rho=\{<B,M>,<B,O>,<B,S>,<B,D>,<O,M>,<O,S>,<O,D>,<M,S>,$$
$$<M,D>,<S,D>\}.$$

У загальному випадку можна розглядати *n*-місні відношення, де якоюсь властивістю пов'язані між собою не пари, а *n*-ки елементів. Тоді *n*-арне відношення – це множина впорядкованих *n*-ок елементів. Наприклад, для *n*=3 на множині всіх студентів ОНПУ можна задати тримісне відношення ρ «жити в одній кімнаті гуртожитку». Тоді множина ρ буде складатися з усіх трійок студентів, кожна з яких проживає в одній кімнаті.

Областю визначення бінарного відношення ρ (позначається далі D_ρ) називається множина:

$$D_\rho=\{x\mid \exists\, y:\ \ <x,y>\in\rho\}.$$

Областю значень бінарного відношення ρ (позначається далі R_ρ) називається множина:

$$R_\rho=\{y\mid \exists\, x:\ \ <x,y>\in\rho\}.$$

2. Декартовий добуток множин. Властивості декартового добутку множин

Прямим (чи декартовим) добутком множин називається множина:

$$X\times Y=\{<x,y>\mid x\in X,\quad y\in Y\}.$$

Деякі властивості декартового добутку аналогічні властивостям добутку чисел:

$$(X_1 \cup X_2) \times Y = (X_1 \times Y) \cup (X_2 \times Y);$$

$$Y \times (X_1 \cup X_2) = (Y \times X_1) \cup (Y \times X_2);$$

$$(X_1 - X_2) \times Y = (X_1 \times Y) - (X_2 \times Y);$$

$$Y \times (X_1 - X_2) = (Y \times X_1) - (Y \times X_2);$$

$$(X_1 \cap X_2) \times Y = (X_1 \times Y) \cap (X_2 \times Y);$$

$$Y \times (X_1 \cap X_2) = (Y \times X_1) \cap (Y \times X_2).$$

Доведемо першу властивість. Для цього треба показати: будь-який елемент множини $(X_1 \cup X_2) \times Y$ є елементом множини $(X_1 \times Y) \cup (X_2 \times Y)$; будь-який елемент множини $(X_1 \times Y) \cup (X_2 \times Y)$ є елементом множини $(X_1 \cup X_2) \times Y$. Дві умови можна об'єднати в одну: якщо елемент належить множині $(X_1 \cup X_2) \times Y$, то це рівносильне тому, що він належить множині $(X_1 \times Y) \cup (X_2 \times Y)$. Для першої властивості маємо:

$$\left(\quad <x,y> \in (X_1 \cup X_2) \times Y \quad \right) \Leftrightarrow \left(\quad x \in X_1 \cup X_2 \quad i \quad y \in Y \quad \right) \Leftrightarrow$$

$$\Leftrightarrow \left(\quad (x \in X_1 \quad чи \quad x \in X_2) \quad и \quad y \in Y \quad \right) \Leftrightarrow$$

$$\Leftrightarrow \left(\quad (x \in X_1 \quad и \quad y \in Y) \quad чи \quad (x \in X_2 \quad и \quad y \in Y) \quad \right) \Leftrightarrow$$

$$\Leftrightarrow \left(\quad <x,y> \in X_1 \times Y \quad чи \quad <x,y> \in X_2 \times Y \quad \right) \Leftrightarrow$$

$$\Leftrightarrow \left(\quad <x,y> \in (X_1 \times Y) \cup (X_2 \times Y) \quad \right),$$

що й було потрібно довести.

Будь-яке бінарне відношення ρ є підмножиною деякого декартового добутку $X \times Y$, такого, що $D_\rho \subseteq X$, $R_\rho \subseteq Y$.

3. Матриця бінарного відношення, заданого на скінченній множині

Задати бінарне відношення на скінченній множині можна не тільки за допомогою перерахування впорядкованих пар, які цьому бінарному відношенню належать, але й за допомогою матриці. Так бінарному

відношенню $\rho \subseteq X \times Y$, де $X = \{x_1, x_2, ..., x_n\}$, $Y = \{y_1, y_2, ..., y_m\}$ ставиться у відповідність прямокутна $n \times m -$матриця C з елементами $c_{ij}, i = 1,2,...,n,\ j = 1,2,...,m$. Елементи c_{ij} визначаються відповідно до формули:

$$c_{ij} = \begin{cases} 1, & якщо \quad x_i \ \rho \ y_j \\ 0 & інакше \end{cases}$$

тобто $c_{ij} = 1$, якщо між x_i і y_j має місце відношення ρ, чи $c_{ij} = 0$, якщо воно відсутнє.

Для прикладу, розглянутого вище, де відношення ρ визначалося як відношення «бути старше» на множині $A = \{M, O, S, D, B\}$, відповідна матриця буде мати вигляд:

ρ	M	O	S	D	B
M	0	0	1	1	0
O	1	0	1	1	0
S	0	0	0	1	0
D	0	0	0	0	0
B	1	1	1	1	0

4. Властивості бінарних відношень

Нехай $\rho \subseteq X \times X$. Це відношення називається:

1. *Рефлексивним*, якщо для $\forall x \in X$: $x\rho x$, тобто кожний елемент множини X пов'язаний відношенням ρ з самим собою. Наприклад, відношення паралельності для прямих на площині є рефлексивним, оскільки кожна пряма паралельна самій собі;
2. *Антирефлексивним,* якщо не існує елемента множини X, пов'язаного відношенням ρ з самим собою. Наприклад, відношення «бути матір'ю», задане на множині людей, є антирефлексивним, оскільки ніяка людина не може бути матір'ю для себе;
3. *Симетричним,* якщо з того, що $x\rho y$ випливає, що $y\rho x$, тобто якщо x знаходиться в відношенні ρ до y, то і y знаходиться в відношенні ρ до x. Наприклад, відношення «вчитися в одному університеті» є симетричним;

4. *Антисиметричним,* якщо для $\forall x, y \in X$ з одночасної істинності $x\rho y$ і $y\rho x$ буде випливати, що $y = x$, тобто ні для яких елементів x і y, що різняться, не виконуються одночасно $x\rho y$ і $y\rho x$. Наприклад, відношення «бути вище» на множині студентів групи;
5. *Транзитивним,* якщо з того, що $x\rho y$ і $y\rho z$ випливає, що $x\rho z$. Наприклад, відношення «бути молодше» на множині людей.

Для бінарного відношення, що має певні властивості, його матриця також має характерні ознаки:

- Для рефлексивного відношення $\rho \subseteq X \times X$ головна діагональ його матриці буде містити тільки одиниці;
- Для антирефлексивного відношення $\rho \subseteq X \times X$ головна діагональ його матриці буде містити тільки нулі;
- Для симетричного відношення $\rho \subseteq X \times X$ його матриця буде симетрична щодо головної діагоналі;
- Для антисиметричного відношення $\rho \subseteq X \times X$ у його матриці будуть відсутні одиниці, симетричні щодо головної діагоналі.

Питання

1. Що називається бінарним відношенням? Навести приклади бінарних відношень.
2. Що таке область визначення, область значення бінарного відношення? Навести приклади.
3. Що таке впорядкована пара елементів?
4. Як визначається декартовий добуток множин?
5. Властивості декартового добутку множин. Довести.
6. Способи завдання бінарного відношення на скінченній множині.
7. Як визначається матриця бінарного відношення?
8. Яке бінарне відношення називається рефлексивним/антирефлексивним? Які особливості мають матриці таких відношень? Навести приклади.
9. Яке бінарне відношення називається симетричним/антисиметричним? Які особливості мають матриці таких відношень? Навести приклади.
10. Яке бінарне відношення називається транзитивним? Навести приклади.

Тема 4. ВІДНОШЕННЯ ЕКВІВАЛЕНТНОСТІ Й ПОРЯДКУ

План

1. Покриття й розбивка множини.
2. Відношення еквівалентності.
3. Відношення порядку.
4. Операції над бінарними відношеннями.

1. Покриття й розбивка множини

Нехай $E = \{E_1, E_2, ...\} = \{E_i\}_{i \in I}$ – деяке сімейство (сукупність) множин.

Сімейство E називається ***покриттям*** множини A, якщо кожний елемент А належить хоча б одній з множин E_i, тобто

$$A \subseteq \bigcup_{i \in I} E_i .$$

Якщо покриття E таке, що його елементи попарно не перетинаються ($E_i \cap E_j = \varnothing, i \neq j$), і всі $E_i \subseteq A$, то таке покриття називається ***розбивкою*** множини А.

Приклад. $A = \{1,2,3\}$. Тоді $E = \{\{1,2\},\{2,3\}\{3,1\}\}$ - покриття, але не розбивка, $E = \{\{1\},\{2\}\{3\}\}$ - розбивка і покриття, $\{\{1\},\{2\}\}$ - не є ні покриттям, ні розбивкою.

Розбивка множини А завжди є його покриттям; покриття не завжди є розбивкою.

Приклад. На рис.1 побудована діаграма Вена для сукупності множин A, B, C, D, E, F, S. Сімейство множин $\{A, B, C, D, E, F\}$ утворює покриття множини S, оскільки $S \subseteq A \cup B \cup C \cup D \cup E \cup F$, але $\{A, B, C, D, E, F\}$ не є розбивкою множини, оскільки можна вказати таку множину з $\{A, B, C, D, E, F\}$, яка не є підмножиною S, наприклад: $A \not\subset S$.

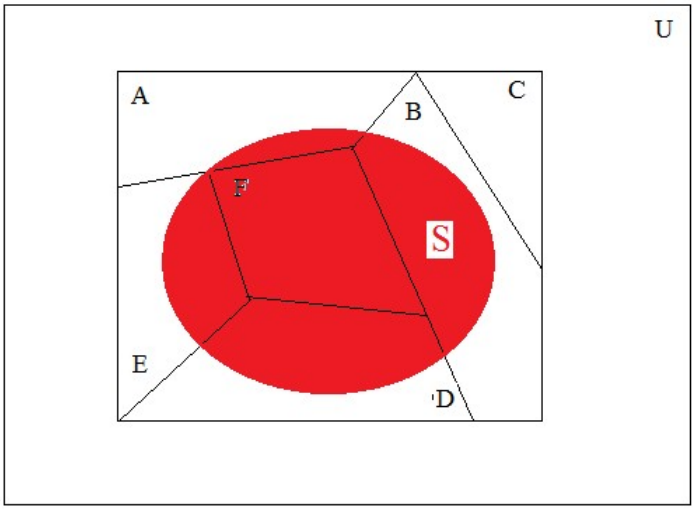


Рис.1.

2. Відношення еквівалентності

Визначення. Нехай задано бінарне відношення $\rho \subseteq X \times X$. Якщо це відношення є одночасно рефлексивним, симетричним і транзитивним, то воно називається *відношенням еквівалентності*.

Приклад. Нехай X - це множина таких дійсних чисел, що $0 \le x < 1$. Відношення ρ має місце між елементами $x, y \in X$ тоді й тільки тоді, коли їх різниця є раціональним числом, тобто коли $(x-y) \in Q$. Таке відношення є рефлексивним, оскільки $<x,x> \in \rho$ для $\forall x \in X\ ((x-x)=0 \in Q)$; є симетричним, оскільки, якщо $(x-y) \in Q$, то $(y-x) = -(x-y) \in Q$, тобто якщо $<x,y> \in \rho$, то і $<y,x> \in \rho$; транзитивним, оскільки, якщо $(x-y) \in Q$ і $(y-z) \in Q$, то $(x-z) = (x-y+y-z) = (x-y)+(y-z) \in Q$, тобто з того, що $<x,y> \in \rho$ і $<y,z> \in \rho$, випливає, що $<x,z> \in \rho$. Таким чином, розглянуте відношення є відношенням еквівалентності.

Приклад. Відношення рівносильності, задане на множині формул, є відношенням еквівалентності.

Приклад. Відношення «проживання в одному будинку» на множині жителів міста Одеса є відношенням еквівалентності.

Якщо бінарне відношення $\rho \subseteq X \times X$ є відношенням еквівалентності, воно розбиває множину X на непересічні підмножини так, що елементи одної підмножини знаходяться у відношенні ρ, а між елементами з різних підмножин відношення ρ не має місця. Отримані підмножини утворюють розбивку множини X і називаються *класами еквівалентності*.

Для останнього прикладу кожний клас еквівалентності буде містити жителів одного конкретного будинку.

Теорема. Якщо множина X розбита на непересічні підмножини, об'єднання яких дає множину X, то відношення «бути в одній підмножині» є відношенням еквівалентності. Усяке відношення еквівалентності виходить описаним способом з деякої розбивки.

Скільки різних відношень еквівалентності можна задати на множині $X = \{1,2,3\}$? Кількість різних відношень еквівалентності визначиться кількістю різних розбивок множини: $\{1,2,3\}$, $\{\{1\},\{2\},\{3\}\}$, $\{\{1,2\},\{3\}\}$, $\{\{1,3\},\{2\}\}$, $\{\{1\},\{2,3\}\}$

3. Відношення порядку

Визначення. Бінарне відношення $\rho \subseteq X \times X$ називається відношенням *нестрогого порядку*, якщо воно є одночасно рефлексивним, антисиметричним і транзитивним.

Визначення. Бінарне відношення $\rho \subseteq X \times X$ називається відношенням *строгого порядку*, якщо воно є одночасно антирефлексивним, антисиметричним і транзитивним.

Відношення нестрогого й строгого порядку разом називаються *відношеннями порядку*.

Приклади бінарних відношень нестрого порядку: «бути не старше» на множині людей, «бути не більше» на множині дійсних чисел.

Приклади бінарних відношень строго порядку: «бути старше» на множині людей, «бути більше» на множині дійсних чисел.

Нехай $\rho \subseteq X \times X$ - відношення порядку. Елементи $x, y \in X$ називаються *порівнянними* по відношенню порядку ρ на множині X, якщо виконується $x \rho y$ чи $y \rho x$.

Множина X, на якій задано відношення порядку ρ, може бути:

- *Повністю впорядкованою множиною*, якщо будь-які $x, y \in X$ порівнянні по відношенню порядку ρ. У такому випадку говорять, що відношення ρ задає повний порядок на множині X. Наприклад, відношення «бути молодше» задає повний порядок на множині всіх людей;
- *Частково впорядкованою множиною*, якщо існує $x, y \in X$, які не порівнянні по відношенню порядку ρ. У такому випадку говорять, що відношення ρ задає частковий порядок на множині X. Наприклад, відношення «бути начальником» задає частковий порядок на множині співробітників деякої організації.

На множині $R \times R$ усіх пар дійсних чисел можна ввести частковий порядок, вважаючи, що $\langle x1, x2 \rangle \le \langle y1, y2 \rangle$, якщо $x1 \le x2$ і $y1 \le y2$. Цей порядок уже не буде повним: пари $\langle 0,1 \rangle$ і $\langle 1,0 \rangle$ не порівнянні.

4. Операції над бінарними відношеннями

Оскільки бінарні відношення визначаються як деякі множини впорядкованих пар ($\rho \subseteq X \times X$ чи $\rho \subseteq X \times Y$), то для них можна визначити ті ж операції, що й над іншими множинами.

1. *Об'єднанням* бінарних відношень ρ_1 і ρ_2 називається таке бінарне відношення ρ, для якого має місце співвідношення:
$$\rho = \rho_1 \cup \rho_2 = \{ < x, y > \mid < x, y > \in \rho_1 \quad \textit{чи} \quad < x, y > \in \rho_2 \}$$
2. *Перерізом* бінарних відношень ρ_1 і ρ_2 називається таке бінарне відношення ρ, для якого має місце співвідношення:
$$\rho = \rho_1 \cap \rho_2 = \{ < x, y > \mid < x, y > \in \rho_1 \quad i \quad < x, y > \in \rho_2 \}$$
3. *Різницею* бінарних відношень ρ_1 і ρ_2 називається таке бінарне відношення ρ, для якого має місце співвідношення:
$$\rho = \rho_1 \setminus \rho_2 = \{ < x, y > \mid < x, y > \in \rho_1 \quad i \quad < x, y > \notin \rho_2 \}$$
4. *Доповненням* бінарного відношення ρ_1 називається таке бінарне відношення ρ, для якого має місце співвідношення:

$\rho = \overline{\rho}_1 = \{< x, y > \mid < x, y > \in U \quad i \quad < x, y > \notin \rho_1\}$, де $U = X \times X$ (якщо $\rho_1 \subseteq X \times X$) чи $U = X \times Y$ (якщо $\rho_1 \subseteq X \times Y$)

5. *Зворотним* відношенням до бінарного відношення ρ_1 називається таке бінарне відношення ρ, для якого має місце співвідношення:

$$\rho = \rho_1^{-1} = \{< x, y > \mid < y, x > \in \rho_1\}.$$

Приклад. Нехай ρ - бінарне відношення «бути керівником», яке визначено на множині X співробітників деякої організації. Тоді бінарні відношення $\overline{\rho}$, ρ^{-1} мають наступний сенс:

$\overline{\rho}$ - «не бути керівником»

ρ^{-1} - «бути підлеглим».

Згадані відношення мають властивості, відображені в таблиці 1.

Таблиця 1.

Відношення	Рефлексивне	Антирефлексивне	Симетричне	Антисиметричне	Транзитивне
ρ	-	+	-	+	+
$\overline{\rho}$	+	-	-	-	-
ρ^{-1}	-	+	-	+	+

Питання

1. Що таке покриття множини? Навести приклади.
2. Чи для будь-якої множини можна побудувати покриття? Відповідь обгрунтувати.
3. Чим покриття множини відрізняється від розбивки цієї множини? Навести приклади.
4. Чи завжди покриття множини є її розбивкою?
5. Чи може покриття множини бути її розбивкою?
6. Чи завжди розбивка множини є її покриттям?
7. Яке бінарне відношення називається відношенням еквівалентності? Навести приклади відношень еквівалентності.
8. Яке бінарне відношення називається відношення нестрогого/строгого порядку? Навести приклади.
9. Яка множина називається повністю впорядкованою? Навести приклади.
10. Яка множина називається частково впорядкованою? Навести приклади.
11. Які операції над бінарними відношеннями можна визначити?

Тема 5. ОСНОВНІ ПОНЯТТЯ МАТЕМАТИЧНОЇ ЛОГІКИ

План

1. Поняття висловлення. Прості й складені висловлення
2. Основні логічні операції. Пріоритет логічних операцій
3. Логічні функції. Поняття таблиці істинності

1. Поняття висловлення. Прості й складені висловлення

Основним об'єктом традиційних розділів логіки є висловлення.

Визначення. *Висловлення* – це розповідне речення, щодо якого точно можна сказати, що воно або істинне, або хибне. Висловлення не може бути одночасно істинним і хибним.

Усі наукові знання, події повсякденного життя, ситуації, що виникають у процесах керування, формулюються у вигляді висловлень.

Приклади висловлень:

1. «Згідно із Законом України « Про захист персональних даних», який регулює правові відносини, пов'язані із захистом і обробкою персональних даних, в органах державної влади й органах місцевого самоврядування, організаціях, установах, на підприємствах усіх форм власності в обов'язковому порядку організують відділ або призначається відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних при їхній обробці й зберіганні» - це розповідне речення є істинним. Це висловлення.

2. «Людина - безсмертна» - це розповідне речення, воно є хибним. Це висловлення.

Для того, щоб оперувати розповідними реченнями як висловленнями, ми повинні знати про кожне з них, істинно воно або хибне. Необхідно відзначити, що в ряді випадків істинність або хибність висловлення залежить від того, яку конкретну реальність ми намагаємося з його допомогою описати. Наприклад, істинність або хибність речення «У понеділок був дощ» залежить від того, про який саме понеділок мова йде, однак для кожного конкретного понеділка це висловлення обов'язкове або істинно, або хибне. У такому випадку говорять, що дане висловлення істинне або хибне в даній інтерпретації (контексті).

Скрізь далі будемо припускати, що контекст заданий і висловлення має певне істиносне значення. Це дозволяє відволіктися від безпосереднього змісту висловлення й обмежитися тільки тою його властивістю, що воно є або ІСТИНОЮ, або НЕПРАВДОЮ.

Будемо позначати висловлення: $A, B, C, \ldots$.

Будемо називати висловлення *простим* (або *елементарним*), якщо воно розглядається як якесь неподільне ціле (аналогічно елементу множини). Зазвичай до них відносять висловлення, що не містять логічних зв'язок (І, ЧИ, ЯКЩО...ТО, та ін).

З існуючих елементарних висловлень за допомогою логічних зв'язок, які в природній мові визначаються союзами «І», «АБО», часткою «НЕ»,

словосполученнями «ЯКЩО…. ТО……», «АБО…..АБО….», «ТОДІ Й ТІЛЬКИ ТОДІ, КОЛИ….» та ін., формуються нові висловлення - *складені* (або *складні*). Наприклад, «Я поступив в Одеський політех **І** моя майбутня спеціальність - це програмна інженерія»; «На підприємстві буде створений відділ, що займається захистом персональних даних при їхній обробці й зберіганні **АБО** на підприємстві буде призначена відповідальна особа, що займається захистом персональних даних при їхній обробці й зберіганні».

