Міністерство освіти та науки України
Національний технічний університет України
«Київський політехнічний інститут»
Навчально-науковий комплекс
«Інститут прикладного системного аналізу»

ДИСКРЕТНА МАТЕМАТИКА

частково впорядковані множини, решітки, булеві алгебри

Для студентів математичних спеціальностей університетів

Київ 2009

Книга є навчальним посібником для студентів математичних спеціальностей університетів і відповідає навчальній програмі з дисципліни «Дискретна математика». Посібник містить теоретичні відомості з основних розділів дискретної математики і орієнтований для студентів 1-2 курсів, які володіють базовими поняттями лінійної алгебри та математичного аналізу.

Міністерство освіти та науки України
Національний технічний університет України
«Київський політехнічний інститут»
Навчально-науковий комплекс
«Інститут прикладного системного аналізу»

ДИСКРЕТНА МАТЕМАТИКА

Частково впорядковані множини, решітки, булеві алгебри

Для студентів математичних спеціальностей університетів

Затверджено
на засіданні кафедри
математичних методів
системного аналізу

Протокол №?? від ????????????? року

Київ 2009

Навчальний посібник з дисципліни «Дискретна математика». Автори: І.Спекторський, О.Стусь - К.: НТУУ «КПІ», ННК «ІПСА», 2009. - 136 с.

Навчальне видання

Дискретна математика

Частково впорядковані множини, решітки, булеві алгебри

Для студентів математичних спеціальностей університетів

Відповідальний редактор: Романенко Віктор Демидович

Зміст

Вступ

«Дискретна математика» – одна з основних фундаментальних дисциплін у загальнонауковій підготовці студентів за спеціальностями 7.080203 «Системний аналіз і управління», 7.080204 «Соціальна інформатика» та 7.080404 «Інтелектуальні системи прийняття рішень». Курс дискретної математики є базовим для таких дисциплін, як «Теорія ймовірностей та математична статистика», «Спеціалізовані мови програмування», «Експертні системи» та інших. Під час вивчення курсу використовують основні визначення та теореми дисциплін «Математичний аналіз» та «Лінійна алгебра».

У навчальному посібнику подано теоретичний матеріал за розділами «Частково впорядковані множини та решітки», «Булеві алгебри» та «Булеві функції. Критерій функціональної повноти». Матеріал, згідно з робочою програмою дисципліни «Дискретна математика», розраховано на викладання протягом п'яти лекцій.

Означення та теореми проілюстровано прикладами. Прості твердження та твердження, що можуть бути доведені за аналогією, запропоновано як вправи для самостійної роботи.

Послідовність і стиль подання матеріалу повністю відповідають робочій програмі та задовольняють потреби суміжних математичних і прикладних дисциплін.

Розділ 1

Частково впорядковані множини

1.1. Основні поняття

Як один із основних об'єктів розглянемо частково впорядковану множину (ЧВМ), тобто пару $\langle \mathcal{A}, \preccurlyeq \rangle$, де $\mathcal{A}$ – непорожня множина, «$\preccurlyeq$» – відношення часткового порядку на $\mathcal{A}$ [1].

Поняття «відношення часткового порядку» (зазвичай вживають термін «відношення порядку») вважаємо цілком зрозумілим. Далі у цій главі розглянемо інші фундаментальні поняття, які або вже відомі, або є дуже простими і не потребують додаткових пояснень.

Позначення $a \preccurlyeq b$ є лише зручним скороченням для позначення $(a, b) \in R$, де $R \subset (\mathcal{A} \times \mathcal{A})$ – відношення порядку, задане на множині $\mathcal{A}$.

Якщо $a \preccurlyeq b$ ($b \succcurlyeq a$) для $a, b \in \mathcal{A}$, то говорять, що елемент a *передує* (*нестрого передує*) елементу b, або елемент b *слідує* (*нестрого слідує*) за елементом a.

Поряд із нестрогим передуванням (слідуванням) природним чином вводять відношення «$\prec$» *строгого передування* та відношення «$\succ$» *стро-*

гого слідування. Відношення «$\prec$» та «$\preccurlyeq$» пов'язані одне з одним співвідношеннями

$$(x \prec y) \Leftrightarrow ((x \preccurlyeq y) \wedge (x \neq y)); \qquad (x \preccurlyeq y) \Leftrightarrow ((x \prec y) \vee (x = y)).$$

Елементи $a, b \in \mathcal{A}$ називають *порівнянними*, якщо $a \preccurlyeq b$ або $b \preccurlyeq a$. Якщо будь-які два елементи ЧВМ $\langle \mathcal{A}, \preccurlyeq \rangle$ порівнянні, множину $\mathcal{A}$ називають *лінійно впорядкованою множиною* або *ланцюгом*.

Означення 1.1. Говорять, що елемент $a \in \mathcal{A}$ безпосередньо передує елементу $b \in \mathcal{A}$ (b безпосередньо слідує за a), якщо

$$\nexists x \in \mathcal{A}\colon a \prec x \prec b.$$

Приклад 1.1. 1. У ЧВМ $\langle \mathbb{N}, \leqslant \rangle$ елемент $a \in \mathbb{N}$ безпосередньо передує елементу $b \in \mathbb{N}$ тоді і тільки тоді, коли $b = a + 1$. Так, елемент 2 безпосередньо передує елементу 3, але не елементу 4.

2. У ЧВМ $\langle \mathbb{R}, \leqslant \rangle$ безпосереднє передування неможливе, оскільки для кожної пари $a < b$ знайдеться $x \in \mathbb{R}$, такий, що $a < x < b$ (достатньо взяти $x = (a + b)/2$).

3. На множині $\mathbb{N}$ розглянемо відношення подільності:

$$(a \preccurlyeq b) \Leftrightarrow (b \,\vdots\, a),$$

тобто a передує b тоді і тільки тоді, коли b ділиться на a.

Відношення подільності на множині натуральних чисел рефлексивне, антисиметричне і транзитивне, а отже, справді є відношенням часткового порядку. Легко зрозуміти, що у ЧВМ $\langle \mathbb{N}, \vdots \rangle$ елемент a безпосередньо передує елементу b тоді і тільки тоді, коли $b = pa$, де p – просте число.

Зауваження 1.1. Дуже часто відношення порядку «$\preccurlyeq$» природне для множини $\mathcal{A}$: «$\leqslant$» на числових множинах, відношення «$\subset$» на множинах множин тощо. У таких випадках, посилаючись на ЧВМ, відношення порядку не вказують; так, говорять «частково впорядкована множина $\mathbb{R}$» замість «частково впорядкована множина $\langle \mathbb{R}, \leqslant \rangle$».

1.1.1. Принцип дуальності для частково впорядкованих множин

Сформулюємо у вигляді вправи простий результат, покладений в основу принципу дуальності.

Вправа 1.1. Якщо $R \subset (\mathcal{A} \times \mathcal{A})$ – відношення порядку, то обернене відношення $R^{-1} \subset (\mathcal{A} \times \mathcal{A})$ також є відношенням порядку.

Відношення слідування «$\succcurlyeq$», за визначенням, обернене до відношення передування «$\preccurlyeq$», а отже, за результатом вправи 1.1, є відношенням порядку. Отже, з кожною ЧВМ $\langle \mathcal{A}, \preccurlyeq \rangle$ пов'язана *дуальна* ЧВМ $\langle \mathcal{A}, \succcurlyeq \rangle$:

$$\langle \mathcal{A}, \preccurlyeq \rangle^* = \langle \mathcal{A}, \succcurlyeq \rangle\,; \quad a \preccurlyeq^* b \Leftrightarrow a \succcurlyeq b \Leftrightarrow b \preccurlyeq a.$$

Очевидно, що «двічі дуальна» ЧВМ $\langle \mathcal{A}, \preccurlyeq \rangle^{**}$ (дуальна до дуальної) збігається з вихідною ЧВМ. Інакше кажучи, якщо ЧВМ $\langle \mathcal{A}, \preccurlyeq \rangle^*$ дуальна до $\langle \mathcal{A}, \preccurlyeq \rangle$, то $\langle \mathcal{A}, \preccurlyeq \rangle$ також дуальна до $\langle \mathcal{A}, \preccurlyeq \rangle^*$ (до вказаних ЧВМ іноді застосовуватимемо термін «взаємодуальність»).

Приклад 1.2. До ЧВМ $\langle \mathbb{N}, \leqslant \rangle$ дуальною є $\langle \mathbb{N}, \geqslant \rangle$. Якщо $a < b$, то a передує b у сенсі $\langle \mathbb{N}, \leqslant \rangle$, але у дуальній ЧВМ елемент b передує a.

У теорії ЧВМ часто використовують *принцип дуальності*: якщо правдиве деяке твердження, сформульоване у термінах, пов'язаних з відношенням «$\preccurlyeq$», то справджується також дуальне твердження, яке отримують із вихідного заміною відношення «$\preccurlyeq$» на відношення «$\succcurlyeq$».

Коректність принципу дуальності обґрунтовується тим фактом, що доведення дуального твердження можна отримати з доведення вихідного твердження заміною «$\preccurlyeq$» на «$\succcurlyeq$», тобто переходячи до дуальної ЧВМ.

Зауважимо, що у складних випадках слід явно виписати формулювання та доведення дуального твердження, замінивши у вихідному твердженні та його доведенні «$\preccurlyeq$» на «$\succcurlyeq$».

Принцип дуальності часто допомагає встановити додаткові взаємозв'язки між термінами, оскільки дуже багато понять у теорії ЧВМ формулюються «дуальними парами»; для формулювання дуальних тверджень достатньо замінити такі терміни на відповідні дуальні.

Конкретні приклади використання принципу дуальності зустрічаються далі у формулюванні означень та доведенні тверджень різного рівня складності.

1.1.2. Діаграми Гессе

Нехай $\langle \mathcal{A}, \preccurlyeq \rangle$ – скінченна ЧВМ, тобто $A = \{a_1, a_2, \ldots, a_n\}$. У цьому випадку для зображення впорядкування часто використовують графи спеціального вигляду:

- граф містить n вершин, які відповідають елементам a_1, a_2, ..., a_n;
- вершини a_i та a_j з'єднують ребром тоді і тільки тоді, коли елемент a_i безпосередньо передує елементу a_j;
- якщо $a_i \prec a_j$, вершину a_j розташовують на площині вище за a_i.

Зрозуміло, що описані умови однозначно задають відношення порядку. Такий граф називають діаграмою *Гессе*[1] частково впорядкованої множини $\langle \mathcal{A}, \preccurlyeq \rangle$.

Приклад 1.3. Нехай $n \in \mathbb{N}$, $\mathcal{L}_n = \{k \in \mathbb{N} : n \vdots k\}$ ($\mathcal{L}_n$ – множина натуральних дільників фіксованого числа n). Множина $\mathcal{L}_n$ частково впорядкована за відношенням подільності «$\vdots$». Діаграми Гессе множини $\langle \mathcal{L}_n, \vdots \rangle$ для різних значень n зображено на рис. 1.1.

[1] Людвиг Отто Гессе (1811–1874) – німецький математик, автор фундаментальних робіт у галузі диференціальної геометрії та варіаційного числення; у цих працях використовував інваріантний визначник із других похідних, який нині називають гессіаном.

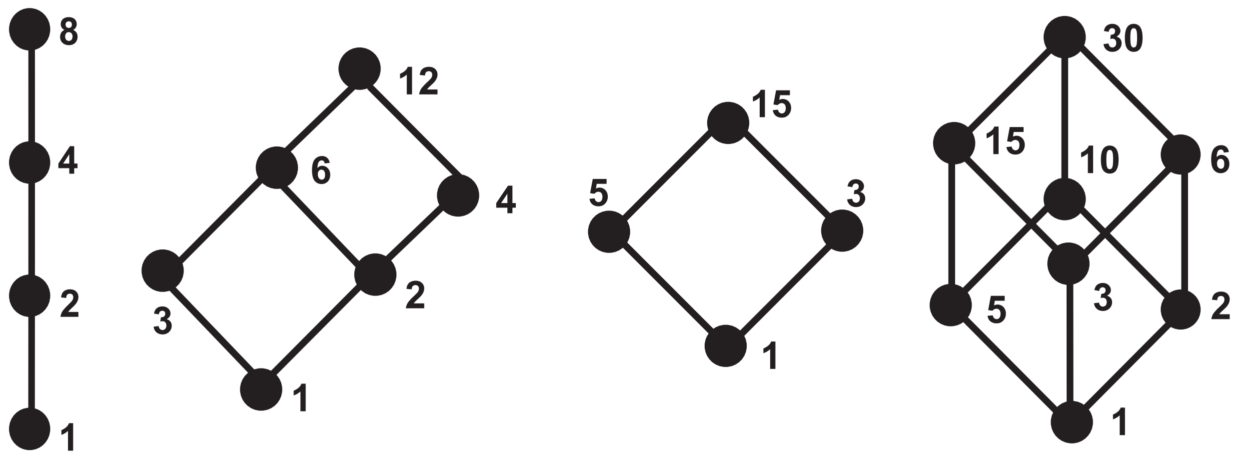


Рис. 1.1. Діаграми Гессе множини $\langle \mathcal{L}_{\mathbf{n}}, \vdots \rangle$ для $n = 8;\ 12;\ 15;\ 30$

Приклад 1.4. Розглянемо ЧВМ

$$\{\{1,2,3,4,5\},\{1,2,3,5\},\{1,2,4,5\},\{1,5\},\{2,5\},\varnothing\},$$

де $(A \preccurlyeq B) \Leftrightarrow (A \subset B)$.

Елементами цієї множини є шість множин, між якими встановлено класичне часткове впорядкування «бути підмножиною». Відповідну діаграму Гессе зображено на рис. 1.2.

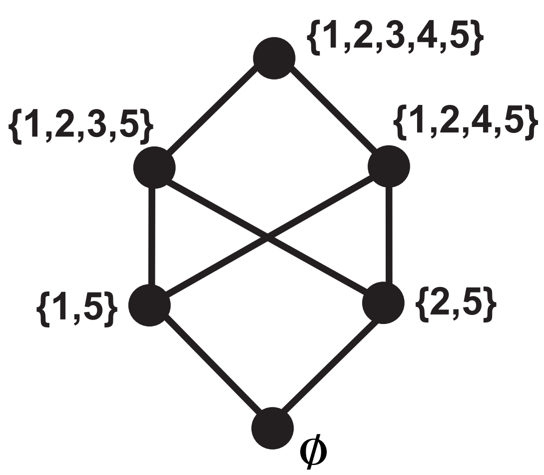


Рис. 1.2. Діаграма Гессе множини $\{\{1,2,3,4,5\},$ $\{1,2,3,5\},\{1,2,4,5\},\{1,5\},\{2,5\},\varnothing\}$

Очевидно, що діаграма Гессе дуальної ЧВМ є «вертикальним віддзеркалюванням» діаграми вихідної ЧВМ (рис. 1.3).

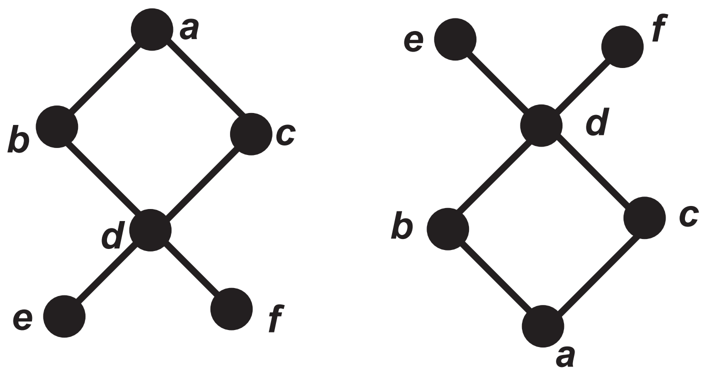


Рис. 1.3. Приклад діаграм Гессе взаємодуальних ЧВМ

1.1.3. Максимальні і мінімальні елементи

Нехай $\langle \mathcal{A}, \preccurlyeq \rangle$ – довільна ЧВМ, $B \subset \mathcal{A}$, $B \neq \varnothing$.

Означення 1.2. Елемент $M \in B$ називають максимальним для множини B, якщо

$$\forall x \in B\colon (x \succcurlyeq M) \Rightarrow (x = M).$$

Елемент $m \in B$ називають мінімальним для множини B, якщо

$$\forall x \in B\colon (x \preccurlyeq m) \Rightarrow (x = m).$$

Поняття максимального та мінімального елемента взаємодуальні: якщо елемент максимальний (мінімальний) для підмножини B деякої ЧВМ $\langle \mathcal{A}, \preccurlyeq \rangle$, то у відповідній дуальній ЧВМ $\langle \mathcal{A}, \succcurlyeq \rangle$ цей елемент буде для B мінімальним (максимальним).

Зауваження 1.2. Максимальність елемента $M \in B$ еквівалентна умові

$$\forall x \in B\colon (x \preccurlyeq M) \text{ або } (x \text{ та } M \text{ непорівнянні}).$$

Аналогічно, мінімальність елемента $m \in B$ еквівалентна умові

$$\forall x \in B\colon (x \succcurlyeq m) \text{ або } (x \text{ та } m \text{ непорівнянні}).$$

Приклад 1.5. 1. Розглянемо ЧВМ $\mathcal{A} = \{a, b, c, d, e, f, g\}$ з діаграмою Гессе, зображеною на рис. 1.4.

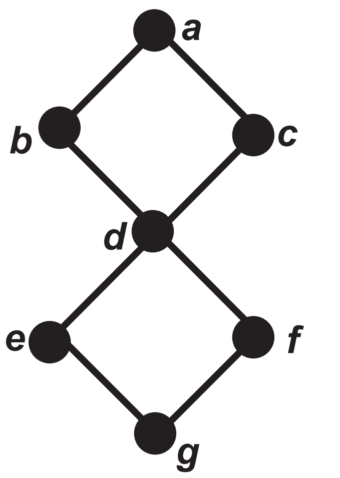


Рис. 1.4

Підмножина $B_1 = \{a, b, c\}$ містить один максимальний елемент a та два мінімальних елементи b і c.

Підмножина $B_2 = \{b, d, e\}$ містить один максимальний елемент b та один мінімальний елемент e.

У підмножині $B_3 = \{e, f\}$ обидва елементи є одночасно і мінімальними, і максимальними.

Сама множина $\mathcal{A} = \{a, b, c, d, e, f, g\}$ (як підмножина самої себе) містить один максимальний елемент a та один мінімальний елемент g.

2. Розглянемо ЧВМ $\langle \mathbb{Z}, \leqslant \rangle$. Підмножина $\mathbb{N}$ містить один мінімальний елемент 1 і не містить максимальних. Сама множина $\mathbb{Z}$ не містить ані жодного мінімального елемента, ані жодного максимального.

Наведений приклад показує, що задана підмножина B може містити один або декілька максимальних та один або декілька мінімальних елементів, може містити максимальні елементи і не містити мінімальних (або навпаки), і може взагалі не містити ані максимальних елементів, ані мінімальних.

Приклад 1.6. Для множини натуральних чисел $\mathbb{N}$ у ЧВМ $\langle \mathbb{R}, \leqslant \rangle$ елемент 1 мінімальний, максимальних елементів немає; у дуальній ЧВМ $\langle \mathbb{R}, \geqslant \rangle$ для множини $\mathbb{N}$ елемент 1 максимальний, мінімальних елементів немає.

Вправа 1.2. Довести, що будь-яка непорожня скінченна $B \subset A$ містить принаймні один максимальний і принаймні один мінімальний елементи.

1.1.4. Найбільші і найменші елементи

Нехай $\langle \mathcal{A}, \preccurlyeq \rangle$ – довільна ЧВМ, $B \subset \mathcal{A}$, $B \neq \varnothing$.

Означення 1.3. Елемент $M \in B$ називають найбільшим для множини B, якщо

$$\forall x \in B \colon (x \preccurlyeq M).$$

Елемент $m \in B$ називають найменшим для множини B, якщо

$$\forall x \in B \colon (x \succcurlyeq m).$$

Поняття найбільшого та найменшого елемента взаємодуальні: якщо елемент є найбільшим (найменшим) для підмножини B деякої ЧВМ $\langle \mathcal{A}, \preccurlyeq \rangle$, то у відповідній дуальній ЧВМ $\langle \mathcal{A}, \succcurlyeq \rangle$ цей елемент буде для B найменшим (найбільшим).

На відміну від максимального та мінімального елементів (див. зауваження 1.2), найбільший та найменший елементи для множини $B \subset \mathcal{A}$ мають бути порівнянними з кожним елементом із B.

Очевидно, що у ланцюзі $\mathcal{A}$ поняття «найбільший» і «максимальний» («найменший» і «мінімальний») збігаються для будь-якої підмножини $B \subset \mathcal{A}$, оскільки в ланцюзі всі елементи попарно порівнянні. Проте, як показує приклад 1.7, для довільних ЧВМ поняття «найбільший» і «максимальний» («найменший» і «мінімальний») розрізняються.

Лема 1.1. *Для будь-якої фіксованої множини $B \subset \mathcal{A}$ існує не більше одного найбільшого і не більше одного найменшого елемента.*

Доведення. Припустимо, що множина $B \subset \mathcal{A}$ містить найбільші елементи $M_1 \in B$ та $M_2 \in B$. Тоді, за визначенням найбільшого елемента, отримуємо: $M_1 \preccurlyeq M_2$ та $M_2 \preccurlyeq M_1$. Тепер, використовуючи антисиметричність відношення порядку, отримуємо рівність $M_1 = M_2$.

Твердження леми для найменшого елемента можна отримати за принципом дуальності, тобто повторивши доведення для найбільшого елемента із заміною «$\preccurlyeq$» на «$\succcurlyeq$» і поняття «найбільший» на відповідне дуальне «найменший». □

Зрозуміло, що найбільший (найменший) елемент для $B \subset \mathcal{A}$ одночасно є для $B \subset \mathcal{A}$ максимальним (мінімальним). Однак, як буде видно у прикладі 1.7, зворотне твердження неправильне: максимальний (мінімальний) елемент не обов'язково є найбільшим (найменшим).

Вправа 1.3. Нехай множина $B \subset A$ містить найбільший елемент M. Довести, що B не містить інших максимальних елементів. Сформулювати відповідне дуальне твердження.

Приклад 1.7. Для порівняння понять «найбільший» і «максимальний» («найменший» і «мінімальний») переглянемо множину із прикладу 1.5: $\mathcal{A} = \{a, b, c, d, e, f, g\}$ (діаграму Гессе зображено на рис. 1.4).

Підмножина $B_1 = \{a, b, c\}$ містить найбільший елемент a (він же максимальний) і не містить найменшого (однак є два мінімальних елементи – b та c).

Підмножина $B_2 = \{b, d, e\}$ містить найбільший елемент b (він же максимальний) і найменший елемент e (він же мінімальний).

У підмножині $B_3 = \{e, f\}$ немає ані найбільшого, ані найменшого елементів, однак обидва елементи e та f одночасно і мінімальні, і максимальні.

Сама множина $\mathcal{A} = \{a, b, c, d, e, f, g\}$ має найбільший елемент a (він же максимальний) і найменший елемент g (він же мінімальний).

Вправа 1.4. Нехай скінченна непорожня множина $B \subset A$ містить точно один максимальний елемент. Довести, що цей елемент є для множини B найбільшим. Сформулювати відповідне дуальне твердження. Показати, що для нескінченної B ці твердження можуть не виконуватися.

1.2. Верхні й нижні межі. Супремум та інфімум

Нехай $\langle \mathcal{A}, \preccurlyeq \rangle$ – довільна ЧВМ, $B \subset \mathcal{A}$, $B \neq \varnothing$.

Означення 1.4. Елемент $M \in \mathcal{A}$ називають верхньою межею для множини B, якщо

$$\forall x \in B \colon (x \preccurlyeq M).$$

Елемент $m \in \mathcal{A}$ називають нижньою межею для множини B, якщо

$$\forall x \in B \colon (x \succcurlyeq m).$$

Поняття верхньої та нижньої межі взаємодуальні: якщо елемент є верхньою (нижньою) межею для підмножини B деякої ЧВМ $\langle \mathcal{A}, \preccurlyeq \rangle$, то у відповідній дуальній ЧВМ $\langle \mathcal{A}, \succcurlyeq \rangle$ цей елемент є нижньою (верхньою) межею для B.

На відміну від найбільшого (найменшого) елемента, верхня (нижня) межа для $B \subset \mathcal{A}$ може не належати підмножині B. Очевидно, що найбільший (найменший) елемент для B можна визначити як верхню (нижню) межу B, що належить B.

Приклад 1.8. Розглянемо множину $\mathcal{A} = \{a, b, c, d, e, f, g\}$ із прикладу 1.5 (діаграму Гессе зображено на рис. 1.4).

Підмножина $B_1 = \{a, b, c\}$ має одну верхню межу a (вона ж найбільший елемент для B_1, оскільки $a \in B_1$) і чотири нижні межі – d, e, f, g (B_1 не містить найменшого елемента, оскільки жодна із нижніх меж B_1 не належить B_1).

Підмножина $B_2 = \{b, d, e\}$ має верхні межі a та b (найбільший елемент – $b \in B_2$) і нижні межі e та g (найменший елемент – $e \in B_2$).

Підмножина $B_3 = \{e, f\}$ має чотири верхні межі – a, b, c, d та одну нижню межу g (найбільшого та найменшого елементів B_3 не містить).

Сама множина $\mathcal{A} = \{a, b, c, d, e, f, g\}$ має одну верхню межу a (вона ж найбільший елемент для $\mathcal{A}$) і нижню межу g (вона ж найменший елемент для $\mathcal{A}$).

Приклад 1.9. Частково впорядкована множина $\langle \mathbb{N}, \leqslant \rangle$ (як підмножина самої себе) не має жодної верхньої межі і має одну нижню межу $1 \in \mathbb{N}$.

Підмножина парних чисел $\{2k : k \in \mathbb{N}\} \in \mathbb{N}$ не має жодної верхньої межі і має дві нижні межі 1 та 2.

Означення 1.5. Точною верхньою межею (супремумом) множини $B \subset \mathcal{A}$ називають елемент $\sup B \in \mathcal{A}$, який є найменшим у множині верхніх меж множини B. Точною нижньою межею (інфімумом) множини $B \subset \mathcal{A}$ називають елемент $\inf B \in \mathcal{A}$, який є найбільшим у множині нижніх меж множини B.

Переформулюємо означення 1.5 у вигляді, зручнішому для практичного використання у випадках, коли треба довести, що певний елемент є супремумом або інфімумом.

Для того, щоб елемент $M \in \mathcal{A}$ був точною верхньою межею множини $B \subset \mathcal{A}$, необхідне і достатнє виконання двох умов:

- елемент M є верхньою межею для B; (1.1)
- якщо $\widetilde{M} \in \mathcal{A}$ – довільна верхня межа для $B \subset \mathcal{A}$, то $M \preccurlyeq \widetilde{M}$. (1.2)

Для того, щоб елемент $m \in \mathcal{A}$ був точною нижньою межею множини $B \subset \mathcal{A}$, необхідне і достатнє виконання двох умов:

- елемент m є нижньою межею для B;
- якщо $\widetilde{m} \in \mathcal{A}$ – довільна нижня межа для $B \subset \mathcal{A}$, то $m \succcurlyeq \widetilde{m}$.

Очевидно, що поняття супремуму та інфімуму взаємодуальні, що дає можливість спростити доведення багатьох тверджень.

Розглянемо твердження, яке допомагає визначати супремум (інфімум) у важливому практичному випадку.

Лема 1.2. *Якщо верхня (нижня) межа множини $B \subset \mathcal{A}$ належить самій множині B, ця межа є точною.*

Доведення. Твердження доведемо для супремуму (твердження для інфімуму отримуємо за принципом дуальності).

Нехай $M \in B \subset \mathcal{A}$, і M – верхня межа для B. Для елемента M перевіримо умови (1.1) та (1.2).

Умова (1.1) виконується за припущенням леми. Нехай $\widetilde{M} \in A$ – довільна верхня межа множини B. Оскільки $M \in B$, отримуємо, що $M \preccurlyeq \widetilde{M}$. Отже, умова (1.2) також виконується, і M є супремумом для множини B. □

Зауваження 1.3. Супремум (інфімум) множини $B \subset \mathcal{A}$, як і довільна верхня (нижня) межа B, не обов'язково належить підмножині B.

Вправа 1.5. Довести еквівалентність тверджень:

1. Елемент M – найбільший для множини B.
2. $M = \sup B$ і $M \in B$.
3. M – верхня межа для B і $M \in B$.

Використовуючи принцип дуальності, сформулювати й довести відповідне твердження для найменшого елемента, інфімуму і нижньої межі.

Оскільки супремум – найменший елемент у множині верхніх меж (інфімум – найбільший елемент у множині нижніх меж), із леми 1.1 випливає твердження про єдиність точних граней.

Лема 1.3. *Для будь-якої множини $B \subset \mathcal{A}$ існує не більше одного супремуму і не більше одного інфімуму.*

Вправа 1.6. Довести лему 1.3 самостійно.

Приклад 1.10. Розглянемо ЧВМ із діаграмою, зображеною на рис. 1.5.

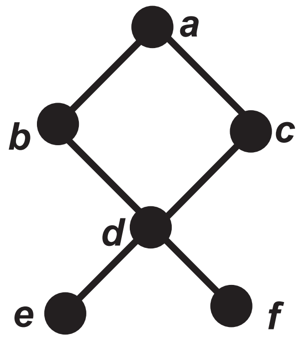


Рис. 1.5

Множина $\{d, e, f\}$ має чотири верхні межі – a, b, c, d, серед яких d – найменша. Отже, $\sup\{d, e, f\} = d$. Крім того, d – найбільший елемент для множини $\{d, e, f\}$, оскільки $d = \sup\{d, e, f\} \in \{d, e, f\}$. Множина $\{d, e, f\}$ не має точної нижньої межі, оскільки взагалі не має нижніх меж.

Приклад 1.11. Розглянемо ЧВМ із діаграмою, зображеною на рис. 1.6.

Підмножина $\{d, e\}$ має три верхні межі – a, b, c, – але жодна з них не є найменшою (множина $\{a, b, c\}$ не має найменшого елемента). Отже, точної верхньої межі (супремуму) для $\{d, e\}$ не існує.

Очевидно, що $\inf\{d, e\} = f$, оскільки f – єдина нижня межа множини $\{d, e\}$. Зазначимо, що f не є найменшим елементом для $\{d, e\}$, оскільки $f \notin \{d, e\}$ (найменшого елемента для $\{d, e\}$, очевидно, немає).

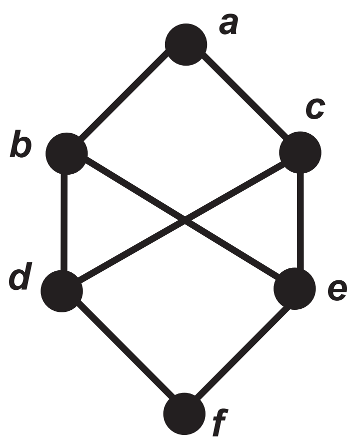


Рис. 1.6

Верхні і нижні межі, зокрема супремуми та інфімуми, мають багато цікавих властивостей [3; 5]. Наведемо декілька важливих тверджень, які надалі використаємо під час вивчення решіток і булевих алгебр.

Лема 1.4. $(a \preccurlyeq b) \Leftrightarrow (\sup\{a, b\} = b) \Leftrightarrow (\inf\{a, b\} = a)$.

Доведення. 1. Нехай $a, b \in \mathcal{A}$, $a \preccurlyeq b$. Тоді b – верхня межа для $\{a, b\}$, звідки $b = \sup\{a, b\}$ за лемою 1.2. Аналогічно, a – нижня межа для $\{a, b\}$ і, за лемою 1.2, $a = \inf\{a, b\}$.

2. Нехай $a, b \in \mathcal{A}$, $b = \sup\{a, b\}$. Тоді b – верхня межа для $\{a, b\}$, звідки $a \preccurlyeq b$.

3. Нехай $a, b \in \mathcal{A}$, $a = \inf\{a, b\}$. Тоді a – нижня межа для $\{a, b\}$, звідки $a \preccurlyeq b$. □

Із леми 1.4 випливає, що супремуми (так само, як і інфімуми) усіх двохелементних підмножин множини $\mathcal{A}$ однозначно визначають відношення передування на множині $\mathcal{A}$. Тобто, якщо відомі значення $\sup\{a, b\}$ для всіх $a, b \in \mathcal{A}$ або $\inf\{a, b\}$ для всіх $a, b \in \mathcal{A}$, то відоме також відношення порядку «$\preccurlyeq$» ($\sup\{a, b\}$ або $\inf\{a, b\}$ можуть і не існувати, але у цьому випадку елементи a та b однозначно непорівнянні).

Теорема 1.1. *Нехай $B_1, B_2 \subset \mathcal{A}$, і нехай існують $\sup B_1$, $\sup B_2$ та $\sup\{\sup B_1, \sup B_2\}$. Тоді існує $\sup(B_1 \cup B_2)$, і справджується рівність*

$$\sup\{\sup B_1, \sup B_2\} = \sup(B_1 \cup B_2). \tag{1.3}$$

Нехай існують елементи $\inf B_1$, $\inf B_2$ та $\inf\{\inf B_1, \inf B_2\}$. Тоді існує $\inf(B_1 \cup B_2)$, і справджується рівність

$$\inf\{\inf B_1, \inf B_2\} = \inf(B_1 \cup B_2). \tag{1.4}$$

Доведення. Доведемо твердження теореми для супремуму (твердження для інфімуму отримуємо за принципом дуальності). Потрібно довести, що елемент $M = \sup\{\sup B_1, \sup B_2\}$ є точною верхньою межею для множини $B_1 \cup B_2$. Для доведення перевіримо умови (1.1) та (1.2).

1. $M \succcurlyeq \sup B_1$, звідки $M \succcurlyeq x_1$ для всіх $x_1 \in B_1$. Аналогічно $M \succcurlyeq x_2$ для всіх $x_2 \in B_2$. Таким чином, $M \succcurlyeq x$ для всіх $x \in (B_1 \cup B_2)$, а отже, M – верхня межа для $B_1 \cup B_2$.

2. Нехай $\widetilde{M} \in \mathcal{A}$ – деяка верхня межа множини $B_1 \cup B_2$. Тоді, очевидно, $\widetilde{M}$ – верхня межа для множини B_1, а отже, $\sup B_1 \preccurlyeq \widetilde{M}$. Аналогічно, $\widetilde{M}$ – верхня межа для множини B_2, і $\sup B_2 \preccurlyeq \widetilde{M}$. Отже, $\widetilde{M}$ є верхньою межею для множини $\{\sup B_1, \sup B_2\}$, звідки $\widetilde{M} \succcurlyeq M = \sup\{\sup B_1, \sup B_2\}$. □

Наслідок. *Нехай* $a, b, c \in \mathcal{A}$, *і нехай існують* $\sup\{a, b\}$, $\sup\{b, c\}$, $\sup\{\sup\{a, b\}, c\}$, $\sup\{a, \sup\{b, c\}\}$. *Тоді існує* $\sup\{a, b, c\}$, *і справджується рівність*

$$\sup\{a, \sup\{b, c\}\} = \sup\{\sup\{a, b\}, c\} = \sup\{a, b, c\}.$$

Нехай $a, b, c \in \mathcal{A}$, *і нехай існують* $\inf\{a, b\}$, $\inf\{b, c\}$, $\inf\{\inf\{a, b\}, c\}$, $\inf\{a, \inf\{b, c\}\}$. *Тоді існує* $\inf\{a, b, c\}$, *і справджується рівність*

$$\inf\{a, \inf\{b, c\}\} = \inf\{\inf\{a, b\}, c\} = \inf\{a, b, c\}.$$

Наголосимо, що у твердженні теореми 1.1 вимагається існування точних меж у лівих частинах рівностей (1.3) та (1.4); існування супремуму (інфімуму) у правих частинах цих рівностей постулюється твердженням теореми. Цікаво, що існування супремуму у лівій частині (1.3) не випливає із існування супремумів у правій частині (1.3) (аналогічно для рівності (1.4)).

Приклад 1.12. Для ЧВМ із прикладу 1.11 (діаграму Гессе зображено на рис. 1.6) розглянемо підмножини $B_1 = \{d, e\}$, $B_2 = \{b\}$. Очевидно, що $\sup B_2 = b$, $\sup(B_1 \cup B_2) = \sup\{b, d, e\} = b$, однак для множини $B_1 = \{d, e\}$ супремуму не існує.

Теорема 1.2. *Нехай* $B \subset \mathcal{A}$, $a \in B$, *і нехай існує* $\sup B$. *Тоді існує* $\inf\{a, \sup B\}$, *і справджується рівність*

$$a = \inf\{a, \sup B\}.$$

Нехай існує $\inf B$. *Тоді існує* $\sup\{a, \inf B\}$, *і справджується рівність*

$$a = \sup\{a, \inf B\}.$$

Доведення. Доведемо твердження теореми для виразу $\inf\{a, \sup B\}$ (твердження для виразу $a = \sup\{a, \inf B\}$ отримуємо за принципом дуальності).

Елемент $a \in B$ є нижньою межею для $\{a, \sup B\}$, оскільки $a \preccurlyeq a$, $a \preccurlyeq \sup B$. Тепер рівність $a = \inf\{a, \sup B\}$ випливає із твердження леми 1.2, оскільки елемент a є нижньою межею для $\{a, \sup B\}$ і $a \in \{a, \sup B\}$. $\square$

Наслідок. *Нехай існує* $\sup\{a, b\}$. *Тоді існує* $\inf\{a, \sup\{a, b\}\}$, *і справджується рівність*

$$a = \inf\{a, \sup\{a, b\}\}.$$

Нехай існує $\inf\{a, b\}$. *Тоді існує* $\sup\{a, \inf\{a, b\}\}$, *і справджується рівність*

$$a = \sup\{a, \inf\{a, b\}\}.$$

Зауваження 1.4. В умові теореми 1.2 передбачається існування $\sup B$ ($\inf B$); існування $\inf\{a, \sup B\}$ (відповідно $\sup\{a, \inf B\}$) постулюється твердженням теореми.

Розділ 2

Решітки

2.1. Основні поняття

Поняття «операція на множині», «замкнена операція на множині», «бінарна операція на множині», «алгебрична структура» вважаємо відомими [1].

Означення 2.1. Решіткою (структурою)[1] називають алгебричну структуру $\langle L, \vee, \wedge \rangle$, де L – непорожня множина; «$\vee$», «$\wedge$» – замкнені бінарні операції на L, які задовольняють такі умови:

1) $a \vee b = b \vee a$, $a \wedge b = b \wedge a$ (комутативність);

2) $a \vee (b \vee c) = (a \vee b) \vee c$, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (асоціативність);

3) $a \vee (a \wedge b) = a$, $a \wedge (a \vee b) = a$ (абсорбція або поглинання).

Операції «$\vee$», «$\wedge$» називають відповідно диз'юнкцією та кон'юнкцією (вживаються також інші назви: об'єднання і перетин, супремум та інфімум тощо). Наведені умови (комутативність, асоціативність, абсорбція) називають аксіомами решітки.

[1]Терміни «решітка» і «структура» – однаково поширені синоніми, проте у цій роботі використовуватимемо термін «решітка», оскільки терміном «структура» називатимемо загальні алгебричні структури з довільним набором операцій.

Зауваження 2.1. В україномовній літературі паралельно вживають терміни «решітка» і «ґратки».

Зауваження 2.2. Оскільки операції «$\vee$» та «$\wedge$» асоціативні, дужки у виразах $(a \vee b) \vee c$ та $(a \wedge b) \wedge c$ згідно зі стандартними домовленостями будемо опускати:

$$(a \vee b) \vee c = a \vee b \vee c, \quad (a \wedge b) \wedge c = a \wedge b \wedge c.$$

Приклад 2.1. 1. Нехай S – непорожня сукупність множин, замкнена відносно операцій об'єднання і перетину (наприклад, кільце множин). Тоді $\langle S, \cup, \cap \rangle$ – решітка. Зазначимо, що S не обов'язково є кільцем множин, оскільки достатньою умовою є замкненість відносно об'єднання і перетину. Так, існують сукупності множин, які не утворюють кільце множин, але утворюють решітку відносно об'єднання і перетину:

$$S = \{\varnothing, \{a, b\}, \{a, b, c\}\};$$
$$S = \{\{a\}, \{a, b\}, \{a, c\}, \{a, b, c\}\}.$$

2. Нехай L – непорожня сукупність висловлень, замкнена відносно операцій диз'юнкції та кон'юнкції. Тоді $\langle L, \vee, \wedge \rangle$ – решітка.

Оскільки аксіоми решітки $\langle L, \vee, \wedge \rangle$ сформульовані «дуальними парами», алгебрична структура $\langle L, \wedge, \vee \rangle$ також є решіткою із диз'юнкцією «$\vee$» і кон'юнкцією «$\wedge$». Решітку $\langle L, \wedge, \vee \rangle$ називають *дуальною* до решітки $\langle L, \vee, \wedge \rangle$.

Отже, у решітках виконується принцип дуальності: якщо для решітки $\langle L, \vee, \wedge \rangle$ справедливе деяке твердження, сформульоване з використанням операцій «$\vee$» та «$\wedge$», то справджується і дуальне твердження, отримане із вихідного заміною «$\vee$» на «$\wedge$» та «$\wedge$» на «$\vee$». Доведення дуального твердження отримуємо переходом до дуальної решітки, тобто може бути побудоване із доведення вихідного твердження заміною «$\vee$» на «$\wedge$» та «$\wedge$» на «$\vee$».

Теорема 2.1 (властивість ідемпотентності)**.** *Нехай* $\langle L, \vee, \wedge \rangle$ *– решітка,* $a \in L$*. Тоді*

$$a \vee a = a, \quad a \wedge a = a.$$

Доведення. Доведемо тотожність $a \vee a = a$; доведення дуальної тотожності отримуємо за принципом дуальності.

Двічі застосовуючи властивість абсорбції, отримуємо (на другому кроці уведено позначення $b = a \vee a$)

$$a \vee a = a \vee \underbrace{(a \wedge (a \vee a))}_{a} = a \vee (a \wedge \underbrace{(a \vee a)}_{b}\,) = a \vee (a \wedge b) = a. \qquad \square$$

2.2. Решітка як частково впорядкована множина

Нехай $\langle L, \vee, \wedge \rangle$ – решітка. Введемо на L бінарне відношення «$\preccurlyeq$»: $a \preccurlyeq b \Leftrightarrow a \vee b = b$.

Вправа 2.1. Довести, що $a \vee b = b \Leftrightarrow a \wedge b = a$.

З урахуванням результату вправи 2.1, отримуємо еквівалентність

$$a \preccurlyeq b \Leftrightarrow a \vee b = b \Leftrightarrow a \wedge b = a. \tag{2.1}$$

Лема 2.1. *Відношення «$\preccurlyeq$» є відношенням часткового порядку, тобто* $\langle L, \preccurlyeq \rangle$ *– ЧВМ.*

Доведення. Потрібно довести, що відношення «$\preccurlyeq$» рефлексивне, антисиметричне і транзитивне.

1. Рефлексивність. Нехай $a \in L$. Тоді $a \preccurlyeq a \Leftrightarrow a \vee a = a$, що справджується за ідемпотентністю (теорема 2.1).

2. Антисиметричність. Нехай $a \preccurlyeq b$; $b \preccurlyeq a$. Доведемо, що $b = a$.

З урахуванням еквівалентності (2.1), отримуємо:

$$\begin{cases} a \preccurlyeq b \Leftrightarrow a \wedge b = a \\ b \preccurlyeq a \Leftrightarrow a \wedge b = b \end{cases} \Leftrightarrow \;\; a = b.$$

3. Транзитивність. Нехай $a \preccurlyeq b$; $b \preccurlyeq c$. Доведемо, що $a \preccurlyeq c$.

З урахуванням аксіом решітки отримуємо:

$$a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a.$$

Отже, $a \wedge c = a$, звідки $a \preccurlyeq c$.

Лему доведено. □

Приклад 2.2. Нехай S – сукупність множин, замкнена за операціями «$\cup$» та «$\cap$». Тоді отримуємо решітку $\langle S, \cup, \cap \rangle$ з відношенням порядку

$$A \preccurlyeq B \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A \Leftrightarrow A \subset B.$$

Отже, з решіткою множин $\langle S, \cup, \cap \rangle$ пов'язане класичне відношення «$\subset$» – бути підмножиною.

Уведене відношення «$\preccurlyeq$» на L будемо називати *відношенням порядку, пов'язаним з решіткою* $\langle L, \vee, \wedge \rangle$.

Зауваження 2.3. Очевидно, що дуальній решітці $\langle L, \wedge, \vee \rangle$ відповідає відношення порядку «$\succcurlyeq$», тобто із взаємодуальними решітками пов'язані взаємодуальні ЧВМ.

Виявляється, що впорядкування «$\preccurlyeq$», пов'язане з решіткою $\langle L, \vee, \wedge \rangle$, повністю визначає операції «$\wedge$» і «$\vee$», тобто ЧВМ $\langle L, \preccurlyeq \rangle$ повністю визначає решітку $\langle L, \vee, \wedge \rangle$.

Теорема 2.2. *Нехай* $\langle L, \vee, \wedge \rangle$ *– решітка з пов'язаним з нею відношенням порядку «*$\preccurlyeq$*». Тоді диз'юнкцію і кон'юнкцію решітки визначають співвідношення*

$$a \vee b = \sup\{a, b\}; \tag{2.2}$$

$$a \wedge b = \inf\{a, b\}. \tag{2.3}$$

Доведення. Доведемо співвідношення $a \vee b = \sup\{a, b\}$, тобто елемент $M = a \vee b$ є супремумом для множини $\{a, b\}$. Для цього достатньо перевірити виконання умов (1.1) і (1.2).

1. $M \wedge a = (a \vee b) \wedge a = a$, тобто $M \succcurlyeq a$. Аналогічно $M \succcurlyeq b$, тобто M є верхньою межею для $\{a, b\}$.

2. Нехай $\widetilde{M} \in L$ – довільна верхня межа для $\{a, b\}$, тобто $\widetilde{M} \succcurlyeq a$, $\widetilde{M} \succcurlyeq b$. Тоді отримуємо:

$$M \vee \widetilde{M} = (a \vee b) \vee \widetilde{M} = a \vee (b \vee \widetilde{M}) = a \vee \widetilde{M} = \widetilde{M},$$

тобто $M \vee \widetilde{M} = \widetilde{M}$, звідки $M \preccurlyeq \widetilde{M}$.

Співвідношення $a \wedge b = \inf\{a, b\}$ отримуємо за принципом дуальності. Теорему доведено. □

Співвідношення (2.2) і (2.3), як і очікувалось, є взаємодуальними (див. зауваження 2.3).

Вправа 2.2. Узагальнити співвідношення (2.2) і (2.3) на випадок скінченної кількості аргументів:

$$a_1 \vee a_2 \vee \cdots \vee a_n = \sup\{a_1, a_2, \ldots, a_n\}; \tag{2.4}$$

$$a_1 \wedge a_2 \wedge \cdots \wedge a_n = \inf\{a_1, a_2, \ldots, a_n\}. \tag{2.5}$$

2.3. Частково впорядкована множина як решітка

У главі 2.1 для довільної решітки було побудовано ЧВМ за еквівалентністю (2.1), і ця ЧВМ цілком визначає вихідну решітку за співвідношеннями (2.2) й (2.3). Розглянемо зворотну проблему: чи існує для довільної ЧВМ $\langle L, \preccurlyeq \rangle$ решітка $\langle L, \vee, \wedge \rangle$, яку можна побудувати за співвідношеннями (2.2) й (2.3) і яка повністю визначатиме задану ЧВМ за еквівалентністю (2.1)?

Отже, нехай $\langle L, \preccurlyeq \rangle$ – довільна ЧВМ. Чи визначають бінарні операції $a \wedge b = \inf\{a, b\}$ та $a \vee b = \sup\{a, b\}$ решітку $\langle L, \vee, \wedge \rangle$? Якщо так, то чи збігається відношення порядку «$\preccurlyeq_L$» цієї решітки з відношенням порядку «$\preccurlyeq$» вихідної ЧВМ? Очевидно, що для позитивної відповіді потрібно, щоб принаймні існували $\inf\{a, b\}$ та $\sup\{a, b\}$ для всіх $a, b \in L$. Виявляється, що цієї умови цілком достатньо.

Теорема 2.3. *Нехай для кожної пари $a, b \in L$ існують $\inf\{a, b\}$ та $\sup\{a, b\}$, і нехай $a \vee b = \sup\{a, b\}$, $a \wedge b = \inf\{a, b\}$. Тоді алгебрична структура $\langle L, \vee, \wedge \rangle$ є решіткою з відношенням порядку, яке збігається з відношенням порядку вихідної ЧВМ.*

Доведення. Для алгебричної структури $\langle L, \vee, \wedge \rangle$ перевіримо аксіоми решітки.

1. Комутативність. Ця властивість очевидна:

$$a \vee b = \sup\{a, b\} = \sup\{b, a\} = b \vee a; \quad a \wedge b = \inf\{a, b\} = \inf\{b, a\} = b \wedge a.$$

2. Асоціативність. Ця властивість випливає із наслідка до теореми 1.1:

$$(a \vee b) \vee c = \sup\{\sup\{a, b\}, c\} = \sup\{a, \sup\{b, c\}\} = a \vee (b \vee c);$$
$$(a \wedge b) \wedge c = \inf\{\inf\{a, b\}, c\} = \inf\{a, \inf\{b, c\}\} = a \wedge (b \wedge c).$$

3. Абсорбція. Ця властивість випливає із наслідка до теореми 1.2:

$$(a \vee b) \wedge a = \inf\{\sup\{a, b\}, a\} = a; \quad (a \wedge b) \vee a = \sup\{\inf\{a, b\}, a\} = a.$$

Отже, алгебрична структура $\langle L, \vee, \wedge \rangle$ є решіткою. Позначимо через «$\preccurlyeq_L$» відношення порядку, пов'язане з решіткою $\langle L, \vee, \wedge \rangle$:

$$a \preccurlyeq_L b \Leftrightarrow a \vee b = b \Leftrightarrow a \wedge b = a$$

(нагадаємо, що еквівалентність $a \vee b = b \Leftrightarrow a \wedge b = a$ справджується для довільної решітки).

Відношення порядку «$\preccurlyeq_L$» збігається з вихідним відношенням «$\preccurlyeq$», оскільки, за лемою 1.4,

$$a \preccurlyeq_L b \Leftrightarrow a \vee b = b \Leftrightarrow \sup\{a, b\} = b \Leftrightarrow a \preccurlyeq b.$$

Теорему доведено. □

Із теорем 2.2 і 2.3 випливає, що кожну решітку можна розглядати як частково впорядковану множину, для якої існують супремум та інфімум усіх двохелементних підмножин. Зв'язок між операціями решітки і відношенням порядку на решітці є взаємно однозначний і встановлюється еквівалентністю (2.1) та співвідношеннями (2.2) й (2.3).

Отже, отримуємо альтернативне визначення решітки.

Означення 2.2 (альтернативне визначення решітки)**.** Решіткою називають частково впорядковану множину, для якої існують супремум та інфімум усіх двохелементних підмножин.

Наведене альтернативне визначення решітки часто зустрічається в літературі [3; 4; 5]. У цьому випадку диз'юнкцію і кон'юнкцію визначають через співвідношення (2.2) та (2.3), після чого доводять комутативність, асоціативність й абсорбцію як властивості решітки.

Приклад 2.3. Частково впорядкована множина, зображена на рис. 1.4 є решіткою, оскільки існують обидві точні межі для всіх двохелементних множин. Нагадаємо, що диз'юнкцію і кон'юнкцію визначають через співвідношення (2.2) та (2.3), і ці операції, за теоремою 2.3, задовольняють три аксіоми решітки (тобто аксіоми решітки можна не перевіряти).

Приклад 2.4. Частково впорядковані множини, зображені на рис. 1.5 та 1.6, не є решітками, оскільки не для кожної двохелементної підмножини цих ЧВМ існують супремум та інфімум.

Приклад 2.5. Частково впорядкована множина $\langle \mathbb{R}, \leqslant \rangle$ є решіткою з операціями:

$$a \vee b = \sup\{a, b\} = \max\{a, b\} = \begin{cases} a, & \text{якщо } a \geqslant b, \\ b, & \text{якщо } a < b; \end{cases}$$

$$a \wedge b = \inf\{a, b\} = \min\{a, b\} = \begin{cases} b, & \text{якщо } a \geqslant b, \\ a, & \text{якщо } a < b. \end{cases}$$

Приклад 2.6. Будь-який ланцюг є решіткою, оскільки всі елементи ланцюга попарно порівнянні, і супремум та інфімум двохелементних підмножин визначені лемою 1.4. Зазначимо, що ЧВМ $\langle \mathbb{R}, \leqslant \rangle$, розглянута у прикладі 2.5, є ланцюгом.

Приклад 2.7. Розглянемо ЧВМ $\langle \mathcal{L}_n, \vdots \rangle$ натуральних дільників фіксованого числа $n \in \mathbb{N}$ (див. приклад 1.1). Доведемо, що ця ЧВМ є решіткою з операціями:

$$a \vee b = \sup\{a, b\} = \text{НСК}(a, b); \quad a \wedge b = \inf\{a, b\} = \text{НСД}(a, b), \tag{2.6}$$

де $\text{НСК}(a, b)$ і $\text{НСД}(a, b)$ – відповідно найменше спільне кратне і найбільший спільний дільник чисел $a, b \in \mathcal{L}_n$.

Наголосимо, що терміни «найбільший спільний дільник» та «найменше спільне кратне» сформульовані з посиланням на традиційне числове впорядкування «$\leqslant$», проте ЧВМ $\mathcal{L}_n$ впорядкована за відношенням подільності «$\vdots$».

Для акуратного доведення співвідношень (2.6) розглянемо розкладання числа n на прості множники:

$$n = p_1^{n_1} p_2^{n_2} \dots p_m^{n_m},$$

де p_j $(j = 1, 2, \dots, m)$ – прості числа; n_j $(j = 1, 2, \dots, m)$ – цілі невід'ємні показники.

Кожний елемент $a \in \mathcal{L}_n$ можна розкласти на прості множники:

$$a = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m},$$

де $0 \leqslant a_j \leqslant n_j$. Оскільки розкладання числа на прості множники є єдиним, показники a_j $(j = 1, 2, \dots, m)$ визначені однозначно. Отже, кожному елементу $a \in \mathcal{L}_n$ взаємно однозначно відповідає вектор показників a_j, $j = 1, 2, \dots, m$:

$$a \leftrightarrows (a_1, a_2, \dots, a_m).$$

Для елементів $a, b \in \mathcal{L}_n$ подільність $b \vdots a$ еквівалентна співвідношенню між відповідними векторами показників:

$$a \preccurlyeq b \Leftrightarrow b \vdots a \Leftrightarrow \begin{cases} a_j \leqslant b_j, \\ j = 1, 2, \dots, m. \end{cases}$$

Випишемо відповідні вектори показників для НСК(a, b) та НСД(a, b):

$$\begin{aligned} \text{НСК}(a, b) &\rightleftarrows (\max\{a_1, b_1\}, \max\{a_2, b_2\}, \dots, \max\{a_m, b_m\}); \\ \text{НСД}(a, b) &\rightleftarrows (\min\{a_1, b_1\}, \min\{a_2, b_2\}, \dots, \min\{a_m, b_m\}), \end{aligned} \tag{2.7}$$

де $\max\{x, y\}$ і $\min\{x, y\}$ стандартним чином позначають відповідно більше і менше із чисел $x, y \in \mathbb{R}$ за стандартним числовим порівнянням «$\leqslant$».

Нехай $c \in \mathcal{L}_n$ – спільне кратне елементів a та b, тобто $c \succcurlyeq a$; $c \succcurlyeq b$. Тоді для відповідних показників маємо:

$$\begin{cases} c_j \geqslant a_j \\ c_j \geqslant b_j \end{cases} \Rightarrow \ c_j \geqslant \max\{a_j, b_j\}, \quad j = 1, 2, \dots, m,$$

звідки випливає передування НСК$\{a, b\} \preccurlyeq c$. Таким чином, НСК(a, b) є найменшим у сенсі передування «$\preccurlyeq$» серед спільних кратних елементів a та b, тобто НСК$(a, b) = \sup(a, b)$. Аналогічно (переходячи до дуальних співвідношень) отримуємо: $\text{НСД}(a,b) = \inf(a,b)$. Отже, обидва співвідношення (2.6) доведені.

Застосований прийом (замість натурального числа розглядати вектор показників розкладу на прості множники) суттєво допомагає у дослідженні решітки $\langle \mathcal{L}_n, \text{НСК}, \text{НСД}\rangle$, оскільки зводить задачу до дослідження ланцюга $\langle \{1, 2, \ldots, n_j\}, \leqslant \rangle$.

Вправа 2.3. Довести логічні наслідки:

$$\begin{cases} a_1 \preccurlyeq c \\ a_2 \preccurlyeq c \end{cases} \Rightarrow (a_1 \vee a_2) \preccurlyeq c; \tag{2.8}$$

$$\begin{cases} c \preccurlyeq b_1 \\ c \preccurlyeq b_2 \end{cases} \Rightarrow c \preccurlyeq (b_1 \wedge b_2); \tag{2.9}$$

$$\begin{cases} a_1 \preccurlyeq b_1 \\ a_2 \preccurlyeq b_1 \\ a_1 \preccurlyeq b_2 \\ a_2 \preccurlyeq b_2 \end{cases} \Rightarrow (a_1 \vee a_2) \preccurlyeq (b_1 \wedge b_2). \tag{2.10}$$

Вказівка. Для доведення тверджень (2.8) і (2.9) використати співвідношення (2.2) й (2.3), а також визначення супремуму й інфімуму як точної верхньої та точної нижньої меж. Твердження (2.10) можна отримати, використовуючи твердження (2.8) і (2.9).

Вправа 2.4. Узагальнити твердження (2.10):

$$\begin{cases} a_i \preccurlyeq b_j \\ 1 \leqslant i \leqslant m, \ 1 \leqslant j \leqslant n \end{cases} \Rightarrow (a_1 \vee a_2 \vee \cdots \vee a_m) \preccurlyeq (b_1 \wedge b_2 \wedge \cdots \wedge b_n). \tag{2.11}$$

Насамкінець сформулюємо два прості твердження, які випливають безпосередньо із твердження (2.10):

$$x \vee (y \wedge z) \preccurlyeq (x \vee y) \wedge (x \vee z); \tag{2.12}$$

$$x \preccurlyeq z \Rightarrow x \vee (y \wedge z) \preccurlyeq (x \vee y) \wedge z. \tag{2.13}$$

Вправа 2.5. Довести твердження (2.12) і (2.13).

2.4. Дистрибутивні решітки

Означення 2.3. Решітку $\langle L, \vee, \wedge \rangle$ називають дистрибутивною, якщо для всіх $a, b, c \in L$ виконуються тотожності

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c); \tag{2.14}$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c). \tag{2.15}$$

Співвідношення дистрибутивності (2.14) та (2.15) утворюють «дуальну пару», а отже, для вивчення дистрибутивних решіток можна використовувати принцип дуальності.

Виявляється, що для визначення дистрибутивної решітки достатньо, щоб справджувалася лише одна із двох тотожностей дистрибутивності.

Лема 2.2. *Нехай у решітці $\langle L, \vee, \wedge \rangle$ для всіх $a, b, c \in L$ справджується хоча б одна з тотожностей* (2.14) *або* (2.15)*. Тоді решітка $\langle L, \vee, \wedge \rangle$ є дистрибутивною.*

Доведення. Нехай у решітці $\langle L, \vee, \wedge \rangle$ виконується тотожність (2.14).

Використовуючи тотожність (2.14) та аксіоми решітки, отримуємо:

$$(a \wedge b) \vee (a \wedge c) = ((a \wedge b) \vee a) \wedge ((a \wedge b) \vee c) = a \wedge ((a \wedge b) \vee c) =$$
$$= a \wedge ((a \vee c) \wedge (b \vee c)) = (a \wedge (a \vee c)) \wedge (b \vee c) = a \wedge (b \vee c).$$

Отже, тотожність (2.15) випливає із тотожності (2.14). Наслідок (2.15) $\Rightarrow$ (2.14) можна отримати за принципом дуальності.

Лему доведено. $\square$

Приклад 2.8. Нехай S – непорожня сукупність множин, замкнена відносно операцій об'єднання і перетину. Тоді решітка множин $\langle S, \cup, \cap\rangle$ є дистрибутивною.

Приклад 2.9. Будь-який ланцюг $\langle L, \preccurlyeq\rangle$ – дистрибутивна решітка. Доведення є нескладним завдяки попарній порівнянності елементів ланцюга.

Зафіксуємо елементи $a, b, c \in L$ і безпосередньо перевіримо тотожність (2.14) для різних варіантів взаємного лінійного впорядкування елементів a, b, c. Очевидно, кількість таких варіантів дорівнює $3! = 6$, однак завдяки симетричності входження b і c у тотожність (2.14) можемо без втрати загальності вважати $b \preccurlyeq c$. Отже, отримуємо три варіанти взаємного впорядкування a, b, c:

$$a \preccurlyeq b \preccurlyeq c; \quad b \preccurlyeq a \preccurlyeq c; \quad b \preccurlyeq c \preccurlyeq a.$$

Перевіримо тотожність (2.14) для випадку $a \preccurlyeq b \preccurlyeq c$ (інші два випадки можна перевірити аналогічно). Враховуючи співвідношення (2.2) і (2.3), отримуємо:

$$a \vee (b \wedge c) = a \vee b = b; \quad (a \vee b) \wedge (a \vee c) = b \wedge c = b.$$

Приклад 2.10. Решітка $\langle \mathcal{L}_n, \text{НСК}, \text{НСД}\rangle$ (див. приклад 2.7) для кожного фіксованого $n \in \mathbb{N}$ є дистрибутивною. Це стає очевидним, якщо знову для кожного елемента решітки $\mathcal{L}_n$ записати вектор показників розкладання цього елемента на прості множники. Тоді, враховуючи співвідношення (2.7), достатньо перевірити дистрибутивність ланцюга $\langle\{1, 2, \ldots, n_j\}, \leqslant\rangle$ із операціями $\max\{x, y\}$ та $\min\{x, y\}$. Але, як було доведено у прикладі 2.9, будь-який ланцюг є дистрибутивною решіткою.

Приклад 2.11. Решітки $\mathcal{K}_1$ і $\mathcal{K}_2$, діаграми яких зображено на рис. 2.1 і 2.2, не є дистрибутивними.

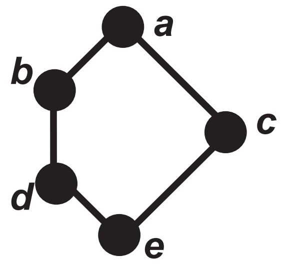


Рис. 2.1. Решітка $\mathcal{K}_1$

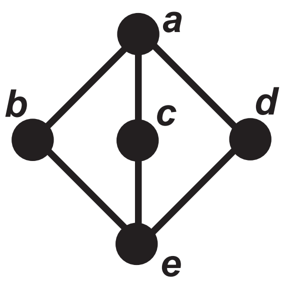


Рис. 2.2. Решітка $\mathcal{K}_2$

Справді, для решітки $\mathcal{K}_1$ отримуємо:

$$d \vee (b \wedge c) = d \vee e = d; \quad (d \vee b) \wedge (d \vee c) = b \wedge a = b.$$

Аналогічно, для решітки $\mathcal{K}_2$:

$$b \vee (c \wedge d) = b \vee e = b; \quad (b \vee c) \wedge (b \vee d) = a \wedge a = a.$$

Виявляється, що решітки $\mathcal{K}_1$ і $\mathcal{K}_2$ у деякому розумінні вичерпують приклади недистрибутивних решіток. Для формулювання відповідної теореми наведемо два прості визначення.

Означення 2.4. Решітки $\langle L_1, \vee_1, \wedge_1 \rangle$ та $\langle L_2, \vee_2, \wedge_2 \rangle$ називають ізоморфними, якщо існує бієкція (ізоморфізм) $f\colon L_1 \to L_2$, така, що

$$f(a \vee_1 b) = f(a) \vee_2 f(b); \quad f(a \wedge_1 b) = f(a) \wedge_2 f(b), \quad a, b \in \mathcal{L}_1.$$

Означення 2.5. Підмножину $L_1 \subset L$ називають підрешіткою решітки $\langle L, \vee, \wedge \rangle$, якщо L_1 є решіткою за тими ж операціями «$\vee$» і «$\wedge$», які визначені у решітці L.

Зауваження 2.4. Очевидно, що непорожня підмножина $L_1 \subset L$ є підрешіткою решітки $\langle L, \vee, \wedge \rangle$ тоді і тільки тоді, коли L_1 замкнена відносно операцій «$\vee$», «$\wedge$» решітки L.

Теорема 2.4 (критерій дистрибутивності)**.** *Решітка є дистрибутивною тоді і тільки тоді, коли вона не містить підрешіток, ізоморфних решіткам $\mathcal{K}_1$ та $\mathcal{K}_2$.*

Теорему 2.4 буде доведено у главі 2.7 (див. зауваження 2.10).

Приклад 2.12. 1. Ланцюг не може містити підрешіток, ізоморфних $\mathcal{K}_1$ та $\mathcal{K}_2$, оскільки $\mathcal{K}_1$ та $\mathcal{K}_2$ містять непорівнянні пари елементів. Отже, кожний ланцюг є дистрибутивною решіткою. Нагадаємо, що дистрибутивність ланцюга була доведена безпосередньо (див. приклад 2.9).

2. Решітка із діаграмою на рис. 2.3 не є дистрибутивною, оскільки містить підрешітку $\{a_1, a_2, a_3, a_4, a_6\}$, ізоморфну $\mathcal{K}_1$ (рис. 2.4).

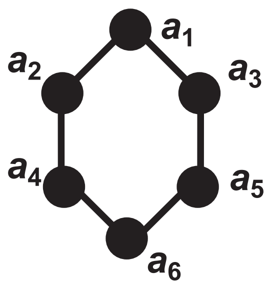


Рис. 2.3

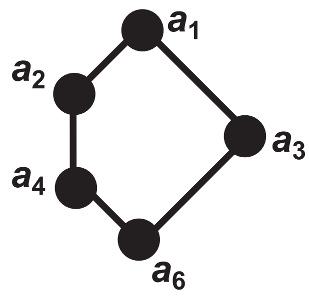


Рис. 2.4

3. Решітка із діаграмою на рис. 2.5 не є дистрибутивною, оскільки містить підрешітку $\{a_1, a_2, a_3, a_4, a_6\}$ (рис. 2.6), ізоморфну $\mathcal{K}_2$.

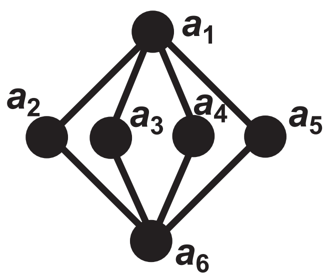


Рис. 2.5

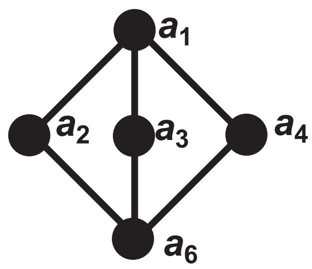


Рис. 2.6

4. Решітка із діаграмою на рис. 2.7 є дистрибутивною, оскільки не містить підрешіток, ізоморфних $\mathcal{K}_1$ або $\mathcal{K}_2$.

Зазначимо, що підмножина $\{a_1, a_2, a_3, a_4, a_6\}$ за впорядкуванням вихідної решітки (діаграму зображено на рис. 2.8) є решіткою, ізоморфною $\mathcal{K}_1$. Однак решітка $\langle \{a_1, a_2, a_3, a_4, a_6\}, \preccurlyeq \rangle$ не є підрешіткою вихідної решітки, оскільки $a_2 \wedge a_3$ має різне значення у вихідній решітці та у решітці $\langle\{a_1, a_2, a_3, a_4, a_6\}, \preccurlyeq\rangle$:

- у вихідній решітці: $a_2 \wedge a_3 = a_5$;
- у решітці $\langle\{a_1, a_2, a_3, a_4, a_6\}, \preccurlyeq\rangle$: $a_2 \wedge a_3 = a_6$.

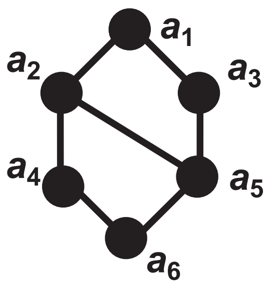


Рис. 2.7

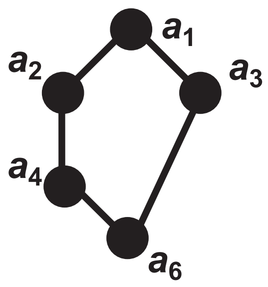


Рис. 2.8

Слід також зазначити, що для перевірки факту, чи є підмножина $\{a_1, a_2, a_3, a_4, a_6\} \subset L$ підрешіткою, достатньо перевірити замкненість цієї підмножини за операціями вихідної решітки L (див. зауваження 2.4). У цьому прикладі досить зазначити, що у вихідній решітці

$$a_2 \wedge a_3 = a_5 \notin \{a_1, a_2, a_3, a_4, a_6\},$$

що означає незамкненість $\{a_1, a_2, a_3, a_4, a_6\}$ відносно $\wedge$.

Насамкінець наведемо ще одне важливе твердження, справедливе для дистрибутивних решіток.

Лема 2.3. *Нехай $\langle L, \vee, \wedge\rangle$ – дистрибутивна решітка, $a, x, y \in L$. Тоді справджується логічний наслідок*

$$\begin{cases} x \vee a = y \vee a \\ x \wedge a = y \wedge a \end{cases} \Rightarrow \ x = y.$$

Доведення. Нехай $x \vee a = y \vee a$; $x \wedge a = y \wedge a$. Тоді, враховуючи дистрибутивність, отримуємо:

$$x = x \wedge (x \vee a) = x \wedge (y \vee a) = (x \wedge y) \vee (x \wedge a) =$$
$$= (x \wedge y) \vee (y \wedge a) = y \wedge (x \vee a) = y \wedge (y \vee a) = y.$$

Лему доведено. □

2.5. Обмежені решітки

Означення 2.6. Нехай $\langle L, \vee, \wedge \rangle$ – решітка. Решітку L називають обмеженою зверху, якщо існує елемент $1_L = \sup L$. Решітку L називають обмеженою знизу, якщо існує елемент $0_L = \inf L$. Решітку, що обмежена і зверху, і знизу, називають обмеженою.

Очевидно, що обмеженість решітки означає існування найбільшого 1_L і найменшого 0_L елементів для множини L.

Елементи $1_L \in L$ і $0_L \in L$ називають відповідно *одиницею* та *нулем* решітки L. Якщо це не викликає непорозумінь, індекс L у позначеннях 1_L та 0_L часто пропускають:

$$1 = 1_L; \quad 0 = 0_L.$$

Очевидно, що з переходом до дуальної решітки нуль і одиниця решітки міняються місцями: нуль вихідної решітки збігається з одиницею дуальної і навпаки.

Приклад 2.13. 1. Із співвідношень (2.4) і (2.5) випливає, що будь-яка скінченна решітка $L = \{a_1, a_2, \ldots, a_n\}$ є обмеженою:

$$1 = a_1 \vee a_2 \vee \cdots \vee a_n = \sup\{a_1, a_2, \ldots, a_n\};$$
$$0 = a_1 \wedge a_2 \wedge \cdots \wedge a_n = \inf\{a_1, a_2, \ldots, a_n\}.$$

2. Решітка $\langle \mathbb{N}, \leqslant \rangle$ обмежена лише знизу: елемент $1 \in \mathbb{N}$ є нулем решітки.

3. Решітка $\mathcal{L}_n$ для будь-якого фіксованого $n \in \mathbb{N}$ обмежена:

$$1_{\mathcal{L}_n} = n; \quad 0_{\mathcal{L}_n} = 1.$$

4. Розглянемо частково впорядковану множину $\mathcal{L}_0 = \mathbb{N} \cup \{0\}$ з таким відношенням порядку:

$$(a \preccurlyeq b) \Leftrightarrow (b \,\vdots\, a), \text{ якщо } a, b \in \mathbb{N};$$
$$\forall\, a \in \mathbb{N} \cup \{0\} \colon (a \preccurlyeq 0).$$

Використовуючи метод, що був застосований до ЧВМ $\langle \mathcal{L}_n, \,\vdots\, \rangle$ з натуральним n (див. приклад 2.7), легко довести, що ЧВМ $\langle \mathcal{L}_0, \preccurlyeq \rangle$ є решіткою. Очевидно, решітка $\langle \mathcal{L}_0, \preccurlyeq \rangle$ обмежена:

$$1_{\mathcal{L}_0} = 0; \quad 0_{\mathcal{L}_0} = 1.$$

Зауваження 2.5. Використання для одиниці і нуля решітки позначень 1 та 0 без індексу, який вказує на конкретну решітку, може призвести до конфлікту позначень. Так, числові решітки (зокрема, $\mathcal{L}_0$) містять елементи, для яких позначення 1 та 0 є стандартними (тобто, числа 1 та 0), і ці елементи можуть не бути відповідно одиницею і нулем решітки. Більше того, у решітці $\mathcal{L}_0$ число 1 є нулем решітки, а число 0 – одиницею решітки. Однак у більшості випадків, зокрема під час розгляду абстрактних решіток, використання позначень 1 та 0 замість 1_L та 0_L вважається цілком виправданим.

Для обмежених решіток справджується корисна тотожність, відома під назвою «*властивість нейтральності*».

Лема 2.4. *Нехай $\langle L, \vee, \wedge \rangle$ – обмежена решітка, $a \in L$. Тоді*

$$a \vee 0 = a; \quad a \wedge 1 = a.$$

Доведення. Твердження леми випливає із еквівалентності (2.1) та означення нуля й одиниці решітки. □

Зазначимо, що тотожності нейтральності, як і слід було очікувати, є взаємно дуальними.

2.6. Доповнені решітки

У цій главі решітки вважаємо обмеженими.

Означення 2.7. Елемент $b \in L$ називають доповненням до елемента $a \in L$, якщо

$$a \vee b = 1; \quad a \wedge b = 0.$$

Безпосередньо з означення доповнення випливає очевидний факт: якщо $b \in L$ є доповненням до $a \in L$, то $a \in L$ є доповненням до $b \in L$ (елементи a і b називатимемо взаємодоповненими).

Приклад 2.14. 1. У будь-якій обмеженій решітці елементи 0 та 1 є взаємодоповненими, і ці елементи інших доповнень не мають.

2. В обмеженому ланцюзі $\langle L, \preccurlyeq \rangle$ доповнення мають лише 1 і 0.

3. У решітці $\mathcal{K}_1$ (діаграма на рис. 2.1) елементи a та e є відповідно одиницею і нулем решітки. Легко перевірити, що елемент c має два доповнення – b та d.

4. У решітці $\mathcal{K}_2$ (діаграма на рис. 2.2) елементи a та e є відповідно одиницею і нулем решітки. Легко перевірити, що елементи b, c, d є попарно взаємодоповненими (доповненнями до кожного із цих трьох елементів є два інших).

Отже, доповнення до деяких елементів може взагалі не існувати, а деякі елементи можуть мати декілька доповнень.

Вправа 2.6. Нехай елементи a і b взаємодоповнені та $a \preccurlyeq b$. Довести, що $a = 0$ та $b = 1$.

Означення 2.8. Решітку, кожний елемент якої має хоча б одне доповнення, називають доповненою.

Приклад 2.15. 1. Двохелементний ланцюг $\{0, 1\}$ $(0 \prec 1)$ є доповненою решіткою.