2. Основні логічні операції. Пріоритет логічних операцій

Визначимо перераховані зв'язки формально, беручи до уваги тільки те, що кожне висловлення визначається тільки своїм істиносним значенням: НЕПРАВДА або ІСТИНА:

1. *Кон'юнкцією* (операцією логічного «І», логічним добутком) двох висловлень A, B називається висловлення, яке позначається $A \& B$ чи $A \wedge B$, чи AB (читається: A **і** B) і є істинним, коли оба висловлення A, B істинні, і хибним в усіх інших випадках (тобто: коли A - істинне, а B - хибне; коли A - хибне, а B - істинне; коли A - хибне і B - хибне); Наприклад, висловлення ***C***: «Завтра я піду в кіно з Ігорем **І** Мишею» буде істинним тільки тоді, коли будуть окремо істинними висловлення ***A***:«Завтра я піду в кіно з Ігорем», ***B***: «Завтра я піду в кіно з Мишею», кон'юнкція яких і привела до висловлення ***C***. Хибність хоча б одного зі складових ***A*** або ***B*** приведе до хибності ***C***.
2. *Диз'юнкцією* (операцією логічного «АБО», логичної суми) двох висловлень A, B називається висловлення, яке позначається $A \vee B$ (читається: A або B) і є хибним, коли обидва висловлення A, B хибні, і істинним в усіх інших випадках (тобто: коли A - істинне, а B - хибне; коли A - хибне, а B - істинне; коли A - істинне, і B - істинне). Наприклад, висловлення ***C***: «Завтра я піду в кіно з Ігорем **АБО** Мишею» буде істинним, якщо буде істинним хоча б одне з висловлень ***A***: «Завтра я піду в кіно з Ігорем», В: «Завтра я піду в кіно з Мишею», диз'юнкція яких і привела до висловлення ***C***.
3. *Запереченням* (інверсією) висловлення A називається висловлення, яке є істинним, коли висловлення A хибне, і хибним – інакше. Позначення: $\overline{A}$. Читається: не A; не вірно, що A.
4. *Імплікацією* двох висловлень A, B називається висловлення, яке позначається $A \to B$ (читається: якщо A, то B; з A випливає B; A тягне B), яке хибне тільки в тому випадку, коли A істинне, а B хибне. В усіх інших випадках $A \to B$ істинне. Висловлення A називається *посилкою* імплікації, а висловлення B - *висновком*.

5. *Еквівалентністю* (рівнозначністю) двох висловлень A, B називається висловлення, істинне, коли істинісні значення A і B співпадають, і хибне в протилежному випадку. Позначення: $A \leftrightarrow B$. Читається: A еквівалентно B; A тоді й тільки тоді, коли B.
6. *Виключним «АБО»* (чи додаванням по модулю 2) двох висловлень A, B називається висловлення, істинне, коли істинісні значення A і B не співпадають, і хибне в протилежному випадку. Позначення: $A \oplus B$. Читається: або A, або B. Розуміється - у розділовому сенсі.

Усі перераховані операції 1-6 називаються логічними операціями. Всяке висловлення, складене з деяких вхідних висловлень за допомогою застосування логічних операцій 1-6, будемо називати формулою алгебри висловлень. Наприклад, формулою є: $(A \leftrightarrow B)\& C$, $A \vee B \to C \& D$.

Логічні операції мають певний пріоритет друг відносно друга (у відсутності дужок, які задають цей пріоритет явно):

1. Заперечення;
2. Кон'юнкція;
3. Диз'юнкція;
4. Імплікація і еквівалентність.

Наприклад, в формулі $A \vee B \to C \& D$ першою виконається операція $C \& D$, другою - $A \vee B$, а імплікація буде третьою. Однак, якщо в цій же формулі поставити дужки, то порядок операцій можна змінити: для $(A \vee (B \to C))\& D$ першою буде виконана імплікація $B \to C$, потім диз'юнкція $A \vee (B \to C)$, а лише останньою – кон'юнкція.

3. Логічні функції. Поняття таблиці істинності

Вхідні висловлення можуть бути постійними, тобто мати певні значення: ІСТИНА або НЕПРАВДА, а можуть не мати конкретного фіксованого значення (про них відомо лише, що вони можуть приймати значення: ІСТИНА або НЕПРАВДА). Перші висловлення будемо називати постійними елементарними висловленнями, другі - змінними елементарними висловленнями.

Приклад. Записати логічними формулами наступні два висловлення:

1. «Якщо мало працюєш над домашнім завданням і при цьому займаєшся не систематично, то приходиш на заняття непідготовленим або шукаєш поважну причину для пропуску занять». Дане складне висловлення складається з декількох простих:

A - «Мало працюєш над домашнім завданням»;

B - «Займаєшся не систематично»;

C - «Приходиш на заняття непідготовленим»;

D - «Шукаєш поважну причину для пропуску занять».

З урахуванням введених позначень для простих висловлень і визначених вище логічних операцій складне висловлення може бути представлено символьно у вигляді наступної логічної формули:

$$(A \,\&\, B) \to (C \vee D). \qquad (1)$$

2. «Якщо аналіз системи захисту інформації банку показує, що вона є неефективною й при цьому дорогою, то начальник відділу інформаційної безпеки повинен буде звільнений або, у найкращому разі, одержати догану». Дане складне висловлення складається з декількох простих:

A - «Аналіз системи захисту інформації банку показує, що вона є неефективною»;

B - «Аналіз системи захисту інформації банку показує, що вона є дорогою»;

C - «Начальник відділу інформаційної безпеки повинен буде звільнений»;

D - «Начальник відділу інформаційної безпеки одержить догану».

З урахуванням введених позначень для простих висловлень і визначених вище логічних операцій складне висловлення може бути представлено символьно у вигляді наступної логічної формули:

$$(A \,\&\, B) \to (C \vee D). \qquad (2)$$

При порівнянні (1) і (2) видно, що обидва складних висловлення описуються однією логічною формулою, хоча мають різний зміст (символи елементарних висловлень A, B, C, D змістовно інтерпретуються по-різному). У математичній логіці вивчається будова складних логічних висловлень, виражених формулами, незалежно від змісту простих висловлень, що їх складають. Тому два висловлення, наведені в прикладі, логічно не розрізняються. Істинісні значення цих і інших складних висловлень, що описуються даною логічною формулою $(A \,\&\, B) \to (C \vee D)$, будуть визначатися тільки тим, істинне або хибне кожне вхідне в них висловлення A, B, C, D. Оскільки кожне із цих висловлень може бути або істинним, або хибним, тобто мати одне із двох значень, то кількість різних комбінацій значень для четвірки A, B, C, D - 2^4. При цьому змістовних інтерпретацій цієї формули, очевидно, нескінченно багато.

Далі для простоти й зручності будемо позначати «ІСТИНУ» за допомогою «1», а «НЕПРАВДУ» - за допомогою «0».

Із усього вищесказаного випливає, що будь-яка формула алгебри висловлень визначає деяку функцію, аргументами якої є змінні елементарні висловлення. При цьому й аргументи, і сама функція можуть приймати тільки два значення: 0 і 1. Така функція, яку далі будемо називати логічною, може бути повністю описана скінченною таблицею, яка називається

таблицею істинності. Наприклад, таблиця істинності для формули $A \& B$ має вигляд:

A	B	$A \& B$
0	0	0
0	1	0
1	0	0
1	1	1

Останній елемент кожного рядка таблиці дає значення формули при тих значеннях аргументів, що входять у неї, які знаходяться у перших двох позиціях рядка.

Якщо формула має більш складний вид, то при побудові таблиці стовпці формуються з урахуванням зручності обчислень. Наприклад, для формули $(A \& B) \to (C \vee D)$ зручним буде спочатку обчислити значення $A \& B$, $C \vee D$ при всіляких значеннях вхідних у них змінних, а потім уже значення $(A \& B) \to (C \vee D)$. Відповідна таблиця буде мати 2^4 рядків.

A	B	C	D	$A \& B$	$C \vee D$	$(A \& B) \to (C \vee D)$
0	0	0	0	0	0	1
0	0	0	1	0	1	1
0	0	1	0	0	1	1
0	0	1	1	0	1	1
0	1	0	0	0	0	1
0	1	0	1	0	1	1
0	1	1	0	0	1	1
0	1	1	1	0	1	1
1	0	0	0	0	0	1
1	0	0	1	0	1	1
1	0	1	0	0	1	1
1	0	1	1	0	1	1
1	1	0	0	1	0	0
1	1	0	1	1	1	1
1	1	1	0	1	1	1
1	1	1	1	1	1	1

З останньої таблиці явно видно, що висловлення, представлене логічною формулою $(A \& B) \to (C \vee D)$, буде хибним тільки в одному випадку: коли висловлення A і B - істинні, а висловлення C і D - хибні.

Питання

1. Що називається висловленням? Навести приклади висловлень.
2. Чи може висловлення бути одночасно істинним і хибним?

3. Яке висловлення називається простим (елементарним)? Навести приклади.
4. Яке висловлення називається складним? Навести приклади.
5. Що таке постійне й змінне висловлення?
6. Перерахувати логічні операції. Коли значення кожної з перерахованих операцій дорівнює 1? Дорівнює 0?
7. Пріоритет логічних операцій. Для чого в логічних формулах використовуються дужки?
8. Чи може одна логічна формула відповідати різним за змістом висловленням?
9. Яка функція називається логічною?
10. Що таке таблиця істинності логічної формули? Навести приклади побудови таблиць істинності.

Тема 6. РІВНОСИЛЬНІ ФОРМУЛИ АЛГЕБРИ ЛОГІКИ

План

1. Рівносильні логічні формули.
2. Проблема розв'язності.
3. Нормальні форми.

1. Рівносильні логічні формули

Дві формулі U_1 і U_2 називаються рівносильними, якщо при будь-яких значеннях $X_1, X_2, \ldots, X_n$, де $X_1, X_2, \ldots, X_n$ - це сукупність усіх змінних, що входять в U_1 і U_2, ці формули приймають однакові значення. Наприклад, $\overline{\overline{A}}$ рівносильна A, $A \& \overline{A} \vee B$ рівносильна B.

Рівносильність логічних формул може бути встановлена шляхом побудови таблиць істинності для кожної з них: якщо таблиці містять однакові значення в стовпцях для результуючих формул при однакових значеннях усіх вхідних у формули змінних, то формули рівносильні.

Приклади рівносильних формул:

$\overline{\overline{X}}$	рівносильна	X	(1)
$X \& Y$	рівносильна	$Y \& X$	(2)
$(X \& Y) \& Z$	рівносильна	$X \& (Y \& Z)$	(3)
$X \vee Y$	рівносильна	$Y \vee X$	(4)
$(X \vee Y) \vee Z$	рівносильна	$X \vee (Y \vee Z)$	(5)
$X \& (Y \vee Z)$	рівносильна	$X \& Y \vee X \& Z$	(6) - I
$X \vee (Y \& Z)$	рівносильна	$(X \vee Y) \& (X \vee Z)$	(7) -II
$X \vee (X \& Y)$	рівносильна	X	(8)
$X \& (X \vee Y)$	рівносильна	X	(9)
$\overline{X \vee Y}$	рівносильна	$\overline{X} \& \overline{Y}$	(10)
$\overline{X \& Y}$	рівносильна	$\overline{X} \vee \overline{Y}$	(11)
$X \vee X$	рівносильна	X	(12)
$X \vee \overline{X}$	рівносильна	1	(13)
$X \& X$	рівносильна	X	(14)
$X \& \overline{X}$	рівносильна	0	(15)
$X \& 1$	рівносильна	X	(16)
$X \vee 0$	рівносильна	X	(17)

Формули (6) і (7) називаються відповідно першим і другим дистрибутивними законами.

Доведемо рівносильність (10) за допомогою таблиць істинності:

X	Y	$X \vee Y$	$\overline{X \vee Y}$
0	0	0	1
0	1	1	0
1	0	1	0
1	1	1	0

X	Y	$\overline{X}$	$\overline{Y}$	$\overline{X} \& \overline{Y}$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	0	0	0

Порівняння таблиць істинності говорить про рівносильність формул $\overline{X \vee Y}$ і $\overline{X} \& \overline{Y}$ (одним кольором у таблицях зафарбовані відповідні рядки).

Логічні операції $\&, \vee, \rightarrow, \leftrightarrow, \bar{}$ не є незалежними. Дійсно,

$$X \rightarrow Y = \overline{X} \vee Y \tag{18}$$

$$X \leftrightarrow Y = (X \rightarrow Y) \& (Y \rightarrow X) = (\overline{X} \vee Y) \& (\overline{Y} \vee X) \tag{19}$$

Доведемо формулу (18) за допомогою таблиці істинності:

X	Y	$X \rightarrow Y$	$\overline{X}$	$\overline{X} \vee Y$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

Співпадіння виділених у таблиці стовпців доводить рівносильність (18). Для формули (19) зробимо аналогічним чином:

X	Y	$X \leftrightarrow Y$	$\overline{X}$	$\overline{X} \vee Y$	$\overline{Y}$	$\overline{Y} \vee X$	$(\overline{X} \vee Y) \& (\overline{Y} \vee X)$
0	0	1	1	1	1	1	1
0	1	0	1	1	0	0	0
1	0	0	0	0	1	1	0
1	1	1	0	1	0	1	1

Співпадіння виділених у таблиці стовпців доводить рівносильність (19).

Таким чином, для запису будь-якої логічної формули замість набору $\&, \vee, \rightarrow, \leftrightarrow, \bar{}$, що складається з 5-ти логічних операцій, можна завжди скористатися тільки трьома: $\&, \vee, \bar{}$.

Кількість операцій, через які виражаються всі інші, можна зменшити до двох. Ці пари: $\&, \bar{}$ чи $\vee, \bar{}$. Дійсно, враховуючи рівносильні формули (1) – (17), отримуємо:

$$X \vee Y \overset{\text{формула (1)}}{=} \overline{\overline{X}} \vee \overline{\overline{Y}} \overset{\text{формула (11)}}{=} \overline{\overline{X} \& \overline{Y}},$$

тобто диз'юнкція виражається через заперечення й кон'юнкцію, а тому усі основні логічні операції можна виразити тільки через $\&, \bar{}$.

Аналогічно, оскільки має місце

$$X \,\&\, Y \overset{\text{формула (1)}}{=} \overline{\overline{X} \,\&\, \overline{Y}} \overset{\text{формула (10)}}{=} \overline{\overline{X} \vee \overline{Y}},$$

тобто кон'юнкція виражається через заперечення і диз'юнкцію, то усі основні логічні операції можна виразити тільки через $\vee, \bar{}$.

2. Проблема розв'язності

Логічна формула називається ***тотожно істинною***, якщо вона при всіх значеннях вхідних у неї змінних висловлень приймає значення 1.

Приклад: $\overline{X} \vee X = 1$ при будь-яких значеннях X.

Логічна формула називається ***здійсненною***, якщо існує хоча б один такий набір значень вхідних у неї змінних висловлень, на якому вона приймає значення 1.

Приклад: $X \to Y = 1$, коли $X = 1$, $Y = 1$. Оскільки ми змогли вказати такий набір значень змінних X, Y, на якому формула $X \to Y$ істинна, то вона здійсненна.

Логічна формула називається ***нездійсненною***, або ***тотожно хибною***, якщо вона при будь-яких значеннях вхідних у неї змінних висловлень приймає значення 0.

Приклад. $\overline{X} \,\&\, X = 0$ при будь-яких значеннях X, тому формула $\overline{X} \,\&\, X$ є тотожно хибною.

Для формули логіки часто вирішується задача про те, чи є вона тотожно істинною. Така задача в класичній логіці називається проблемою розв'язності. Найпростіший спосіб для розв'язку такої задачі: побудова таблиці істинності формули й аналіз стовпця значень формули (чи є в цьому стовпці нулі).

3.Нормальні форми

Елементарним добутком називається кон'юнкція (добуток) змінних і/або їх заперечень. При цьому вхідні в елементарний добуток змінні або їх заперечення будуть називатися множниками.

Приклад. $\overline{X} \,\&\, X$, $\overline{X} \,\&\, Y \,\&\, Z \,\&\, \overline{T}$. Для останньої формули $\overline{X}, Y, Z, \overline{T}$ - множники.

Елементарною сумою називається диз'юнкція (сума) змінних і/або їх заперечень. При цьому вхідні в елементарну суму змінні або їх заперечення будуть називатися доданками.

Приклад. $\overline{X} \vee X$, $\overline{X} \vee Y \vee Z$. Для останньої формули $\overline{X}, Y, Z$ - доданки.

Теорема. Щоб елементарна сума була тотожно істинною, необхідно й достатньо, щоб у ній була хоча б одна пара доданків, з яких один є деякою змінною, а інший - її запереченням.

Доказ.

Достатність. Нехай є елементарна сума, у складі якої є пари доданків, з яких один є деякою змінною, а інший - її запереченням, тобто формула виглядає наступним чином: $A \vee ... \vee \underbrace{\overline{X} \vee X} \vee ... \vee Z$. Частина цієї формули, позначена фігурною дужкою, дорівнює 1, у силу чого вся сума буде істинною при будь-яких значення змінних, які входять у неї.

Необхідність. Припустимо, що елементарна сума є тотожно істинною, але не містить ні одної пари доданків, з яких один є деякою змінною, а інший - її запереченням, тобто доданків виду $\overline{X} \vee X$. Тоді кожній змінній, що не знаходиться під знаком заперечення, можна дати значення 0, а кожній змінній, що стоїть під знаком заперечення - 1. У цьому випадку вся сума виявиться рівною 0, що суперечить її тотожній істинності.

Теорема. Щоб елементарний добуток був тотожно хибним, необхідно й достатньо, щоб у ньому містилася хоча б одна пара множників, з яких один є деякою змінною, а інший - її запереченням.

Доказ самостійно.

Визначення. Логічна формула, рівносильна даній формулі, що представляє собою суму елементарних добутків, називається ***диз'юнктивною нормальною формою*** (ДНФ) даної формули.

Для кожної логічної формули існує ДНФ, яка отримується з використанням I дистрибутивного закону.

Визначення. Логічна формула, рівносильна даній формулі, що представляє собою добуток елементарних сум, називається ***кон'юнктивною нормальною формою*** (КНФ) даної формули.

Для кожної логічної формули існує КНФ, яка отримується з використанням II дистрибутивного закону.

Приклад. Знайти КНФ і ДНФ для формули $\overline{X \vee Y} \leftrightarrow X \,\&\, Y$. Для розв'язку поставленого завдання, у першу чергу, перетворимо дану формулу в рівносильну, що використовує тільки ті три логічні операції, які фігурують у ДНФ і КНФ: $\&, \vee, \bar{}$:

$$\overline{X \vee Y} \leftrightarrow X \,\&\, Y \overset{\text{формула (19)}}{=} \left(\overline{X \vee Y} \rightarrow X \,\&\, Y\right) \& \left(X \,\&\, Y \rightarrow \overline{X \vee Y}\right) \overset{\text{формула (18)}}{=}$$

$$= \left(\overline{\overline{X \vee Y}} \vee X \,\&\, Y\right) \& \left(\overline{X \,\&\, Y} \vee \overline{X \vee Y}\right) \overset{\text{формула (1)}}{=} \left(X \vee Y \vee X \,\&\, Y\right) \& \left(\overline{X \,\&\, Y} \vee \overline{X \vee Y}\right)$$

Оскільки в КНФ і ДНФ знак заперечення може бути тільки над змінною, то скористаємося далі для рівносильних перетворень (10) і (11):

$$(X \vee Y \vee X \,\&\, Y) \,\&\, \left(\overline{X \,\&\, Y} \vee \overline{X \vee Y}\right) = (X \vee Y \vee X \,\&\, Y) \,\&\, \left(\overline{X} \vee \overline{Y} \vee \overline{X} \,\&\, \overline{Y}\right) \overset{(8)}{=}$$

$$= (X \vee Y) \,\&\, \left(\overline{X} \vee \overline{Y}\right)$$

Отримана в результаті формула є добутком елементарних сум, тобто КНФ. Застосуємо до неї І дистрибутивний закон:

$$(X \vee Y) \,\&\, \left(\overline{X} \vee \overline{Y}\right) = X \,\&\, \left(\overline{X} \vee \overline{Y}\right) \vee Y \,\&\, \left(\overline{X} \vee \overline{Y}\right) = X \,\&\, \overline{X} \vee X \,\&\, \overline{Y} \vee Y \,\&\, \overline{X} \vee Y \,\&\, \overline{Y}$$

У результаті отримана сума елементарних добутків, яка є ДНФ.

Питання

1. Які дві формулі U_1 і U_2 називаються рівносильними?
2. Як може бути встановлена рівносильність логічних формул?
3. Як за допомогою таблиці істинності довести рівносильність формул?
4. Довести всі надані приклади рівносильних формул.
5. Перший і другий дистрибутивні закони. Довести.
6. Які операції є основними серед логічних операцій?
7. Скільки логічних операцій вистачає для запису будь-якої логічної формули? Чому?
8. Яка логічна формула називається тотожно істинною?
9. Яка логічна формула називається здійсненою?
10. Яка логічна формула називається тотожно хибною?
11. Що таке елементарний добуток?
12. Що таке елементарна сума?
13. Коли елементарна сума є тотожно істинною?
14. Коли елементарний добуток є тотожно хибним?
15. Що називається ДНФ, КНФ логічної формули?

Тема 7. ДОСКОНАЛІ НОРМАЛЬНІ ФОРМИ ЛОГІЧНИХ ФОРМУЛ

План

1. Критерії тотожної істинності, тотожної хибності логічних формул.
2. Досконалі нормальні форми.
3. Критерій рівносильності довільних логічних формул.

1. Критерії тотожної істинності, тотожної хибності логічних формул

Для кожної логічної формули КНФ і ДНФ визначаються неоднозначно. Так у попередній лекції для формули $\overline{X \vee Y} \leftrightarrow X \,\&\, Y$ була знайдена КНФ: $(X \vee Y) \,\&\, \left(\overline{X} \vee \overline{Y}\right)$. Однак з урахуванням рівносильних перетворень:

$$(X \vee Y) \,\&\, \left(\overline{X} \vee \overline{Y}\right) \overset{(16)}{=} (X \vee Y) \,\&\, \left(\overline{X} \vee \overline{Y}\right) \& 1 \overset{(13)}{=} (X \vee Y) \,\&\, \left(\overline{X} \vee \overline{Y}\right) \& \left(X \vee \overline{X}\right)$$

отримуємо, що логічна формула $(X \vee Y) \,\&\, \left(\overline{X} \vee \overline{Y}\right) \& \left(X \vee \overline{X}\right)$ також є КНФ для $\overline{X \vee Y} \leftrightarrow X \,\&\, Y$.

Аналогічні результати можуть бути отримані й для ДНФ.

Твердження 1. Для того, щоб логічна формула була тотожно істинною, необхідно й достатньо, щоб кожний множник її КНФ мав, принаймні, два доданки, з яких один є деякою змінною, а другий - її запереченням.

Дійсно, у цьому випадку кожна елементарна сума, що є множником КНФ, буде дорівнювати 1, а тоді й уся кон'юнкція також виявиться рівною одиниці, тобто тотожно істинною.

Твердження 1 відіграє важливу роль. Дійсно, для розв'язку питання про те, чи є конкретна формула тотожно істинною, можна побудувати її КНФ. Якщо отримана КНФ задовольняє твердженню 1, то одержуємо позитивну відповідь на поставлене питання.

Приклад. З'ясувати, чи є формула $\left(A \to B\right) \& \overline{B} \to \overline{A}$ тотожно істинною. Проведемо розв'язок цього завдання двома способами:

1. За допомогою КНФ, рівносильній даній формулі;
2. За допомогою таблиці істинності.

Побудуємо КНФ для заданої логічної формули:

$$\left(A \to B\right) \& \overline{B} \to \overline{A} \overset{(18)}{=} \overline{\left(\overline{A} \vee B\right) \& \overline{B}} \vee \overline{A} \overset{(11)}{=} \overline{\overline{A} \vee B} \vee B \vee \overline{A} \overset{(10)}{=}$$

$$= A \,\&\, \overline{B} \vee B \vee \overline{A} \overset{(7)}{=} \left(A \vee B \vee \overline{A}\right) \& \left(\overline{B} \vee B \vee \overline{A}\right) \tag{1}$$

Як видно, кожний множник отриманої КНФ має два доданки, один з яких - змінна, а інший - її заперечення: у першому множнику $\left(A \vee B \vee \overline{A}\right)$ - ці доданки A і $\overline{A}$; у другому множнику $\left(\overline{B} \vee B \vee \overline{A}\right)$ - ці доданки B і $\overline{B}$. Відповідно до твердження 1 це говорить про тотожну істинність заданої

логічної формули. Якщо рівносильні викладки в (1) продовжити, то отримаємо:

$$(A \to B) \& \overline{B} \to \overline{A} = (A \vee B \vee \overline{A}) \& (\overline{B} \vee B \vee \overline{A}) = (1 \vee B) \& (1 \vee \overline{A}) = 1 \& 1 = 1$$

При побудові таблиці істинності формули $(A \to B) \& \overline{B} \to \overline{A}$ маємо:

A	B	$A \to B$	$\overline{B}$	$(A \to B) \& \overline{B}$	$\overline{A}$	$(A \to B) \& \overline{B} \to \overline{A}$
0	0	1	1	1	1	1
0	1	1	0	0	1	1
1	0	0	1	0	0	1
1	1	1	0	0	0	1

тобто наша логічна формула завжди приймає значення 1, тобто є тотожно істинною.

Твердження 2. Для того, щоб логічна формула була тотожно хибною, необхідно й достатньо, щоб кожний доданок її ДНФ мав, принаймні, два множники, з яких один є деякою змінною, а другий - її запереченням.

Дійсно, у цьому випадку кожний елементарний добуток, що є доданком ДНФ, буде дорівнювати 0, а тоді й уся диз'юнкція також виявиться рівної нулю, тобто тотожно хибною.

Для розв'язку питання про те, чи є конкретна формула тотожно хибною, можна скористатися твердженням 2: побудувати її ДНФ і перевірити: якщо отримана ДНФ задовольняє твердженню 2, то одержуємо позитивну відповідь на поставлене питання.

2. Досконалі нормальні форми

Нехай логічна формула $U(X_1, X_2, ..., X_n)$ не є тотожно хибною.

Визначення. Досконалою диз'юнктивною нормальною формою (ДДНФ) формули $U(X_1, X_2, ..., X_n)$, яка містить n різних змінних $X_1, X_2, ..., X_n$, називається така ДНФ, яка має наступні властивості:

1. В ній немає двох однакових доданків;
2. Жодний доданок не містить двох однакових множників;
3. Ніякий доданок не містить змінної разом з її запереченням;
4. У кожному доданку є в якості множника або змінна X_i, або її заперечення $\overline{X}_i$, де $i = 1,2,...,n$.

Нехай дана довільна формула $U(X_1, X_2, ..., X_n)$. Для отримання її ДДНФ необхідно:

- привести її спочатку до якої-небудь ДНФ;

- якщо який-небудь доданок, який позначимо через B, взагалі не містить змінну X_i, то замінити його рівносильною формулою: $X_i \,\&\, B \vee \overline{X}_i \,\&\, B$, оскільки

$$B = 1 \,\&\, B = \left(X_i \vee \overline{X}_i\right) \,\&\, B = X_i \,\&\, B \vee \overline{X}_i \,\&\, B .$$

  Таким чином, умова 4 буде виконаною;
- при наявності однакових доданків, виключити всі з них, крім одного. При наявності в доданках однакових множників, виключити всі з них, крім одного.
- Вилучити всі ті доданки, які містять яку-небудь змінну разом з її запереченням, тому що такі доданки представляють із себе тотожно хибні вирази. Результат – ДДНФ.

Якщо $U\left(X_1, X_2, ..., X_n\right)$ - тотожно хибна формула, то в процесі побудови ДДНФ усі доданки будуть вилучені, ми не отримаємо ДДНФ.

ДДНФ для логічної формули визначається однозначно.

Приклад. Для формули $X \vee Y \,\&\, \left(X \vee \overline{Y}\right)$ побудувати ДДНФ.

Спочатку побудуємо яку-небудь ДНФ для заданої формули:

$$X \vee Y \,\&\, \left(X \vee \overline{Y}\right) \overset{(6)}{=} X \vee Y \,\&\, X \vee Y \,\&\, \overline{Y} = \left[\begin{array}{l} \textit{Оскільки задана формула} \\ \textit{залежить від двох змінних } X \textit{ і } Y, \\ \textit{а в першому доданку відсутній } Y, \\ \textit{то замінимо перший доданок } X \textit{ на} \\ X \,\&\, Y \vee X \,\&\, \overline{Y} \end{array}\right] =$$

$$= X \,\&\, Y \vee X \,\&\, \overline{Y} \vee Y \,\&\, X \vee Y \,\&\, \overline{Y} = \left[\begin{array}{l} \textit{перший } X \,\&\, Y \textit{ і третій } Y \,\&\, X \\ \textit{доданки о}\text{днакові, } \textit{тому} \\ \textit{залишимо з них тільки один} \end{array}\right] =$$

$$= X \,\&\, Y \vee X \,\&\, \overline{Y} \vee Y \,\&\, \overline{Y} = \left[\begin{array}{l} \textit{останній доданок містить змінну} \\ \textit{і її заперечення, тому цей доданок} \\ \textit{усувається} \end{array}\right] =$$

$$= X \,\&\, Y \vee X \,\&\, \overline{Y}$$

ДДНФ для заданої формули має вид: $X \,\&\, Y \vee X \,\&\, \overline{Y}$.

Аналогічним чином визначається досконала кон’юнктивна нормальна форма (ДКНФ) логічної формули.

Нехай логічна формула $U\left(X_1, X_2, ..., X_n\right)$ не є тотожно істинною.

Визначення. Досконалою кон'юнктивною нормальною формою (ДКНФ) формули $U(X_1, X_2,...,X_n)$, яка містить n різних змінних $X_1, X_2,...,X_n$, називається така КНФ, яка має наступні властивості:

1. У ній немає двох однакових множників;
2. Жоден множник не містить двох однакових доданків;
3. Ніякий множник не містить змінної разом з її запереченням;
4. У кожному множнику є в якості доданка або змінна X_i, або її заперечення $\overline{X}_i$, де $i = 1,2,...,n$.

Нехай дана довільна формула $U(X_1, X_2,...,X_n)$. Для отримання її ДКНФ необхідно:

- привести її спочатку до якої-небудь КНФ;
- якщо який-небудь множник, який позначимо через B, взагалі не містить змінну X_i, то замінити його рівносильною формулою: $(X_i \vee B)\&(\overline{X}_i \vee B)$, оскільки

$$B = 0 \vee B = (X_i \,\&\, \overline{X}_i) \vee B = (X_i \vee B)\&(\overline{X}_i \vee B).$$

  Таким чином, умова 4 буде виконаною;
- при наявності однакових множників, вилучити всі з них, крім одного. При наявності в множнику однакових доданків, вилучити всі з них, крім одного.
- Вилучити всі ті множники, які містять яку-небудь змінну разом з її запереченням, тому що такі множники представляють із себе тотожно істинні вирази. Результат – ДКНФ.

3. Критерій рівносильності довільних логічних формул

Досконалі нормальні форми (ДНФ) дозволяють сформулювати критерій рівносильності двох довільних логічних формул $\Im$ і $\aleph$. Можна вважати, що $\Im$ і $\aleph$ містять однакові змінні. Дійсно: якщо це не так, тобто, наприклад, формула $\Im$ не містить деяку змінну X, яка входить в формулу $\aleph$, то $\Im$ можна замінити рівносильною формулою: $\Im\&(X \vee \overline{X})$, яка вже містить X. Після цього формули $\Im$ і $\aleph$ приводяться до досконалих диз'юнктивних (або кон'юнктивних) нормальних форм. Якщо $\Im$ і $\aleph$ рівносильні формули, то в силу єдиності ДНФ як диз'юнктивні, так і кон'юнктивні нормальні форми цих формул повинні співпадати. Таким чином порівняння ДНФ формул $\Im$ і $\aleph$ вирішує питання про їх рівносильність.

Питання

1. Скільки різних КНФ (ДНФ) можна побудувати для логічної формули? Навести приклади.

2. Сформулювати критерій (необхідну й достатню умову) тотожної істинності логічної формули. Навести приклади тотожно істинних формул.
3. Сформулювати критерій (необхідну й достатню умову) тотожної хибності логічної формули. Навести приклади тотожно хибних формул.
4. Що називається ДДНФ логічної формули?
5. Що називається ДКНФ логічної формули?
6. Правила побудови ДДНФ, ДКНФ. Навести приклади побудови ДДНФ, ДКНФ для логічної формули.
7. Критерій рівносильності довільних логічних формул.

Тема 8. ОСНОВНІ СХЕМИ ЛОГІЧНО ПРАВИЛЬНИХ МІРКУВАНЬ

План

1. Вступ
2. Правила висновку, заперечення, твердження-заперечення, заперечення-твердження, транзитивності.
3. Закон протиріччя
4. Правила контрапозиції, складної контрапозиції, перерізу.
5. Правила імпортації посилок, експортації посилок, ділем.

1. Вступ

Поряд із правилами побудови складних висловлень - логічних формул математична логіка містить правила перетворення логічних формул. Правила перетворення реалізують загальнологічні закони й забезпечують логічно правильні міркування.

Якщо опис системи, процесу, явища і т.д. представлений сукупністю складних висловлень - логічних формул, істинних для даної системи (у даній інтерпретації її простих висловлень), то за допомогою припустимих перетворень наявних логічних представлень про систему може бути виконаний їхній аналіз (синтез), можуть бути отримані нові характеристи зазначеної системи (істинні для даної системи) і т.і. Таким чином, за допомогою припустимих у логіці перетворень з'являється можливість одержання нових знань із наявних.

Процес отримання нових знань, виражених висловленнями, з інших знань, також виражених висловленнями, називається міркуванням (умовиводом). Вхідні висловлення називаються посилками (гіпотезами, умовами), а отримувані висловлення - висновком (наслідком).

Нижче приводяться найбільше використовувані схеми логічно правильних міркувань.

2. Правила висновку, заперечення, твердження-заперечення, заперечення-твердження, транзитивності

1. ***Правило висновку***: *Якщо з висловлення A випливає висловлення B і справедливо (істинно) висловлення A, то справедливо B*. Позначення:

$$\frac{A \to B, \quad A}{B}.$$

Приклади. Якщо студент був відсутній на модулі (A), він не написав модульну роботу (B). Студент був відсутній на модулі. Отже, він не написав модульну роботу.

Якщо один кут у трикутнику прямий (A), то два інші кути - гострі (B). Один кут трикутника прямий, отже два інших - гострі.

Якщо неавторизований доступ до інформаційної системи банку відбувся (A), то винним, у першу чергу, є начальник відділу інформаційної безпеки (B).

Логічна формула, що відображає правило висновку, виглядає наступним чином: $(A \to B) \& A \to B$. Ця формула є тотожно істинною:

$$(A \to B) \& A \to B = \overline{(\overline{A} \vee B) \& A} \vee B = \overline{\overline{A} \vee B} \vee \overline{A} \vee B = A \& \overline{B} \vee \overline{A} \vee B =$$

$$= (A \vee \overline{A} \vee B) \& (\overline{B} \vee \overline{A} \vee B)$$

Отримали КНФ для $(A \to B) \& A \to B$. Кожний множник отриманої КНФ містить змінну разом з її запереченням: перший множник A, $\overline{A}$, другий - B, $\overline{B}$, що відповідно до твердження 1 з лекції 7 говорить про тотожну істинність $(A \to B) \& A \to B$ і підтверджує правильність правила висновку.

2. ***Правило заперечення****: Якщо з A випливає B, і висловлення B хибне, то хибне і A (це використовується при доказі від противного).* Позначення:

$$\frac{A \to B, \quad \overline{B}}{\overline{A}}.$$

Приклади. Довести, що будь-яка скінченна множина M є обмеженою. Доказ від противного: нехай множина M є необмеженою (висловлення A), але тоді істиною є те, що ця множина нескінченна (висловлення B). Але множина M скінченна, тобто B – хибне, тому і A хибне, тобто наше припущення A – хибне, тобто множина M – обмежена (істинно висловленя «*не A*»).

Якщо студент був відсутній на модулі (A), він не написав модульну роботу (B). Студент написав модульну роботу. Отже він НЕ був відсутній на модулі.

Якщо неавторизований доступ до інформаційної системи банку відбувся (висловлення A), то винним, у першу чергу, є начальник відділу інформаційної безпеки (висловлення B). Начальник відділу інформаційної безпеки ні в чому не винний, отже неавторизованого доступу до інформаційної системи банку не відбулося.

Логічна формула, що відображає правило заперечення, виглядає наступним чином: $(A \to B) \& \overline{B} \to \overline{A}$. Ця формула є тотожно істинною:

$$(A \to B) \& \overline{B} \to \overline{A} = \overline{(\overline{A} \vee B) \& \overline{B}} \vee \overline{A} = \overline{\overline{A} \vee B} \vee B \vee \overline{A} = A \& \overline{B} \vee B \vee \overline{A} =$$

$$= (A \vee B \vee \overline{A}) \& (\overline{B} \vee B \vee \overline{A})$$

Отримали КНФ для $(A \to B) \& \overline{B} \to \overline{A}$. Кожний множник отриманої КНФ містить змінну разом з її запереченням: перший множник A, $\overline{A}$, другий - B, $\overline{B}$, що відповідно до твердження 1 з лекції 7 говорить про тотожну істинність $(A \to B) \& \overline{B} \to \overline{A}$ і підтверджує правильність правила заперечення.

3.***Правила твердження-заперечення***: *Якщо істинним є тільки одне з висловлень A чи B, і істинно одне з них, то друге хибне.* Позначення:

$$\frac{A \oplus B, \quad A}{\overline{B}}, \quad \frac{A \oplus B, \quad B}{\overline{A}}.$$

Приклад. 17 листопада я поїду на конференцію в Київ (висловлення A) або у відрядження у Вінницю (висловлення B). 17 я поїду в Київ, отже у Вінницю я не поїду.

Логічні формули, що відображають правила твердження-заперечення, виглядають наступним чином: $(A \oplus B) \& A \to \overline{B}$, $(A \oplus B) \& B \to \overline{A}$. Ці формули є тотожно істинними. Доведемо це для однієї з них (першої), тому що доказ тотожної істинності другої буде аналогічним.

У першу чергу покажемо, що $A \oplus B = \overline{A}B \vee A\overline{B}$, користуючись таблицею істинності:

A	B	$A \oplus B$	$\overline{A}$	$\overline{B}$	$\overline{A}B$	$A\overline{B}$	$\overline{A}B \vee A\overline{B}$
0	0	0	1	1	0	0	0
0	1	1	1	0	1	0	1
1	0	1	0	1	0	1	1
1	1	0	0	0	0	0	0

Користуючись тим, що $A \oplus B = \overline{A}B \vee A\overline{B}$, побудуємо КНФ для $(A \oplus B) \& A \to \overline{B}$:

$$(A \oplus B) \& A \to \overline{B} = \overline{(A \oplus B) \& A} \vee \overline{B} = \overline{\left(\overline{A}B \vee A\overline{B}\right) \& A} \vee \overline{B} = \overline{\overline{A}B} \vee \overline{A\overline{B}} \vee \overline{A} \vee \overline{B} =$$

$$= \overline{\overline{A}B} \,\&\, \overline{A\overline{B}} \vee \overline{A} \vee \overline{B} = \left(A \vee \overline{B}\right) \& \left(\overline{A} \vee B\right) \vee \overline{A} \vee \overline{B} = \left(A \vee \overline{B} \vee \overline{A} \vee \overline{B}\right) \& \left(\overline{A} \vee B \vee \overline{A} \vee \overline{B}\right)$$

Оскільки кожний множник отриманої КНФ містить серед доданків змінну і її заперечення, то $(A \oplus B) \& A \to \overline{B}$ є тотожно істинною формулою.

4.***Правила заперечення-твердження:*** *Якщо істинним є тільки одне з висловлень A чи B, і невірно одне з них, то друге є істинним.* Позначення:

$$\frac{A \oplus B, \quad \overline{A}}{B}, \quad \frac{A \oplus B, \quad \overline{B}}{A}.$$

Доказ аналогічний правилу 3.

5. ***Правило транзитивності****: Якщо з A випливає B, а з B випливає C, то з A випливає C.*

Позначення:

$$\frac{A \to B, \quad B \to C}{A \to C}.$$

Приклад. Якщо студент систематично займається (висловлення A), то він опанує матеріал дисциплін, що йому читаються (висловлення B). Якщо студент опанує матеріал дисциплін, що йому читаються (B), то він здасть сесію в строк (висловлення C).

Логічна формула, що відображає правило транзитивності, виглядає наступним чином: $(A \to B)\&(B \to C) \to (A \to C)$. Ця формула є тотожно істинною:

$$(A \to B)\&(B \to C) \to (A \to C) = \overline{(\overline{A} \vee B)\&(\overline{B} \vee C)} \vee (\overline{A} \vee C) =$$

$$= \overline{\overline{A} \vee B} \vee \overline{\overline{B} \vee C} \vee \overline{A} \vee C = A\,\&\,\overline{B} \vee B\,\&\,\overline{C} \vee \overline{A} \vee C =$$

$$= A\,\&\,\overline{B} \vee (B \vee \overline{A} \vee C)\&(\overline{C} \vee \overline{A} \vee C) =$$

$$= (A \vee B \vee \overline{A} \vee C)\&(\overline{B} \vee B \vee \overline{A} \vee C)\&(A \vee \overline{C} \vee \overline{A} \vee C)\&(\overline{B} \vee \overline{C} \vee \overline{A} \vee C)$$

Отримали КНФ для $(A \to B)\&(B \to C) \to (A \to C)$. Кожний множник отриманої КНФ містить змінну разом з її запереченням: перший множник A, $\overline{A}$, другий - B, $\overline{B}$, третій - A, $\overline{A}$, четвертий множник - C, $\overline{C}$, що відповідно до твердження 1 з лекції 7 говорить про тотожну істинність $(A \to B)\&(B \to C) \to (A \to C)$ і підтверджує правильність правила транзитивності.

3. Закон протиріччя

6. ***Закон протиріччя (від противного):*** *Якщо з A випливає B і $\overline{B}$, то A хибне.*

Позначення:

$$\frac{A \to B, \quad A \to \overline{B}}{\overline{A}}.$$

Приклад. Розглянемо висловлення A: Скінченна множина X є необмеженою. Тоді з (A) випливає:

- X має найбільший і найменший елементи (висловлення B) ;
- Не вірно, що X має найбільший і найменший елементи (висловлення $\overline{B}$), тому не вірним є висловлення A, що відповідає дійсності.

Логічна формула, що відображає закон протиріччя, виглядає наступним чином: $(A \to B)\&(A \to \overline{B}) \to \overline{A}$. Ця формула є тотожно істинною:

$$(A \to B)\&(A \to \overline{B}) \to \overline{A} = \overline{(\overline{A} \vee B)\&(\overline{A} \vee \overline{B})} \vee \overline{A} = \overline{\overline{A} \vee B} \vee \overline{\overline{A} \vee \overline{B}} \vee \overline{A} =$$

$$= A\,\&\,\overline{B} \vee A\,\&\,B \vee \overline{A} = (A \vee A)\&(A \vee B)\&(\overline{B} \vee A)\&(\overline{B} \vee B) \vee \overline{A} =$$

$$= (A \vee A \vee \overline{A})\&(A \vee B \vee \overline{A})\&(\overline{B} \vee A \vee \overline{A})\&(\overline{B} \vee B \vee \overline{A})$$

Отримали КНФ для $(A \to B)\&(A \to \overline{B}) \to \overline{A}$. Кожний множник отриманої КНФ містить змінну разом з її запереченням, що говорить про тотожну істинність $(A \to B)\&(A \to \overline{B}) \to \overline{A}$ і підтверджує правильність закону протиріччя.

4. Правила контрапозиції, складної контрапозиції, перерізу

7. ***Правило контрапозиції****: Якщо з A випливає B, то з того, що невірне B, випливає те, що невірне A.*

Позначення:

$$\frac{A \to B}{\overline{B} \to \overline{A}}.$$

Приклад. Якщо Іван мій син (A), то я старша за Івана (B). Якщо я не старша за Івана, то він мені не син.

Логічна формула, що відображає правило контрапозиції, виглядає наступним чином: $(A \to B) \to (\overline{B} \to \overline{A})$. Ця формула є тотожно істинною:

$$(A \to B) \to (\overline{B} \to \overline{A}) = \overline{\overline{A} \vee B} \vee B \vee \overline{A} = A\,\&\,\overline{B} \vee B \vee \overline{A} = (A \vee B \vee \overline{A})\&(\overline{B} \vee B \vee \overline{A})$$

Отримали КНФ для $(A \to B) \to (\overline{B} \to \overline{A})$. Кожний множник отриманої КНФ містить змінну разом з її запереченням, що говорить про тотожну істинність $(A \to B) \to (\overline{B} \to \overline{A})$ і підтверджує правильність правила контрапозиції.

8. ***Правило складної контрапозиції****: Якщо з A і B випливає C, то з A і $\overline{C}$ випливає $\overline{B}$.*

Позначення:

$$\frac{A \,\&\, B \to C}{A \,\&\, \overline{C} \to \overline{B}}.$$

Приклад. Якщо одягти гумові чоботи (A) і взяти парасольку (B), то в дощ не вимокнеш (C). Якщо ти одяг гумові чоботи й вимокнув у дощ, то ти не взяв парасольку.