2. Обмежений ланцюг $\langle L, \preccurlyeq \rangle$ з трьома або більше елементами не є доповненою решіткою.

3. Решітки $\mathcal{K}_1$ і $\mathcal{K}_2$ є доповненими.

4. Розглянемо решітку $\langle \mathcal{L}_n, \vdots \rangle$ (див. приклад 2.7), $n = p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}$, де p_1, p_2, $\ldots$, p_m – прості числа, $n_1, n_2, \ldots, n_m \in \mathbb{N}$. Використовуючи метод із прикладу 2.7 легко довести, що елемент $a = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ має доповнення тоді і тільки тоді, коли $a_k \in \{0, n_k\}$, $k = 1, 2, \ldots, m$. Звідси випливає, що решітка $\langle \mathcal{L}_n, \vdots \rangle$ є доповненою тоді і тільки тоді, коли $n_k = 1$, $k = 1, 2, \ldots, m$, тобто коли число $n = p_1 p_2 \cdots p_m$ є добутком попарно різних простих чисел.

Наведемо ще один результат, справедливий для дистрибутивних обмежених решіток.

Теорема 2.5. *У дистрибутивній обмеженій решітці кожний елемент має не більше одного доповнення.*

Вправа 2.7. Довести теорему 2.5 самостійно.

Вказівка. Скористатись лемою 2.3.

Зауваження 2.6. Сформульована теорема іноді допомагає доводити недистрибутивність решіток. Так, можна зробити висновок про недистрибутивність решіток $\mathcal{K}_1$ і $\mathcal{K}_2$, оскільки деякі елементи цих решіток мають більше одного доповнення.

Зауваження 2.7. Теорема 2.5 не має зворотного наслідку, тобто існують недистрибутивні обмежені решітки, елементи яких мають не більше одного доповнення. Такою, наприклад, є решітка із діаграмою на рис. 2.9.

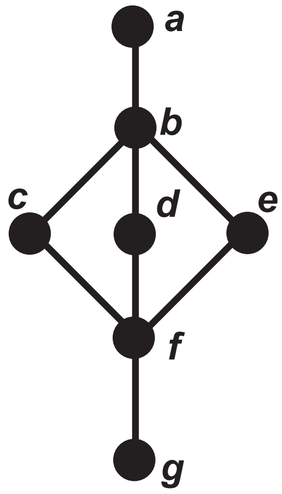


Рис. 2.9. Недистрибутивна решітка, кожен елемент якої має не більше одного доповнення

Легко зрозуміти, що у зображеній решітці доповнення мають лише одиниця решітки (елемент a) та нуль решітки (елемент g), які є взаємодоповненими та інших доповнень не мають (див. приклад 2.14, п. 1). Однак ця решітка недистрибутивна, оскільки містить підрешітку $\{b, c, d, e, f\}$, ізоморфну $\mathcal{K}_2$.

Детальніше про зв'язок між дистрибутивністю та наявністю доповнень див. у роботі [3].

2.7. Модулярні решітки

Означення 2.9. Решітку $\langle L, \vee, \wedge \rangle$ називають модулярною, якщо

$$\forall\, x, y, z \in L \colon x \preccurlyeq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z. \tag{2.16}$$

Очевидно, що твердження (2.16) збігається із дуальним (з точністю до застосування комутативності та перейменування змінних під кванторами загальності):

$$\forall\, x, y, z \in L \colon x \succcurlyeq z \Rightarrow x \wedge (y \vee z) = (x \wedge y) \vee z. \tag{2.17}$$

Твердження, еквівалентне своєму дуальному, іноді називають *самодвоїстим*. Із самодвоїстості закону модулярності (2.16) випливає, що для вивчення модулярних решіток можна використовувати принцип дуальності.

Вправа 2.8. Довести, що будь-яка дистрибутивна решітка є модулярною.

Приклад 2.16. 1. Решітка множин $\langle S, \cup, \cap \rangle$ є дистрибутивною, а отже (див. вправу 2.8) є модулярною.

2. Решітка $\mathcal{K}_1$ не є модулярною; решітка $\mathcal{K}_2$ недистрибутивна, але модулярна. Для зручності посилань знову наведемо діаграми решіток $\mathcal{K}_1$ і $\mathcal{K}_2$, дещо змінивши позначення елементів (рис. 2.10 і 2.11).

Для решітки $\mathcal{K}_1$ (рис. 2.10) отримуємо:

$$c \preccurlyeq a; \quad c \vee (b \wedge a) = c \vee 0 = c; \quad (c \vee b) \wedge a = 1 \wedge a = a,$$

що означає немодулярність $\mathcal{K}_1$.

Для решітки $\mathcal{K}_2$ тотожність (2.16) можна перевірити безпосередньо. Справді, у $\mathcal{K}_2$ (рис. 2.11) передування $x \preccurlyeq z$ можливе лише в одному із трьох випадків: $x = 0$, $z = 1$, $x = z$. Очевидно, що для кожного із цих випадків рівність $x \vee (y \wedge z) = (x \vee y) \wedge z$ справджується.

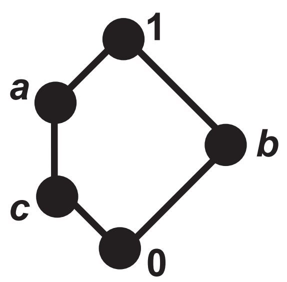


Рис. 2.10. Решітка $\mathcal{K}_1$ – найпростіша немодулярна решітка

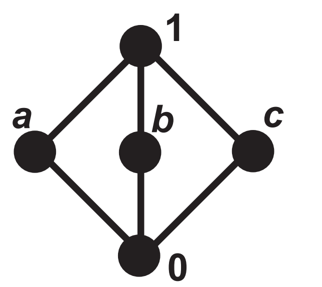


Рис. 2.11. Решітка $\mathcal{K}_2$ – найпростіша недистрибутивна модулярна решітка

3. Нехай X – фіксований лінійний простір. Розглянемо множину підпросторів L_X простору X, упорядковану за природним відношенням порядку «$\subset$». З'ясуємо, чи є ЧВМ $\langle L_X, \subset \rangle$ решіткою.

Максимальний (за відношенням «$\subset$») підпростір, який є підмножиною кожного із двох заданих підпросторів $A, B \in L_X$, є перетин $A \cap B$. Мінімальним підпростором, який містить обидва підпростори A і B, є сума просторів $A + B$; зауважимо, що мінімальною підмножиною, яка містить A і B, є об'єднання $A \cup B$, але $A \cup B$ не обов'язково є підпростором X. Отже, для будь-яких $A, B \in L_X$ існує супремум та інфімум $\{A, B\}$, які визначають диз'юнкцію і кон'юнкцію:

$$A \vee B = \sup\{A, B\} = A + B; \quad A \wedge B = \inf\{A, B\} = A \cap B.$$

Отже, ЧВМ $\langle L_X, \subset\rangle$ можна розглядати як решітку $\langle L_X, +, \cap\rangle$. Неважко довести [3], що ця решітка модулярна.

Зазначимо, що решітка $\langle L_X, \subset\rangle$ не є дистрибутивною, за винятком випадків одновимірного або нульового X, оскільки простір X з двома або більше вимірами містить підрешітку, ізоморфну $\mathcal{K}_2$ – нульовий підпростір, площину (двовимірний підпростір) і три різні прямі (одновимірні підпростори) у цій площині.

4. Нехай $\langle G, *\rangle$ – фіксована група. Можна довести [4], що множина нормальних дільників групи $\langle G, *\rangle$ за відношенням «$\subset$» є модулярною решіткою.

Зазначимо, що множина всіх підгруп групи $\langle G, *\rangle$ за відношенням «$\subset$» є решіткою, але ця решітка не обов'язково є модулярною. Так, решітка всіх підгруп групи підстановок S_3 модулярна, але решітка всіх підгруп групи S_4 немодулярна.

Решітки підгруп детально досліджено, наприклад, у роботах [2;4].

2.7.1. Критерій модулярності

Виявляється, що $\mathcal{K}_1$ є в деякому сенсі найпростішою немодулярною решіткою.

Теорема 2.6 (критерій модулярності)**.** *Решітка $\langle L, \vee, \wedge\rangle$ модулярна тоді і тільки тоді, коли вона не містить підрешіток, ізоморфних $\mathcal{K}_1$.*

Доведення. Очевидно, що жодна модулярна решітка не може містити підрешітки, ізоморфної $\mathcal{K}_1$, оскільки $\mathcal{K}_1$ немодулярна. Доведемо, що кожна немодулярна решітка містить деяку підрешітку, ізоморфну $\mathcal{K}_1$.

Нехай решітка L немодулярна, тобто для деяких $x, y, z \in L$ маємо:

$$x \preccurlyeq z; \quad x \vee (y \wedge z) \neq (x \vee y) \wedge z,$$

звідки, з урахуванням твердження (2.13), отримуємо строге передування

$$x \vee (y \wedge z) \prec (x \vee y) \wedge z. \tag{2.18}$$

Доведемо, що підрешітку, ізоморфну $\mathcal{K}_1$, утворюють елементи

$$x \vee y,\ z \wedge y,\ x \vee (y \wedge z),\ (x \vee y) \wedge z,\ y. \tag{2.19}$$

Запишемо очевидні співвідношення передування:

$$z \wedge y \preccurlyeq x \vee (y \wedge z) \prec (x \vee y) \wedge z \preccurlyeq x \vee y; \quad z \wedge y \preccurlyeq y \preccurlyeq x \vee y.$$

Усі записані передування є строгими. Справді, припустивши рівність $z \wedge y = x \vee (y \wedge z)$, отримуємо:

$$x \preccurlyeq (y \wedge z) \Rightarrow \begin{cases} x \preccurlyeq y \\ x \preccurlyeq z \end{cases} \Rightarrow\ x \vee (y \wedge z) = (x \vee y) \wedge z = y \wedge z,$$

що суперечить нерівності (2.18). Отже, $z \wedge y \prec x \vee (y \wedge z)$. Аналогічно отримуємо строге передування $(x \vee y) \wedge z \prec x \vee y$. Нарешті, припустивши рівність $z \wedge y = y$ (аналогічно $y = x \vee y$), отримуємо передування $y \preccurlyeq z$ (відповідно $x \preccurlyeq y$), звідки також легко отримуємо суперечність нерівності (2.18). Отже, маємо такі передування:

$$z \wedge y \prec x \vee (y \wedge z) \prec (x \vee y) \wedge z \prec x \vee y; \quad z \wedge y \prec y \prec x \vee y.$$

Далі зазначимо, що y не дорівнює елементам $x \vee (y \wedge z)$ та $(x \vee y) \wedge z$. Дійсно, припустивши рівність $y = x \vee (y \wedge z)$ (аналогічно $y = (x \vee y) \wedge z$), отримуємо передування $x \preccurlyeq y$ (відповідно $y \preccurlyeq z$), яке суперечить нерівності (2.18). Отже, всі елементи з набору (2.19) попарно різні.

Для доведення того, що набір (2.19) утворює підрешітку решітки L і що ця підрешітка ізоморфна $\mathcal{K}_1$, достатньо обчислити попарні диз'юнкції і кон'юнкції цих елементів. Оскільки для порівнянних елементів диз'юнкція і кон'юнкція визначаються лемою (1.4), потрібно обчислити лише диз'юнкцію і кон'юнкцію y з елементами $x \vee (y \wedge z)$ та $(x \vee y) \wedge z$.

Користуючись аксіомами решітки, отримуємо:

$$y \vee (x \vee (y \wedge z)) = x \vee y \vee (y \wedge z) = x \vee y;$$
$$y \wedge ((x \vee y) \wedge z) = y \wedge (x \vee y) \wedge z = y \wedge z.$$

Вираз $y \vee ((x \vee y) \wedge z)$ обчислимо, скориставшись співвідношеннями

$$x \vee y = (y \vee (x \vee (y \wedge z))) \preccurlyeq (y \vee ((x \vee y) \wedge z)) \preccurlyeq x \vee y,$$

звідки, враховуючи антисиметричність відношення порядку, отримуємо:

$$y \vee ((x \vee y) \wedge z) = x \vee y.$$

Аналогічно (дуальними міркуваннями) отримуємо рівність

$$y \wedge (x \vee (y \wedge z)) = y \wedge z.$$

Оскільки елементи в (2.19) попарно різні, за лемою (1.4) легко отримати непорівнянність елемента y з елементами $x \vee (y \wedge z)$ та $(x \vee y) \wedge z$.

Таким чином, визначена п'ятиелементна підмножина (2.19) замкнена відносно диз'юнкції і кон'юнкції вихідної решітки $\langle L, \vee, \wedge \rangle$, і впорядкування між цими елементами (рис. 2.12) збігається із впорядкуванням решітки $\mathcal{K}_1$.

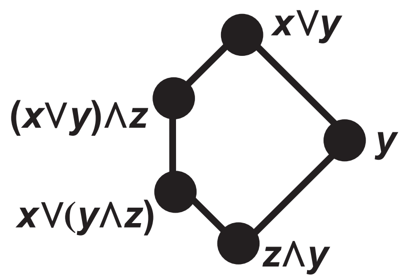


Рис. 2.12

Теорему доведено. $\square$

Вправа 2.9. Дослідити на модулярність усі решітки із прикладу 2.12.

2.7.2. Дистрибутивні трійки

Відомо, що навіть у недистрибутивних решітках існують трійки елементів a, b, c, для яких справджуються закони дистрибутивності:

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c); \tag{2.20}$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c); \tag{2.21}$$

$$b \vee (a \wedge c) = (b \vee a) \wedge (b \vee c); \tag{2.22}$$

$$b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c); \tag{2.23}$$

$$c \vee (a \wedge b) = (c \vee a) \wedge (c \vee b); \tag{2.24}$$

$$c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b). \tag{2.25}$$

Зауваження 2.8. Формально для елементів a, b, c можна виписати 12 рівностей дистрибутивності – по 6 переставлень елементів a, b, c у рівностях (2.14) і (2.15). Однак, враховуючи комутативність диз'юнкції та кон'юнкції, можна помітити симетричність рівностей (2.14) і (2.15) відносно переставлень елементів b і c. Таким чином, для кожної трійки a, b, c є сенс розглядати шість рівностей дистрибутивності, і це будуть саме рівності (2.20)–(2.25).

Приклад 2.17. Нехай $\langle L, \vee, \wedge \rangle$ – обмежена решітка. Тоді для трійок 1, b, c та 0, b, c ($b, c \in L$) справджуються всі шість законів (2.20)–(2.25).

Приклад 2.18. У решітці $\mathcal{K}_2$ (рис. 2.11) жоден із законів (2.20)–(2.25) не виконується для трійки a, b, c, однак усі ці шість законів виконуються для трійки 1, b, c, а також для будь-якої іншої трійки, яка містить 1 або 0 (приклад 2.17).

У довільних решітках для фіксованої трійки a, b, c деякі із законів (2.20)–(2.25) можуть виконуватися, а інші – не виконуватися.

Вправа 2.10. Перевірити, які із законів (2.20)–(2.25) справджуються для трійки a, b, c у решітці $\mathcal{K}_1$ (рис. 2.10).

У модулярних решітках аналіз дистрибутивності для фіксованої трійки елементів суттєво спрощується.

Теорема 2.7. *Нехай $\langle L, \vee, \wedge \rangle$ – модулярна решітка, $a, b, c \in L$ – деякі фіксовані елементи. Тоді шість рівностей (2.20)–(2.25) – еквівалентні твердження (виконуються чи не виконуються одночасно).*

Доведення. Доведемо наслідок (2.20) $\Rightarrow$ (2.23).

Нехай рівність (2.20) виконується. Тоді, обчисливши кон'юнкцію між елементом b і обома частинами (2.20), отримуємо:

$$b \wedge (a \vee (b \wedge c)) = b \wedge (a \vee b) \wedge (a \vee c).$$

Оскільки $b \succcurlyeq b \wedge c$, до лівої частини отриманої рівності можемо застосувати властивість модулярності (у формі (2.17)). Одночасно спрощуючи праву частину за абсорбцією, отримуємо рівність

$$(b \wedge a) \vee (b \wedge c) = b \wedge (a \vee c),$$

яка збігається із рівністю (2.23).

Аналогічно, обчисливши диз'юнкцію між елементом a й обома частинами рівності (2.23), можемо довести наслідок (2.23) $\Rightarrow$ (2.20). Таким чином, маємо еквівалентність (2.20) $\Leftrightarrow$ (2.23).

Далі, користуючись принципом дуальності, отримуємо еквівалентність (2.21) $\Leftrightarrow$ (2.22).

Переставивши в отриманих еквівалентностях елементи b та c, отримуємо еквівалентності (2.20) $\Leftrightarrow$ (2.25) та (2.21) $\Leftrightarrow$ (2.24).

Нарешті, переставивши a та c в еквівалентностях (2.20) $\Leftrightarrow$ (2.23) та (2.21) $\Leftrightarrow$ (2.22), отримуємо еквівалентності (2.24) $\Leftrightarrow$ (2.23) та (2.25) $\Leftrightarrow$ (2.22).

Таким чином, отримуємо ланцюжок еквівалентностей

$$(2.20) \Leftrightarrow (2.23) \Leftrightarrow (2.24) \Leftrightarrow (2.21) \Leftrightarrow (2.22) \Leftrightarrow (2.25),$$

що завершує доведення теореми. □

Говорять, що елементи a, b, c утворюють *дистрибутивну трійку*, якщо ці елементи задовольняють шість рівностей (2.20)–(2.25).

Зауваження 2.9. Легко перевірити, що будь-яке переставлення елементів дистрибутивної трійки залишає цю трійку дистрибутивною. Звідси випливає, що дистрибутивну трійку можна розглядати як множину із трьох елементів (без упорядкування).

Вправа 2.11. Для модулярної решітки довести дистрибутивність трійки $\{a, b, c\}$ у випадку, якщо $a \preccurlyeq b$.

Очевидно, що решітка є дистрибутивною тоді і тільки тоді, коли будь-яка трійка її елементів є дистрибутивною.

Нагадаємо (див. приклад 2.18), що в недистрибутивних решітках, зокрема в модулярних, деякі трійки елементів можуть бути дистрибутивними.

Ще раз наголосимо, що вимога модулярності у теоремі 2.7 є суттєвою (вправа 2.10).

Для дослідження дистрибутивності важливими є елементи

$$M(a, b, c) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c);$$
$$m(a, b, c) = (a \wedge b) \vee (a \wedge c) \vee (b \wedge c).$$

Вправа 2.12. Довести нерівність $m(a, b, c) \preccurlyeq M(a, b, c)$ для довільних $a, b, c \in L$ для довільної (не обов'язково модулярної) решітки $\langle L, \vee, \wedge \rangle$.

Вказівка. Використати співвідношення (2.11).

Теорема 2.8. *Нехай $\langle L, \vee, \wedge \rangle$ – модулярна решітка, $a, b, c \in L$ – деякі фіксовані елементи. Тоді необхідною й достатньою умовою дистрибутивності трійки $\{a, b, c\}$ є виконання рівності $M(a, b, c) = m(a, b, c)$.*

Доведення. Необхідність. Нехай трійка $\{a, b, c\}$ дистрибутивна. Тоді можемо застосувати до виразу $(a \vee b) \wedge (a \vee c)$ у складі $M(a, b, c)$ закон (2.20):

$$M(a, b, c) = (a \vee (b \wedge c)) \wedge (b \vee c).$$

Тепер, оскільки $(b \vee c) \succcurlyeq (b \wedge c)$, можемо застосувати до отриманого виразу закон модулярності у формі (2.17):

$$(a \vee (b \wedge c)) \wedge (b \vee c) = (a \wedge (b \vee c)) \vee (b \wedge c).$$

Нарешті, застосувавши закон (2.21), отримуємо:

$$M(a, b, c) = (a \wedge (b \vee c)) \vee (b \wedge c) = ((a \wedge b) \vee (a \wedge c)) \vee (b \wedge c) = m(a, b, c).$$

Достатність. Нехай для елементів $a, b, c \in L$ виконується рівність $M(a, b, c) = m(a, b, c)$. Тоді, обчисливши диз'юнкцію обох частин цієї рівності з елементом a, отримуємо:

$$a \vee ((a \vee b) \wedge (a \vee c) \wedge (b \vee c)) = a \vee (a \wedge b) \vee (a \wedge c) \vee (b \wedge c).$$

Використовуючи абсорбцію для правої частини отриманої рівності і модулярність для лівої частини ($a \preccurlyeq (a \vee b) \wedge (a \vee c)$), отримуємо:

$$(a \vee b \vee c) \wedge (a \vee b) \wedge (a \vee c) = a \vee (b \wedge c).$$

Нарешті, використовуючи абсорбцію, отримуємо одне із співвідношень дистрибутивності для трійки $\{a, b, c\}$:

$$(a \vee b) \wedge (a \vee c) = a \vee (b \wedge c).$$

Отже, враховуючи теорему 2.7, робимо висновок про дистрибутивність трійки $\{a, b, c\}$. Теорему доведено. $\square$

2.7.3. Критерій дистрибутивності для модулярних решіток

Нагадаємо, що будь-яка дистрибутивна решітка є модулярною (див. вправу 2.8), але існують недистрибутивні модулярні решітки – одним із прикладів є $\mathcal{K}_2$.

Виявляється, що $\mathcal{K}_2$ у деякому сенсі найпростіша недистрибутивна модулярна решітка.

Теорема 2.9 (критерій дистрибутивності для модулярних решіток)**.** *Модулярна решітка є дистрибутивною тоді і тільки тоді, коли вона не містить підрешіток, ізоморфних решітці* $\mathcal{K}_2$.

Доведення. Очевидно, що жодна дистрибутивна решітка не може містити підрешітки, ізоморфної $\mathcal{K}_2$, оскільки решітка $\mathcal{K}_2$ не є дистрибутивною. Отже, залишається довести, що довільна модулярна недистрибутивна решітка обов'язково містить підрешітку, ізоморфну $\mathcal{K}_2$.

Нехай $\langle L, \vee, \wedge \rangle$ – модулярна недистрибутивна решітка, тобто для деяких $x, y, z \in L$ маємо нерівність

$$x \vee (y \wedge z) \neq (x \vee y) \wedge (x \vee z),$$

звідки з урахуванням твердження (2.12) отримуємо строге передування

$$x \vee (y \wedge z) \prec (x \vee y) \wedge (x \vee z). \tag{2.26}$$

Введемо до розгляду елементи

$$\begin{aligned} e_x &= (y \wedge z) \vee (x \wedge (y \vee z)); \\ e_y &= (x \wedge z) \vee (y \wedge (x \vee z)); \\ e_z &= (x \wedge y) \vee (z \wedge (x \vee y)). \end{aligned}$$

Доведемо, що підрешітку, ізоморфну $\mathcal{K}_2$, утворюють елементи

$$M(x, y, z),\ m(x, y, z),\ e_x,\ e_y,\ e_z. \tag{2.27}$$

Елементи e_x, e_y, e_z є самодвоїстими (збігаються зі своїми дуальними). Справді, для e_x за законом модулярності отримуємо:

$$\begin{gathered}(y \wedge z) \preccurlyeq (y \vee z) \Rightarrow (y \wedge z) \vee (x \wedge (y \vee z)) = \\ = ((y \wedge z) \vee x) \wedge (y \vee z) = (y \vee z) \wedge (x \vee (y \wedge z)).\end{gathered} \tag{2.28}$$

Самодвоїстість e_y та e_z отримуємо переставлянням елементів x, y, z у співвідношенні (2.28). Враховуючи, що елементи $M(x, y, z)$ і $m(x, y, z)$ взаємодуальні, можемо у подальших міркуваннях використовувати принцип дуальності.

Для доведення, що елементи (2.27) утворюють підрешітку, ізоморфну $\mathcal{K}_2$, обчислимо попарні диз'юнкції і кон'юнкції цих елементів. Почнемо із обчислення $e_x \vee e_y$:

$$e_x \vee e_y = (y \wedge z) \vee (x \wedge (y \vee z)) \vee (x \wedge z) \vee (y \wedge (x \vee z)) =$$

$$(\text{оскільки } y \wedge z \preccurlyeq y \wedge (x \vee z) \text{ та } x \wedge z \preccurlyeq x \wedge (y \vee z)\ )$$

$$= (x \wedge (y \vee z)) \vee (y \wedge (x \vee z)) =$$

$$(\text{оскільки } x \wedge (y \vee z) \preccurlyeq x \vee z\,)$$

$$= ((x \wedge (y \vee z)) \vee y) \wedge (x \vee z) =$$

$$(\text{оскільки } y \preccurlyeq y \vee z)$$

$$= ((x \vee y) \wedge (y \vee z)) \wedge (x \vee z) = M(x, y, z).$$

Переставляючи в отриманій рівності $e_x \vee e_y = M(x, y, z)$ елементи x, y, z, отримуємо:

$$e_x \vee e_y = e_x \vee e_z = e_y \vee e_z = M(x, y, z). \tag{2.29}$$

За дуальністю маємо:

$$e_x \wedge e_y = e_x \wedge e_z = e_y \wedge e_z = m(x, y, z). \tag{2.30}$$

Враховуючи отримані з рівностей (2.29) та (2.30) передування

$$\begin{aligned} &m(x, y, z) \preccurlyeq e_x \preccurlyeq M(x, y, z);\\ &m(x, y, z) \preccurlyeq e_y \preccurlyeq M(x, y, z);\\ &m(x, y, z) \preccurlyeq e_z \preccurlyeq M(x, y, z) \end{aligned} \tag{2.31}$$

і лему 1.4, яка визначає диз'юнкцію і кон'юнкцію порівнянних елементів, можемо вважати обчисленими всі попарні диз'юнкції і кон'юнкції елементів (2.27). Оскільки всі попарні диз'юнкції і кон'юнкції елементів (2.27) належать множині з елементів (2.27), ця множина замкнена за операціями вихідної решітки, а отже (див. зауваження 2.4) утворює підрешітку вихідної решітки $\langle L, \vee, \wedge\rangle$.

Доведемо, що елементи (2.27) є попарно різними. Припустивши, що $e_x = e_y$, отримуємо:

$$e_x \vee e_y = e_x \vee e_x = e_x,$$

звідки, враховуючи рівність (2.29), отримуємо: $e_x = e_y = M(x, y, z)$. Аналогічно, обчислюючи $e_x \wedge e_y$, отримуємо рівність $e_x = e_y = m(x, y, z)$. Отже, з припущення $e_x = e_y$ випливає рівність $M(x, y, z) = m(x, y, z)$, яка, враховуючи теорему 2.8, суперечить нерівності (2.26). Таким чином, $e_x \neq e_y$, і, за аналогічними міркуваннями, $e_x \neq e_z$ та $e_y \neq e_z$, тобто три елементи e_x, e_y, e_z є попарно різними.

Припустимо, що $e_x = M(x, y, z)$. Тоді, враховуючи вирази (2.30) і (2.31), отримаємо:

$$\begin{aligned} &m(x, y, z) = e_x \wedge e_y = M(x, y, z) \wedge e_y = e_y;\\ &m(x, y, z) = e_x \wedge e_z = M(x, y, z) \wedge e_z = e_z. \end{aligned}$$

Отже, з припущення $e_x = M(x, y, z)$ випливає $e_y = e_z = m(x, y, z)$, що суперечить доведеній вище нерівності $e_y \neq e_z$. Таким чином, доведено нерівність $e_x \neq M(x, y, z)$.

Аналогічно отримуємо нерівності $e_y \neq M(x, y, z)$ та $e_z \neq M(x, y, z)$, тобто жоден з елементів e_x, e_y, e_z не дорівнює елементу $M(x, y, z)$. Дуальними міркуваннями отримуємо, що жоден з елементів e_x, e_y, e_z не дорівнює $m(x, y, z)$.

Отже, всі елементи (2.27) справді попарно різні, тобто отримана підрешітка $\{M(x, y, z), m(x, y, z), e_x, e_y, e_z\}$ містить точно п'ять елементів і, враховуючи співвідношення (2.29), (2.30), (2.31), діаграма Гессе цієї підрешітки має вигляд, зображений на рис. 2.13.

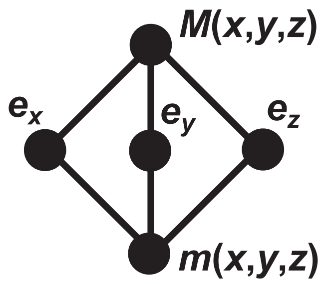


Рис. 2.13

Отже, елементи (2.27) утворюють підрешітку, ізоморфну решітці $\mathcal{K}_2$. Теорему доведено. □

Зауваження 2.10. Теорема 2.4 (критерій дистрибутивності) є безпосереднім наслідком теорем 2.6 і 2.9.

Розділ 3

Булеві алгебри

3.1. Основні поняття

Означення 3.1. Булевою алгеброю називають алгебричну структуру $\left\langle A, \vee, \wedge, \bar{\ }, 0, 1 \right\rangle$ із визначеними на непорожній множині A замкненими бінарними операціями «$\vee$» та «$\wedge$», замкненою унарною операцією «$\bar{\ }$» і фіксованими елементами $0, 1 \in A$ (нуль-арними операціями на A), які задовольняють умови:

1) $a \vee b = b \vee a$, $a \wedge b = b \wedge a$ (комутативність);

2) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ (дистрибутивність);

3) $a \vee 0 = a$, $a \wedge 1 = a$ (нейтральність);

4) $a \vee \overline{a} = 1$, $a \wedge \overline{a} = 0$ (доповненість).

Бінарні операції «$\vee$», «$\wedge$» називають відповідно диз'юнкцією та кон'юнкцією (вживають також інші назви: об'єднання й перетин, сума і добуток тощо); унарну операцію «$\bar{\ }$» називають доповненням. Елементи 0 та 1 називають відповідно нулем і одиницею булевої алгебри. Наведені умови (комутативність, дистрибутивність, нейтральність, доповненість) називають аксіомами булевої алгебри.

Приклад 3.1. 1. Найпростішою булевою алгеброю є структура $\langle\{0,1\},\vee,\wedge,\neg,0,1\rangle$; елементи 1 та 0 вважаються логічними, тобто позначають відповідно істинність і хибність; логічні операції «$\vee$», «$\wedge$» й «$\neg$» (диз'юнкція, кон'юнкція і заперечення) діють за законами алгебри висловлень.

2. Одним із найважливіших прикладів булевої алгебри є структура $\langle S,\cup,\cap,\ ^c,\varnothing,U\rangle$, де S – довільна алгебра множин із природними операціями (відповідно об'єднання, перетин і доповнення), роль нуля та одиниці відіграють відповідно порожня множина $\varnothing$ й універсальна множина U.

Оскільки аксіоми булевої алгебри сформульовані «дуальними парами», для булевих алгебр справджується принцип дуальності, аналогічний принципу дуальності для решіток: якщо у булевій алгебрі $\big\langle A,\vee,\wedge,\ \bar{}\ ,0,1\big\rangle$ правдиве деяке твердження, сформульоване з використанням операцій «$\vee$», «$\wedge$», «$\bar{\ }$» та елементів 0 і 1, то справджується дуальне твердження, отримане із вихідного заміною «$\vee$» на «$\wedge$», «$\wedge$» на «$\vee$», 0 на 1 та 1 на 0.

Із аксіом булевої алгебри можна вивести багато важливих законів. Наведемо деякі з них.

1. Закон універсальних меж: $a\vee 1=1$;
$a\wedge 0=0$.

2. Закон абсорбції (поглинання): $a\vee(a\wedge b)=a$;
$a\wedge(a\vee b)=a$.

3. Закон ідемпотентності: $a\vee a=a$;
$a\wedge a=a$.

4. Закон асоціативності (сполучний закон): $a\vee(b\vee c)=(a\vee b)\vee c$;
$a\wedge(b\wedge c)=(a\wedge b)\wedge c$.

5. Закон єдиності доповнення: система рівнянь $\begin{cases} a\vee x=1, \\ a\wedge x=0 \end{cases}$ відносно x має єдиний розв'язок $x=\overline{a}$ (тобто якщо $a\vee x=1$ та $a\wedge x=0$, то $x=\overline{a}$).

6. Закон інволютивності (подвійного заперечення): $\overline{\overline{a}} = a$.
7. Закони (правила) де Моргана: $\overline{a \vee b} = \overline{a} \wedge \overline{b}$;
$\overline{a \wedge b} = \overline{a} \vee \overline{b}$.
8. Закони склеювання: $(a \vee b) \wedge (a \vee \overline{b}) = a$;
$(a \wedge b) \vee (a \wedge \overline{b}) = a$.
9. Закони Порецького[1]: $a \wedge (\overline{a} \vee b) = a \wedge b$;
$a \vee (\overline{a} \wedge b) = a \vee b$.

Доведемо один із законів універсальних меж:

$$a \vee 1 = (a \vee 1) \wedge 1 = (a \vee 1) \wedge (a \vee \overline{a}) = a \vee (1 \wedge \overline{a}) = a \vee \overline{a} = 1.$$

Доведення другого закону універсальних меж можна побудувати за принципом дуальності.

Вправа 3.1. Довести закони 2–9 самостійно.

Вказівка. Тотожності зручно доводити у тій самій послідовності, в якій вони тут наведені. Крім того, завдяки принципу дуальності досить довести лише одну тотожність з кожної дуальної пари.

3.2. Булеві алгебри і решітки

3.2.1. Булева алгебра як решітка

Теорема 3.1. *Нехай* $\langle A, \vee, \wedge, \bar{}\,, 0, 1 \rangle$ *– булева алгебра. Тоді:*

1) алгебрична структура $\langle A, \vee, \wedge \rangle$ *– решітка;*

2) решітка $\langle A, \vee, \wedge \rangle$ *– обмежена, дистрибутивна, доповнена.*

[1] Порецький Платон Сергійович (1846–1907) – російський астроном і математик; активно займався проблемами математичної логіки, зокрема – розв'язанням логічних рівнянь.

Доведення. Алгебрична структура $\langle A, \vee, \wedge \rangle$ є дистрибутивною решіткою, оскільки комутативність і дистрибутивність – аксіоми булевої алгебри, а асоціативність та абсорбцію можна вивести із аксіом булевої алгебри безпосередньо (див. вправу 3.1).

Із аксіоми нейтральності отримуємо, що нуль та одиниця булевої алгебри є нулем і одиницею решітки:

$$(0 \preccurlyeq a) \Leftrightarrow (0 \vee a = a); \ (1 \succcurlyeq a) \Leftrightarrow (1 \wedge a = a) \quad (a \in A), \tag{3.1}$$

тобто $0 = \inf A$, $1 = \sup A$.

Із аксіоми доповненості випливає, що кожен елемент $a \in A$ має в решітці $\langle A, \vee, \wedge \rangle$ доповнення $\overline{a}$. □

3.2.2. Решітка як булева алгебра

Нехай $\langle A, \vee, \wedge \rangle$ – решітка, і нехай ця решітка обмежена, дистрибутивна і доповнена. За властивостями доповненості і дистрибутивності кожен елемент $a \in A$ має єдине доповнення $\overline{a}$. Отже, можемо ввести на множині A унарну операцію взяття доповнення: $a \mapsto \overline{a}$.

Теорема 3.2. *Нехай $\langle A, \vee, \wedge \rangle$ – обмежена, дистрибутивна і доповнена решітка з нулем 0 та одиницею 1. Тоді алгебрична структура $\left\langle A, \vee, \wedge, \overline{}, 0, 1 \right\rangle$ ($\overline{a}$ – доповнення до $a \in A$) є булевою алгеброю.*

Доведення. Справедливість аксіом комутативності і дистрибутивності випливає із означення дистрибутивної решітки, нейтральність випливає із обмеженості вихідної решітки $\langle A, \vee, \wedge \rangle$ (див. еквівалентності (3.1)). Аксіома доповненості фактично є визначенням доповнення $\overline{a}$ до елемента $a \in A$. □

Із теорем 3.1 і 3.2 випливає, що булеву алгебру можна еквівалентним чином визначити як решітку, яка є обмеженою, дистрибутивною і доповненою.

Приклад 3.2. Решітка $\langle \mathcal{L}_n, \vdots \rangle$ для будь-якого $n \in \mathbb{N}$ дистрибутивна та обмежена (див. приклади 2.7 і 2.10), однак доповненою ця решітка є лише у випадку $n = p_1 p_2 \cdots p_m$, де p_1, p_2, ..., p_m – попарно різні прості числа (див. приклад 2.15, п. 4). Отже, решітка $\langle \mathcal{L}_n, \vdots \rangle$ є булевою алгеброю тоді і тільки тоді, коли n є добутком попарно різних простих чисел (розклад n на прості множники «вільний від квадратів»).

Розглядаючи булеву алгебру як решітку, а отже і як ЧВМ, можемо розширити еквівалентність (2.1), використовуючи операцію доповнення.

Вправа 3.2. Довести еквівалентності ($a, b \in A$):

$$\begin{gathered} a \preccurlyeq b \Leftrightarrow a \vee b = b \Leftrightarrow a \wedge b = a \Leftrightarrow a \wedge \overline{b} = 0 \Leftrightarrow \overline{a} \vee b = 1; \\ a \preccurlyeq b \Leftrightarrow \overline{b} \preccurlyeq \overline{a}. \end{gathered} \tag{3.2}$$

Приклад 3.3. В алгебрі множин $\langle S, \cup, \cap, {}^c, \varnothing, U \rangle$ еквівалентності (3.2) набувають вигляду відомих співвідношень:

$$\begin{gathered} A \subset B \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A \Leftrightarrow A \cap \overline{B} = 0 \Leftrightarrow \overline{A} \cup B = 1; \\ A \subset B \Leftrightarrow \overline{B} \subset \overline{A}, \end{gathered}$$

де $A, B \in S$.

3.3. Булеві алгебри та ідемпотентні кільця

3.3.1. Булева алгебра як ідемпотентне кільце

Нехай $\left\langle A, \vee, \wedge, {}^{-}, 0, 1 \right\rangle$ – булева алгебра. На множині A введемо бінарні операції суми і множення:

$$\begin{gathered} a \oplus b = (a \wedge \overline{b}) \vee (\overline{a} \wedge b); \\ a \cdot b = a \wedge b. \end{gathered} \tag{3.3}$$

Теорема 3.3. $\langle A, \oplus, \cdot \rangle$ – *ідемпотентне кільце з одиницею* $1 \in A$.

Доведення. Насамперед наголосимо, що одиницею і нулем кільця $\langle A, \oplus, \cdot \rangle$ мають бути саме елементи 1 та 0, які є одиницею і нулем вихідної булевої алгебри $\langle A, \vee, \wedge, \bar{\ }, 0, 1 \rangle$. Також нагадаємо, що в ідемпотентному кільці елемент збігається зі своїм протилежним, тобто $a = -a$ (або, в еквівалентному вигляді, $a \oplus a = 0$).

Очевидно, що для алгебричної структури $\langle A, \oplus, \cdot \rangle$ треба довести аксіоми кільця, властивість ідемпотентності для множення та нейтральність елемента $1 \in A$ відносно множення ($a, b, c \in A$):

1) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$;

2) $a \oplus b = b \oplus a$;

3) $a \oplus 0 = a$;

4) $a \oplus a = 0$;

5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

6) $(a \oplus b) \cdot c = a \cdot c \oplus b \cdot c, \quad c \cdot (a \oplus b) = c \cdot a \oplus c \cdot b$;

7) $a^2 = a$;

8) $a \cdot 1 = 1 \cdot a = a$.

Доведення тотожностей 1–8 суттєво спроститься, якщо врахувати, що із комутативності кон'юнкції «$\wedge$» випливає комутативність множення «$\cdot$» (нагадаємо, що будь-яке ідемпотентне кільце комутативне, однак наразі ще не доведено, що алгебрична структура $\langle A, \oplus, \cdot \rangle$ є кільцем). Наведені тотожності можна перевірити, підставляючи замість операцій «$\oplus$» і «$\cdot$» відповідні вирази за визначенням (3.3) з подальшим спрощенням отриманих виразів.

Тотожності 2–5, 7 та 8 досить очевидні, якщо врахувати рівності

$$\overline{0} = 1; \quad \overline{1} = 0. \tag{3.4}$$

Зазначимо, що рівності (3.4) не є аксіомами булевої алгебри, однак вони випливають із закону єдиності доповнення:

$$\begin{cases} 0 \vee 1 = 1 \\ 0 \wedge 1 = 0 \end{cases} \Rightarrow\ 1 = \overline{0}; \quad \begin{cases} 1 \vee 0 = 1 \\ 1 \wedge 0 = 0 \end{cases} \Rightarrow\ 0 = \overline{1}.$$

Доведемо тотожності 1 (асоціативність операції «$\oplus$») та 6 (дистрибутивність «$\cdot$» відносно «$\oplus$»).

Для лівої частини тотожності 1, використовуючи закони булевої алгебри, зокрема дистрибутивність і правило де Моргана, отримуємо:

$$\begin{gathered}
(a \oplus b) \oplus c = ((a \wedge \overline{b}) \vee (\overline{a} \wedge b)) \oplus c = \\
= \big(((a \wedge \overline{b}) \vee (\overline{a} \wedge b)) \wedge \overline{c}\big) \vee \Big(\overline{((a \wedge \overline{b}) \vee (\overline{a} \wedge b))} \wedge c\Big) = \\
= \big((a \wedge \overline{b} \wedge \overline{c}) \vee (\overline{a} \wedge b \wedge \overline{c})\big) \vee \big(((\overline{a} \vee b) \wedge (a \vee \overline{b})) \wedge c\big) = \\
= (a \wedge \overline{b} \wedge \overline{c}) \vee (\overline{a} \wedge b \wedge \overline{c}) \vee \left((\underbrace{(\overline{a} \wedge a)}_{=0} \vee (\overline{a} \wedge \overline{b}) \vee (b \wedge a) \vee \underbrace{(b \wedge \overline{b})}_{=0}) \wedge c \right) = \\
= (a \wedge \overline{b} \wedge \overline{c}) \vee (\overline{a} \wedge b \wedge \overline{c}) \vee \big(((\overline{a} \wedge \overline{b}) \vee (a \wedge b)) \wedge c\big) = \\
= (a \wedge \overline{b} \wedge \overline{c}) \vee (\overline{a} \wedge b \wedge \overline{c}) \vee (\overline{a} \wedge \overline{b} \wedge c) \vee (a \wedge b \wedge c) = \\
= (a \wedge b \wedge c) \vee (a \wedge \overline{b} \wedge \overline{c}) \vee (\overline{a} \wedge b \wedge \overline{c}) \vee (\overline{a} \wedge \overline{b} \wedge c).
\end{gathered}$$

Очевидно, що отриманий вираз симетричний відносно входжень a, b та c, тобто не змінюється із переставленням цих літер. Враховуючи комутативність операції «$\oplus$» (тотожність 2 є очевидною), можемо подати праву частину тотожності 1 у вигляді $(b \oplus c) \oplus a$. Вираз $(b \oplus c) \oplus a$ можна отримати із виразу $(a \oplus b) \oplus c$ переставленням (циклічним зсувом) літер a, b та c, що завершує доведення тотожності 1.

Щодо двох тотожностей 6, то з урахуванням комутативності операції «$\cdot$» достатньо довести одну із них, наприклад першу. Для лівої і правої частин першої тотожності 6 отримуємо:

$$(a \oplus b) \cdot c = ((a \wedge \overline{b}) \vee (\overline{a} \wedge b)) \wedge c = (a \wedge \overline{b} \wedge c) \vee (\overline{a} \wedge b \wedge c);$$
$$a \cdot c \oplus b \cdot c = ((a \wedge c) \wedge \overline{(b \wedge c)}) \vee (\overline{(a \wedge c)} \wedge (b \wedge c)) =$$
$$= (a \wedge c \wedge (\overline{b} \vee \overline{c})) \vee ((\overline{a} \vee \overline{c}) \wedge b \wedge c) = (a \wedge c \wedge \overline{b}) \vee (\overline{a} \wedge b \wedge c),$$

застосувавши на останньому кроці закон Порецького. Отже, першу (а з урахуванням комутативності «·» і другу) тотожність 6 доведено.

Теорему доведено. □

3.3.2. Ідемпотентне кільце як булева алгебра

Нехай $\langle A, \oplus, \cdot \rangle$ – ідемпотентне кільце з одиницею $1 \in A$. На множині A введемо операції диз'юнкції «$\vee$», кон'юнкції «$\wedge$» і доповнення «$\bar{\ }$»:

$$\begin{aligned} a \vee b &= a \oplus b \oplus a \cdot b; \\ a \wedge b &= a \cdot b; \\ \overline{a} &= 1 \oplus a. \end{aligned} \tag{3.5}$$

Теорема 3.4. $\left\langle A, \vee, \wedge, \bar{\ }, 0, 1 \right\rangle$ *– булева алгебра, де* $0, 1 \in A$ *є нулем та одиницею кільця* $\langle A, \oplus, \cdot \rangle$.

Доведення. Потрібно довести чотири дуальні пари тотожностей – аксіом булевої алгебри:

1) $a \vee b = b \vee a$, $a \wedge b = b \wedge a$;

2) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;

3) $a \vee 0 = a$, $a \wedge 1 = a$;

4) $a \vee \overline{a} = 1$, $a \wedge \overline{a} = 0$.

Наведені тотожності можна перевірити, підставляючи замість операцій «$\wedge$», «$\vee$» й «$\bar{\ }$» відповідні вирази за визначенням (3.5) з подальшим спрощенням отриманих виразів. Зазначимо, що принцип дуальності у цьому випадку застосовувати не можна, оскільки тотожності 1–4 будемо доводити із аксіом ідемпотентного кільця, які не є дуальними парами.

Нагадаємо, що в ідемпотентному кільці обидві операції «$\oplus$» та «$\cdot$» комутативні, звідки випливають рівності 1 (комутативність). Також дуже легко перевірити тотожності 3 (нейтральність) та 4 (доповненість). Доведемо тотожності 2 (дистрибутивність):

$$a \vee (b \wedge c) = a \vee (b \cdot c) = a \oplus b \cdot c \oplus a \cdot b \cdot c;$$

$$(a \vee b) \wedge (a \vee c) = (a \oplus b \oplus a \cdot b) \cdot (a \oplus c \oplus a \cdot c) =$$

$$= a^2 \oplus a \cdot c \oplus a^2 \cdot c \oplus b \cdot a \oplus b \cdot c \oplus b \cdot a \cdot c \oplus a^2 \cdot b \oplus a \cdot b \cdot c \oplus a^2 \cdot b \cdot c =$$

$$= a \oplus a \cdot c \oplus a \cdot c \oplus a \cdot b \oplus b \cdot c \oplus a \cdot b \cdot c \oplus a \cdot b \oplus a \cdot b \cdot c \oplus a \cdot b \cdot c =$$

$$= a \oplus b \cdot c \oplus a \cdot b \cdot c;$$

$$a \wedge (b \vee c) = a \cdot (b \oplus c \oplus b \cdot c) = a \cdot b \oplus a \cdot c \oplus a \cdot b \cdot c;$$

$$(a \wedge b) \vee (a \wedge c) = a \cdot b \oplus a \cdot c \oplus a \cdot b \cdot a \cdot c = a \cdot b \oplus a \cdot c \oplus a \cdot b \cdot c.$$

Отже, теорему доведено. $\square$

3.3.3. Взаємна оберненість переходів між булевою алгеброю та ідемпотентним кільцем

Нехай $\langle A, \oplus, \cdot \rangle$ – ідемпотентне кільце з одиницею, $\left\langle A, \vee, \wedge, \bar{\ }, 0, 1 \right\rangle$ – булева алгебра, побудована з ідемпотентного кільця $\langle A, \oplus, \cdot \rangle$ за співвідношеннями (3.5). Розглянемо ідемпотентне кільце $\left\langle A, \hat{\oplus}, \hat{\cdot} \right\rangle$, побудоване із булевої алгебри $\left\langle A, \vee, \wedge, \bar{\ }, 0, 1 \right\rangle$ за співвідношеннями (3.3):

$$a \mathbin{\hat{\oplus}} b = (a \wedge \overline{b}) \vee (\overline{a} \wedge b);$$

$$a \mathbin{\hat{\cdot}} b = a \wedge b.$$

Теорема 3.5. *Операції «$\hat{\oplus}$» та «$\hat{\cdot}$» збігаються з операціями «$\oplus$» та «$\cdot$» відповідно, тобто*

$$a \mathbin{\hat{\oplus}} b = a \oplus b; \;\; a \mathbin{\hat{\cdot}} b = a \cdot b, \quad \forall\, a, b \in A.$$

Доведення. Тотожність $a \mathbin{\hat{\cdot}} b = a \cdot b$ є тривіальною, оскільки обидві операції збігаються з кон'юнкцією «$\wedge$». Доведемо першу тотожність:

$$a \mathbin{\hat{\oplus}} b = (a \wedge \overline{b}) \vee (\overline{a} \wedge b) = (a \cdot (1 \oplus b)) \oplus ((1 \oplus a) \cdot b) \oplus \underbrace{a \cdot \overline{b} \cdot \overline{a} \cdot b}_{=0} =$$

$$= a \oplus a \cdot b \oplus b \oplus a \cdot b = a \oplus b.$$

На другому переході використано очевидну рівність $x \cdot \overline{x} = x \wedge \overline{x} = 0$, $x \in A$. $\square$

Нехай тепер $\left\langle A, \vee, \wedge, \overline{}, 0, 1 \right\rangle$ – булева алгебра, $\langle A, \oplus, \cdot \rangle$ – ідемпотентне кільце з одиницею, побудоване із булевої алгебри $\left\langle A, \vee, \wedge, \overline{}, 0, 1 \right\rangle$ за співвідношеннями (3.3). Розглянемо булеву алгебру $\left\langle A, \hat{\vee}, \hat{\wedge}, \widehat{\overline{}}, 0, 1 \right\rangle$, побудовану із кільця $\langle A, \oplus, \cdot \rangle$ за співвідношеннями (3.5):

$$a \mathbin{\hat{\vee}} b = a \oplus b \oplus a \cdot b;$$
$$a \mathbin{\hat{\wedge}} b = a \cdot b;$$
$$\widehat{\overline{a}} = 1 \oplus a.$$

Теорема 3.6. *Операції «$\hat{\vee}$», «$\hat{\wedge}$» та «$\widehat{\overline{}}$» збігаються з операціями «$\vee$», «$\wedge$» та «$\overline{}$» відповідно, тобто*

$$a \mathbin{\hat{\vee}} b = a \vee b; \;\; a \mathbin{\hat{\wedge}} b = a \wedge b; \;\; \widehat{\overline{a}} = \overline{a}, \quad \forall\, a, b \in A.$$

Доведення. Тотожність $a \mathbin{\hat{\wedge}} b = a \wedge b$ є тривіальною, оскільки обидві операції збігаються з множенням «$\cdot$». Доведемо рівність для доповнень:

$$\widehat{\overline{a}} = 1 \oplus a = (1 \wedge \overline{a}) \vee (\overline{1} \wedge a) = \overline{a} \vee 0 = \overline{a}.$$

Рівність для диз'юнкцій отримуємо автоматично, оскільки правила де Моргана справедливі для будь-якої булевої алгебри:

$$a \vee b = \overline{\overline{a} \wedge \overline{b}} = a \mathbin{\hat{\vee}} b.$$

Теорему доведено. □

З теорем 3.3–3.6 видно, що будь-яку булеву алгебру можна розглядати як ідемпотентне кільце з одиницею і будь-яке ідемпотентне кільце з одиницею можна розглядати як булеву алгебру:

$$\left\langle A, \vee, \wedge, \bar{\ }, 0, 1 \right\rangle \leftrightarrow \langle A, \oplus, \cdot \rangle\,,$$

відповідність між операціями булевої алгебри та кільця визначається співвідношеннями (3.3) та (3.5).

Оскільки поняття «булева алгебра» та «ідемпотентне кільце з одиницею» – еквівалентні визначення однієї алгебричної структури, ідемпотентне кільце з одиницею часто називають *булевим кільцем*.

Приклад 3.4. Двохелементну булеву алгебру $\left\langle \{0,1\}, \vee, \wedge, \bar{\ }, 0, 1 \right\rangle$ можна розглядати як булеве кільце $\langle \{0,1\}, \oplus, \cdot \rangle$ з одиницею 1; елементи 0 та 1 позначають логічну істинність та хибність; операції «$\vee$» (диз'юнкція), «$\wedge$» (кон'юнкція), «$\bar{\ }$» (заперечення) та «$\oplus$» (сума за модулем 2) діють за законами алгебри висловлень; позначення «$\cdot$» еквівалентне позначенню «$\wedge$». Співвідношення (3.3) та (3.5) у цьому випадку набувають вигляду відомих тотожностей алгебри висловлень. Також очевидно, що булеве кільце $\langle \{0,1\}, \oplus, \cdot \rangle$ ізоморфне кільцю класів лишків $\mathbb{Z}_2$.

Приклад 3.5. Алгебру множин $\langle S, \cup, \cap, {}^c, \varnothing, U \rangle$ можна розглядати як булеве кільце (кільце множин) $\langle S, \triangle, \cap \rangle$ з одиницею U. Зазначимо, що позначення «$\cap$» (переріз множин) використано і для кон'юнкції у булевій алгебрі, і для множення у булевому кільці. Співвідношення (3.3) та (3.5) у цьому випадку набувають вигляду відомих тотожностей алгебри множин (тривіальні для цього випадку рівності між кон'юнкцією та множенням не виписуємо):

$$A \triangle B = (A \cap B^c) \cup (A^c \cap B);$$
$$A \cup B = A \triangle B \triangle (A \cap B);$$
$$A^c = U \triangle A.$$

3.4. Скінченні булеві алгебри

У цій главі розглядаємо скінченні булеві алгебри, тобто булеві алгебри $\langle A, \vee, \wedge, \bar{\ }, 0, 1 \rangle$ із скінченною множиною A.

3.4.1. Поняття і властивості атомів

Означення 3.2. Елемент $a \in A$ називають атомом булевої алгебри $\langle A, \vee, \wedge, \bar{\ }, 0, 1 \rangle$, якщо a безпосередньо слідує за нулем 0. Множину всіх атомів булевої алгебри A позначатимемо через A_1.

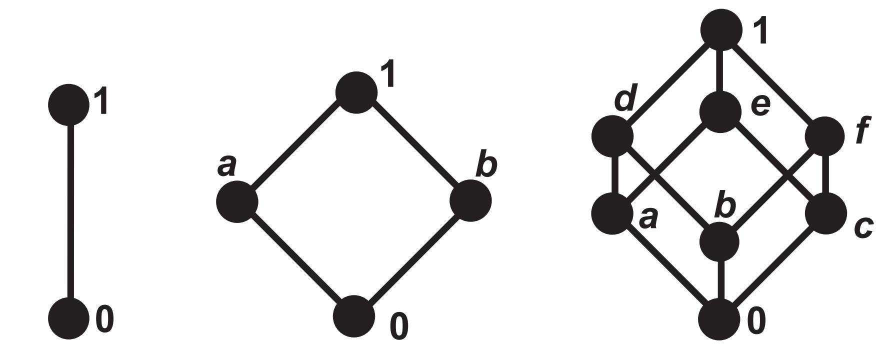
Приклад 3.6. 1. Нехай U – скінченна універсальна множина. Тоді алгебра множин $\langle 2^U, \cup, \cap, \ ^c, \varnothing, U \rangle$ – скінченна булева алгебра, атомами якої є одноелементні множини: $(2^U)_1 = \{\{a\} \colon a \in U\}$.

2. Решітка дільників $\langle \mathcal{L}_n, \vdots \rangle$ є скінченною булевою алгеброю, якщо $n = p_1 p_2 \cdots p_m$, де p_1, p_2, …, p_m – попарно різні прості числа (див. приклад 3.2). Очевидно, що числа p_k $(k = 1, 2, \ldots, m)$ і є атомами цієї булевої алгебри: $(\mathcal{L}_n)_1 = \{p_1, p_2, \ldots, p_m\}$.

3. У двохелементній булевій алгебрі $\langle \{0, 1\}, \vee, \wedge, \bar{\ }, 0, 1 \rangle$ єдиним атомом є елемент 1.

Очевидно, що на діаграмі Гессе атоми відповідають вершинам, суміжним з нулем булевої алгебри.

Приклад 3.7. Діаграми Гессе булевих алгебр A, B, C з одним, двома та трьома атомами відповідно зображено на рис. 3.1.



$A_1 = \{1\}$ $\quad$ $B_1 = \{a, b\}$ $\quad$ $C_1 = \{a, b, c\}$

Рис. 3.1

Лема 3.1. *Нехай A – скінченна булева алгебра, $c \in A$, $c \neq 0$. Тоді існує $a \in A_1$, такий, що $a \preccurlyeq c$ (кожному ненульовому елементу скінченної булевої алгебри передує хоча б один атом).*

Доведення. Якщо c – атом, твердження леми виконується ($c \in A_1$, $c \preccurlyeq c$). Отже, нехай c – не атом. Тоді, оскільки c не слідує за нулем безпосередньо, має існувати елемент $c_1 \neq 0$, $c_1 \prec c$. Якщо c_1 – атом, твердження леми виконується. Якщо c_1 – не атом, має існувати елемент $c_2 \neq 0$, $c_2 \prec c_1$ і, за транзитивністю відношення «$\prec$», $c_2 \prec c$. Взагалі, якщо $c_k \prec c$, $c_k \neq 0$, $c_k \notin A_1$, має існувати $c_{k+1} \neq 0$, $c_{k+1} \prec c_k \prec c$. Оскільки булева алгебра A скінченна, а всі елементи $c \succ c_1 \succ c_2 \cdots \succ c_k \succ c_{k+1}$ попарно різні, вказаний процес має обірватися. Отже, на деякому n-му кроці отримуємо: $c \succ c_1 \succ c_2 \cdots \succ c_n$, $c_n \in A_1$, що доводить твердження леми. □

Зауваження 3.1. Поняття атома можна ввести для довільних (не обов'язково скінченних) булевих алгебр і навіть для довільних решіток. Однак на нескінченні булеві алгебри твердження щойно доведеної леми не поширюється; більше того, можна навести приклад нескінченної булевої алгебри, яка не містить жодного атома. Детальніше про атомарність довільних булевих алгебр і решіток див. у роботах [5; 6].

Насамкінець доведемо два простих твердження, які випливають із визначення атома.

Лема 3.2. *Нехай* $a_1, a_2 \in A_1$, $a_1 \neq a_2$. *Тоді* $a_1 \wedge a_2 = 0$.

Доведення. Розглянемо елемент $c = a_1 \wedge a_2 = \inf\{a_1, a_2\}$. Із визначення інфімуму маємо: $c \preccurlyeq a_1$, $c \preccurlyeq a_2$. Будь-якому атому a передує лише сам атом a та елемент 0. Елемент c не може дорівнювати одночасно обом атомам a_1 і a_2, оскільки $a_1 \neq a_2$; отже, $c = a_1 \wedge a_2 = 0$. □

Лема 3.3. *Нехай* $a_1, a_2, \ldots, a_n \in A_1$, $a_i \neq a_j$ *для* $i \neq j$. *Тоді* $a_1 \vee a_2 \vee \cdots \vee a_n = a_1 \oplus a_2 \oplus \cdots \oplus a_n$.

Доведення. Доведення проведемо математичною індукцією за $n \geqslant 2$.

1. База індукції. Нехай $n = 2$. Тоді, використовуючи рівності (3.5), отримуємо:

$$a_1 \vee a_2 = a_1 \oplus a_2 \oplus a_1 \cdot a_2 = a_1 \oplus a_2 \oplus (a_1 \wedge a_2) = a_1 \oplus a_2.$$

2. Припущення індукції. Нехай твердження леми виконується для $n = n_0 \geqslant 2$.

3. Крок індукції. Нехай $n = n_0 + 1$. Тоді

$$a_{n_0+1} \wedge (a_1 \vee a_2 \vee \cdots \vee a_{n_0}) = (a_{n_0+1} \wedge a_1) \vee (a_{n_0+1} \wedge a_2) \vee \cdots \vee (a_{n_0+1} \wedge a_{n_0}) = 0.$$

Відтак, враховуючи припущення індукції та співвідношення (3.5), отримуємо:

$$a_1 \vee a_2 \vee \cdots \vee a_{n_0} \vee a_{n_0+1} = (a_1 \vee a_2 \vee \cdots \vee a_{n_0}) \oplus a_{n_0+1} = a_1 \oplus a_2 \oplus \cdots \oplus a_{n_0} \oplus a_{n_0+1}.$$

Лему доведено. □

Зауваження 3.2. Очевидно, що твердження леми 3.3 справджується для будь-яких $a_1, a_2, \ldots, a_n \in A$, таких, що $a_i \wedge a_j = 0$ для $i \neq j$.

3.4.2. Реалізація скінченної булевої алгебри у вигляді алгебри множин

Наведемо визначення ізоморфності булевих алгебр.

Означення 3.3. Булеві алгебри $\left\langle A, \vee, \wedge, \bar{\ }, 0, 1 \right\rangle$ і $\left\langle B, \hat{\vee}, \hat{\wedge}, \widehat{\bar{\ }}, \hat{0}, \hat{1} \right\rangle$ називаються ізоморфними, якщо існує бієкція (ізоморфізм) $f\colon A \to B$, така, що зберігає диз'юнкцію, кон'юнкцію та доповнення, тобто для довільних $a, a_1, a_2 \in A$

$$f(a_1 \vee a_2) = f(a_1) \mathbin{\hat{\vee}} f(a_2), \quad f(a_1 \wedge a_2) = f(a_1) \mathbin{\hat{\wedge}} f(a_2), \quad f(\overline{a}) = \widehat{\overline{f(a)}}.$$

Зауваження 3.3. Очевидно, що для ізоморфності булевих алгебр достатньо, щоб бієкція зберігала тільки дві операції – доповнення та одну із двох бінарних операцій (диз'юнкцію або кон'юнкцію), оскільки диз'юнкцію можна виразити через кон'юнкцію та доповнення (або кон'юнкцію через диз'юнкцію та доповнення) за допомогою правил де Моргана.

Вправа 3.3. Довести, що ізоморфізм f зберігає нуль та одиницю булевої алгебри, тобто $f(0) = \hat{0}$, $f(1) = \hat{1}$.

Доведемо, що довільна скінченна булева алгебра A ізоморфна деякій алгебрі множин, а саме алгебрі 2^{A_1} усіх підмножин множини атомів булевої алгебри A.

Для елемента $c \in A$ введемо позначення $A_c = \{a \in A_1 \colon a \preccurlyeq c\}$, тобто A_c позначає множину атомів, які передують елементу $c \in A$. Очевидно, що $A_0 = \varnothing$. Для $c = 1$ отримуємо множину всіх атомів булевої алгебри A, що узгоджується з уведеним в означенні 3.2 позначенням A_1 (с. 64).

Теорема 3.7. *Нехай $c \in A$, $c \neq 0$. Тоді $c = \bigvee\limits_{a \in A_c} a$ (довільний ненульовий елемент c збігається з диз'юнкцією атомів, які йому передують).*

Доведення. Позначимо $\tilde{c} = \bigvee\limits_{a \in A_c} a$. Потрібно довести рівність $\tilde{c} = c$.

Із співвідношення (2.4) та леми 3.3 випливає:

$$\tilde{c} = \sup A_c = \bigoplus_{a \in A_c} a.$$

Оскільки елемент c – верхня межа для A_c, із визначення супремуму випливає: $\tilde{c} = \sup A_c \preccurlyeq c$. Припустимо, що твердження теореми не справджується, тобто $\tilde{c} \prec c$. Оскільки $(\tilde{c} = c) \Leftrightarrow (\tilde{c} \oplus c = 0)$, із припущення $\tilde{c} \neq c$ отримуємо: $\tilde{c} \oplus c \neq 0$. Тепер із леми 3.1 випливає існування атома a_0, такого, що $a_0 \preccurlyeq \tilde{c} \oplus c$.

Доведемо, що $a_0 \in A_c$. Враховуючи передування $\tilde{c} \preccurlyeq c$ і використовуючи властивості булевої алгебри як ідемпотентного кільця, отримуємо:

$$(\tilde{c} \oplus c) \wedge c = (\tilde{c} \oplus c) \cdot c = \tilde{c} \cdot c \oplus c \cdot c = (\tilde{c} \wedge c) \oplus c = \tilde{c} \oplus c,$$

що доводить передування $\tilde{c} \oplus c \preccurlyeq c$. Таким чином, $a_0 \preccurlyeq \tilde{c} \oplus c \preccurlyeq c$, тобто $a_0 \in A_c$.

Розглянемо вираз $a_0 \cdot (\tilde{c} \oplus c)$. Оскільки $a_0 \preccurlyeq \tilde{c} \oplus c$, отримуємо рівність $a_0 \cdot (\tilde{c} \oplus c) = a_0$. Однак, використовуючи властивості булевої алгебри як ідемпотентного кільця, отримуємо:

$$a_0 \cdot (\tilde{c} \oplus c) = a_0 \cdot \tilde{c} \oplus a_0 \cdot c = (a_0 \wedge \tilde{c}) \oplus (a_0 \wedge c) = a_0 \oplus a_0 = 0.$$

Отже, отримана суперечність $a_0 = 0$ (атом a_0 дорівнює нулю) доводить хибність припущення $\tilde{c} \prec c$, тобто $\tilde{c} = c$. Теорему доведено. □

Наслідок. *Якщо* $A_{c_1} = A_{c_2}$ $(c_1, c_2 \in A)$, *то* $c_1 = c_2$.

Доведення. За доведеною теоремою отримуємо:

$$c_1 = \bigvee_{a \in A_{c_1}} a = \bigvee_{a \in A_{c_2}} a = c_2. \qquad \square$$

Зауваження 3.4. Вважаючи, що $\bigvee\limits_{a \in \varnothing} a = 0$, поширюємо теорему 3.7 на випадок $c = 0$: довільний елемент $c \in A$ збігається з диз'юнкцією атомів, які йому передують.

Теорема 3.8. *Нехай $c \in A$, $c = \bigvee\limits_{a \in B} a$, де $B \subset A_1$. Тоді $B = A_c$ (елемент можна зобразити у вигляді диз'юнкції атомів єдино можливим способом).*

Доведення. Для довільного атома $a_0 \in A_1$ отримуємо:

$$c \wedge a_0 = \left(\bigvee_{a \in B} a \right) \wedge a_0 = \bigvee_{a \in B} (a \wedge a_0).$$

Враховуючи результат леми 3.2, для кон'юнкції атомів a та a_0 маємо:

$$(a \wedge a_0) = \begin{cases} 0, & \text{якщо } a \neq a_0; \\ a_0, & \text{якщо } a = a_0, \end{cases}$$

звідки отримуємо:

$$c \wedge a_0 = \bigvee_{a \in B} (a \wedge a_0) = \begin{cases} 0, & \text{якщо } a_0 \notin B; \\ a_0, & \text{якщо } a_0 \in B. \end{cases} \tag{3.6}$$

Проте, враховуючи визначення атома,

$$\inf\{c, a_0\} = c \wedge a_0 = \begin{cases} 0, & \text{якщо } a_0 \notin A_c; \\ a_0, & \text{якщо } a_0 \in A_c. \end{cases} \tag{3.7}$$

Таким чином, зі співвідношень (3.6) і (3.7) для довільного атома a_0 маємо еквівалентність $(a_0 \in A_c) \Leftrightarrow (a_0 \in B)$, що доводить рівність $A_c = B$. □

Для скінченної булевої алгебри A з множиною атомів A_1 введемо відображення $f \colon A \to 2^{A_1}$, що діє за правилом

$$f(c) = A_c, \quad c \in A.$$

Лема 3.4. *Введене відображення f є бієкцією.*

Доведення. Ін'єктивність f встановлюється наслідком з теореми 3.7:

$$(f(c_1) = f(c_2)) \Leftrightarrow (A_{c_1} = A_{c_2}) \Rightarrow (c_1 = c_2).$$

Доведемо сюр'єктивність f. Для довільної множини $B \in 2^{A_1}$ ($B \subset A_1$) визначимо $c = \bigvee\limits_{a \in B} a$, звідки за теоремою 3.8 $B = A_c = f(c)$.

Отже, відображення f одночасно ін'єктивне і сюр'єктивне. Лему доведено. □

Із доведеної леми отримуємо несподіваний наслідок: скінченна булева алгебра A містить 2^n елементів, де $n = \mathrm{card}(A_1)$ – кількість атомів в A. Так, булеві алгебри з одним, двома та трьома атомами містять відповідно два, чотири та вісім елементів (рис. 3.1).

Теорема 3.9. *Нехай* $\left\langle A, \vee, \wedge, \bar{\ }, 0, 1 \right\rangle$ *– скінченна булева алгебра з множиною атомів* A_1. *Тоді відображення* $f\colon A \to 2^{A_1}$, *що діє за правилом* $f(c) = A_c$ $(c \in A)$, *є ізоморфізмом між* $\left\langle A, \vee, \wedge, \bar{\ }, 0, 1 \right\rangle$ *та булевою алгеброю* $\left\langle 2^{A_1}, \cup, \cap, {}^{c}, \varnothing, A_1 \right\rangle$ *множини всіх підмножин множини* A_1. *Ізоморфізм між булевими алгебрами* A *та* 2^{A_1} *можна встановити відображенням* $f\colon A \to 2^{A_1}$, $f(c) = A_c$ $(c \in A)$.

Доведення. З урахуванням результату леми 3.4 та зауваження 3.3, для доведення теореми залишилось показати, що відображення f зберігає кон'юнкцію і доповнення, тобто для довільних $a, a_1, a_2 \in A$ довести рівності

$$A_{a_1 \wedge a_2} = A_{a_1} \cap A_{a_2}, \quad A_{\overline{a}} = (A_a)^c.$$

Доведемо ці рівності модельним способом. Для довільного $x \in A_{a_1 \wedge a_2}$, використовуючи рівність (2.3), отримуємо:

$$(x \in A_{a_1 \wedge a_2}) \Leftrightarrow (x \preccurlyeq a_1 \wedge a_2) \Rightarrow \begin{cases} x \preccurlyeq a_1 \\ x \preccurlyeq a_2 \end{cases} \Leftrightarrow \begin{cases} x \in A_{a_1} \\ x \in A_{a_2} \end{cases} \Leftrightarrow (x \in A_{a_1} \cap A_{a_2}),$$

тобто $A_{a_1 \wedge a_2} \subset A_{a_1} \cap A_{a_2}$. Зафіксувавши $x \in A_{a_1} \cap A_{a_2}$, використовуючи рівність (2.9), отримуємо:

$$(x \in A_{a_1} \cap A_{a_2}) \Leftrightarrow \begin{cases} x \in A_{a_1} \\ x \in A_{a_2} \end{cases} \Leftrightarrow \begin{cases} x \preccurlyeq a_1 \\ x \preccurlyeq a_2 \end{cases} \Rightarrow (x \preccurlyeq a_1 \wedge a_2) \Leftrightarrow (x \in A_{a_1 \wedge a_2}),$$

тобто $A_{a_1} \cap A_{a_2} \subset A_{a_1 \wedge a_2}$. Отже, рівність $A_{a_1 \wedge a_2} = A_{a_1} \cap A_{a_2}$ доведено.

Для доведення рівності $A_{\overline{a}} = (A_a)^c$ зафіксуємо довільний атом $x \in A_1$ і розглянемо вираз $x \wedge (a \vee \overline{a})$:

$$x \wedge (a \vee \overline{a}) = (x \wedge a) \vee (x \wedge \overline{a}) = \begin{cases} 0, \text{ якщо } x \notin A_a \text{ та } x \notin A_{\overline{a}}; \\ x, \text{ якщо } x \in A_a \text{ або } x \in A_{\overline{a}}, \end{cases}$$

тобто, враховуючи очевидну рівність $x \wedge (a \vee \overline{a}) = x$, отримуємо, що атом x передує принаймні одному елементу a або $\overline{a}$. Припустивши, що x передує обом елементам a та $\overline{a}$, з урахуванням наслідка (2.9), отримуємо суперечність: $x \preccurlyeq a \wedge \overline{a} = 0$. Таким чином, атом x передує точно одному з елементів a або $\overline{a}$, тобто

$$(x \in A_{\overline{a}}) \Leftrightarrow (x \notin A_a) \Leftrightarrow (x \in (A_a)^c),$$

що доводить рівність $A_{\overline{a}} = (A_a)^c$. Теорему доведено. $\square$

Приклад 3.8. Діаграми Гессе булевої алгебри із трьох атомів та відповідної алгебри підмножин множини атомів зображено на рис. 3.2.

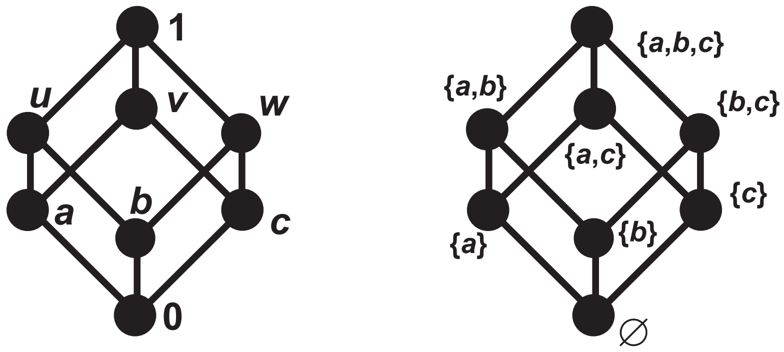


Рис. 3.2. Булева алгебра з атомами a, b, c та алгебра $2^{\{a,b,c\}}$ підмножин множини її атомів

Ізоморфізм f діє таким чином: $f(0) = \varnothing$; $f(a) = \{a\}$; $f(b) = \{b\}$; $f(c) = \{c\}$; $f(u) = \{a, b\}$; $f(v) = \{a, c\}$; $f(w) = \{b, c\}$; $f(1) = \{a, b, c\}$.

Приклад 3.9. Для булевої алгебри $\mathcal{L}_n$ дільників фіксованого числа $n = p_1 p_2 \cdots p_m$, де p_1, p_2, $\ldots$, p_m – попарно різні прості числа, отримуємо множину атомів $(\mathcal{L}_n)_1 = \{p_1, p_2, \ldots, p_m\}$. Ізоморфізм $f\colon \mathcal{L}_n \to 2^{\{p_1, p_2, \ldots, p_m\}}$ має вигляд

$$f(c) = \{p_k \, (k = 1, 2, \ldots, m)\colon \; c \,\vdots\, p_k\},$$

тобто кожному елементу $c \in \mathcal{L}_n$ відповідає множина тих атомів p_k $(k = 1, 2, \ldots, m)$, які є дільниками числа c.

Зауваження 3.5. Теорема 3.9 про реалізацію скінченної булевої алгебри у вигляді алгебри множин допускає узагальнення на довільні, не обов'язково скінченні булеві алгебри: кожна булева алгебра ізоморфна деякій алгебрі множин (не обов'язково алгебрі множин вигляду 2^U, де U – деяка універсальна множина). Нагадаємо, що нескінченна булева алгебра може не містити жодного атома, і в цьому випадку ізоморфна їй алгебра множин не може мати вигляду 2^U, де U – деяка універсальна множина. Теорема про реалізацію довільної булевої алгебри у вигляді алгебри множин відома як теорема М. Стоуна[1] [6].

3.5. Диз'юнктивні і кон'юнктивні нормальні форми

3.5.1. Поняття виразу над булевою алгеброю

Нехай $\langle A, \vee, \wedge, \bar{\ }, 0, 1 \rangle$ – довільна булева алгебра. Для позначення довільних елементів із A використовуватимемо малі літери англійського

[1] Стоун Маршалл Гарвей (1903–1989) – американський математик, автор низки робіт з топології та функціонального аналізу.

алфавіту з індексами або без (a, b, c_1, $x_{2,5}$ і т. д.), які у цьому контексті називатимемо змінними.