Логічна формула, що відображає правило складної контрапозиції, виглядає наступним чином: $(A \,\&\, B \to C) \to (A \,\&\, \overline{C} \to \overline{B})$. Ця формула є тотожно істинною:

$$(A \,\&\, B \to C) \to (A \,\&\, \overline{C} \to \overline{B}) = \overline{\overline{A \,\&\, B} \vee C} \vee (\overline{A \,\&\, \overline{C}} \vee \overline{B}) = A \,\&\, B \,\&\, \overline{C} \vee \overline{A} \vee C \vee \overline{B} =$$

$$= (A \vee \overline{A} \vee C \vee \overline{B}) \,\&\, (B \vee \overline{A} \vee C \vee \overline{B}) \,\&\, (\overline{C} \vee \overline{A} \vee C \vee \overline{B})$$

Отримали КНФ для $(A \,\&\, B \to C) \to (A \,\&\, \overline{C} \to \overline{B})$. Кожний множник отриманої КНФ містить змінну разом з її запереченням, що говорить про тотожну істинність $(A \,\&\, B \to C) \to (A \,\&\, \overline{C} \to \overline{B})$ і підтверджує правильність правила складної контрапозиції.

9. ***Правило перерізу***: *Якщо з A випливає B, а з B і C випливає D, то з A і C випливає D.*

Позначення:

$$\frac{A \to B, \quad B \,\&\, C \to D}{A \,\&\, C \to D}.$$

Приклад. Якщо ти живеш в Одесі (A), то влітку до тебе приїжджають знайомі відпочивати (B). Якщо знайомі приїжджають (B) і залишаються на все літо (C), то твоя відпустка зіпсована (D).

Логічна формула, що відображає правило перерізу, виглядає наступним чином: $(A \to B) \,\&\, (B \,\&\, C \to D) \to (A \,\&\, C \to D)$. Ця формула є тотожно істинною:

$$(A \to B)\&(B\,\&\,C \to D) \to (A\,\&\,C \to D) = \overline{(\overline{A} \vee B)\&(\overline{B\,\&\,C} \vee D)} \vee (\overline{A\,\&\,C} \vee D) =$$

$$= \overline{\overline{A} \vee B} \vee \overline{\overline{B\,\&\,C} \vee D} \vee \overline{A} \vee \overline{C} \vee D = A\overline{B} \vee BC\overline{D} \vee \overline{A} \vee \overline{C} \vee D =$$

$$= (A \vee BC\overline{D} \vee \overline{A} \vee \overline{C} \vee D)(\overline{B} \vee BC\overline{D} \vee \overline{A} \vee \overline{C} \vee D) =$$

$$= (A \vee B \vee \overline{A} \vee \overline{C} \vee D)(A \vee C \vee \overline{A} \vee \overline{C} \vee D)(A \vee \overline{D} \vee \overline{A} \vee \overline{C} \vee D)\&$$

$$\&\,(\overline{B} \vee B \vee \overline{A} \vee \overline{C} \vee D)(\overline{B} \vee C \vee \overline{A} \vee \overline{C} \vee D)(\overline{B} \vee \overline{D} \vee \overline{A} \vee \overline{C} \vee D)$$

Отримали КНФ для $(A \to B)\&(B\,\&\,C \to D) \to (A\,\&\,C \to D)$. Кожний множник отриманої КНФ містить змінну разом з її запереченням, що говорить про тотожну істинність $(A \to B)\&(B\,\&\,C \to D) \to (A\,\&\,C \to D)$ і підтверджує правильність правила перерізу.

5. Правила імпортації посилок, експортації посилок, ділем

10. ***Правило імпортації (об'єднання посилок):*** *Якщо з A випливає те, що з B випливає C, то C випливає з A і B.*

Позначення:

$$\frac{A \to (B \to C)}{A\,\&\,B \to C}.$$

Приклад. Якщо я живу в Одесі (A), то якщо я залишаюся у відпустці вдома (В), то відпустка пропала (З).

Логічна формула, що відображає правило імпортації, виглядає наступним чином: $(A \to (B \to C)) \to (A\,\&\,B \to C)$. Ця формула є тотожно істинною:

$$(A \to (B \to C)) \to (A\,\&\,B \to C) = \overline{\overline{A} \vee \overline{B} \vee C} \vee (\overline{AB} \vee C) = \overline{\overline{A} \vee \overline{B}}\,\&\,\overline{C} \vee \overline{A} \vee \overline{B} \vee C =$$

$$= AB\overline{C} \vee \overline{A} \vee \overline{B} \vee C = (A \vee \overline{A} \vee \overline{B} \vee C)(B \vee \overline{A} \vee \overline{B} \vee C)(\overline{C} \vee \overline{A} \vee \overline{B} \vee C)$$

Отримали КНФ для $(A \to (B \to C)) \to (A\,\&\,B \to C)$. Кожний множник отриманої КНФ містить змінну разом з її запереченням, що говорить про тотожну істинність $(A \to (B \to C)) \to (A\,\&\,B \to C)$ і підтверджує правильність правила імпортації.

11. ***Правило експортації (роз'єднання посилок):*** *Якщо C випливає з A і B, то з A випливає, що з B випливає C.*

Позначення:

$$\frac{A \,\&\, B \to C}{A \to (B \to C)}.$$

Логічна формула, що відображає правило експортації, виглядає наступним чином: $(A \,\&\, B \to C) \to (A \to (B \to C))$. Ця формула є тотожно істинною:

$$(A \,\&\, B \to C) \to (A \to (B \to C)) = \overline{\overline{AB} \vee C} \vee \left(\overline{A} \vee \left(\overline{B} \vee C\right)\right) = AB\overline{C} \vee \overline{A} \vee \overline{B} \vee C =$$

$$\left(A \vee \overline{A} \vee \overline{B} \vee C\right)\left(B \vee \overline{A} \vee \overline{B} \vee C\right)\left(\overline{C} \vee \overline{A} \vee \overline{B} \vee C\right)$$

Отримана КНФ і підтверджує правильність правила экспортации.

12. ***Правила ділем:***

а) $\dfrac{A \to C, \quad B \to C, \quad A \vee B}{C}$; б) $\dfrac{A \to B, \quad A \to C, \quad \overline{C} \vee \overline{B}}{\overline{A}}$

в) $\dfrac{A \to B, \quad C \to D, \quad A \vee C}{B \vee D}$ г) $\dfrac{A \to B, \quad C \to D, \quad \overline{B} \vee \overline{D}}{\overline{A} \vee \overline{C}}$.

Завдання. Довести правильність правил дилем.

Питання

Сформулювати і довести:

1. Правило висновку,
2. Правило заперечення,
3. Правило твердження-заперечення,
4. Правило заперечення-твердження,
5. Правило транзитивності,
6. Закон протиріччя,
7. Правило контрапозиції,
8. Правило складної контрапозиції,
9. Правило перерізу,
10. Правило імпортації посилок,
11. Правило експортації посилок,
12. Правила ділем.

Тема 9. ДВОЇСТІ ФОРМУЛИ І ЇХ ВЛАСТИВОСТІ

План

1. Двоїсті операції й двоїсті формули.
2. Представлення довільної двозначної функції за допомогою логічної формули.

1. Двоїсті операції й двоїсті формули

Припустимо, що логічні формули містять тільки операції кон'юнкції, диз'юнкції й заперечення. Будемо говорити, що операція «$\&$» двоїста до операції «$\vee$» і навпаки.

Формули $\mathfrak{I}$ і $\mathfrak{I}^*$ називаються ***двоїстими***, якщо одна виходить із іншою заміною кожної операції на двоїсту із збереженням порядку операцій.

Приклад. Нехай

$$\mathfrak{I} = X \,\&\, (Y \vee Z \,\&\, (U \vee V)),$$

Тоді

$$\mathfrak{I}^* = X \vee Y \,\&\, (Z \vee U \,\&\, V).$$

Твердження. Якщо формули $\mathfrak{I}(X_1, X_2, ..., X_n)$ і $\mathfrak{I}^*(X_1, X_2, ..., X_n)$ - двоїсті формули, а $X_1, X_2, ..., X_n$ - всі елементарні висловлення, що в них входять, то

$$\overline{\mathfrak{I}}(X_1, X_2, ..., X_n) = \mathfrak{I}^*(\overline{X}_1, \overline{X}_2, ..., \overline{X}_n) \qquad (1)$$

чи

$$\overline{\mathfrak{I}}(\overline{X}_1, \overline{X}_2, ..., \overline{X}_n) = \mathfrak{I}^*(X_1, X_2, ..., X_n). \qquad (2)$$

Закон двоїстості. Якщо $\mathfrak{I}_1(X_1, X_2, ..., X_n)$ і $\mathfrak{I}_2(X_1, X_2, ..., X_n)$ - рівносильні формули, то й двоїсті до них $\mathfrak{I}_1^*(X_1, X_2, ..., X_n)$ і $\mathfrak{I}_2^*(X_1, X_2, ..., X_n)$ - рівносильні.

Доказ. Нехай $\mathfrak{I}_1(X_1, X_2, ..., X_n) = \mathfrak{I}_2(X_1, X_2, ..., X_n)$. Тоді

$$\mathfrak{I}_1(\overline{X}_1, \overline{X}_2, ..., \overline{X}_n) = \mathfrak{I}_2(\overline{X}_1, \overline{X}_2, ..., \overline{X}_n)$$

$$\Downarrow$$

$$\overline{\mathfrak{I}}_1(\overline{X}_1, \overline{X}_2, ..., \overline{X}_n) = \overline{\mathfrak{I}}_2(\overline{X}_1, \overline{X}_2, ..., \overline{X}_n)$$

З (2) випливає, що

$$\overline{\mathfrak{I}}_1(\overline{X}_1, \overline{X}_2, ..., \overline{X}_n) = \mathfrak{I}_1^*(X_1, X_2, ..., X_n),$$

$$\overline{\mathfrak{I}}_2(\overline{X}_1, \overline{X}_2, ..., \overline{X}_n) = \mathfrak{I}_2^*(X_1, X_2, ..., X_n),$$

звідки й отримуємо, що

$$\Im_1 * (X_1, X_2, ..., X_n) = \Im_2 * (X_1, X_2, ..., X_n),$$

що й було потрібно довести.

2. Представлення довільної двозначної функції за допомогою логічної формули

Нехай $F(X_1, X_2, ..., X_n)$ - довільна функція, що залежить від *n* змінних $X_1, X_2, ..., X_n$, причому й змінні, й сама функція приймають тільки два значення - ІСТИНА й НЕПРАВДА (1 і 0).

Таку функцію можна представити за допомогою логічної формули:

$$F(И, И, ..., И) \& X_1 \& X_2 \& ... \& X_n \vee F(И, ..., И, Л) \& X_1 \& ... \& X_{n-1} \& \overline{X}_n \vee$$
$$\vee F(И, ..., И, Л, Л) X_1 \& ... \& \overline{X}_{n-1} \& \overline{X}_n \vee ... \vee F(Л, Л, ..., Л) \& \overline{X}_1 \& \overline{X}_2 \& ... \& \overline{X}_n \quad (3)$$

Кожний доданок суми (3) - це добуток, у якому перший множник є значенням функції $F(X_1, X_2, ..., X_n)$ при деяких певних значеннях змінних $X_1, X_2, ..., X_n$, інші ж множники є змінними $X_i, i = 1,2,...,n,$ або запереченнями цих змінних. Під знаком заперечення знаходяться ті й тільки ті змінні, які в першому множнику мають значення НЕПРАВДА. Розглянута сума (3) містить усілякі доданки такого виду. Формула (3) визначає функцію $F(X_1, X_2, ..., X_n)$. Дійсно, дамо певні значення змінним, наприклад, $X_1 = Л, X_2 = И, ..., X_n = И$. Значення поданої функції – це $F(Л, И, ..., И)$. Розглянемо доданок з (3):

$$F(Л, И, ..., И) \& \overline{X}_1 \& X_2 \& ... \& X_n. \quad (4)$$

У цьому доданку всі множники, крім, можливо, першого, мають значення ІСТИНА. Тоді значення $F(Л, И, ..., И) \& \overline{X}_1 \& X_2 \& ... \& X_n$ буде співпадати зі значенням $F(Л, И, ..., И)$. У всякому іншому доданку знаки заперечення над змінними розподіляються інакше, ніж в (4), але тоді в добуток множником увійде або НЕПРАВДА без заперечення, або ІСТИНА із запереченням, а значить такий добуток буде дорівнювати НЕПРАВДі. Таким чином, при розглянутій підстановці в змінні значень ІСТИНА й НЕПРАВДА всі доданки, крім одного - (4), мають значення НЕПРАВДА, а доданок (4) - значення $F(Л, И, ..., И)$. Тоді вся сума (3) має значення $F(Л, И, ..., И)$.

Приклад. Нехай функція $F(A, B, C)$ визначена в вигляді таблиці:

A	B	C	$F(A,B,C)$	Відповідний доданок у логічній формулі
0	0	0	0	$F(Л,Л,Л)\,\&\,\overline{A}\,\&\,\overline{B}\,\&\,\overline{C}=0\,\&\,\overline{A}\,\&\,\overline{B}\,\&\,\overline{C}=0$
0	0	1	0	$F(Л,Л,И)\,\&\,\overline{A}\,\&\,\overline{B}\,\&\,C=0\,\&\,\overline{A}\,\&\,\overline{B}\,\&\,C=0$
0	1	0	1	$F(Л,И,Л)\,\&\,\overline{A}\,\&\,B\,\&\,\overline{C}=1\,\&\,\overline{A}\,\&\,B\,\&\,\overline{C}=\overline{A}\,\&\,B\,\&\,\overline{C}$
0	1	1	0	$F(Л,И,И)\,\&\,\overline{A}\,\&\,B\,\&\,C=0\,\&\,\overline{A}\,\&\,B\,\&\,C=0$
1	0	0	1	$F(И,Л,Л)\,\&\,A\,\&\,\overline{B}\,\&\,\overline{C}=1\,\&\,A\,\&\,\overline{B}\,\&\,\overline{C}=A\,\&\,\overline{B}\,\&\,\overline{C}$
1	0	1	1	$F(И,Л,И)\,\&\,A\,\&\,\overline{B}\,\&\,C=1\,\&\,A\,\&\,\overline{B}\,\&\,C=A\,\&\,\overline{B}\,\&\,C$
1	1	0	1	$F(И,И,Л)\,\&\,A\,\&\,B\,\&\,\overline{C}=1\,\&\,A\,\&\,B\,\&\,\overline{C}=A\,\&\,B\,\&\,\overline{C}$
1	1	1	0	$F(И,И,И)\,\&\,A\,\&\,B\,\&\,C=0\,\&\,A\,\&\,B\,\&\,C=0$

У логічну формулу внесемо лише ненульові доданки:

$$F(A,B,C)=\overline{A}\,\&\,B\,\&\,\overline{C}\vee A\,\&\,\overline{B}\,\&\,\overline{C}\vee A\,\&\,\overline{B}\,\&\,C\vee A\,\&\,B\,\&\,\overline{C}\,.$$

Очевидно, що отримана формула є ДДНФ.

Питання

1. Які формули $\mathfrak{Z}$ і $\mathfrak{Z}^{*}$ називаються двоїстими?
2. Сформулювати і довести закон двоїстості.
3. Представлення довільної двозначної функції за допомогою логічної формули.
4. Яку логічну формулу отримаємо в результаті представлення довільної двозначної функції за допомогою логічної формули?

Тема 10. ОСНОВНІ ПОНЯТТЯ ТЕОРІЇ ГРАФІВ

План

1. Вступ.
2. Визначення графа і його елементів.

1. Вступ

Графи є зручним і наочним засобом опису зв'язків між об'єктами, для їхнього графічного представлення.

Неформально граф можна розглядати як множину точок і з'єднуючих ці точки ліній зі стрілками або без них.

Першою роботою теорії графів як математичної дисципліни вважають статтю Ейлера (1736 р.), у якій розглядалася задача про Кенингсбергскі мости. Ейлер показав, що не можна обійти сім міських мостів і повернутися у вихідну точку, пройшовши по кожному мості рівно один раз. Наступний імпульс теорія графів отримала через майже 100 років з розвитком досліджень по електричних мережах, кристалографії, органічній хімії й іншим наукам.

Із графами, самі того не помічаючи, ми зустрічаємося постійно. Наприклад, графом є схема ліній метрополітену. Точками на ній представлені станції, а лініями - шляху руху поїздів. Досліджуючи свій родовід і зводячи його до далекого предка, ми будуємо так зване генеалогічне древо. І це древо - граф.

Але граф використовують аж ніяк не тільки як ілюстрацію. Наприклад, розглядаючи граф, що зображує мережу доріг між населеними пунктами, можна визначити маршрут проїзду від пункту A до пункту B. Якщо таких маршрутів виявиться декілька, хотілося б вибрати в певному сенсі оптимальний, наприклад, самий короткий або самий безпечний. Для розв'язку задачі вибору потрібно проводити певні обчислення над графами. При розв'язку подібних завдань зручно використовувати алгебраїчну техніку, та й саме поняття графа необхідно формалізувати.

Теорія графів дуже широко використовується, тому що її мова, з одного боку, наочна і зрозуміла, а з іншого - зручна у формальному дослідженні. Мовою теорії графів формулюються й вирішуються багато завдань керування, у тому числі, завдання мережевого планування й керування, аналізу й проектування організаційних структур керування, аналізу процесів функціонування й цілепокладання, багато завдань ухвалення рішення в умовах невизначеності й ін.

Графічне представлення у вузькому сенсі - це опис досліджуваної системи, процесу, явища засобами теорії графів у вигляді сукупності двох класів об'єктів: ***вершин*** і з'єднуючих їх ліній - ***ребер*** (або ***дуг***). Графи і їх складові характеризуються певними властивостями й набором припустимих перетворень (операцій) над ними.

При зображенні графа не всі деталі рисунка однаково важливі. Зокрема, не суттєвими є геометричні властивості ребер (довжина, кривизна і т.д.) і взаємне розташування вершин на площині.

2. Визначення графа і його елементів

Графи, як ми вже відзначали в прикладах, є спосіб "візуалізації" зв'язків між певними об'єктами. Зв'язки ці можуть бути "спрямованими", як, наприклад, у генеалогічному древі, або "неспрямованими" (мережа доріг із двобічним рухом). Відповідно до цього в теорії графів виділяють два основні типи графів: ***орієнтовані*** і ***неорієнтовані***.

Визначення. Граф G - це скінченна непорожня множина V, що містить p вершин, і множина X, що містить q ребер, які представляють з себе пари вершин.

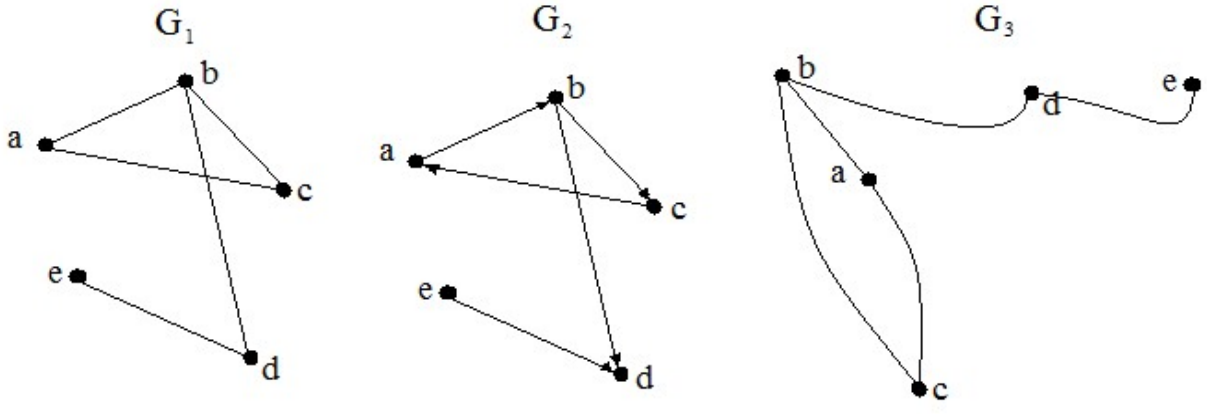
Для неорієнтованого графа ребра являють собою неупорядковані пари вершин з множини V, для орієнтованого графа ребра - це впорядковані пари вершин з V (тобто в орієнтованому графі для кожного ребра важливий напрямок: з якої вершини ребро виходить і в яку вершину входить).

Приклад. На рис.1 наведені приклади неорієнтованих графів G_1 і G_3 (рис.1(а, в)), орієнтованого G_2 графа (рис.1(б)). Позначимо V_1, V_2, V_3 - множини вершин відповідно графів G_1, G_2, G_3, а X_1, X_2, X_3 - відповідно множини їх ребер. Тоді:

$$V_1 = \{a,b,c,d,e\},\ X_1 = \{\{a,b\},\{a,c\},\{b,c\},\{b,d\},\{d,e\}\};$$

$$V_2 = \{a,b,c,d,e\},\ X_2 = \{< a,b >,< b,c >,< c,a >,< b,d >,< e,d >\};$$

$$V_3 = \{a,b,c,d,e\},\ X_3 = \{\{a,b\},\{a,c\},\{b,c\},\{b,d\},\{d,e\}\}.$$



а б с

Рис.1.

Відмітимо, що ребра для неорієнтованих графів G_1 і G_3 – це просто пари вершин, а для орієнтованого графа G_2 - упорядковані пари вершин.

Ілюстрацією того, що при зображенні графа несуттєвими є геометричні властивості ребер (довжина, кривизна і т.д.) і взаємне розташування вершин на площині, є графи G_1 і G_3. Незважаючи на те, що їх зображення різні, ці графи однакові, або рівні: $G_1 = G_3$, оскільки $V_1 = V_3$, а $X_1 = X_3$.

Якщо вершини *u* і *v* графа *G* з'єднані ребром, вони будуть називатися ***суміжними*** вершинами графа. Так для графа G_1 (рис.1(а)) вершини *a* і *b* є суміжними, а вершини *a* і *e* не є суміжними.