Поняття *виразу над булевою алгеброю* $\langle A, \vee, \wedge, \bar{\ }, 0, 1 \rangle$ (або просто виразу) інтуїтивно зрозуміле, і такі вирази вже неодноразово використовували, проте формалізація потребує чітких визначень.

Означення 3.4. Множину виразів над $\langle A, \vee, \wedge, \bar{\ }, 0, 1 \rangle$ визначають такими трьома умовами:

- змінна й елементи 0 та 1 є виразами;
- якщо $\mathcal{A}$ та $\mathcal{B}$ – вирази, то $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \wedge \mathcal{B})$, $\overline{\mathcal{A}}$ – також вирази;
- інших виразів немає.

Приклад 3.10. Записи $(x \vee \overline{y})$; $(x_1 \wedge (a \vee y))$; $(1 \vee a)$ є виразами. Запис $x \vee y \wedge z$, згідно з означенням 3.4, не є виразом.

Надалі запис $x \to y$ вважатимемо скороченням для $\overline{x} \vee y$, запис $x \leftrightarrow y$ – скороченням для $(x \to y) \wedge (y \to x)$, запис $x \oplus y$ – скороченням для $\overline{x \leftrightarrow y}$. Зазначимо, що в алгебрі висловлень (див. приклад 3.1, п. 1) позначення «$\to$», «$\leftrightarrow$» та «$\oplus$» відповідають операціям імплікації, еквіваленції та сумі за модулем 2.

Щоб спростити запис, у виразах опускатимемо зовнішні дужки, що не містять додаткової інформації, проте неминуче з'являються, якщо у виразі є хоча б одна операція «$\wedge$» або «$\vee$». Так, замість виразу $(x \vee y)$ писатимемо $x \vee y$.

Для позначення виразів будемо використовувати англійську літеру E з індексами або без. За потреби у дужках вказуватимемо список змінних, які можуть міститись у певному виразі (у цьому випадку говоритимемо про вираз над відповідними змінними). Так, $E(x, y, z)$ може позначати будь-який вираз над трьома змінними x, y, z (можливо, у записі використовуються не всі три): $E(x, y, z) = (x \vee y) \wedge z$; $E(x, y, z) = x \vee \overline{y}$; $E(x, y, z) = \overline{z}$.

Кожний вираз $E(x_1, \ldots, x_n)$ над булевою алгеброю A природно визначає деяке відображення із $A^{\times n}$ в A. Так, у випадку алгебри множин $\langle S, \cup, \cap, {}^c, \varnothing, U \rangle$ вирази $E_1(A_1, A_2) = A_1 \cup A_2$, $E_2(A_1, A_2) = A_1 \cap A_2$, $E_3(A_1, A_2) = A_1 \cap A_2^c$ визначають відповідно операції об'єднання, перетину та різниці.

Зауваження 3.6. Для позначення елементів алгебри множин традиційно використовують великі літери англійського алфавіту.

Водночас кожне відображення із $A^{\times n}$ в A, задане деяким виразом над булевою алгеброю A, можна подати різними виразами. Так, вирази $E_1(x, y) = x \vee y$; $E_2(x, y) = y \vee (\overline{y} \wedge x)$ та $E_3(x, y) = x \vee (\overline{x} \wedge y)$ визначають одне й те саме відображення $(x, y) \mapsto x \vee y$. Вирази, які визначають однакові відображення, називатимемо *еквівалентними*.

Насамкінець зазначимо, що у випадку, коли булева алгебра A містить більше двох елементів, не кожне відображення $f\colon A^{\times n} \to A$ можна задати виразом над A (див. приклад 3.22 на с. 85).

3.5.2. Диз'юнктивні нормальні форми

Означення 3.5. Вираз над булевою алгеброю називають кон'юнктом, якщо він має вигляд кон'юнкції змінних або їх доповнень.

Приклад 3.11. Вирази $x \wedge \overline{y}$, $(x \wedge y) \wedge \overline{z}$, $\overline{x}$, y – кон'юнкти. Вираз $x \vee y$ – не кон'юнкт.

Оскільки вирази $(x \wedge y) \wedge z$ та $x \wedge (y \wedge z)$ визначають одне й те саме відображення, дужки у записі кон'юнкта будемо опускати. Так, замість $(x \wedge y) \wedge \overline{z}$ або $x \wedge (y \wedge \overline{z})$ записуватимемо $x \wedge y \wedge \overline{z}$.

Надалі ототожнюватимемо кон'юнкти, які відрізняються лише послідовністю запису аргументів кон'юнкції. Так, не будемо розрізняти кон'юнкти $x \wedge y \wedge \overline{z}$, $x \wedge \overline{z} \wedge y$ та $\overline{z} \wedge y \wedge x$.

Зазначимо, що кон'юнкт із двома або більше входженнями деякої змінної можна замінити еквівалентним кон'юнктом без повторних входжень цієї змінної. Надалі вважатимемо, що кожна змінна входить у кон'юнкт не більше одного разу.

Кількість змінних у кон'юнкті називають *довжиною кон'юнкта*. За визначенням, вважатимемо вираз 1 кон'юнктом довжини 0, цей кон'юнкт називають *порожнім*. Кон'юнкт $E(x_1, \ldots, x_n)$, який містить усі n змінних, називатимемо *кон'юнктом повної довжини*. Очевидно, що говорити про повну чи неповну довжину кон'юнкта можна лише тоді, коли визначено, над якими змінними розглядається цей кон'юнкт. Так, кон'юнкт $x \wedge \overline{y}$ має повну довжину як кон'юнкт над змінними x, y, але має неповну довжину як кон'юнкт над x, y, z.

Означення 3.6. Вираз над булевою алгеброю називають диз'юнктивною нормальною формою (ДНФ), якщо він має вигляд диз'юнкції скінченної кількості кон'юнктів.

Надалі у записі ДНФ опускатимемо зовнішні дужки, а також ототожнюватимемо ДНФ, які відрізняються лише послідовністю запису кон'юнктів. Отже, ДНФ набуває вигляду $E_1 \vee E_2 \vee \cdots \vee E_k$, де $E_1, E_2, \ldots, E_k$ – довільні кон'юнкти. Вважатимемо, що кон'юнкти E_1, $E_2, \ldots$, E_k попарно різні (ДНФ не містить однакових кон'юнктів).

Приклад 3.12. Такі вирази є ДНФ:

1) $(x \wedge \overline{y}) \vee (y \wedge z) \vee (\overline{x} \wedge y \wedge \overline{z})$ (три кон'юнкти довжиною 2, 2 і 3 відповідно);

2) $\overline{x} \wedge y$ (один кон'юнкт довжиною 2);

3) $x \vee \overline{y}$ (два кон'юнкти, обидва довжиною 1);

4) 1 (один порожній кон'юнкт).

За визначенням, вираз 0 також вважають диз'юнктивною нормальною формою, яка не містить жодного кон'юнкта.

Теорема 3.10. *Будь-який вираз над булевою алгеброю можна зобразити у вигляді ДНФ (для будь-якого виразу існує еквівалентна ДНФ).*

Доведення. Наведемо конкретний метод зведення виразу до ДНФ.

1. Використовуючи правила де Моргана $\overline{E_1 \vee E_2} = \overline{E}_1 \wedge \overline{E}_2$ та інволютивність $\overline{\overline{E}} = E$ забезпечуємо, щоб операції доповнення застосовувалися лише безпосередньо до змінних.

2. Використовуючи потрібну кількість разів закон дистрибутивності $E_1 \wedge (E_2 \vee E_3) = (E_1 \wedge E_2) \vee (E_1 \wedge E_3)$ забезпечуємо, щоб операція кон'юнкції не застосовувалася до виразів, які містять диз'юнкцію.

3. Застосовуючи закони ідемпотентності, нейтральності та універсальних меж забезпечуємо, щоб кон'юнкти в отриманому виразі не містили повторних входжень однієї змінної

Наведений метод за скінченну кількість кроків зводить вираз до ДНФ. □

Приклад 3.13. Зведемо до ДНФ вираз $x \wedge \overline{((x \vee \overline{y}) \wedge \overline{x \wedge \overline{z}})}$ та $x \vee (y \wedge \overline{x \wedge \overline{z}})$:

$$x \wedge \overline{((x \vee \overline{y}) \wedge \overline{x \wedge \overline{z}})} = x \wedge ((\overline{x} \wedge y) \vee (x \wedge \overline{z})) = (x \wedge \overline{x} \wedge y) \vee (x \wedge x \wedge \overline{z}) = x \wedge \overline{z};$$

$$x \vee (y \wedge \overline{x \wedge \overline{z}}) = x \vee (y \wedge (\overline{x} \vee z)) = x \vee (y \wedge \overline{x}) \vee (y \wedge z).$$

Зображення виразу у вигляді ДНФ ніколи не буває єдиним. Так, наприклад, $x = x \vee (x \wedge y) = (x \wedge \overline{y}) \vee (x \wedge y)$.

Означення 3.7. Диз'юнктивну нормальну форму називають досконалою (ДДНФ), якщо вона містить лише кон'юнкти повної довжини.

Приклад 3.14. Такі ДНФ є досконалими:

1) $E(x, y) = (x \wedge y) \vee (\overline{x} \wedge y)$;

2) $E(x, y, z) = (x \wedge y \wedge \overline{z}) \vee (\overline{x} \wedge y \wedge z)$;

3) $E(x) = x$.

Нагадаємо, що повнота чи неповнота довжини кон'юнкта, а отже і досконалість чи недосконалість ДНФ, залежать від того, над якими змінними розглядається заданий вираз. Так, ДНФ $\overline{x}$ досконала як вираз над однією змінною x і недосконала як вираз над змінними x, y.

Вираз 0, який за визначенням вважають диз'юнктивною нормальною формою без жодного кон'юнкта, також є досконалою диз'юнктивною нормальною формою, оскільки не містить жодного кон'юнкта неповної довжини.

Теорема 3.11. *Будь-який вираз над булевою алгеброю можна зобразити у вигляді ДДНФ.*

Доведення. З урахуванням теореми 3.10 можна вважати, що заданий вираз – ДНФ. Опишемо конкретну процедуру зведення ДНФ до ДДНФ. Припустимо, що у вираз входить кон'юнкт E неповної довжини, який не містить змінної x. Такий кон'юнкт E застосуванням закону склеювання можемо замінити на диз'юнкцію двох кон'юнктів більшої довжини (із додатковою змінною x):

$$E = (E \wedge x) \vee (E \wedge \overline{x}).$$

Таке перетворення виконуватимемо для кожного кон'юнкта неповної довжини. Легко зрозуміти, що за скінченну кількість кроків усі кон'юнкти отриманої ДНФ матимуть повну довжину. □

Приклад 3.15. 1. Зведемо до ДДНФ вираз $E(x,y) = (x \wedge \overline{y}) \vee \overline{x}$. Другий кон'юнкт має неповну довжину (не вистачає змінної y). Застосуванням закону склеювання отримуємо:

$$E(x,y) = (x \wedge \overline{y}) \vee \overline{x} = (x \wedge \overline{y}) \vee (\overline{x} \wedge y) \vee (\overline{x} \wedge \overline{y}).$$

2. Зведемо до ДДНФ вираз $E(x,y,z) = (x \wedge y) \vee \overline{z}$. Неповну довжину мають перший і другий кон'юнкти: перший кон'юнкт не містить змінної z, у другому кон'юнкті не вистачає двох змінних – x та y. Спочатку зведемо до повної довжини перший кон'юнкт:

$$(x \wedge y) = (x \wedge y \wedge z) \vee (x \wedge y \wedge \overline{z}).$$

Тепер до кон'юнкта $\overline{z}$ додамо по черзі змінні x та y:

$$\overline{z} = (x \wedge \overline{z}) \vee (\overline{x} \wedge \overline{z}) = (x \wedge y \wedge \overline{z}) \vee (x \wedge \overline{y} \wedge \overline{z}) \vee (\overline{x} \wedge y \wedge \overline{z}) \vee (\overline{x} \wedge \overline{y} \wedge \overline{z}).$$

Виключаючи повторення кон'юнкта $(x \wedge y \wedge \overline{z})$, остаточно отримуємо:

$$E(x, y, z) = (x \wedge y \wedge z) \vee (x \wedge y \wedge \overline{z}) \vee (x \wedge \overline{y} \wedge \overline{z}) \vee (\overline{x} \wedge y \wedge \overline{z}) \vee (\overline{x} \wedge \overline{y} \wedge \overline{z}).$$

3. Зведемо до ДДНФ вираз $E(x, y) = 1$. Маємо один порожній кон'юнкт, до якого потрібно додати дві змінні:

$$E(x, y) = x \vee \overline{x} = (x \wedge y) \vee (x \wedge \overline{y}) \vee (\overline{x} \wedge y) \vee (\overline{x} \wedge \overline{y}).$$

3.5.3. Кон'юнктивні нормальні форми

Визначення диз'юнкта, кон'юнктивної та досконалої кон'юнктивної нормальних форм є дуальними до визначень кон'юнкта, диз'юнктивної та досконалої диз'юнктивної нормальних форм відповідно.

Означення 3.8. Вираз над булевою алгеброю називають диз'юнктом, якщо він має вигляд диз'юнкції змінних або їх доповнень.

Приклад 3.16. Вирази $x \vee \overline{y}$, $(x \vee y) \vee \overline{z}$, $\overline{x}$, y – диз'юнкти. Вираз $x \wedge y$ – не диз'юнкт.

Оскільки вирази $(x \vee y) \vee z$ та $x \vee (y \vee z)$ визначають одне й те саме відображення, дужки у записі диз'юнкта будемо опускати. Так, замість $(x \vee y) \vee \overline{z}$ або $x \vee (y \vee \overline{z})$ використовуватимемо запис $x \vee y \vee \overline{z}$. Крім того, ототожнюватимемо диз'юнкти, які відрізняються лише послідовністю запису аргументів диз'юнкції. Так, не будемо розрізняти диз'юнкти $x \vee y \vee \overline{z}$, $x \vee \overline{z} \vee y$ і $\overline{z} \vee y \vee x$. Вважатимемо також, що кожна змінна входить у диз'юнкт не більше одного разу.

Кількість змінних у диз'юнкті називають *довжиною диз'юнкта*. Вираз 0 за визначенням вважають диз'юнктом довжини 0 і називають *порожнім*. Диз'юнкт $E(x_1, \ldots, x_n)$, який містить усі n змінних, називатимемо *диз'юнктом повної довжини*. Очевидно, що говорити про повну чи неповну довжину диз'юнкта можна лише тоді, коли визначено, над якими змінними розглядається цей вираз: диз'юнкт $x \vee \overline{y}$ має повну довжину над змінними x, y, але має неповну довжину над x, y, z.

Означення 3.9. Вираз над булевою алгеброю називають кон'юнктивною нормальною формою (КНФ), якщо він має вигляд кон'юнкції скінченної кількості диз'юнктів.

Надалі у записі КНФ будемо опускати зовнішні дужки, а також ототожнюватимемо КНФ, які відрізняються лише послідовністю запису диз'юнктів. Таким чином, КНФ набуває вигляду $E_1 \wedge E_2 \wedge \cdots \wedge E_k$, де $E_1, E_2, \ldots, E_k$ – довільні диз'юнкти. Вважатимемо надалі, що диз'юнкти E_1, E_2,…, E_k попарно різні (КНФ не містить однакових диз'юнктів).

Приклад 3.17. Такі вирази є КНФ:

1) $(x \vee \overline{y}) \wedge (y \vee z) \wedge (\overline{x} \vee y \vee \overline{z})$ (три диз'юнкти довжиною 2, 2 і 3 відповідно);

2) $\overline{x} \vee y$ (один диз'юнкт довжиною 2);

3) $x \wedge \overline{y}$ (два диз'юнкти, обидва довжиною 1);

4) 0 (один порожній диз'юнкт).

За визначенням, вираз 1 також вважають кон'юнктивною нормальною формою, що не містить жодного диз'юнкта.

Теорема 3.12. *Будь-який вираз над булевою алгеброю можна зобразити у вигляді КНФ (для будь-якого виразу існує еквівалентна КНФ).*

Доведення. Метод зведення виразу до КНФ з точністю до дуальності повторює метод зведення виразу до ДНФ (див. доведення теореми 3.10). □

Приклад 3.18. Обчислимо КНФ виразів $x \vee \overline{((x \wedge \overline{y}) \vee \overline{x \vee \overline{z}})}$ та $x \wedge (y \vee \overline{x \vee \overline{z}})$:

$$x \vee \overline{((x \wedge \overline{y}) \vee \overline{x \vee \overline{z}})} = x \vee ((\overline{x} \vee y) \wedge (x \vee \overline{z})) = (x \vee \overline{x} \vee y) \wedge (x \vee x \vee \overline{z}) = x \vee \overline{z};$$
$$x \wedge (y \vee \overline{x \vee \overline{z}}) = x \wedge (y \vee (\overline{x} \wedge z)) = x \wedge (y \vee \overline{x}) \wedge (y \vee z).$$

Зображення виразу у вигляді КНФ ніколи не є єдиним. Так, наприклад, $x = x \wedge (x \vee y) = (x \vee \overline{y}) \wedge (x \vee y)$.

Означення 3.10. Кон'юнктивну нормальну форму називають досконалою (ДКНФ), якщо вона містить лише диз'юнкти повної довжини.

Приклад 3.19. Такі КНФ є досконалими:

1) $E(x, y) = (x \vee y) \wedge (\overline{x} \vee y)$;

2) $E(x, y, z) = (x \vee y \vee \overline{z}) \wedge (\overline{x} \vee y \vee z)$;

3) $E(x) = x$.

Очевидно, що досконалість чи недосконалість КНФ залежить від того, над якими змінними розглядається вираз. Так, КНФ $\overline{x}$ досконала як вираз над однією змінною x і недосконала як вираз над змінними x, y.

Вираз 1, який за визначенням вважають кон'юнктивною нормальною формою без жодного диз'юнкта, також є досконалою кон'юнктивною нормальною формою, оскільки не містить жодного диз'юнкта неповної довжини.

Теорема 3.13. *Будь-який вираз над булевою алгеброю можна зобразити у вигляді ДКНФ.*

Доведення. Процедура зведення КНФ до ДКНФ дуальна процедурі зведення ДНФ до ДДНФ (див. доведення теореми 3.11). $\square$

Приклад 3.20. 1. Зведемо до ДКНФ вираз $E(x, y) = (x \vee \overline{y}) \wedge \overline{x}$. Другий диз'юнкт має неповну довжину (не вистачає змінної y). Застосуванням закону склеювання отримуємо:

$$E(x, y) = (x \vee \overline{y}) \wedge \overline{x} = (x \vee \overline{y}) \wedge (\overline{x} \vee y) \wedge (\overline{x} \vee \overline{y}).$$

2. Зведемо до ДКНФ вираз $E(x, y, z) = (x \vee y) \wedge \overline{z}$. Неповну довжину мають перший і другий диз'юнкти: перший диз'юнкт не містить змінної z, у другому диз'юнкті не вистачає двох змінних – x та y. Спочатку зведемо до повної довжини перший диз'юнкт:

$$(x \vee y) = (x \vee y \vee z) \wedge (x \vee y \vee \overline{z}).$$

Тепер до диз'юнкта $\overline{z}$ додамо по черзі змінні x та y:

$$\overline{z} = (x \vee \overline{z}) \wedge (\overline{x} \vee \overline{z}) = (x \vee y \vee \overline{z}) \wedge (x \vee \overline{y} \vee \overline{z}) \wedge (\overline{x} \vee y \vee \overline{z}) \wedge (\overline{x} \vee \overline{y} \vee \overline{z}).$$

Виключаючи повторення диз'юнкта $(x \vee y \vee \overline{z})$, остаточно отримуємо:

$$E(x, y, z) = (x \vee y \vee z) \wedge (x \vee y \vee \overline{z}) \wedge (x \vee \overline{y} \vee \overline{z}) \wedge (\overline{x} \vee y \vee \overline{z}) \wedge (\overline{x} \vee \overline{y} \vee \overline{z}).$$

3. Зведемо до ДКНФ вираз $E(x, y) = 0$. Маємо один порожній диз'юнкт, до якого потрібно додати дві змінні:

$$E(x, y) = x \wedge \overline{x} = (x \vee y) \wedge (x \vee \overline{y}) \wedge (\overline{x} \vee y) \wedge (\overline{x} \vee \overline{y}).$$

3.5.4. Досконалі диз'юнктивні та кон'юнктивні нормальні форми і таблиці істинності

У п. 3.5.1 зазначалось, що будь-який вираз $E(x_1, \ldots, x_n)$ над булевою алгеброю $\langle A, \vee, \wedge, \bar{}, 0, 1\rangle$ можна розглядати як відображення $E\colon A^{\times n} \to A$. Розглянемо випадок, коли аргументи цього відображення набувають лише значення 0 або 1, тобто $x_k \in \{0, 1\}$, $k = 1, 2, \ldots, n$. Легко зрозуміти, що у цьому випадку відображення E також набуває значення 0 або 1, тобто $E(x_1, \ldots, x_n) \in \{0, 1\}$. Справді, якщо $\mathcal{A}, \mathcal{B} \in \{0, 1\}$, то $\mathcal{A} \vee \mathcal{B} \in \{0, 1\}$, $\mathcal{A} \wedge \mathcal{B} \in \{0, 1\}$, $\overline{\mathcal{A}} \in \{0, 1\}$, і, за означенням 3.4, $E(x_1, \ldots, x_n) \in \{0, 1\}$. Таким чином, вираз $E(x_1, \ldots, x_n)$ можна розглядати як «звужене» відображення $E : \{0, 1\}^{\times n} \to \{0, 1\}$. Фактично звужуватимемо наш розгляд до алгебри висловлень (хоча формально $E(x_1, \ldots, x_n)$ – вираз над довільною булевою алгеброю $\langle A, \vee, \wedge, \bar{}, 0, 1\rangle$).

Нехай $E(x_1, \ldots, x_n)$ – кон'юнкт повної довжини. Із 2^n можливих наборів $(x_1, x_2, \ldots, x_n) \in \{0, 1\}^{\times n}$ кон'юнкт $E(x_1, \ldots, x_n)$ набуває значення 1 лише на одному наборі, коли всі аргументи зовнішньої кон'юнкції дорівнюють 1.

Таблиця 3.1

x	y	$x \wedge \overline{y}$
0	0	0
0	1	0
1	0	1
1	1	0

Так, кон'юнкт $E(x, y) = x \wedge \overline{y}$ набуває значення 1 на наборі $(1, 0)$, тобто у випадку $x = 1, y = 0$. За аналогією до алгебри висловлень будемо говорити про таблицю істинності для $E(x, y) = x \wedge \overline{y}$ (табл. 3.1).

Кожному кон'юнкту $E(x_1, \ldots, x_n)$ повної довжини поставимо у відповідність набір $(a_1, \ldots, a_n) \in \{0, 1\}^{\times n}$, такий, що $E(a_1, a_2, \ldots, a_n) = 1$. Навпаки, для довільного набору $(a_1, a_2, \ldots, a_n) \in \{0, 1\}^{\times n}$ існує один і тільки один кон'юнкт $E(x_1, \ldots, x_n)$ повної довжини, який саме на цьому наборі набуває значення 1. Отже, отримуємо взаємно однозначну відповідність між множиною наборів $\{0, 1\}^{\times n}$ і множиною кон'юнктів $E(x_1, \ldots, x_n)$ повної довжини: кожному кон'юнкту відповідає набір із елементів 0 та 1, на якому цей кон'юнкт набуває значення 1. Так, кон'юнкту $E(x, y, z) = x \wedge \overline{y} \wedge z$ відповідає набір $(1, 0, 1)$, кон'юнкту $E(x_1, x_2, x_3, x_4) = \overline{x_1} \wedge \overline{x_2} \wedge x_3 \wedge \overline{x_4}$ відповідає набір $(0, 0, 1, 0)$.

Зауваження 3.7. Кон'юнкт $E(x_1, \ldots, x_n)$ довжини $n - 1$ набуває значення 1 на двох наборах із $\{0, 1\}^{\times n}$, оскільки змінна, що не міститься в $E(x_1, \ldots, x_n)$, може набувати довільного значення 0 або 1, а значення інших змінних фіксовані. Взагалі, кон'юнкт $E(x_1, \ldots, x_n)$ довжини $n - k$ $(0 \geqslant k \geqslant n - 1)$ набуває значення 1 на 2^k наборах із $\{0, 1\}^{\times n}$, оскільки існує 2^k наборів значень для k змінних, що не входять у $E(x_1, \ldots, x_n)$. Так, кон'юнкт $E(x, y, z) = \overline{x}$ довжини $1 = 3 - 2$ набуває значення 1 на $2^2 = 4$ наборах із $\{0, 1\}^{\times n}$: $(0, 0, 0)$, $(0, 0, 1)$, $(0, 1, 0)$, $(0, 1, 1)$.

Зазначимо, що тривіальному випадку $k = 0$ відповідає порожній кон'юнкт $E(x_1, \ldots, x_n) = 1$ довжиною $0 = n - n$, який набуває значення 1 на всіх 2^n наборах із $\{0, 1\}^{\times n}$.

Нехай тепер $E(x_1, \ldots, x_n)$ – деяка ДДНФ, що є диз'юнкцією m кон'юнктів $E_i(x_1, \ldots, x_n)$, $i = 1, 2, \ldots, m$. Очевидно, що $E(x_1, \ldots, x_n)$ набуває значення 1 на тих і тільки тих наборах із $\{0, 1\}^{\times n}$, коли набуває значення 1 один із кон'юнктів $E_i(x_1, \ldots, x_n)$, $i = 1, 2, \ldots, m$. Оскільки всі кон'юнкти у складі ДДНФ попарно різні і мають повну довжину, а отже набувають значення 1 на різних m наборах, отримуємо m наборів із $\{0,1\}^{\times n}$, на яких $E(x_1, \ldots, x_n)$ набуває значення 1. Так, ДДНФ $E(x, y, z) = (x \wedge \overline{y} \wedge z) \vee (\overline{x} \wedge \overline{y} \wedge \overline{z})$ набуває значення 1 на наборах $(1, 0, 1)$ та $(0, 0, 0)$. Отже, ДДНФ для виразу $E(x_1, \ldots, x_n)$ однозначно визначається його «одиничними» наборами, тобто множиною наборів із $\{0,1\}^{\times n}$, на яких цей вираз набуває значення 1.

Наведемо відповідні дуальні міркування стосовно ДКНФ. Кожному диз'юнкту повної довжини взаємно однозначно відповідає набір із елементів 0 та 1, на якому цей диз'юнкт набуває значення 0. Так, диз'юнкту $E(x, y, z) = x \vee \overline{y} \vee z$ відповідає набір $(0, 1, 0)$. Довільна ДКНФ $E(x_1, \ldots, x_n)$, що є кон'юнкцією m диз'юнктів, набуває значення 0 на тих і тільки тих m наборах із $\{0,1\}^{\times n}$, коли набуває значення 0 один із її диз'юнктів. Так, ДКНФ $E(x, y, z) = (x \vee \overline{y} \vee z) \wedge (\overline{x} \vee \overline{y} \vee \overline{z})$ набуває значення 0 на наборах $(0, 1, 0)$ та $(1, 1, 1)$. Отже, ДКНФ для виразу $E(x_1, \ldots, x_n)$ однозначно визначається його «нульовими» наборами, тобто множиною наборів із $\{0,1\}^{\times n}$, на яких цей вираз набуває значення 0.

Таким чином, доведено таке твердження:

Теорема 3.14. *Кожен вираз над булевою алгеброю можна зобразити у вигляді ДДНФ та ДКНФ єдино можливим способом, з точністю до переставлення кон'юнктів ДДНФ (диз'юнктів ДКНФ) та аргументів усередині кон'юнктів у складі ДДНФ (аргументів диз'юнктів у складі ДКНФ).*

Отже, для побудови ДДНФ і ДКНФ достатньо знати значення виразу $E(x_1, \ldots, x_n)$ на наборах із $\{0,1\}^{\times n}$, тобто його таблицю істинності. Звідси отримуємо такий важливий факт.

Наслідок. *Відображення $E : A^{\times n} \to A$, що задається виразом $E(x_1, \ldots, x_n)$ над булевою алгеброю $\langle A, \vee, \wedge, \bar{}, 0, 1 \rangle$, однозначно визна-*

чається значеннями $E(x_1, \ldots, x_n)$ *на* $\{0,1\}^{\times n}$.

Інакше кажучи, якщо відображення $E_1 : A^{\times n} \to A$ та $E_2 : A^{\times n} \to A$, задані відповідно виразами $E_1(x_1, \ldots, x_n)$ та $E_2(x_1, \ldots, x_n)$ над булевою алгеброю $\langle A, \vee, \wedge, ^{-}, 0, 1 \rangle$, збігаються на $\{0,1\}^{\times n}$, то вони збігаються на всій області визначеності $A^{\times n}$.

Таблицю істинності для виразу $E : A^{\times n} \to A$ часто задають у вигляді вектора значень – набору із $\{0,1\}^{\times 2^n}$, який являє собою правий стовпець таблиці істинності. У цьому випадку вважають, що рядки таблиці істинності впорядковані за зростанням наборів із $\{0,1\}^{\times n}$ як чисел у двійковій системі: $(0, \ldots, 0, 0)$, $(0, \ldots, 0, 1)$, $(0, \ldots, 1, 0)$, $(0, \ldots, 1, 1)$, $\ldots$, $(1, \ldots, 1, 0)$, $(1, \ldots, 1, 1)$.

Приклад 3.21. Нехай таблиця істинності виразу $E(x, y, z)$ задана вектором значень (11100101).

Випишемо цю таблицю істинності в явному вигляді, вказавши для кожного «одиничного» набору $E(x, y, z)$ (коли вираз набуває значення 1) відповідний кон'юнкт, а для кожного «нульового» набору (коли вираз набуває значення 0) – відповідний диз'юнкт (табл. 3.2).

Таблиця 3.2

x	y	z	$E(x,y,z)$	диз'юнкт/кон'юнкт
0	0	0	1	$\overline{x} \wedge \overline{y} \wedge \overline{z}$
0	0	1	1	$\overline{x} \wedge \overline{y} \wedge z$
0	1	0	1	$\overline{x} \wedge y \wedge \overline{z}$
0	1	1	0	$x \vee \overline{y} \vee \overline{z}$
1	0	0	0	$\overline{x} \vee y \vee z$
1	0	1	1	$x \wedge \overline{y} \wedge z$
1	1	0	0	$\overline{x} \vee \overline{y} \vee z$
1	1	1	1	$x \wedge y \wedge z$

Тепер можна виписати ДДНФ як диз'юнкцію вказаних кон'юнктів та ДКНФ як кон'юнкцію вказаних диз'юнктів:

ДДНФ: $(\overline{x} \wedge \overline{y} \wedge \overline{z}) \vee (\overline{x} \wedge \overline{y} \wedge z) \vee (\overline{x} \wedge y \wedge \overline{z}) \vee (x \wedge \overline{y} \wedge z) \vee (x \wedge y \wedge z)$;

ДКНФ: $(x \vee \overline{y} \vee \overline{z}) \wedge (\overline{x} \vee y \vee z) \wedge (\overline{x} \vee \overline{y} \vee z)$.

Наголосимо, що у вигляді ДДНФ і ДКНФ можна зобразити лише такі відображення $f : A \to A$, які задані деяким виразом над булевою алгеброю A. Однак у випадку, якщо A містить більше двох елементів (тобто містить хоча б один елемент окрім 0 та 1), не кожне відображення на A можна задати виразом над A.

Приклад 3.22. Розглянемо випадок булевої алгебри з чотирма елементами (рис. 3.3).

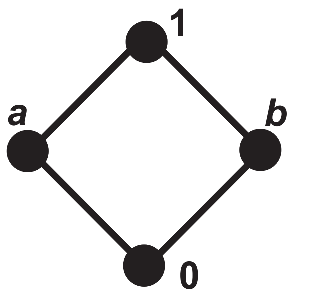


Рис. 3.3

Очевидно, існують лише чотири ДДНФ з однією змінною x: 0, x, $\overline{x}$, $x \vee \overline{x} = 1$, і жоден із цих виразів не задає такого відображення $f : A \to A$, щоб $f(0) = 0$, $f(1) = 1$, $f(a) = b$, $f(b) = a$. Так, $\overline{a} = b$ та $\overline{b} = a$, однак $\overline{0} = 1$ та $\overline{1} = 0$.

3.6. Мінімізація диз'юнктивних нормальних форм

3.6.1. Основні поняття

Встановлено (див. наслідок до теореми 3.14), що відображення на булевій алгебрі A, задане виразом над A, однозначно фіксується значеннями цього виразу на наборах з елементів 0 та 1. Таким чином, для аналізу ДНФ як способу задання відображень достатньо обмежитись випадком двохелементної булевої алгебри $A = \{0, 1\}$. Отже, тут вважатимемо булеву алгебру A двохелементною.

Як уже зазначалось, зображення виразу над булевою алгеброю у вигляді ДНФ ніколи не є єдиним, тобто для кожного виразу завжди можна навести декілька еквівалентних ДНФ. Для практичного використання найчастіше більш придатна така ДНФ, яка є у певному сенсі «простішою»: ДНФ $x \vee y$ можна вважати «простішою» порівняно з $x \vee (\overline{x} \wedge y)$. Дамо точні визначення.

Означення 3.11. Кон'юнкт $E_1(x_1, \ldots, x_n)$ називають імплікантою функції, яка задана виразом $E(x_1, \ldots, x_n)$, якщо $E(x_1, \ldots, x_n)$ набуває значення 1 на всіх наборах із $\{0, 1\}^{\times n}$, коли набуває значення 1 вираз $E_1(x_1, \ldots, x_n)$.

Зауваження 3.8. Кон'юнкт E_1 є імплікантою виразу E тоді і тільки тоді, коли імплікація $E_1 \to E$ набуває значення 1 на всіх наборах із елементів 0 та 1.

Якщо вираз E є ДНФ, то, очевидно, кожен кон'юнкт у складі E є імплікантою цього виразу. Так, для виразу $x \vee (\overline{x} \wedge y)$ кон'юнкти x і $\overline{x} \wedge y$ є імплікантами.

Ще один простий факт сформулюємо у вигляді вправи.

Вправа 3.4. Для будь-якої імпліканти E_1 виразу E можна вказати таку ДНФ виразу E, яка містить кон'юнкт E_1.

Вказівка. Кон'юнкт E_1 є імплікантою також і для виразу $E \vee E_1$.

Зауваження 3.9. З урахуванням результату вправи 3.4 отримуємо: кон'юнкт E_1 є імплікантою виразу E тоді і тільки тоді, коли E_1 входить до складу деякої ДНФ виразу E.

Означення 3.12. Імпліканту E_1 виразу E називають простою, якщо видалення будь-якої змінної з кон'юнкта E_1 приводить до кон'юнкта, який не є імплікантою виразу E.

Природно вважати, що видалення змінної із кон'юнкта одиничної довжини приводить до порожнього кон'юнкта, тобто до виразу 1. Отже, імпліканта одиничної довжини (тобто змінна або доповнення до змінної) є простою завжди, окрім випадку, коли розглядаються імпліканти виразу, еквівалентного 1.

Приклад 3.23. Вираз $E(x, y) = x \vee (\overline{x} \wedge y)$ допускає імпліканти x, y і $\overline{x} \wedge y$. Очевидно, імпліканти x, y прості, імпліканта $\overline{x} \wedge y$ непроста – можна видалити змінну x, отримавши імпліканту y.

Означення 3.13. Диз'юнктивну нормальну форму E називають тупиковою, якщо виконуються дві умови:

1) кожна імпліканта у складі E проста;

2) жодну імпліканту у складі E не можна викреслити, зберігши еквівалентність виразу E.

Приклад 3.24. 1. Вирази 0, 1, x, $\overline{x}$, $x \vee \overline{y}$, $(x \wedge y) \vee (\overline{x} \wedge \overline{y})$, $x \vee (\overline{y} \wedge z)$ – тупикові ДНФ.

2. Диз'юнктивна нормальна форма $x \vee (\overline{x} \wedge \overline{y})$ не тупикова, оскільки друга імпліканта не проста: $x \vee (\overline{x} \wedge \overline{y}) = x \vee \overline{y}$.

3. Диз'юнктивна нормальна форма $(x \wedge y) \vee (\overline{x} \wedge z) \vee (y \wedge z)$ містить лише прості імпліканти, однак імпліканту $y \wedge z$ можна викреслити: $(x \wedge y) \vee (\overline{x} \wedge z) \vee (y \wedge z) = (x \wedge y) \vee (\overline{x} \wedge z)$. Отже, вихідна ДНФ не тупикова.

Легко зрозуміти, що кожен вираз над булевою алгеброю допускає принаймні одну тупикову форму, однак вирази з трьома та більше змінними можуть мати більше однієї тупикової ДНФ (відповідні приклади будуть наведені у п. 3.6.2). Вибір конкретної тупикової ДНФ визначається *критерієм мінімальності*, який обирають з огляду на конкретну практичну задачу. Мінімізація ДНФ передбачає пошук тупикових ДНФ, і, якщо їх декілька – вибір оптимальної за обраним критерієм. Існують різноманітні критерії мінімальності [7], наведемо два найпоширеніших:

- загальна довжина ДНФ (тобто сума довжин кон'юнктів);
- кількість кон'юнктів у складі ДНФ.

Методи пошуку тупикових ДНФ поділяють на алгебричні, з використанням аналітичних перетворень, і геометричні, з наочним зображенням одиничних наборів ДНФ на площині. Зазначимо, що алгебричні методи мінімізації комп'ютерно-орієнтовані, натомість геометричні методи орієнтовані здебільшого на візуальний аналіз, тобто на людину.

Розглядувані методи мінімізації ДНФ можна дуальними міркуваннями перенести на КНФ [8].

3.6.2. Геометричні методи мінімізації ДНФ. Карти Карно

Один із найпоширеніших геометричних методів пошуку тупикових форм запропонував у 1953 р. американський інженер Моріс Карно. Цей метод пов'язаний із зображенням одиничних наборів виразу на спеціальних картах, які у наш час називають *картами Карно*[1].

У класичному вигляді метод карт Карно застосовують для виразів, у яких не більш ніж чотири змінні, тобто для виразів $E(x_1, \ldots, x_n)$ з $n = 2, 3, 4$ (відкидаючи тривіальні випадки $n = 0$ та $n = 1$).

Для побудови карти Карно для виразу $E(x_1, x_2, \ldots, x_n)$ множину змінних $\{x_1, \ldots, x_n\}$ розбивають на дві підмножини $\{x_1, \ldots, x_m\}$ та $\{x_{m+1}, \ldots, x_n\}$, кожна з яких має містити одну або дві змінні. Карти Карно для виразу $E(x_1, x_2, \ldots, x_n)$ можна розглядати як таблицю істинності спеціального вигляду: кожному набору із $\{0,1\}^{\times n}$ взаємно однозначно відповідає одна комірка таблиці (двовимірної карти). Стовпці цієї таблиці нумерують наборами із $\{0,1\}^{\times m}$, які відповідають змінним $\{x_1, \ldots, x_m\}$, рядки таблиці нумерують наборами із $\{0,1\}^{\times(n-m)}$, які відповідають змінним $\{x_{m+1}, \ldots, x_n\}$.

Так, якщо $n = 2$ (мінімізація виразу $E(x, y)$), стовпці нумерують значеннями змінної x, рядки – значеннями змінної y, отримуючи два стовпці і два рядки. Якщо $n = 3$ (вираз $E(x, y, z)$), рядки можна нумерувати значеннями змінної z, стовпці – значеннями пари змінних (x, y), отримуючи два рядки і чотири стовпці; можна також виділити пару змінних (x, y) для нумерації рядків, а змінну z – для нумерації стовпців, отримуючи чотири рядки і два стовпці. Якщо $n = 4$ (вираз $E(x, y, z, t)$), стовпці можна нумерувати значеннями пари змінних (x, y), рядки – значеннями (z, t), отримуючи чотири рядки і чотири стовпці.

[1] Варіант методу карт Карно відомий також як діаграми Вейча.

Введемо технічне визначення: набори $\alpha, \beta \in \{0,1\}^{\times k}$ назвемо *сусідніми*, якщо вони відрізняються значеннями лише за однією координатою. Так, для $n = 2$ набори $(0,0)$ і $(0,1)$ сусідні, набори $(0,1)$ і $(1,0)$ не сусідні. Очевидно, кожен набір $\alpha \in \{0,1\}^{\times k}$ має точно k сусідніх наборів, які можна отримати, змінюючи значення однієї з k координат набору α. Так, для набору $(1,0)$ сусідніми є два набори $(0,0)$ і $(1,1)$.

Для роботи з картою Карно потрібно, щоб сусіднім рядкам відповідали сусідні набори із $\{0,1\}^{\times m}$, сусіднім стовпцям – сусідні набори із $\{0,1\}^{\times (n-m)}$; крайні (верхній і нижній) рядки та крайні (правий і лівий) стовпці вважають сусідніми. Для зручності проставлятимемо на карті не самі набори, а відповідні кон'юнкти. Так, у випадку змінних (z,t) замість набору $(1,0)$ вказуватимемо кон'юнкт $z \wedge \bar{t}$.

Загальний вигляд карт Карно для випадку двох, трьох і чотирьох змінних подано на рис. 3.4 (біля кон'юнктів проставлено відповідні значення змінних, у подальших прикладах наводитимемо лише кон'юнкти).

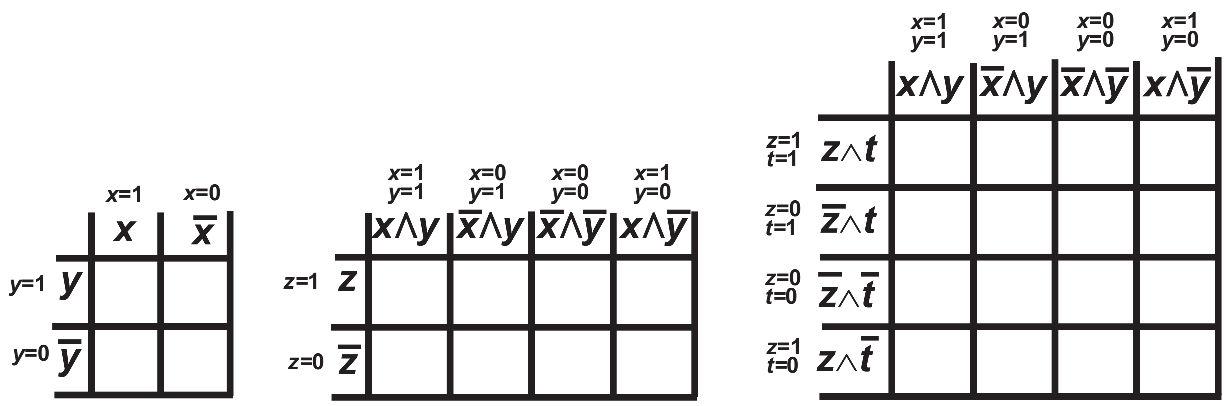


Рис. 3.4. Загальний вигляд карт Карно для $n = 2, 3, 4$

Кожна комірка таблиці взаємно однозначно відповідає одному набору аргументів і заповнюється значенням заданого виразу на цьому наборі. Зазвичай у комірках проставляють лише значення 1; комірки, які відповідають нульовим наборам, залишають порожніми.

Приклад 3.25. Наведемо карти Карно для виразів $E(x,y) = \overline{x} \vee y$; $E(x,y,z) = \overline{x} \vee (y \wedge z)$; $E(x,y,z,t) = x \vee (\overline{x} \wedge \overline{y} \wedge \overline{z} \wedge \overline{t})$ (рис. 3.5).

	x	$\overline{x}$
y	1	1
$\overline{y}$		1

$\overline{x} \vee y$

	$x \wedge y$	$\overline{x} \wedge y$	$\overline{x} \wedge \overline{y}$	$x \wedge \overline{y}$
z	1	1	1	
$\overline{z}$		1	1	

$\overline{x} \vee (y \wedge z)$

	$x \wedge y$	$\overline{x} \wedge y$	$\overline{x} \wedge \overline{y}$	$x \wedge \overline{y}$
$z \wedge t$	1			1
$\overline{z} \wedge t$	1			1
$\overline{z} \wedge \overline{t}$	1		1	1
$z \wedge \overline{t}$	1			1

$x \vee (\overline{x} \wedge \overline{y} \wedge \overline{z} \wedge \overline{t})$

Рис. 3.5. Приклади карт Карно

З'ясуємо, як розташовані на карті Карно одиничні набори окремих кон'юнктів. Кон'юнкту повної довжини n відповідає один одиничний набір і одна комірка на карті. Нехай тепер кон'юнкт K має довжину $n-1$, тобто не містить однієї змінної x. Тоді, за законом склеювання, $K = (K \wedge x) \vee (K \wedge \overline{x})$, тобто K є склеюванням двох кон'юнктів повної довжини $K \wedge x$ та $K \wedge \overline{x}$ за змінною x, і два одиничні набори цих кон'юнктів є одиничними наборами K. Таким чином, одиничні набори кон'юнкта K сусідні, оскільки відрізняються лише за однією координатою, яка відповідає змінній x. Отже, одиничні набори кон'юнкта K відповідають сусіднім коміркам, тобто утворюють прямокутник із двох комірок (нагадаємо, що крайні рядки і крайні стовпці вважають сусідніми).

Приклад 3.26. Кон'юнкт $K_1(x,y) = \overline{x}$ є склеюванням за змінною y кон'юнктів повної довжини $\overline{x} \wedge y$ та $\overline{x} \wedge \overline{y}$. На карті Карно одиничні набори кон'юнкта $\overline{x}$ утворюють прямокутник із двох комірок, які відповідають кон'юнктам $\overline{x} \wedge y$ та $\overline{x} \wedge \overline{y}$ (рис. 3.6). Кон'юнкт $K_2(x,y,z) = x \wedge \overline{z}$ є склеюванням за y двох кон'юнктів повної довжини $x \wedge y \wedge \overline{z}$ та $x \wedge \overline{y} \wedge \overline{z}$. Одиничні набори кон'юнкта $\overline{x}$ утворюють на карті прямокутник із двох комірок, які відповідають кон'юнктам $x \wedge y \wedge \overline{z}$ та $x \wedge \overline{y} \wedge \overline{z}$ (рис. 3.7).

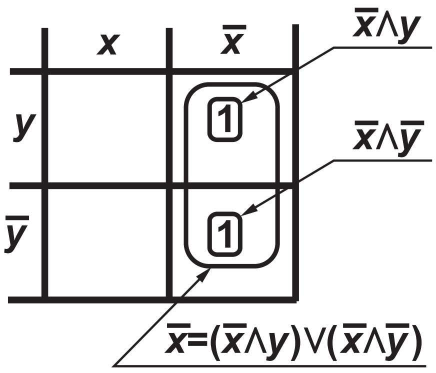


Рис. 3.6. Карта Карно для кон'юнкта $K_1(x, y) = \overline{x}$

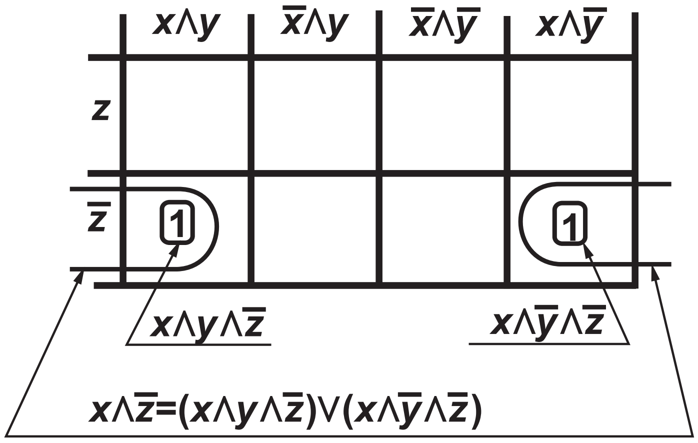


Рис. 3.7. Карта Карно для кон'юнкта $K_2(x, y, z) = x \wedge \overline{z}$

Індукцією за $k \geqslant 0$ легко довести, що одиничні набори будь-якого кон'юнкта з $n - k$ змінними утворюють на карті Карно прямокутник із 2^k комірок: доведення зводиться до поетапного склеювання кон'юнктів більшої довжини, що на карті Карно відповідає склеюванню сусідніх прямокутників.

Приклад 3.27. Прямокутники, утворені одиничними наборами кон'юнктів $K_1(x, y, z, t) = \overline{t}$ та $K_2(x, y, z, t) = x \wedge z$, зображено на рис. 3.8.

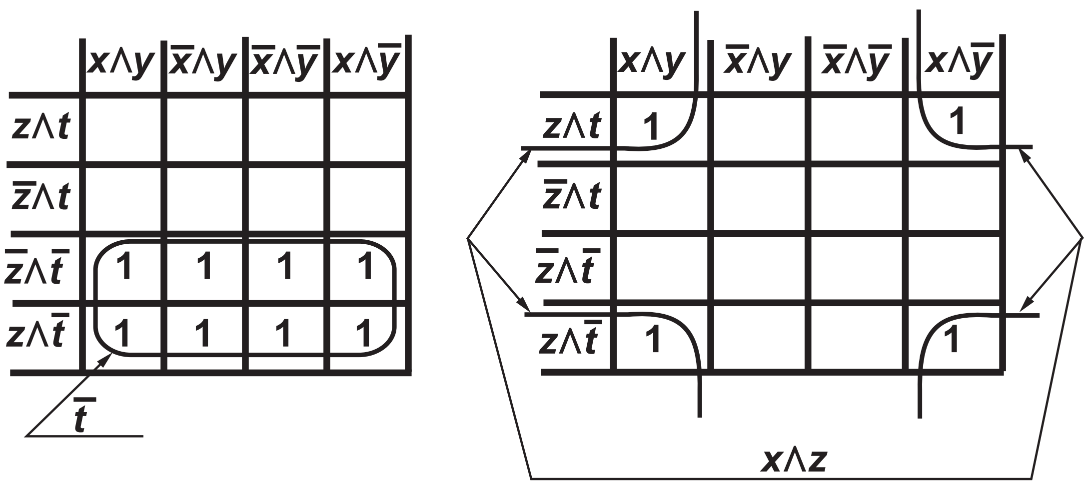


Рис. 3.8. Карти Карно для $K_1(x, y, z, t) = \overline{t}$ та $K_2(x, y, z, t) = x \wedge z$

Чотири одиничні набори кон'юнкта z розташовані у комірках на першому й останньому рядках та у першому й останньому стовпцях, тобто утворюють зв'язний прямокутник.

Надалі говоритимемо, що комірка карти Карно відповідає змінній x_j без доповнення (відповідно з доповненням), якщо у відповідному наборі аргументів $x_j = 1$ (відповідно $x_j = 0$). Іншими словами, комірка відповідає x_j у тій самій формі (без доповнення або з доповненням), у якій ця змінна входить у кон'юнкт, що нумерує рядок або стовпець цієї комірки.

Для пошуку на карті Карно прямокутника одиничних наборів заданого кон'юнкта K можна використовувати такий метод. Якщо деяка змінна x входить у кон'юнкт K без доповнення, комірки одиничних наборів кон'юнкта K відповідатимуть змінній x без доповнення. Якщо змінна x входить у K з доповненням, комірки одиничних наборів кон'юнкта K відповідатимуть змінній x з доповненням. Якщо змінна x взагалі не входить у кон'юнкт K, одиничні набори кон'юнкта K будуть розміщені в комірках, які відповідають змінній x як з доповненням, так і без доповнення – у цьому випадку кон'юнкт K є склеюванням кон'юнктів більшої довжини за змінною x.

Приклад 3.28. Знову розглянемо кон'юнкти $K_1(x, y, z, t) = \bar{t}$ та $K_2(x, y, z, t) = x \wedge z$ із прикладу 3.27. Для кон'юнкта $K_1(x, y, z, t) = \bar{t}$ одиничні набори на карті Карно міститимуться у тих і тільки тих комірках, які відповідають змінній t з доповненням, тобто у третьому та четвертому рядках; за змінними x, y, z, які не входять в кон'юнкт, відбувається склеювання, і кон'юнкт має $2^3 = 8$ одиничних наборів. Одиничні набори кон'юнкта $K_2(x, y, z, t) = x \wedge z$ міститимуться у чотирьох кутових комірках, які відповідають змінним x та z без доповнення (це прямокутник, оскільки крайні рядки і крайні стовпці є сусідніми); за змінними y, z, які не входять у кон'юнкт, відбувається склеювання, і кон'юнкт має $2^2 = 4$ одиничні набори.

Вправа 3.5. Для ДНФ, розглянутих у прикладі 3.25, вкажіть на картах Карно прямокутники одиничних наборів для кожного кон'юнкта.

Отже, одиничні набори довільного кон'юнкта з $n-k$ змінними на карті Карно утворюють прямокутник із 2^k комірок. Легко зрозуміти, що існує також і зворотна відповідність: кожен прямокутник на карті Карно із 2^k комірок відповідає одиничним наборам деякого кон'юнкта з $n-k$ змінними. Цей кон'юнкт легко встановити, визначивши змінні, які входять до нього: якщо змінна x відповідає всім коміркам заданого прямокутника однаково без доповнення, то x входитиме в шуканий кон'юнкт без доповнення; якщо змінна x відповідає всім коміркам заданого прямокутника з доповненням, то x входитиме в шуканий кон'юнкт з доповненням; якщо змінна x відповідає деяким коміркам прямокутника без доповнення, а деяким коміркам прямокутника відповідає з доповненням, змінна x не увійде в шуканий кон'юнкт (за x відбувається склеювання). Зокрема, якщо $k=0$, маємо кон'юнкт повної довжини $n-0=n$, якому на карті Карно відповідає прямокутник із $2^0=1$ комірки, тобто одна комірка. Якщо $k=n$, маємо кон'юнкт довжини $n-n=0$, якому на карті відповідає прямокутник із 2^n комірок, тобто займає всі комірки.

Вправа 3.6. Застосуйте описаний метод до карт Карно, зображених на рис. 3.6, 3.7 і 3.8.

Отже, існує взаємно однозначна відповідність між кон'юнктами довжиною $n-k$ і прямокутниками на карті Карно із 2^k комірок: одиничні набори кон'юнкта утворюють на карті відповідний прямокутник.

Із означення простої імпліканти випливає, що імпліканта K заданого виразу E є простою тоді і тільки тоді, коли на карті Карно для виразу E прямокутник одиничних наборів кон'юнкта K не входить до жодного іншого прямокутника із 2^k комірок, заповнених одиницями.

Приклад 3.29. Два прямокутники, які відповідають простим імплікантам виразу $E(x,y,z,t)=x\vee(\overline{x}\wedge\overline{y}\wedge\overline{z}\wedge\overline{t})$, зображено на рис. 3.9.

Легко переконатись, що прямокутники, які відповідають іншим імплікантам виразу E, містяться в одному з прямокутників, який відповідає простій імпліканті x або $\overline{y} \wedge \overline{z} \wedge \overline{t}$. Так, прямокутник імпліканти $x \wedge y$ міститься у прямокутнику простої імпліканти x.

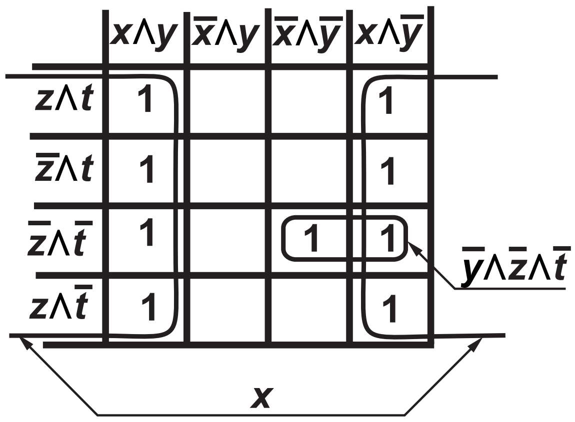


Рис. 3.9. Прості імпліканти виразу $E(x, y, z, t) = x \vee (\overline{x} \wedge \overline{y} \wedge \overline{z} \wedge \overline{t})$

Якщо вираз заданий у вигляді ДНФ, тобто є диз'юнкцією кон'юнктів, множина одиничних наборів є об'єднанням прямокутників, кожен з яких відповідає одному кон'юнкту. Пошук тупикових ДНФ очевидно зводиться до покриття одиничних наборів заданого виразу системою прямокутників із виконанням таких умов:

- кожен прямокутник має містити 2^k комірок ($k \in \mathbb{N} \cup \{0\}$);
- жоден прямокутник не можна збільшити у межах одиничних наборів так, щоб він містив 2^k комірок ($k \in \mathbb{N} \cup \{0\}$);
- жоден прямокутник не може цілком дублюватися іншими прямокутниками (проте окремі одиниці прямокутника можуть входити в інші прямокутники).

Прямокутники, які задовольняють зазначені умови, називатимемо допустимими.

Приклад 3.30. Вираз $E(x, y) = \overline{x} \vee (x \wedge y)$ допускає одну тупикову форму $\overline{x} \vee y$ із двох простих імплікант $\overline{x}$ та y, відповідну карту Карно зображено на рис. 3.10. Вираз $E(x, y, z) = \overline{x} \vee (x \wedge y \wedge z)$ допускає одну тупикову форму $\overline{x} \vee (y \wedge z)$ із простих імплікант $\overline{x}$ та $y \wedge z$ (рис. 3.11).

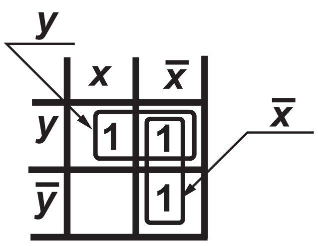


Рис. 3.10. Тупикова форма для $E(x, y) = \overline{x} \vee (x \wedge y)$

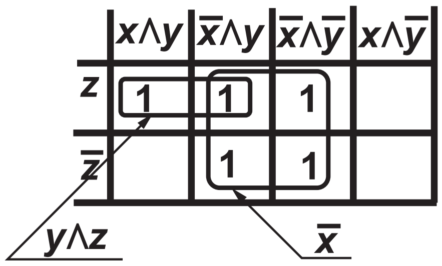


Рис. 3.11. Тупикова форма для $E(x, y, z) = \overline{x} \vee (x \wedge y \wedge z)$

Шукаючи покриття для тупикової форми, не слід автоматично використовувати найбільші прямокутники (які відповідають найкоротшим імплікантам). Приклад 3.31 демонструє, що такі прямокутники, як і будь-які інші, можуть повністю дублюватися іншими прямокутниками і не потрапити до шуканого покриття.

Приклад 3.31. Карту Карно для виразу з вектором значень (1101111010000100) зображено на рис. 3.12.

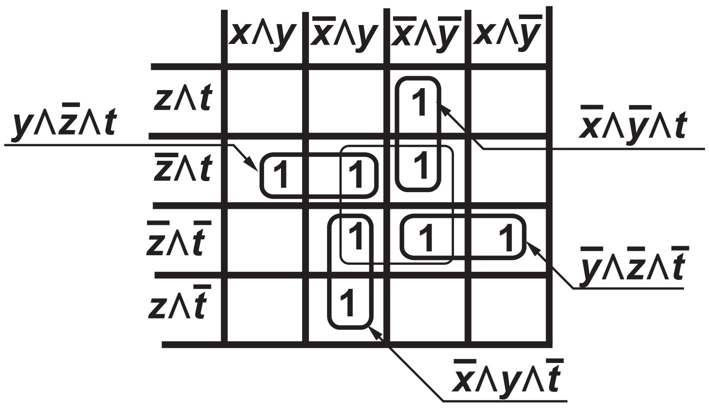


Рис. 3.12. Мінімізація ДНФ з вектором значень (1101111010000100)

Відповідна тупикова форма $(\overline{x} \wedge \overline{y} \wedge t) \vee (\overline{y} \wedge \overline{z} \wedge \overline{t}) \vee (y \wedge \overline{z} \wedge t) \vee (\overline{x} \wedge y \wedge \overline{t})$ не містить найкоротшої імпліканти $\overline{x} \wedge \overline{z}$, тобто покриття на карті Карно не включає відповідного найбільшого прямокутника із чотирьох комірок (на рисунку обведений тонкою лінією).

Вирази з трьома та більше змінними можуть допускати декілька тупикових форм. У цьому випадку побудову покриття слід починати з таких комірок, які можна накрити лише одним допустимим прямокутником. Відповідні прямокутники відповідатимуть простим імплікантам, які увійдуть в усі тупикові форми; такі імпліканти називають *ядровими*, сукупність ядрових імплікант називають *диз'юнктивним ядром* (або просто ядром) заданого виразу. Якщо ядро накриває всі одиничні набори заданого виразу, цей вираз допускає лише одну тупикову форму. Якщо ж залишились одиничні набори, які не потрапили до жодної ядрової імпліканти, то відповідні комірки можна накрити різними допустимими прямокутниками і вираз допускає декілька тупикових форм.

Приклад 3.32. Диз'юнктивна нормальна форма з вектором значень (10111001) допускає дві тупикові форми: $(y \wedge z) \vee (\overline{y} \wedge \overline{z}) \vee (\overline{x} \wedge \overline{z})$ та $(y \wedge z) \vee (\overline{y} \wedge \overline{z}) \vee (\overline{x} \wedge y)$, відповідні карти Карно подано на рис. 3.13. Імпліканти $y \wedge z$ та $\overline{y} \wedge \overline{z}$ ядрові, оскільки містять комірки, що не дублюються жодним іншим допустимим прямокутником. Єдину комірку, не покриту ядром (відповідає набору $\overline{x} \wedge y \wedge \overline{z}$), можна накрити двома допустимими прямокутниками, які відповідають простим імплікантам $\overline{x} \wedge \overline{z}$ та $\overline{x} \wedge y$.

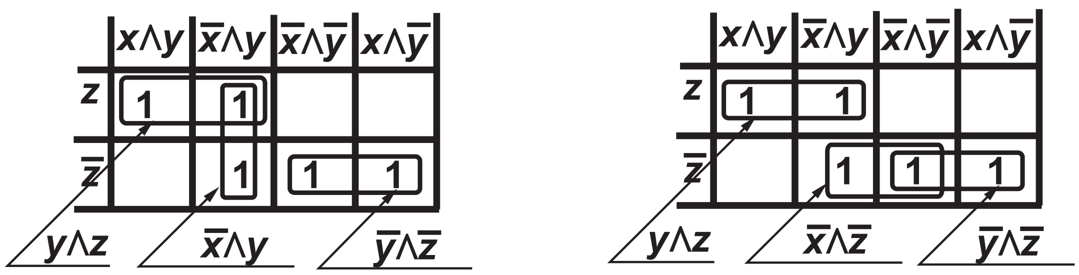


Рис. 3.13. Дві тупикові форми для ДНФ з вектором значень (10111001)

Вираз може взагалі не містити ядрових імплікант (мати порожнє ядро) – такою, наприклад, є ДНФ, задана вектором значень (01111110).

Зі збільшенням n максимальна кількість тупикових форм для виразу $E(x_1, \ldots, x_n)$ швидко зростає. Для $n \geqslant 2$ вираз завжди має одну тупикову форму, вираз із трьома змінними може допускати до 5 тупикових форм, для виразів із чотирма змінними максимальна кількість тупикових форм досягає 58. У роботі [9] наведено оцінки для кількості тупикових форм для великих n.

Детальніше про карти Карно можна прочитати, наприклад, у роботах [8; 9].

3.6.3. Алгебричні методи мінімізації ДНФ

Розглядуваними алгебричними методами мінімізації можна отримати ДНФ, яка є диз'юнкцією всіх простих імплікант заданого виразу.

Вправа 3.7. Довести, що диз'юнкція всіх простих імплікант виразу E утворює ДНФ цього виразу.

Вказівка. Достатньо довести, що кожен одиничний набір виразу E є одиничним набором деякої простої імпліканти.

Диз'юнктивну нормальну форму, яка складається з усіх простих імплікант, називають *скороченою*. Скорочена ДНФ у загальному випадку не є тупиковою, але будь-яку тупикову ДНФ можна отримати із скороченої ДНФ відкиданням деяких імплікант.

Приклад 3.33. Для виразу з не більш ніж двома змінними скорочена форма завжди тупикова. Справді, випадки $n = 0$ та $n = 1$ тривіальні, випадок $n = 2$, як легко перевірити на картах Карно, допускає не більше двох простих імплікант, що унеможливлює дублювання однієї простої імпліканти іншими. Так, для виразу з вектором значень (1101) маємо дві прості імпліканти і скорочену ДНФ $\overline{x} \vee y$, яка є тупиковою.

Приклад 3.34. Вираз з вектором значень (1101111010000100) із прикладу 3.31 допускає п'ять простих імплікант; його скорочена ДНФ $(\overline{x} \wedge \overline{y} \wedge t) \vee (\overline{y} \wedge \overline{z} \wedge \overline{t}) \vee (y \wedge \overline{z} \wedge t) \vee (\overline{x} \wedge y \wedge \overline{t}) \vee (\overline{x} \wedge \overline{z})$ не є тупиковою, оскільки останню імпліканту можна відкинути (її одиничні набори дублюються одиничними наборами інших імплікант).

Побудова скороченої ДНФ із КНФ. Нехай вираз E заданий у вигляді довільної КНФ (не обов'язково досконалої). Метод полягає у застосуванні закону дистрибутивності $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ доти, доки це можливо; отримані кон'юнкції спрощуємо, використовуючи закони $a \wedge a = a$, $x \wedge \overline{x} = 0$, $0 \wedge a = 0$, $0 \vee a = a$; використовуємо закон поглинання $a \vee (a \wedge b) = a$ доти, поки це можливо. Нескладно довести [9], що у результаті маємо отримати скорочену ДНФ.

Приклад 3.35. Застосуємо описаний метод до КНФ $(x \vee \overline{y}) \wedge (y \vee z)$. За законом дистрибутивності отримуємо:

$$(x \vee \overline{y}) \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \vee (\overline{y} \wedge y) \vee (\overline{y} \wedge z).$$

Відкидаючи передостанній кон'юнкт, який дорівнює 0, отримуємо:

$$(x \vee \overline{y}) \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \vee (\overline{y} \wedge z).$$

Закон поглинання застосувати неможливо; отже, отримана ДНФ скорочена. Легко переконатись, що ця форма не тупикова – кон'юнкт $(x \wedge z)$ можна викреслити, оскільки його одиничні набори дублюються одиничними наборами двох інших кон'юнктів.

Приклад 3.36. Застосуємо описаний метод до КНФ $(x \vee \overline{y}) \wedge (x \vee z)$. За законом дистрибутивності отримуємо:

$$(x \vee \overline{y}) \wedge (x \vee z) = (x \wedge x) \vee (x \wedge z) \vee (\overline{y} \wedge x) \vee (\overline{y} \wedge z).$$

Спрощуючи перший за законом ідемпотентності і відкидаючи другий і третій кон'юнкти за законом поглинання, отримуємо скорочену форму:

$$(x \vee \overline{y}) \wedge (x \vee z) = x \vee (\overline{y} \wedge z).$$

Легко переконатися, що отримана ДНФ є тупиковою, оскільки жодну із двох простих імплікант не можна викреслити.

Приклад 3.37. Побудуємо скорочену ДНФ для виразу з вектором значень (01111110). Вираз має лише два нульових набори, і можемо легко виписати відповідну КНФ: $(x \vee y \vee z) \wedge (\overline{x} \vee \overline{y} \vee \overline{z})$. Застосовуючи закон дистрибутивності та спрощуючи отримані кон'юнкції, отримуємо:

$$\begin{gathered}(x \vee y \vee z) \wedge (\overline{x} \vee \overline{y} \vee \overline{z}) = \\ = (x \wedge \overline{x}) \vee (x \wedge \overline{y}) \vee (x \wedge \overline{z}) \vee (y \wedge \overline{x}) \vee (y \wedge \overline{y}) \vee (y \wedge \overline{z}) \vee \\ \vee (z \wedge \overline{x}) \vee (z \wedge \overline{y}) \vee (z \wedge \overline{z}) = \\ = (x \wedge \overline{y}) \vee (x \wedge \overline{z}) \vee (y \wedge \overline{x}) \vee (y \wedge \overline{z}) \vee (z \wedge \overline{x}) \vee (z \wedge \overline{y}).\end{gathered}$$

Закон поглинання до отриманих кон'юнктів застосувати неможливо. Отже, отримана ДНФ є скороченою, тобто містить всі прості імпліканти заданого виразу. Легко переконатись (наприклад, за допомогою карт Карно), що ця форма не є тупиковою.

Метод Квайна.[1] Цей метод передбачає, що вираз заданий у вигляді ДДНФ. Суть методу полягає у застосуванні двох тотожностей:

1) $(A \wedge x) \vee (A \wedge \overline{x}) = (A \wedge x) \vee (A \wedge \overline{x}) \vee A$ (неповне склеювання);

2) $(A \wedge B) \vee A = A$ (поглинання).

Тотожності застосовують зліва направо; спочатку застосовують неповне склеювання доти, поки це можливо, а потім, поки можливо – поглинання.

Вправа 3.8. Довести, що результатом роботи алгоритму Квайна є скорочена ДНФ.

Вказівка. Будь-яку імпліканту заданого виразу можна отримати з кон'юнктів повної довжини, застосувавши скінченну кількість разів неповне склеювання.

[1] Віллард Ван Орман Квайн (1908–2000) – американський логік і філософ, опублікував низку робіт з математичної логіки.

Зазначимо, що на першому етапі роботи алгоритму вираз ускладнюється, оскільки з'являються нові кон'юнкти меншої довжини; однак на другому етапі ці короткі кон'юнкти дають змогу позбутися кон'юнктів більшої довжини. Очевидно, що кон'юнкт K, отриманий на першому етапі неповним склеюванням кон'юнктів K_1 і K_2, на другому етапі їх поглине. Неважко зрозуміти, що справджується і зворотний наслідок: на другому етапі поглинаються ті й тільки ті кон'юнкти, які використовувалися на першому етапі для неповного склеювання. Тому на першому етапі слід указувати, які саме кон'юнкти використовуються для неповного склеювання, навіть якщо один кон'юнкт можна отримати кількома варіантами.

Приклад 3.38. Застосуємо метод Квайна для отримання скороченої ДНФ виразу $E(x,y) = (x \wedge y) \vee (x \wedge \overline{y}) \vee (\overline{x} \wedge \overline{y})$; наголосимо, що вираз, як і передбачає метод Квайна, заданий у вигляді ДДНФ. За законом склеювання отримуємо:

$$(x \overset{1}{\wedge} y) \vee (x \overset{2}{\wedge} \overline{y}) \vee (\overline{x} \overset{3}{\wedge} \overline{y}) = (x \wedge y) \vee (x \wedge \overline{y}) \vee (\overline{x} \wedge \overline{y}) \vee \overset{1,2}{x} \vee \overset{2,3}{\overline{y}},$$

де номери над кон'юнктами у правій частині рівності позначають номери кон'юнктів вихідного виразу, використані для неповного склеювання.

До нових кон'юнктів неповне склеювання застосувати неможливо, і можемо переходити до другого етапу. Для неповного склеювання були використані всі кон'юнкти довжини 2, а отже всі ці кон'юнкти поглинаються породженими кон'юнктами довжини 1. Після застосування закону поглинання остаточно отримуємо: $E(x,y) = x \vee \overline{y}$.

Оскільки на першому етапі до виразу лише додаються нові кон'юнкти, недоцільно переписувати кон'юнкти вихідного виразу, які у будь-якому випадку залишаються без змін. Крім того, оскільки закон неповного склеювання можна застосовувати лише до кон'юнктів однакової довжини, спочатку слід застосувати цей закон до кон'юнктів довжини n

вихідної ДДНФ, отримуючи кон'юнкти довжини $n-1$; далі закон неповного склеювання слід застосувати до кон'юнктів довжини $n-1$, отримуючи кон'юнкти довжини $n-2$, і т. д.; процес має завершитись за скінченну кількість кроків.

Приклад 3.39. Застосуємо метод Квайна для отримання скороченої ДНФ виразу $E(x,y,z) = (x \wedge y) \vee (\overline{x} \wedge z) \vee (y \wedge \overline{z})$. Зведемо вираз до ДДНФ і пронумеруємо кон'юнкти повної довжини:

$$E(x,y,z) = (x \wedge \overset{1}{y} \wedge z) \vee (x \wedge \overset{2}{y} \wedge \overline{z}) \vee (\overline{x} \wedge \overset{3}{y} \wedge z) \vee (\overline{x} \wedge \overset{4}{\overline{y}} \wedge z) \vee (\overline{x} \wedge \overset{5}{y} \wedge \overline{z}).$$

Застосовуючи закон неповного склеювання і продовжуючи загальну нумерацію, отримуємо такі кон'юнкти довжини 2:

6) $x \wedge y$ (1,2);

7) $y \wedge z$ (1,3);

8) $y \wedge \overline{z}$ (2,5);

9) $\overline{x} \wedge z$ (3,4);

10) $\overline{x} \wedge y$ (3,5).

Деякі з кон'юнктів довжини 2 допускають подальше неповне склеювання:

11) y (6,10);

12) y (7,8).

Кон'юнкт y отримано двома способами, однак для подальшого поглинання важливо вказати всі варіанти склеювання.

Подальше неповне склеювання неможливе, тому переходимо до етапу поглинання. У неповному склеюванні не були задіяні лише кон'юнкти під номерами 9 ($\overline{x} \wedge z$) і 11 (y). Отже, отримуємо таку скорочену ДНФ, яка у цьому випадку, очевидно, є тупиковою: $E(x,y,z) = (\overline{x} \wedge z) \vee y$.

Для побудови тупикових форм знайдені прості імпліканти зводять в *імплікантну таблицю*, рядки якої нумерують простими імплікантами, а стовпці – кон'юнктами повної довжини, які входять до складу ДДНФ заданого виразу. У комірки імплікантної таблиці вписують символ «$*$», якщо проста імпліканта, що відповідає рядку комірки, поглинає кон'юнкт повної довжини, який відповідає стовпцю. Побудова тупикової ДНФ зводиться до знаходження ненадлишкової множини простих імплікант, які б у сукупності поглинали всі кон'юнкти повної довжини заданого виразу. Ненадлишковість множини простих імплікант означає, що будь-яка власна її підмножина не поглинає принаймні один із кон'юнктів повної довжини із ДДНФ заданого виразу.

Приклад 3.40. Застосуємо метод Квайна для отримання скороченої ДНФ виразу $E(x,y,z) = (x \wedge y) \vee (\overline{x} \wedge z) \vee (x \wedge y \wedge z)$. Зведення до ДДНФ і неповне склеювання проводимо аналогічно попереднім прикладам:

$$E(x,y,z) = (x \wedge \overset{1}{y} \wedge z) \vee (x \wedge \overset{2}{y} \wedge \overline{z}) \vee (\overline{x} \wedge \overset{3}{y} \wedge z) \vee (\overline{x} \wedge \overset{4}{\overline{y}} \wedge z);$$

5) $x \wedge y$ (1,2);

6) $y \wedge z$ (1,3);

7) $\overline{x} \wedge z$ (3,4).

Закон неповного склеювання до отриманих кон'юнктів застосувати неможливо. На другому етапі поглинаються кон'юнкти 1–4, тобто остаточно отримуємо таку скорочену ДНФ: $E(x,y,z) = (x \wedge y) \vee (\overline{x} \wedge z) \vee (y \wedge z)$.

Побудуємо імплікантну таблицю (табл. 3.3).