Ребро, що проходить через вершину, називається ***інцидентним*** цій вершині. Так для графа G_1 (рис.1(а)) ребро $\{a,b\}$ інцидентно вершині *a* і вершині *b*, але не інцидентно вершині *e*.

Якщо два різні ребра інцидентні одній вершині, то вони називаються ***суміжними***. Приклад суміжних ребер: $\{a,b\}$ і $\{a,c\}$ для графа G_1 (рис.1(а)).

Якщо граф містить єдину вершину й не містить ребер, то він називається ***тривіальним***.

Ребра, інцидентні одній парі вершин, називаються ***кратними*** (ребро $\{d,e\}$ графа *G* на рис.2 має кратність 2). Граф, що містить кратні ребра, називається ***мультиграфом***. Ребро, кінцями якого є співпадаючі вершини, називається ***петлею*** (ребро $\{e,e\}$ графа *G* на рис.2).

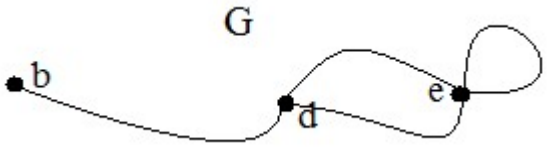


Рис.2.

Граф називається скінченним, якщо множина його елементів (вершин і ребер) скінченна, порожнім, якщо його множина вершин (а тому і ребер) порожня.

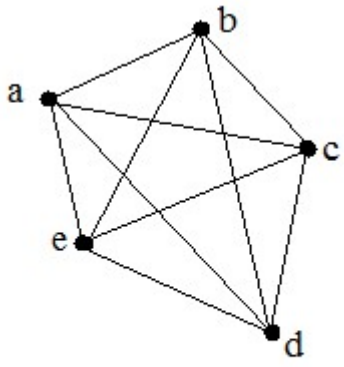


Рис.3

Граф без петель і кратних ребер називається ***повним***, якщо кожна пара його вершин з'єднана ребром. Приклад повного графа з 5 вершинами представлений на рис.3.

Доповненням графа *G* називається граф $\bar{G}$, що має ті ж вершини, що й граф *G*, і тільки ті ребра, які треба додати до ребер графа *G*, щоб отримати повний граф. Приклад графа *G* і його доповнення представлений на рис.4.

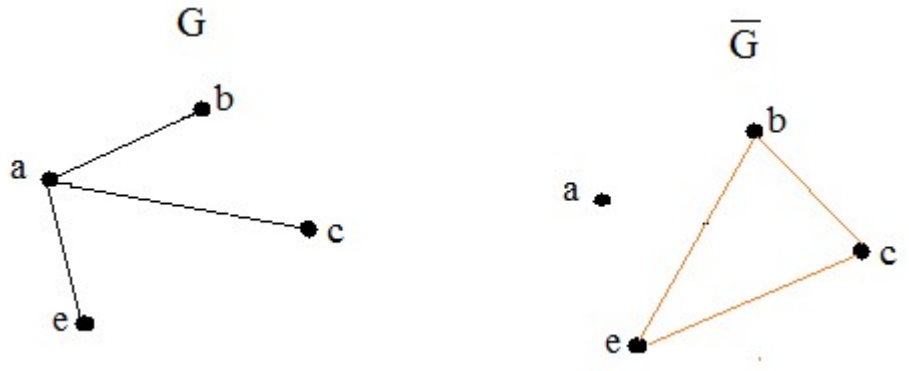
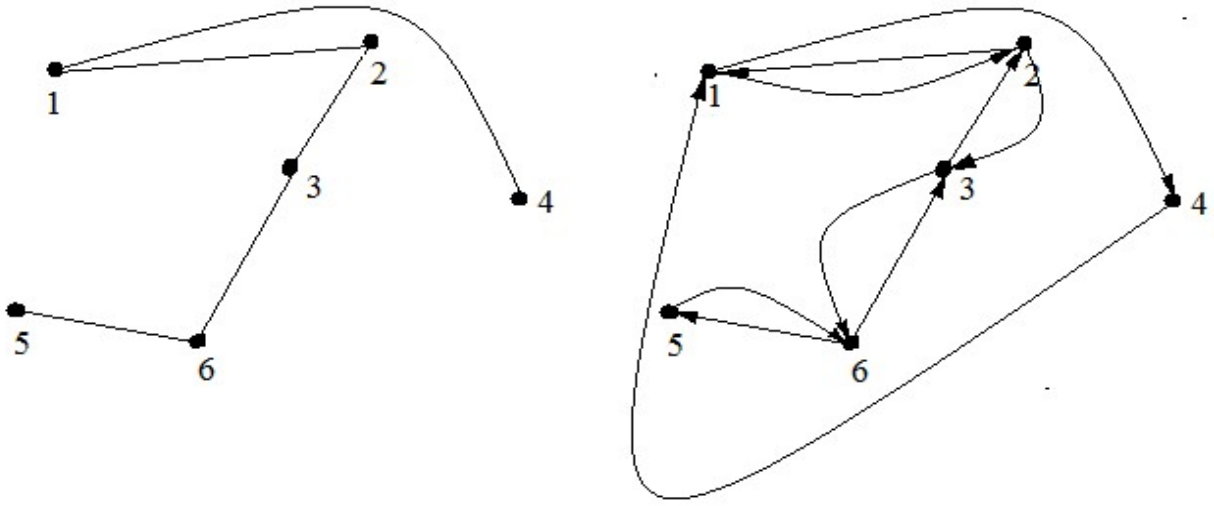


Рис.4.

Кожному неорієнтованому графу (рис. 5(а)) відповідає орієнтований граф (рис. 5(б)) з тою ж множиною вершин, у якому кожне неорієнтоване ребро замінено двома орієнтованими ребрами протилежних напрямків, інцидентними тим же вершинам.



а б

Рис.5.

Ступенем вершини v неорієнтованого графа G називається кількість ребер $\rho(v)$, інцидентних вершині v. Для графа, представленого на рис.5(а), маємо:

$$\rho(1) = \rho(2) = \rho(3) = \rho(6) = 2, \rho(4) = \rho(5) = 1.$$

У неорієнтованому графі сума ступенів усіх вершин дорівнює подвоєному числу ребер графа. Петля в ступінь відповідної вершини дає внесок 2.

Для вершин орієнтованого графа визначаються два локальні ступені: $\rho_1(v)$- число ребер з початком у вершині v; $\rho_2(v)$- число ребер, для яких вершина v є кінцем. В орієнтованому графі суми ступенів усіх вершин $\rho_1(v)$ і $\rho_2(v)$ дорівнюють кількості ребер цього графа, тобто, якщо кількість ребер графа дорівнює m, то

$$\sum_{v \in V} \rho_1(v) = \sum_{v \in V} \rho_2(v) = m \,.$$

Питання

1. Для чого використовуються графи?
2. З яких основних елементів складається граф? Навести приклади.
4. Який граф називається неорієнтованим, орієнтованим?
5. Якими двома множинами задається неорієнтований граф, орієнтований граф?
6. Які вершини графа називаються суміжними?
7. Які ребра графа називаються суміжними?
8. Коли ребро графа називається інцидентним вершині?
9. Який граф називається тривіальним?
10. Які ребра графа називаються кратними?
11. Що таке петля в графі?
12. Який граф називається повним?
13. Який граф $\bar{G}$ називається доповненням до графа G?
14. Що називається ступенем вершини неорієнтованого графа, орієнтованого графа? Навести приклади.
15. Чому в неорієнтованому графі дорівнює сума ступенів усіх вершин?
16. Чому в орієнтованому графі дорівнюють суми ступенів усіх вершин $\rho_1(v)$ і $\rho_2(v)$?

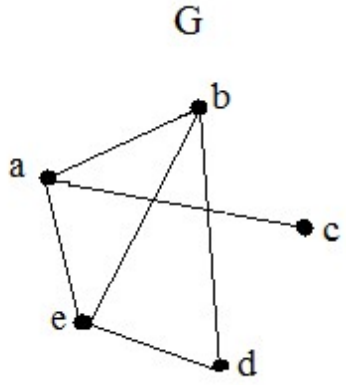
Тема 11. СПОСОБИ ЗАВДАННЯ ГРАФІВ

План

1. Матриця суміжності графа.
2. Матриця інцидентності графа.
3. Схеми машинного представлення неорієнтованих графів.
4. Порівняння різних схем машинного представлення графів. Переваги, недоліки

1. Матриця суміжності графа

Нехай є скінченний неорієнтований граф *G* (рис.1(а)), який має *n* вершин. ***Матриця суміжності*** цього графа - квадратна *n*n* матриця, кожний рядок і кожний стовпець якої відповідає конкретній вершині графа. На перетинанні рядка й стовпця в матриці суміжності буде ненульове значення, якщо відповідні вершини є в графі суміжними, і нуль - інакше. Якщо матриця не містить кратних ребер, то для позначення суміжності вершин використовується одиниця (рис.1(б)).



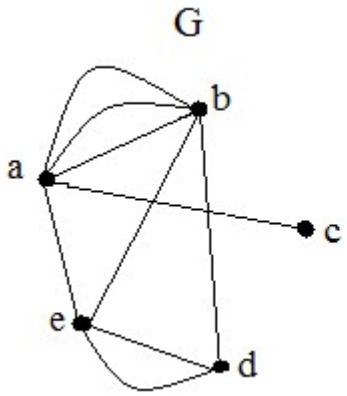
а

	a	b	c	d	e
a	0	1	1	0	1
b	1	0	0	1	1
c	1	0	0	0	0
d	0	1	0	0	1
e	1	1	0	1	0

б

Рис.1.

Для врахування можливої кратності ребер на перетинанні рядка й стовпця, відповідних до суміжних вершин неорієнтованого графа, ставиться кількість ребер, що їх з'єднує (рис. 2).



а

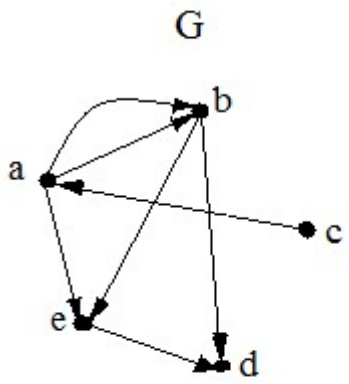
	a	b	c	d	e
a	0	3	1	0	1
b	3	0	0	1	1
c	1	0	0	0	0
d	0	1	0	0	2
e	1	1	0	2	0

б

Рис.2.

Очевидно, матриця суміжності неорієнтованого графа є симетричною, оскільки, якщо вершина v суміжна з вершиною w, то w буде суміжна з вершиною v.

Для орієнтованого графа на перетинанні рядка, що відповідає вершині v, і стовпця, що відповідає вершині w, у матриці суміжності ставиться число, рівне кількості ребер, що починаються у вершині v і закінчуються у вершині w (рис.3).



	a	b	c	d	e
a	0	2	0	0	1
b	0	0	0	1	1
c	1	0	0	0	0
d	0	0	0	0	0
e	0	0	0	1	0

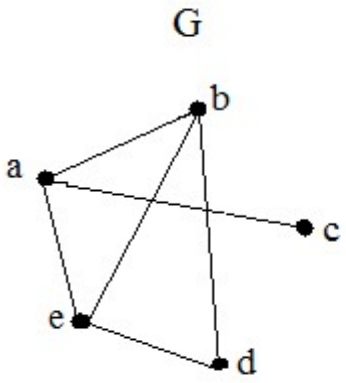
а б

Рис.3.

Для орієнтованого графа матриця суміжності симетричною не буде.

2. Матриця інцидентності графа

Матриця інцидентності графа G, який містить m вершин і n ребер – це прямокутна $m \times n$ – матриця, кожний рядок якої відповідає черговій вершині, а кожний стовпець - черговому ребру графа. На перетинанні рядка, що відповідає вершині v, і стовпця, що відповідає ребру r, у неорієнтованому графі ставиться 1, якщо ребро r інцидентно вершині v, і 0, коли інакше. Приклад представлений на рис.4.

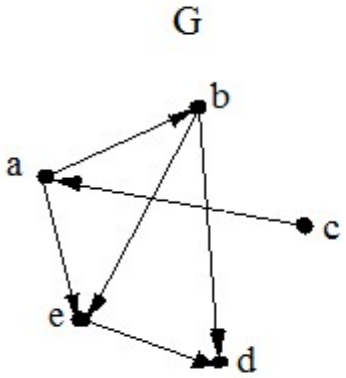


	{a,b}	{a,c}	{a,e}	{b,e}	{b,d}	{d,e}
a	1	1	1	0	0	0
b	1	0	0	1	1	0
c	0	1	0	0	0	0
d	0	0	0	0	1	1
e	0	0	1	1	0	1

а б

Рис.4

Для орієнтованого графа інцидентність ребра r вершині v в матриці інцидентності відмічається -1, якщо вершина v є початком ребра r, відмічається 1, якщо вершина v є кінцем ребра r (рис.5).



а

	⟨a,b⟩	⟨a,e⟩	⟨c,a⟩	⟨b,e⟩	⟨b,d⟩	⟨e,d⟩
a	-1	–1	1	0	0	0
b	1	0	0	–1	–1	0
c	0	0	–1	0	0	0
d	0	0	0	0	1	1
e	0	1	0	1	0	–1

б

Рис.5.

3. Схеми машинного представлення неорієнтованих графів.

Граф G з множиною вершин V і множиною ребер X будемо позначати: $G = (V, X)$. Якщо $Y \subseteq V$, то суміжна множина для Y є

$$Adj(Y) = \{x \in V \setminus Y \mid \{x, y\} \in X \text{ для деякого } y \in Y\}.$$

Інакше: $Adj(Y)$ є множина вузлів $G = (V, X)$, що не належать Y, але є суміжними хоча б з одним вузлом з Y, або інакше: $Adj(Y)$ - це множина сусідів тих вузлів, що входять в Y.

Характеристики алгоритмів, які оперують із графами, зазвичай дуже чутливі до способу їх представлення.

Нехай $G = (V, X)$ — неорієнтований граф з n вершинами. *Списком суміжності* для вершини $x \in V$ називається множина

$$Adj(x) = \{y \in V \setminus \{x\} \mid y \text{ суміжна з } x\}$$

Структура суміжності графа G — це множина списків суміжності для всіх його вершин. Таку структуру можна реалізувати, зберігаючи послідовно списки суміжності вузлів в одномірному масиві A довжинии $2|X|$, і використовуючи додатковий індексний масив A_{ind} довжини $n+1$, який містить покажчики початку кожного списку суміжності в масиві A ($A(n+1)$ — адреса першої вільної комірки в масиві A) (рис.6). Загальна довжина масивів при такій схемі зберігання — $2|X| + |V| + 1$.

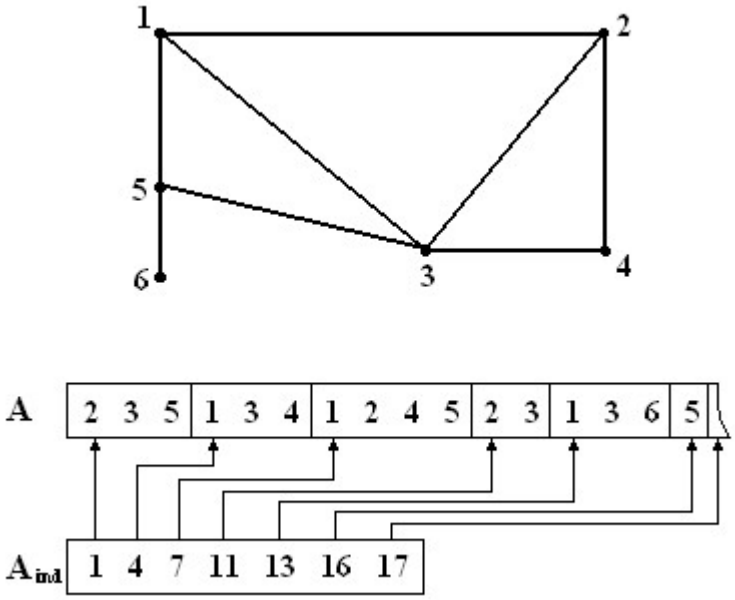


Рис.6. Приклад структури суміжності графа

Сусіди поточного вузла $\bar{x} \in V$ в масиві A розташовуються в позиціях, починаючи з $A_{ind}(\bar{x})$ і закінчуючи $A_{ind}(\bar{x}+1)-1$, таким чином, їх пошук не є складним, що є дуже значною перевагою розглянутої схеми зберігання. Однак внесення при необхідності змін у структуру суміжності графа очевидно викличе утруднення. Дійсно, додавання (виключення) вузлів (ребер) із графа приведе до модифікації не тільки списків суміжності відповідних вузлів, але може затребувати зміни всього масиву A (і відповідним чином A_{ind}) (рис.7), що, звичайно, не бажано.

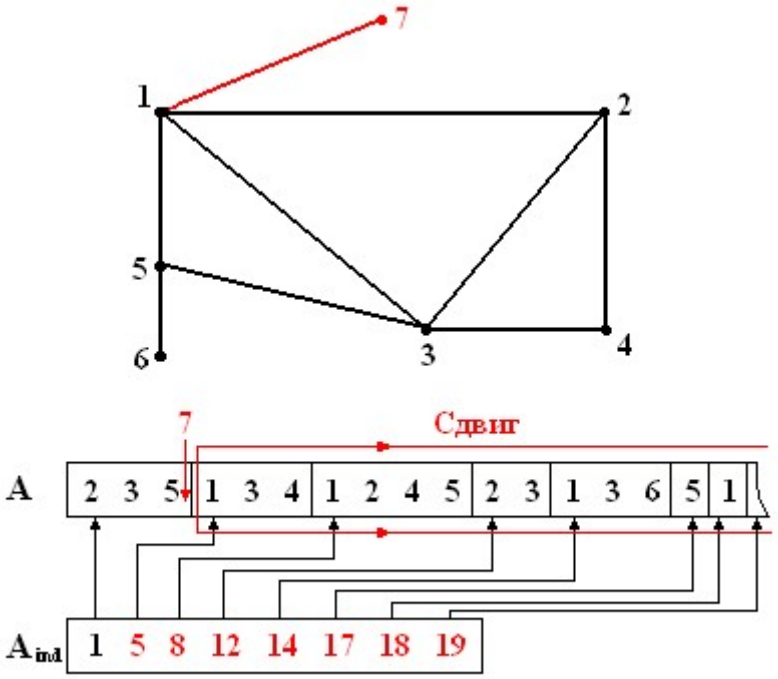


Рис.7. Модифікація структури суміжності графа при додаванні вершини

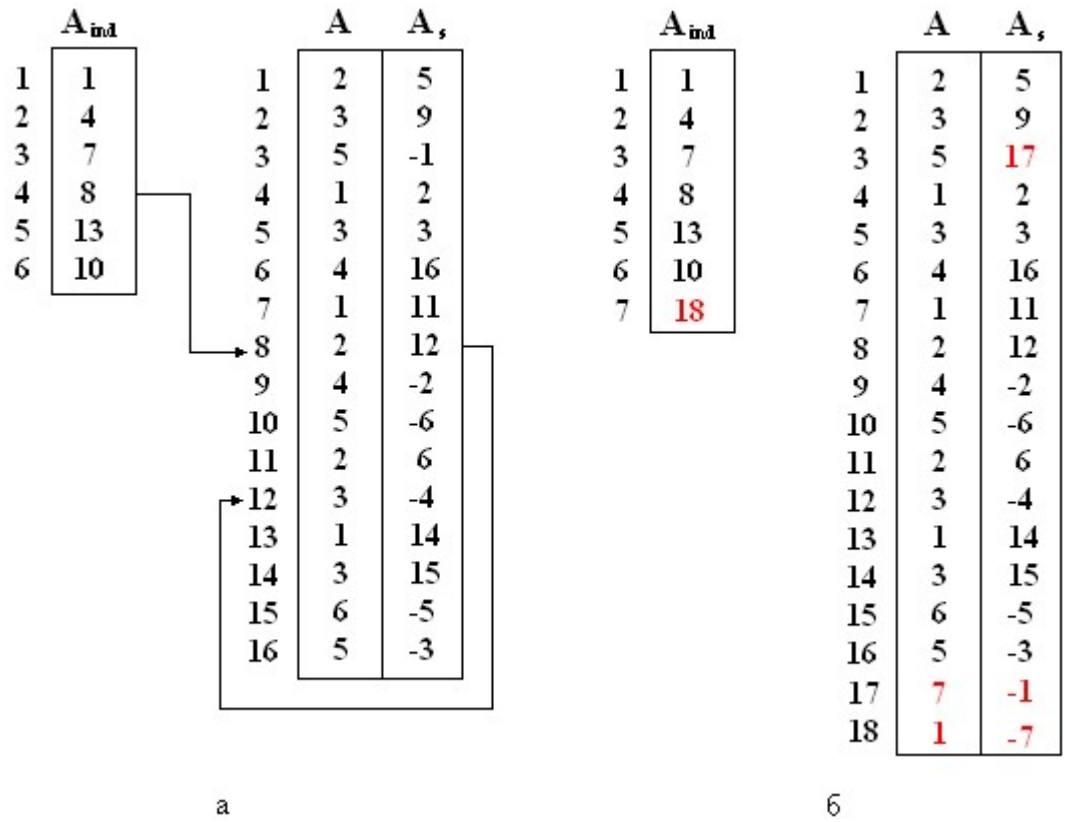
Однією з найбільш простих схем зберігання графа є *таблиця зв'язків* - двовимірний масив, який має n рядків і m стовпців, де m — максимальний ступінь вершин в $G = (V, X)$. Список суміжності i-го вузла зберігається в i-ому рядку. Для графа, наведеного на рис.6, таблиця зв'язків буде мати вигляд:

$$\begin{bmatrix} 2 & 3 & 5 & - \\ 1 & 3 & 4 & - \\ 1 & 2 & 4 & 5 \\ 2 & 3 & - & - \\ 1 & 3 & 6 & - \\ 5 & - & - & - \end{bmatrix}.$$

Дана схема зберігання надзвичайно проста при реалізації, доступ до списку суміжності чергового вузла - це доступ до відповідного рядка матриці, модифікація графа приводить до зміни елементів відповідних рядків матриці без порушення загальної структури (якщо при модифікації не змінюється *m*). Однак ця схема може бути надзвичайно неефективною, якщо велика кількість вузлів графа має ступінь, (значно) меншу, ніж максимальна, оскільки її вимоги до пам'яті визначаються як *mn* елементів, що зберігаються.

Найбільш зручною з погляду можливостей проведення модифікацій графа є схема, яка використовує поле зв'язків. Дана схема містить три одномірні масиви *A*, A_s, A_{ind}, перші два з яких мають довжини $2|X|$, останній — $|V|$. Значенням покажчика $A_{ind}(i)$ є початок списка суміжності *i*-го вузла в масиві *A*. Якщо *A(k)* — це черговий сусід *i*-го вузла, то $A_s(k)$ — покажчик місця розташування наступного його сусіда в масиві *A*. Від'ємне значення $A_s(k)$ говорить про закінчення списку суміжності розглянутого вузла.

Загальна довжина масивів при такому способі представлення графа — $4|X| + |V|$, що значно більше, чим у першій схемі. Однак модифікація графа вимагає лише незначних змін у вже сформованій частині масивів. Для графів, представлених на рис.6,7, відповідні схеми - на рис.8.



а б

Рис.8. Схема зберігання, заснована на полі зв'язків: вхідний граф (а); граф після додавання вершини (б)

4. Порівняння різних схем машинного представлення графів. Переваги, недоліки

Схема зберігання $G = (X, E)$	***Переваги***	***Недоліки***	***Загальні запити до пам'яті***
Заснована на структурі суміжності графа	Проста організація пошуку сусідів поточного вузла	Викликає труднощі внесення змін у структуру суміжності графа. Додавання (виключення) вузлів (ребер) із графа приведе до модифікації всього масиву A і A_{ind}	$2\|X\|+\|V\|+1$
Таблиця зв'язків	Схема проста при реалізації, доступ до списку суміжності вузла - це доступ до відповідного рядка матриці; модифікація графа приводить до зміни елементів відповідних рядків матриці без порушення загальної структури (якщо при модифікації не змінюється m).	Схема може бути надзвичайно неефективною, якщо велика кількість вузлів графа має ступінь, значно менший, ніж максимальний	mn n - кількість вершин, m — максимальний ступінь вершин в $G = (X, E)$
Заснована на полі зв'язків	Найбільш зручна для модифікацій графа	Найбільші запити до пам'яті в порівнянні з усіма розглянутими схемами	$4\|X\|+\|V\|$

Таким чином, вибір схеми зберігання графа визначається тим набором задач, які розв'язуються на його основі.

Питання

1. Що представляє із себе матриця суміжності неорієнтованого графа, які властивості вона має?
2. Як у матриці суміжності неорієнтованого графа враховується кратність ребра?
3. Як формується матриця суміжності орієнтованого графа, якими особливостями, стосовно матриці суміжності неорієнтованого графа, вона володіє?
4. Що таке матриця інцидентності графа?
5. Чим відрізняються матриці інцидентності орієнтованого й неорієнтованого графів?
6. Що таке список суміжності вершини графа?
7. Що являє собою структура суміжності неорієнтованого графа?
8. Як формується схема машинного представлення графа, заснована на структурі суміжності?
9. Основний недолік схеми машинного представлення графа, заснованої на структурі суміжності.
10. Що представляє із себе таблиця зв'язків графа? Переваги й недоліки такої схеми машинного представлення графа.

Тема 12. ОПЕРАЦІЇ НАД ГРАФАМИ

План

1. Графи і бінарні відношення.
2. Ізоморфізм графів.
3. Поняття підграфа і надграфа.
4. Видалення елементів графа.
5. Маршрути, шляхи, ланцюги, цикли

1. Графи і бінарні відношення

Відношенню ρ, заданому на множині $V = \{v_1, v_2, ..., v_n\}$, взаємно однозначно відповідає орієнтований граф G без кратних ребер з множиною вершин V, в якому ребро $\langle v_1, v_2 \rangle$ існує тоді й тільки тоді, коли $v_1 \rho v_2$.

Властивостям бінарних відношень відповідають певні властивості відповідних їм графів:

- Симетричному бінарному відношенню ρ відповідає орієнтований граф G, у якому кожне існуюче орієнтоване ребро $\langle v_i, v_j \rangle$ має пару: ребро протилежного напрямку $\langle v_j, v_i \rangle$;
- Антисиметричному бінарному відношенню ρ відповідає орієнтований граф G, який не містить пар вершин із протилежно спрямованими ребрами;
- Якщо ρ рефлексивне, то граф G має петлі у всіх вершинах;
- Якщо ρ антирефлексивне, то граф G не має петель;
- Якщо ρ транзитивне, то в графі G для кожної пари ребер $\langle v_i, v_j \rangle, \langle v_j, v_k \rangle$ існує ребро $\langle v_i, v_k \rangle$.

Розглянемо приклад. По графу G, зображеному на рис.1, що задає деяке бінарне відношення ρ, визначити властивості цього відношення.

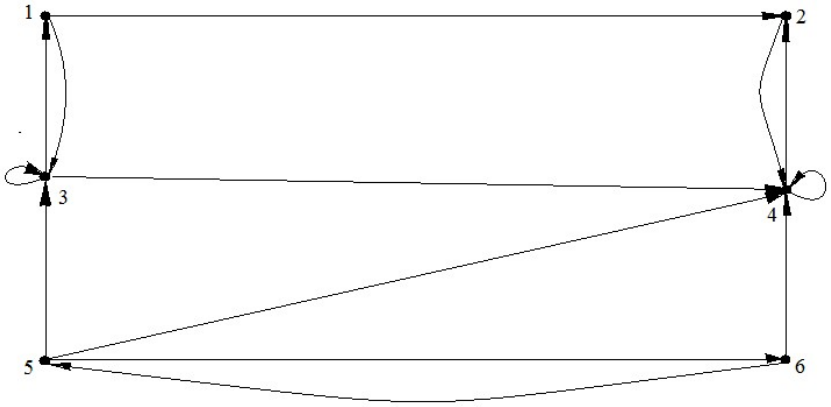


Рис.1.

Відношення ρ не є рефлексивним, оскільки існують вершини без петель: 1,2,5,6.

Відношення ρ не є антирефлексивним, оскільки існують вершини з петлями: 3,4.

Відношення ρ не є симетричним, оскільки в графі існують ребра, наприклад, $\langle 1,2\rangle$, для якого немає протилежно спрямованого ребра, тобто відсутнє ребро $\langle 2,1\rangle$.

Відношення ρ не є антисиметричним, оскільки в графі існують ребра, наприклад, $\langle 1,3\rangle$, для якого є протилежно спрямоване ребро $\langle 3,1\rangle$.

Відношення ρ не є транзитивним, оскільки існує, наприклад, пара ребер графа $G:\langle 1,2\rangle,\langle 2,4\rangle$, але ребра $\langle 1,4\rangle$ немає.

2. Ізоморфізм графів

Два графа G_1 і G_2 називаються ***ізоморфними*** (позначається $G_1 \cong G_2$ або $G_1 = G_2$), якщо між їхніми множинами вершин можна встановити взаємно однозначну відповідність, що зберігає суміжність. Наприклад, графи, зображені на рис.2, є ізоморфними при відповідності між вершинами $v_i \leftrightarrow u_i$.

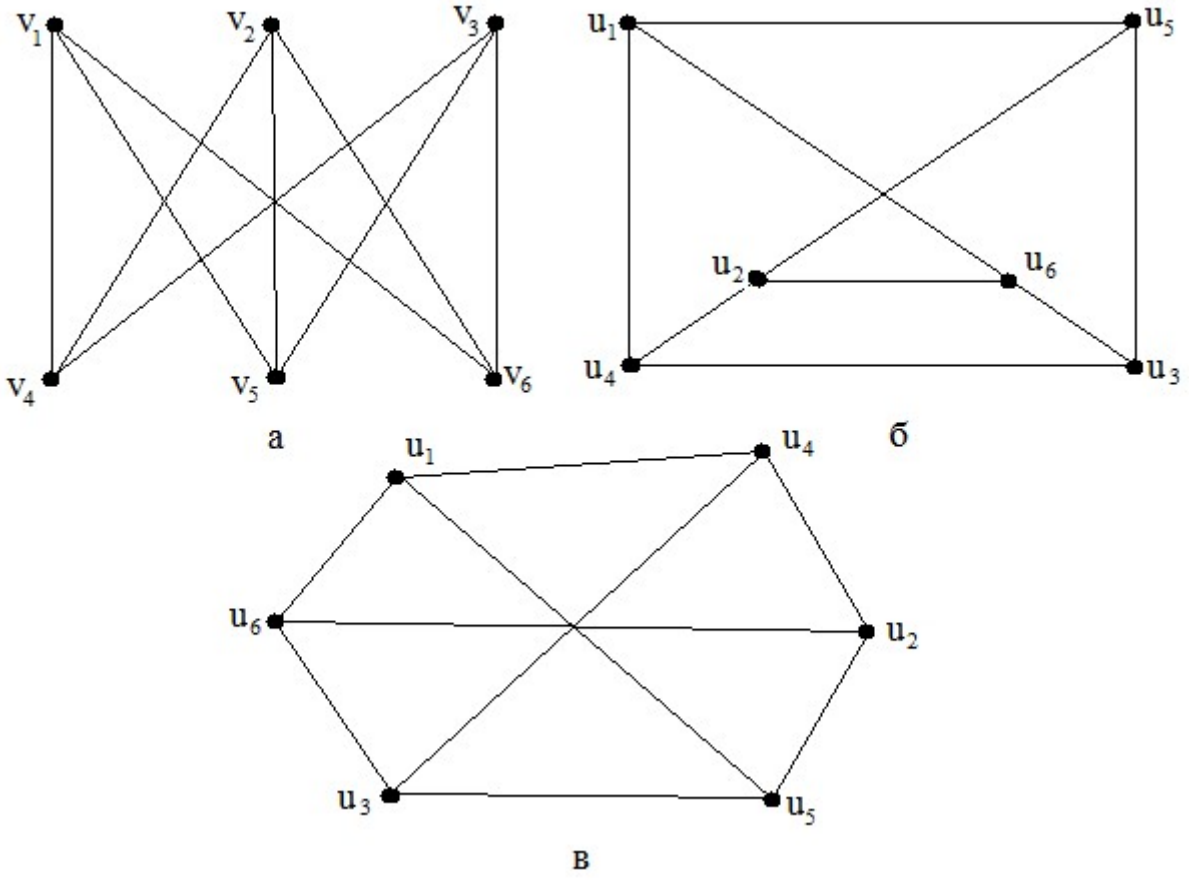


Рис.2.

Ізоморфні графи відрізняються тільки мітками вершин.

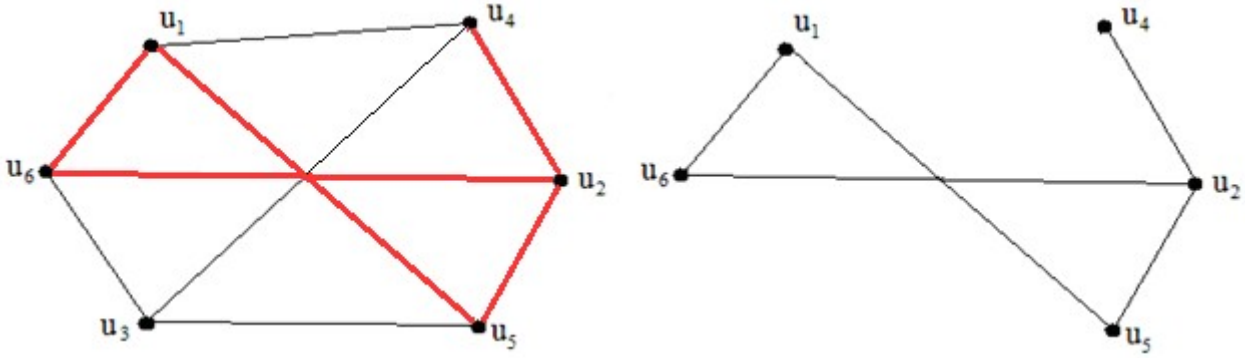
Відношення ізоморфізму між графами є відношенням еквівалентності.

Установити, що графи не є ізоморфними, легко, коли ці графи мають різні кількісні характеристики, наприклад, різна кількість вершин, різна кількість ребер, максимальна/мінімальний ступінь вершин в одному графі відрізняється від максимального/ мінімального ступеня вершин іншого графа й ін.

Інваріант графа G – це число, пов'язане з G, яке приймає одне й те саме значення на будь-якому графі, ізоморфному G. Кількість вершин і кількість ребер графа є його інваріантами.

3. Поняття підграфа і надграфа

Підграфом графа G називається граф, у якого всі вершини й ребра належать графові G. Приклад представлений на рис.3 (тут рис.3(а) – поданий граф, рис.3(б) – його підграф).

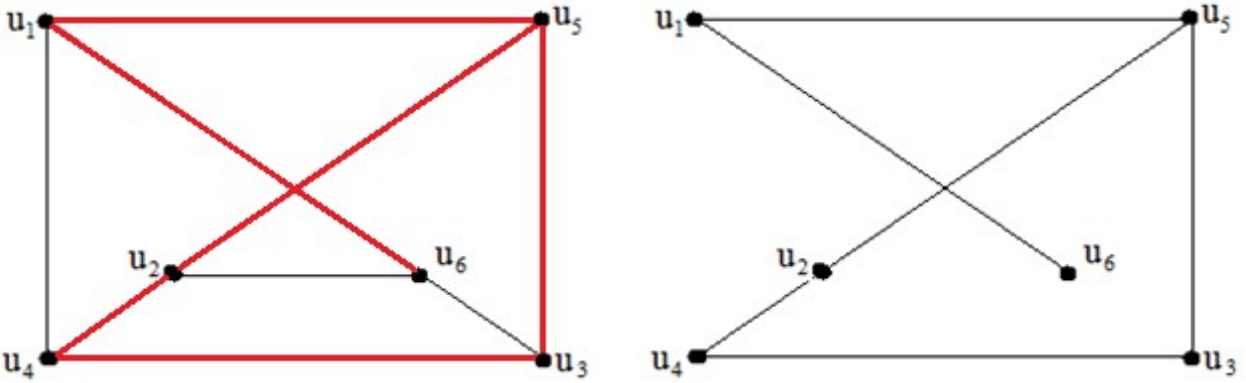


а б

Рис.3.

Якщо G_1 - підграф графа G, то G називається ***надграфом*** графа G_1. На рис.3(а) зображений граф, що є надграфом для графа, зображеного на рис.3(б).

Остовний підграф – це підграф G, що містить усі його вершини. Приклад остовного підграфа представлений на рис.4(б) для графа, представленого на рис.4(а).



а б

Рис.4.

Для будь-якої підмножини S множини вершин графа $G(V,X)$ (тобто $S \subseteq V$) ***породженим*** підграфом (позначається $\langle S \rangle$) називається максимальний підграф графа $G(V,X)$, множиною вершин якого є S. Таким чином дві вершини з S суміжні в графі $\langle S \rangle$ тоді й тільки тоді, коли вони суміжні у вхідному графі $G(V,X)$.

Розглянемо приклад графів на рис. 5. Тут: G_2 - остовний підграф G, G_1 остовним підграфом графа G не є; G_1 - породжений підграф графа G, G_2 породженим підграфом графа G не є.

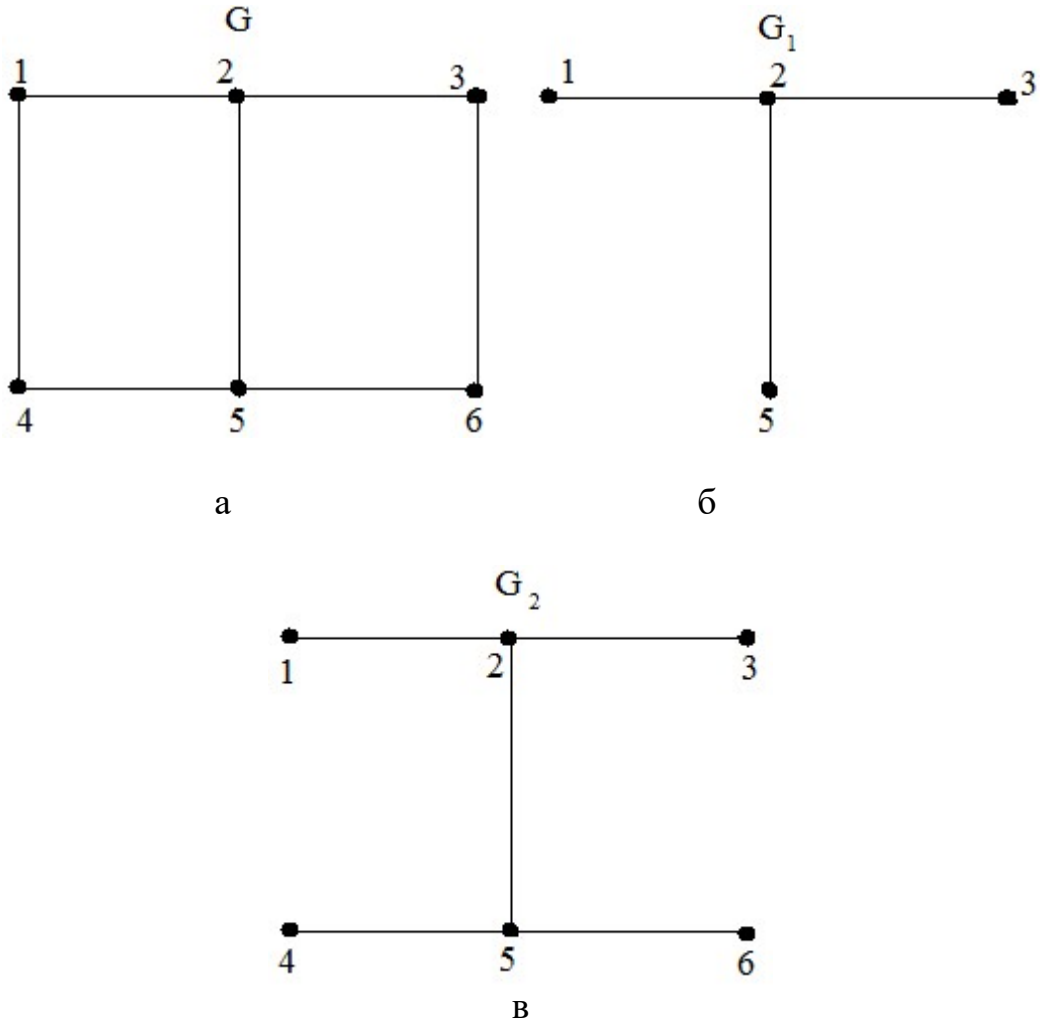


Рис.5.

4. Видалення елементів графа

Видалення вершини v_i з графа G приводить до підграфу $G - v_i$, що містить всі вершини графа G, за виключенням v_i, і все ребра графа G, не інцидентні v_i. Іншими словами, $G - v_i$ є максимальний підграф графа G, що не містить v_i.

Видалення ребра $\langle v_i, v_j \rangle$ з графа G приводить до остовного підграфу, що містить всі ребра графа G за виключенням ребра $\langle v_i, v_j \rangle$, тобто граф $G - \langle v_i, v_j \rangle$ є максимальний підграф G, що не містить $\langle v_i, v_j \rangle$.

Видалення довільної множини вершин або ребер із графа G визначається як послідовне видалення всіх елементів цієї множини. Приклади для графа G (рис.6(а)) представлені на рис.6(б,в).

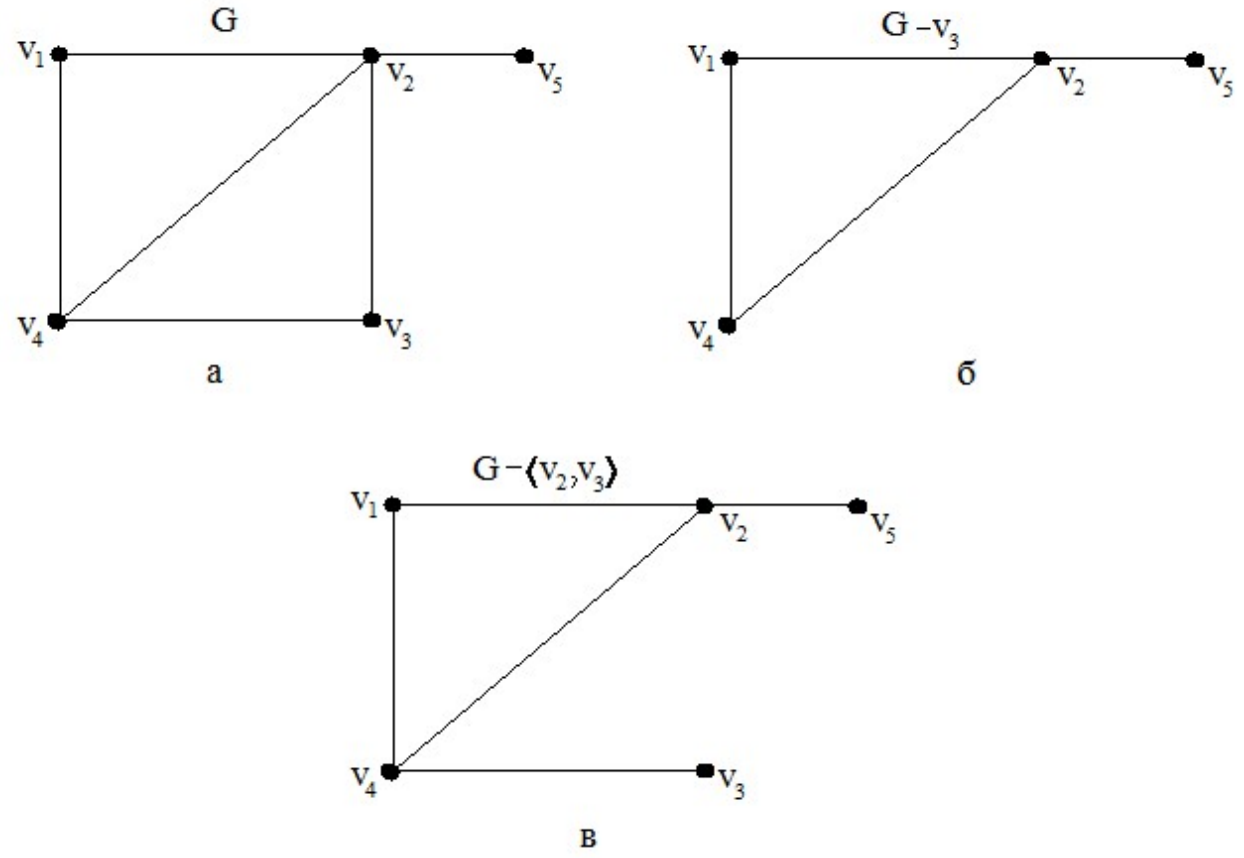


Рис.6.