Таблиця 3.3

	$x \wedge y \wedge z$	$x \wedge y \wedge \overline{z}$	$\overline{x} \wedge y \wedge z$	$\overline{x} \wedge \overline{y} \wedge z$
$x \wedge y$	$*$	$*$		
$\overline{x} \wedge z$			$*$	$*$
$y \wedge z$	$*$		$*$	

Із табл. 3.3 видно, що імпліканти $x \wedge y$ та $\overline{x} \wedge z$ ядрові, оскільки кон'юнкт $x \wedge y \wedge \overline{z}$ поглинається лише імплікантою $x \wedge y$, кон'юнкт $\overline{x} \wedge \overline{y} \wedge z$ – лише імплікантою $\overline{x} \wedge z$. Втім, дві ядрові імпліканти поглинають усі чотири кон'юнкти із ДДНФ заданого виразу. Таким чином, проста імпліканта $y \wedge z$ дублюється ядром і не потрапить у жодну тупикову форму. Отже, маємо для виразу E одну тупикову форму $(x \wedge y) \vee (\overline{x} \wedge z)$.

З прикладу 3.40 видно, що для знаходження тупикових ДНФ за допомогою імплікантної таблиці доцільно визначити:

1) ядрові імпліканти, які увійдуть до будь-якої тупикової ДНФ;

2) кон'юнкти повної довжини, які поглинаються ядром.

Очевидно, що визначені ядрові імпліканти та кон'юнкти повної довжини, які поглинаються ядром, можна виключити із подальшого розгляду, тобто пошук тупикових форм зводиться до покриття неядровими імплікантами тих кон'юнктів повної довжини, які не поглинуло ядро. Отже, доцільно побудувати *спрощену імплікантну таблицю*, яку отримують із імплікантної таблиці викреслюванням тих рядків, які відповідають ядровим імплікантам, та тих стовпців, які відповідають кон'юнктам повної довжини, що поглинаються ядром. Зазначимо, що у прикладі 3.40 спрощена імплікантна таблиця не містить жодного стовпця, тобто є порожньою – єдина тупикова ДНФ містить лише ядрові імпліканти.

Приклад 3.41. Застосуємо метод Квайна до виразу з вектором значень (10111001) із прикладу 3.32. Зведення до ДДНФ і неповне склеювання проводимо аналогічно попереднім прикладам:

$$E(x,y,z) = (x \wedge \overset{1}{y} \wedge z) \vee (x \wedge \overset{2}{\overline{y}} \wedge \overline{z}) \vee (\overline{x} \wedge \overset{3}{y} \wedge z) \vee (\overline{x} \wedge \overset{4}{y} \wedge \overline{z}) \vee (\overline{x} \wedge \overset{5}{\overline{y}} \wedge \overline{z});$$

6) $y \wedge z$ (1,3);

7) $\overline{y} \wedge \overline{z}$ (2,5);

8) $\overline{x} \wedge y$ (3,4);

9) $\overline{x} \wedge \overline{z}$ (4,5).

Побудуємо імплікантну таблицю (табл. 3.4).

Таблиця 3.4

	$x \wedge y \wedge z$	$x \wedge \overline{y} \wedge \overline{z}$	$\overline{x} \wedge y \wedge z$	$\overline{x} \wedge y \wedge \overline{z}$	$\overline{x} \wedge \overline{y} \wedge \overline{z}$
$y \wedge z$	$*$		$*$		
$\overline{y} \wedge \overline{z}$		$*$			$*$
$\overline{x} \wedge y$			$*$	$*$	
$\overline{x} \wedge \overline{z}$				$*$	$*$

Ядро містить імпліканти $y \wedge z$ та $\overline{y} \wedge \overline{z}$, які поглинають кон'юнкти повної довжини $x \wedge y \wedge z$, $x \wedge \overline{y} \wedge \overline{z}$ та $\overline{x} \wedge y \wedge z$. Таким чином, спрощена імплікантна таблиця містить два рядки та один стовпчик (табл. 3.5).

Таблиця 3.5

	$\overline{x} \wedge y \wedge \overline{z}$
$\overline{x} \wedge y$	$*$
$\overline{x} \wedge \overline{z}$	$*$

Із спрощеної імплікантної таблиці видно, що тупикова ДНФ має містити одну із двох неядрових імплікант. Отже, отримуємо дві тупикові ДНФ: $(y \wedge z) \vee (\overline{y} \wedge \overline{z}) \vee (\overline{x} \wedge y)$ та $(y \wedge z) \vee (\overline{y} \wedge \overline{z}) \vee (\overline{x} \wedge \overline{z})$, що підтверджує результат, отриманий у прикладі 3.32 за допомогою карт Карно.

У складніших випадках для пошуку тупикових форм можна застосувати метод, пов'язаний із алгеброю висловлень: кожній неядровій імпліканті S поставимо у відповідність висловлення $A_S =$ «Імпліканта S входить до тупикової ДНФ». Тепер для кожного кон'юнкта K у складі вихідної ДДНФ можна побудувати висловлення $B_K =$ «K поглинає принаймні одна імпліканта тупикової ДНФ», яке, очевидно, є диз'юнкцією тих висловлень A_S, для яких S поглинає кон'юнкт K. Нарешті, у коректно побудованій тупиковій ДНФ прості імпліканти мають поглинати всі кон'юнкти повної довжини із вихідної ДДНФ, тобто коректність тупикової ДНФ означає істинність кон'юнкції всіх висловлень B_K. Метод передбачає зведення отриманої формули алгебри висловлень до ДНФ застосуванням законів дистрибутивності та, якщо це можливо, поглинання. В отриманій ДНФ кожен кон'юнкт задає певну тупикову ДНФ: кожна літера у складі кон'юнкта відповідає входженню до тупикової ДНФ відповідної неядрової імпліканти.

Приклад 3.42. Застосуємо наведений метод до виразу з вектором значень (10111001), для якого ядрові імпліканти і спрощена імплікантна таблиця знайдені у прикладі 3.41. Поставимо у відповідність двом неядровим простим імплікантам літери A та B, які позначають умову входження відповідної імпліканти до тупикової ДНФ (табл. 3.6).

Таблиця 3.6

		$\overline{x} \wedge y \wedge \overline{z}$
A	$\overline{x} \wedge y$	$*$
B	$\overline{x} \wedge \overline{z}$	$*$

Умова коректності тупикової ДНФ (поглинання неядровими простими імплікантами кон'юнкта $\overline{x}\wedge y\wedge\overline{z}$, який не поглинувся ядром) має тривіальний вигляд $A + B$, де «+» позначає операцію диз'юнкції з алгебри висловлень. Отже, маємо дві тупикові ДНФ, які відповідають входженню однієї з двох неядрових імплікант. З урахуванням ядрових імплікант отримуємо такі тупикові ДНФ: $(y\wedge z)\vee(\overline{y}\wedge\overline{z})\vee(\overline{x}\wedge y)$ та $(y\wedge z)\vee(\overline{y}\wedge\overline{z})\vee(\overline{x}\wedge\overline{z})$.

Приклад 3.43. Застосуємо наведений метод до скороченої ДНФ для виразу із вектором значень (01111110), знайдену в прикладі 3.37:

$$E(x, y, z) = (x \wedge \overline{y}) \vee (x \wedge \overline{z}) \vee (\overline{x} \wedge y) \vee (y \wedge \overline{z}) \vee (\overline{x} \wedge z) \vee (\overline{y} \wedge z).$$

Побудуємо імплікантну таблицю (табл. 3.7).

Таблиця 3.7

		$\overline{x} \wedge \overline{y} \wedge z$	$\overline{x} \wedge y \wedge \overline{z}$	$\overline{x} \wedge y \wedge z$	$x \wedge \overline{y} \wedge \overline{z}$	$x \wedge \overline{y} \wedge z$	$x \wedge y \wedge \overline{z}$
A	$x \wedge \overline{y}$				$*$	$*$	
B	$x \wedge \overline{z}$				$*$		$*$
C	$\overline{x} \wedge y$		$*$	$*$			
D	$y \wedge \overline{z}$		$*$				$*$
E	$\overline{x} \wedge z$	$*$		$*$			
F	$\overline{y} \wedge z$	$*$				$*$	

Оскільки кожен кон'юнкт повної довжини поглинається принаймні двома простими імплікантами, ядро заданого виразу порожнє, що унеможливлює спрощення імплікантної таблиці. Для побудови тупикових ДНФ пронумеруємо прості імпліканти літерами A–F, які позначають умову входження відповідної імпліканти до тупикової ДНФ. Випишемо у вигляді формули алгебри висловлень умову коректності тупикової ДНФ (прості імпліканти мають поглинати всі кон'юнкти повної довжини із вихідної ДДНФ):

$$(E+F)\&(C+D)\&(C+E)\&(A+B)\&(A+F)\&(B+D),$$

де «+» та «&» позначають операції над висловленнями – відповідно диз'юнкцію та кон'юнкцію. Зведемо цю формулу до ДНФ (знак «&» для скорочення запису опускатимемо):

$$\begin{gathered}ADE+BCF+ABCE+ABCF+ABDE+ACDE+ACDF+ADEF+\\+BCDF+BCEF+BDEF+ABCDE+ABCDF+ABCEF+\\+ABDEF+ACDEF+BCDEF+ABCDEF.\end{gathered}$$

Застосувавши закон поглинання, отримуємо остаточну умову

$$ADE+BCF+ABCE+ACDF+BDEF,$$

що означає наявність п'яти тупикових форм:

$$\begin{gathered}(x\wedge\overline{y})\vee(y\wedge\overline{z})\vee(\overline{x}\wedge z);\\(x\wedge\overline{z})\vee(\overline{x}\wedge y)\vee(\overline{y}\wedge z);\\(x\wedge\overline{y})\vee(x\wedge\overline{z})\vee(\overline{x}\wedge y)\vee(\overline{x}\wedge z);\\(x\wedge\overline{y})\vee(\overline{x}\wedge y)\vee(y\wedge\overline{z})\vee(\overline{y}\wedge z);\\(x\wedge\overline{z})\vee(y\wedge\overline{z})\vee(\overline{x}\wedge z)\vee(\overline{y}\wedge z).\end{gathered}$$

Зауваження 3.10. Описаний метод пошуку тупикових форм можна застосовувати до вихідної (не спрощеної) імплікантної таблиці, однак це може дещо ускладнити обчислення за рахунок появи ядрових імплікант.

Зауваження 3.11. У комп'ютерній реалізації алгоритму Квайна доцільно використовувати спеціальну нумерацію кон'юнктів. Для довільного кон'юнкта $E(x_1, \ldots, x_n)$ кожній змінній x_k ставлять у відповідність один із трьох символів: «1», якщо x_k входить до E без доповнення; «0», якщо x_k входить до E з доповненням; «–», якщо x_k взагалі не входить до кон'юнкта E. Так, кон'юнкту $E(x, y, z, t) = x \wedge \overline{z} \wedge t$ відповідає код $1{-}01$. Отримані коди розбивають на групи за кількістю входжень символа «1», що суттєво підвищує ефективність пошуку кон'юнктів для склеювання, оскільки достатньо перевіряти пари кодів із «сусідніх» груп [8].

Метод Блейка. Цей метод передбачає, що вираз заданий у вигляді довільної ДНФ (не обов'язково досконалої), і полягає у застосуванні двох тотожностей:

1) $(A \wedge x) \vee (B \wedge \overline{x}) = (A \wedge x) \vee (B \wedge \overline{x}) \vee (A \wedge B)$ (узагальнене склеювання);

2) $(A \wedge B) \vee A = A$ (поглинання).

Тотожності застосовують зліва направо; спочатку застосовують узагальнене склеювання доти, поки це можливо, а потім, поки можливо — поглинання. Можна довести [9], що у результаті маємо отримати скорочену ДНФ.

Як і в методі Квайна, на першому етапі вираз суттєво ускладнюється, оскільки з'являються нові кон'юнкти, однак на другому етапі ці нові кон'юнкти дають можливість позбутися інших кон'юнктів більшої довжини.

На відміну від неповного склеювання, узагальнене склеювання можна застосовувати до кон'юнктів різної довжини. Крім того, кон'юнкт K, отриманий із кон'юнктів K_1 і K_2 узагальненим склеюванням, не обов'язково поглинає K_1 і K_2, що ускладнює застосування методу Блейка порівняно з методом Квайна. Однак метод Блейка має перевагу: вихідний вираз можна не зводити до ДДНФ.

Приклад 3.44. Застосуємо метод Блейка для отримання скороченої ДНФ виразу $(x \wedge y) \vee (\overline{x} \wedge z) \vee (y \wedge \overline{z})$ із прикладу 3.39. Для зручності посилань пронумеруємо кон'юнкти вихідної ДНФ:

$$E(x, y, z) = (x \overset{1}{\wedge} y) \vee (\overline{x} \overset{2}{\wedge} z) \vee (y \overset{3}{\wedge} \overline{z}).$$

Застосовуючи узагальнене склеювання і продовжуючи загальну нумерацію, отримуємо такі кон'юнкти:

4) $y \wedge z$ (1,2);

5) $\overline{x} \wedge y$ (2,3).

Отримані кон'юнкти не допускають узагальненого склеювання між собою, однак допускають узагальнене склеювання з кон'юнктами 1–3:

6) y (4,3);

7) y (1,5).

Подальше узагальнене склеювання неможливе, і можна переходити до поглинання. Очевидно, кон'юнкт y поглинає всі кон'юнкти, окрім $\overline{x} \wedge z$, тож остаточно отримуємо таку скорочену ДНФ: $E(x, y, z) = (\overline{x} \wedge z) \vee y$.

Розділ 4

Булеві функції. Функціональна повнота

4.1. Основні поняття

У комп'ютерній математиці особливу роль відіграють відображення $f\colon \{0,1\}^{\times n} \to \{0,1\}$, $n \geqslant 0$, які називають *булевими функціями* (слово «булева» іноді опускатимемо). Елементи 0 та 1 можна вважати логічними хибністю й істинністю, але це можуть бути елементи довільної природи.

Вивчаючи булеві функції, зазвичай говорять про функції на множині $\{0,1\}$ від n аргументів (змінних), використовуючи запис $f(x_1, \ldots, x_n)$, де $x_1, \ldots, x_n \in \{0,1\}$. Число n, яке називають *арністю* функції f, за потреби вказують верхнім індексом у дужках, тобто використовують позначення $f^{(n)}$.

Випадок $n = 0$, за визначенням, відповідає функціям із значеннями у множині $\{0,1\}$, які не залежать від жодного аргумента, тобто константам 0 та 1.

Для $n = 1$ маємо 4 *унарні* функції $f^{(1)}\colon \{0,1\} \to \{0,1\}$ (табл. 4.1).

Таблиця 4.1. **Булеві функції однієї змінної**

x	01	Позначення	Назва
$f_0^{(1)}$	00	0	Константа 0
$f_1^{(1)}$	01	x	Тотожна функція
$f_2^{(1)}$	10	$\overline{x}$	Заперечення
$f_3^{(1)}$	11	1	Константа 1

Для $n = 2$ маємо 16 *бінарних* булевих функцій $f^{(2)}\colon \{0,1\}^{\times 2} \to \{0,1\}$, які подано у табл. 4.2.

Таблиця 4.2. **Булеві функції двох змінних**

x y	0011 0101	Позначення	Назва
$f_0^{(2)}$	0000	0	Константа 0
$f_1^{(2)}$	0001	$x \wedge y$	Кон'юнкція
$f_2^{(2)}$	0010	$\overline{x \to y}$	Заперечення від імплікації
$f_3^{(2)}$	0011	x	Проекція на перший аргумент
$f_4^{(2)}$	0100	$\overline{y \to x}$	Заперечення від оберненої імплікації
$f_5^{(2)}$	0101	y	Проекція на другий аргумент
$f_6^{(2)}$	0110	$x \oplus y$	Сума за модулем 2 (виключне «або»)
$f_7^{(2)}$	0111	$x \vee y$	Диз'юнкція
$f_8^{(2)}$	1000	$x \downarrow y$	Стрілка Пірса (заперечення диз'юнкції)
$f_9^{(2)}$	1001	$x \leftrightarrow y$	Еквіваленція
$f_{10}^{(2)}$	1010	$\overline{y}$	Заперечення від другого аргумента
$f_{11}^{(2)}$	1011	$y \to x$	Обернена імплікація
$f_{12}^{(2)}$	1100	$\overline{x}$	Заперечення від першого аргумента
$f_{13}^{(2)}$	1101	$x \to y$	Імплікація
$f_{14}^{(2)}$	1110	$x \vert y$	Штрих Шеффера (заперечення кон'юнкції)
$f_{15}^{(2)}$	1111	1	Константа 1

Вправа 4.1. Довести, що для $n \geqslant 0$ існує 2^{2^n} булевих функцій арності n.

Вказівка. Використовуючи комбінаторний принцип добутку, довести загальний факт: для скінченних множин A і B, які містять відповідно n_1 та n_2 елементів, існує $n_2^{n_1}$ відображень із A у B.

Булеві функції позначатимемо літерами f, g, h з індексами або без них, змінні – літерами x, y, z з індексами або без них. Множину всіх булевих функцій довільної скінченної арності позначають через P_2.

Якщо розглядати 1 та 0 як логічні істинність і хибність, то більшість бінарних функцій, визначених у табл. 4.2 (диз'юнкція, кон'юнкція, імплікація та ін.), набувають змісту відомих логічних операцій в алгебрі висловлень; унарна операція доповнення, визначена у табл. 4.1, відповідає логічному запереченню. Отже (див. приклад 3.4), алгебрична структура $\left\langle \{0,1\}, \vee, \wedge, \bar{\ }, 0, 1 \right\rangle$ є булевою алгеброю з відповідним булевим кільцем $\langle \{0,1\}, \oplus, \cdot \rangle$, де «$\cdot$» можна розглядати або як кон'юнкцію, або як арифметичне множення (інші операції визначені у табл. 4.1 і 4.2).

Означення 4.1. Говорять, що функція $f^{(n)}(x_1, \ldots, x_j, \ldots, x_n)$ містить фіктивну змінну x_j, якщо існує функція $g^{(n-1)}$, така, що

$$f^{(n)}(x_1, \ldots, x_j, \ldots, x_n) = g^{(n-1)}(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n)$$

для всіх $x_k \in \{0,1\}$, $1 \leqslant k \leqslant n$. Змінну, яка не є фіктивною, називають істотною.

Приклад 4.1. 1. Функція $f(x,y) = (x \wedge \overline{y}) \vee \overline{y} = \overline{y}$ містить одну фіктивну змінну x, змінна y істотна.

2. Функція $f(x) = x \wedge \overline{x} = 0$ не містить жодної істотної змінної – єдина змінна x є фіктивною.

Функції називають еквівалентними, якщо одну із цих функцій можна отримати з іншої додаванням та (або) вилученням фіктивних змінних.

Інакше кажучи, еквівалентні функції збігаються з точністю до фіктивних аргументів. Надалі, якщо не вказано інше, еквівалентні функції не розрізнятимемо.

Приклад 4.2. 1. Функція $f(x, y, z) = \overline{y}$ еквівалентна унарній функції $g(x) = \overline{x}$ (або, що те ж саме, $g(y) = \overline{y}$).

2. Функція $f(x) = x \vee \overline{x} = 1$ не залежить від жодного істотного аргумента та еквівалентна константі 1.

Визначимо рекурсивно поняття формули над непорожньою множиною (класом) булевих функцій $K \subset P_2$.

Означення 4.2. 1. Нехай $f^{(n)} \in K$. Тоді $f(x_1, \ldots, x_n)$ – формула над K.

2. Нехай $f^{(n)} \in K$, $E_1, \ldots, E_n$ – формули над K або змінні (не обов'язково різні). Тоді $f^{(n)}(E_1, \ldots, E_n)$ – формула над K.

3. Інших формул над класом K немає.

Так, над набором $K = \{\to, \vee\}$ можна, з-поміж інших, виписати формули $x \to y$, $x \to x$, $x \to (y \vee z)$, $x \to (y \vee x)$. Наголосимо, що для класичних бінарних функцій традиційно використовують інфіксну форму запису: $x \vee y$ замість $\vee(x, y)$; $x \to y$ замість $\to(x, y)$ і т. д.

Кожна формула над заданим класом $K \subset P_2$ природним чином задає булеву функцію, строге рекурсивне визначення надано, наприклад, у роботах [7; 10; 11]. Якщо булева функція f реалізована деякою формулою над класом K, то говорять, що f є *суперпозицією* функцій із набору K. Зазвичай функцію можна реалізувати різними формулами над заданим набором $K \subset P_2$. Так, у випадку $K = \{\to, 0\}$ константу 1 можна реалізувати, зокрема, формулами $x \to x$, $0 \to x$ та $0 \to (x \to x)$.

Означення 4.3. Замиканням непорожнього набору функцій $K \subset P_2$ називають множину функцій, які можна реалізувати формулами над набором K. Замикання набору K позначають через $[K]$.

Приклад 4.3. 1. $[\{\overline{x}\}] = \{\overline{x}, x\}$. Наголосимо, що над набором $[\{\overline{x}\}]$ існує нескінченна кількість формул $\overline{x}$, $\overline{\overline{x}}$, $\overline{\overline{\overline{x}}}$, і т. д., однак ці формули реалізують лише дві функції – тотожне відображення і доповнення.

2. $[\{\overline{x}, 0\}] = \{\overline{x}, x, 0, 1\}$.

3. $[\{\vee\}] = \{x,\ x_1 \vee x_2,\ x_1 \vee x_2 \vee x_3,\ \ldots\}$, тобто замикання набору $\{\vee\}$ містить нескінченну кількість функцій; тотожна функція x реалізується формулою $x \vee x$.

4. $[\{\vee, \wedge, \overline{x}\}] = P_2$, оскільки будь-яку булеву функцію можна зобразити у вигляді ДДНФ (або ДКНФ), тобто реалізувати формулою із використанням диз'юнкції, кон'юнкції та доповнення (див. п. 3.5.4). Зазначимо, що константи як спеціальні випадки ДДНФ і ДКНФ слід розглядати окремо: $0 = x \wedge \overline{x}$; $1 = x \vee \overline{x}$.

Зауваження 4.1. У попередньому прикладі і далі функції задаємо як з використанням відповідного функціонального символу («$\vee$», «$\to$» «$\bar{\ }$»), так і через формулу («$x \vee y$», «$x \to y$», «$\overline{x}$»). Обидва способи цілком коректні та можуть використовуватись без обмежень.

Зауваження 4.2. Якщо клас функцій $K \subset P_2$ містить тотожну функцію $f(x) = x$, замикання $[K]$ можна визначити таким кроком рекурсії: якщо $g_1^{(n)}, \ldots, g_m^{(n)} \in [K]$ та $g_0^{(m)} \in [K]$, то $[K]$ містить функцію $h^{(n)}$, яку визначає співвідношення

$$h^{(n)}(x_1, \ldots, x_n) = g_0^{(m)}(g_1^{(n)}(x_1, \ldots, x_n), \ldots, g_m^{(n)}(x_1, \ldots, x_n)).$$

Арності функцій g_k $(1 \leqslant k \leqslant m)$ справді можна вважати однаковими, оскільки функції визначаємо з точністю до фіктивних аргументів, тобто функції меншої арності можна доповнити відповідною кількістю фіктивних змінних.

Наведемо кілька елементарних властивостей оператора функціонального замикання:

- $[[K]] = [K]$, тобто повторне замикання не додає нових функцій;

- $[K_1 \cap K_2] \subset [K_1] \cap [K_2]$, тобто замикання перетину є підмножиною перетину замикань. Зазначимо, що рівності у загальному випадку може не бути – достатньо розглянути $K_1 = \{\overline{x}, 0\}$, $K_2 = \{\overline{x}, 1\}$;
- $[K_1 \cup K_2] \supset [K_1] \cup [K_2]$, тобто замикання об'єднання є надмножиною об'єднання замикань. Рівності у загальному випадку немає – достатньо розглянути $K_1 = \{\overline{x}\}$, $K_2 = \{\vee\}$.

Означення 4.4. Непорожній клас функцій $K \subset P_2$ називають функціонально замкненим або просто замкненим, якщо $[K] = K$.

Іншими словами, клас функцій $K \subset P_2$ є замкненим тоді і тільки тоді, коли суперпозиціями функцій із K не можна отримати «нових» функцій, які не належать K.

Приклад 4.4. 1. Клас P_2, очевидно, замкнений, оскільки за визначенням містить усі булеві функції.

2. Класи $\{0\}$, $\{0, 1\}$, $\{x\}$, $\{x, \overline{x}\}$, $\{x, 1\}$, $\{x, \overline{x}, 0, 1\}$ замкнені.

3. Клас $\{x, \overline{x}, 0\}$ незамкнений, оскільки $1 = \overline{0} \in [\{x, \overline{x}, 0\}]$.

4. Клас функцій $\{x_1 \vee \cdots \vee x_n : n \geqslant 1\}$ замкнений. Наголосимо, що цей клас не містить констант 0 та 1.

Наведемо два елементарні факти щодо властивості замкненості.

1. Нехай $K \subset P_2$, $K \neq \varnothing$. Тоді клас $[K]$ замкнений.

2. Нехай $K_1, K_2 \subset P_2$ – замкнені класи і $K_1 \cap K_2 \neq \varnothing$. Тоді клас $K_1 \cap K_2$ замкнений.

Зазначимо, що об'єднання замкнених класів може не бути замкненим класом – достатньо розглянути $K_1 = \{\overline{x}, x\}$; $K_2 = \{0\}$.

Означення 4.5. Непорожній клас функцій $K \subset P_2$ називають функціонально повним або просто повним, якщо $[K] = P_2$.

Іншими словами, клас функцій $K \subset P_2$ є повним тоді і тільки тоді, коли суперпозиціями функцій із K можна отримати всі булеві функції.

Приклад 4.5. 1. Клас P_2, очевидно, повний.

2. Клас $\{\vee, \wedge, \overline{x}\}$ повний, оскільки, як зазначалось у прикладі 4.3, п. 4, будь-яку булеву функцію можна задати у вигляді ДДНФ або ДКНФ, використовуючи техніку, описану у п. 3.5.4. Нагадаємо, що константи слід розглядати окремо: $0 = x \wedge \overline{x}$; $1 = x \vee \overline{x}$. Класи $\{\vee, \overline{x}\}$ та $\{\wedge, \overline{x}\}$ також повні, оскільки, використовуючи правило де Моргана, диз'юнкцію можна виразити через кон'юнкцію і доповнення, а кон'юнкцію – через диз'юнкцію і доповнення:

$$x \vee y = \overline{\overline{x} \wedge \overline{y}}; \quad x \wedge y = \overline{\overline{x} \vee \overline{y}}.$$

3. Клас $\{\wedge, \oplus, 1\}$ є повним, оскільки диз'юнкцію і доповнення можна виразити через функції цього набору за допомогою співвідношень (3.5), які визначають перехід від булевого кільця до булевої алгебри.

4. Клас $\{\to, \overline{x}\}$ є повним, оскільки диз'юнкцію можна виразити через функції цього набору за допомогою співвідношення $x \vee y = \overline{x} \to y$, а повнота набору $\{\vee, \overline{x}\}$ вже встановлена (п. 2 цього прикладу).

5. Клас $\{\to, 0\}$ є повним, оскільки доповнення можна виразити через функції цього набору за допомогою співвідношення $\overline{x} = x \to 0$, а повнота набору $\{\to, \overline{x}\}$ вже встановлена (п. 4 цього прикладу).

4.2. Основні функціонально замкнені класи булевих функцій

Існує нескінченна кількість замкнених класів булевих функцій. Повний опис замкнених класів у P_2 навів американський математик Еміль Леон Пост (1897–1954), на його честь функціонально замкнені класи в P_2 часто називають класами Поста [10; 11]. У роботі [11] розглянуто предикатний опис замкнених класів у P_2 з узагальненням на векторнозначні булеві функції.

У теорії функціональної повноти вирішальну роль відіграють п'ять замкнених класів, які буде розглянуто далі.

4.2.1. Функції, які зберігають константу

Означення 4.6. Говорять, що функція $f \in P_2$ зберігає константу 0, якщо $f(0, 0, \ldots, 0) = 0$. Говорять, що функція $f \in P_2$ зберігає константу 1, якщо $f(1, 1, \ldots, 1) = 1$. Множину функцій, які зберігають 0, позначають через T_0; множину функцій, які зберігають 1, позначають через T_1.

Приклад 4.6. 1. Функції x; $x \vee y$; $x \wedge y$ зберігають обидві константи, тобто належать обом класам T_0 й T_1. Так, $0 \wedge 0 = 0$; $1 \wedge 1 = 1$, отже $x \wedge y \in T_0$ та $x \wedge y \in T_1$.

2. Функції $x \to y$ та $x \leftrightarrow y$ належать класу T_1, але не належать T_0. Так, $0 \to 0 = 1 \neq 0$, $1 \to 1 = 1$, отже $x \to y \notin T_0$, $x \to y \in T_1$.

3. Легко перевірити, що $x \oplus y \in T_0$, однак $x \oplus y \notin T_1$.

4. Очевидно, що $\overline{x} \notin T_0$ та $\overline{x} \notin T_1$.

Лема 4.1. *Класи T_0 та T_1 функціонально замкнені.*

Доведення. Оскільки обидва класи містять тотожну функцію, можна скористатись зауваженням 4.2. Доведемо замкненість класу T_0. Нехай $g_1^{(n)}, \ldots, g_m^{(n)} \in T_0$ та $g_0^{(m)} \in T_0$. Враховуючи визначення формули над функціональним класом та результат зауваження 4.2, достатньо довести, що до класу T_0 належить функція

$$h^{(n)}(x_1, \ldots, x_n) = g_0^{(m)}(g_1^{(n)}(x_1, \ldots, x_n), \ldots, g_m^{(n)}(x_1, \ldots, x_n)).$$

Оскільки $g_k^{(n)}(0, 0, \ldots, 0) = 0$, $1 \leqslant k \leqslant m$, для функції h отримуємо:

$$h^{(n)}(0, 0, \ldots, 0) = g_0^{(m)}(0, 0, \ldots, 0) = 0,$$

тобто $h^{(n)} \in T_0$, що доводить функціональну замкненість класу T_0. Аналогічно можна довести замкненість T_1 (із заміною константи 0 на 1). $\square$

Теорема 4.1 (лема про функцію, що не зберігає константу)**.**

1. Нехай $f \notin T_0$, $f \in T_1$. Тоді $1 \in [\{f\}]$, тобто константу 1 можна реалізувати формулою, що містить лише функцію f.

2. Нехай $f \notin T_1$, $f \in T_0$. Тоді $0 \in [\{f\}]$, тобто константу 0 можна реалізувати формулою, що містить лише функцію f.

3. Нехай $f \notin T_0$, $f \notin T_1$. Тоді $\overline{x} \in [\{f\}]$, тобто функцію $\overline{x}$ можна реалізувати формулою, що містить лише функцію f.

Доведення. 1. Нехай $f^{(n)} \notin T_0$, $f^{(n)} \in T_1$. Розглянемо функцію $g(x) = f(x, x, \ldots, x) \in [\{f\}]$. Оскільки функція f зберігає 1 і не зберігає 0, отримуємо:

$$g(0) = f(0, 0, \ldots, 0) = 1; \quad g(1) = f(1, 1, \ldots, 1) = 1,$$

тобто $g(x) = 1$ для довільного $x \in \{0, 1\}$. Отже, функція g еквівалентна константі 1.

2. Нехай $f \notin T_1$, $f \in T_0$. Розглянемо функцію $g(x) = f(x, x, \ldots, x)$. Аналогічно попередньому пункту, отримуємо, що $g(x) = 0$ для довільного $x \in \{0, 1\}$. Отже, функція g еквівалентна константі 0.

3. Нехай $f \notin T_0$, $f \notin T_1$. Знову розглянемо функцію $g(x) = f(x, \ldots, x)$. Оскільки функція f не зберігає 0 і не зберігає 1, отримуємо:

$$g(0) = f(0, 0, \ldots, 0) = 1; \quad g(1) = f(1, 1, \ldots, 1) = 0,$$

тобто $g(x) = \overline{x}$ для довільного $x \in \{0, 1\}$. □

Доведення має конструктивний характер: ми не просто доводимо можливість отримати із функції f константу або доповнення, а вказуємо конкретний спосіб їх отримання.

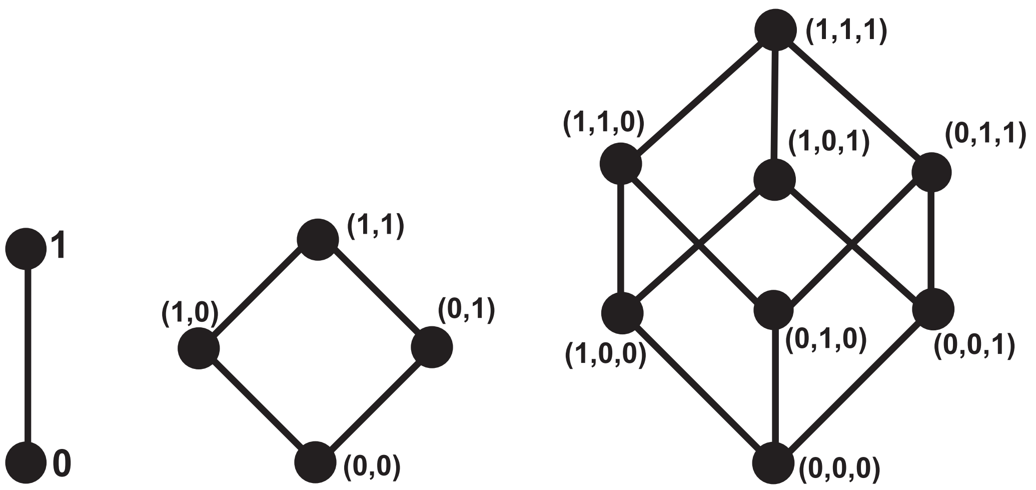
Приклад 4.7. 1. Розглянемо $f(x, y) = x \oplus y$. Очевидно, що $f \notin T_1$, $f \in T_0$. Користуючись методом, застосованим у доведенні теореми 4.1, отримуємо константу 0: $g(x) = x \oplus x = 0$.

2. Розглянемо $f(x, y) = x \to y$. Очевидно, що $f \notin T_0$, $f \in T_1$. Користуючись тим самим методом, отримуємо константу 1: $g(x) = x \to x = 1$.

3. Розглянемо $f(x, y) = x \downarrow y = \overline{x \vee y}$ (стрілка Пірса). Очевидно, що $f \notin T_0$, $f \notin T_1$. Користуючись тим самим методом, отримуємо доповнення: $g(x) = x \downarrow x = \overline{x}$.

4.2.2. Монотонні функції

На множині $\{0,1\}^{\times n}$, $n \geqslant 1$, зафіксуємо «покоординатне» відношення часткового порядку: набір $\alpha \in \{0,1\}^{\times n}$ передує набору $\beta \in \{0,1\}^{\times n}$, якщо $\alpha_k \leqslant \beta_k$ для всіх $k = 1, \ldots, n$; тут і надалі вважатимемо, що $0 < 1$. Для введеного відношення порядку використовуватимемо традиційне позначення $\alpha \preccurlyeq \beta$. Діаграми Гессе для множин $\{0,1\}^{\times 1} = \{0,1\}$, $\{0,1\}^{\times 2}$ і $\{0,1\}^{\times 3}$ відносно введеного відношення порядку зображено на рис. 4.1.



$\langle\{0,1\}, \preccurlyeq\rangle$ $\quad$ $\langle\{0,1\}^{\times 2}, \preccurlyeq\rangle$ $\quad$ $\langle\{0,1\}^{\times 3}, \preccurlyeq\rangle$

Рис. 4.1

Наголосимо, що введене відношення порядку за $n \geqslant 2$ нелінійне (наприклад, набори $(0,1)$ та $(1,0)$ непорівнянні).

Означення 4.7. Булеву функцію $f^{(n)}$ ($n \geqslant 1$) називають монотонною, якщо $f^{(n)}(\alpha) \leqslant f^{(n)}(\beta)$ для всіх $\alpha \preccurlyeq \beta$ ($\alpha, \beta \in \{0,1\}^{\times n}$).

Функції арності 0 (константи 0 та 1) за визначенням вважають монотонними. Втім функцію арності 0 додаванням фіктивного аргумента можна звести до функції арності 1, яка еквівалентна константі та монотонна безпосередньо за означенням 4.7.

Множину монотонних функцій позначають через M.

Приклад 4.8. Очевидно, що $x, x \vee y, x \wedge y \in M$, оскільки збільшення будь-якого аргумента цих функцій не зменшує значення функції.

Приклад 4.9. Очевидно, що $x \to y \notin M$, оскільки $0 \to 0 = 1$ та $1 \to 0 = 0$, але $(0,0) \preccurlyeq (1,0)$.

У роботі [12] наведено ефективний комп'ютерно орієнтований алгоритм перевірки булевої функції на монотонність, який зводиться до порівняння значень функції лише на таких $\alpha, \beta \in \{0,1\}^{\times n}$, якщо α безпосередньо передує β.

Лема 4.2. *Клас M функціонально замкнений.*

Доведення. Доведення зводиться до зауваження 4.2 і проводиться аналогічно доведенню леми 4.1. □

Теорема 4.2 (лема про немонотонну функцію)**.** *Нехай $f \notin M$. Тоді $\overline{x} \in [\{f, 0, 1\}]$, тобто функцію $\overline{x}$ можна реалізувати формулою, що містить лише функцію f та константи 0 і 1.*

Доведення. Нехай $f^{(n)} \notin M$. Зазначимо, що $n \geqslant 1$, оскільки константи 0 та 1 – монотонні функції. Оскільки $f \notin M$, існують набори $\alpha, \beta \in \{0,1\}^{\times n}$, такі, що $\alpha \preccurlyeq \beta$, але $f(\alpha) > f(\beta)$. Оскільки булеві функції набувають лише значень 0 та 1, отримуємо: $f(\alpha) = 1$, $f(\beta) = 0$.

Введемо у розгляд функції $g_k(x)$, $k = 1, 2, \dots, n$:

$$g_k(x) = \begin{cases} 0, \text{ якщо } \alpha_k = \beta_k = 0; \\ 1, \text{ якщо } \alpha_k = \beta_k = 1; \\ x, \text{ якщо } \alpha_k = 0, \ \beta_k = 1. \end{cases}$$

Іншими словами, $g_k(x)$ є або константою $c \in \{0, 1\}$, якщо $\alpha_k = \beta_k = c$, або тотожною функцією x, якщо $\alpha_k \neq \beta_k$, тобто $\alpha_k = 0$, $\beta_k = 1$. Випадок $\alpha_k = 1$, $\beta_k = 0$ неможливий, оскільки $\alpha_k \leqslant \beta_k$ для всіх $k = 1, 2, \dots, n$.

Легко зрозуміти, що $g_k(0) = \alpha_k$, $g_k(1) = \beta_k$ $(1 \leqslant k \leqslant n)$, оскільки

$$g_k(0) = \begin{cases} 0, \text{ якщо } \alpha_k = 0, \ \beta_k \in \{0, 1\}; \\ 1, \text{ якщо } \alpha_k = \beta_k = 1; \end{cases}$$

$$g_k(1) = \begin{cases} 0, \text{ якщо } \alpha_k = \beta_k = 0; \\ 1, \text{ якщо } \beta_k = 1, \ \alpha_k \in \{0, 1\}. \end{cases}$$

Тепер розглянемо функцію $g(x) = f(g_1(x), \dots, g_n(x))$. Очевидно, що $g(0) = f(g_1(0), g_2(0), \dots, g_n(0)) = f(\alpha_1, \alpha_2, \dots, \alpha_n) = f(\alpha) = 1$ та $g(1) = f(g_1(1), \dots, g_n(1)) = f(\beta) = 0$. Таким чином, $g(0) = 1$, $g(1) = 0$, тобто $g(x) = \overline{x}$ для всіх $x \in \{0, 1\}$, що завершує доведення. Наголосимо, що кожна з формул $g_k(x)$ $(1 \leqslant k \leqslant n)$, які підставляємо у $f(x_1, \dots, x_n)$, є або змінною x, або константою 0, або константою 1, тобто функція $g(x) = \overline{x}$ справді задана формулою над $\{f, 0, 1\}$. □

Доведення має конструктивний характер і описує конкретний спосіб отримання функції $\overline{x}$ із довільної немонотонної функції та констант 0 і 1.

Приклад 4.10. 1. Нехай $f(x_1, x_2) = x_1 \to x_2$. Наборами, що спростовують монотонність цієї функції, є $\alpha = (0, 0)$ та $\beta = (1, 0)$. Тоді у позначеннях доведення теореми 4.2 отримуємо: $g_1(x) = x$, оскільки $\alpha_1 = 0$, $\beta_1 = 1$, тобто $\alpha_1 \neq \beta_1$; $g_2(x) = 0$, оскільки $\alpha_2 = \beta_2 = 0$. Отже,

$g(x) = g_1(x) \to g_2(x) = x \to 0 = \overline{x}$.

2. Нехай $f(x_1, x_2) = x_1 \oplus x_2$. Наборами, які спростовують монотонність цієї функції, є, наприклад, $\alpha = (1, 0)$ та $\beta = (1, 1)$, оскільки $0 \oplus 1 = 1 \succ 1 \oplus 1 = 0$. Отже, $g_1(x) = 1$, $g_2(x) = x$, звідки $g(x) = 1 \oplus x = \overline{x}$.

4.2.3. Самодвоїсті функції

Означення 4.8. Функцією, двоїстою до функції $f\colon \{0,1\}^{\times n} \to \{0,1\}$, називають булеву функцію

$$f^*(x_1, \ldots, x_n) = \overline{f(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n)}.$$

Приклад 4.11. 1. Обчислимо функцію, двоїсту до доповнення: $(\overline{x})^* = \overline{\overline{\overline{x}}} = \overline{x}$.

2. Обчислимо функцію, двоїсту до тотожної функції: $(x)^* = \overline{\overline{x}} = x$.

3. Обчислимо функцію, двоїсту до диз'юнкції: $(x \vee y)^* = \overline{\overline{x} \vee \overline{y}} = x \wedge y$.

4. Обчислимо функції, двоїсті до констант: $0^* = \overline{0} = 1$; $1^* = \overline{1} = 0$.

5. Обчислимо функцію, двоїсту до еквіваленції. Використовуючи очевидні тотожності $x \oplus y = \overline{x \leftrightarrow y}$ та $\overline{x} = x \oplus 1$, а також асоціативність і комутативність функції (бінарної операції) «$\oplus$», отримуємо:

$$(x \leftrightarrow y)^* = \overline{\overline{x} \leftrightarrow \overline{y}} = \overline{x} \oplus \overline{y} = (x \oplus 1) \oplus (y \oplus 1) = x \oplus y.$$

6. Обчислимо функцію, двоїсту до імплікації: $(x \to y)^* = \overline{\overline{x} \to \overline{y}} = \overline{x} \wedge y$.

Із означення двоїстої функції можна легко вивести такі твердження:

- $(f^*)^* = f$;
- $(f^* = g) \Rightarrow (g^* = f)$. Наприклад, $(\vee^* = \wedge) \Rightarrow (\wedge^* = \vee)$, $(\leftrightarrow^* = \oplus) \Rightarrow (\oplus^* = \leftrightarrow)$.

Окремо сформулюємо *принцип двоїстості*, який також легко встановити із визначення двоїстої функції: якщо

$$f(x_1, \ldots, x_n) = h(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)),$$

то функцію, двоїсту до f, визначає співвідношення

$$f^*(x_1, \ldots, x_n) = h^*(g_1^*(x_1, \ldots, x_n), \ldots, g_m^*(x_1, \ldots, x_n));$$

однакова арність функцій g_k $(1 \leqslant k \leqslant m)$ не є обмеженням, оскільки функції меншої арності можна доповнити фіктивними змінними.

Зауваження 4.3. Принцип двоїстості можна сформулювати так: якщо функція f задана деякою формулою E, то функцію f^* можна задати формулою E^*, яка отримана із формули E заміною усіх функцій у складі E на відповідні двоїсті.

Приклад 4.12. 1. Функція, двоїста до імплікації $x \to y = \overline{x} \vee y$ безпосередньо обчислена у прикладі 4.11: $(x \to y)^* = \overline{x} \wedge y$. Однак формулу $\overline{x} \wedge y$ можна було б отримати із формули $\overline{x} \vee y$ заміною диз'юнкції на двоїсту функцію, тобто на кон'юнкцію (двоїста до $\overline{x}$ збігається із $\overline{x}$).

2. Використовуючи принцип двоїстості, обчислимо функцію, двоїсту до функції $f(x,y,z) = (x \vee y) \oplus z$. Оскільки $\vee^* = \wedge$ та $\oplus^* = \leftrightarrow$, отримуємо: $f^*(x,y,z) = ((x \vee y) \oplus z)^* = (x \wedge y) \leftrightarrow z$.

Означення 4.9. Булеву функцію f називають самодвоїстою, якщо $f^* = f$. Множину самодвоїстих функцій позначають через S.

Приклад 4.13. 1. Тотожна функція x та доповнення $\overline{x}$ самодвоїсті.

2. Диз'юнкція, еквіваленція та імплікація несамодвоїсті. Взагалі, легко перевірити, що серед функцій двох істотних змінних немає жодної самодвоїстої.

3. Розглянемо функцію $M(x,y,z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$. Очевидно, що $M^*(x,y,z) = m(x,y,z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$. Однак тотожність $M(x,y,z) = m(x,y,z)$ легко встановити безпосередньо, скориставшись законом дистрибутивності, або отримати із теореми 2.8, яка виконується в довільній модулярній решітці, а отже і в булевій алгебрі $\langle \{0,1\}, \vee, \wedge, \bar{\ }, 0, 1 \rangle$. Таким чином, $M(x,y,z) = m(x,y,z) \in S$.

Самодвоїстість булевої функції $f^{(n)}$ легко перевірити за її вектором значень, оскільки протилежні набори $(\alpha_1, \ldots, \alpha_n) \in \{0,1\}^{\times n}$ та $(\overline{\alpha}_1, \ldots, \overline{\alpha}_n) \in \{0,1\}^{\times n}$ розміщені симетрично відносно середини таблиці істинності. Справді, для $n = 2$ маємо розташування наборів (за зростанням у двійковій системі) $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$, і дві пари протилежних наборів $(0,0)$–$(1,1)$ та $(0,1)$–$(1,0)$ розміщені симетрично відносно середини; у загальному випадку цей факт можна довести, наприклад, індукцією за n. Тепер очевидно, що вектор значень самодвоїстої функції $f^{(n)}$ має вигляд $(c_0, c_1, \ldots, c_{2^{n-1}-1}, \overline{c}_{2^{n-1}-1}, \overline{c}_1, \overline{c}_0)$ – на протилежних наборах функція набуває протилежних значень.

Приклад 4.14. 1. Функція арності 3 з вектором значень (01110000) несамодвоїста, оскільки на протилежних наборах (000) та (111) (перша і остання координати у векторі значень) функція набуває значення 0.

2. Серед функцій арності n існує $2^{2^{n-1}}$ самодвоїстих, оскільки вектор значень самодвоїстої функції однозначно визначається значеннями на половині наборів, тобто на 2^{n-1} наборах. Зокрема, серед бінарних функцій (враховуючи фіктивні аргументи) існує $2^{2^{2-1}} = 4$ функції, які визначаються векторами (0011), (0101), (1010) та (1100). Із табл. 4.2 бачимо, що це функції $f_3(x,y) = x$; $f_5(x,y) = y$; $f_{10}(x,y) = \overline{y}$; $f_{12}(x,y) = \overline{x}$; усі ці функції мають фіктивний аргумент, тобто, як зазначалось у прикладі 4.13, не існує жодної самодвоїстої функції двох істотних аргументів.

Лема 4.3. *Клас S функціонально замкнений.*

Доведення. З урахуванням зауваження 4.2, твердження леми випливає із принципу двоїстості. □

Теорема 4.3 (лема про несамодвоїсту функцію)**.** *Нехай $f \notin S$. Тоді $0, 1 \in [\{f, \overline{x}\}]$, тобто константи 0 та 1 можна реалізувати формулою, що містить лише функції f та $\overline{x}$.*

Доведення. Нехай $f^{(n)} \notin S$. Зазначимо, що для доведення достатньо отримати із функцій f та $\overline{x}$ хоча б одну із констант 0 або 1, оскільки другу константу отримуємо, використовуючи доповнення. Зазначимо, що випадок $n = 0$ тривіальний, оскільки тоді функція f є константою 0 або константою 1. Отже, вважатимемо, що $n \geqslant 1$.

Оскільки $f^{(n)} \notin S$, існує такий набір $\alpha \in \{0,1\}^{\times n}$, що $f(\alpha) \neq f^*(\alpha)$. Враховуючи визначення двоїстої функції, маємо:

$$f(\alpha_1, \ldots, \alpha_n) \neq \overline{f(\overline{\alpha}_1, \ldots, \overline{\alpha}_n)}.$$

Оскільки булева функція може набувати лише двох значень, а застосування доповнення змінює значення, отримуємо:

$$f(\alpha_1, \ldots, \alpha_n) = f(\overline{\alpha}_1, \ldots, \overline{\alpha}_n) = c,$$

де $c \in \{0,1\}$ – фіксована константа. Розглянемо унарну функцію $g(x) = f(x \oplus \alpha_1, x \oplus \alpha_2, \ldots, x \oplus \alpha_n)$. Очевидно, що

$$g(0) = f(\alpha_1, \ldots, \alpha_n) = c; \quad g(1) = f(\overline{\alpha}_1, \ldots, \overline{\alpha}_n) = c,$$

тобто $g(0) = g(1) = c$. Отже, $g(x) = c$ для усіх $x \in \{0,1\}$. Зазначимо, що кожна з функцій $x \oplus \alpha_k$ $(1 \leqslant k \leqslant n)$, що їх підставляємо в $f(x_1, \ldots, x_n)$, є або змінною x, або функцією $\overline{x}$, тобто функція $g(x) = c$ справді задана формулою над $\{f, \overline{x}\}$. Отже, отримано одну з констант із $\{0,1\}$, другу константу отримуємо формулою $\overline{c}$, що завершує доведення леми. □

Наголосимо на конструктивності доведення, що надає конкретний спосіб отримання констант 0 та 1 із довільної функції $f \notin S$ та функції $\overline{x}$.

Приклад 4.15. Розглянемо функцію $f(x_1, x_2) = x_1 \vee x_2$. Очевидно, що $f^*(x_1, x_2) = x_1 \wedge x_2$. Для спростування самодвоїстості f можна взяти, наприклад, набір $\alpha = (0,1)$. Отримуємо:

$$g(x) = f(x \oplus 0, x \oplus 1) = f(x, \overline{x}) = x \vee \overline{x} = 1.$$

Отже, отримали константу $1 = f(x, \overline{x})$; константу 0 отримуємо, застосувавши доповнення: $0 = \overline{1} = \overline{f(x, \overline{x})}$.

4.2.4. Поліном Жегалкіна. Лінійні функції

Розглянемо формули над набором $\{\oplus, \wedge, 0, 1\}$. Відомо (див. приклад 3.4), що множина $\{0, 1\}$ утворює кільце за додаванням «$\oplus$» та множенням «$\wedge$». Орієнтуючись на традиційні позначення, прийняті в теорії кілець, для операції «$\wedge$» будемо використовувати позначення «$\cdot$». Враховуючи комутативність та асоціативність операцій «$\oplus$» та «$\cdot$», не розрізнятимемо формули, які різняться лише порядком аргументів цих операцій, і опускатимемо дужки у формулах з послідовним застосуванням однієї із цих операцій. Так, не будемо розрізняти формули $x \oplus (y \oplus z)$ та $(x \oplus z) \oplus y$; $x \cdot (y \cdot z)$ та $(x \cdot z) \cdot y$, і записуватимемо ці формули без дужок: $x \oplus y \oplus z$ та $x \cdot y \cdot z$. Крім того, вважатимемо пріоритет операції «$\cdot$» вищим за пріоритет «$\oplus$», опускаючи дужки з обох боків формули із зовнішньою операцією «$\cdot$». Так, замість $x \oplus (y \cdot z)$ писатимемо $x \oplus y \cdot z$. Нарешті, якщо аргументами «$\cdot$» є змінні, символ «$\cdot$» іноді опускатимемо, тобто замість $a \cdot x \cdot y$ частіше писатимемо axy.

Означення 4.10. Поліномом Жегалкіна[1] з n змінними називають формулу

$$
\begin{gathered}
a \oplus a_1x_1 \oplus a_2x_2 \oplus \dots \oplus a_nx_n \oplus a_{1,2}x_1x_2 \oplus a_{1,3}x_1x_3 \oplus \dots \oplus a_{n-1,n}x_{n-1}x_n \oplus \\
\oplus a_{1,2,3}x_1x_2x_3 \oplus \dots \oplus a_{n-2,n-1,n}x_{n-2}x_{n-1}x_n \oplus \dots \oplus a_{1,2,\dots,n}x_1x_2\cdots x_n,
\end{gathered}
$$

де $a_{j_1,j_2,\dots,j_k}$ $(0 \leqslant k \leqslant n)$ – фіксовані коефіцієнти 0 або 1.

Для тривіального випадку $n = 0$ поліном Жегалкіна має вигляд a, тобто є константою 0 або 1. Наведемо загальний вигляд поліномів Жегалкіна для випадків $n = 1, 2, 3$, використовуючи для змінних традиційні позначення x, y, z:

[1] Жегалкін Іван Іванович (1869–1947) – радянський математик, автор робіт з математичної логіки та основ математики; запропонував розглядати математичну логіку як алгебру лишків за модулем 2, яку у наш час називають алгеброю Жегалкіна.

$f^{(1)}(x) = a \oplus a_1 x;$

$f^{(2)}(x, y) = a \oplus a_1 x \oplus a_2 y \oplus a_{1,2} xy;$

$f^{(3)}(x, y, z) = a \oplus a_1 x \oplus a_2 y \oplus a_3 z \oplus a_{1,2} xy \oplus a_{1,3} xz \oplus a_{2,3} yz \oplus a_{1,2,3} xyz.$

Зазначимо, що поліном Жегалкіна можна розглядати як суму (за операцією «$\oplus$») кон'юнктів вигляду $x_{j_1} x_{j_2} \cdots x_{j_k}$ – такий кон'юнкт входить до полінома тоді і тільки тоді, коли $a_{j_1,j_2,\ldots,j_k} = 1$; якщо $a_{j_1,j_2,\ldots,j_k} = 0$, відповідний кон'юнкт $x_{j_1} x_{j_2} \cdots x_{j_k}$ до полінома не входить. Зазначимо, що коефіцієнту a відповідає порожній кон'юнкт 1.

Приклад 4.16. Наведемо зображення у вигляді поліномів Жегалкіна для деяких простих функцій, які легко встановити із тотожностей 3.5:

$\overline{x} = 1 \oplus x;$

$x \vee y = x \oplus y \oplus xy;$

$x \leftrightarrow y = \overline{x \oplus y} = 1 \oplus x \oplus y;$

$x \to y = \overline{x} \vee y = \overline{x \wedge \overline{y}} = 1 \oplus x \cdot (1 \oplus y) = 1 \oplus x \oplus xy.$

Теорема 4.4. *Будь-яку булеву функцію можна зобразити у вигляді полінома Жегалкіна єдиним способом (з точністю до переставлення аргументів операцій «$\oplus$» та «$\cdot$»).*

Доведення. Можливість зображення випливає із того, що будь-яку булеву функцію можна подати у вигляді ДДНФ або ДКНФ, використовуючи техніку, описану у підрозділі 3.5.4. Для диз'юнкції і доповнення поліноми Жегалкіна наведені у прикладі 4.16, відтак достатньо «розкрити дужки» за законом дистрибутивності, спростити доданки за ідемпотентністю $x \cdot x = x$ та «звести подібні члени» за законом $x \oplus x = 0$.

Для доведення єдиності зображення функції у вигляді полінома Жегалкіна достатньо порівняти кількість поліномів Жегалкіна з n змінними і кількість булевих функцій фіксованої арності n. Із комбінаторного принципу добутку легко встановити, що над змінними $x_1, x_2, \ldots, x_n$ існує в точності 2^n кон'юнктів $x_{j_1} x_{j_2} \cdots x_{j_k}$ $(0 \leqslant k \leqslant n)$, оскільки для кожної із n змінних під час формування кон'юнкта існує два варіанти –

входити або не входити до кон'юнкта. Кожен із цих 2^n кон'юнктів може входити або не входити до полінома, звідки отримуємо 2^{2^n} способів побудови полінома Жегалкіна з n змінними. Отже, кількість поліномів Жегалкіна з n змінними збігається із кількістю булевих функцій арності n (див. вправу 4.1). Враховуючи, що для кожної булевої функції $f^{(n)}$ існує принаймні один спосіб зображення у вигляді полінома Жегалкіна, отримуємо єдиність полінома Жегалкіна для кожної функції $f^{(n)}$. Отже, теорему доведено. $\square$

Будувати поліноми Жегалкіна через ДНФ або КНФ (зокрема через ДДНФ або ДКНФ) можна, але це досить неефективно. Якщо функція задана формулою, слід шукати способи еквівалентних перетворень цієї формули, щоб отримати складові частини із простими поліномами Жегалкіна. Так, диз'юнкцію іноді зручно звести до кон'юнкції за законом де Моргана, оскільки кон'юнкція і доповнення мають дуже прості зображення у вигляді полінома Жегалкіна; еквіваленцію слід не розписувати через диз'юнкцію, кон'юнкцію і доповнення, а зобразити як доповнення до «$\oplus$», отримуючи вираз типу $1 \oplus A \oplus B$, – ці прийоми продемонстровано у прикладі 4.16 для імплікації та еквіваленції.

Приклад 4.17. 1. Користуючись наведеними рекомендаціями, знайдемо поліном Жегалкіна для функції $f(x, y, z) = \overline{x} \vee (y \leftrightarrow z)$:

$$\overline{x} \vee (y \leftrightarrow z) = \overline{x \wedge \overline{y \leftrightarrow z}} = 1 \oplus x \cdot (y \oplus z) = 1 \oplus xy \oplus xz.$$

2. Для функції $f(x, y) = \overline{x} \leftrightarrow (x \vee y)$ отримуємо:

$$\overline{x} \leftrightarrow (x \vee y) = \overline{\overline{x} \oplus (x \oplus y \oplus xy)} = 1 \oplus 1 \oplus x \oplus x \oplus y \oplus xy = y \oplus xy.$$

У наш час розроблено ефективні універсальні методи обчислення коефіцієнтів полінома Жегалкіна за вектором значень вихідної функції [12].

Означення 4.11. Булеву функцію $f^{(n)}$ називають лінійною, якщо її поліном Жегалкіна містить лише кон'юнкти не більше ніж з однією змінною: $f^{(n)}(x_1, x_2, \ldots, x_n) = a \oplus a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n$. Множину лінійних функцій позначають через L.

Приклад 4.18. 1. Функції 0, 1, x, $\overline{x}$, $x \oplus y$, $x \leftrightarrow y$ лінійні, оскільки їх поліноми Жегалкіна не містять інших кон'юнктів, окрім порожнього кон'юнкта 1 та кон'юнктів з однією змінною x та y. Зазначимо, що функція 0 не містить жодного кон'юнкта, а отже за визначенням є лінійною.

2. Функції $x \wedge y = xy$; $x \vee y = x \oplus y \oplus xy$; $x \to y = 1 \oplus x \oplus xy$ нелінійні, оскільки їх поліноми Жегалкіна містять «нелінійний» кон'юнкт xy.

Лема 4.4. *Клас L функціонально замкнений.*

Доведення. З урахуванням зауваження 4.2, твердження леми випливає із лінійності суперпозиції лінійних функцій. □

Теорема 4.5 (лема про нелінійну функцію)**.** *Нехай $f \notin L$. Тоді $x \wedge y \in [\{f, \overline{x}, 0\}]$, тобто кон'юнкцію можна реалізувати формулою, що містить лише функції f, $\overline{x}$ та 0.*

Доведення. Нехай $f^{(n)} \notin L$, $n \geqslant 2$ (всі функції арності 0 та 1 лінійні). Спочатку доведемо, що суперпозицією функції $f^{(n)}$ та константи 0 (функція $\overline{x}$ на цьому етапі не потрібна) можна отримати деяку нелінійну функцію арності 2. Оскільки функція f нелінійна, її поліном Жегалкіна має містити принаймні один нелінійний кон'юнкт, тобто кон'юнкт довжиною 2 або більше. Серед нелінійних кон'юнктів функції f зафіксуємо кон'юнкт E найменшої довжини m (очевидно, $2 \leqslant m \leqslant n$); якщо поліном містить декілька нелінійних кон'юнктів однакової мінімальної довжини m (наприклад, декілька кон'юнктів довжиною $m = 2$), зафіксуємо будь-який із них. Без втрати загальності можна вважати, що зафіксований кон'юнкт E містить змінні $x_1, x_2, \ldots, x_m$:

$$\begin{aligned} f(x_1, \ldots, x_n) = \underbrace{a \oplus x_{j_1} \oplus \cdots \oplus x_{j_k}}_{\text{лінійна частина}} \oplus \underbrace{x_1x_2 \cdots x_m}_{\text{кон'юнкт } E} \oplus \\ \oplus \underbrace{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots}_{\text{інші кон'юнкти довжини } m \text{ або більше}} . \end{aligned} \tag{4.1}$$

Розглянемо бінарну функцію

$$g(x, y) = f^{(n)}(\underbrace{x, y, y, \ldots, y}_{m}, \underbrace{0, \ldots, 0}_{n-m}),$$

отриману із $f(x_1, \ldots, x_n)$ підстановкою x замість x_1, y замість $x_2, \ldots, x_m$ та 0 замість $x_{m+1}, \ldots, x_n$. За такої заміни лінійна частина полінома (4.1) залишиться лінійною, кон'юнкт $E(x_1, \ldots, x_m)$ набуде вигляду $E(x, y, y, \ldots, y) = xy$, а всі інші нелінійні кон'юнкти стануть тотожним нулем, оскільки кожен з них має довжину не менше за m і є відмінним від $E(x_1, \ldots, x_m)$, а отже містить принаймні одну змінну зі списку $x_{m+1}, \ldots, x_n$. Таким чином, поліном Жегалкіна для $g(x, y)$ має вигляд:

$$g(x, y) = a \oplus a_1 x \oplus a_2 y \oplus xy, \tag{4.2}$$

тобто $g(x, y) \notin L$. Зазначимо, що за побудовою $g \in [\{f, 0\}]$, тобто із функції $f^{(n)}$ та константи 0 отримано бінарну нелінійну функцію $g^{(2)}$.

Тепер для доведення теореми достатньо реалізувати кон'юнкцію $x \wedge y = xy$ як суперпозицію функцій $g(x, y)$ та $\overline{x}$ (константа 0 на цьому етапі не знадобиться). Покажемо, що існують такі константи $\gamma, \gamma_1, \gamma_2 \in \{0, 1\}$, що

$$g(x \oplus \gamma_1, y \oplus \gamma_2) \oplus \gamma = xy. \tag{4.3}$$

Використавши розклад (4.2), отримуємо:

$$g(x \oplus \gamma_1, y \oplus \gamma_2) \oplus \gamma = (a \oplus a_1\gamma_1 \oplus a_2\gamma_2 \oplus \gamma_1\gamma_2 \oplus \gamma) \oplus (a_1 \oplus \gamma_2) \cdot x \oplus (a_2 \oplus \gamma_1) \cdot y \oplus xy.$$

Для забезпечення рівності (4.3) отримуємо систему рівнянь

$$\begin{cases} a_1 \oplus \gamma_2 = 0; \\ a_2 \oplus \gamma_1 = 0; \\ a \oplus a_1\gamma_1 \oplus a_2\gamma_2 \oplus \gamma_1\gamma_2 \oplus \gamma = 0, \end{cases}$$

яка має єдиний розв'язок відносно $\gamma, \gamma_1, \gamma_2$:

$$\begin{cases} \gamma_1 = a_2; \\ \gamma_2 = a_1; \\ \gamma = a \oplus a_1 a_2. \end{cases}$$

Теорему доведено.

Зазначимо, що для побудови кон'юнкції було використано функцію $h(z) = c \oplus z$, яка залежно від параметра $c \in \{0, 1\}$ збігається з тотожною функцією ($h(z) = z$, якщо $c = 0$) або з доповненням ($h(z) = \overline{z}$, якщо $c = 1$), тобто $h(z)$ можна використовувати для побудови xy як суперпозиції функцій $g(x, y)$ та $\overline{x}$. □

Звернемо увагу на конструктивність доведення: отримано конкретний спосіб побудови кон'юнкції із довільної нелінійної функції, константи 0 та функції $\overline{x}$.

Приклад 4.19. Побудуємо кон'юнкцію $x \wedge y$ як суперпозицію функції $f(x_1, x_2, x_3, x_4) = x_1 \oplus x_3 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2x_3x_4$, константи 0 і функції $\overline{x}$. Використовуючи схему доведення леми про нелінійну функцію, спочатку побудуємо із f та константи 0 бінарну нелінійну функцію $g(x, y)$. Функція f задана поліномом Жегалкіна, який містить 2 нелінійних кон'юнкти з трьома змінними і один – з чотирма. Отже, за нелінійний кон'юнкт E мінімальної довжини можемо вибрати будь-який із двох кон'юнктів довжиною 3; виберемо $E = x_1x_3x_4$. У доведенні теореми для простоти позначень вважалось, що кон'юнкт E залежить від перших m змінних. Однак перенумеровувати змінні не будемо, оскільки нумерація змінних не впливає на схему побудови $g(x, y)$ – підставимо у $f(x_1, x_2, x_3, x_4)$ змінну x замість x_1, змінну y замість x_3 та x_4; замість змінної x_2, яка не входить до обраного кон'юнкта E, підставимо 0:

$$g(x, y) = f(x, 0, y, y) = x \oplus y \oplus xyy \oplus 0 \cdot yy \oplus x \cdot 0 \cdot yy = x \oplus y \oplus xy.$$

Згідно з позначеннями розкладу (4.2), отримуємо: $a = 0$, $a_1 = 1$, $a_2 = 1$. Для побудови кон'юнкції із функції $g(x, y)$ і $\overline{x}$ за розкладом (4.3) обчислимо константи γ, γ_1 і γ_2:

$$\gamma_1 = a_2 = 1;\ \gamma_2 = a_1 = 1;\ \gamma = a \oplus a_1 a_2 = 1,$$

звідки остаточно отримуємо:

$$x \wedge y = g(x \oplus 1, y \oplus 1) \oplus 1 = \overline{g(\overline{x}, \overline{y})} = \overline{\overline{x} \oplus \overline{y} \oplus \overline{x} \cdot \overline{y}}.$$

4.3. Критерій функціональної повноти

Теорема 4.6. *Клас булевих функцій $K \subset P_2$ є функціонально повним тоді і тільки тоді, коли K не є підмножиною жодного із п'яти класів T_0, T_1, M, S, L:*

$$([K] = P_2) \Leftrightarrow \begin{cases} K \not\subset T_0; \\ K \not\subset T_1; \\ K \not\subset M; \\ K \not\subset S; \\ K \not\subset L. \end{cases}$$

Доведення. Необхідність. Припустимо, що $K \subset T_0$. Тоді із замкненості класу T_0 отримуємо: $[K] \subset [T_0] = T_0$. Але $T_0 \neq P_2$ (наприклад, $\overline{x} \notin T_0$), звідки отримуємо, що умова $K \not\subset T_0$ необхідна для повноти класу K. Аналогічно, класи T_1, M, S, L замкнені, і жоден з них не збігається з P_2 ($\overline{x} \notin T_1$; $\overline{x} \notin M$; $x \wedge y \notin S$; $x \wedge y \notin L$), звідки отримуємо необхідність для повноти K умов $K \not\subset T_1$; $K \not\subset M$; $K \not\subset S$; $K \not\subset L$.

Достатність. Нехай виконуються умови $K \not\subset T_0$; $K \not\subset T_1$; $K \not\subset M$; $K \not\subset S$; $K \not\subset L$. Це означає, що клас K містить функції $f_{T_0} \notin T_0$; $f_{T_1} \notin T_1$;

$f_M \notin M$; $f_S \notin S$; $f_L \notin L$. Підкреслимо, що функції f_{T_0}, f_{T_1}, f_M, f_S, f_L не обов'язково попарно різні. Так, клас K може містити кон'юнкцію, яка не міститься у класах S та L, і її можна взяти за f_S та f_L. Більше того, стрілка Пірса $x \downarrow y = \overline{x \vee y}$ не міститься в жодному із п'яти вказаних класів, тобто, якщо $x \downarrow y \in K$, стрілку Пірса можна взяти за кожну із функцій f_{T_0}, f_{T_1}, f_M, f_S, f_L.

Тепер для доведення повноти K достатньо реалізувати $x \wedge y$ та $\overline{x}$ суперпозиціями функцій $f_{T_0}, f_{T_1}, f_M, f_S, f_L \in K$, оскільки набір $\{x \wedge y, \overline{x}\}$ функціонально повний (див. приклад 4.5). Спочатку отримаємо константи 0 і 1 та функцію $\overline{x}$ із функцій $f_{T_0}, f_{T_1}, f_M, f_S$ (нелінійна функція на цьому етапі не знадобиться), для чого розглянемо окремо два випадки.

1. Нехай $f_{T_0} \in T_1$; $f_{T_1} \in T_0$, тобто обидві функції f_{T_0} та f_{T_1} не зберігають однієї з констант і зберігають іншу. У цьому випадку, згідно з лемою про функцію, що не зберігає константу, із функцій f_{T_0} та f_{T_1} отримуємо константи 0 та 1:

$$\begin{cases} f_{T_0} \notin T_0 \\ f_{T_0} \in T_1 \end{cases} \Rightarrow \quad 1 \in [\{f_{T_0}\}]; \qquad \begin{cases} f_{T_1} \notin T_1 \\ f_{T_1} \in T_0 \end{cases} \Rightarrow \quad 0 \in [\{f_{T_1}\}].$$

Тепер $\overline{x}$ можна отримати за лемою про немонотонну функцію: $\overline{x} \in [\{f_M, 0, 1\}]$.

2. Нехай $f_{T_0} \notin T_1$ або $f_{T_1} \notin T_0$, тобто принаймні одна із функцій f_{T_0} або f_{T_1} не зберігає обидві константи. Тоді, за лемою про функцію, що не зберігає константу, можемо отримати $\overline{x}$, використовуючи f_{T_0} або f_{T_1}:

$$\begin{cases} f_{T_0} \notin T_0 \\ f_{T_0} \notin T_1 \end{cases} \Rightarrow \quad \overline{x} \in [\{f_{T_0}\}] \quad \text{або} \quad \begin{cases} f_{T_1} \notin T_0 \\ f_{T_1} \notin T_1 \end{cases} \Rightarrow \quad \overline{x} \in [\{f_{T_1}\}].$$

Тепер можна отримати константи 0 та 1 за лемою про несамодвоїсту функцію: $0, 1 \in [\{f_S, \overline{x}\}]$.

Отже, в обох випадках із функцій $f_{T_0}, f_{T_1}, f_M, f_S$ отримуємо 0, 1 та $\overline{x}$. Тепер $x \wedge y$ можна отримати за лемою про нелінійну функцію: $x \wedge y \in [\{f_L, \overline{x}, 0\}]$. Теорему доведено. $\square$

Зауваження 4.4. Очевидно, що для будь-якого функціонально повного набору $K \subset P_2$ існує функціонально повний піднабір $K_1 \subset K$, який містить не більше ніж п'ять функцій. Насправді завжди можна знайти функціонально повний піднабір, що містить не більш ніж чотири функції, оскільки для доведення повноти в одному випадку знадобилась немонотонна функція, а в другому – несамодвоїста.

Приклад 4.20. 1. Дослідимо на функціональну повноту набір функцій $\{\to, \oplus\}$. Для зручності побудуємо таблицю належності цих функцій до класів T_0, T_1, M, S, L (табл. 4.3).

Таблиця 4.3

	T_0	T_1	M	S	L
$\to$	$-$	$+$	$-$	$-$	$-$
$\oplus$	$+$	$-$	$-$	$-$	$+$

Належність чи неналежність функції до функціонального класу позначено відповідно символами «$+$» та «$-$». Такі таблиці називають *таблицями Поста*. Видно, що кожен стовпець таблиці містить принаймні один «$-$», тобто набір $\{\to, \oplus\}$ не є підмножиною жодного із п'яти класів T_0, T_1, M, S, L, а отже є функціонально повним.

2. Дослідимо на функціональну повноту набір $\{\to, \leftrightarrow\}$. Побудуємо таблицю Поста для функцій цього набору (табл. 4.4).

Таблиця 4.4

	T_0	T_1	M	S	L
$\to$	$-$	$+$	$-$	$-$	$-$
$\leftrightarrow$	$-$	$+$	$-$	$-$	$+$

Набір $\{\leftrightarrow, \oplus\}$ є підмножиною класу T_1, а отже не є функціонально повним. Так, із цього набору не можна отримати константи 0, функції $\overline{x}$, і взагалі жодної функції, яка не належить T_1.

3. Набір $\{x \downarrow y\}$ є функціонально повним, оскільки стрілка Пірса не належить жодному із класів T_0, T_1, M, S, L (табл. 4.5). Аналогічно, повним є набір $\{x|y\}$, що містить лише штрих Шеффера.

Таблиця 4.5

	T_0	T_1	M	S	L
$\downarrow$	$-$	$-$	$-$	$-$	$-$

У наш час теорія функціональної повноти узагальнена на функції $f : \{0, 1, \ldots, k-1\}^{\times n} \to \{0, 1, \ldots, k-1\}$ (k-значна логіка), множину таких функцій позначають через P_k; критерії функціональної повноти у P_k досліджуються, наприклад, в [7].

Список літератури

1. Кук Д. Компьютерная математика [Текст] / Д. Кук, Г. Бейз. – М.: Наука, 1990. – 384 с. – 23000 экз. – ISBN 5-02-014216-6.
2. Курош А. Г. Лекции по общей алгебре [Текст] / А. Г. Курош. – М.: Физматлит, 1973. – 400 с. – 30000 экз.
3. Скорняков Л. А. Элементы теории структур [Текст] / Л. А. Скорняков. – М.: Наука, 1970. – 148 с. – 12000 экз.
4. Биркгоф Г. Теория решеток [Текст] / Г. Биркгоф. – М.: Наука, 1984. – 568 с. – 9400 экз.
5. Яглом И. М. Булева структура и ее модели [Текст] / И. М. Яглом. – М.: Сов. радио, 1980. – 192 с. – 25000 экз.
6. Владимиров Д. А. Булевы алгебры [Текст] / Д. А. Владимиров. – М.: Наука, 1969. – 320 с. – 15000 экз.
7. Яблонский С. В. Введение в дискретную математику [Текст] / С. В. Яблонский. – М.: Наука, 1986. – 384 с. – 30000 экз.
8. Бондаренко М. Ф. Дискретна математика [Текст] / М. Ф. Бондаренко, Н. В. Білоус, А. Г. Руткас. – Харків: «Компанія СМІТ», 2004. – 480 с. – 1000 пр. – ISBN 966-8530-10-1.
9. Донской В. И. Дискретная математика [Текст] / В. И. Донской. – Симферополь: СОНАТ, 2000. – 360 с. – 5000 экз. – ISBN 966-7347-42-7.

10. Яблонский С. В. Функции алгебры логики и классы Поста [Текст] / С. В. Яблонский, Г. П. Гаврилов, В. Б. Кудрявцев. – М.: Наука, 1966. – 119 с.
11. Марченков С. С. Замкнутые классы булевых функций [Текст] / С. С. Марченков. – М.: Физматлит, 2000. – 128 с. – 1000 экз. – ISBN 5-9221-0066-1.
12. Гаврилов Г. П. Задачи и упражнения по дискретной математике [Текст] / Г. П. Гаврилов, А. А. Сапоженко. – М.: Физматлит, 2005. – 416 с. – ISBN 5-9221-0477-2.

Покажчик термінів