5. Маршрути, шляхи, ланцюги, цикли

Нехай G - неорієнтований граф.

Маршрутом в графі G називається послідовність

$$v, \{v, w\}, w, \{w, t\}, t, ..., m, \{m, p\}, p$$

вершин і ребер цього графа, яка починається й закінчується вершиною, а кожне ребро послідовності інцидентне двом вершинам, одна з яких безпосередньо передує йому, а інша безпосередньо іде за ним. Зазначений маршрут з'єднує вершини v і p і його можна позначити: $v, w, t, ..., m, p$ (тобто указати послідовність вершин).

Маршрут називається ***замкненим***, якщо $v = p$, тобто початкова й кінцева вершини маршруту співпадають.

Маршрут називається ***ланцюгом***, якщо всі його ребра різні, ***простим ланцюгом***, якщо всі вершини, а отже й ребра, різні.

Замкнений ланцюг називається ***циклом***. Замкнений простий ланцюг називається ***простим циклом***.

Для графа, зображеного на рис.7(а), маршрут $v_1\, v_2\, v_5\, v_2\, v_3$ (рис.7(б)) ланцюгом не є; маршрут $v_1\, v_2\, v_5\, v_4\, v_2\, v_3$ (рис.7(в)) є ланцюгом, але не простим; $v_1\, v_2\, v_5\, v_4$ (рис.7(г)) – простий ланцюг; $v_2\, v_4\, v_5\, v_2$ (рис.7(д)) – простий цикл.

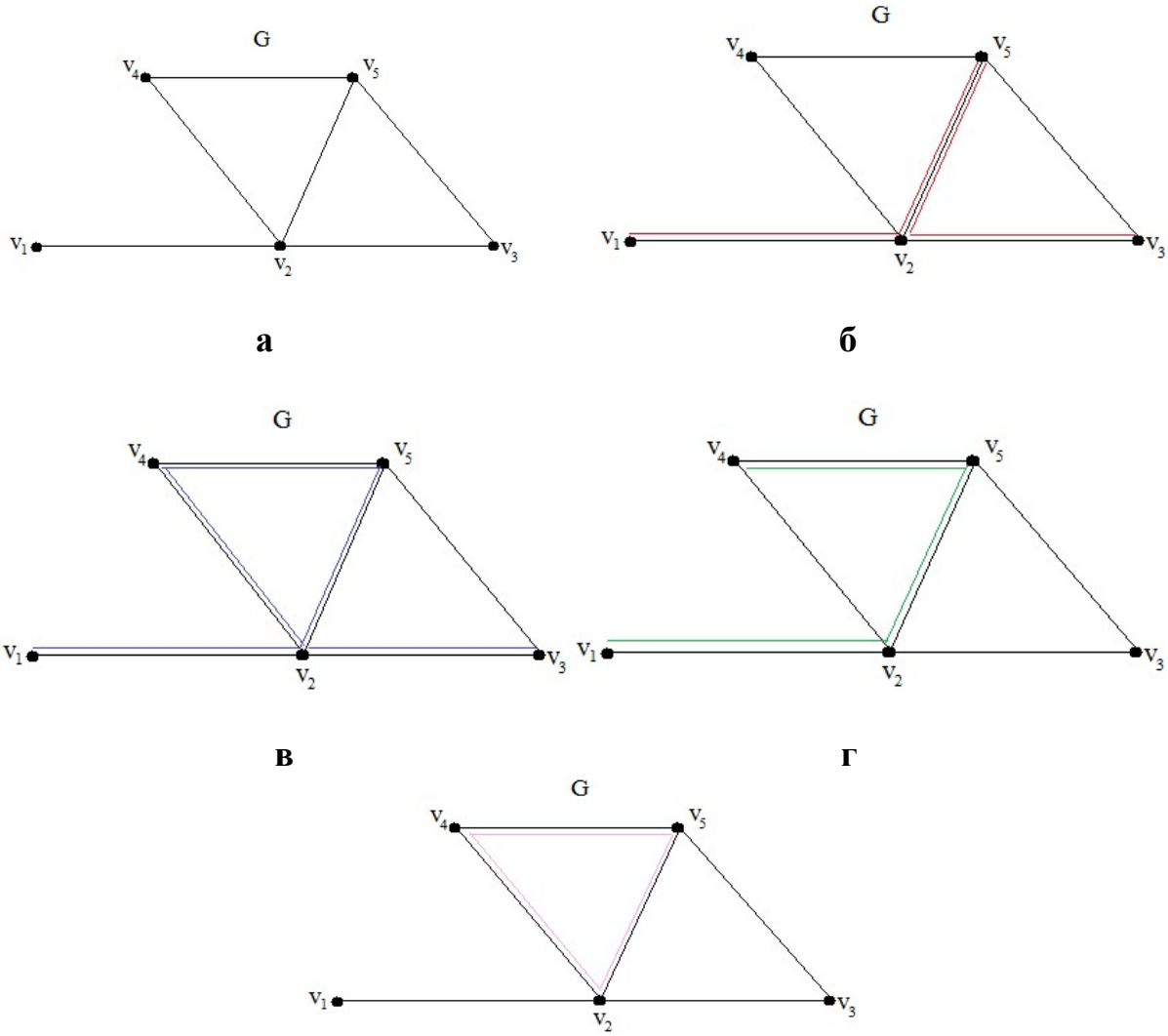


Рис.7.

Нехай G - орієнтований граф.

Шляхом в графі G називається послідовність

$$v, \langle v, w\rangle, w, \langle w, t\rangle, t, ..., m, \langle m, p\rangle, p$$

вершин і орієнтованих ребер цього графа, яка починається й закінчується вершиною, для кожного ребра послідовності попередня йому вершина є його початком, а наступна за ним вершина - його кінцем. Кінець попереднього

ребра співпадає з початком наступного. Зазначений шлях з'єднує вершини v і p і його можна позначити: $v, w, t, ..., m, p$ (тобто указати послідовність вершин).

Шлях називається ***орієнтованим ланцюгом (ланцюгом)***, якщо кожне ребро в ньому зустрічається не більш одного разу, ***простим ланцюгом***, якщо вершини в ньому не повторюються. Замкнений ланцюг називається ***циклом***, простий замкнений ланцюг називається ***простим циклом.***

На рис. 8(а) представлений приклад орієнтованого графу G, для якого послідовність вершин $v_1\ v_2\ v_5\ v_3\ v_2$ шляхом не є, оскільки ребра $\langle v_3, v_2 \rangle$ в графі G немає (рис. 8(б)); послідовність $v_1\ v_2\ v_5\ v_4\ v_2$ - шлях (рис.8(в)); $v_1\ v_2\ v_5\ v_4\ v_2\ v_5$ - є шлях, але не є ланцюгом (рис.8(г)); $v_2\ v_5\ v_4\ v_2\ v_3$ - є ланцюгом, але не простим (рис.8(д)); $v_4\ v_2\ v_5\ v_3$ - простий ланцюг (рис.8(е)).

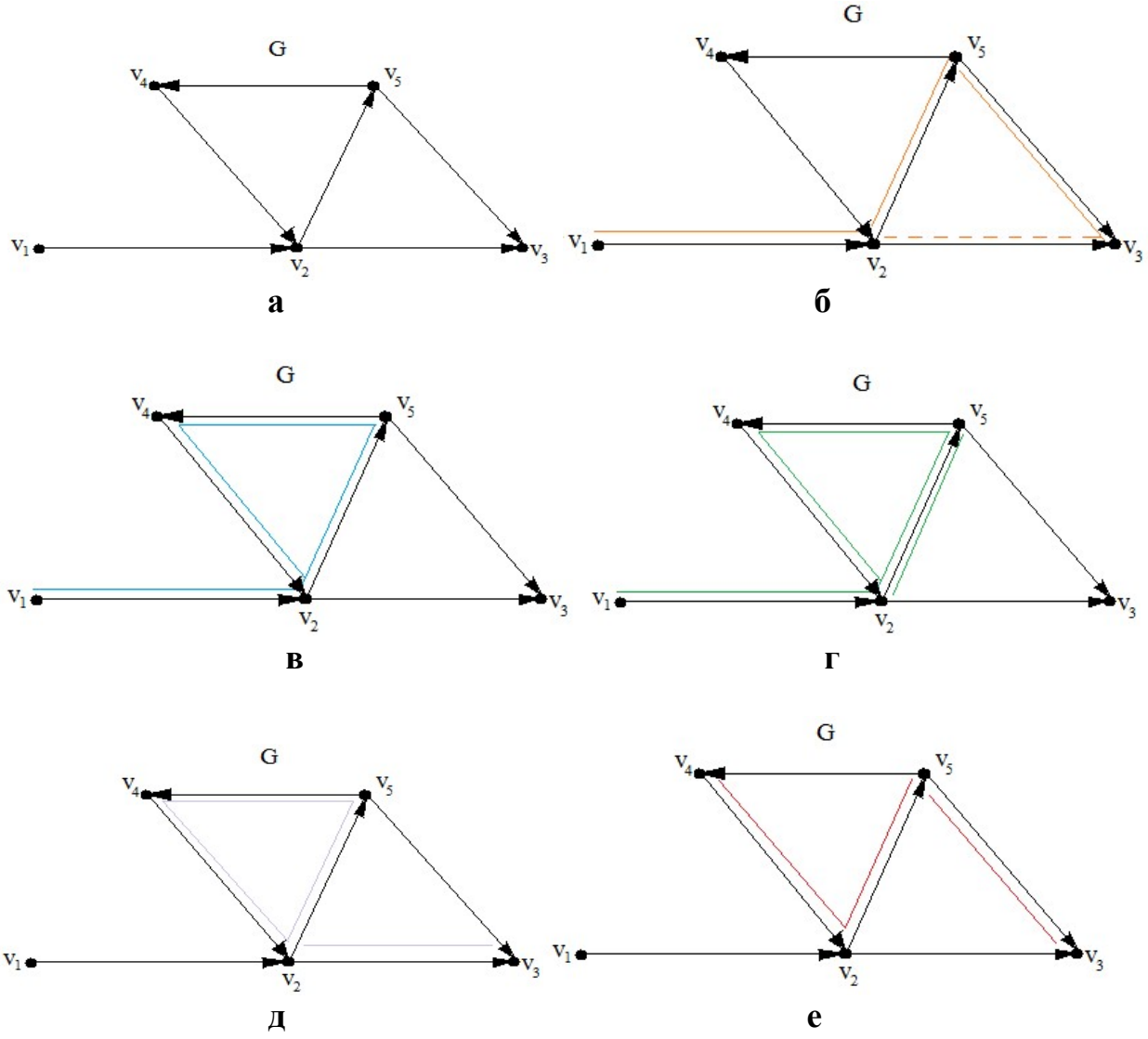


Рис.8.

Граф, який не містить циклів, називається ***ациклічним***.

Число ребер маршруту (шляху) називається його ***довжиною***.

Нехай G - неорієнтований граф. Дві його вершини v_i і v_j називаються ***зв'язаними***, якщо існує маршрут з кінцями у вершинах v_i і v_j.

Граф G називається ***зв'язним***, якщо будь-яка пара його вершин зв'язана.

Відстанню між вершинами v_i і v_j неорієнтованого графа G називається мінімальна з довжин ланцюгів, що з'єднують вершини v_i і v_j.

Питання

1.Яким чином бінарному відношенню ρ, заданому на множині $V = \{v_1, v_2, ..., v_n\}$, ставиться в відповідність орієнтований граф?

2. Як по властивостях відповідних бінарним відношенням графів визначити властивості самих бінарних відношень? Навести приклади.

3. Які два графа називаються ізоморфними? Навести приклади ізоморфних графів, пояснити з чого випливає їхній ізоморфізм.

4. Чим відрізняються між собою ізоморфні графи?

5. Що називається інваріантом графа?

6. Що називається підграфом, надграфом графа? Навести приклади.

7. Який підграф графа називається остовним? Навести приклади.

8. Який підграф графа називається породженим? Навести приклади.

9. Як у графі відбувається видалення вершини, видалення ребра? Навести приклади.

10. Що називається маршрутом у неорієнтованому графі?

11. Який маршрут у неорієнтованому графі називається замкненим?

12. Який маршрут у неорієнтованому графі називається ланцюгом, простим ланцюгом? Навести приклади.

13. Що таке цикл, простий цикл неорієнтованого графа?

14. Що називається шляхом в орієнтованому графі?

15. Що в орієнтованому графі називається ланцюгом, простим ланцюгом? Навести приклади.

16. Що таке цикл, простий цикл орієнтованого графа?

17. Який граф називається ациклічним? Навести приклади.

18. Що називається довжиною маршруту, шляху?

19. Які вершини неорієнтованого графа називаються зв'язаними?

20. Який граф називається зв'язним?

21. Як визначається відстань між вершинами неорієнтованого графа?

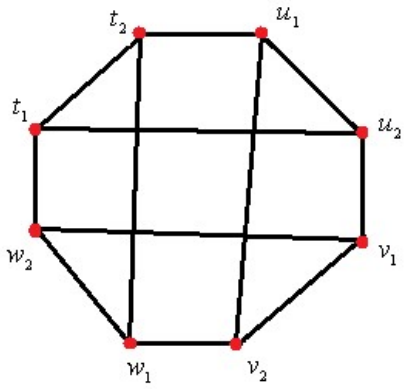
Тема 13. ХАРАКТЕРИСТИКИ ГРАФА

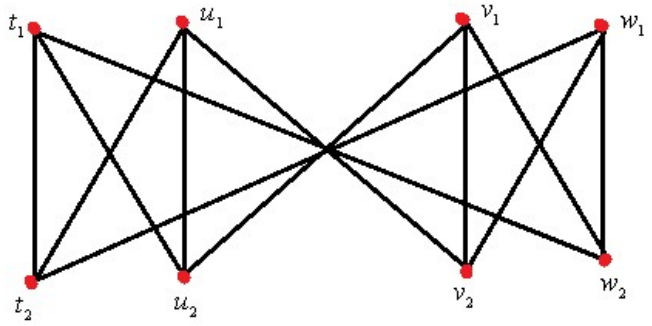
План

1. Поняття дводольного графа. Об'єднання й з'єднання графів.
2. Відношення зв'язаності вершин як відношення еквівалентності.
3. Відстань між вершинами неорієнтованого графа.
4. Зв’язність орієнтованого графа.
5. Дерево. Ліс.

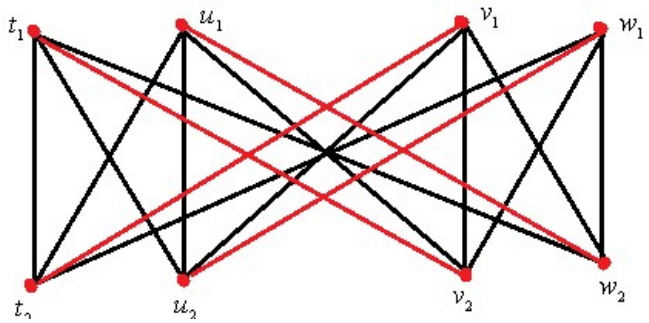
1. Поняття дводольного графа. Об'єднання й з'єднання графів

Граф $G=(V,X)$ називається дводольним, або біграфом, якщо множину його вершин можна розбити на дві підмножини V_1 і V_2 таким чином, що будь-яке ребро графа з'єднує вершини з різних підмножин V_1 і V_2. Будемо казати, що ребра графа $G=(V,X)$ з'єднують множини V_1 і V_2. Наприклад:





Якщо граф містить усі ребра, що з'єднують множини V_1 і V_2, то цей граф називається повним дводольним графом:



Нехай графи G_1 і G_2 мають непересічні множини вершин V_1 і V_2 і непересічні множини ребер X_1 і X_2.

Об'єднанням $G_1 \cup G_2$ таких графів називається граф, множиною вершин якого є $V=V_1 \cup V_2$, а множиною ребер $X=X_1 \cup X_2$.

З'єднання графів G_1+G_2 складається з $G_1 \cup G_2$ і всіх ребер, що з’єднують V_1 і V_2.

2. Відношення зв'язаності вершин як відношення еквівалентності

Нехай G - неорієнтований граф. Будемо вважати, що будь-яка вершина в графі зв'язана із самою собою (навіть при відсутності петлі). Тоді бінарне відношення «бути зв'язаними», задане на множині вершин довільного графа, є відношенням еквівалентності. Дійсно, це відношення рефлексивне, симетричне й транзитивне. У силу цього відношення зв'язаності вершин розбиває всю множину вершин V графа на класи еквівалентності $V_1,...,V_k$: в один клас еквівалентності попадають попарно зв'язані вершини; якщо вершини не є зв'язаними, вони будуть в різних класах, тобто:

$$V = \bigcup_{i=1}^{k} V_i, \quad V_i \bigcap V_j = \varnothing \ при \ i \neq j \ .$$

Підграф графа G, породжений V_i, називається ***зв'язним компонентом*** графа G. На рис.1 граф G три зв'язних компонента: G_1, G_2, G_3, породжені відповідно класами еквівалентності: $V_1 = \{1,2,3\}$, $V_2 = \{4,5\}$, $V_3 = \{6,7,8,9,10,11\}$.

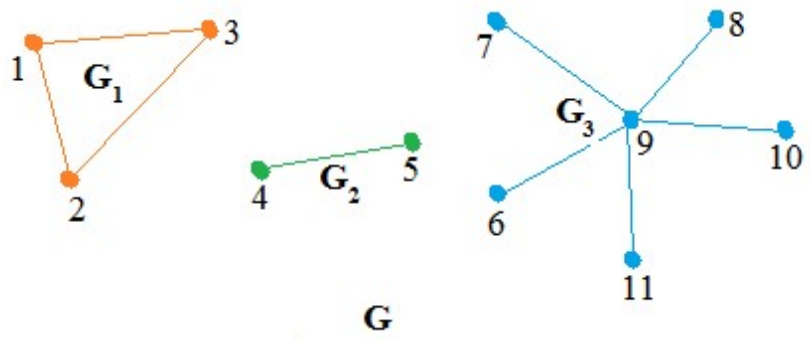


Рис.1.

Ребро графа G, видалення якого приводить до збільшення кількості зв'язних компонентів цього графа, називається ***мостом*** графа. Для графа, представленого на рис.1, ребро $\{9,11\}$ є мостом, оскільки після його видалення кількість зв'язних компонентів збільшиться: стане дорівнювати 4 (рис.2). При цьому одна зі зв'язних компонентів - це одна вершина 11. Ця вершина має ступінь, що дорівнює 0. Така вершина називається ***ізольованою*** вершиною графа.

Вершина, видалення якої із графа приводить до збільшення кількості зв'язних компонентів цього графа, називається ***точкою зчленування*** графа. Для графа, представленого на рис.1, вершина 9 є його точкою зчленування.

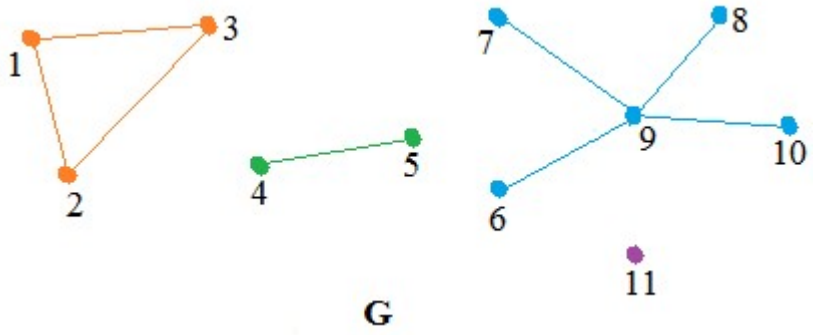


Рис.2.

3. Відстань між вершинами неорієнтованого графа

Розглянемо дві вершини 2 і 7 неорієнтованого графа *G* (рис.3). Ці вершини в графі з'єднано декількома маршрутами, самими короткими з яких є прості ланцюги (вони виділені на рис.3 червоним, синім і зеленим кольором). При цьому ***довжиною маршруту*** називається кількість вхідних у нього ребер. ***Відстанню*** між двома вершинами в графі називається довжина найкоротшого простого ланцюга графа, що з'єднує ці вершини. У розглянутому прикладі відстань між вершинами 2 і 7 дорівнює 3 (довжина ланцюга 2,3,5,7), оскільки довжини інших ланцюгів (2,3,4,5,7 і 2,3,5,6,7) більше трьох: вони дорівнюють 4.

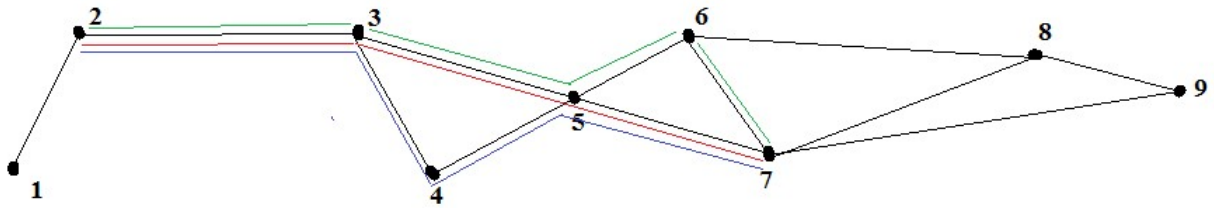


Рис.3.

Ексцентриситетом вершини *v* графа *G* називається найбільша з відстаней від цієї вершини до будь-якої іншої вершини графа. Так для графа, представленого на рис.4, відстані від вершини 1 до вершин 2, 3, 4, 5,6,7 відповідно дорівнюють 1, 2, 3, 3, 4, 4, тобто ексцентриситет вершини 1 дорівнює 4.

Діаметром графа називається максимальна з відстаней між парами його вершин. Діаметр графа дорівнює максимальному ексцентриситету вершин графа.

Для графа, представленого на рис.4, його діаметр дорівнює 4.

Вузли графа, відстань між якими дорівнює діаметру графа, називаються ***периферійними***.

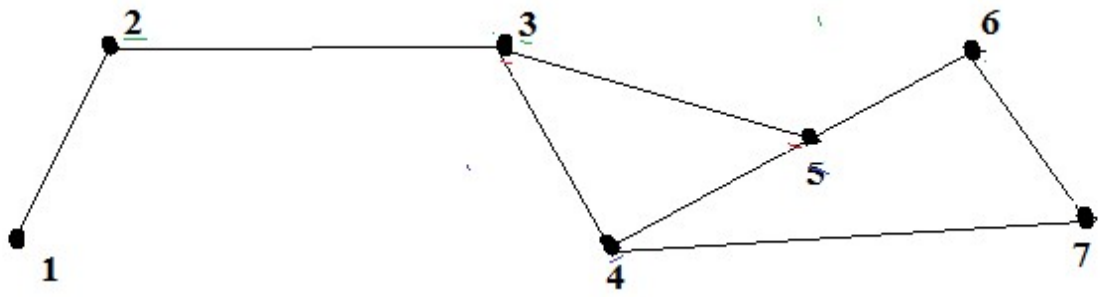
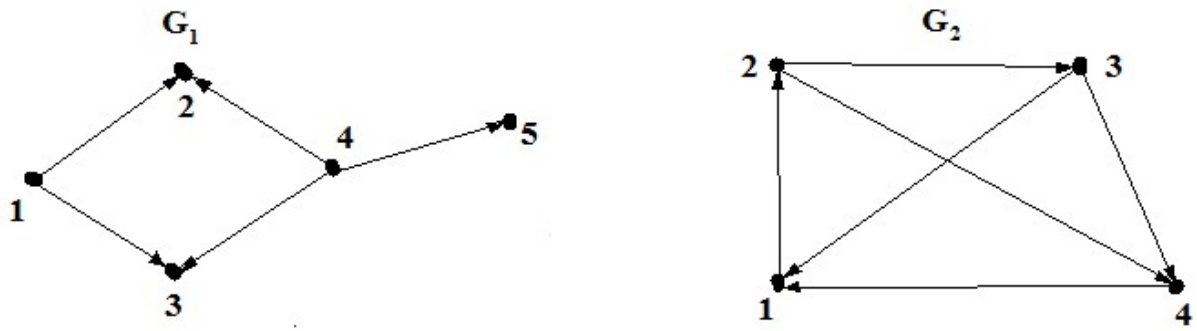


Рис.4.

4. Зв’язність орієнтованого графа

Нехай G - орієнтований граф. Будемо називати його ***зв'язним***, якщо він зв'язний без врахування орієнтації ребер, і ***сильно зв'язним***, якщо з будь-якої його вершини v' в будь-яку вершину v'' існує шлях. На рис.5(а) граф G_1 є зв'язним, оскільки безврахування орієнтованості ребер між будь-якими двома вершинами цього графа існує маршрут, однак цей граф не є сильно зв'язним, оскільки, наприклад, вершини 1 і 4 цього графа не зв'язані ніяким шляхом. На рис.5(б) зображений граф є сильно зв'язним, оскільки будь-які дві вершини цього графа зв'язані шляхом.



а б

Рис.5.

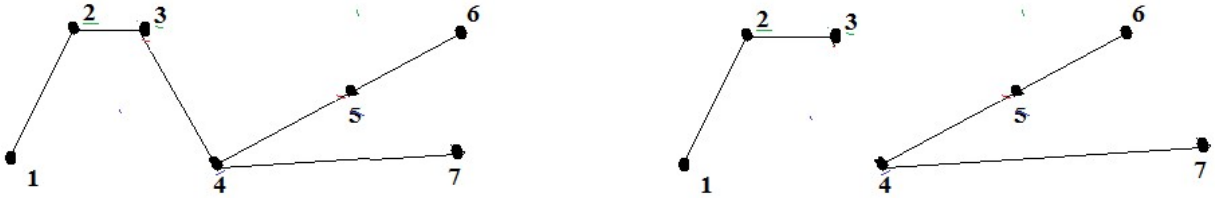
5. Дерево. Ліс

Неорієнтований граф називається ***деревом***, якщо він зв'язний і не містить циклів (а тому не містить петель і кратних ребер) (рис.6(а)). Дерево - це мінімальний зв'язний граф: при видаленні хоча б одного ребра він втрачає зв'язність.

Дерево з n вершинами має $n-1$ ребро. Усі ребра в дереві є мостами.

Лісом називається незв'язний граф без циклів (рис.6(б)). Зв'язні компоненти лісу є деревами.

Вершини дерева, ступінь яких дорівнює одиниці, називаються ***листами*** (або ***висячими вершинами***). На рис.6(а) вершини 1, 6, 7 – листи.



а б

Рис.6.

У дереві будь-які дві вершини зв'язані єдиним ланцюгом.

Питання

1. Який граф $G = (V, X)$ називається дводольним?
2. Який граф називається повним дводольним графом?
3. Що називається об'єднанням графів?
4. Що називається з'єднанням графів?
5. Показати, що відношення зв'язаності вершин є відношенням еквівалентності.
6. Що називається зв'язним компонентом графа?
7. Що називається мостом графа?
8. Що називається точкою зчленування графа?
9. Що називається відстанню між двома вершинами в графі?
10. Що таке ексцентриситет вершини? Діаметр графа?
11. Зв’язність орієнтованого графа.
12. Який граф називається деревом, лісом?

Тема 14. ВИКОРИСТАННЯ ТЕОРІЇ ГРАФІВ ПРИ МОДЕЛЮВАННІ ГРУПИ СУПРОТИВНИКА СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

План

1. Використання зваженого графа при моделюванні групи супротивника, атаки на систему захисту інформації.
2. Використання операцій над графами для моделювання процесу руйнування групи супротивника

1. Використання зваженого графа при моделюванні групи супротивника, атаки на систему захисту інформації

Традиційним шляхом для представлення групи людей із вказівкою взаємних відносин між ними є використання теорії графів. Це обумовлене багатьма факторами, серед яких наочність одержуваної моделі, можливість адекватного відображення за допомогою стандартних операцій на графах реальних дій над групами й подій у групах, існуванням розробленого математичного апарата для роботи із графами, включаючи велику кількість евристичних методів їх обробки, що добре зарекомендували себе на практиці.

У даний момент у науковому світі надзвичайно активізувалася робота з математичного моделювання терористичних організацій і інших типів кримінальних груп, метою яких є, зокрема, несанкціонований доступ до інформації, її підміна й інші неавторизовані дії.

Розглянемо задачі, пов'язані з організацією протидії групам супротивника, розв'язок яких здійснюється з використанням графових математичних моделей супротивника. Окремі індивідууми представляються в такій моделі у вигляді вузлів (вершин), пари яких з'єднуються ребром при існуванні певного взаємозв'язку між відповідними членами розглянутої групи.

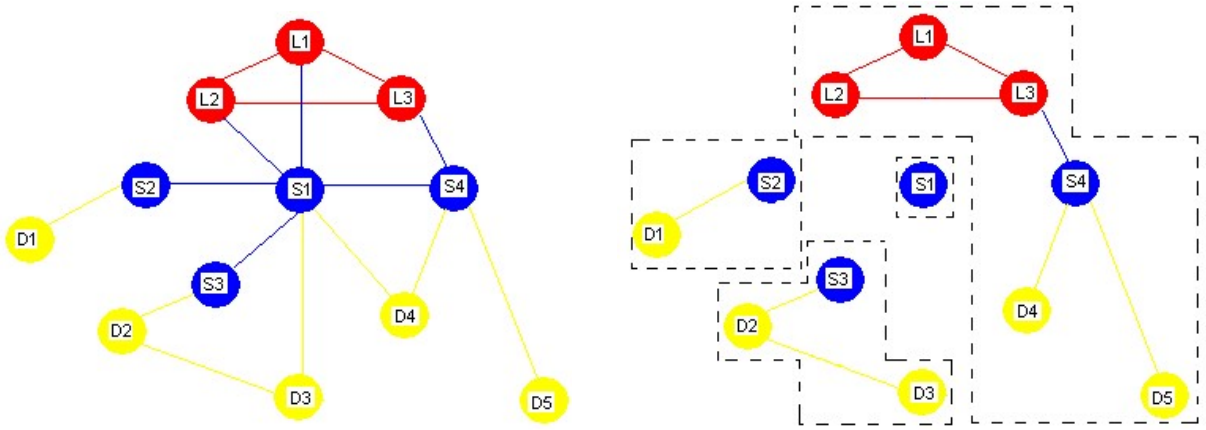
Нехай група супротивника у своїй ієрархії має 3 основних рівня: лідера (керівника) або декількох лідерів, представників з'єднуючої ланки (керівництво на місцях) і безпосередніх виконавців. При побудові найпростішої графової моделі (неорієнтований незважений граф) кожному члену організації супротивника відповідає вершина, ребра графа з'єднують вершини в тому випадку, якщо між відповідними їм членами існує безпосередній зв'язок. Приклад такої моделі представлений на рис.1(а), де вузли, відповідні до лідерів організації, середній ланці й виконавцям, для наочності мають відповідно червоний, синій і жовтий колір. Граф очевидно є зв'язним. Як правило, безпосереднього зв'язку між лідерами й виконавцями не існує, хоча така можливість і не виключається.

Традиційно графові моделі супротивника використовуються для розв'язку наступних задач:

1. Визначення членів групи супротивника, блокування (видалення) яких *реально можливо здійснити*, при цьому блокування приведе до *розпаду* організації супротивника на декілька незв'язаних між собою частин.

Результатом такого розпаду може виявитися як повне знищення групи, так і зниження ефективності її діяльності.

Мовою графів дане завдання буде формулюватися наступним чином: необхідно визначити точку зчленування або множину вузлів (множину, що містить мінімальну кількість вузлів), видалення яких приведе до розпаду зв'язного графа на декілька компонент. У прикладі, наведеному на рис.1(а), точкою зчленування є *S1*. Блокування цього єдиного члена організації супротивника приводить до її розпаду на чотири частини, причому три з них стають «обезголовленими», а тому недієздатними (рис.1(б)). Відмітимо, що таке можливо не завжди.



а б

Рис.1. Приклад графової моделі групи супротивника: (а - первісний вид; б - вид після видалення точки зчленування графа

2. Виділення в організації супротивника таких зв'язків між його членами, видалення яких приводить до розпаду групи на окремі частини, незв'язані між собою, що очевидно значно обмежить можливості діяльності розглянутої структури.

   Мовою графів завдання формулюється наступним чином: визначити множину ребер (мінімальну множину ребер) у графові, видалення яких приведе до його розпаду на декілька компонент.

Для отримання задовільного результату при розв'язку поставлених задач графова модель супротивника повинна мати максимально можливу інформативність, враховувати ієрархію розглянутої групи супротивника. Для цього будемо використовувати в якості моделі супротивника неорієнтований ***зважений*** граф: кожній вершині й кожному ребру такого графа ставиться у відповідність деяке число - вага.

Вага вершини формується, виходячи з апріорних даних про відповідного члена групи супротивника, з врахуванням

а) його поінформованості про об'єкт, на який спрямована увага;

б) матеріальних і часових можливостей для здійснення відведеної даному члену групи ролі (в операції здійснення несанкціонованого доступу до інформації);

в) значимості розглянутого члена в групі.

Врахування усіх перерахованих вище складових частин вагових коефіцієнтів автоматично виділить лідерів (вершини з найбільшими значеннями ваг) і інших менш значимих членів групи.

Вага ребра визначається залежно від

а) реальної цінності інформації, що передається за допомогою даної лінії зв'язку (наприклад, інформація, передана від керівників групи підлеглим, є більш значимою, чим інформація, що циркулює між безпосередніми виконавцями);

б) надійності розглянутої лінії зв'язку (наприклад, зв'язок при безпосередньому контакті є більш надійним, чим при використанні телефонної лінії).

Приклад зваженого графа-моделі наведений на рис.2 (порядок нумерації відповідає ієрархії членів організації, у середині вузла - його номер, поруч із вузлом - його вага, поруч із ребром у дужках - вага ребра).

2.Використання операцій над графами для моделювання процесу руйнування групи супротивника

Задачі 1,2 були сформульовані в загальному виді. Результат видалення деяких членів групи або блокування якихось зв'язків, що приводить до її розпаду на окремі підгрупи, у реальності може виявитися зовсім незначним з погляду зниження дієздатності супротивника. Наприклад, якщо зруйнувати зв'язок між членами S4 і D5 (міст у графовій моделі супротивника (рис.1(а))), це чи навряд нанесе відчутний удар по всій групі, тому що частина, що залишилася без D5, збереже як абсолютну більшість своїх членів, так і наявність усіх ієрархічних ланок.

Одним з основних питань при моделюванні груп супротивника й активних дій над ними є питання про те, коли розглянуту структуру можна вважати зруйнованою, або знищеною.

Розглянемо можливий розв'язок для задачі 1. Для розв'язку цієї задачі по графовій моделі групи визначається множина усіх простих, або «командних», ланцюгів, початок і кінець яких відповідає лідерові й безпосередньому виконавцеві відповідно. По отриманій множині визначається сукупність вузлів графа, кожний з яких є присутнім хоча б в одному ланцюзі, причому кожний ланцюг вносить у цю сукупність єдиний вузол. Видалення із графа такої сукупності (cutset), зруйнує в ньому всі існуючі «командні» ланцюги. У цьому випадку робиться висновок про знищення групи супротивника.

Розглянемо можливий алгоритм для здійснення руйнування групи супротивника, використовуючи в якості моделі запропонований вище зважений неорієнтований граф. Для цього побудуємо для графа-моделі кореневу структуру рівнів (КСР) з коренем у вузлі, що має найбільшу вагу, тобто, що відповідає лідерові (варіант, коли значення максимальної ваги

відповідає декільком вершинам, розглядається нижче). Для зручності подальшого викладу позначимо цей вузол x. КСР $\Im(x)$ є розбивка множини вершин V графа:

$$\Im(x) = \{L_0(x), L_1(x), ..., L_{l(x)}(x)\},$$

така, що $L_0(x) = \{x\}, L_1(x) = Adj(L_0(x)), L_i(x) = Adj(L_{i-1}(x)) - L_{i-2}(x)$, $i = 2,3,...,l(x)$, де $Adj(L_{i-1}(x))$- множина вузлів графа, що не належать $L_{i-1}(x)$, але суміжних хоча б з одним вузлом з $L_{i-1}(x)$. Ексцентриситет $l(x)$ вузла x стосовно структури рівнів називається довжиною $\Im(x)$, а ширина $w(x)$ структури $\Im(x)$ визначається як

$$w(x) = \max\{|L_i(x)| \,|\, 0 \le i \le l(x)\}.$$

Для графа, представленого на рис.2, коренева структура рівнів, описана вище, буде мати вигляд, представлений на рис.3.

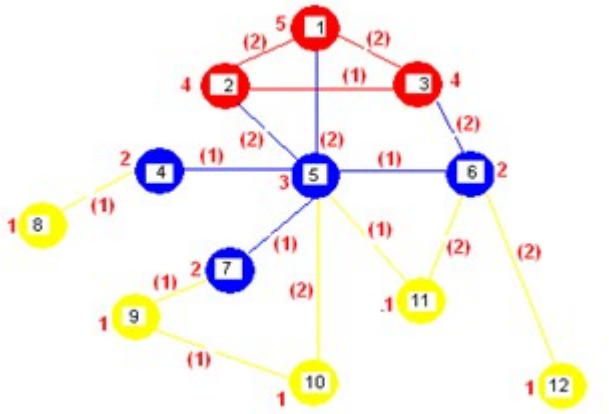


Рис.2. Модель групи супротивника у вигляді зваженого графа

Усі «командні» ланцюги - це очевидно прості ланцюги графа, що виходять із нульового рівня кореневої структури й закінчуються або вершиною, ступінь якої дорівнює 1, або вершиною, що лежить в останньому рівні КСР; якщо v_k, v_m - дві послідовні вершини такого ланцюга, то номер рівня в КСР, що містить v_k, не більше номера рівня, у який потрапила вершина v_m. Вузли, що потрапили в один рівень структури, визначать ту сукупність, видалення якої приведе до розпаду графа на компоненти за рахунок розриву всіх ланцюгів зв'язку, тобто до блокування групи супротивника. Спосіб побудови КСР приведе до того, що лідери будуть «відрізані» від безпосередніх виконавців, що позбавить можливості організованих активних дій дану групу.

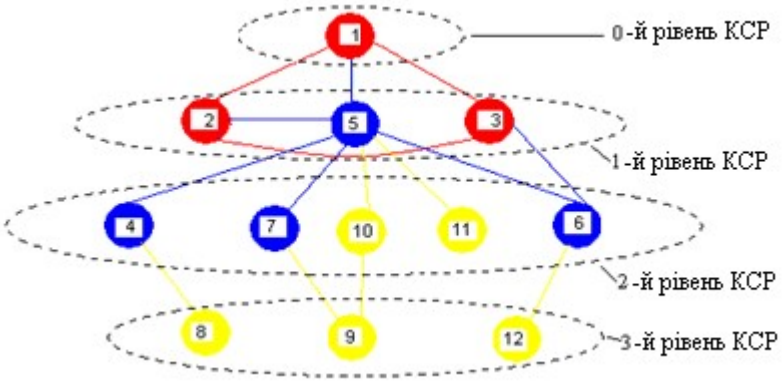


Рис.3. Коренева структура рівней

Нехай є кілька вершин з максимальною вагою. Тоді при побудові КСР роль «кореня» буде відігравати не один вузол: усі вершини графа з максимальними ваговими значеннями, що відповідають лідерам супротивника, розміщуються на нульовому рівні структури. Інші кроки для виділення відокремлюючої множини графа залишаються без зміни.

Вузли якого рівня вибрати, щоб завдати більшої шкоди групі супротивника при блокуванні відповідних членів?

Для чисельної оцінки збитку, що завдається кримінальному угрупованню, скористаємося матрицею суміжності графа-моделі. Для графа, представленого на рис.2, ця матриця має вигляд:

$$PROT = \begin{matrix} 5 & 2 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 4 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 1 & 3 & 1 & 1 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 1 & 1 & 0 & 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}$$

(на головній діагоналі - вагові коефіцієнти вершин, позадіагональні елементи - вагові коефіцієнти ребер). У силу неорієнтованості графа матриця є симетричною. Вона повністю визначає граф, а тому характеризує всю групу супротивника. Кожна з характеристик такої матриці є характеристикою й реальної людської групи.

Назвемо ***ваговою енергією групи супротивника*** (E_{tr})енергію сигналу, цифровим представленням якого є матриця суміжності графової моделі супротивника:

$$E_{tr} = \|PROT\|^2,$$

де $\|\bullet\|$- евклідова матрична норма. Виключення певного члена групи (певної вершини графа разом з інцидентними ребрами) для матриці суміжності буде виражатися у видаленні з неї рядка й стовпця, номера яких відповідають номеру виключеної вершини. Енергію групи після виключення з неї членів $x_{k_1}, x_{k_2}, ..., x_{k_p}$ будемо позначати $E_{tr}(x_{k_1}, x_{k_2}, ..., x_{k_p})$. Цей числовий показник буде використовуватися для порівняння результатів передбачуваного блокування тих або інших членів групи супротивника. Залежно від підсумків порівняння робиться висновок про доцільність блокування конкретної сукупності членів групи.

Звичайно, такий алгоритм не гарантує відокремлення лідерів від безпосередніх виконавців, але розбивка на зв'язні компоненти в кожному разі приведе до ослаблення групи й потребує певного часу на її відновлення.

Питання

1. Чим обумовлене традиційне використання теорії графів для представлення групи людей із вказівкою взаємних відносин між ними?
2. Як будується граф, що представляє модель групи людей?
3. Для розв'язку яких задач традиційно використовуються графові моделі супротивника?
4. Що таке зважений граф?
5. Як визначається вага вершини, ребра в графовій моделі групи супротивника?
6. Як операції над графами використовуються для моделювання процесу руйнування групи супротивника?
7. Що таке коренева структура рівней графа?
8. Що таке вагова енергія групи супротивника?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА ТА ІНШІ ДЖЕРЕЛА

Базова

1. Дискретна математика : підручник / Ю. В. Нікольський, В.В. Пасічник, Ю. М. Щербина ; за наук. ред. д-ра техн. наук, проф. В. В. Пасічника. – 7-ме видання, випр. та допов. – Львів : ПП "Магнолія 2006"; ЛНУ ім. Івана Франка, 2024. – 432 с.
2. Дискретна математика: навчальний посібник для студентів закладів вищої освіти/ М.П. Богдан, Л.В.Васильєва. – Краматорськ: ДДМА, 2019. – 80 с.
3. Oscar Levin. Discrete Mathematics: An Open Introduction - 4th Edition. University of Northern Colorado, 2024. – 527 p.
4. Коцовський В. М. Основи дискретної математики: навчальний посібник. Ужгород: ПП «АУТДОР-ШАРК», 2020. 128 с.
5. Клесов, О. І. Елементарна теорія чисел та елементи криптографії [Електронний ресурс] : підручник / О. І. Клесов. – Електронні текстові дані (1 файл: 5,35 Мбайт). – Київ : ТВіМС, 2016. – 412 с.
6. Скасків Л. В. Теорія чисел та основні структури сучасної математики : навчальний посібник / Л. В. Скасків. – Ірпінь : Університет ДФС України, 2021. – 70 с.
7. Елементи теорії чисел: навч. посіб. /О.І.Оглобліна, С.Сушко, Ю.В.Шрамко. – Суми: Сумський державний університет, 2015. – 186 с.

Допоміжна

8. Кобозєва, А.А. Аналіз захищеності інформаційних систем / А.А.Кобозєва, В.О.Хорошко, І.О.Мачалін. – К.: Вид. ДУІКТ, 2010. – 316 с.
9. Трохимчук, М.С.Нікітченко. Дискретна математика у прикладах і задачах

Інтернет ресурси

1. http://window.edu.ru/resource/869/44869
2. https://www.ukma.edu.ua/~bogd/Discrete%20Mathematics/PosibnykNew.pdf
3. http://uareferats.com/index.php/book/details/14